



Fortgeschrittene Konzepte und Verfahren von AMS

AMS-Benutzerhandbuch für Fortgeschrittene



Version October 3, 2025

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AMS-Benutzerhandbuch für Fortgeschrittene: Fortgeschrittene Konzepte und Verfahren von AMS

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, die Kunden zu verwirren oder Amazon in einer Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Managed Services?	1
Informationen zu diesem Handbuch	2
Betriebspläne	2
Beschleunigen Sie den Betriebsplan	3
Erweiterter Betriebsplan	3
Erste Schritte	4
Wichtige Begriffe	4
Service description (Service-Beschreibung)	11
Funktionen des erweiterten Betriebsplans AMS von AWS Managed Services (AMS)	11
Was wir tun, was wir nicht tun	17
AMS-Verantwortungsmatrix (RACI)	18
Grundkomponenten der AMS-Umgebung	42
AMS-Kontolimits	45
AMS-Servicelevel-Ziele (SLOs)	48
Unterstützte AWS Dienste	49
Unterstützte Konfigurationen	52
Nicht unterstützte Betriebssysteme	55
Erweiterte AMS-Schnittstellen	56
VPC-Endpunkte	57
AMS-geschützte Namespaces	58
Reservierte AMS-Präfixe	60
AMS-Wartungsfenster	61
AMS-Informationsressourcen	61
AMS-Konformität	62
Von AMS unterstützte Compliance-Standards	62
Gemeinsame Verantwortlichkeit	67
AMS Amazon-Maschinenbilder (AMIs)	67
Verbesserte Sicherheit AMIs	70
So funktioniert die Integration zwischen AD FS und AMS	70
Von AMS verwaltetes Active Directory	72
Bereitstellungen von Anwendungen	75
Serviceverwaltung	77
Kontoverwaltung	77
Beginn des Dienstes	78

Kundenbeziehungsmanagement (CRM)	79
CRM-Prozess	79
CRM-Besprechungen	80
Vereinbarungen für CRM-Treffen	81
Monatliche CRM-Berichte	82
Kostenoptimierung	83
Framework zur Kostenoptimierung	83
Verantwortungsmatrix für die Kostenoptimierung	86
Servicezeiten	88
Hilfe erhalten	89
Verwaltung geplanter Ereignisse	90
AMS PEM-Kriterien	90
Arten von PEM	90
Der AMS PEM-Prozess	91
PEM FAQs	91
Netzwerkarchitektur	93
MALZ Netzwerkarchitektur	93
Über die Landezone-Netzwerkarchitektur mit mehreren Konten	93
Wählen Sie ein MALZ oder mehrere MALZs	96
Landing Zone-Konten mit mehreren Konten	101
SALZ Netzwerkarchitektur	138
AMS landing zone Shared Services mit einem Konto	139
AMS einrichten	140
AMS-Standardeinstellungen	141
Standardeinstellungen für die DNS-Auflösung (MALZ)	141
EC2 IAM-Instanzprofil	142
Warnmeldungen aus der Basisüberwachung in AMS	152
Standardeinstellungen für die Aufbewahrung und Rotation von Protokollen	171
Verwendung der AMS-Konsolen	172
Verwenden der AMS-API und CLI	174
AMS-API-HTTP-Endpunkte für REST-Aufrufe	174
Installation oder Aktualisierung der AMS-CLI	174
Verwenden der AMS-API in CLI, Ruby, Python und Java	176
AMS bring dein eigenes EPS mit	186
Aktivieren Sie BYOEPS für Ihr Konto	188
Empfangen von AMS-Benachrichtigungen	191

AMS AMI-Benachrichtigungen mit SNS	192
Servicebenachrichtigungen	196
Benachrichtigungen über RFC-Statusänderungen	197
Privates und öffentliches DNS einrichten	201
Verwaltung des Ausgangsverkehrs mit AMS	202
Bereitstellung von IAM-Ressourcen	204
Automatisierte IAM-Bereitstellung	205
Berechtigungen mit IAM-Rollen und -Profilen einrichten	232
Eine neue IAM-Benutzerrolle oder ein neues Instance-Profil anfordern	232
Beschränken Sie Berechtigungen mit IAM-Rollenrichtlinienerklärungen	233
Beschränken Sie Berechtigungen mit Amazon EC2 IAM-Instanzprofilen	234
AD FS-Anspruchsregel und SAML-Einstellungen	235
Konfigurationen von ADFS-Anspruchsregeln	235
Web-Konsole	236
API- und CLI-Zugriff mit SAML	236
Mit Netzwerk-ACL einschränken	240
AMS auf Outposts	241
AWS Outposts Installations- und Betriebsmanagement	241
Bereitstellung von AMS-verwalteten Ressourcen auf AWS Outposts	244
Einschränkungen von AMS bei AWS Outposts	245
AMS zur Einhaltung gesetzlicher Vorschriften AWS Outposts	246
AMS ist aktiviert AWS Outposts FAQs	247
Verwenden von Markierungen	249
Automatisches Tagging der AMS-Infrastruktur	251
Von AMS empfohlene Tags	252
Notizen zu Massenaktualisierungen taggen	257
Ressourcenplaner	259
Resource Scheduler bereitstellen	260
Resource Scheduler anpassen	260
Resource Scheduler verwenden	261
Kostenschätzer für AMS Resource Scheduler	262
Bewährte Methoden für AMS Resource Scheduler	263
AWS Systems Manager in AMS Advanced	265
Verfügbare AMS Advanced SSM-Dokumente	266
AMS Advanced SSM-Dokumentversionen	266
Systems Manager-Preise	267

Offboard-AMS-Konten	267
Offboard von landing zone Zone-Konten mit einem Konto	268
Offboarding von Landingzone-Konten mit mehreren Konten	273
Verwaltungsmodi ändern	295
Übersicht der Modi	296
Arten von Modi und Konten in AMS	297
AMS-Modi und Anwendungen oder Workloads	301
Anwendungsfälle für AMS-Modi in der realen Welt	309
RFC-Modus	312
Erfahre mehr über RFCs	313
Was sind Änderungstypen?	355
Behebung von RFC-Fehlern	369
Direkter Änderungsmodus	380
Erste Schritte mit dem Direct Change-Modus	381
Sicherheit und Compliance	384
Änderungsmanagement im Direct Change-Modus	390
Stapel im Direct Change-Modus erstellen	392
Anwendungsfälle für den Direct Change Mode	395
Entwicklermodus	396
Erste Schritte mit dem Entwicklermodus	397
Sicherheits und Compliance	400
Änderungsmanagement	401
Bereitstellen der Infrastruktur	408
Detektivische Kontrollen	408
Protokollierung, Überwachung und Ereignisverwaltung	408
Vorfalmanagement	409
Patch-Management	409
Kontinuitätsmanagement	409
Sicherheits- und Zugriffsmanagement	410
Self-Service-Bereitstellungsmodus in AMS	410
Erste Schritte mit dem SSP-Modus in AMS	411
Amazon API Gateway	412
Alexa for Business	413
Amazon AppStream 2.0	414
Amazon Athena	417
Amazon Bedrock	418

Amazon CloudSearch	420
Amazon CloudWatch Synthetics	421
Amazon Cognito	422
Amazon Comprehend	424
Amazon Connect	425
Amazon Data Firehose	427
DevOpsAmazon-Guru	428
Amazon DocumentDB (mit MongoDB-Kompatibilität)	429
Amazon-DynamoDB	431
Amazon Elastic Container Registry	432
EC2 Image Builder	433
Amazon ECS auf AWS Fargate	435
Amazon EKS auf AWS Fargate	438
Amazon EMR	441
Amazon EventBridge	445
Amazon Forecast	447
Amazon FSx	450
Amazon FSx für OpenZFS	452
Amazon FSx für NetApp ONTAP	453
Amazon Inspector Classic	455
Amazon Kendra	456
Amazon Kinesis Data Streams	457
Amazon Kinesis Video Streams	458
Amazon Lex	459
Amazon MQ	460
Amazon Managed Service für Apache Flink	462
Amazon Managed Streaming für Apache Kafka	463
Amazon Managed Service für Prometheus	464
Amazon Personalize	465
Amazon QuickSight	468
Amazon Rekognition	470
Amazon SageMaker KI	471
Amazon Simple Email Service	475
Amazon Simple Workflow Service	476
Amazon Textract	477
Amazon Transcribe	478

Amazon WorkSpaces	479
AMS Code-Dienste	482
AWS Amplify	485
AWS AppSync	486
AWS App Mesh	487
AWS Audit Manager	488
AWS Batch	490
AWS Certificate Manager	491
AWS Private Certificate Authority	492
AWS CloudEndure	495
AWS CloudHSM	497
AWS CodeBuild	498
AWS CodeCommit	500
AWS CodeDeploy	502
AWS CodePipeline	503
AWS Compute Optimizer	505
AWS DataSync	506
AWS Device Farm	508
AWS Elastic Disaster Recovery	509
AWS Elemental MediaConvert	510
AWS Elemental MediaLive	511
AWS Elemental MediaPackage	512
AWS Elemental MediaStore	513
AWS Elemental MediaTailor	514
AWS Global Accelerator	515
AWS Glue	516
AWS Lake Formation	518
AWS Lambda	520
AWS License Manager	521
AWS Migration Hub	522
AWS Outposts	523
AWS Resilience Hub	524
AWS Secrets Manager	525
AWS Security Hub CSPM	529
AWS Service Catalog AppRegistry	529
AWS Shield	530

AWS Snowball Edge	532
AWS Step Functions	533
AWS Systems Manager Parameter speichern	534
AWS Systems Manager -Automatisierung	536
AWS Transfer Family	540
AWS Transit Gateway	541
AWS WAF	542
AWS Well-Architected Tool	544
AWS X-Ray	545
VM Import/Export	546
Vom Kunden verwalteter Modus	547
Erste Schritte mit dem vom Kunden verwalteten Modus	548
AMS- und AWS Service Catalog	548
Erste Schritte mit Service Catalog	549
Service Catalog in AMS, bevor Sie beginnen	549
Finden Sie die Daten, die Sie benötigen (SKMS)	554
Was ist Service-Wissensmanagement?	554
Finden Sie VPC IDs	555
Subnetz finden IDs	557
Finde AMI IDs	560
Finden Sie die Sicherheitsgruppe (SG) IDs	561
Finden Sie IAM-Entitäten	562
Finden Sie den Stapel IDs	563
Suchen Sie nach Instanzen IDs oder IP-Adressen	565
Finden ARNs	567
Finden Sie Ressourcen nach ARN	569
Suchen Sie nach Kontoeinstellungen	570
Finden FQDNs	572
Finden Sie Verfügbarkeitszonen (AZs)	573
Finden Sie SNS-Themen	574
Suchen Sie nach Backup-Einstellungen	574
Zugriffsverwaltung	576
Was ist Access Management?	576
Warum und wann greifen wir auf Ihr Konto zu	577
Wie und wann benutzt man Root	582
AMS Advanced-Konsole und EC2 Amazon-Zugriff	583

Zugriff auf die AWS Management-Konsole und die AMS-Konsole	584
Temporärer Zugriff auf die AMS-Konsole	584
Zugreifen auf Instanzen mithilfe von Bastionen	585
DNS-freundliche Bastionsnamen	587
Kosteneinsparung bei Bastionen in der Single-Account-Landezone (SALZ)	588
Verwendung von Bastion-IP-Adressen	589
Beispiele für den Instanzzugriff	590
Team- oder rollenbasierte Zugriffskontrolle in einem AMS-Konto	601
Automatisierte EC2 Instanzkonfiguration	602
Voraussetzungen für die automatisierte Instanzkonfiguration	602
Automatische Installation des SSM-Agenten	603
Voraussetzungen	603
Fordern Sie die automatische Installation des SSM-Agenten an	604
So funktioniert die automatische Installation des SSM-Agenten	605
Automatisierte Änderungen	605
Automatisches Aktualisieren von Code auf Linux-Instances	605
Automatisches Aktualisieren von PBIS auf Linux-Instances	606
Automatisches Aktualisieren der Mindestversion von SSM und Agenten CloudWatch	607
CloudWatch Konfigurationsdateien, Aktualisierungsdetails	608
Automatisch konfigurierte Protokolle	609
Überwachung und Veranstaltungsmanagement	611
Was ist Überwachung?	612
Was überwacht das AMS-Überwachungssystem?	613
Proaktive Überwachung des Active Directory-Vertrauens durch die Landing Zone mit einem einzigem Konto	614
So funktioniert die Überwachung	614
EC2 Benachrichtigungen, gruppiert nach Instanzen	616
Tag-basierte Warnmeldung	617
Die Überwachungskonfiguration für ein Konto anzeigen	618
Änderung der Überwachungskonfiguration für ein Konto	619
Benachrichtigungen über anwendungsbezogene Vorfälle in AMS	619
Bereitstellung AppRegistry in Ihrem AMS-Konto und Erstellung von Anwendungen	620
Erstellen Sie Tags, um die Anreicherung von Kundenvorgängen zu ermöglichen	620
Passen Sie den Schweregrad der AMS-Supportfälle für Ihre Anwendungen an	621
Überprüfen Sie die erforderlichen Berechtigungen	622
Benutzen OpsCenter	622

Warnmeldungen	623
Empfangen von Benachrichtigungen	623
Tag-basierte Warnmeldungen	624
Automatische AMS-Behebung von Warnmeldungen	625
Zusätzliche CloudWatch Alarme erstellen	634
Erstellung benutzerdefinierter CloudWatch Metriken und Alarme	636
Verwenden von CloudWatch Application Insights für .Net und SQL Server	637
AMS-Ereignisrouter	638
Von AMS bereitgestellte Amazon EventBridge Managed Rules	639
Verwaltete Regeln für AMS erstellen	639
Verwaltete Regeln für AMS bearbeiten	639
Verwaltete Regeln für AMS löschen	639
Vertrauenswürdiger Remediator	640
Wichtigste Vorteile	640
Wie funktioniert Trusted Remediator	641
Wichtige Begriffe	641
Beginnen Sie mit Trusted Remediator	643
Unterstützte Compute Optimizer Optimizer-Empfehlungen	646
Unterstützte Prüfungen Trusted Advisor	651
Konfigurieren Sie die Problembehebung	715
Entscheidungsworkflow für den Ausführungsmodus	720
Tutorials zur Problembehebung konfigurieren	720
Arbeiten Sie mit Abhilfemaßnahmen	723
Behebungsprotokolle	727
Bewährte Methoden	730
FAQs	730
Verwaltung von Protokollen	734
Was ist Protokollverwaltung?	734
So funktioniert die AMS-Protokollierung	734
Zugriff auf Ihre Logs	735
Aggregierte AMS-Serviceprotokolle	735
Protokolle für gemeinsame Dienste von AMS	751
Amazon Elastic Compute Cloud (Amazon EC2) — Protokolle auf Systemebene	754
Integration mit Splunk	756
Anpassung Ihrer Log-Konfiguration	756
Änderung der CloudWatch Protokollspeicherung	756

Protokollierung für unterstützte Dienste aktivieren	757
Sicherheitsmanagement	758
Datenschutz in AMS	758
Amazon Macie	759
GuardDuty	761
DNS-Firewall mit Amazon Route 53-Resolver	764
AWS Certificate Manager (ACM) -Zertifikat	766
Datenverschlüsselung in AMS	766
Identitäts- und Zugriffsverwaltung	768
IAM-Sicherheitsvorkehrungen für die Multi-Account Landing Zone (MALZ)	768
Authentifizierung mit Identitäten	769
Protokollierung und Überwachung von Sicherheitsereignissen	791
Endpunktsicherheit (EPS)	791
Prozess zur Abwehr von Schadsoftware	796
Amazon Inspector-Sicherheit	798
Reaktion auf AMS-Vorfälle	800
Compliance-Validierung	801
Die Landing Zone für mehrere Konten zeigt den Compliance-Status Ihres AWS-Config-Regeln	801
Einschränkungen der Richtlinien für die Kontrolle des AMS-Landezonendienstes für mehrere Konten	802
Ausfallsicherheit	803
Sicherheit der Infrastruktur	803
Bewährte Methoden für die Gewährleistung der Sicherheit	836
Nicht standardmäßige EPS-Einstellungen für die AMS-Landingzone mit mehreren Konten ..	836
AMS-Leitplanken	837
Richtlinien zur Steuerung des MALZ-Service	837
Reaktion auf Sicherheitsvorfälle	837
Funktionsweise	838
Vorbereitung	839
Detect	840
Analysieren	841
Enthalten	842
Ausrotten	844
Wiederherstellung	845
Bericht nach dem Vorfall	845

Runbooks zur Reaktion auf Sicherheitsvorfälle	846
Sicherheitsüberprüfungen für Änderungsanfragen in AMS Advanced	852
Prozess des Kundensicherheitsrisikomanagements	853
AMS Fortgeschrittene technische Standards	854
Standardsteuerungen in AMS Advanced	854
Änderungen, die hohe oder sehr hohe Sicherheitsrisiken in Ihrer Umgebung mit sich bringen	882
Kontinuitätsmanagement	886
Was ist Kontinuitätsmanagement?	886
So funktioniert Kontinuitätsmanagement	886
Backup-Pläne	887
Backup-Tresore	890
Arten von Backup-Änderungen	892
Überwachung und Berichterstattung für Backups	892
Reaktion auf die Notfallwiederherstellung	893
Planung der Notfallwiederherstellung	893
An mehreren Standorten oder hochverfügbar (HA)	894
Warmer Bereitschaftsmodus	895
Pilot light	896
Sicherung und Wiederherstellung	897
Patch-Management	903
AMS Patch Orchestrator: ein tagbasiertes Patching-Modell	905
Verwenden von Patch Orchestrator	906
Voraussetzungen für Patch Orchestrator	910
Fenster patchen	911
Patch-Benachrichtigungen	912
Patch-Baselines	915
Für Patch Orchestrator reservierte Tags	915
Patchen auf Abruf	916
AMS-Standard-Patching	916
Unterstützte Betriebssysteme	917
Unterstützte Patches	918
Patching und Infrastrukturdesign	921
So funktioniert das AMS-Standard-Patching	921
Fehler beim AMS-Standard-Patchen	927
Aktionen, die Sie beim AMS-Standard-Patching ergreifen können	927

AMS-Standard-Patching FAQs	931
Serviceverpflichtungen für Patches	933
Standard-Patching	934
Kritisches Patchen	936
Berichte und Optionen	940
Berichte auf Anfrage	940
AMS-Patchberichte	941
AMS Backup-Berichte	950
Berichte von Top Talkers zur Vermeidung von Vorfällen und Überwachung	953
Bericht „Einzelheiten zu Abrechnungsgebühren“	955
Trusted Remediator-Berichte	956
Self-Service-Berichte	960
Interne API-Operationen	961
Patch-Bericht (täglich)	964
Backup-Bericht (täglich)	974
Zwischenfallbericht (wöchentlich)	978
Abrechnungsbericht (monatlich)	982
Aggregierte Berichte	985
Dashboards für AMS-Selfservice-Berichte	987
Datenaufbewahrungsrichtlinie	995
Offboard von SSR	996
Holen Sie sich Unterstützung	997
Vorfallmanagement	997
Was ist Incident Management?	999
Verpflichtungen im Bereich Incident Management	1000
Beispiele für das Incident-Management	1004
Verwaltung von Serviceanfragen	1010
Wann sollte eine Serviceanfrage verwendet werden	1011
So funktioniert die Verwaltung von Serviceanfragen	1012
Eine Serviceanfrage testen	1013
Eine Serviceanfrage erstellen	1013
Überwachung und Aktualisierung von Serviceanfragen	1016
Beantwortung von AMS-generierten Serviceanfragen	1018
Fragen zur Abrechnung	1018
Betrieb auf Abruf	1019
AMS Operations on Demand anfordern	1030

Änderungen an den Operations on Demand-Angeboten vornehmen	1031
Dokumentverlauf	1032
Frühere Aktualisierungen	1051
.....	mlxxxiv

Was ist AWS Managed Services?

Willkommen bei AWS Managed Services (AMS), dem Infrastrukturbetriebsmanagement für Amazon Web Services (AWS). AMS ist ein Unternehmensservice, der die kontinuierliche Verwaltung Ihrer AWS Infrastruktur ermöglicht.

Dieses Benutzerhandbuch richtet sich an IT- und Anwendungsentwickler. Grundkenntnisse in Bezug auf IT-Funktionalität, Netzwerke und Anwendungsbereitstellung werden vorausgesetzt.

AMS implementiert bewährte Verfahren und wartet Ihre Infrastruktur, um Ihren betrieblichen Aufwand und Ihr Risiko zu reduzieren. AMS bietet Services über den gesamten Lebenszyklus für die Bereitstellung, den Betrieb und den Support Ihrer Infrastruktur und automatisiert allgemeine Aktivitäten wie Änderungsanforderungen, Überwachung, Patch-Management, Sicherheit und Backup-Services. AMS setzt Ihre Unternehmens- und Sicherheitsinfrastrukturrichtlinien durch und ermöglicht es Ihnen, Lösungen und Anwendungen mit Ihrem bevorzugten Entwicklungsansatz zu entwickeln.

Sehen Sie sich [diese Diagramme](#) an, um die AMS-Architektur besser zu verstehen.

Themen

- [Über dieses AMS-Benutzerhandbuch](#)
- [AMS-Betriebspläne](#)
- [Erste Schritte mit AWS Managed Services](#)
- [Die wichtigsten Begriffe von AMS](#)
- [Service description \(Service-Beschreibung\)](#)
- [AMS-Informationsressourcen](#)
- [AMS-Konformität](#)
- [AMS Amazon-Maschinenbilder \(AMIs\)](#)
- [So funktioniert die Integration zwischen AD FS und AMS](#)
- [Von AMS verwaltetes Active Directory](#)
- [Bereitstellungen von AMS-Anwendungen](#)

 Note

Neue AWS-Regionen werden häufig hinzugefügt. Informationen zu den neuesten von AMS unterstützten AWS-Regionen und den neuesten AMS-unterstützten Betriebssystemen finden Sie unter [Unterstützte Konfigurationen](#)
[Weitere Informationen AWS-Regionen finden Sie unter Verwalten. AWS-Regionen](#)

AMS ist bestrebt, unsere Dienstleistungen auf der Grundlage Ihres Feedbacks kontinuierlich zu verbessern. Wir verwenden verschiedene Mechanismen, um Ihnen Self-Service zu ermöglichen, sich wiederholende Aufgaben zu automatisieren, AWS-Services und neue Funktionen zu implementieren, sobald diese veröffentlicht werden. Sie können jederzeit eine AMS-Serviceanfrage einreichen, um neue Funktionen oder Funktionsverbesserungen vorzuschlagen.

Die AMS-Geschäftszeiten sind 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr.

AMS folgt einer Reihe von Methoden für das IT-Servicemanagement (ITSM), die sich darauf konzentrieren, die IT-Services an den Bedürfnissen Ihres Unternehmens auszurichten.

Über dieses AMS-Benutzerhandbuch

Dieses Benutzerhandbuch richtet sich an AMS Advanced-Kunden mit einer landing zone mit mehreren Konten oder mit einem einzigen Konto. Weitere Informationen zu den AMS-Landingzone-Angeboten finden Sie in den [Allgemeinen Geschäftsbedingungen von AMS](#) sowie unter [Multi-Account-Landingzone-Architektur und Single-Account-Landingzone-Architektur](#).

AMS-Betriebspläne

AWS Managed Services (AMS) ist mit zwei Betriebsplänen erhältlich: AMS Accelerate und AMS Advanced. Ein Betriebsplan bietet einen bestimmten Funktionsumfang und hat unterschiedliche Serviceniveaus, technische Fähigkeiten, Anforderungen, Preise und Einschränkungen. Unsere Betriebspläne bieten Ihnen die Flexibilität, für jede Ihrer AWS Workloads die Betriebskapazitäten auszuwählen, die am besten geeignet sind. In diesem Abschnitt werden die Funktionen und Unterschiede sowie die mit den einzelnen Plänen verbundenen Verantwortlichkeiten, Funktionen und Vorteile beschrieben, sodass Sie verstehen, welcher Betriebsplan für Ihre Kunden am besten geeignet ist.

Einen detaillierten Funktionsvergleich der beiden Betriebspläne finden Sie unter [Funktionen von AWS Managed Services](#).

AMS Accelerate-Betriebsplan

AMS Accelerate ist der AMS-Betriebsplan, der Sie beim day-to-day Infrastrukturmanagement Ihrer neuen oder bestehenden AWS Umgebung unterstützt. AMS Accelerate bietet Betriebsdienstleistungen wie Überwachung, Vorfallmanagement und Sicherheit. AMS Accelerate bietet auch ein optionales Patch-Add-on für EC2 Amazon-basierte Workloads, die regelmäßig gepatcht werden müssen.

Mit AMS Accelerate entscheiden Sie, in welchen AWS-Konten AWS-Regionen AMS Accelerate betrieben werden soll, in welchen AWS-Regionen AMS Accelerate betrieben werden soll, welche Add-Ons Sie benötigen und welche Service Level Agreements (SLAs) Sie benötigen. Weitere Informationen finden Sie unter [Verwenden des AMS Accelerate-Betriebsplans](#) und in der [Servicebeschreibung](#).

Erweiterter AMS-Betriebsplan

AMS Advanced bietet Services über den gesamten Lebenszyklus für die Bereitstellung, den Betrieb und den Support Ihrer Infrastruktur. Zusätzlich zu den von AMS Accelerate bereitgestellten Betriebsdiensten umfasst AMS Advanced auch zusätzliche Dienste wie Landezonenmanagement, Infrastrukturänderungen und -bereitstellung, Zugriffsmanagement und Endpunktsicherheit.

AMS Advanced stellt eine landing zone bereit, in die Sie Ihre AWS Workloads migrieren und AMS-Betriebsdienste in Anspruch nehmen können. Unsere verwalteten Landezonen mit mehreren Konten sind mit der Infrastruktur vorkonfiguriert, um Authentifizierung, Sicherheit, Vernetzung und Protokollierung zu erleichtern.

AMS Advanced umfasst auch ein Änderungs- und Zugriffsmanagementsystem, das Ihre Workloads schützt, indem es unbefugten Zugriff oder die Implementierung riskanter Änderungen an Ihrer Infrastruktur verhindert. AWS Kunden müssen mithilfe unseres Change-Management-Systems eine Änderungsanforderung (RFC) erstellen, um die meisten Änderungen in Ihren AMS Advanced-Konten zu implementieren. Sie erstellen RFCs aus einer Bibliothek automatisierter Änderungen, die von unseren Sicherheits- und Betriebsteams vorab geprüft wurden, oder fordern manuelle Änderungen an, die von unserem Betriebsteam geprüft und implementiert werden, wenn sie sowohl als sicher erachtet werden als auch von AMS Advanced unterstützt werden.

AMS Advanced bietet auch andere SLAs. Weitere Informationen finden Sie in der [Servicebeschreibung AWS Managed Services AMS Advanced](#).

Erste Schritte mit AWS Managed Services

Einzelheiten zu den ersten Schritten mit dem AMS-Service für mehrere Konten in der landing zone finden Sie in der Einführung in [AWS Managed Services Onboarding](#). Die beiden Onboarding-Leitfäden enthalten Beschreibungen des Service sowie Fragen, die Sie berücksichtigen sollten, um Ihnen den Einstieg zu erleichtern. Informieren Sie sich unter [AWS Managed Services Resources über den Funktionsumfang](#) und die aktuellen Ressourcen von [AWS Managed Services](#).

Die wichtigsten Begriffe von AMS

- AMS Advanced: Die im Abschnitt „Servicebeschreibung“ der AMS Advanced-Dokumentation beschriebenen Dienste. Siehe [Servicebeschreibung](#).
- AMS Advanced-Konten: AWS Konten, die jederzeit alle Anforderungen der AMS Advanced Onboarding Requirements erfüllen. Informationen zu den Vorteilen von AMS Advanced, Fallstudien und zur Kontaktaufnahme mit einem Vertriebsmitarbeiter finden Sie unter [AWS Managed Services](#).
- AMS Accelerate-Konten: AWS Konten, die jederzeit alle Anforderungen der AMS Accelerate Onboarding-Anforderungen erfüllen. Siehe [Erste Schritte mit AMS Accelerate](#).
- AWS Managed Services: AMS und/oder AMS Accelerate.
- AWS Managed Services Services-Konten: Die AMS-Konten und/oder AMS Accelerate-Konten.
- Kritische Empfehlung: Eine Empfehlung, die im AWS Rahmen einer Serviceanfrage ausgesprochen wurde und Sie darüber informiert, dass Ihre Maßnahmen zum Schutz vor potenziellen Risiken oder Störungen Ihrer Ressourcen oder der AWS-Services Wenn Sie sich entscheiden, einer kritischen Empfehlung bis zum angegebenen Datum nicht zu folgen, tragen Sie die alleinige Verantwortung für alle Schäden, die sich aus Ihrer Entscheidung ergeben.
- Vom Kunden angeforderte Konfiguration: Jede Software, Dienste oder andere Konfigurationen, die nicht identifiziert sind in:
 - Beschleunigen: [Unterstützte Konfigurationen](#) oder [AMS Accelerate; Servicebeschreibung](#).
 - AMS Advanced: [Unterstützte Konfigurationen](#) oder [AMS Advanced; Servicebeschreibung](#).
- Kommunikation mit einem Vorfall: AMS teilt Ihnen einen Incident mit oder Sie beantragen einen Incident bei AMS über einen Incident, der im Support Center für AMS Accelerate und in der AMS Console for AMS erstellt wurde. Die AMS Accelerate Console bietet eine Zusammenfassung der Vorfälle und Serviceanfragen auf dem Dashboard sowie Links zum Support Center für weitere Informationen.

- **Verwaltete Umgebung:** Die AMS Advanced-Konten und/oder die AMS Accelerate-Konten, die von AMS betrieben werden.

Für AMS Advanced gehören dazu Multi-Account-Landingzone-Konten (MALZ) und Single-Account-Landingzone-Konten (SALZ).

- **Startdatum der Abrechnung:** Der nächste Werktag nach Erhalt AWS der in der AWS Managed Services Onboarding-E-Mail angeforderten Informationen. Die AWS Managed Services Onboarding-E-Mail bezieht sich auf die E-Mail, die von Ihnen gesendet wird AWS , um die Informationen zu sammeln, die für die Aktivierung von AWS Managed Services auf Ihren Konten erforderlich sind.

Für Konten, die später von Ihnen registriert wurden, ist das Startdatum der Rechnungsstellung der nächste Tag, an dem AWS Managed Services eine Benachrichtigung über die Aktivierung von AWS Managed Services für das registrierte Konto gesendet hat. Eine Benachrichtigung zur Aktivierung von AWS Managed Services erfolgt in folgenden Fällen:

1. Sie gewähren Zugriff auf ein kompatibles AWS Konto und übergeben es an AWS Managed Services.
 2. AWS Managed Services entwirft und erstellt das AWS Managed Services Services-Konto.
- **Kündigung des Dienstes:** Sie können die AWS Managed Services für alle AWS Managed Services Services-Konten oder für ein bestimmtes AWS Managed Services Services-Konto aus beliebigem Grund kündigen, indem Sie eine Serviceanfrage mit einer Frist von AWS mindestens 30 Tagen angeben. Am Tag der Kündigung des Service können Sie entweder:
 1. AWS übergibt Ihnen die Kontrolle über alle AWS Managed Services Services-Konten oder gegebenenfalls die angegebenen AWS Managed Services Services-Konten oder
 2. Die Parteien entfernen die AWS Identity and Access Management Rollen, die AWS Zugriff gewähren, von allen AWS Managed Services Services-Konten oder den angegebenen AWS Managed Services Services-Konten, sofern zutreffend.
 - **Kündigungsdatum des Dienstes:** Das Kündigungsdatum des Dienstes ist der letzte Tag des Kalendermonats, der auf das Ende der 30-tägigen Kündigungsfrist folgt. Fällt das Ende der erforderlichen Kündigungsfrist nach dem 20. Tag des Kalendermonats, ist das Kündigungsdatum der letzte Tag des folgenden Kalendermonats. Im Folgenden finden Sie Beispielszenarien für Kündigungstermine.
 - Wenn die Kündigung am 12. April erfolgt, endet die Kündigungsfrist von 30 Tagen am 12. Mai. Das Kündigungsdatum des Dienstes ist der 31. Mai.

- Wenn am 29. April eine Kündigungsfrist erteilt wird, endet die Kündigungsfrist von 30 Tagen am 29. Mai. Das Kündigungsdatum des Dienstes ist der 30. Juni.
- Bereitstellung von AWS Managed Services: AWS stellt Ihnen die AWS Managed Services zur Verfügung und Sie können ab dem Startdatum des Services für jedes AWS Managed Services-Konto auf AWS Managed Services zugreifen und diese nutzen.
- Kündigung für bestimmte AWS Managed Services-Konten: Sie können die AWS Managed Services für ein bestimmtes AWS Managed Services Services-Konto aus beliebigem Grund kündigen, indem AWS Sie dies durch eine Serviceanfrage („Anfrage zur Kündigung eines AMS-Kontos“) mitteilen.

Bedingungen für das Incident-Management:

- Ereignis: Eine Änderung in Ihrer AMS-Umgebung.
- Warnung: Immer wenn ein unterstütztes Ereignis einen Schwellenwert AWS-Service überschreitet und einen Alarm auslöst, wird eine Warnung erstellt und eine Benachrichtigung an Ihre Kontaktliste gesendet. Darüber hinaus wird ein Vorfall in Ihrer Incident-Liste erstellt.
- Vorfall: Eine ungeplante Unterbrechung oder Leistungsverschlechterung Ihrer AMS-Umgebung oder AWS Managed Services, die zu einer von AWS Managed Services oder Ihnen gemeldeten Beeinträchtigung führt.
- Problem: Eine gemeinsame Grundursache für einen oder mehrere Vorfälle.
- Lösung eines Vorfalls oder Lösung eines Vorfalls:
 - AMS hat alle nicht verfügbaren AMS-Dienste oder -Ressourcen im Zusammenhang mit diesem Vorfall wieder in den verfügbaren Zustand versetzt, oder
 - AMS hat festgestellt, dass nicht verfügbare Stacks oder Ressourcen nicht auf einen verfügbaren Zustand zurückgesetzt werden können, oder
 - AMS hat eine von Ihnen autorisierte Wiederherstellung der Infrastruktur eingeleitet.
- Reaktionszeit bei Vorfällen: Der Zeitunterschied zwischen dem Zeitpunkt, zu dem Sie einen Vorfall erstellen, und dem Zeitpunkt, zu dem AMS eine erste Antwort über die Konsole, E-Mail, das Service Center oder das Telefon bereitstellt.
- Zeit zur Behebung eines Vorfalls: Der Zeitunterschied zwischen dem Zeitpunkt, zu dem entweder AMS oder Sie einen Vorfall auslösen, und dem Zeitpunkt, zu dem der Vorfall behoben wird.
- Priorität des Vorfalls: Wie Vorfälle von AMS oder von Ihnen als „Niedrig“, „Mittel“ oder „Hoch“ priorisiert werden.
 - Niedrig: Ein unkritisches Problem mit Ihrem AMS-Service.

- Medium: Ein AWS-Service in Ihrer verwalteten Umgebung ist verfügbar, funktioniert aber nicht wie vorgesehen (gemäß der entsprechenden Servicebeschreibung).
- Hoch: Entweder (1) die AMS-Konsole oder ein oder mehrere AMS APIs in Ihrer verwalteten Umgebung sind nicht verfügbar; oder (2) ein oder mehrere AMS-Stacks oder Ressourcen in Ihrer verwalteten Umgebung sind nicht verfügbar und die Nichtverfügbarkeit verhindert, dass Ihre Anwendung ihre Funktion erfüllt.

AMS kann Vorfälle gemäß den oben genannten Richtlinien neu kategorisieren.

- Wiederherstellung der Infrastruktur: Erneutes Bereitstellen vorhandener Stacks auf der Grundlage von Vorlagen der betroffenen Stacks und Initiierung einer Datenwiederherstellung auf der Grundlage des letzten bekannten Wiederherstellungspunkts, sofern von Ihnen nicht anders angegeben, wenn eine Behebung des Vorfalls nicht möglich ist.

Bedingungen für die Infrastruktur:

- Verwaltete Produktionsumgebung: Ein Kundenkonto, in dem sich die Produktionsanwendungen des Kunden befinden.
- Verwaltete Nichtproduktionsumgebung: Ein Kundenkonto, das nur Anwendungen enthält, die nicht zur Produktion gehören, z. B. Anwendungen für Entwicklung und Tests.
- AMS-Stack: Eine Gruppe von einer oder mehreren AWS Ressourcen, die von AMS als eine Einheit verwaltet werden.
- Unveränderliche Infrastruktur: Ein für Amazon EC2 Auto Scaling Scaling-Gruppen (ASGs) typisches Infrastrukturwartungsmodell, bei dem aktualisierte Infrastrukturkomponenten (im AWS AMI) bei jeder Bereitstellung ersetzt werden, anstatt direkt aktualisiert zu werden. Die Vorteile einer unveränderlichen Infrastruktur bestehen darin, dass alle Komponenten synchron bleiben, da sie immer auf derselben Basis generiert werden. Die Unveränderlichkeit ist unabhängig von einem Tool oder Workflow zum Erstellen des AMI.
- Veränderbare Infrastruktur: Ein Infrastrukturwartungsmodell, das typisch für Stacks ist, die keine Amazon EC2 Auto Scaling Scaling-Gruppen sind und eine einzelne Instance oder nur wenige Instances enthalten. Dieses Modell entspricht am ehesten der traditionellen, hardwarebasierten Systembereitstellung, bei der ein System zu Beginn seines Lebenszyklus bereitgestellt wird und dann im Laufe der Zeit Updates auf dieses System übertragen werden. Alle Aktualisierungen des Systems werden einzeln auf die Instanzen angewendet und können aufgrund von Anwendungs- oder Systemneustarts zu Systemausfällen führen (abhängig von der Stack-Konfiguration).

- Sicherheitsgruppen: Virtuelle Firewalls für Ihre Instance zur Steuerung des ein- und ausgehenden Datenverkehrs. Sicherheitsgruppen wirken auf der Instance-Ebene und nicht auf der Subnetzebene. Daher kann jeder Instance in einem Subnetz in Ihrer VPC ein anderer Satz von Sicherheitsgruppen zugewiesen werden.
- Service Level Agreements (SLAs): Teil der AMS-Verträge mit Ihnen, die das erwartete Serviceniveau definieren.
- SLA nicht verfügbar und nicht verfügbar:
 - Eine von Ihnen eingereichte API-Anfrage, die zu einem Fehler führt.
 - Eine von Ihnen eingereichte Konsolenanfrage, die zu einer 5xx-HTTP-Antwort führt (der Server ist nicht in der Lage, die Anfrage auszuführen).
 - Alle AWS-Service Angebote, die Stacks oder Ressourcen in Ihrer von AMS verwalteten Infrastruktur bilden, befinden sich im Status „Serviceunterbrechung“, wie im [Service Health Dashboard](#) angezeigt.
 - Die Nichtverfügbarkeit, die direkt oder indirekt auf einen AMS-Ausschluss zurückzuführen ist, wird bei der Entscheidung über die Inanspruchnahme von Servicegutschriften nicht berücksichtigt. Dienste gelten als verfügbar, sofern sie nicht die Kriterien für die Nichtverfügbarkeit erfüllen.
- Servicelevel-Ziele (SLOs): Teil der AMS-Verträge mit Ihnen, in denen spezifische Serviceziele für AMS-Services definiert werden.

Bedingungen für das Patchen:

- Obligatorische Patches: Wichtige Sicherheitsupdates zur Behebung von Problemen, die den Sicherheitsstatus Ihrer Umgebung oder Ihres Kontos gefährden könnten. Ein „Kritisches Sicherheitsupdate“ ist ein Sicherheitsupdate, das vom Hersteller eines AMS-unterstützten Betriebssystems als „Kritisch“ eingestuft wird.
- Angekündigte oder veröffentlichte Patches: Patches werden in der Regel nach einem bestimmten Zeitplan angekündigt und veröffentlicht. Neue Patches werden angekündigt, wenn festgestellt wird, dass der Patch benötigt wird. In der Regel wird der Patch bald danach veröffentlicht.
- Patch-Add-on: Tag-basiertes Patchen für AMS-Instances, das die AWS Systems Manager (SSM) -Funktionalität nutzt, sodass Sie Instances taggen und diese Instances mithilfe einer Baseline und eines von Ihnen konfigurierten Fensters patchen lassen können.
- Patch-Methoden:
 - In-Place-Patching: Patchen, das durch Ändern vorhandener Instanzen erfolgt.

- AMI-Ersatz-Patching: Patching, das durch Ändern des AMI-Referenzparameters einer vorhandenen EC2 Auto Scaling Scaling-Gruppenstartkonfiguration erfolgt.
- Patch-Anbieter (Betriebssystemanbieter, Drittanbieter): Patches werden vom Anbieter oder vom zuständigen Gremium der Anwendung bereitgestellt.
- Patch-Typen:
 - Kritisches Sicherheitsupdate (CSU): Ein Sicherheitsupdate, das vom Hersteller eines unterstützten Betriebssystems als „Kritisch“ eingestuft wurde.
 - Wichtiges Update (IU): Ein Sicherheitsupdate, das vom Hersteller eines unterstützten Betriebssystems als „wichtig“ eingestuft wurde, oder ein nicht sicherheitsrelevantes Update, das vom Hersteller eines unterstützten Betriebssystems als „Kritisch“ eingestuft wurde.
 - Anderes Update (OU): Ein Update des Herstellers eines unterstützten Betriebssystems, bei dem es sich nicht um eine CSU oder eine IU handelt.
- Unterstützte Patches: AMS unterstützt Patches auf Betriebssystemebene. Upgrades werden vom Anbieter veröffentlicht, um Sicherheitslücken oder andere Fehler zu beheben oder die Leistung zu verbessern. Eine Liste der derzeit unterstützten OSs Konfigurationen finden Sie unter [Support-Konfigurationen](#).

Sicherheitsbedingungen:

- Detective Controls: Eine Bibliothek mit von AMS erstellten oder aktivierten Monitoren, die einen kontinuierlichen Überblick über vom Kunden verwaltete Umgebungen und Workloads für Konfigurationen bieten, die nicht den Sicherheits-, Betriebs- oder Kundenkontrollen entsprechen, und Maßnahmen ergreifen, indem sie Eigentümer benachrichtigen, Ressourcen proaktiv ändern oder beenden.

Bedingungen für Serviceanfragen:

- Serviceanfrage: Eine Anfrage von Ihnen nach einer Maßnahme, die AMS in Ihrem Namen ergreifen soll.
- Warnmeldung: Eine Benachrichtigung, die von AMS auf Ihrer Seite mit der Liste der Serviceanfragen veröffentlicht wird, wenn eine AMS-Warnung ausgelöst wird. Der für Ihr Konto konfigurierte Kontakt wird ebenfalls über die konfigurierte Methode (z. B. E-Mail) benachrichtigt. Wenn Ihre Instanzen/Ressourcen Kontakt-Tags enthalten und Ihrem Cloud Service Delivery Manager (CSDM) Ihre Zustimmung für tagbasierte Benachrichtigungen erteilt haben, werden die

Kontaktinformationen (Schlüsselwert) im Tag auch bei automatisierten AMS-Benachrichtigungen benachrichtigt.

- Servicebenachricht: Eine Mitteilung von AMS, die auf Ihrer Seite mit der Liste Ihrer Serviceanfragen veröffentlicht wird.

Verschiedene Bedingungen:

- AWS Managed Services-Schnittstelle: Für AMS: Die AWS Managed Services Advanced Console, AMS CM API und Support API. Für AMS Accelerate: Die Support Konsole und die Support API.
- Kundenzufriedenheit (CSAT): AMS CSAT verfügt über umfassende Analysen, darunter Bewertungen der Fallkorrespondenz zu jedem Fall oder jeder etwaigen Korrespondenz, vierteljährliche Umfragen usw.
- DevOps: DevOps ist eine Entwicklungsmethodik, die sich nachdrücklich für Automatisierung und Überwachung aller Schritte einsetzt. DevOps zielt auf kürzere Entwicklungszyklen, eine höhere Bereitstellungshäufigkeit und zuverlässigere Releases ab, indem die traditionell getrennten Funktionen von Entwicklung und Betrieb auf einer Grundlage der Automatisierung zusammengeführt werden. Wenn Entwickler den Betrieb verwalten können und der Betrieb die Entwicklung beeinflusst, können Probleme und Probleme schneller entdeckt und gelöst werden, und Geschäftsziele lassen sich leichter erreichen.
- ITIL: Die Information Technology Infrastructure Library (ITIL genannt) ist ein ITSM-Framework, mit dem der Lebenszyklus von IT-Services standardisiert werden soll. ITIL ist in fünf Phasen unterteilt, die den IT-Servicelebenszyklus abdecken: Servicestrategie, Servicedesign, Serviceübergang, Servicebetrieb und Serviceverbesserung.
- IT-Servicemanagement (ITSM): Eine Reihe von Praktiken, die IT-Services auf die Bedürfnisse Ihres Unternehmens abstimmen.
- Managed Monitoring Services (MMS): AMS betreibt sein eigenes Überwachungssystem, den Managed Monitoring Service (MMS), das AWS Gesundheitsereignisse verarbeitet und CloudWatch Amazon-Daten sowie Daten von anderen aggregiert und AMS-Betreiber (rund um die Uhr online) über alle Alarme informiert AWS-Services, die über ein Amazon Simple Notification Service (Amazon SNS) -Thema ausgelöst wurden.
- Namespace: Wenn Sie IAM-Richtlinien erstellen oder mit Amazon Resource Names (ARNs) arbeiten, identifizieren Sie einen AWS-Service mithilfe eines Namespace. Sie verwenden Namespaces bei der Identifikation von Aktionen und Ressourcen.

Service description (Service-Beschreibung)

AMS Advanced (AMS) ist ein Betriebsplan des AWS Managed Services Services-Service zur Verwaltung des Betriebs Ihrer AWS Infrastruktur. AMS Advanced bietet routinemäßige Infrastrukturoperationen wie Patch-, Continuity- und Sicherheitsmanagement sowie IT-Managementprozesse wie Incident-, Change- und Serviceanforderungsmanagement. Eine Liste der unterstützten Services finden Sie unter [Unterstützte AWS Dienste](#).

YouTube Video: [Wie kann AMS mir helfen, betriebliche Exzellenz in der Cloud zu erreichen?](#)

Themen

- [Funktionen des erweiterten Betriebsplans AMS von AWS Managed Services \(AMS\)](#)
- [Was wir tun, was wir nicht tun](#)
- [AMS-Verantwortungsmatrix \(RACI\)](#)
- [Grundkomponenten der AMS-Umgebung](#)
- [AMS-Kontolimits](#)
- [AMS-Servicelevel-Ziele \(SLOs\)](#)
- [Unterstützte AWS Dienste](#)
- [Unterstützte Konfigurationen](#)
- [Funktionen für nicht unterstützte Betriebssysteme in AMS](#)
- [Erweiterte AMS-Schnittstellen](#)
- [AMS VPC-Endpunkte](#)
- [AMS-geschützte Namespaces](#)
- [Reservierte AMS-Präfixe](#)
- [AMS-Wartungsfenster](#)

Funktionen des erweiterten Betriebsplans AMS von AWS Managed Services (AMS)

AMS Advanced bietet die folgenden Funktionen für unterstützte AWS Dienste:

- Protokollierung, Überwachung, Leitplanken und Eventmanagement:

AMS konfiguriert und überwacht Ihre verwaltete Umgebung für die Protokollierung von Aktivitäten und definiert Warnmeldungen auf der Grundlage einer Vielzahl von Zustandsprüfungen.

Warnmeldungen werden von AMS im Hinblick auf entsprechende AWS-Services untersucht, und solche, die sich negativ auf Ihre Nutzung dieser Services auswirken, führen zur Entstehung von Vorfällen. AMS aggregiert und speichert alle Protokolle, die als Ergebnis aller Operationen in CloudWatch CloudTrail, und Systemprotokolle in Amazon S3 generiert wurden. Sie können verlangen, dass zusätzliche Warnmeldungen eingerichtet werden. Zusätzlich zu den präventiven Kontrollen von AMS setzt AMS Konfigurationsleitplanken und Erkennungskontrollen ein, um Sie kontinuierlich vor Fehlkonfigurationen zu schützen, die die Betriebs- und Sicherheitsintegrität der verwalteten Konten beeinträchtigen könnten, und um Ihre Kontrollen wie Tagging und Compliance durchzusetzen. Wenn eine überwachte Steuerung erkannt wird, wird ein Alarm ausgelöst, der auf der Grundlage vordefinierter AMS-Standardwerte, die von Ihnen geändert werden können, zur Benachrichtigung, Änderung oder Kündigung von Ressourcen führt.

- **Kontinuitätsmanagement (Backup und Wiederherstellung):**

AMS bietet Backups von Ressourcen mithilfe der standardmäßigen, vorhandenen AWS-Backup-Funktionalität in einem von Ihnen festgelegten, geplanten Intervall. Wiederherstellungsaktionen aus bestimmten Snapshots können von AMS mit Ihrem RFC ausgeführt werden. Datenänderungen, die zwischen den Snapshot-Intervallen auftreten, liegen in Ihrer Verantwortung für die Sicherung. Sie können außerhalb der geplanten Intervalle einen RFC für Sicherungs- oder Snapshot-Anfragen einreichen. Falls die Availability Zone (AZ) in einer AWS Region nicht verfügbar ist, stellt AMS mit Ihrer Zustimmung die verwaltete Umgebung wieder her, indem neue Stacks auf der Grundlage von Vorlagen und verfügbaren EBS-Snapshots der betroffenen Stacks neu erstellt werden.

- **Sicherheits- und Zugriffsmanagement:**

AMS bietet Endpunktsicherheit (EPS), z. B. die Konfiguration von Viren- und Anti-Malware-Schutz. Sie können auch Ihr eigenes EPS-Tool und Ihre eigenen EPS-Prozesse verwenden und AMS nicht für EPS verwenden, indem Sie die Funktion Bring Your Own EPS (BYOEPS) verwenden. AMS konfiguriert auch AWS Standardsicherheitsfunktionen, die von Ihnen beim Onboarding genehmigt wurden, wie AWS Identity and Access Management (IAM-) Rollen und EC2 Amazon-Sicherheitsgruppen, und verwendet AWS Standardtools (z. B. Amazon Macie AWS Security Hub CSPM, Amazon GuardDuty), um Sicherheitsprobleme zu überwachen und darauf zu reagieren. Sie verwalten Ihre Benutzer über einen von Ihnen bereitgestellten zugelassenen Verzeichnisdienst. Eine Liste der zugelassenen Verzeichnisdienste finden Sie unter [Unterstützte Konfigurationen](#).

AMS umfasst Endpoint Security (EPS), einschließlich Virenschutz (AV), und Anti-Malware-Schutz, Malware und Erkennung von Eindringlingen (Trend Micro). Sicherheitsgruppen werden pro Stack-Vorlage definiert und beim Start je nach Sichtbarkeit der Sicherheitsgruppen der Anwendung (öffentlich/privat) geändert.

Der Zugriff auf Systeme wird über Change Management Requests for change () RFCs angefordert. Die Zugriffsverwaltung bietet Zugriff auf bestimmte Ressourcen wie EC2 Amazon-Instances AWS-Managementkonsole, die und APIs. Nachdem Sie beim Onboarding und beim Zusammenschluss mit AWS eine unidirektionale Vertrauensstellung mit einer AMS Microsoft Active Directory-Bereitstellung eingerichtet haben, können Sie Ihre vorhandenen Unternehmensanmeldedaten für alle Interaktionen verwenden.

- Patch-Verwaltung:

AMS wendet Updates für EC2 Instanzen für unterstützte Betriebssysteme (OSs) und Software an, auf denen unterstützte Betriebssysteme vorinstalliert sind, und installiert diese. Eine Liste der unterstützten Betriebssysteme finden Sie unter [Unterstützte Konfigurationen](#).

AMS bietet zwei Modelle für das Patchen an:

- AMS-Standard-Patch für herkömmliches kontobasiertes Patchen und
- AMS Patch Orchestrator für tagbasiertes Patchen.

Im AMS-Standard-Patch wählen Sie ein monatliches Wartungsfenster, in dem AMS die meisten Patching-Aktivitäten durchführt. AMS installiert wichtige Sicherheitsupdates außerhalb des ausgewählten Wartungsfensters (mit entsprechenden Benachrichtigungen) und wichtige Updates während des ausgewählten Wartungsfensters. AMS aktualisiert die Tools für das Infrastrukturmanagement zusätzlich während des ausgewählten Wartungsfensters. Sie können Stacks vom Patch-Management ausschließen oder Updates ablehnen, wenn Sie möchten.

Mit AMS Patch Orchestrator wird von Ihnen ein standardmäßiges Wartungsfenster pro Konto definiert, in dem AMS Patching-Aktivitäten durchführen kann. Sie können zusätzliche benutzerdefinierte Wartungsfenster für AMS planen, um eine bestimmte, von Ihnen definierte Gruppe von Instanzen mit Tags zu patchen. AMS wendet alle verfügbaren Updates an, aber Sie können Updates filtern oder ablehnen, indem Sie eine benutzerdefinierte Patch-Baseline erstellen. Bei beiden Modellen gilt: Wenn Sie ein unter Patch Management bereitgestelltes Update genehmigen oder ablehnen, es sich aber später anders überlegen, sind Sie dafür verantwortlich, das Update über einen RFC zu initiieren. AMS verfolgt den Patch-Status von Ressourcen und hebt Systeme hervor, die im monatlichen Geschäftsbericht nicht aktuell sind. Das Patch-Management ist auf Stacks in der verwalteten Umgebung beschränkt, einschließlich aller von AMS verwalteten Anwendungen und unterstützten AWS-Services mit Patching-Funktionen (z. B. RDS). Um alle Arten von Infrastrukturkonfigurationen zu unterstützen, wenn ein Update veröffentlicht wird, aktualisiert AMS a) die EC2 Instance und b) stellt Ihnen ein aktualisiertes AMS-AMI zur Verfügung, das Sie verwenden können. Es liegt in Ihrer Verantwortung, alle zusätzlichen Anwendungen

zu installieren, zu konfigurieren, zu patchen und zu überwachen, die oben nicht ausdrücklich behandelt wurden.

- Verwaltung von Änderungen:

Das AMS-Änderungsmanagement ist der Mechanismus, mit dem Sie Änderungen in Ihrer verwalteten Umgebung kontrollieren können. AMS verwendet eine Kombination aus präventiven und detektiven Kontrollen, um diesen Prozess zu vereinfachen, und bietet je nach ausgewähltem AMS-Modus ein unterschiedliches Maß an Kontrolle und damit verbundene Risiken.

Alle Aktionen in Ihrer AMS-Umgebung sind angemeldet AWS CloudTrail.

Weitere Informationen zu AMS Change Management und den verschiedenen Modi finden Sie im [AMS Change Management-Leitfaden](#) und [AMS-Modi](#).

- Automatisiertes Bereitstellungsmanagement und Self-Service-Verwaltung:

Sie können AWS-Ressourcen auf AMS Advanced auf verschiedene Arten bereitstellen:

- Änderungsanträge zur Bereitstellung und Konfiguration einreichen () RFCs
- Bereitstellung über AWS Service Catalog
- Bereitstellung im [Direct Change-Modus](#)
- Bereitstellung im [Entwicklermodus](#). Denken Sie daran, dass die im Entwicklermodus erstellten Ressourcen nicht von AMS verwaltet werden.
- Konfigurieren Sie AWS-Services direkt mithilfe von Self-Service Provisioning für Select AWS-Services (siehe [Unterstützte AWS Dienste](#)).

- Verwaltung von Vorfällen:

AMS benachrichtigt Sie proaktiv über Vorfälle, die von AMS entdeckt wurden. AMS reagiert sowohl auf von Kunden eingereichte als auch auf von AMS generierte Vorfälle und behebt Vorfälle auf der Grundlage der Priorität des Vorfalls. Sofern nicht anders von Ihnen angewiesen, werden Vorfälle, die von AMS als Risiko für die Sicherheit Ihrer verwalteten Umgebung eingestuft werden, sowie Vorfälle im Zusammenhang mit der Verfügbarkeit von AMS und anderen AWS-Services proaktiv behandelt. AMS ergreift Maßnahmen bei allen anderen Vorfällen, sobald Ihre Genehmigung eingegangen ist. Wiederkehrende Vorfälle werden durch den Problemmanagementprozess behoben.

- Problemmanagement:

AMS führt Trendanalysen durch, um Probleme zu identifizieren und zu untersuchen und die Grundursache zu ermitteln. Probleme werden entweder durch eine Behelfslösung oder durch

eine dauerhafte Lösung behoben, die ein erneutes Auftreten ähnlicher future Auswirkungen auf den Service verhindert. Sobald das Problem behoben ist, kann für jeden Vorfall mit hoher Wahrscheinlichkeit ein Bericht nach dem Vorfall (PIR) angefordert werden. Der PIR erfasst die Grundursache und die ergriffenen Präventivmaßnahmen, einschließlich der Umsetzung präventiver Maßnahmen.

- **Berichterstattung:**

AMS stellt Ihnen einen monatlichen Servicebericht zur Verfügung, der die wichtigsten Leistungskennzahlen von AMS zusammenfasst, darunter eine Zusammenfassung und Einblicke, betriebliche Kennzahlen, verwaltete Ressourcen, Einhaltung der AMS Service Level Agreements (SLA) und Finanzkennzahlen zu Ausgaben, Einsparungen und Kostenoptimierung. Die Berichte werden vom AMS Cloud Service Delivery Manager (CSDM) bereitgestellt, der Ihnen zugewiesen wurde.

- **Verwaltung von Serviceanfragen:**

Um Informationen über Ihre verwaltete Umgebung, AMS oder AWS Serviceangebote anzufordern, reichen Sie Serviceanfragen über die AMS-Konsole ein. Sie können eine Serviceanfrage mit Anleitungen zu AWS Diensten und Funktionen oder zur Anforderung zusätzlicher AMS-Services einreichen.

- **Servicedesk:**

AMS besetzt den technischen Betrieb mit Vollzeitmitarbeitern von Amazon, um nicht automatisierte Anfragen zu bearbeiten, einschließlich Incident Management, Service Request Management und Change Management. Der Service Desk ist rund um die Uhr an 365 Tagen im Jahr geöffnet.

- **Vorgesehene Ressourcen:**

Jedem Kunden werden ein Cloud Service Delivery Manager (CSDM) und ein Cloud Architect (CA) zugewiesen.

- CSDMs kann direkt kontaktiert werden. In allen Phasen der Implementierung, der Migration und des betrieblichen Lebenszyklus führen sie Serviceprüfungen durch und bieten Berichte und Einblicke in die Bereitstellung. CSDMs führen monatliche Geschäftsüberprüfungen durch und führen detaillierte Angaben zu finanziellen Ausgaben, Empfehlungen zur Kosteneinsparung, zur Nutzung der Dienste und zur Risikoberichterstattung durch. Sie befassen sich eingehend mit Statistiken zur betrieblichen Leistung und geben Empfehlungen zu Verbesserungsmöglichkeiten.
- CAs können direkt kontaktiert werden und bieten technisches Fachwissen, um Ihnen zu helfen, Ihre AWS Cloud-Nutzung zu optimieren. Zu den Aktivitäten von CA gehören beispielsweise die Auswahl von Workloads für die Migration, die Unterstützung beim Onboarding zusätzlicher

Konten und Workloads, die technische Leitung bei betrieblichen Aktivitäten wie Spieltagen, Notfallwiederherstellungstests, Problemmanagement und technische Beratung, um das Beste aus AMS herauszuholen und. AWS CAs fördern technische Diskussionen auf allen Ebenen Ihres Unternehmens und unterstützen Sie beim Incident-Management, beim Eingehen von Kompromissen, bei der Festlegung von Best Practices und bei der Minimierung technischer Risiken.

- **Entwicklermodus:**

Mit dieser Funktion können Sie Infrastrukturentwürfe und -bereitstellungen innerhalb von AMS-konfigurierten Konten [1] schnell iterieren, indem Sie neben dem Zugriff auf den AMS-Change-Management-Prozess auch direkten Zugriff auf den AWS-Service APIs und die AWS-Konsole gewähren. Ressourcen, die außerhalb des Change-Management-Prozesses mit Berechtigungen im Entwicklermodus bereitgestellt oder konfiguriert wurden, liegen in Ihrer Verantwortung (siehe „Automatisiertes Bereitstellungsmanagement und Self-Service-Bereitstellungsmanagement“). Ressourcen, die über den AMS-Change-Management-Prozess bereitgestellt werden, werden wie andere vom Change Management bereitgestellte Workloads auf AMS unterstützt.

- **AWS-Unterstützung:**

AMS-Kunden können die Stufe des AWS-Supports wählen, die sie zur Ergänzung ihres AMS Operations-Plans benötigen. Bei AMS registrierte Konten können entweder Business Support oder Enterprise Support abonniert werden. Weitere Informationen zu den Unterschieden bei den Supportplänen finden Sie unter [AWS-Supportpläne](#).

- **Vom Kunden verwaltetes Konto:**

Mit dieser Funktion können Sie AWS-Konten in derselben verwalteten Umgebung anfordern, aber der laufende Betrieb von Workloads und AWS-Ressourcen innerhalb dieser Konten liegt in Ihrer Verantwortung. AMS stellt vom Kunden verwaltete Konten bereit, aber sobald die Konten erstellt wurden, werden für diese Konten keine weiteren AMS-Funktionen oder -Services bereitgestellt. AWS registriert keine von Kunden verwalteten Konten für Premium-Support auf Unternehmensebene. Es liegt in Ihrer Verantwortung, kundenverwaltete Konten für den AWS-Support zu dem von Ihnen gewählten Support-Tarif zu registrieren.

- **Firewall-Verwaltung:**

AMS bietet eine optionale verwaltete Firewall-Lösung für unterstützte Firewall-Dienste, die die Filterung von ausgehendem Internetverkehr für Netzwerke in Ihrer verwalteten Umgebung ermöglicht. Davon ausgenommen sind öffentlich zugängliche Dienste, die die AWS-Netzwerkinfrastruktur nicht nutzen und deren Datenverkehr direkt ins Internet geht. Die Lösung

kombiniert branchenführende Firewall-Technologie mit AMS-Infrastrukturmanagementfunktionen zur Bereitstellung, Überwachung, Verwaltung, Skalierung und Wiederherstellung der Firewall-Infrastruktur.

Wenn Sie AMS einbinden, erhalten Sie eine vollständige Liste Ihrer AMS-Netzwerkinfrastruktur. Um jederzeit eine aktualisierte Liste der Dienste zu erhalten, die zur Unterstützung Ihrer AMS-Infrastruktur ausgeführt werden, reichen Sie eine Serviceanfrage mit Einzelheiten zu den gewünschten Informationen ein. Um eine Änderung Ihres Netzwerkdesigns anzufordern, erstellen Sie eine Serviceanfrage, in der die Änderungen beschrieben werden, die Sie vornehmen möchten, z. B. das Hinzufügen einer VPC oder die Anforderung einer Änderung der Sicherheitsgruppenregel.

Was wir tun, was wir nicht tun

AMS bietet Ihnen einen standardisierten Ansatz für die Bereitstellung der AWS-Infrastruktur und bietet das erforderliche kontinuierliche Betriebsmanagement. Eine vollständige Beschreibung der Rollen, Verantwortlichkeiten und unterstützten Services finden Sie in der [Servicebeschreibung](#).

Note

Um AMS aufzufordern, einen zusätzlichen AWS-Service bereitzustellen, reichen Sie eine Serviceanfrage ein. Weitere Informationen finden Sie unter [Serviceanfragen stellen](#).

- Was wir tun:

Nachdem Sie das Onboarding abgeschlossen haben, können Sie in der AMS-Umgebung Änderungsanfragen (RFCs), Incidents und Serviceanfragen entgegennehmen. Ihre Interaktion mit dem AMS-Service dreht sich um den Lebenszyklus eines Anwendungsstapels. Neue Stacks werden anhand einer vorkonfigurierten Liste von Vorlagen bestellt, in bestimmten Virtual Private Cloud (VPC) -Subnetzen gestartet, während ihrer Betriebsdauer durch Änderungsanforderungen (RFCs) geändert und rund um die Uhr auf Ereignisse und Vorfälle überwacht.

Aktive Anwendungs-Stacks werden von AMS überwacht und verwaltet, einschließlich Patches, und erfordern während der gesamten Lebensdauer des Stacks keine weiteren Maßnahmen, es sei denn, eine Änderung ist erforderlich oder der Stack wird außer Betrieb genommen. Von AMS festgestellte Vorfälle, die den Zustand und die Funktion des Stacks beeinträchtigen, wird eine Benachrichtigung generiert. Möglicherweise müssen Sie Maßnahmen ergreifen, um diese zu

beheben oder zu überprüfen. Fragen zu Anleitungen und andere Anfragen können gestellt werden, indem Sie eine Serviceanfrage einreichen.

Darüber hinaus können Sie mit AMS kompatible AWS-Services aktivieren, die nicht von AMS verwaltet werden. Informationen zu AWS-AMS-kompatiblen Diensten finden Sie unter [Self-Service-Bereitstellungsmodus](#).

- Was wir NICHT tun:

AMS vereinfacht zwar die Anwendungsbereitstellung durch die Bereitstellung einer Reihe manueller und automatisierter Optionen, Sie sind jedoch für die Entwicklung, das Testen, die Aktualisierung und das Management Ihrer Anwendung verantwortlich. AMS bietet Unterstützung bei der Behebung von Infrastrukturproblemen, die sich auf Anwendungen auswirken, AMS kann jedoch nicht auf Ihre Anwendungsconfigurationen zugreifen oder diese validieren.

AMS-Verantwortungsmatrix (RACI)

Note

Um seinen Verpflichtungen rechtzeitig nachzukommen, benötigt AWS Managed Services (AMS) möglicherweise Eingaben von Ihnen, um über eine angemessene Vorgehensweise zu entscheiden. AMS wird sich mit dem zuständigen Kundenkontakt in Verbindung setzen, um all diese Klarstellungen und Informationen zu erhalten. AMS erwartet eine Antwort auf solche Anfragen innerhalb von 24 Geschäftsstunden. Falls innerhalb von 24 Geschäftsstunden keine Antwort erfolgt, kann AMS in Ihrem Namen eine Maßnahme ergreifen.

In der AMS-Matrix „Verantwortliche, Rechenschaftspflichtige, Konsultierte und Informierte“ (RACI) wird die Hauptverantwortung für eine Vielzahl von Aktivitäten entweder dem Kunden oder AMS übertragen.

AMS verwaltet Ihre AWS-Infrastruktur. Die folgende Tabelle bietet einen Überblick über die Verantwortlichkeiten von Kunde und AMS für Aktivitäten im Lebenszyklus einer Anwendung, die in einer von AMS verwalteten Umgebung ausgeführt wird.

AMS ist nicht verantwortlich für die folgenden Aktivitäten im Zusammenhang mit vom Kunden verwalteten Konten oder der darin ausgeführten Infrastruktur. Daher ist dieser RACI nicht anwendbar.

- R steht für verantwortliche Partei, die die Arbeit zur Erfüllung der Aufgabe erledigt.
- C steht für konsultiert; eine Partei, deren Meinung eingeholt wird, in der Regel als Fachexperten, und mit der bilaterale Kommunikation besteht.
- I steht für informiert, d. h. eine Partei, die über den Fortschritt informiert wird, oft erst, wenn die Aufgabe oder das Ergebnis abgeschlossen ist.
- Self-Service Provisioning bezieht sich auf Ressourcen, die vom Kunden mit Self-Service über die AWS API oder die Konsole bereitgestellt werden, einschließlich Entwicklermodus und Self-Service Provisioned Services.

Note

Einige Abschnitte enthalten „R“ sowohl für AMS als auch für Kunden. Dies liegt daran, dass im Modell der AWS gemeinsamen Verantwortung sowohl AMS als auch die Kunden gemeinsam Verantwortung übernehmen, um Infrastruktur- und Anwendungsprobleme zu lösen.

Um Self-Service-Bereitstellungsfunktionen bereitzustellen, hat AMS erweiterte IAM-Rollen mit Rechtegrenzen eingerichtet, um unbeabsichtigte Änderungen durch direkten Servicezugriff zu verhindern. AWS Rollen verhindern nicht alle Änderungen, und Sie sind dafür verantwortlich, Ihre internen Kontrollen und die Einhaltung der Vorschriften einzuhalten und sicherzustellen, dass alle in AWS Anspruch genommenen Dienste die erforderlichen Zertifizierungen erfüllen. Wir nennen dies den Self-Service-Bereitstellungsmodus. [Einzelheiten zu den AWS Compliance-Anforderungen finden Sie unter AWS Compliance.](#)

Für Ressourcen, die Sie über Self-Service bereitstellen, bietet AMS Vorfallmanagement, detektive Kontrollen und Leitplanken, Berichterstattung, zugewiesene Ressourcen (Cloud Service Delivery Manager und Cloud Architect), Sicherheit und Zugriff sowie technischen Support bei Serviceanfragen. Darüber hinaus übernehmen Sie gegebenenfalls die Verantwortung für das Kontinuitätsmanagement, das Patch-Management, die Infrastrukturüberwachung und das Änderungsmanagement für Ressourcen, die außerhalb des AMS-Change-Management-Systems bereitgestellt oder konfiguriert wurden.

Aktivität	Kunde	AWS Managed Services (AMS)
Anwendungslebenszyklus		
Anwendungsentwicklung	R	I
Analyse und Entwurf der Anforderungen an die Anwendungsinfrastruktur	R	C
Design und Optimierung für AMS-Stacks, die nicht dem Standard entsprechen	R	C
Design und Optimierung des AMS-Standardstapels	I	R
Bereitstellen von Anwendungen	R	C
Bereitstellung der AWS-Infrastruktur	C	R
Anwendungsüberwachung	R	I
Testen/Optimierung von Anwendungen	R	I
Anleitung zur AWS-Infrastrukturoptimierung	I	R
Überwachung der AWS-Infrastruktur	I	R
Beheben und lösen Sie Anwendungsprobleme	R	C
Behebung und Behebung von AWS-Netzwerkproblemen	C	R
Beheben und lösen Sie Probleme mit dem Betriebssystem und der Infrastruktur	C	R
	R	C
Self-Service-Bereitstellung		
Anwendungs- und ITSM-Integration		

Aktivität	Kunde	AWS Managed Services (AMS)
Anwendungsintegration mit AWS-Servicangeboten	R	C
ITSM-Integration mit der AWS Managed Services Services-Schnittstelle	R	C
Netzwerkfunktionen		
Einrichtung und Konfiguration von VPC und VPC in verwalteter Umgebung	C	R
Weisen Sie privaten Adressraum zu (z. B. /16 VPCs)	R	C
Konfiguration und Betrieb von Managed Services, die nicht von AWS stammen, vom Kunden verwaltet Firewalls/Proxy/Bastions/HOSTs	R	C
Konfiguration und Betrieb der AWS-Sicherheit Groups/NAT/Customer Bastions/NACL in der verwalteten Umgebung	I	R
Netzwerkkonfiguration (z. B. DirectConnect) und Implementierung innerhalb des Kundennetzwerks	R	C
Netzwerkkonfiguration und Implementierung innerhalb der verwalteten Umgebung	C	R
Konfiguration der verwalteten Umgebung		
Definieren Sie die Auto Scaling Scaling-Standard-einstellungen für Baseline-Stack-Vorlagen	I	R

Aktivität	Kunde	AWS Managed Services (AMS)
Empfehlen Sie die RI-Optimierung	C	R
Erwerben Sie RI- und PIOP-Kapazität	R	C
Entfernen Sie Kapazität, wenn die Kapazität überlastet ist (sofern dies durch die Kundenanwendung unterstützt wird)	C	R
Kundenspezifische AWS-Informationen für AWS Managed Services erstellen/aktualisieren	C	R
S3-Konfiguration	C	R
Self-Service-Bereitstellung	R	C
Glacier-Konfiguration	C	R
Definieren Sie die Archivierungsrichtlinie	R	C
Konfiguration der Archivierungsrichtlinie	C	R
Auswahl des Wartungsfensters für Kunden	R	I
AWS-RDS-Verwaltung		
Den Zustand der source/replica/RO Replikation überwachen	I	R
Identifizieren Sie die RCA des Quell-Failovers	I	R
Automatisierte Snapshot-Konfiguration (Backup)	C	R
Self-Service-Bereitstellung	R	C

Aktivität	Kunde	AWS Managed Services (AMS)
Koordinieren und planen Sie das DB-Engine-Patchmanagement	C	R
Self-Service-Bereitstellung	R	C
Empfehlen Sie DB-Speicher und PIOP-Kapazität	C	R
Self-Service-Bereitstellung	R	C
Empfehlen Sie die Instanzgröße für laufende Datenbanken	C	R
Self-Service-Bereitstellung	R	C
Empfehlen Sie die RI-Optimierung für eine verwaltete Umgebung	C	R
Self-Service-Bereitstellung	R	C
RDS-Leistungsüberwachung () CloudWatch	C	R
Self-Service-Bereitstellung	R	C
Konfiguration des RDS-Event-Abonnements (SNS)	C	R
Self-Service-Bereitstellung	R	C
Konfiguration der RDS-Sicherheitsgruppe	C	R
Self-Service-Bereitstellung	R	C
Konfiguration der RDS-Engine parameter/option	R	C
Design der DB-Tabelle	R	I

Aktivität	Kunde	AWS Managed Services (AMS)
DB-Indizierung	R	I
DB-Protokollanalyse	R	I
AMS-Änderungsmanagement		
Einen Kunden erstellen RFCs (z. B. Zugriff auf Ressourcen, creating/updating/deleting managed stacks, deploying/updating Anwendungen, Änderungen an der Konfiguration von AWS Serviceangeboten)	R	I
Kunde genehmigen RFCs	I	R
Erstellung von AWS Managed Services RFCs (z. B. Zugriff auf Ressourcen, Erstellung von Ressourcen im Namen des Kunden, Anwenden von Betriebssystem-Updates als Teil von Patch Management)	I	R
Genehmigung nicht automatisiert RFCs	R	I
Anfrage für neue Änderungstypen einreichen	R	C
Neue Änderungstypen erstellen	I	R
Pflege des Änderungskalenders der Anwendung	R	C
Hinweis auf das bevorstehende Wartungsfenster	I	R
AWS Service Catalog		
Erstellen Sie Portfolios und Produkte	R	I
Verteilen Sie Produkte an Endbenutzer	R	I

Aktivität	Kunde	AWS Managed Services (AMS)
Erstellen Sie eine Bibliothek mit Tags und Tag-Optionen	R	C
Portfolios und Produkte mit Endbenutzern teilen	R	I
Portfolios und Produkte überarbeiten/aktualisieren	R	I
Portfolios und Produkte erstellen und Einschränkungen zuweisen	R	C
Ordnen Sie Serviceaktionen Produkten zu	R	C
Aktualisieren Sie die bereitgestellten Ressourcen mit der neuen Version des Produkts	R	I
Bereitstellung		
Kundenspezifische Ergänzungen zum Basis-AMI von AWS Managed Services	R	C
Konfigurieren Sie zusätzliche genehmigte Änderungstypen, die zur Bereitstellung von Stack-Vorlagen verwendet werden	C	R
Starten Sie verwaltete Stacks und zugehörige AWS-Ressourcen, die über den AMS-Change-Management-Prozess oder den AWS Service Catalog eingereicht wurden.	I	R
	R	I
Self-Service-Bereitstellung		

Aktivität	Kunde	AWS Managed Services (AMS)
Install/Update benutzerdefinierte Anwendungen und Anwendungen von Drittanbietern auf Instances, die über den AMS-Change-Management-Prozess oder den AWS Service Catalog bereitgestellt wurden.	R	I
Bereitstellung — Stack-Architektur		
Bereitstellung von Betriebssystemlizenzen (einschließlich Nutzungsgebühren für die jeweiligen AWS-Services — z. B. EC2 und RDS)	I	R
	R	I
Self-Service-Bereitstellung		
Definieren Sie grundlegende Infrastrukturvorlagen (Stacks) für die Anwendungsbereitstellung über das AMS-Change-Management-System.	I	R
	R	I
Self-Service-Bereitstellung		
Die Erstellung der Baseline wurde genehmigt 8 AMIs	I	R
Evaluieren Sie den Bestand der Kundenanwendungen und ermitteln Sie anhand der verfügbaren Infrastrukturvorlagen (Stacks), ob sie passen	R	C
Definieren Sie einzigartige Stacks, die zusätzlich zu den Basisvorlagenangeboten angeboten werden	R	C
Protokollierung, Überwachung und Eventmanagement		
Aufzeichnung von AWS-Infrastrukturänderungsprotokollen	I	R

Aktivität	Kunde	AWS Managed Services (AMS)
Aufzeichnung aller Anwendungsänderung protokolle	R	C
Installation und Konfiguration von Agenten und Skripten für Patching, Sicherheit, Überwachung usw. der AWS-Infrastruktur, die über den AMS- Change-Management-Prozess bereitgestellt wird.	I	R
Self-Service-Bereitstellung	R	C
Definieren Sie kundenspezifische Überwachu ngs- und Incident-Anforderungen	R	C
Konfiguration von Warnmeldungen für die verwaltete Umgebung	I	R
Überwachung aller von AMS konfigurierten Warnmeldungen	I	R
Self-Service-Bereitstellung	R	C
Untersuchung von Infrastrukturwarnungen zur Benachrichtigung über Vorfälle	I	R
Self-Service-Bereitstellung	R	C
Untersuchung von Anwendungsalarmen	R	C
Verwaltung von Vorfällen		
Proaktive Benachrichtigung von Vorfällen in der AWS-Infrastruktur auf der Grundlage von Überwachung	I	R
Self-Service-Bereitstellung	R	C

Aktivität	Kunde	AWS Managed Services (AMS)
Bewältigen Sie Leistungsprobleme und Ausfälle von Anwendungen	R	I
Kategorisieren Sie die Priorität des Vorfalls	I	R
Reaktion auf Vorfälle bereitstellen	I	R
Sorgen Sie für die Lösung von Vorfällen und die Wiederherstellung der Infrastruktur	C	R
 Note SLAs gelten nicht für instanzbasierte Ressourcen, die außerhalb von AMS Change Management bereitgestellt werden, einschließlich Ressourcen, die im Self-Service-Provisioning und im Entwicklermodus bereitgestellt wurden.		
Verwaltung von Problemen		
Identifizieren Sie Probleme in einer verwalteten Umgebung	C	R
Führen Sie RCA für Probleme in einer verwalteten Umgebung durch	C	R
Behebung von Problemen in einer verwalteten Umgebung	C	R
Identifizieren und beheben Sie Anwendungsprobleme	R	I
Sicherheitsmanagement		

Aktivität	Kunde	AWS Managed Services (AMS)
Sicherheit der Kundeninfrastruktur als and/or Grundlage für den Prozess zur Einhaltung der Sicherheitsbestimmungen, wie er beim Onboarding des Kunden festgelegt und vereinbart wurde.	C	R
	R	C
Self-Service-Bereitstellung		
Aufrechterhaltung gültiger Lizenzen für Managed EPS	R	C
Managed EPS konfigurieren	I	R
Self-Service-Bereitstellung	R	C
Managed EPS aktualisieren	I	R
Self-Service-Bereitstellung	R	C
Überwachung von Malware auf Instanzen, die über den AMS CM-Prozess bereitgestellt wurden.	I	R
	R	C
Self-Service-Bereitstellung		
Pflege und Aktualisierung von Virensignaturen	I	R
Self-Service-Bereitstellung	R	C
Behebung von mit Malware infizierten Instanzen	C	R
	R	C
Self-Service-Bereitstellung		
Verwaltung von Sicherheitsereignissen	C	R
Sicherheit — Zugriffsverwaltung		

Aktivität	Kunde	AWS Managed Services (AMS)
Verwalten Sie den Lebenszyklus von Benutzern und deren Berechtigungen für lokale Verzeichnisdienste, die für den Zugriff auf AWS Managed Services verwendet werden	R	I
Betreiben Sie föderierte Authentifizierungssysteme für den Kundenzugriff auf AWS die Konsole/ APIs	R	C
Akzeptieren und pflegen Sie das Active Directory-Vertrauen (AD) von AWS Managed Services AD zum vom Kunden verwalteten AD	R	C
Erstellen Sie während des Onboardings kontoübergreifende IAM-Admin-Rollen innerhalb jedes verwalteten Kontos	R	C
Sichern Sie die AWS Root-Anmeldeinformationen für jedes Konto	I	R
Definieren Sie IAM-Ressourcen für die verwaltete Umgebung	C	R
Verwalten Sie privilegierte Anmeldeinformationen für den Betriebssystemzugriff für AMS-Techniker	I	R
Verwaltet privilegierte Zugangsdaten für den Betriebssystemzugriff, die dem Kunden von AMS zur Verfügung gestellt wurden	R	I
Reaktion auf Sicherheitsvorfälle — Bereiten Sie sich darauf vor		
Kommunikation		

Aktivität	Kunde	AWS Managed Services (AMS)
Stellen Sie AMS Kontaktinformationen für die Kundensicherheit bereit, die AMS bei Benachrichtigungen über Sicherheitsereignisse und Sicherheitseskalationen verwenden kann	R	I
Speichern und verwalten Sie die vom Kunden bereitgestellten Sicherheitskontaktdaten, um sie bei Sicherheitsereignissen und Sicherheitseskalationen zu verwenden	CI	R
Training		
Stellen Sie dem Kunden Unterlagen zur Verfügung, um AMS bei der Reaktion auf Vorfälle zu unterstützen	I	R
Üben Sie die gemeinsame Verantwortung bei der Reaktion auf Sicherheitsvorfälle im Rahmen von Sicherheitsvorfällen	RI	RC
Ressourcenmanagement		
Konfigurieren Sie das unterstützte Sicherheitsmanagement AWS-Services für Warnmeldungen, Korrelation von Warnmeldungen, Geräuschreduzierung und zusätzliche Regeln	I	R
Pflegen Sie Ihr Inventar (AWS Ressourcen) und informieren Sie sich über den Wert und die Wichtigkeit von Anlagen. Diese Informationen sind bei der Strategie zur Eindämmung von Zwischenfällen hilfreich	R	CI
Verwenden Sie AWS Tags, um Ressourcen und Workloads zu identifizieren	R	CI

Aktivität	Kunde	AWS Managed Services (AMS)
Definieren und konfigurieren Sie die Aufbewahrung und Archivierung von Protokollen	CI	R
Sicheres Baselining von Konfigurationen AWS-Konto, Richtlinien und Zugriffsmanagement	CI	RC
Reaktion auf Sicherheitsvorfälle — Erkennen		
Protokollierung, Indikatoren und Überwachung		
Konfigurieren Sie die Protokollierung und Überwachung, um das Ereignismanagement für Instanzen und Konten zu ermöglichen	CI	R
Monitor wird AWS-Services für Sicherheitstwarnungen unterstützt	I	R
Stellen Sie Sicherheitstools für Endgeräte bereit und verwalten Sie sie	CI	R
Überwachen Sie Instanzen mit dem von AMS unterstützten Endpoint Security Tool auf Malware	I	R
Informieren Sie den Kunden per ausgehender Nachrichtenübermittlung über erkannte Ereignisse	I	R
Leiten Sie Benachrichtigungen und alle nachfolgenden Updates an die Entscheidungsträger für bestimmte Konten und Workloads weiter, um die Reaktionszeit auf Vorfälle zu verkürzen	R	CI

Aktivität	Kunde	AWS Managed Services (AMS)
Definition, Bereitstellung und Wartung von AMS-Standarderkennungsdiensten (z. B. Amazon GuardDuty und AWS Config)	CI	R
Protokollen von AWS Infrastrukturänderungen aufzeichnen	I	RC
Aktivieren und konfigurieren Sie die Protokollierung und Überwachung, um die Ereignisverwaltung für die Anwendung zu aktivieren	R	C
Implementieren und verwalten Sie eine Zulassungsliste, eine Ablehnungsliste und benutzerdefinierte Erkennungen für unterstützte AWS Sicherheitsdienste (z. B. Amazon GuardDuty)	RCI	R
Berichterstattung über Sicherheitsereignisse		
AMS über eine verdächtige Aktivität oder eine aktive Sicherheitsuntersuchung benachrichtigen	R	CI
Informieren Sie den Kunden über festgestellte Sicherheitsereignisse und Vorfälle	I	R
Informieren Sie über ein geplantes Ereignis, das den Prozess zur Reaktion auf Sicherheitsvorfälle auslösen könnte	R	CI
Reaktion auf Sicherheitsvorfälle — Analysieren		
Untersuchung und Analyse		

Aktivität	Kunde	AWS Managed Services (AMS)
Führen Sie eine erste Reaktion auf eine unterstützte Sicherheitswarnung durch, die von einer unterstützten Erkennungsquelle generiert wurde	I	RC
Beurteilen Sie die false/true positiven Ergebnisse anhand der verfügbaren Daten	RI	RC
Generieren Sie eine Momentaufnahme der betroffenen Instanzen, die Sie bei Bedarf mit dem Kunden teilen können	I	R
Führen Sie forensische Aufgaben wie Chain of Custody, Dateisystemanalyse, Speicherforensik und Binäranalyse durch	R	CI
Sammeln Sie Anwendungsprotokolle, um die Untersuchung zu unterstützen	R	I
Sammeln Sie Daten und Protokolle, um die Untersuchung von Sicherheitswarnungen zu unterstützen	RCI	RC
Nehmen SMEs Sie AWS-Services an Sicherheitsuntersuchungen teil	CI	R
Binden Sie bei der Untersuchung Drittanbieter ein (z. B. für die Untersuchung von EPS-Anti-Malware und für die Zusammenarbeit mit dem TrendMicro Support-Team)	RCI	I
Teilen Sie während einer Untersuchung Ermittlungsprotokolle vom Support AWS-Services an Kunden weiter	I	R
Kommunikation		

Aktivität	Kunde	AWS Managed Services (AMS)
Senden Sie Warnmeldungen und Benachrichtigungen von AMS-Erkennungsquellen für verwaltete Ressourcen	I	R
Verwalten Sie Warnmeldungen und Benachrichtigungen für Sicherheitsereignisse in Anwendungen	R	I
Wenden Sie sich bei der Untersuchung eines Sicherheitsvorfalls an den Sicherheitsbeauftragten des Kunden	R	I
Reaktion auf Sicherheitsvorfälle — Eindämmen		
Eindämmungsstrategie und Umsetzung		
Entscheiden Sie sich für die Umsetzung der vereinbarten Eindämmungsstrategie und vereinbaren Sie die Konsequenzen, die sich auf die Verfügbarkeit der Dienste während des Eindämmungszeitfensters auswirken könnten	R	CI
Erstellen Sie zur weiteren Analyse eine Sicherungskopie der betroffenen Systeme	CI	R
Beschränken Sie Anwendungen und Workloads (durch anwendungsspezifische Konfiguration oder Reaktionsaktivitäten)	R	CI
Definieren Sie die Eindämmungsstrategie auf der Grundlage des Sicherheitsvorfalls und der betroffenen Ressource	CI	R
Aktivieren Sie die Verschlüsselung und sichere Speicherung von Point-in-Time-Backups der betroffenen Systeme	CI	R

Aktivität	Kunde	AWS Managed Services (AMS)
Führen Sie unterstützte Containment-Aktionen für AWS Ressourcen wie EC2 Instanzen, Netzwerk und IAM aus	CI	R
Reaktion auf Sicherheitsvorfälle — Eliminieren		
Strategie und Umsetzung der Ausrottung		
Definieren Sie die Eliminierungsoptionen auf der Grundlage des Sicherheitsvorfalls und der betroffenen Ressource für die Workloads der Kundenanwendungen	R	CI
Legen Sie die vereinbarte Ausrottungsstrategie, den Zeitpunkt der Durchführung und die Konsequenzen fest	R	CI
Definieren Sie die Schritte zur Beseitigung auf der Grundlage des Sicherheitsvorfalls und der betroffenen Ressource auf AMS-verwalteten Workloads	CI	R
Eliminierung und Absicherung von AWS Ressourcen wie EC2 Instanzen, Netzwerk und IAM-Beseitigung	CI	R
Eliminierung und Absicherung von Anwendungen und Workloads (durch anwendungsspezifische Konfiguration oder Reaktionsaktivitäten)	R	I
Reaktion auf Sicherheitsvorfälle — Wiederherstellung		
Vorbereitung und Durchführung der Wiederherstellung		
Konfigurieren Sie Backup-Pläne und -Ziele wie vom Kunden gewünscht	R	I

Aktivität	Kunde	AWS Managed Services (AMS)
Überprüfen Sie die Backup-Pläne zur Wiederherstellung von AMS-verwalteten Workloads	CI	R
Führen Sie Aktivitäten zur Wiederherstellung von Backups für unterstützte Ressourcen durch AWS-Services	I	R
Backup die Kundenanwendung, die APP-Konfiguration und die Bereitstellungseinstellungen und überprüfen Sie die Backup-Pläne, um Kundenanwendungen und Workloads nach einem Vorfall wiederherzustellen	R	I
Stellen Sie Anwendungen und Kunden-Workloads wieder her (durch anwendungsspezifische Wiederherstellungsschritte)	R	I
Reaktion auf Sicherheitsvorfälle — Bericht nach dem Vorfall		
Berichterstattung nach dem Vorfall		
Teilen Sie dem Kunden nach dem Vorfall bei Bedarf die entsprechenden Erfahrungen und Maßnahmen mit	I	R
Patch-Verwaltung ⁹		
Halten Sie Ausschau nach geeigneten Updates für unterstützte Betriebssysteme und Software, bei denen das unterstützte Betriebssystem für EC2 Instanzen vorinstalliert ist.	I	R
Self-Service-Bereitstellung	R	C

Aktivität	Kunde	AWS Managed Services (AMS)
Informieren Sie den Kunden über bevorstehende Updates (gilt nur für AMS Standard Patch)	I	R
Schließt bestimmte Updates (and/or bestimmte Stacks) von den Patch-Aktivitäten aus	R	I
Definieren Sie standardmäßige und benutzerdefinierte Zeitpläne für Wartungsfenster und andere Parameter (z. B. Dauer des Wartungsfensters) für die Installation von Patches (gilt für AMS-Patch) Nur Orchestrator)	R	I
Definieren Sie benutzerdefinierte Patch-Baselines, um bestimmte Patches zu filtern und auszuschließen (gilt nur für AMS Patch Orchestrator)	R	I
Markieren Sie Instanzen, um sie benutzerdefinierten Wartungsfenstern und Patch-Baselines zuzuordnen (gilt nur für AMS Patch Orchestrator)	R	I
Verfolgen Sie im monatlichen Geschäftsbericht den Patch-Status von Ressourcen und heben Sie Systeme hervor, die nicht aktuell sind.	C	R
Patchen Sie das Windows-Betriebssystem und die auf dem Betriebssystem installierten Microsoft-Pakete, die von Windows Update gesteuert werden Self-Service-Bereitstellung	I R	R -

Aktivität	Kunde	AWS Managed Services (AMS)
Patchen Sie installierte Anwendungen, Software oder Anwendungsabhängigkeiten, die nicht von Windows Update verwaltet werden	R	I
Self-Service-Bereitstellung	R	-
Patchen Sie das Linux-Betriebssystem und alle Pakete, die für die Verwaltung durch den systemeigenen Paketmanager aktiviert sind (z. B. Yum, Apt, Zypper)	I	R
Self-Service-Bereitstellung	R	-
Patchen Sie installierte Anwendungen, Software oder Anwendungsabhängigkeiten, die nicht vom systemeigenen Paketmanager des Linux-Betriebssystems verwaltet werden	R	I
Self-Service-Bereitstellung	R	-
Kontinuitätsmanagement		
Geben Sie Backup-Zeitpläne an	R	I
Führen Sie Backups nach Zeitplan aus.	I	R
Self-Service-Bereitstellung	R	C
Backups validieren	R	I
Fordern Sie Aktivitäten zur Wiederherstellung von Backups an	R	I
Führen Sie Aktivitäten zur Wiederherstellung von Backups aus.	I	R
Self-Service-Bereitstellung	R	C

Aktivität	Kunde	AWS Managed Services (AMS)
Stellen Sie die betroffenen Stacks wieder her und VPCs	I	R
Self-Service-Bereitstellung	R	C
Stellen Sie die betroffene benutzerdefinierte Anwendung oder Anwendung eines Drittanbieters wieder her	R	C
Berichterstellung		
Bereiten Sie einen monatlichen Servicebericht vor und stellen Sie ihn bereit	I	R
AMS aktiviert AWS Outposts	R	I
Konfiguration und Abruf des API-Auditverlaufs bei Bedarf (CloudTrail).	I	R
Self-Service-Bereitstellung	R	I
Stellen Sie über die AWS Managed Services Services-Schnittstelle Zugriff auf den Vorfallauf bereit	I	R
Stellen Sie über die AWS Managed Services Services-Schnittstelle Zugriff auf den Änderungsverlauf bereit.	I	R
Self-Service-Bereitstellung	N/A	N/A
Verwaltung von Serviceanfragen		
Fordern Sie Informationen mithilfe von Serviceanfragen an	R	I
Beantworten Sie Serviceanfragen	I	R

Aktivität	Kunde	AWS Managed Services (AMS)
Verwaltete Firewall		
Fordern Sie die Bereitstellung einer von AMS verwalteten Firewall an	R	I
Entwurf und Optimierung der von AMS verwalteten Firewall-Architektur	I	R
Bereitstellung der AWS-Infrastruktur und der von AMS verwalteten Firewall-Appliance	I	R
Bereitstellung von Firewall-Lizenzen (einschließlich Nutzungsgebühren für die entsprechenden AWS-Services — z. B. EC2)	R	I
Definieren Sie die Standard-Zulassungsliste für Domänen	I	R
Anfrage zum Hinzufügen, Ändern und Löschen von benutzerdefinierten Zulassungslisten und Sicherheitsrichtlinien	R	I
Konfiguration von Warnmeldungen für die von AMS verwaltete Firewall	I	R
Überwachung aller von AMS verwalteten Firewalls konfigurierten Warnmeldungen	I	R
Führen Sie Backups der Firewall-Konfiguration aus	I	R
Fordern Sie Aktivitäten zur Wiederherstellung von Backups an	R	I
Aktualisieren Sie die bereitgestellten Ressourcen mit der neuen Version des Produkts	I	R

Aktivität	Kunde	AWS Managed Services (AMS)
Aufzeichnen von AMS-verwalteten Firewall-Protokollen	I	R
Leiten Sie Protokolle von der von AMS verwalteten Firewall weiter an CloudWatch	I	R
Fordern Sie Konfigurationsänderungen in der von AMS verwalteten Firewall an	R	I
Genehmigen Sie Konfigurationsänderungen in der von AMS verwalteten Firewall	I	R
Führen Sie Konfigurationsänderungen in der von AMS verwalteten Firewall aus	I	R

⁸ AMS bietet EC2 nur AMLs für Amazon

⁹ AMS ist OSeS nur dann für End of Life verantwortlich, wenn der Kunde eine erweiterte Support-Vereinbarung mit dem Betriebssystemanbieter unterzeichnet

Grundkomponenten der AMS-Umgebung

Multi-Account Landing Zone

Dies ist eine Schätzung der Komponenten und potenziellen Kosten der Infrastruktur in den Kernkonten. Andere Kosten wie Bandbreite, CloudWatch detaillierte Überwachung, Protokollierung, Alarmer, Route53, Amazon S3, Simple Notification Service (Amazon SNS), Snapshots oder reservierte Amazon-Instances sind nicht enthalten. EC2

Sie zahlen für die Komponenten, die für die von AMS verwaltete AWS-Landingzone-Infrastruktur benötigt werden. Schätzungen zufolge belaufen sich die Kosten für eine einfache AMS-Landezone-Umgebung mit mehreren Konten auf 2.450 USD pro Monat und 50 USD für ein einfaches Anwendungskonto.

Informationen zu den Preisen finden Sie unter [AWS-Preise](#).

Grundlegende Umgebungskomponenten

Komponente	Est. Kosten	Beschreibung
Verwaltungskonto	60\$	Ein AWS Organizations Management-Konto; erstellt und verwaltet Mitgliedskonten finanziell. Es enthält das AWS Landing Zone (ALZ) -Framework, Kontokonfigurationsstapelsätze und AWS Organization Service Control-Richtlinien (SCPs). • Directory Service: 35\$ • CloudTrail: 7\$ • CloudWatch: 6\$ • Andere: 12\$
Konto für gemeinsame Dienste	2000 USD	Enthält die Infrastruktur und die Ressourcen, die für die Zugriffsverwaltung (d. h. Active Directory), die Endpunktsicherheitsverwaltung (Trend Micro) und Ihre Bastionen (SSH/RDP) erforderlich sind. Die Schätzung liegt bei 2400\$ pro Monat. In dieser Schätzung sind die Kosten für die Trend Micro Lizenzen nicht enthalten. • EC2: 800\$ (mit der Mindestanzahl an Bastions) • RDS: 300\$ (PRO SEKUNDE) • VPC (Endpunkte): 400\$ • Directory Service: 300\$ • CloudWatch: 100\$ • GuardDuty : 15\$ • Secrets Manager: 10\$ • Datenübertragung: 10\$ • Config: 10\$ • Andere: 45\$
Netzwerkkonto	350\$	Der zentrale Knotenpunkt für Netzwerk-Routing zwischen AMS-Konten, Ihrem lokalen Netzwerk und ausgehendem Datenverkehr ins Internet. Enthält

Komponente	Est. Kosten	Beschreibung
		außerdem öffentliche DMZ-Bastionen (den Zugangspunkt für AMS-Techniker, um auf Hosts in Ihrer AMS-Umgebung zuzugreifen). Der Preis kann sich je nach Verkehr über das Transit Gateway und Direct Connect erhöhen. • EC2: 250\$ (Bastions) • VPC: 80\$ • Andere: 20\$
Konto protokollieren	20\$	Ein S3-Bucket mit Kopien der AWS CloudTrail - und AWS Config-Protokolldateien von jedem Ihrer AMS-Umgebungskonten. Die Kosten steigen, je mehr Protokolle gesammelt werden. • S3: 10\$ • CloudWatch: 5\$ • Andere: 5\$
Sicherheitskonto	20\$	Die zentrale Anlaufstelle für sicherheitsrelevante Operationen und die zentrale Anlaufstelle für die Weiterleitung von Benachrichtigungen und Warnmeldungen an die AMS-Steuerflugzeugdienste. Enthält außerdem das Amazon Guard Duty-Verwaltungskonto. Die Kosten steigen, da mehr Ereignisse mit Amazon analysiert werden GuardDuty. • CloudWatch: 15\$ • Andere: 5\$

Single-Account Landing Zone

In der folgenden Tabelle sind die Komponenten einer von AMS verwalteten Beispielinfrastruktur aufgeführt.

Grundlegende Umgebungskomponenten, letzte Aktualisierung 2020/07/09

Name	Instance-Typ	BS	Anzahl der Komponenten	
mc-eps-dsm	m5.large	Linux	2	
MC-Management	m5.large	Windows	2	
mc-bastion-dmz-ssh	m5.large	Linux	2	
mc-bastion-customer-rdp	m5.large	Windows	2	
mc-eps-relay	m5.large	Linux	2	
Verzeichnisdienste	N/A	N/A		
zusätzliche Komponenten	N/A	N/A		

Informationen zu den Preisen finden Sie unter [AWS-Preise](#).

AMS-Kontolimits

In der AMS-Landezone mit mehreren Konten sind drei verschiedene Arten von Limits zu berücksichtigen: AMS-API-Limits, AMS-Ressourcenlimits und AWS-Limits.

In der landing zone für ein einzelnes Konto sind zwei unterschiedliche Arten von Beschränkungen zu berücksichtigen: AMS-API-Limits und AWS-Limits.

API-Beschränkungen für AMS-Konten

In diesem Abschnitt werden die Grenzwerte auf Kontoebene beschrieben, nach deren Ablauf AWS Managed Services (AMS) den AMS SKMS API-Service drosselt. Das heißt, wenn Sie einen der aufgelisteten Anrufe APIs mehr als 10 Mal pro Sekunde aufrufen, wird einer der Anrufe „gedrosselt“ (Sie erhalten eine). `ThrottlingException` In seltenen Fällen kann eine externe oder nachgelagerte Abhängigkeit die AMS-API drosseln und dann kann AMS Ihre API-Aufrufe mit einer möglicherweise niedrigeren Geschwindigkeit drosseln.

 Note

Für Informationen zur AMS SKMS-API laden Sie die Referenz über den Tab Berichte der AWS Artifact-Konsole herunter.

Für jede aufgelistete AMS SKMS-API wird der Vorgang nach 10 TPS (Transaktionen pro Sekunde) gedrosselt:

- GetStack
- GetSubnet
- GetVpc
- ListAmis
- ListStackSummaries
- ListSubnetSummaries
- ListVpcSummaries

Ressourcenlimits für AMS-Landingzone-Konten mit mehreren Konten

Die Ressourcenlimits für Konten beziehen sich auf AMS-Landingzone-Anwendungskonten VPCs und Subnetze mit mehreren Konten.

Ressourcenbeschränkungen für Anwendungskonten

Es gibt ein Soft-Limit von 50 Anwendungskonten pro Organisation. Wenn Sie einen Anwendungsfall für mehr als 50 Anwendungskonten haben, wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM), um Ihre Anforderungen mitzuteilen.

VPCs und Ressourcenbeschränkungen für Subnetze

Es gibt ein Soft-Limit von 10 VPCs pro Anwendungskonto innerhalb der vordefinierten AWS-Region für das Unternehmen.

Jede VPC kann über 1 bis 10 private Subnetzstufen verfügen, die sich über 2 bis 3 Verfügbarkeitszonen erstrecken. Darüber hinaus kann jede VPC über 0 bis 5 öffentliche Subnetzstufen verfügen, die sich über 2 bis 3 Verfügbarkeitszonen erstrecken. Wenn Sie Anforderungen haben, die über diese Grenzen hinausgehen, informieren Sie Ihren CSDM oder Cloud Architect, um Ihren Anwendungsfall zu überprüfen.

Verhältnis zwischen Anmeldung landing zone Konto für mehrere Konten bei AMS

In der AMS-Landezone mit mehreren Konten wird ein Konto pro Anwendung unterstützt. Für jedes Anwendungskonto fallen jedoch geringe Kosten an, und Ihnen werden die Anzahl der Verbindungen zum Transit Gateway pro Stunde und die Menge des Datenverkehrs, der über AWS Transit Gateway fließt, in Rechnung gestellt. Je stärker also die Anwendungen auf Konten aufgeteilt sind VPCs, desto höher sind die Kosten.

Um die Kosten zu senken und dennoch eine angemessene Aufgabentrennung zu gewährleisten, empfiehlt AMS, 1) Anwendungen nach Teams mit eng miteinander verknüpften Geschäftsprozessen zu gruppieren und 2) Anwendungen, die sich in unterschiedlichen Phasen (Produktion oder Nicht-Produktion) befinden oder von unterschiedlichen Teams verwaltet werden, nicht miteinander zu vermischen. Auf diese Weise haben Sie weniger Konten, die Zugriffsverwaltung und die Aufgabentrennung werden einfacher, und die Verkehrskosten könnten gesenkt werden.

Ein Beispiel: Ein Unternehmen produziert eine Trading-Anwendung und eine Portfoliomanagement-Anwendung. Beide Anwendungen werden vom IT-Team für Investitionen verwaltet und tauschen viel Traffic miteinander aus. In diesem Szenario kann das Unternehmen davon profitieren, beide Anwendungen in demselben Konto und derselben VPC zu gruppieren, da das IT-Team für Investitionen keinen Zugriff auf mehrere Anwendungskonten beantragen muss und das Unternehmen dadurch Traffic-Kosten spart. In diesem Fall sollte das Unternehmen ein weiteres Konto für dieselben Anwendungen einrichten, die sich in der Entwicklungsphase befinden, und dem Entwicklungsteam Zugriff gewähren.

In einem anderen Szenario produziert das Unternehmen derzeit eine Lohn- und Gehaltsabrechnungsanwendung und eine Buchhaltungsanwendung, die jeweils von den IT- und Buchhaltungs-IT-Teams verwaltet werden. Obwohl die Lohnbuchhaltungsanwendung Informationen mit der Buchhaltungsanwendung austauschen muss, empfehlen wir, beide Anwendungen in verschiedene Konten zu unterteilen, eines pro Team, und über das Netzwerkkonto eine Verbindung zwischen beiden Anwendungen VPCs herzustellen. Auf diese Weise verhindert das Unternehmen, dass das IT-Team der Personalabteilung Änderungen anfordert, die sich auf die Infrastruktur der Buchhaltungsanwendungen auswirken, von denen es nichts weiß.

Tipps zur Gruppierung von Konten in Organisationseinheiten (OUs). Eine OU ist ein logischer Gruppierungsmechanismus, der es Ihnen ermöglicht, Konten zu kategorisieren (zu gruppieren) und Richtlinien und Konfigurationen auf der Grundlage dieser Gruppen anzuwenden. Der empfohlene Ansatz für die Erstellung OUs besteht darin, sie auf Richtlinien zu stützen, die auf eine bestimmte Gruppe von Konten angewendet werden müssen, und nicht auf der internen Hierarchie der Teams

innerhalb Ihrer Berichtsstruktur. Eine Organisationseinheit entspricht nicht der Organisationseinheit eines Active Directory, und von dem Versuch, die AD-Organisationseinheitenstruktur darin zu replizieren, AWS Organizations wird abgeraten, da dies zu einer schwierig zu verwaltenden Betriebsstruktur führt. and/or

AWS Kontogrenzen

AWS Kontolimits gelten für Ihre AWS Managed Services (AMS) -Konten. Die einfachste Methode, Standard- und aktuelle Grenzwerte für AWS Dienste zu ermitteln, ist die Nutzung von [AWS Service Quotas](#). AMS empfiehlt, die Größe der einzelnen Dienstlimits an die Größe anzupassen, die für die Ausführung der Dienste im Konto erforderlich ist. Limits wirken wie Leitplanken, um Ihre Konten zu schützen, was die Sicherheit und die Kosten angeht. Wenn Sie ein bestimmtes Limit erhöhen möchten, reichen Sie eine Serviceanfrage bei AMS ein, und AMS Operations erhöht das Limit in Ihrem Namen. Das Standardlimit (oder Kontingent) für RDS-Instances ist beispielsweise 40; wenn Ihr Workload 50 RDS-Instances erfordert, stellen Sie eine Serviceanfrage an AMS Operations, um das Limit auf den gewünschten Wert anzuheben.

AMS-Servicelevel-Ziele (SLOs)

In der folgenden Tabelle werden die Ziele des AWS Managed Services (AMS) -Service beschrieben. Service Level Agreements (SLAs) für andere Aspekte des AMS-Service, einschließlich Incident Management, werden in dem SLA-Dokument behandelt, das Ihnen bei Ihrem AMS-Abonnement ausgehändigt wurde. Für weitere Informationen wenden Sie sich an Ihren CSDM.

Ziele des AMS Service Levels

Funktion	Leistungsindikator (PI)	Plus (Business Days, M-F 8AM to 6PM local time)	Prämie (Calendar Days, 24 x 7)
Änderungsmanagement	Zeit, die für die automatische Terminierung oder Ablehnung benötigt wird RFCs	<=30 Minuten	<=30 Minuten
	Zeitpunkt der Initiierung der geplanten	<=1 Minute	<=1 Minute

Funktion	Leistungsindikator (PI)	Plus (Business Days, M-F 8AM to 6PM local time)	Prämie (Calendar Days, 24 x 7)
	Ausführung RFCs im Vergleich zur geplanten Ausführungszeit		
	Zeitaufwand bis approve/reject nicht automatisiert RFCs, verfügbar im CT-Katalog	<=48 Stunden	<=24 Stunden
	Zeitaufwand bis zur approve/reject Nichtautomatisierung nicht im RFCs CT-Katalog verfügbar	<=5 Tage	<=5 Tage
Umgang mit Problemen	Zeitaufwand für die Fertigstellung der Ursachenanalyse (RCA)	<=10 Tage	<=10 Tage
Verwaltung von Serviceanfragen	Reaktionszeit für die erste und jede weitere Antwort	<=8 Stunden	<=4 Stunden

Unterstützte AWS Dienste

AWS Managed Services (AMS) bietet Support-Services für das Betriebsmanagement für die folgenden AWS Services. Jeder AWS Service ist anders, weshalb das Niveau des Betriebsmanagements und der Support von AMS je nach Art und Merkmalen des zugrunde liegenden AWS Services variieren. Spezifische AWS Dienste werden auf der Grundlage der Komplexität und des Umfangs der von AMS erbrachten Unterstützungsdienste für das Betriebsmanagement gruppiert.

Note

Die drei Gruppen A, B und C geben die Preise als Prozentsatz der gesamten monatlichen Ausgaben pro Konto für den AMS-Service auf der Grundlage des Supportplans (Plus oder Premium) für AMS-Kunden vor dem 16. März 2021 an. AMS-Kunden, die nach dem 16. März 2021 an Bord gegangen sind, sollten eine Serviceanfrage für zusätzliche Preisinformationen stellen. Gruppe A gibt an, dass keine zusätzlichen Gebühren anfallen. Gruppe B gibt eine zusätzliche Gebühr von 12% (Plus) oder 18% (Premium) an. Gruppe C gibt eine zusätzliche Gebühr von 25% (Plus) oder 42% (Premium) an.

Ein Stern (*) steht für Dienste, die in einer AMS-verwalteten Umgebung von einem Kunden mithilfe der AWS Konsole und bereitgestellten APIs werden. Weitere Informationen zur Verantwortung des Kunden bei der Bereitstellung und Konfiguration von Diensten auf diese Weise [Funktionen des erweiterten Betriebsplans AMS von AWS Managed Services \(AMS\)](#) finden Sie unter „Automatisiertes Bereitstellungsmanagement und Self-Service-Bereitstellungsmanagement“.

Zwei Sterne (**) bedeuten, dass Amazon EC2 on als Service der Gruppe B abgerechnet AWS Outposts wird. Alle anderen Ressourcen, die auf gehostet werden, AWS Outposts werden zum Standardtarif abgerechnet.

Unterstützte Dienste AWS

Gruppe A	Gruppe B	Gruppe C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift

Gruppe A	Gruppe B	Gruppe C
AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream* Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces*	Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

Gruppe A	Gruppe B	Gruppe C
	AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

Wenn Sie AWS Managed Services mit der Bereitstellung von Services für Software oder Services beauftragen, die im Folgenden nicht ausdrücklich als unterstützt gekennzeichnet sind, werden alle AWS Managed Services, die für solche vom Kunden angeforderten Konfigurationen bereitgestellt werden, gemäß den Servicebedingungen als „Beta-Service“ behandelt.

Unterstützte Konfigurationen

Dies sind die Konfigurationen, die AWS Managed Services (AMS) unterstützt:

- Sprache: AMS ist in englischer Sprache verfügbar.
- Firewall-Dienste:
 - DNS-Firewall mit Amazon Route 53-Resolver
 - Firewall der nächsten Generation der Palo Alto VM-Serie
- Sicherheitssoftware: Deep Security von Trend Micro (erforderlich). AWS Marketplace: [Trend Micro Deep Security](#)
- Zugelassene Verzeichnisdienste: Microsoft Active Directory (AD)
- [Unterstützte AWS Dienste](#).
- Unterstützte AWS Regionen:

AMS ist in einer Untergruppe aller AWS Regionen tätig, das AMS API/CLI wird jedoch nur in der Region „USA Ost (Nord-Virginia)“ betrieben. Wenn Sie entweder die AMS Change Management API (amscm) oder die AMS Service Knowledge Management API (amsskms), in einer Region außerhalb der USA Ost) ausführen, müssen Sie den Befehl ergänzen `--region us-east-1`.

- USA Ost (Virginia)
- USA West (Nordkalifornien)
- USA West (Oregon)
- USA Ost (Ohio)
- Kanada (Zentral)
- Südamerika (São Paulo)
- EU (Irland)
- EU (Frankfurt)
- EU (London)
- EU West (Paris)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Amazon Machine Images (AMIs): AMS bietet sicherheitsoptimierte Images (AMIs), die auf dem CIS Level 1-Benchmark basieren, für eine Untergruppe von Betriebssystemen, die von AMS unterstützt werden. Informationen zu Betriebssystemen, für die ein Image mit verbesserter

Sicherheit verfügbar ist, finden Sie im AMS Security User Guide. Um auf dieses Handbuch zuzugreifen AWS Artifact, filtern Sie unter die Registerkarte Berichte nach AWS Managed Services. Um darauf zuzugreifen AWS Artifact, wenden Sie sich an Ihren CSDM oder lesen Sie unter [Erste Schritte mit AWS Artifact](#) nach.

- Unterstützte Betriebssysteme:

Unterstützte Betriebssysteme (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (voraussichtliches Enddatum des AMS-Supports am 30. Juni 2026)
- Oracle Linux 9.x, 8.x
- RedHat Enterprise Linux (RHEL) 9.x, 8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server für SAP 15 SP3 und höher
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Unterstützte Betriebssysteme () ARM64

- Amazon Linux 2023
- Amazon Linux 2 (voraussichtliches Enddatum des AMS-Supports am 30. Juni 2026)

- Unterstützte Betriebssysteme mit End of Support (EOS):

Note

Betriebssysteme mit Ende des Support (EOS) laufen außerhalb des allgemeinen Supportzeitraums des Betriebssystemherstellers und bergen ein erhöhtes Sicherheitsrisiko. EOS-Betriebssysteme gelten nur dann als unterstützte Konfigurationen, wenn für AMS erforderliche Agenten das Betriebssystem unterstützen und...

1. Sie haben einen erweiterten Support mit dem Betriebssystemanbieter abgeschlossen, der es Ihnen ermöglicht, Updates zu erhalten, oder
2. alle Instanzen, die ein EOS-Betriebssystem verwenden, befolgen die [Sicherheitskontrollen](#), die von AMS im Advanced User Guide beschrieben wurden, oder
3. Sie halten sich an alle anderen von AMS geforderten ausgleichenden Sicherheitskontrollen.

Falls AMS nicht mehr in der Lage ist, ein EOS-Betriebssystem zu unterstützen, gibt AMS eine [wichtige Empfehlung](#) zur Aktualisierung des Betriebssystems heraus.

Zu den für AMS erforderlichen Agenten gehören unter anderem: Amazon AWS Systems Manager CloudWatch, Endpoint Security (EPS) -Agent und Active Directory (AD) Bridge (nur Linux).

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3 und SP4 SP5
- SUSE Linux Enterprise Server für SAP 15 SP2
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Service für SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- RedHat Enterprise Linux (RHEL) :7.x
- Oracle Linux 7.5-7.9

Funktionen für nicht unterstützte Betriebssysteme in AMS

Ein nicht unterstütztes Betriebssystem ist jedes Betriebssystem, das nicht in der aufgeführt ist.

[Unterstützte Konfigurationen](#) AMS betrachtet Instances mit nicht unterstützten Betriebssystemen als „vom Kunden angeforderte Konfigurationen“, die den Nutzungsbedingungen für [AWS Betas und Previews](#) unterliegen.

Die folgenden begrenzten AMS-Funktionen sind für Instances mit nicht unterstützten Betriebssystemen verfügbar:

Funktionalität	Hinweise
Vorfallmanagement	AMS reagiert auf Vorfälle.
Verwaltung von Serviceanfragen	AMS reagiert auf Serviceanfragen.
Änderungsanträge (RFCs)	AMS bewertet die RFCs Ausführung. Nicht unterstützte Betriebssysteme können die Ausführungsfähigkeit beeinträchtigen. RFCs
Überwachung	AMS überwacht und reagiert auf EC2 Amazon-Systemstatusprüfungen und Instance-Statusprüfungen.

Funktionalität	Hinweise
	Zu den Systemstatusprüfungen gehören: Verlust der Netzwerkkonnektivität, Verlust der Systemleistung, Softwareprobleme auf dem physischen Host und Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen. Zu den Instanzstatusprüfungen gehören: falsche Netzwerk- oder Startkonfiguration, erschöpfter Arbeitsspeicher, beschädigtes Dateisystem und inkompatibler Kernel.
Sicherheitsmanagement	AMS überwacht die EC2 GuardDuty Ergebnisse von Amazon und reagiert darauf.
Backup-Verwaltung	AMS bietet Continuity Management in AMS Advanced für die EC2 Verwendung von AMS-kundenspezifischen AWS Backup Plänen und Tresoren.

Erweiterte AMS-Schnittstellen

- **AMS Advanced-Konsole:** Sie verwenden die AMS Advanced-Konsole RFCs, um Vorfälle zu erstellen, zu melden und darauf zu reagieren, Serviceanfragen zu stellen und Informationen zu bestehenden VPCs und Stacks zu finden. Wenn Sie sich nicht sicher sind, was Sie tun sollen, oder wenn Sie Hilfe mit AMS oder Ihren verwalteten Ressourcen benötigen, erstellen Sie über diese Oberfläche eine Serviceanfrage.
- **AWS-Managementkonsole:** Viele AWS Konsolen können für die Anzeige von AMS-Informationen nützlich sein, zum Beispiel:
 - **EC2 Amazon-Konsole:** Wird verwendet, um Instance-Informationen wie Bastion-IP-Adressen, Amazon EC2 Auto Scaling Scaling-Gruppen und Load Balancer anzuzeigen.
 - **Einhaltung der Landing AWS Config Zone-Regeln für mehrere Konten:** Sie können den Compliance-Status für alle Ihre Konten einsehen und Ressourcen identifizieren, die diese Anforderungen nicht erfüllen.

- **AWS CloudFormation Konsole:** Wird verwendet, um Stack-Informationen einschließlich Stapel anzuzeigen IDs (Amazon RDS-Stacks und Amazon RDS-Instance sowie Informationen zu Ereignissen finden Sie IDs hier).
- **Amazon RDS-Konsole:** Dient zum Anzeigen von Ereignisinformationen, z. B. einem Beitrag, der in einer WordPress App auf einer Website in Ihrem Konto veröffentlicht wurde. Beachten Sie, dass Sie über die Amazon RDS-Instance-ID verfügen müssen.

Je nach Modus Ihrer Anmelderolle haben Sie unterschiedliche Zugriffsebenen auf die AWS Management Console. Weitere Informationen zu Modi finden Sie unter [AMS-Modi](#).

- **AMS Advanced Change Management API — Lesen/Schreiben:** Verwenden Sie die Change Management API (CM API), um Ergänzungen und spezifische Änderungen an Ihrer verwalteten Infrastruktur, einschließlich Ressourcenüberwachung, Protokoll-, Backup- und Patch-Konfigurationen, anzufordern. Verwenden Sie diese API auch, um Zugriff auf Ressourcen anzufordern, Ressourcen zu löschen und AMIs IAM-Instanzprofile zu erstellen und zu erstellen. Sie können über die AMS-CLI und auf die CM-API zugreifen SDKs.
- **AMS SKMS API — Schreibgeschützt:** Verwenden Sie diese API, um verwaltete Ressourcen aufzulisten und Informationen abzurufen, die für die Meldung oder Vorbereitung von Änderungsanträgen benötigt werden.
- **Support API:** Verwenden Sie die Support Standard-API, um Vorfälle und Serviceanfragen programmgesteuert zu erstellen und darauf zu reagieren. Weitere Informationen finden Sie unter [Erste Schritte mit Support](#).
- **AWS APIs— Schreibgeschützt:** Ihr Haupt-IT-Administrator kann den verwenden, AWS APIs um alle verwalteten Ressourcen einzusehen, CloudTrail Protokolle, Rechnungsinformationen und viele andere Lesefunktionen einzusehen.

AMS VPC-Endpunkte

Mit einem VPC-Endpunkt können Sie eine private Verbindung zu Ihrer VPC herstellen, AWS-Services ohne dass ein Internet-Gateway erforderlich ist. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit den Ressourcen in dem Service zu kommunizieren.

Endpunkte sind virtuelle Geräte. Es sind horizontal skalierte, redundante und hochverfügbare VPC-Komponenten, die die Kommunikation zwischen Instances in Ihrer VPC und Services ermöglicht, ohne die Verfügbarkeit oder Bandbreite Ihres Netzwerkdatenverkehrs zu gefährden. Weitere Informationen finden Sie unter [VPC-Endpoints](#).

Es gibt zwei Arten von VPC-Endpunkten: Schnittstellenendpunkte und Gateway-Endpunkte.

- Gateway-Endpunkte: Für die VPC im Konto ist standardmäßig ein Amazon S3 S3-Gateway-Endpunkt aktiviert.
- Schnittstellen-Endpunkte: Instances in Ihrer AMS-Umgebung können mit unterstützten Services kommunizieren, ohne das Amazon-Netzwerk zu verlassen. Dies ist optional für die landing zone mit einem Konto und ist standardmäßig nicht im Konto aktiviert. Senden Sie eine Serviceanfrage an AMS Operations, um dies zu aktivieren. Für die landing zone mit mehreren Konten sind die Schnittstellenendpunkte jedoch standardmäßig im Shared Services-Konto aktiviert.

Liste der von AMS unterstützten Schnittstellenendpunkte:

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- EC2 Amazon-API
- AWS Key Management Service
- Amazon CloudWatch
- CloudWatch Amazon-Veranstaltungen
- CloudWatch Amazon-Protokolle
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

AMS-geschützte Namespaces

Die Liste der geschützten Namespaces für AWS Managed Services (AMS). Wenn Sie mit AWS Ressourcen arbeiten, vermeiden Sie Konflikte mit AMS, indem Sie diese Namespaces nicht verwenden. Einzelheiten zu anderen AWS Service-Namespaces finden Sie unter [Amazon Resource Names \(ARNs\) und AWS Service Namespaces](#).

- `ams - *` (Dies ist der bevorzugte Benennungsstandard für neue Ressourcen)
- `/ams/ *` (Dies ist der bevorzugte Benennungsstandard für pfadbasierte Ressourcen)

- `AWSManagedServices*` (Dies ist gegebenenfalls der bevorzugte Benennungsstandard für Ressourcen) CamelCase
- `ams*` und `AMS*` und `Ams*`
- `AWS_*` und `aws*`
- `*/aws_reserved/*`
- `CloudTrail*` und `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-*`
- `eps` und `EPS`
- `EPSTMarketplaceSubscriptionRole`
- `EPSDB*`
- `IAMPolicy*`
- `INGEST*`
- `LandingZone*`
- `Managed_Services*`
- `managementhost`
- `mc*` und `MC*` und `Mc*`
- `MMS*`
- `ms-`
- `NewAMS*`
- `Root*`
- `sentinel*` und `Sentinel*`
- `sentinel.int.`
- `StateMachine*`
- `StackSet-ams*`
- `StackSet-AWS-Landing-Zone`
- `TemplateId*`
- `UnhealthyInServiceBastion`
- `VPC_*`

Reservierte AMS-Präfixe

AMS-Ressourcenattribute müssen bestimmten Mustern entsprechen. Beispielsweise dürfen Profilnamen, Namen, BackupVault Tagnamen usw. von IAM-Instanzen nicht mit reservierten AMS-Präfixen beginnen. Diese reservierten Präfixe sind:

```
*/aws_reserved/*
ams- *
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc- *
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc *
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
```

AMS-Wartungsfenster

Das AWS Managed Services Maintenance Window (oder Maintenance Window) führt Wartungsaktivitäten für AWS Managed Services (AMS) durch und findet jeden zweiten Donnerstag im Monat von 15:00 Uhr bis 16:00 Uhr pazifischer Zeit statt. AMS kann das Wartungsfenster 48 Stunden im Voraus ändern. Dies ist für AWS Managed Services (AMS) vorgesehen, um Wartungsaktivitäten für verwaltete Infrastrukturen durchzuführen, z. B. die Bereitstellung neuer AMS AMIs.

In Ihrem Wartungsfenster installiert AMS die Patches, und Sie legen Ihr Wartungsfenster beim Onboarding fest. Sie können auch dem vorgeschlagenen Patchfenster zustimmen, das in Ihrer Benachrichtigung zum Patch-Service angegeben ist, oder ein anderes Fenster vorschlagen.

Anleitungen zur Erstellung eines Wartungsfensters finden Sie unter [Wartungsfenster](#).

AMS-Informationsressourcen

AMS bietet verschiedene Informationsressourcen, um Ihnen zum Erfolg zu verhelfen.

- AMS Accelerate-Benutzerhandbuch: Hilft Ihnen, die von AMS Accelerate bereitgestellten Komponenten und Funktionen sowie deren Verwendung zu verstehen. Hier finden Sie Hintergrundinformationen zu AMS Accelerate und Details zu Standardeinstellungen, Ressourcen und Beispiele für Anleitungen. [HTML-Index](#), [PDF](#)
- AMS Advanced-Benutzerhandbuch: Hilft Ihnen, die von AMS Advanced bereitgestellten Komponenten und Funktionen sowie deren Verwendung zu verstehen. Hier finden Sie Hintergrundinformationen zu AMS Advanced und Details zu Standardeinstellungen, Ressourcen und Anleitungen. [HTML-Index](#), [PDF](#)
- AMS Advanced Application Guide: Beschreibt die Schritte zur Bereitstellung von Anwendungen in der AWS Managed Services Services-Infrastruktur. Hier finden Sie Informationen zu Methoden und Überlegungen zur Bereitstellung und Wartung von Anwendungen. [HTML-Index](#), [PDF](#).
- AMS Advanced Onboarding Guide: Beschreibt die ersten Schritte zur Erstellung der grundlegenden AWS Managed Services Services-Landingzone-Infrastruktur mit mehreren Konten oder Einzelkonten in einem AMS-Konto. Hier finden Sie Informationen zu den Grundlagen und zur Validierung von AMS-Konten sowie Fragen zur Vorbereitung auf das Onboarding bei AMS. [HTML-Index](#), [PDF](#).

- **AMS Advanced Change Type Reference:** Enthält Referenzmaterial zu den aktuellen Änderungstypen, die AWS Managed Services bereitstellt, einschließlich Schemas für Änderungstypen und exemplarische Vorgehensweisen für jeden Änderungstyp sowie Tipps. Enthält allgemeine Informationen zu Änderungstypen. Hilft Ihnen, alle Aspekte von Änderungsanträgen (RFCs) und AMS-Änderungstypen () zu verstehen. CTs Hier finden Sie Einzelheiten zu den Änderungstypen, einschließlich Links zu relevanten Informationen. [HTML-Index](#), [PDF](#).
- **AMS CM (Change Management) API-Referenz:** Beschreibt die AWS Managed Services CM API, die Operationen zur Erstellung und Überwachung von Änderungsanforderungen bereitstellt und Informationen über Ihre Ressourcen bereitstellt, die von Managed Services verwaltet werden. [HTML-Index](#).
- **AMS-Sicherheitsleitfäden:** Beschreiben Sie proprietäre AMS-Sicherheitsinformationen.
Privat; verfügbar auf der Registerkarte AMS-Berichte in der AWS Artifact Console.
- **AMS-Entwicklerressourcen:** Zugriff auf die AMS-CLI und das SDK, sowohl für amscm als auch für amsskms. Siehe <https://console.aws.amazon.com/managedservices/>.
- **YouTube AMS-Videos:** Wichtige Kundenabläufe werden im Video erklärt. Sehen Sie sich die [YouTube Schulungsvideos zu AWS Managed Services](#) an.
- **AMS-Blogbeiträge:** Spezialinformationen zu AWS Managed Services. Siehe [AWS-Blogs](#).

AMS-Konformität

AMS wurde nach den folgenden Standards geprüft und kann als Teil von Lösungen eingesetzt werden, für die Sie eine Konformitätszertifizierung erhalten müssen.

Von AMS unterstützte Compliance-Standards

AMS unterstützt AWS Compliance-Standards. Weitere Informationen zu AWS Compliance-Programmen finden Sie unter [AWS Compliance](#).

Dies sind die aktuellen Compliance-Standards, die von AMS unterstützt werden.

FedRAMP: Die US-Bundesregierung ist bestrebt, ihre Dienste dem amerikanischen Volk auf die innovativste, sicherste und kostengünstigste Weise anzubieten. Cloud Computing spielt eine wichtige Rolle dabei, wie die Bundesregierung betriebliche

Effizienz steigern und bei Bedarf Innovationen umsetzen kann, um ihre Mission landesweit voranzutreiben. Aus diesem Grund nutzen viele Bundesbehörden heute AWS-Cloud-Services, um Bundesdaten zu verarbeiten, zu speichern und zu übertragen.

Weitere Informationen finden Sie unter [FedRAMP](#).

HIPAA: [AWS hat sein Programm zur Einhaltung des Health Insurance Portability and Accountability Act \(HIPAA\) um AMS als HIPAA-fähigen Service erweitert](#). Wenn Sie ein Business Associate Agreement (BAA) mit AWS abgeschlossen haben, können Sie AMS verwenden, um Ihre HIPAA-konformen Anwendungen zu erstellen.

In diesem [Whitepaper mit Schwerpunkt HIPAA](#) erfahren Sie, wie Sie AMS für die Verarbeitung und Speicherung von Gesundheitsinformationen nutzen können. Weitere Informationen finden Sie unter [HIPAA-Compliance](#).

HITRUST: Das Health Information Trust Alliance Common Security Framework (HITRUST CSF) nutzt national und international anerkannte Standards und Vorschriften wie GDPR, ISO, NIST, PCI und HIPAA, um umfassende grundlegende Sicherheits- und Datenschutzkontrollen zu schaffen.

[Weitere Informationen finden Sie unter HITRUST CSF.](#)

ISO ISO/IEC 27001:2013 ist ein Sicherheitsmanagementstandard, der bewährte Verfahren für das Sicherheitsmanagement und umfassende Sicherheitskontrollen gemäß den 27002-Leitlinien für bewährte Verfahren festlegt. ISO/IEC Grundlage dieser Zertifizierung ist die Entwicklung und Implementierung eines strengen Sicherheitsprogramms, das die Entwicklung und Implementierung eines Informationssicherheitsmanagementsystems (ISMS) umfasst, das festlegt, wie AWS die Sicherheit kontinuierlich auf ganzheitliche und umfassende Weise verwaltet.

Weitere Informationen finden Sie unter [ISO/IEC 27001:2013](#).

ISO ISO/IEC 27017:2015 enthält Leitlinien zu den Aspekten der Informationssicherheit von Cloud Computing und empfiehlt die Implementierung cloudspezifischer Informationssicherheitskontrollen, die die Leitlinien der Normen 27002 und 27001 ergänzen. ISO/IEC Dieser Verhaltenskodex enthält zusätzliche Leitlinien zur Implementierung von Informationssicherheitskontrollen, die speziell für Cloud-Dienstleister gelten.

Weitere Informationen finden Sie unter [ISO/IEC 27017:2015 Compliance](#).

ISO 27018: ISO/IEC 27018:2019 ist ein Verhaltenskodex, der sich auf den Schutz personenbezogener Daten in der Cloud konzentriert. Es basiert auf dem ISO/IEC Informationssicherheitsstandard 27002 und enthält Leitlinien zur Implementierung von ISO/IEC 27002-Kontrollen, die für personenbezogene Daten (PII) in öffentlichen Clouds gelten. Es enthält auch eine Reihe zusätzlicher Kontrollen und zugehöriger Leitlinien, die darauf abzielen, die Anforderungen an den Schutz personenbezogener Daten in öffentlichen Clouds zu erfüllen, die im bestehenden ISO/IEC Kontrollsatz 27002 nicht berücksichtigt wurden.

Weitere Informationen finden Sie unter [ISO/IEC 27018:2019 Compliance](#).

ISO 9001: ISO 9001:2015 beschreibt einen prozessorientierten Ansatz zur Dokumentation und Überprüfung der Struktur, Verantwortlichkeiten und Verfahren, die für ein effektives Qualitätsmanagement innerhalb einer Organisation erforderlich sind. Bestimmte Abschnitte der Norm enthalten Informationen zu Themen wie:

- Anforderungen an ein Qualitätsmanagementsystem, einschließlich der Dokumentation eines Qualitätshandbuchs, der Dokumentenkontrolle und der Festlegung von Prozessinteraktionen
- Verantwortlichkeiten des Managements
- Verwaltung der Ressourcen, einschließlich der Humanressourcen und des Arbeitsumfelds einer Organisation
- Entwicklung von Dienstleistungen, einschließlich der Schritte vom Entwurf bis zur Bereitstellung
- Kundenzufriedenheit
- Messung, Analyse und Verbesserung des QMS durch Aktivitäten wie interne Audits sowie Korrektur- und Präventivmaßnahmen

Weitere Informationen finden Sie unter Einhaltung der [Norm ISO 9001:2015](#).

PCI: AMS verfügt über eine Konformitätsbescheinigung für den Data Security Standard (DSS) der Payment Card Industry (PCI) Version 3.2 auf Service Provider-Stufe 1. Kunden, die AWS-Produkte und -Services zum Speichern, Verarbeiten oder Übertragen von Karteninhaberdaten verwenden, können AMS für die Verwaltung ihrer eigenen PCI-DSS-Konformitätszertifizierung verwenden.

Weitere Informationen über PCI DSS, einschließlich der Anforderung einer Kopie des AWS PCI Compliance Package, finden Sie unter [PCI DSS Level 1](#). Wichtig ist, dass Sie in AMS detaillierte Kennwortrichtlinien konfigurieren müssen, damit sie den Standards von PCI DSS Version 3.2 entsprechen. Einzelheiten dazu, welche Richtlinien durchgesetzt werden müssen, finden Sie unter [Aktivieren der PCI-Konformität für Ihr AWS Microsoft AD-Verzeichnis](#).

SOC: AMS System & Organization Control (SOC) Reports sind unabhängige Prüfungsberichte von Drittanbietern, die belegen, wie AMS wichtige Compliance-Kontrollen und -Ziele erreicht. Der Zweck dieser Berichte besteht darin, Ihnen und Ihren Prüfern zu helfen, die AMS-Kontrollen zu verstehen, die zur Unterstützung von Betriebsabläufen und zur Einhaltung von Vorschriften eingeführt wurden. Es gibt drei Arten von AMS SOC-Berichten:

- AWS SOC 1-Bericht — [Mit AWS Artifact herunterladen](#)
- AWS SOC 2: Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit — [Mit AWS Artifact herunterladen](#)
- [AWS SOC 3: Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit](#)

Weitere Informationen finden Sie unter [SOC-Compliance](#).

Gemeinsame Verantwortlichkeit

Sicherheit, einschließlich PCI-Konformität, ist eine [gemeinsame Verantwortung](#). Es ist wichtig zu verstehen, dass der AMS-Compliance-Status nicht automatisch für Anwendungen gilt, die Sie in der AWS Cloud ausführen. Sie müssen sicherstellen, dass Ihre Nutzung der AWS Dienste den Standards entspricht. Weitere Informationen darüber, wie AMS mit Kunden bei bestimmten Aktivitäten zusammenarbeitet, finden Sie im AMS [AMS-Verantwortungsmatrix \(RACI\)](#).

AMS Amazon-Maschinenbilder (AMIs)

AMS erstellt jeden Monat aktualisierte Amazon Machine Images (AMIs) für AMS-unterstützte Betriebssysteme. Darüber hinaus produziert AMS auch sicherheitsoptimierte Images (AMIs), die auf dem CIS Level 1-Benchmark für eine Untergruppe der von [AMS unterstützten Betriebssysteme](#) basieren. Informationen darüber, für welche Betriebssysteme ein Image mit verbesserter Sicherheit verfügbar ist, finden Sie im AMS Security User Guide, das auf der Seite AWS Artifact -> Berichte (finden Sie die Option Berichte im linken Navigationsbereich) verfügbar ist und nach AWS Managed Services gefiltert ist. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

Um Benachrichtigungen zu erhalten, wenn neue AMS veröffentlicht AMIs werden, können Sie ein Amazon Simple Notification Service (Amazon SNS) -Benachrichtigungsthema namens „AMS AMI“ abonnieren. Einzelheiten finden Sie unter [AMS-AMI-Benachrichtigungen mit SNS](#).

Die AMS-AMI-Namenskonvention lautet: `customer-ams-<operating system>-<release date> - <version>`. (zum Beispiel `customer-ams-rhel6-2018.11-3`)

Verwenden Sie nur AMS AMIs , die mit `beginnencustomer`.

AMS empfiehlt, immer das neueste AMI zu verwenden. Das neueste finden Sie auf einer der AMIs folgenden Arten:

- Schauen Sie in der AMS-Konsole auf der AMIsSeite nach.
- Anzeige der neuesten AMS AMI-CSV-Datei, verfügbar in Ihrem CSDM oder über diese ZIP-Datei: [AMS 11.2024 AMI-Inhalt und CSV-Datei in einer ZIP-Datei](#).

Frühere AMI-ZIP-Dateien finden Sie in der [Dokumentenhistorie](#).

- Diesen SKMS AMS-Befehl ausführen (AMS SKMS SDK erforderlich):

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

AMS AMI-Inhalt zur Basis hinzugefügt AWS AMIs, nach Betriebssystem (OS)

- Linux AMIs:
 - [AWS CLI-Tools](#)
 - [NTP](#)
 - [Trend Micro Endpoint Protection Service Agent](#)
 - [Code verteilen](#)
 - [PBIS//AD Bridge ist mehr als vertrauenswürdig](#)
 - [SSM-Agent](#)
 - Yum Upgrade für kritische Patches
 - Benutzerdefinierte AMS-Skripts/Verwaltungssoftware (Steuerung von Start, AD-Join, Überwachung, Sicherheit und Protokollierung)
- Windows-Server AMIs:
 - [Microsoft.NET Framework 4.5](#)
 - [PowerShell 5.1](#)
 - [AWS Tools für Windows PowerShell](#)
 - PowerShell AMS-Module zur Steuerung von Start, AD-Join, Überwachung, Sicherheit und Protokollierung
 - [Trend Micro Endpoint Protection Service Agent](#)
 - [SSM-Agent](#)
 - [CloudWatch Kundendienstmitarbeiter](#)
 - EC2Konfigurationsdienst (über Windows Server 2012 R2)
 - EC2Starten (Windows Server 2016 und Windows Server 2019)
 - EC2LaunchV2 (Windows Server 2022 und höher)

Linux-basiert: AMIs

- Amazon Linux 2023 (neueste Nebenversion) (Minimales AMI wird nicht unterstützt)

- Amazon Linux 2 (neueste Nebenversion)
- Amazon Linux (2ARM64)
- Red Hat Enterprise 7 (neueste Nebenversion)
- Red Hat Enterprise 8 (neueste Nebenversion)
- Red Hat Enterprise 9 (neueste Nebenversion)
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux: Eine Produktübersicht, Preisinformationen, Nutzungsinformationen und Supportinformationen finden Sie unter [Amazon Linux AMI \(HVM/64-Bit\)](#) und [Amazon Linux 2](#).

Weitere Informationen finden Sie unter [Amazon Linux FAQs 2](#).

- RedHat Enterprise Linux (RHEL): Eine Produktübersicht, Preisinformationen, Nutzungsinformationen und Supportinformationen finden Sie unter [Red Hat Enterprise Linux \(RHEL\) 7 \(HVM\)](#).
- Ubuntu Linux 18.04: Eine Produktübersicht, Preisinformationen, Nutzungsinformationen und Supportinformationen finden Sie [unter Ubuntu](#) 18.04 LTS — Bionic.
- SUSE Linux Enterprise Server für SAP-Anwendungen 15: SP6
 - Führen Sie die folgenden Schritte einmal pro Konto aus:
 1. Navigieren Sie zur AWS Marketplace.
 2. Suchen Sie nach dem SUSE 15 SAP-Produkt.
 3. Wählen Sie Weiter, um ein Abonnement abzuschließen.
 4. Wählen Sie Bedingungen akzeptieren aus.
 - Führen Sie jedes Mal, wenn Sie eine neue SUSE Linux Enterprise Server for SAP Applications SP6 15-Instanz starten müssen, die folgenden Schritte aus:
 1. Notieren Sie sich die AMI-ID für das abonnierte SUSE Linux Enterprise Server for SAP Applications 15 AMI.
 2. Eine Bereitstellung erstellen | Erweiterte Stack-Komponenten | EC2 Stack | Änderungstyp erstellen ct-14027q0sjyt1h RFC. *InstanceAmiId* Ersetzen Sie es durch die AWS Marketplace AMI-ID, die Sie abonniert haben.

Windows-basiert AMIs:

Microsoft Windows Server (2016, 2019 und 2022), basierend auf dem neuesten Windows AMIs.

Beispiele für die Erstellung AMIs finden Sie unter [Create AMI](#).

AMS AMIs auslagern:

AMS entzieht Ihnen während des Offboardings keine AMIs Informationen, um Auswirkungen auf Ihre Abhängigkeiten zu vermeiden. Wenn Sie AMS AMIs aus Ihrem Konto entfernen möchten, können Sie die `cancel-image-launch-permission` API verwenden, um bestimmte Informationen zu verbergen. AMIs Sie können beispielsweise das folgende Skript verwenden, um alle AMS auszublenden AMIs , die zuvor mit Ihrem Konto geteilt wurden:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

Sie müssen die AWS CLI v2 installiert haben, damit das Skript fehlerfrei ausgeführt werden kann. Die Installationsschritte für AWS CLI finden Sie unter [Installation oder Aktualisierung der neuesten Version der AWS-CLI](#). Einzelheiten zu dem `cancel-image-launch-permission` Befehl finden Sie unter [cancel-image-launch-permission](#).

Verbesserte Sicherheit AMIs

AMS stellt für eine Untergruppe der von AMS unterstützten Betriebssysteme sicherheitsoptimierte Images (AMIs) bereit, die auf dem CIS Level 1-Benchmark basieren. Informationen darüber, für welche Betriebssysteme ein Image mit verbesserter Sicherheit verfügbar ist, finden Sie im Kundensicherheitshandbuch für AWS Managed Services (AMS). Um auf dieses Handbuch zuzugreifen, öffnen Sie es AWS Artifact, wählen Sie im linken Navigationsbereich Berichte aus und filtern Sie dann nach AWS Managed Services. Anweisungen zum Zugriff erhalten AWS Artifact Sie bei Ihrem CSDM oder unter [Erste Schritte mit AWS Artifact](#).

So funktioniert die Integration zwischen AD FS und AMS

Eine unidirektionale Vertrauensstellung zwischen Ihrem lokalen Netzwerk und der AMS-Domäne ist die Standardmethode für den Zugriff auf Stacks und VPCs. Wenn eine VPC und ein Stack erstellt werden, wird der Zugriff über vorkonfigurierte Active Directory-Sicherheitsgruppen gewährt. Darüber

hinaus AWS-Managementkonsole kann der Zugriff auf die mithilfe des Active Directory Federation Service (AD FS) oder einer anderen Verbundsoftware, die SAML unterstützt, für eine einmalige Anmeldung (SSO) an der Management Console konfiguriert werden. AWS

 Note

AMS kann Verbindungen zu vielen Verbunddiensten wie Ping, Okta usw. herstellen. Sie sind nicht auf AD FS beschränkt. Hier finden Sie ein Beispiel für eine Verbundtechnologie, die Ihnen zur Verfügung steht.

Die Informationen hier stammen aus diesem Blogbeitrag: [Aktivieren des Verbunds für die AWS Verwendung von Windows Active Directory, AD FS und SAML 2.0](#).

1. Der Flow wird initiiert, wenn ein Benutzer (nennen wir ihn Bob) die AD FS-Beispielwebsite (<https://Fully.Qualified.Domain.Name>) aufruft. Here/adfs/ls/IdpInitiatedSignOn.aspx) innerhalb seiner Domäne. Wenn Sie AD FS installieren, erhalten Sie ein neues virtuelles Verzeichnis mit dem Namen adfs für Ihre Standardwebsite, das diese Seite enthält.
2. Die Anmeldeseite authentifiziert Bob gegenüber AD. Je nachdem, welchen Browser Bob verwendet, wird er möglicherweise zur Eingabe seines AD-Benutzernamens und Kennworts aufgefordert.
3. Bobs Browser empfängt eine SAML-Assertion in Form einer Authentifizierungsantwort von AD FS.
4. Bobs Browser sendet die SAML-Assertion an den AWS Anmeldeendpunkt für SAML (/saml). <https://signin.aws.amazon.com> Hinter den Kulissen verwendet die Anmeldung die [AssumeRoleWithSAML-API](#), um temporäre Sicherheitsanmeldedaten anzufordern, und erstellt dann eine Anmelde-URL für AWS-Managementkonsole
5. Bobs Browser empfängt die Anmelde-URL und wird zur Konsole weitergeleitet.

Aus Bobs Sicht läuft der Prozess transparent ab. Er beginnt auf einer internen Website und endet auf der AWS-Managementkonsole, ohne jemals AWS Anmeldeinformationen angeben zu müssen.

 Note

Weitere Informationen zur Konfiguration des Verbunds mit der AMS-Konsole finden Sie unter:

- Landing Zone für mehrere Konten: [Konfiguration des Verbunds zur AMS-Konsole](#)

- Landing Zone für ein einzelnes Konto: [Konfiguration des Verbunds zur AMS-Konsole](#)

Weitere Informationen finden Sie im [Anhang: AD FS-Anspruchsregel und SAML-Einstellungen](#). Informationen zur Verwendung von AWS Microsoft AD zur Unterstützung Ihrer Active Directory-fähigen Anwendungen in der AWS Cloud, die Compliance-Anforderungen unterliegen, finden Sie unter [Microsoft AD-Compliance verwalten](#).

Von AMS verwaltetes Active Directory

AMS bietet jetzt einen neuen Dienst namens Managed Active Directory (auch bekannt als Managed AD) an, der es AMS ermöglicht, sich um den Betrieb Ihrer Active Directory-Infrastruktur (AD) zu kümmern, während Sie gleichzeitig die Kontrolle über Ihre Active Directory-Verwaltung behalten.

Die AMS-Unterstützung für Managed AD ähnelt der AMS-Unterstützung für den Amazon Relational Database Service (Amazon RDS). In beiden Fällen AWS (einschließlich AMS) werden die Erstellung und Verwaltung der Infrastruktur, auf der der Service ausgeführt wird, unterstützt, während Sie gleichzeitig die Zugriffskontrolle und alle Verwaltungsfunktionen übernehmen. Dieses Modell bietet die folgenden Vorteile:

- Schränkt Sicherheitsrisiken ein: AWS AMS benötigt keine Administratorrechte für Ihre Domain.
- Direkte Integrationen: Sie können Ihr aktuelles Autorisierungsmodell verwenden und es in AD integrieren, ohne eine Schnittstelle zu AMS herstellen zu müssen.

Hinweise:

- Weder AMS noch Sie haben Zugriff auf Ihre Managed AD-Domänencontroller, sodass keine Software auf den Domain-Controllern installiert werden kann. Dies ist wichtig, da Lösungen von Drittanbietern, für die Software auf Domänencontrollern installiert werden muss, nicht zulässig sind.

Access funktioniert wie folgt:

- AWS Verzeichnisdienst-Team: Hat Zugriff auf Domänencontroller.
- AMS: Hat Zugriff auf den Directory Service APIs, um bestimmte Aktionen auf der Domain auszuführen. Zu diesen Aktionen gehören das Erstellen von AD-Snapshots, das Ändern des AD-Schemas und andere Aktionen.
- Sie: Sie haben Zugriff auf die Domain (AD), um Benutzer, Gruppen usw. zu erstellen.

- Wir empfehlen Ihnen, vor der Migration Ihres Unternehmens-AD einen Machbarkeitsnachweis für Managed AD durchzuführen, da nicht alle Funktionen einer herkömmlichen AD-Umgebung in einer Managed AD-Umgebung verfügbar sind.
- AMS wird Ihr AD-Management nicht verwalten oder Ihnen diesbezüglich weiterhelfen. AMS stellt beispielsweise keine Leitlinien zur Struktur der Organisationseinheit, zur Gruppenrichtlinienstruktur, zu Konventionen zur Benennung von AD-Benutzern usw. bereit.

Das funktioniert wie folgt:

1. AMS installiert eine neue AWS-Konto für Sie, getrennt von und zusätzlich zu Ihrem AMS-Konto, und stellt über Directory Service eine Active Directory (AD) -Umgebung AWS bereit (siehe auch [Was ist AWS Directory Service?](#)).

Die folgenden Informationen müsste ein Systemintegrator von Ihnen einholen, damit AMS Managed AD integrieren kann:

- Informationen zum Konto
 - Konto-ID des AWS-Konto , das für Ihr von AMS verwaltetes AD erstellt wurde: Nummer AWS-Konto
 - Region, in der Sie Ihr Managed AD einbinden möchten für: AWS-Region
- Informationen zu verwaltetem Active Directory:
 - Microsoft AD Edition: Standard/Enterprise. AWS Microsoft AD (Standard Edition) umfasst 1 GB Verzeichnisobjektspeicher. Diese Kapazität kann bis zu 5.000 Benutzer oder 30.000 Verzeichnisobjekte, einschließlich Benutzer, Gruppen und Computer, unterstützen. AWS Microsoft AD (Enterprise Edition) umfasst 17 GB Verzeichnisobjektspeicher, der bis zu 100.000 Benutzer oder 500.000 Objekte unterstützen kann.

Weitere Informationen finden Sie unter [AWS Directory Service FAQs](#).

- Domain-FQDN: Der FQDN für Ihre AMS Managed AD-Domain.
- Domain-NetBIOS-Name: Der NetBIOS-Name für Ihre AMS Managed AD-Domäne.
- Kontonummern der AMS-Standardkonten, für die Sie eine Managed AD-Integration wünschen (AMS konfiguriert eine unidirektionale Vertrauensstellung vom AD des AMS-Standardkontos zum Managed AD)
- Sind Änderungen am Active Directory-Schema erforderlich und wenn ja, welche Änderungen?
- Standardmäßig werden zwei Domänencontroller bereitgestellt. Benötigen Sie mehr? Falls ja, wie viele benötigen Sie und aus welchem Grund?

- Netzwerke für verwaltete Active Directory-Informationen:
 - Managed AD VPC CIDR für Domänencontroller (ein CIDR in Ihrem privaten Subnetzbereich für die Managed AD-Domänencontroller):
 - Subnetz CIDR 1 für Domänencontroller: [Ihr CIDR, muss Teil von AMS Managed AD VPC CIDR sein]
 - Subnetz CIDR 2 für Domänencontroller: [Ihr CIDR, muss Teil von AMS Managed AD VPC CIDR sein]

Beispiel:

- Verwaltetes AD-VPC-CIDR: 192.168.0.0/16
- CIDR 1 für Domänencontroller: 192.168.1.0/24
- CIDR 2 für Domänencontroller: 192.168.2.0/24

Um IP-Adresskonflikte zu vermeiden, stellen Sie sicher, dass das von Ihnen angegebene Managed AD VPC CIDR nicht mit einem anderen privaten Subnetz-CIDR in Konflikt steht, das Sie in Ihrem Unternehmensnetzwerk verwenden.

- VPN-Technologie (optional): [Direct Connect/Direct Connect und VPN]
 - Die autonome BGP Systemnummer (ASN) Ihres Gateways: [Vom Kunden bereitgestellte ASN]
 - Die über das Internet routbare IP-Adresse für die externe Schnittstelle Ihres Gateways. Die Adresse muss statisch sein: [Vom Kunden bereitgestellte IP-Adresse]
 - Ob Ihre VPN-Verbindung statische Routen erfordert oder nicht: [ja/nein]
2. AMS stellt Ihnen das Administratorkonto-Passwort für die AD-Umgebung zur Verfügung und fordert Sie auf, das Passwort zurückzusetzen, sodass AMS-Techniker nicht mehr auf Ihre AD-Umgebung zugreifen können.
 3. Um das Passwort für das Administratorkonto zurückzusetzen, stellen Sie mithilfe von Active Directory-Benutzern und -Computern (ADUC) eine Verbindung zu Ihrer Active Directory-Umgebung her. ADUC und andere Remote Server Administration Tools (RSAT) sollten auf administrativen Hosts installiert und ausgeführt werden, die Sie in einer Infrastruktur ohne AMS bereitgestellt haben. Microsoft verfügt über bewährte Methoden zur Sicherung solcher administrativer Hosts. Informationen finden Sie unter [Implementieren sicherer administrativer Hosts](#). Sie verwalten Ihre Active Directory-Umgebung mithilfe dieser administrativen Hosts.
 4. Im täglichen Betrieb kümmert sich AMS um alles, was AWS-Konto bis zum AWS Directory Service reicht, z. B. die VPC-Konfiguration, AD-Backups, Erstellung und Löschung von

AD-Vertrauensstellungen usw. Sie verwenden und verwalten Ihre AD-Umgebung, z. B. Benutzererstellung, Gruppenerstellung, Gruppenrichtlinienerstellung usw.

Die aktuelle RACI-Tabelle finden Sie im Abschnitt „Rollen und Verantwortlichkeiten“ in der [Servicebeschreibung](#) von See.

Bereitstellungen von AMS-Anwendungen

Das AMS-Handbuch für Anwendungsentwickler enthält detaillierte Beschreibungen und exemplarische Vorgehensweisen für die folgenden Bereitstellungen:

- Mit dem AMS Workload Ingest CT können Sie und ein AMS-Cloud-Migrationspartner Ihre vorhandenen Workloads problemlos in eine von AMS verwaltete VPC verschieben. Mithilfe von AMS Workload Ingest können Sie ein AMS-AMI erstellen, indem Sie einen RFC mit der migrierten Instanz Deployment | Ingestion | Stack from Migration Partner | Create CT (ct-257p9zjk14ija) einreichen. Sie müssen eine Instance von Ihrem lokalen Standort auf AWS einen Migrationspartner migrieren lassen, sowie eine AMS-Ziel-VPC und ein Subnetz, in das die Instance aufgenommen wird.

[Einzelheiten finden Sie im AMS Application Developer's Guide unter Workload Ingest.](#)

- Mit der Funktion „CloudFormation Ingest Change Type“ (ct-36cn2avfrrj9v) können Sie auf einfache Weise eine vorhandene CloudFormation Vorlage verwenden, um benutzerdefinierte Stacks in einer von AMS verwalteten VPC bereitzustellen.

[Einzelheiten finden Sie im AMS-Leitfaden für Anwendungsentwickler unter Template Ingest. CloudFormation](#)

- Sie können Ihre lokale Datenbank in eine neue Datenbank in Ihren AMS-verwalteten Amazon S3 S3-Bucket oder Ihre Amazon RDS-Instance importieren. Dazu verwenden Sie die Änderungstypen Deployment | Erweiterte Stackkomponenten | Database Migration Service (DMS), einschließlich Replikationsinstanz erstellen (ct-27apldkhqr0ol), Replikationssubnetzgruppe erstellen (ct-2q5azjd8p1ag5), Replikationsaufgabe erstellen (ct-1d2fml15b9eth), Quellendpunkt erstellen (ct-0attesnjqy2cx) oder Quellendpunkt erstellen (S3) (ct-2oxl37nphsrjz) und Zielendpunkt erstellen (ct-3gf8dolbo8x9p) oder Zielendpunkt erstellen (S3) (ct-05muqzievnxk5).

Einzelheiten finden Sie im AMS Application Developer's Guide unter [Database Migration Service](#).

- Sie können Ihre lokale MS SQL-Datenbank in eine neue Datenbank auf Ihrer von AMS verwalteten RDS-SQL-Instance importieren. Dazu verwenden Sie eine Vielzahl von AMS-Änderungstypen und die Amazon RDS-API sowie AWS Konsolen.

Einzelheiten finden Sie im AMS-Anwendungsleitfaden unter [Database \(DB\) Import to MS SQL RDS](#).

Servicemanagement in AWS Managed Services

Themen

- [Kontoverwaltung in AWS Managed Services](#)
- [Beginn des Dienstes in AWS Managed Services](#)
- [Kundenbeziehungsmanagement \(CRM\)](#)
- [Kostenoptimierung in AWS Managed Services](#)
- [Servicezeiten in AWS Managed Services](#)
- [Hilfe zu AWS Managed Services erhalten](#)

So funktioniert der AMS-Service für Sie.

Kontoverwaltung in AWS Managed Services

In diesem Abschnitt wird die AMS-Kontoverwaltung behandelt.

Ihnen wird ein Cloud Service Delivery Manager (CSDM) zugewiesen, der Ihnen bei AMS beratend zur Seite steht und über ein detailliertes Verständnis Ihres Anwendungsfalls und Ihrer Technologiearchitektur für die verwaltete Umgebung verfügt. CSDMs arbeiten mit Kundenbetreuern, technischen Kundenbetreuern, AWS Managed Services Services-Cloudarchitekten (CAs) und AWS-Lösungsarchitekten (SAs) zusammen, um bei der Einführung neuer Projekte zu helfen und Empfehlungen zu bewährten Methoden während der gesamten Softwareentwicklungs- und Betriebsprozesse zu geben. Das CSDM ist die wichtigste Anlaufstelle für AMS. Die wichtigsten Aufgaben Ihres CSDM sind:

- Organisieren und leiten Sie monatliche Besprechungen zur Servicebewertung mit Kunden.
- Geben Sie Einzelheiten zur Sicherheit, zu Softwareupdates für die Umgebung und zu Optimierungsmöglichkeiten an.
- Machen Sie sich für Ihre Anforderungen, einschließlich Funktionsanfragen für AMS, stark.
- Beantworten und lösen Sie Anfragen zur Abrechnung und Serviceberichterstattung.
- Bieten Sie Einblicke für Empfehlungen zur Finanz- und Kapazitätsoptimierung.

Beginn des Dienstes in AWS Managed Services

Beginn des Service: Das Datum des Servicebeginns für ein AWS Managed Services Services-Konto ist der erste Tag des ersten Kalendermonats, nach dem AWS Sie darüber informiert, dass die in den Onboarding-Anforderungen für dieses AWS Managed Services Services-Konto festgelegten Aktivitäten abgeschlossen wurden. Sofern AWS eine solche Benachrichtigung nach dem 20. Tag eines Kalendermonats sendet, ist das Datum des Servicebeginns der erste Tag des zweiten Kalendermonats nach dem Datum dieser Benachrichtigung.

Beginn des Dienstes

- R steht für verantwortliche Partei, die die Arbeit zur Erfüllung der Aufgabe erledigt.
- I steht für informiert, d. h. eine Partei, die über den Fortschritt informiert wird, oft erst, wenn die Aufgabe oder das Ergebnis abgeschlossen ist.

Beginn der Dienstleistung

Schritt #	Titel des Schritts	Beschreibung	Customer	AMS
1.	Übergabe des AWS-Kontos an Kunden	Der Kunde erstellt ein neues AWS-Konto und übergibt es an AWS Managed Services	R	I
2.	AWS Managed Services Services-Konto — Design	Finalisieren Sie den Entwurf des AWS Managed Services Services-Kontos	I	R
3.	AWS Managed Services Services-Konto — erstellen	Ein AWS Managed Services Services-Konto wird gemäß dem Design in Schritt 2 erstellt	I	R

Kundenbeziehungsmanagement (CRM)

AWS Managed Services (AMS) bietet einen CRM-Prozess (Customer Relationship Management), um sicherzustellen, dass eine klar definierte Beziehung zu Ihnen aufgebaut und aufrechterhalten wird. Die Grundlage dieser Beziehung bildet das Wissen von AMS über Ihre Geschäftsanforderungen. Der CRM-Prozess ermöglicht ein genaues und umfassendes Verständnis von:

- Ihre Geschäftsanforderungen und wie Sie diese Bedürfnisse erfüllen können
- Ihre Fähigkeiten und Einschränkungen
- AMS und Ihre unterschiedlichen Verantwortlichkeiten und Pflichten

Der CRM-Prozess ermöglicht es AMS, einheitliche Methoden zur Erbringung von Dienstleistungen für Sie und zur Steuerung Ihrer Beziehung zu AMS zu verwenden. Der CRM-Prozess umfasst:

- Identifizierung Ihrer wichtigsten Stakeholder
- Aufbau eines Führungsteams
- Durchführung und Dokumentation von Besprechungen zur Leistungsbeurteilung mit Ihnen
- Bereitstellung eines formellen Servicebeschwerdeverfahrens mit einem Eskalationsverfahren
- Implementierung und Überwachung Ihres Zufriedenheits- und Feedback-Prozesses
- Verwaltung Ihres Vertrags

CRM-Prozess

Der CRM-Prozess umfasst die folgenden Aktivitäten:

- Identifizieren und Verstehen Ihrer Geschäftsprozesse und Bedürfnisse. Ihre Vereinbarung mit AMS identifiziert Ihre Stakeholder.
- Definition der Dienstleistungen, die gemäß Ihren Bedürfnissen und Anforderungen erbracht werden sollen.
- Treffen mit Ihnen im Rahmen der Serviceüberprüfung, um alle Änderungen des AMS-Serviceumfangs, der SLA, des Vertrags und Ihrer Geschäftsanforderungen zu besprechen. Es können vorläufige Treffen mit Ihnen abgehalten werden, um Leistungen, Erfolge, Probleme und Aktionspläne zu besprechen.
- Überwachen Sie Ihre Zufriedenheit mithilfe unserer Kundenzufriedenheitsumfrage und des Feedbacks, das Sie bei Besprechungen erhalten.

- Berichterstattung über die Leistung in monatlichen, intern gemessenen Leistungsberichten.
- Wir besprechen den Service gemeinsam mit Ihnen, um Verbesserungsmöglichkeiten zu ermitteln. Dazu gehört auch die regelmäßige Kommunikation mit Ihnen über das Niveau und die Qualität des erbrachten AMS-Dienstes.

CRM-Besprechungen

Die AMS Cloud Service Delivery Manager (CSDMs) führen regelmäßig Treffen mit Ihnen durch, um die einzelnen Servicebereiche (Betrieb, Sicherheit und Produktinnovationen) und die Führungsqualitäten (SLA-Berichte, Zufriedenheitsmaßnahmen und Änderungen Ihrer Geschäftsanforderungen) zu besprechen.

Meeting	Zweck	Mode	Teilnehmer
Wöchentliche Statusüberprüfung (optional)	Ausstehende Probleme oder Vorfälle, Patches, Sicherheitsereignisse, Problemaufzeichnungen Betriebstrend über 12 Wochen (+/- 6) Bedenken des Anwendungsbetreibers Zeitplan für das Wochenende	Kunde vor Ort location/ Telecom/Chime	AMS: CSDM und Cloud-Architekt (CA) Vom Kunden zugewiesene Teammitglieder (z. B.: Cloud-/ Infrastruktur-, Anwendungssupport-, Architekturteams usw.)
Monatlicher Geschäftsbericht	Überprüfen Sie die Leistung auf Serviceniveau (Berichte, Analysen und Trends) Finanzielle Analyse Produkt-Roadmap BESETZUNG	Kunde vor Ort location/ Telecom/Chime	AMS: CSDM, Cloud-Architekt (CA), AMS-Kundenbetreuer, Technischer Produktmanager (TPM) von AMS (optional), AMS

Meeting	Zweck	Mode	Teilnehmer
			OPS-Manager (optional) Sie: Vertreter des Anwendungsbetreibers
Vierteljährlicher Geschäftsbericht	Leistung und Trends der Scorecard und des Service Level Agreements (SLA) (6 Monate) Künftige Pläne/Migrationen für die kommenden 3/6/9/12 Monate Risiko und Risikominderung Wichtige Verbesserungsinitiativen Artikel der Produkt-Roadmap Auf die zukünftige Ausrichtung ausgerichtete Möglichkeiten Finanzdaten Initiativen zur Kosteneinsparung Geschäftsoptimierung	Standort des Kunden vor Ort	AMS: CSDM, Cloud-Architekt, AMS-Kundenbetreuer, AMS-Serviceleiter, AMS-Betriebsleiter Sie: Vertreter des Anwendungsbetreibers, Servicemitarbeiter, Serviceleiter

Vereinbarungen für CRM-Treffen

Das AMS CSDM ist für die Dokumentation des Treffens verantwortlich, einschließlich:

- Erstellung der Tagesordnung, einschließlich Aktionspunkten, Themen und Teilnehmerlisten.
- Erstellung der Liste der Aktionspunkte, die bei jeder Sitzung überprüft werden, um sicherzustellen, dass die Punkte termingerecht abgeschlossen und gelöst werden.

- Verteilung des Sitzungsprotokolls und der Liste der Aktionspunkte per E-Mail an die Besprechungsteilnehmer innerhalb eines Werktages nach der Besprechung.
- Speichern von Besprechungsprotokollen im entsprechenden Dokumentenspeicher.

In Ermangelung des CSDM erstellt und verteilt der AMS-Vertreter, der die Sitzung leitet, das Protokoll.

Note

Ihr CSDM arbeitet mit Ihnen zusammen, um Ihre Kontoverwaltung festzulegen.

Monatliche CRM-Berichte

Ihr AMS CSDM bereitet monatliche Präsentationen zur Serviceleistung vor und versendet sie. Die Präsentationen enthalten Informationen zu folgenden Themen:

- Datum des Berichts
- Zusammenfassung und Einblicke:
 - Wichtige Hinweise: Gesamtzahl und Anzahl der aktiven Stacks, Status der Stack-Patches, Onboarding-Status des Accounts (nur beim Onboarding), Zusammenfassungen der kundenspezifischen Probleme
 - Leistung: Statistiken zur Behebung von Vorfällen, zu Warnmeldungen, Patches, Änderungsanfragen (RFCs), Serviceanfragen sowie zur Verfügbarkeit von Konsole und API
 - Probleme, Herausforderungen, Bedenken und Risiken: Status der kundenspezifischen Probleme
 - Künftige Themen: Kundenspezifische Onboarding- oder Problemlösungspläne
- Verwaltete Ressourcen: Grafiken und Kreisdiagramme von Stapeln
- AMS-Metriken: Überwachungs- und Ereignismetriken, Vorfallkennzahlen, AMS-SLA-Einhaltungskennzahlen, Serviceanforderungskennzahlen, Change-Management-Metriken, Speichermetriken, Kontinuitätskennzahlen, Trusted Advisor Advisor-Metriken und Kostenübersichten (auf verschiedene Arten dargestellt). Anfragen zu Funktionen. Kontaktinformationen.

 Note

Zusätzlich zu den beschriebenen Informationen informiert Sie Ihr CSDM auch über jede wesentliche Änderung des Geltungsbereichs oder der Bedingungen, einschließlich der Inanspruchnahme von Subunternehmern durch AMS für betriebliche Aktivitäten.

AMS generiert Berichte über Patches und Backups, die Ihr CSDM in Ihren monatlichen Bericht aufnimmt. Als Teil des Systems zur Berichtsgenerierung fügt AMS Ihrem Konto einige Infrastrukturen hinzu, auf die Sie nicht zugreifen können:

- Ein S3-Bucket mit den gemeldeten Rohdaten
- Eine Athena-Instanz mit Abfragedefinitionen zum Abfragen der Daten
- Ein Glue Crawler zum Lesen der Rohdaten aus dem S3-Bucket

Kostenoptimierung in AWS Managed Services

AWS Managed Services stellt Ihnen im Rahmen Ihrer monatlichen Geschäftsberichte jeden Monat detaillierte Berichte zur Kostenauslastung und zu Einsparungen bereit (MBRs).

AMS folgt einer Reihe von Standardprozessen und -mechanismen, um Möglichkeiten zur Kosteneinsparung in Ihren verwalteten Konten zu ermitteln und Sie bei der Planung und Einführung der Änderungen zur Optimierung Ihrer AWS-Ausgaben zu unterstützen.

 Note

AMS entwickelt derzeit ein Video, das Ihnen bei der Kostenoptimierung helfen soll. Der erste Schritt besteht darin, Ihnen ein PDF und eine Excel-Tabelle mit bewährten Methoden zur Kostenoptimierung zur Verfügung zu stellen. Um auf diese Ressourcen zuzugreifen, öffnen Sie die ZIP-Datei mit der [Kurzanleitung zur Kostenoptimierung](#).

Framework zur Kostenoptimierung

AMS verfolgt gemeinsam mit Ihnen einen dreistufigen Ansatz, um Ihre AWS-Kosten zu optimieren:

1. Identifizieren Sie Möglichkeiten zur Kostenoptimierung in Ihrer verwalteten Umgebung
2. Stellen Sie Ihnen einen Plan zur Kostenoptimierung vor
3. Unterstützen Sie uns dabei, die Kostenoptimierung auf messbare Weise zu erreichen

Identifizieren Sie Möglichkeiten zur Kostenoptimierung in der verwalteten Umgebung

AMS verwendet AWS native Tools wie Cost Explorer und Trusted Advisor und nutzt gleichzeitig über 20 Kosteneinsparungsmuster in den Bereichen Architekturoptimierung, EC2 instanzorientierte und AWS kundenorientierte Optimierung, um maßgeschneiderte Kosteneinsparungsempfehlungen für Sie zu erstellen.

Einige der Optimierungsempfehlungen beinhalten die folgenden.

Empfehlungen zur architektonischen Optimierung:

- **Optimale Nutzung der S3-Speicherklasse:** Amazon S3 bietet eine Reihe von Speicherklassen, um verschiedene Workload-Anforderungen in Bezug auf Datenzugriff, Ausfallsicherheit und Kosten zu erfüllen. S3 Intelligent-Tiering und S3-Speicherklassenanalysen auf der Grundlage der Workload-Anforderungen ermöglichen es Ihnen, die S3-Kosten effizient zu verwalten.
- **Verwendung von Caching-Architekturen:** Durch die Nutzung von Cache-Instanzen können Sie gegebenenfalls einige Datenbankinstanzen ersetzen und gleichzeitig Ihre IOPS-Anforderungen erfüllen.
- **Einsparungen beim EBS-Upgrade:** Die Migration Ihrer EBS-Volumes von gp2 auf gp3 bietet Kosteneinsparungen von bis zu 20% und Sie können unabhängig von der Volume-Größe von einer vorhersehbaren Basisleistung von 3.000 IOPS und 125 MiB/s profitieren.
- **Einsatz von Elastizität:** Die Funktionen zur auto-scaling AWS ermöglichen eine effektive Ressourcennutzung und Möglichkeiten zur Kostenoptimierung. Durch die regelmäßige Überprüfung und Aktualisierung der Richtlinien zur Instanzskalierung je nach Bedarf können weitere Kosten eingespart werden.

EC2 instanzorientierte Empfehlungen

- **Richtige Dimensionierung von Instanzen:** Die Empfehlungen konzentrierten sich auf die Dimensionierung der Instanzen und die optimale Konfiguration auf der Grundlage der Nutzung. Zu den Empfehlungen gehören auch die Nutzung der Amazon EC2 Auto Scaling Scaling-Funktion und das Ersetzen von EC2 Instances, sofern zutreffend, durch statische Webinhalte auf Amazon S3 usw. AWS Lambda
- **Instance-Planung:** Die Verwendung von AMS Resource Scheduler zum automatischen Starten und Stoppen von Instances auf der Grundlage eines Zeitplans trägt dazu bei, die Kosten einzudämmen, insbesondere für Instances, die nicht zur Produktion gehören und außerhalb der Geschäftszeiten nicht genutzt werden.

- Sparpläne abonnieren: Der Sparplan ist die einfachste Möglichkeit, bei der Nutzung zu sparen. AWS Die EC2 Instance-Sparpläne bieten bis zu 72% Einsparungen bei der Nutzung Ihrer Amazon EC2 Instances im Vergleich zu On-Demand-Preisen. Die Amazon SageMaker AI-Sparpläne bieten bis zu 64% Ersparnis bei der Nutzung Ihrer Amazon SageMaker AI-Services. AMS gibt Ihnen auf der Grundlage Ihrer AWS Ressourcennutzung entsprechende Empfehlungen zu Sparplänen.
- Hinweise zur Nutzung und Nutzung von Reserved Instances (RI): Amazon EC2 Reserved Instances (RI) bieten einen erheblichen discount (bis zu 75%) im Vergleich zu On-Demand-Preisen und ermöglichen eine Kapazitätsreservierung, wenn sie in einer bestimmten Availability Zone verwendet werden.
- Nutzung von Spot-Instances: Fehlertolerante Workloads können Spot-Instances nutzen und die Preise um bis zu 90% senken.
- Kündigung von Instances im Leerlauf: Identifizierung und Meldung von Instances, die sich im Leerlauf befinden oder nur eine geringe Auslastung aufweisen und beendet werden können.

Kundenorientierte Empfehlungen

- Kontobereinigung: Auf Kontoebene identifiziert AMS auch nicht genutzte EBS-Volumes, doppelte CloudTrail Pfade, leere Konten mit ungenutzten Ressourcen usw. und gibt Empfehlungen für die Bereinigung.
- SLA-Empfehlungen: Darüber hinaus überprüft AMS Ihre Plus- und Premium-Konten regelmäßig und empfiehlt, die richtige SLA-Stufe für die Konten zu wählen.
- Optimierung der AMS-Automatisierung: AMS optimiert kontinuierlich die AMS-Automatisierung und die Infrastruktur, die für die Bereitstellung von AMS-Diensten verwendet wird.

Präsentieren Sie Kunden und unterstützen Sie sie bei der Planung

AMS führt monatliche Geschäftsüberprüfungen (MBRs) mit den wichtigsten Kundenakteuren durch und stellt die identifizierten Möglichkeiten, Mechanismen und Empfehlungen zur Kosteneinsparung sowie mögliche Kosteneinsparungen vor. Wir arbeiten weiter mit Ihnen zusammen, um die erforderlichen Änderungen zu planen.

Unterstützung bei der Umsetzung der Empfehlungen und Messung der Kostenauswirkungen

AMS hilft bei der Erzielung und Messung von Kostenauswirkungen und Optimierungsänderungen.

Sie bewerten die Auswirkungen, Risiken und Erfolgskriterien der empfohlenen Änderungen auf die Anwendung und stellen über die AMS-Konsole die entsprechenden Änderungsanträge (RFCs). AMS arbeitet mit Ihnen zusammen und implementiert die Änderungen im Zusammenhang mit der Kostenoptimierung in Ihren verwalteten Konten. AMS misst die Auswirkungen auf die Kosten und bezieht die erzielten Einsparungen in die monatlichen Geschäftsberichte ein (MBRs).

Verantwortungsmatrix für die Kostenoptimierung

Verantwortlichkeiten bei der AMS-Kostenoptimierung.

Kostenoptimierung RACI

Aktivität	Customer	AMS
Zusammenfassung von Empfehlungen zur Kosteneinsparung und Erstellung des Berichts	I	R
Vorlage des Kosteneinsparungsberichts	C	R
Planungsänderungen im Zusammenhang mit Kostenein	R	C

Aktivität	Customer	AMS
sparungen		
Bewertung der Auswirkungen und des Risikos der Änderung	R	C
Erhebung RFCs zur Umsetzung der Änderungen	R	C
Überprüfung RFCs und Umsetzung der Änderungen	C	R
Testen der Anwendung und Validierung der Änderungsimplementierung	R	C

Aktivität	Customer	AMS
Messung der Kostenauswirkungen nach der Änderung und Präsentation beim Kunden	I	R

Servicezeiten in AWS Managed Services

Funktion	AMS für Fortgeschrittene
	Premium-Stufe
Serviceanfrage	24/7
Verwaltung von Zwischenfällen (P2-P3)	Rund um die
Sicherung und Wiederherstellung	24/7
Patch-Management	24/7
Überwachen und Warnen	24/7
Automatisierte Änderungsanforderung (RFC)	24/7
Nicht automatisierter Änderungsantrag (RFC)	24/7
Manager für die Bereitstellung von Cloud-Diensten (CSDM)	Montag bis Freitag: 08:00 — 17:00 Uhr, lokale Geschäftszeiten

Hilfe zu AWS Managed Services erhalten

AMS unterstützt Sie mit Incident Management, Service Request Management und Change Management 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr (gemäß dem für das Konto geltenden AMS Service Level Agreement).

Um ein Leistungsproblem mit dem AWS- oder AMS-Service zu melden, das sich auf Ihre verwaltete Umgebung auswirkt, verwenden Sie die AMS-Konsole und reichen Sie einen Vorfallbericht ein. Einzelheiten finden Sie unter [Einen Vorfall melden](#). Allgemeine Informationen zum AMS Incident Management finden Sie unter [Reaktion auf Vorfälle](#).

Verwenden Sie die AMS-Konsole und reichen Sie eine Serviceanfrage ein, um Informationen oder Ratschläge zu erhalten oder zusätzliche Services von AMS in Anspruch zu nehmen. Einzelheiten finden Sie [unter Serviceanfrage erstellen](#). Allgemeine Informationen zu AMS-Serviceanfragen finden Sie unter [Verwaltung von Serviceanfragen](#).

Verwaltung geplanter Ereignisse in AWS Managed Services

AWS Managed Services (AMS) Planned Event Management (PEM) ist ein AMS-Serviceangebot. PEM engagiert, koordiniert und unterstützt Kundenveranstaltungen und Projekte mithilfe von AMS-Services. PEM hilft bei der Koordination einer Reihe von relevanten Themen RFCs, die dem vereinbarten Umfang und Zeitplan der PEM-Veranstaltung oder des Projekts entsprechen.

AMS PEM-Kriterien

Eine geplante Veranstaltung ist ein umfangs- und zeitgebundenes Projekt. AMS verwendet die von Ihnen bereitgestellten Informationen (einschließlich Plan und Umfang, erwartete Ergebnisse und Änderungen, die der AMS-Betrieb voraussichtlich vornehmen wird), um Sie während der PEM-Aktivitäten effektiv zu unterstützen. Ihre Cloud-Architekten (CAs) überprüfen und bewerten dann die PEM-Aktivität auf Vollständigkeit, technische Implementierung und Einsatz des AMS Operations. Nach der Überprüfung durch CA überprüft AMS Operations die Pläne und stimmt sich mit Ihrem Cloud Service Delivery Manager (CSDM) über die Einbindung des Betriebsteams ab.

Arten von PEM

Im Folgenden sind die verfügbaren PEM-Typen aufgeführt:

- **Spieltage**
 - **Operational Gameday:** Ein szenariobasierter Spielansatz zur operativen Reaktion, der darauf abzielt, die Integration von Prozessen, Personen und Systemen zu validieren.
 - **Security Gameday:** Eine Strategie zur Reaktion auf Sicherheitsvorfälle, die einen szenariobasierten Spielansatz verwendet, um die Integration von Systemen, Prozessen und Personal zu bewerten.
- **BYOEPS:** Verwenden Sie die AMS-Funktion „Bring Your Own Endpoint Security“ (BYOEPS), um den standardmäßigen Trend Micro Deep Security Agent durch Ihre bevorzugte Endpunktsicherheitslösung oder eine benutzerdefinierte Trend Micro Lizenz zu ersetzen. Weitere Informationen finden Sie unter [AMS bring dein eigenes EPS mit](#).
- **Disaster Recovery:** Bei Disaster Recovery-Ereignissen unterstützt AMS Sie bei Ihren geplanten DR-Aktivitäten. Weitere Informationen finden Sie unter [Planung der Notfallwiederherstellung](#).
- **Sicherheitsereignis für Kunden:** Geplante Sicherheitsereignisse. Zum Beispiel Root-Benutzeraktivitäten und Penetrationstests.

- Migrationsunterstützung: Support für geplante Onboarding- und Migrationsaktivitäten.

Dieser Workflow erleichtert die Zusammenarbeit mit AMS bei der Koordination von geplanten Veranstaltungen und Migrationsaktivitäten im Zusammenhang mit dem AMS-Support. Für die vorrangige Ausführung von ist es eine bewährte Methode RFCs, das Operations on Demand (OOD) - Engagement zu verwenden. Weitere Informationen finden Sie unter [Betrieb auf Abruf](#).

Der AMS PEM-Prozess

Der PEM-Prozess besteht aus den folgenden Phasen:

- PEM-Initiierung: Sie arbeiten mit Ihrem CSDM zusammen, um Ihr Ziel für die geplante Veranstaltung zu definieren und zu ermitteln, was von AMS Operations benötigt wird. AMS CAs überprüft die technischen Aspekte des PEM-Plans. Die CAs Zusammenarbeit mit AMS Security and Operations befasst sich mit der Einhaltung von Vorschriften, der Optimierung und Automatisierung der Ausführung sowie der Definition von Aufgaben und Ergebnissen für die Ausführung vor dem PEM. Anschließend erstellt Ihr CSDM das PEM-Ticket und stellt AMS die Projektinformationen und technischen Details zur Verfügung. AMS benötigt eine Vorlaufzeit von 14 Kalendertagen, damit das AMS Operations Team Zeit für die Planung, technische Überprüfung und Zuweisung von Ressourcen hat.
- PEM-Überprüfung: Das AMS Operations Team prüft die PEM-Anfrage und überprüft gemeinsam mit Ihrem CSDM, ob die Informationen im PEM-Plan korrekt und vollständig sind.
- PEM-Akzeptanz: AMS überprüft die bereitgestellten Informationen und teilt dem CSDM mit, in welchem Umfang der Support während der PEM-Aktivität angeboten wird. Wenn das PEM vollständige Informationen enthält und Ihr CSDM dem Umfang der Arbeit zustimmt, ist das PEM genehmigt.
- Vorbereitung und Ausführung: AMS stellt sicher, dass die vor Beginn des PEM erforderlichen Aufgaben erledigt werden, und erleichtert die interne Kommunikation und die Kundenkommunikation. AMS stellt sicher, dass der PEM-Plan ordnungsgemäß ausgeführt wird, und erstellt Status- und Fortschrittsberichte.

PEM FAQs

Wie kontaktiere ich AMS während einer PEM-Veranstaltung mit einer RFC/Service Anfrage (SR)?

- Verwenden Sie die von Ihrem CSDM geteilte PEM-ID in der RFC/SR Betreffzeile des Formats.
PEM-ID
- Sie können auch eine Serviceanfrage (SR) erstellen, um Ihre Anwendungsfälle zu besprechen oder Fragen zu Ihrer geplanten Veranstaltung zu stellen. Wenn Sie eine SR verwenden, muss die PEM nicht gültig sein.

Welche Validierungen werden durchgeführt, wenn ein PEM-bezogener RFC eingereicht wird?

- Überprüfung, ob die Konto-ID auf dem PEM aufgeführt ist.
- Überprüfung, ob der PEM-Status zwischen den angegebenen Start- und Enddaten genehmigt und aktiv ist.

Gibt es SLAs oder SLOs für PEM-Anfragen?

- PEMs sind nicht mit SLAs oder SLOs verknüpft.
- SLAs und SLOs für PEM-bezogene Arbeitselemente (RFC/Service Request) werden von AMS definiert. SLOs

Weitere Informationen finden Sie unter [AMS Service Level Objectives \(SLOs\)](#).

Können wir ein PEM über eine Serviceanfrage (SR) erstellen?

- Nein, die PEM-Erstellung muss vom Cloud Service Delivery Manager (CSDM) verwaltet werden.

Netzwerkarchitektur

AWS Managed Services (AMS) bietet zwei Netzwerkarchitekturen:

- Multi-Account landing zone (MALZ): bietet gemeinsame Dienste — wie Zugriff, Endpunktsicherheit, Netzwerke — von gemeinsam genutzten Konten aus für Workloads, die in separaten Mitgliedskonten bereitgestellt werden.
- Single Account landing zone (SALZ): bietet eigenständige Konten, bei denen allgemeine Dienste wie Zugriff, Endpunktsicherheit und Netzwerke im selben Konto wie der Workload bereitgestellt werden. Es wird für Workloads empfohlen, die ein hohes Maß an Isolation erfordern, da dadurch höhere AWS-Kosten anfallen.

MALZ Netzwerkarchitektur

Über die Landezone-Netzwerkarchitektur mit mehreren Konten

Bevor Sie mit dem Onboarding-Prozess in der AWS Managed Services (AMS) Multi-Account landing zone (MALZ) beginnen, ist es wichtig, die Basisarchitektur oder landing zone, die AMS in Ihrem Namen erstellt, sowie deren Komponenten und Funktionen zu verstehen.

Bei der AMS Multi-Account-Landing Zone handelt es sich um eine Multi-Account-Architektur, die mit der Infrastruktur vorkonfiguriert ist, um Authentifizierung, Sicherheit, Vernetzung und Protokollierung zu erleichtern.

Note

Kostenschätzungen finden Sie unter [Grundkomponenten der AMS-Landezonenumgebung mit mehreren Konten](#).

Themen

- [Service-Region](#)
- [Organisationseinheiten](#)
- [Richtlinien zur Servicesteuerung und AWS-Organisation](#)

Das folgende Diagramm zeigt auf grober Ebene die Kontostruktur und die Aufteilung der Infrastruktur in die einzelnen Konten:

Service-Region

Alle Ressourcen innerhalb einer AMS-Landezone mit mehreren Konten werden aufgrund der aktuellen regionsübergreifenden Beschränkungen mit Active Directory und Transit Gateway in einer einzigen AWS-Region Ihrer Wahl bereitgestellt.

Organisationseinheiten

Eine typische AMS-Landezone mit mehreren Konten besteht aus vier Organisationseinheiten der obersten Ebene (OUs):

- Die zentrale Organisationseinheit (OU) (wird verwendet, um Konten zu gruppieren und als eine einzige Einheit zu verwalten)
- Die Organisationseinheit der Anwendungen
- Die vom Kunden verwaltete Organisationseinheit
- Sie beschleunigen die OU

Mit der von AMS verwalteten landing zone für mehrere Konten können Sie auch benutzerdefinierte AWS-Konten OUs für die Gruppierung und Organisation erstellen und ihnen benutzerdefinierte SCPs Konten zuordnen. Beispiele hierfür finden Sie unter [Verwaltungskonto | Benutzerdefiniertes Konto erstellen OUs und Verwaltungskonto erstellen | Benutzerdefiniertes SCP erstellen \(Überprüfung erforderlich\)](#). AMS bietet vier bestehende Konten, in denen OUs neue Konten angefordert werden können: Accelerate, Applications > Managed, Applications > Development OUs und Customer-managed.

- Beschleunigen Sie OU:

Dies ist eine Organisationseinheit der obersten Ebene in der AMS Multi-Account-Landing landing zone (MALZ). Konten unter dieser Organisationseinheit werden von AMS mit einem RFC (Bereitstellung | Verwaltete landing zone | Verwaltungskonto | Accelerate-Konto erstellen, Typ-ID ändern: ct-2p93tyd5angmi) bereitgestellt. In diesen Accelerate-Anwendungskonten können Sie von beschleunigten Betriebsdiensten wie Überwachung und Warnmeldungen, Vorfallmanagement, Sicherheitsmanagement und Backup-Management profitieren. Weitere Informationen finden Sie unter [AMS Accelerate-Konten](#).

- Anwendungen > verwaltete Organisationseinheit:

In dieser untergeordneten Organisationseinheit der Anwendungs-OU werden die Konten vollständig von AMS verwaltet, einschließlich aller betrieblichen Aufgaben. Zu den operativen Aufgaben gehören die Verwaltung von Serviceanfragen, das Vorfallmanagement, das Sicherheitsmanagement, das Kontinuitätsmanagement, das Patch-Management, die Kostenoptimierung, die Überwachung und das Eventmanagement. Diese Aufgaben werden für das Management Ihrer Infrastruktur ausgeführt. Bei Bedarf OUs können mehrere untergeordnete Objekte erstellt werden, bis die maximale Anzahl an verschachtelten Elementen für AWS-Organisationen erreicht OUs ist. Einzelheiten finden Sie unter [Kontingente für AWS Organizations](#).

- Anwendungen > OU für Entwicklung:

Unter dieser Unter-OU der Anwendungs-OU in der von AMS verwalteten landing zone handelt es sich bei Konten um Konten [im Entwicklernodus](#), die Ihnen erweiterte Berechtigungen zur Bereitstellung und Aktualisierung von AWS-Ressourcen außerhalb des AMS-Change-Management-Prozesses gewähren. Diese Organisationseinheit unterstützt bei Bedarf auch die Erstellung neuer untergeordneter Organisationseinheiten.

- vom Kunden verwaltete Organisationseinheit:

Dies ist eine Organisationseinheit der obersten Ebene in der AMS-Landezone für mehrere Konten. Konten unter dieser Organisationseinheit werden von AMS mit einem RFC bereitgestellt. Bei diesen Konten sind Sie für den Betrieb von Workloads und AWS-Ressourcen verantwortlich. Diese Organisationseinheit unterstützt bei Bedarf auch die Einrichtung neuer untergeordneter Organisationseinheiten.

Als bewährte Methode empfehlen wir, Konten anhand ihrer Funktionen OUs und Richtlinien unter diesen und individuell angeforderten Unterkonten zu gruppieren. OUs

Richtlinien zur Servicesteuerung und AWS-Organisation

AWS stellt Service-Kontrollrichtlinien (SCPs) für die Berechtigungsverwaltung in einer AWS-Organisation bereit. SCPs werden verwendet, um zusätzliche Richtlinien dafür zu definieren, welche Aktionen Benutzer in welchen Fällen ausführen können. OUs Standardmäßig stellt AMS eine Reihe von in der Verwaltung SCPs bereitgestellten Konten bereit, die Schutz auf verschiedenen Standard-OU-Ebenen bieten. Für SCP-Einschränkungen wenden Sie sich bitte an Ihren CSDM.

Sie können auch benutzerdefinierte erstellen SCPs und diese an bestimmte anhängen. OUs Sie können von Ihrem Verwaltungskonto aus mit dem Änderungstyp ct-33ste5yc7hprs angefordert

werden. AMS überprüft dann die angeforderten benutzerdefinierten Daten, bevor sie auf das Ziel angewendet werden. SCPs OUs Beispiele finden Sie unter [Verwaltungskonto | Benutzerdefiniertes Konto OUs und Verwaltungskonto erstellen | Benutzerdefiniertes SCP erstellen \(Überprüfung erforderlich\)](#).

Wählen Sie ein MALZ oder mehrere MALZs

Die folgende Tabelle enthält einige allgemeine Überlegungen zur Entscheidung zwischen einer einzelnen landing zone mit mehreren Konten (MALZ) und mehreren Landezonen mit mehreren Konten (z. B. zwei Landezonen mit mehreren Konten — Prod und Non-Prod). Im Allgemeinen hängt die Wahl von den individuellen Bedürfnissen, gesetzlichen Anforderungen und Betriebspraktiken ab.

Einzelne landing zone mit mehreren Konten im Vergleich zu mehreren Landezonen mit mehreren Konten

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Grundkosten	Niedriger, optimierter Preis von etwa 3.000 USD pro Monat.	Höher, zusätzliche Kosten von etwa 3.000 USD pro Umgebung.
Fakturierung	Einzelrechnung aufgrund eines einzigen Abrechnungs-/Verwaltungskontos.	Separate Rechnung für jede landing zone mit mehreren Konten. Derzeit unterstützt AWS Org keine Multi-Management-Konten mit einer einzigen Rechnung.
Portabilität vorhanden er Reserved Instances () RIs	Niedrig. AWS ist RIs derzeit nicht für mehrere Rechnungskonten konvertierbar. Sie würden eine bestehende landing zone RIs für mehrere Konten wiederverwenden.	Niedriger. Sie würden es wiederverwenden und RIs in allen landing zone mit mehreren Konten verteilen.
Rabatte bei der Staffe lung von Produkten	Hoch. Siehe Mengenrabatte .	Niedrig. Siehe Mengenrabatte .

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Gemeinkosten bei der Ersteinrichtung (im project/migration Zeitplan)	Niedrig. Active Directory-, Netzwerk- und Single Sign-On-Integrationen (SSO) nur einmal.	Hoch. Sie würden Active Directory -, Netzwerkintegration- und SSO-Integrationen für jede landing zone durchführen. Dies könnte zu potenziellen Verzögerungen bei Migration sprojekten führen.
Konfigurierbarkeit gängiger Dienste	Geringer Aufwand. Sie konfigurieren common/shared Dienste wie DNS, Backup, Überwachung, Protokollierung usw.	Hoher Aufwand. Zusätzliche Planung ist erforderlich, um zu klären, wo die gemeinsame Infrastruktur oder die gemeinsamen Dienste installiert werden sollen. Verkehr, der über mehrere Transit-Gateways (TGWs) in jeder landing zone fließt, könnte zu zusätzlichen Kosten führen.
Skalierbarkeit	Mittel. AMS hat derzeit ein praktisches Limit von 150 Konten pro landing zone mit mehreren Konten. Mehrere Teams oder Anbieter, die Anwendungen in demselben Konto ausführen, könnten Zugriff auf Stacks haben, die unterschiedlichen Teams gehören. Diese Einschränkung kann verringert werden, indem der Zugriff auf anwendungsspezifische Stacks auf der ServiceNow Ebene gesteuert wird (durch Integration der AMS ServiceNow Connector -Anwendung und Verwendung von Tags). Fragen Sie die technischen Delivery Manager (TDMs) oder Cloud-Architekten (CAs) von AMS, wie Sie das umsetzen können.	Hoch. Möglichkeit, mehrere landing zone mit mehreren Konten zu nutzen, um die Konten zu verteilen und gleichzeitig eine Trennung auf Konto- oder Anwendungsebene zu erreichen . Die Verwaltung einer großen Anzahl von Konten könnte zu Betriebs- oder Kostengemeinkosten führen.

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Operationelles Risiko	(Hängt davon ab) Niedrig. Operative Integration und Einsatzbereitschaft nur einmal. Geringere Wahrscheinlichkeit von Prozessabweichungen.	(Hängt davon ab) Niedrig. Vielfältige Integrations- und Betriebsaktivitäten. Verschiebungen in mehreren Landezonen während des Berichtszeitraums könnten zu operationellen Risiken führen.
Mehrere AWS-Regionen	Eine einzige AWS-Region. Die AMS-Landezone für mehrere Konten ist auf eine einzige AWS-Region beschränkt. Um mehrere AWS-Regionen abzudecken, verwenden Sie mehrere landing zone mit mehreren Konten.	Mehrere AWS-Regionen. Bei mehreren Landing Zones mit mehreren Konten können Sie jedes MALZ in einer Region einsetzen und sie über Transit Gateway (TGW) -Peering miteinander verbinden.
Kontomigration oder Portabilität	Ja. Das Verschieben von Konten von einer Organisationseinheit zu einer anderen innerhalb derselben AWS-Organisation ist möglich.	Nein. AMS unterstützt keine Migration eines Kontos zwischen Landing Zones, also zwischen AWS Organisationen. Workloads können mit Transit Gateway (TGW) oder VPC-Peering über Landingzonen verteilt werden.
Änderungsmanagement	Mittel. Destruktive Änderungen an gängigen Komponenten wie TGW, Active Directory (AD) oder Outbound (Egress) können sich auf alle Workloads in einer landing zone mit mehreren Konten auswirken. Änderungen an AMS-verwalteten Komponenten werden jedoch intern getestet und in fortlaufenden Updates veröffentlicht.	Niedrig. Destruktive Änderungen an gängigen Komponenten wie TGW, AD oder Outbound (Egress) können sich nur auf die Workloads in dieser speziellen landing zone mit mehreren Konten auswirken.

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Daten- und Zugriffskontrollen	(Hängt davon ab) Geringe Kontrolle, wenn Sie für Prod- und Nicht-Prod-Workloads eine Verbindung zu verschiedenen lokalen ADs und Netzwerken herstellen möchten. SAML-Verbund, TGW-Domänen und Sicherheitsgruppen (SGs) können ebenfalls bei der Implementierung der erforderlichen Kontrollen helfen.	(Hängt davon ab) Hohe Kontrolle, wenn Sie für Prod-Workloads und Non-Prod-Workloads eine Verbindung zu verschiedenen lokalen ADs und Netzwerken herstellen möchten. Verwenden Sie separate Landezonen, um strenge Compliance-Anforderungen zu erfüllen.
Einhaltung von Vorschriften und Sicherheit	(Hängt davon ab) Niedrig, wenn strenge Compliance-Anforderungen zur vollständigen Trennung materieller und immaterieller Arbeitslasten bestehen. Präventive und detektive Kontrollen nach AMS-Standard sind vorhanden.	(Hängt davon ab) Eine landing zone mit mehreren Konten könnte dazu beitragen, strenge Compliance-Anforderungen zu erfüllen, indem materielle und immaterielle Arbeitslasten vollständig getrennt werden. Präventive und detektive Kontrollen nach AMS-Standard sind vorhanden.

Empfehlung: Ohne strikte Einhaltung oder regionsübergreifende Anforderungen würde ein Start mit einer einzigen AMS-Landezone für mehrere Konten ein ausgewogenes Verhältnis zwischen Kosten, Sicherheit, betrieblicher Exzellenz und Komplexität der Migration bieten. Sie können jederzeit eine zusätzliche landing zone einrichten, falls Konto- oder Geschäftsbeschränkungen auftreten.

Einzelne landing zone mit mehreren Konten im Vergleich zu landing zone mit mehreren Konten FAQs

Einige häufig gestellte Fragen bei der Einrichtung einer einzelnen landing zone mit mehreren Konten oder mehrerer Landezonen mit mehreren Konten:

Frage 1: Kann ich mit einer einzigen Landingzone für mehrere Konten beginnen und dann zu einer landing zone mit mehreren Konten wechseln, wenn Kontolimits oder geschäftliche Einschränkungen auftreten?

A: Ja. Sie können jederzeit eine weitere landing zone für mehrere Konten einrichten:

- Es muss ein neues Konto für Rechnungszahler eingerichtet werden (derzeit unterstützt AWS keine Konten mit mehreren Zahlern in einer einzigen AWS-Organisation).
- Der Aufbau der Basisbasis für mehrere Konten dauert bis zu 2 Wochen, sobald der Fragebogen zur landing zone für mehrere Konten ausgefüllt ist.
- Jede landing zone mit mehreren Konten bedeutet zusätzliche Betriebskosten von ~3.000 USD/Monat.
- Für die Einrichtung eines neuen MALZ ist eine Integration von N/W, AD, DNS und SSO erforderlich.
- Alle Reserved Instances (RIs) und Kostensparpläne müssen für die neue landing zone mit mehreren Konten eingerichtet werden (RIs sind nicht übertragbar).
- Die AMS-Landingzone mit mehreren Konten unterstützt keine Migration eines Kontos zwischen Landingzone-Konten mit mehreren Konten, z. B. zwischen AWS-Organisationen. Das Verschieben von Anwendungen von einem Konto auf ein anderes ist jedoch mithilfe von Standardmigrationsmethoden möglich.

Frage 2: Welchen Ansatz verfolgt AMS gegenüber MALZ in Bezug updates/changes auf underlying/shared Infrastruktur und Quantifizierung des Risikos für Kunden? Geben Sie detailliert an, welche Zusicherungen im Prozess enthalten sind. Wie können sich Kunden darauf verlassen, dass MALZ keine Auswirkungen auf updates/changes die Kunden hat? Gibt es Maßnahmen, die der Kunde ergreifen muss, um Störungen zu verhindern?

A: AMS folgt einer strikten Änderungsverfahren und verwendet interne Tools, die es uns ermöglichen, Änderungen an den Kundenumgebungen zu definieren, zu überprüfen, zu planen und durchzuführen.

Der Prozess zur Veröffentlichung von Updates setzt Code-Reviews, Integrationstests, die Bereitstellung in Gamma- und Beta-Umgebungen sowie zusätzliche Backzeit und Tests in Beta- und Gamma-Umgebungen vor der Veröffentlichung in Kundenumgebungen durch. Alle Versionen beinhalten Rollback-Verfahren und werden vom Release-Team und dem Team, das die Änderung erstellt und angefordert hat, genau überwacht. Der Umfang der Releases beschränkt sich auf Stacks, die AMS gehören und von AMS bereitgestellt werden. Im Durchschnitt führen wir mindestens eine Veröffentlichung pro Woche durch.

Darüber hinaus gilt:

- AMS SLA sind anwendbar. Gemäß der AMS-Servicebeschreibung unterliegt jeder Vorfall, der nach einer gemeinsamen Wartung der Infrastruktur auftritt, der entsprechenden Vereinbarung zur Lösung oder Gutschrift.

- Kunden benötigen keine besonderen Präventivmaßnahmen, um Störungen der gemeinsamen Infrastruktur zu verhindern. Kunden haben nur Leseberechtigungen für AWS Org- oder Core OU-Konten, sodass Kunden keine zerstörerischen Änderungen an der MALZ-Kernumgebung vornehmen können. Alle Kundenanfragen an die Core-Infrastruktur müssen von AMS geprüft und genehmigt werden.
- Kunden können bestimmte Änderungen auf Organisationsebene testen, z. B. SCPs/Roles auf Ebene einzelner Konten, die keine Produkte sind, bevor sie Änderungen auf Ebene der App-Organisationseinheit weitergeben. Es steht auf der AMS-Roadmap, mehrere Apps zuzulassen OUs (Q2 2020), wodurch das Risiko einiger Änderungen auf ORGANISATIONSEBENE weiter verringert würde. Das MALZ-Team hat bereits eine separate Organisationseinheit für Konten im „Build-Modus“ veröffentlicht, um eine klare Trennung der Kundenrechte und separate Kontrollen zu gewährleisten.
- Bei den meisten dieser Änderungen handelt es sich um Änderungen, die es AMS ermöglichen, die Arbeitslast effektiv und effizient zu verwalten, ohne dass sie sich unbedingt auf die Arbeitslast der Kunden auswirken. Wenn AMS der Ansicht ist, dass eine Änderung der gemeinsamen Infrastruktur Auswirkungen auf die Arbeitslast der Kunden haben kann, werden sie dann auf das Änderungsfenster der Kunden abgestimmt.

Allgemeine Empfehlung: Beginnen Sie mit mehreren Landezonen für mehrere Konten, wenn:

- Wenn es Ihnen hilft, eine bestimmte Konformität zu erreichen.
- Wenn Sie Multi-Region verwenden müssen.
- Wenn Sie unterschiedliche lokale Workloads ADs und Netzwerke für Workloads und für externe Prod/Material Workloads haben. Prod/Non-Material workloads, to clearly segregate b/w

Landing Zone-Konten mit mehreren Konten

Themen

- [Verwaltungskonto](#)
- [Netzwerkkonto](#)
- [Shared Services-Konto](#)
- [Konto protokollieren und archivieren](#)
- [Sicherheitskonto](#)
- [Arten von Anwendungskonten](#)

- [AMS Tools-Konto \(Workloads migrieren\)](#)

Verwaltungskonto

Das Verwaltungskonto ist Ihr erstes AWS-Konto, wenn Sie mit dem Onboarding bei AMS beginnen. Es verwendet AWS Organizations als Verwaltungskonto (auch bekannt als das Zahlungskonto, das die Gebühren aller Mitgliedskonten bezahlt), wodurch das Konto Mitgliedskonten erstellen und finanziell verwalten kann. Es enthält das AWS-Landing landing zone (ALZ) -Framework, Kontokonfigurationsstapelsätze, AWS Organization Service Control Policies (SCPs) usw.

Weitere Informationen zur Verwendung eines Verwaltungskontos finden Sie unter [Bewährte Methoden für das Verwaltungskonto](#).

Das folgende Diagramm bietet einen allgemeinen Überblick über die im Verwaltungskonto enthaltenen Ressourcen.

Ressourcen im Verwaltungskonto

Abgesehen von den oben genannten Standardservices werden beim Onboarding keine zusätzlichen AWS-Ressourcen im Verwaltungskonto erstellt. Die folgenden Eingaben sind beim Onboarding bei AMS erforderlich:

- Verwaltungskonto-ID: AWS-Konto-ID, die ursprünglich von Ihnen erstellt wurde.
- E-Mails für Kernkonten: Geben Sie die E-Mails an, die den einzelnen Kernkonten zugeordnet werden sollen: Networking, Shared Services, Logging und Sicherheitskonto.
- Serviceregion: Geben Sie die AWS-Region an, in der alle Ressourcen Ihrer AMS-Landezone bereitgestellt werden.

Netzwerkkonto

Das Netzwerkkonto dient als zentraler Knotenpunkt für das Netzwerk-Routing zwischen AMS-Landingzone-Konten mit mehreren Konten, Ihrem lokalen Netzwerk und ausgehendem Datenverkehr ins Internet. Darüber hinaus enthält dieses Konto öffentliche DMZ-Bastionen, über die AMS-Techniker auf Hosts in der AMS-Umgebung zugreifen können. Einzelheiten finden Sie im folgenden allgemeinen Diagramm des Netzwerkkontos.

Architektur von Netzwerkkonten

Das folgende Diagramm zeigt die AMS-Landingzone-Umgebung mit mehreren Konten und zeigt den Netzwerkdatenverkehr zwischen den Konten. Es ist ein Beispiel für eine Konfiguration mit hoher Verfügbarkeit.

AMS konfiguriert alle Netzwerkaspekte für Sie auf der Grundlage unserer Standardvorlagen und der von Ihnen beim Onboarding ausgewählten Optionen. Ein standardmäßiges AWS-Netzwerkdesign wird auf Ihr AWS-Konto angewendet, und eine VPC wird für Sie erstellt und entweder über VPN oder Direct Connect mit AMS verbunden. Weitere Informationen zu Direct Connect finden Sie unter [AWS Direct Connect](#). Zum Standard VPCs gehören die DMZ, Shared Services und ein Anwendungssubnetz. Während des Onboarding-Prozesses VPCs können zusätzliche Informationen angefordert und erstellt werden, die Ihren Anforderungen entsprechen (z. B. Kundenabteilungen, Partner). Nach dem Onboarding erhalten Sie ein Netzwerkdiagramm: ein Umgebungsdokument, das erklärt, wie Ihr Netzwerk eingerichtet wurde.

Note

Informationen zu Standard-Servicelimits und Einschränkungen für alle aktiven Services finden Sie in der Dokumentation zu [AWS-Servicelimits](#).

Unser Netzwerkdesign basiert auf dem „[Prinzip der geringsten Rechte](#)“ von Amazon. Um dies zu erreichen, leiten wir den gesamten eingehenden und ausgehenden Verkehr durch eine DMZ, mit Ausnahme des Datenverkehrs, der aus einem vertrauenswürdigen Netzwerk stammt. Das einzige vertrauenswürdige Netzwerk ist das, das zwischen Ihrer lokalen Umgebung und der VPC mithilfe and/or eines VPN und AWS Direct Connect (DX) konfiguriert wurde. Der Zugriff wird durch die Verwendung von Bastion-Instances gewährt, wodurch ein direkter Zugriff auf Produktionsressourcen verhindert wird. Alle Ihre Anwendungen und Ressourcen befinden sich in privaten Subnetzen, die über öffentliche Load Balancer erreichbar sind. Öffentlicher Ausgangsverkehr fließt über die NAT-Gateways in der Ausgangs-VPC (im Netzwerkkonto) zum Internet Gateway und dann zum Internet. Alternativ kann der Datenverkehr über Ihr VPN oder Direct Connect in Ihre lokale Umgebung fließen.

Private Netzwerkkonnektivität zur AMS-Landezonenumgebung mit mehreren Konten

AWS bietet private Konnektivität entweder über VPN-Konnektivität (Virtual Private Network) oder über Standleitungen mit AWS Direct Connect. Die private Konnektivität in Ihrer Umgebung mit mehreren Konten wird mit einer der im Folgenden beschriebenen Methoden eingerichtet:

- Zentralisierte Edge-Konnektivität mit Transit Gateway
- Direct Connect (DX) and/or VPN mit virtuellen privaten Clouds verbinden (VPCs)

Zentralisierte Edge-Konnektivität mit Transit Gateway

AWS Transit Gateway ist ein Service, mit dem Sie Ihre VPCs und Ihre lokalen Netzwerke mit einem einzigen Gateway verbinden können. Transit Gateway (TGW) kann verwendet werden, um Ihre bestehende Edge-Konnektivität zu konsolidieren und sie über einen einzigen ingress/egress Punkt weiterzuleiten. Das Transit-Gateway wird im Netzwerkkonto Ihrer AMS-Umgebung mit mehreren Konten erstellt. Weitere Informationen zu Transit Gateway finden Sie unter [AWS Transit Gateway](#).

Das AWS Direct Connect (DX) -Gateway wird verwendet, um Ihre DX-Verbindung über eine virtuelle Transitschnittstelle mit dem VPCs oder VPNs , die an Ihr Transit-Gateway angeschlossen sind, zu verbinden. Sie ordnen ein Direct-Connect-Gateway dem Transit Gateway zu. Erstellen Sie anschließend eine virtuelle Transitschnittstelle für Ihre AWS Direct Connect Connect-Verbindung zum Direct Connect-Gateway. Informationen zu virtuellen DX-Schnittstellen finden Sie unter [Virtuelle Schnittstellen von AWS Direct Connect](#).

Diese Konfiguration bietet die folgenden Vorteile. Sie haben folgende Möglichkeiten:

- Verwalten Sie eine einzelne Verbindung für mehrere VPCs oder VPNs , die sich in derselben AWS-Region befinden.
- Werben Sie für Präfixe von On-Premise zu AWS und von AWS zu On-Premise.

Note

[Informationen zur Verwendung eines DX mit AWS-Services finden Sie im Abschnitt Classic im Resiliency Toolkit.](#) Weitere Informationen finden Sie unter [Transit Gateway Gateway-Verknüpfungen](#).

Um die Stabilität Ihrer Konnektivität zu erhöhen, empfehlen wir, dass Sie mindestens zwei virtuelle Transitschnittstellen von verschiedenen AWS Direct Connect Connect-Standorten an das Direct Connect-Gateway anschließen. Weitere Informationen finden Sie in der [AWS Direct Connect Connect-Resilienzempfehlung](#).

DX oder VPN mit dem Konto verbinden VPCs

Mit dieser Option werden die landing zone Zone-Umgebungen VPCs in Ihrem AMS mit mehreren Konten direkt mit Direct Connect oder VPN verbunden. Der Datenverkehr fließt direkt von Direct Connect oder VPN, ohne das Transit-Gateway zu passieren. VPCs

Ressourcen im Netzwerkkonto

Wie im Netzwerkkontodiagramm dargestellt, werden die folgenden Komponenten im Konto erstellt und erfordern Ihre Eingabe.

Das Netzwerkkonto enthält zwei VPCs: Egress VPC und DMZ VPC, auch bekannt als Perimeter-VPC.

AWS-Netzwerkmanager

AWS Network Manager ist ein Service, mit dem Sie Ihre Transit-Gateway-Netzwerke (TGW) ohne zusätzliche Kosten für AMS visualisieren können. Es bietet eine zentrale Netzwerküberwachung sowohl für AWS-Ressourcen als auch für lokale Netzwerke, eine zentrale globale Ansicht ihres privaten Netzwerks in einem Topologiediagramm und auf einer geografischen Karte sowie Nutzungsmetriken wie den in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down Byte-Verbindungsstatus. Weitere Informationen finden Sie unter [AWS Network Manager](#).

Verwenden Sie eine der folgenden Rollen, um auf diese Ressource zuzugreifen:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

Ausgangs-VPC

Die Egress-VPC wird hauptsächlich für den ausgehenden Datenverkehr ins Internet verwendet und besteht aus public/private Subnetzen in bis zu drei Verfügbarkeitszonen (). AZs Network

Address Translation (NAT) -Gateways werden in den öffentlichen Subnetzen bereitgestellt, und Transit Gateway (TGW) VPC-Anlagen werden in den privaten Subnetzen erstellt. Ausgehender oder ausgehender Internetverkehr aus allen Netzwerken wird über TGW durch das private Subnetz geleitet, wo er dann über VPC-Routing-Tabellen an ein NAT weitergeleitet wird.

Für Sie VPCs , die öffentlich zugängliche Anwendungen in einem öffentlichen Subnetz enthalten, ist der aus dem Internet stammende Datenverkehr in dieser VPC enthalten. Rückverkehr wird nicht an die TGW- oder Egress-VPC weitergeleitet, sondern über das Internet-Gateway (IGW) in der VPC zurückgeleitet.

Note

Netzwerk-VPC-CIDR-Bereich: Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 Adressbereich für die VPC in Form eines CIDR-Blocks (Classless Inter-Domain Routing) angeben, z. B. 10.0.16.0/24. Dies ist der primäre CIDR-Block für Ihre VPC.

Das AMS Multi-Account-Landingzone-Team empfiehlt den Bereich 24 (mit mehr IP-Adressen), um einen gewissen Puffer für den Fall bereitzustellen, dass in future andere Ressourcen/Appliances eingesetzt werden.

Verwaltete Palo Alto-Ausgangsfirewall

AMS bietet eine Managed Palo Alto Egress Firewall-Lösung, die das Filtern von ausgehendem Internetverkehr für alle Netzwerke in der Multi-Account Landing Zone-Umgebung (mit Ausnahme von öffentlich zugänglichen Diensten) ermöglicht. Diese Lösung kombiniert die branchenführende Firewall-Technologie (Palo Alto VM-300) mit den Infrastrukturmanagementfunktionen von AMS zur Bereitstellung, Überwachung, Verwaltung, Skalierung und Wiederherstellung der Infrastruktur in konformen Betriebsumgebungen. Dritte, einschließlich Palo Alto Networks, haben keinen Zugriff auf die Firewalls. Sie werden ausschließlich von AMS-Technikern verwaltet.

Steuerung des Verkehrs

Die verwaltete Firewall-Lösung für ausgehenden Datenverkehr verwaltet eine Domain-Zulassungsliste, die aus AMS-erforderlichen Domänen für Dienste wie Backup und Patch sowie aus Ihren definierten Domänen besteht. Wenn ausgehender Internetverkehr an die Firewall weitergeleitet wird, wird eine Sitzung geöffnet, der Datenverkehr wird ausgewertet, und wenn er einer zulässigen Domain entspricht, wird der Datenverkehr an das Ziel weitergeleitet.

Architektur

Die verwaltete Firewall-Lösung für ausgehenden Datenverkehr folgt einem Hochverfügbarkeitsmodell, bei dem je nach Anzahl der Verfügbarkeitszonen () zwei bis drei Firewalls eingesetzt werden. AZs Die Lösung nutzt einen Teil des IP-Bereichs der Standard-Ausgangs-VPC, stellt aber auch eine VPC-Erweiterung (/24) für zusätzliche Ressourcen bereit, die für die Verwaltung der Firewalls erforderlich sind.

Netzwerkfluss

Auf hoher Ebene bleibt das Routing des öffentlichen ausgehenden Datenverkehrs unverändert, mit Ausnahme der Art und Weise, wie der Datenverkehr von der ausgehenden VPC ins Internet geleitet wird:

1. Ausgangsverkehr, der für das Internet bestimmt ist, wird über die VPC-Routentabelle an das Transit Gateway (TGW) gesendet
2. TGW leitet den Verkehr über die TGW-Routentabelle an die Ausgangs-VPC weiter
3. VPC leitet den Verkehr über die Routentabellen des privaten Subnetzes ins Internet weiter.
 - a. In der standardmäßigen Multi-Account-Landingzone-Umgebung wird der Internetverkehr direkt an ein NAT-Gateway (Network Address Translation) gesendet. Die verwaltete Firewall-Lösung konfiguriert die Routing-Tabellen für private Subnetze neu, sodass die Standardroute (0.0.0.0/0) stattdessen auf eine Firewall-Schnittstelle verweist.

Die Firewalls selbst enthalten drei Schnittstellen:

1. Vertrauenswürdige Schnittstelle: Private Schnittstelle für den Empfang von Datenverkehr, der verarbeitet werden soll.
2. Nicht vertrauenswürdige Schnittstelle: Öffentliche Schnittstelle zum Senden von Datenverkehr ins Internet. Da die Firewalls NAT ausführen, akzeptieren externe Server Anfragen von diesen öffentlichen IP-Adressen.
3. Verwaltungsschnittstelle: Private Schnittstelle für Firewall-API, Updates, Konsole usw.

Während des gesamten Routings wird der Verkehr innerhalb derselben Availability Zone (AZ) aufrechterhalten, um den AZ-übergreifenden Verkehr zu reduzieren. Der Verkehr wird nur dann überquert AZs, wenn ein Failover auftritt.

Änderung der Zulassungsliste

Nach dem Onboarding `ams-allowlist` wird eine standardmäßige Zulassungsliste mit dem Namen erstellt, die für AMS erforderliche öffentliche Endpunkte sowie öffentliche Endpunkte für das Patchen von Windows- und Linux-Hosts enthält. Sobald der Betrieb abgeschlossen ist, können Sie in der AMS-Konsole unter der Kategorie Management | Managed Firewall | Outbound (Palo Alto) RFCs erstellen, um Zulassungslisten zu erstellen oder zu löschen oder die Domänen zu ändern. Beachten Sie, dass dies nicht geändert werden kann. `ams-allowlist` Die RFCs werden vollständig automatisiert behandelt (sie sind nicht manuell).

Benutzerdefinierte Sicherheitsrichtlinie

Sicherheitsrichtlinien bestimmen anhand von Datenverkehrsattributen wie der Quell- und Zielsicherheitszone, der Quell- und Ziel-IP-Adresse und dem Dienst, ob eine Sitzung blockiert oder zugelassen wird. Benutzerdefinierte Sicherheitsrichtlinien werden vollständig automatisiert unterstützt RFCs. CTs Informationen zum Erstellen oder Löschen von Sicherheitsrichtlinien finden Sie in der Kategorie Management | Managed Firewall | Outbound (Palo Alto). Das CT zum Bearbeiten einer vorhandenen Sicherheitsrichtlinie finden Sie unter der Kategorie Bereitstellung | Managed Firewall | Outbound (Palo Alto). Sie können neue Sicherheitsrichtlinien erstellen, Sicherheitsrichtlinien ändern oder Sicherheitsrichtlinien löschen.

Note

Die Standardsicherheitsrichtlinie `ams-allowlist` kann nicht geändert werden

CloudWatch PA-Dashboards für ausgehenden Datenverkehr

Zwei Dashboards bieten eine aggregierte Ansicht von Palo Alto (PA). Das AMS-MF-PA-Egress-Config-Dashboard bietet eine Übersicht über die PA-Konfiguration, Links zu Zulassungslisten und eine Liste aller Sicherheitsrichtlinien einschließlich ihrer Attribute. CloudWatch Das AMS-MF-PA-Egress-Dashboard kann so angepasst werden, dass Verkehrsprotokolle gefiltert werden. Um beispielsweise ein Dashboard für eine Sicherheitsrichtlinie zu erstellen, können Sie einen RFC mit einem Filter wie dem folgenden erstellen:

```
fields @timestamp, @message
```

```
| filter @logStream like /pa-traffic-logs/  
| filter @message like /<Security Policy Name>/  
| parse @message  
"  
as x1, @x2, @x3, @x4, @type, @x6, @x7, @source_ip, @destination_ip, @source_nat_ip,  
@dest_nat_ip, @rule, @x13, @x14, @application, @x16, @from_zone, @to_zone,  
@x19, @x20, @x21, @x22, @session_id, @x24, @source_port, @destination_port,  
@source_nat_port, @destination_nat_port, @x29, @protocol, @action, @bytes,  
@bytes_sent, @bytes_received, @packets, @x36, @x37, @category, @x39, @x40, @x41,  
@source_country, @destination_country, @x44, @packets_sent, @packets_received,  
@session_end_reason, @x48, @x49, @x50  
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,  
@destination_ip, @source_port, @destination_port, @session_id, @from_zone,  
@to_zone, @category, @bytes_sent, @bytes_received, @packets_sent, @packets_received,  
@source_country, @destination_country
```

Failover-Modell

Die Firewall-Lösung umfasst zwei bis drei Palo Alto (PA) -Hosts (einer pro AZ). Healthy Check Canaries wird nach einem konstanten Zeitplan ausgeführt, um den Zustand der Hosts zu bewerten. Wenn ein Host als fehlerhaft identifiziert wird, wird AMS benachrichtigt, und der Datenverkehr für diese AZ wird durch Änderung der Routing-Tabelle automatisch auf einen fehlerfreien Host in einer anderen AZ umgeleitet. Da der Workflow zur Integritätsprüfung ständig ausgeführt wird, wird der Datenverkehr wieder auf die richtige AZ mit dem fehlerfreien Host umgeleitet, wenn der Host aufgrund vorübergehender Probleme oder manueller Behebung wieder funktionsfähig ist.

Skalierung

AMS überwacht die Firewall auf Durchsatz- und Skalierungsgrenzen. Wenn die Durchsatzgrenzen die unteren Schwellenwerte (CPU/Netzwerk) überschreiten, erhält AMS eine Warnung. Ein niedriger Schwellenwert deutet darauf hin, dass die Ressourcen fast ausgelastet sind und ein Punkt erreicht ist, an dem AMS die Messwerte im Laufe der Zeit auswertet und Skalierungslösungen vorschlägt.

Backup und Backup

Backups werden beim ersten Start, nach allen Konfigurationsänderungen und in regelmäßigen Abständen erstellt. Beim ersten Start werden Backups pro Host erstellt, aber Konfigurationsänderungen und regelmäßige Intervall-Backups werden auf allen Firewall-Hosts durchgeführt, wenn der Backup-Workflow aufgerufen wird. AMS-Techniker können zusätzliche Backups außerhalb dieser Fenster erstellen oder auf Anfrage Backup-Details bereitstellen.

AMS-Techniker können bei Bedarf die Wiederherstellung von Konfigurations-Backups durchführen. Wenn eine Wiederherstellung erforderlich ist, erfolgt sie auf allen Hosts, um die Konfiguration zwischen den Hosts synchron zu halten.

Eine Wiederherstellung kann auch erfolgen, wenn ein Host eine Instanz vollständig recyceln muss. Eine automatische Wiederherstellung des neuesten Backups erfolgt, wenn eine neue EC2 Instanz bereitgestellt wird. Im Allgemeinen werden Hosts nicht regelmäßig recycelt und sind für schwerwiegende Ausfälle oder erforderliche AMI-Swaps reserviert. Host-Wiederverwendungen werden manuell initiiert, und Sie werden benachrichtigt, bevor eine Wiederverwertung stattfindet.

Abgesehen von den Backups der Firewall-Konfiguration werden Ihre spezifischen Regeln für die Zulassungsliste separat gesichert. Eine Sicherungskopie wird automatisch erstellt, wenn Ihre definierten Regeln für die Zulassungsliste geändert werden. Die Wiederherstellung der Sicherungskopie auf der Zulassungsliste kann bei Bedarf von einem AMS-Techniker durchgeführt werden.

Aktualisierungen

Die AMS Managed Firewall Solution erfordert im Laufe der Zeit verschiedene Updates, um das System zu verbessern, zusätzliche Funktionen hinzuzufügen oder das Firewall-Betriebssystem (OS) oder die Firewall-Software zu aktualisieren.

Die meisten Änderungen wirken sich nicht auf die Betriebsumgebung aus, z. B. die Aktualisierung der Automatisierungsinfrastruktur. Andere Änderungen wie die Rotation der Firewall-Instanz oder das Betriebssystem-Update können jedoch zu Störungen führen. Wenn eine mögliche Betriebsunterbrechung aufgrund von Updates bewertet wird, stimmt sich AMS mit Ihnen ab, um die Wartungsfenster zu berücksichtigen.

Zugriff durch den Bediener

AMS-Betreiber verwenden ihre ActiveDirectory Anmeldeinformationen, um sich beim Palo Alto-Gerät anzumelden, um Operationen durchzuführen (z. B. Patchen, Reagieren auf ein Ereignis usw.). Die Lösung behält die standardmäßigen AMS-Operator-Authentifizierungs- und Konfigurationsänderungsprotokolle bei, um die auf den Palo Alto-Hosts ausgeführten Aktionen nachzuverfolgen.

Standardprotokolle

Standardmäßig befinden sich die von der Firewall generierten Protokolle für jede Firewall im lokalen Speicher. Im Laufe der Zeit werden lokale Protokolle je nach Speicherauslastung gelöscht. Die AMS-

Lösung ermöglicht den Versand von Protokollen von den Maschinen in Echtzeit an CloudWatch Protokolle. Weitere Informationen finden Sie unter [CloudWatch Integration von Protokollen](#).

Die AMS-Techniker haben weiterhin die Möglichkeit, Protokolle bei Bedarf direkt von den Maschinen abzufragen und zu exportieren. Darüber hinaus können Protokolle an ein kundeneigenes Panorama gesendet werden. Weitere Informationen finden Sie unter [Panoramaintegration](#).

Die Lösung erfasst die folgenden Protokolle:

RFC-Statuscodes

Protokolltyp	Beschreibung
Datenverkehr	Zeigt einen Eintrag für den Start und das Ende jeder Sitzung an. Jeder Eintrag enthält Datum und Uhrzeit, Quell- und Zielzonen, Adressen und Ports, den Namen der Anwendung, den Namen der auf den Flow angewendeten Sicherheitsregel, die Regelaktion (Zulassen, Verweigern oder Löschen), die Eingangs- und Ausgangsschnittstelle, die Anzahl der Byte und den Grund für das Sitzungsende. In der Spalte Typ wird angegeben, ob der Eintrag für den Beginn oder das Ende der Sitzung bestimmt ist oder ob die Sitzung verweigert oder abgebrochen wurde. Ein „Drop“ bedeutet, dass die Sicherheitsregel, die den Datenverkehr blockiert hat, eine „beliebige“ Anwendung angegeben hat, während ein „Deny“ bedeutet, dass die Regel eine bestimmte Anwendung identifiziert hat. Wenn der Datenverkehr unterbrochen wird, bevor die Anwendung identifiziert wurde, z. B. wenn eine Regel den gesamten Datenverkehr für einen bestimmten Dienst blockiert, wird die Anwendung als „nicht zutreffend“ angezeigt.
Bedrohung	Zeigt einen Eintrag für jeden von der Firewall generierten Sicherheitsalarm an. Jeder Eintrag enthält Datum und Uhrzeit, einen Namen oder eine URL der Bedrohung, die Quell- und Zielzonen, Adressen und Ports, den Namen der Anwendung sowie die Alarmaktion (zulassen oder blockieren) und den Schweregrad. In der Spalte Typ wird die Art der Bedrohung angegeben, z. B. „Virus“ oder „Spyware“, in der Spalte Name die Beschreibung oder URL der

Protokolltyp	Beschreibung
	Bedrohung und in der Spalte Kategorie die Bedrohungskategorie (z. B. „Keylogger“) oder URL-Kategorie.
URL-Filterung	Zeigt Protokolle für URL-Filter an, die den Zugriff auf Websites kontrollieren und festlegen, ob Benutzer Anmeldeinformationen an Websites senden können.
Konfiguration	Zeigt für jede Konfigurationsänderung einen Eintrag an. Jeder Eintrag enthält Datum und Uhrzeit, den Administratorbenutzernamen, die IP-Adresse, von der aus die Änderung vorgenommen wurde, den Clienttyp (Webinterface oder CLI), die Art der Befehlsausführung, ob der Befehl erfolgreich war oder nicht, den Konfigurationspfad und die Werte vor und nach der Änderung.
System (System)	Zeigt einen Eintrag für jedes Systemereignis an. Jeder Eintrag enthält Datum und Uhrzeit, den Schweregrad des Ereignisses und eine Beschreibung des Ereignisses.
Alarme	Das Alarmprotokoll zeichnet detaillierte Informationen zu Alarmen auf, die vom System generiert werden. Die Informationen in diesem Protokoll werden auch unter Alarme gemeldet. Weitere Informationen finden Sie unter „Alarmeinstellungen definieren“.

Protokolltyp	Beschreibung
Authentifizierung	Zeigt Informationen zu Authentifizierungsereignissen an, die auftreten, wenn Endbenutzer versuchen, auf Netzwerkressourcen zuzugreifen, deren Zugriff durch Authentifizierungsrichtlinienregeln gesteuert wird. Benutzer können diese Informationen verwenden, um Zugriffsprobleme zu beheben und die Benutzerauthentifizierungsrichtlinie nach Bedarf anzupassen. In Verbindung mit Korrelationsobjekten können Benutzer auch Authentifizierungsprotokolle verwenden, um verdächtige Aktivitäten im Netzwerk des Benutzers zu identifizieren, z. B. Brute-Force-Angriffe. Optional können Benutzer Authentifizierungsregeln so konfigurieren, dass Authentifizierungs-Timeouts protokolliert werden. Diese Timeouts beziehen sich auf den Zeitraum, in dem sich ein Benutzer nur einmal für eine Ressource authentifizieren muss, aber wiederholt darauf zugreifen kann. Anhand von Informationen zu den Timeouts können Benutzer entscheiden, ob und wie sie angepasst werden sollen.
Vereinheitlicht	Zeigt die neuesten Protokolleinträge für Verkehr, Bedrohung, URL-Filterung, WildFire Übermittlungen und Datenfilterung in einer einzigen Ansicht an. Die kollektive Protokollansicht ermöglicht es Benutzern, diese verschiedenen Protokolltypen gemeinsam zu untersuchen und zu filtern (anstatt jeden Protokollsatz einzeln zu durchsuchen). Oder Benutzer können wählen, welche Protokolltypen angezeigt werden sollen: Klicken Sie auf den Pfeil links neben dem Filterfeld und wählen Sie Traffic, Bedrohung, URL, Daten, and/or Wildfire aus, um nur die ausgewählten Protokolltypen anzuzeigen.

Verwaltung von Ereignissen

AMS überwacht kontinuierlich die Kapazität, den Zustand und die Verfügbarkeit der Firewall. Von der Firewall generierte Metriken sowie AWS/AMS generierte Metriken werden verwendet, um Alarme zu erstellen, die von den Betriebstechnikern von AMS empfangen werden, die das Problem untersuchen und lösen. Die aktuellen Alarme decken die folgenden Fälle ab:

Ereignisalarme:

- CPU-Auslastung der Firewall-Datenebene

- CPU-Auslastung — CPU der Datenebene (Verarbeitung des Datenverkehrs)
- Die Auslastung der Firewall-Pakete auf Datenebene liegt bei über 80%
 - Paketauslastung — Datenebene (Verarbeitung des Datenverkehrs)
- Nutzung der Firewall-Sitzung auf der Datenebene
- Firewall-Datenebene-Sitzung aktiv
- Aggregierte Firewall-CPU-Auslastung
 - CPU-Auslastung für alle CPUs
- Failover von AZ
 - Alarmt, wenn in einer AZ ein Failover auftritt
- Ungesunder Syslog-Host
 - Der Syslog-Host schlägt die Integritätsprüfung fehl

Management-Alarme:

- Ausfallalarm des Health Check Monitors
 - Wenn der Workflow zur Integritätsprüfung unerwartet fehlschlägt
 - Dies gilt für den Workflow selbst, nicht für den Fall, dass eine Firewall-Integritätsprüfung fehlschlägt
- Alarm bei Ausfall der Passwortrotation
 - Wenn die Passwortrotation fehlschlägt
 - Das API-/Service-Benutzerkennwort wird alle 90 Tage gewechselt

Metriken

Alle Metriken werden erfasst und CloudWatch im Netzwerkkonto gespeichert. Diese können angezeigt werden, indem Sie Konsolenzugriff auf das Netzwerkkonto erhalten und zur CloudWatch Konsole navigieren. Einzelne Metriken können auf der Registerkarte Metriken oder in einer einzigen Dashboard-Ansicht mit ausgewählten Metriken angezeigt werden. Aggregierte Metriken können angezeigt werden, indem Sie zur Registerkarte Dashboard navigieren und AMS-MF-PA-Egress-Dashboard auswählen.

Benutzerdefinierte Metriken:

- Zustandsprüfung

- Namespace: AMS/MF/PA/Egress
 - PARouteTableConnectionsByA-Z
 - PAUnhealthyByInstance
 - PAUnhealthyAggregatedByAZ
 - PAHealthCheckLockState
- Firewall generiert
 - Namespace:/AMS/MF/PA/Egress<instance-id>
 - DataPlaneCPUUtilizationPakt
 - DataPlanePacketBufferUtilization
 - Pfanne GPGateway UtilizationPct
 - panSessionActive
 - panSessionUtilization

CloudWatch Integration von Protokollen

CloudWatch Durch die Integration von Protokollen werden Protokolle von den Firewalls in Logs weitergeleitet, wodurch das Risiko des Verlusts von CloudWatch Protokollen aufgrund der lokalen Speichernutzung verringert wird. Protokolle werden in Echtzeit ausgefüllt, sobald sie von den Firewalls generiert werden, und können bei Bedarf über die Konsole oder API eingesehen werden.

Komplexe Abfragen können für die Protokollanalyse erstellt oder mit CloudWatch Insights als CSV exportiert werden. Darüber hinaus bietet das benutzerdefinierte AMS Managed CloudWatch Firewall-Dashboard auch eine Schnellansicht bestimmter Verkehrsprotokollabfragen und eine grafische Darstellung der Zugriffe und der Richtlinieneinflüsse im Zeitverlauf. Die Verwendung von CloudWatch Protokollen ermöglicht auch die native Integration in andere AWS-Services wie AWS Kinesis.

Note

PA-Protokolle können nicht direkt an einen vorhandenen lokalen Syslog-Collector oder einen Syslog-Collector eines Drittanbieters weitergeleitet werden. Die AMS Managed Firewall-Lösung ermöglicht den Versand von Protokollen von den PA-Maschinen in Echtzeit an AWS CloudWatch Logs. Sie können die CloudWatch Logs Insight-Funktion verwenden, um Ad-hoc-Abfragen auszuführen. Darüber hinaus können Protokolle an die Panorama-Managementlösung Ihres Palo Alto gesendet werden. CloudWatch Protokolle können mithilfe von CloudWatch Abonnementfiltern auch an andere Ziele weitergeleitet werden. Erfahren Sie

im folgenden Abschnitt mehr über Panorama. Weitere Informationen über Splunk finden Sie unter [Integration mit Splunk](#).

Panoramaintegration

AMS Managed Firewall kann optional in Ihr bestehendes Panorama integriert werden. Auf diese Weise können Sie Firewallkonfigurationen von Panorama aus anzeigen oder Protokolle von der Firewall an das Panorama weiterleiten. Die Panorama-Integration mit AMS Managed Firewall ist schreibgeschützt, und Konfigurationsänderungen an den Firewalls von Panorama aus sind nicht zulässig. Panorama wird vollständig von Ihnen verwaltet und konfiguriert. AMS ist nur für die Konfiguration der Firewalls für die Kommunikation mit dem System verantwortlich.

Lizenzen

Der Preis der AMS Managed Firewall hängt von der Art der verwendeten Lizenz (stündlich oder Bring Your Own License, BYOL) und der Instanzgröße ab, in der die Appliance ausgeführt wird. Sie müssen die Instance-Größe und die Lizenzen der Palo Alto-Firewall, die Sie bevorzugen, über den AWS Marketplace bestellen.

- Marketplace-Lizenzen: Akzeptieren Sie die Allgemeinen Geschäftsbedingungen des VM-Series Next-Generation Firewall Bundle 1 über das Netzwerkkonto in MALZ.
- BYOL-Lizenzen: Akzeptieren Sie die Nutzungsbedingungen der VM-Series Next-Generation Firewall (BYOL) über das Netzwerkkonto in MALZ und geben Sie den „BYOL-Authentifizierungscode“, den Sie nach dem Kauf der Lizenz erhalten haben, an AMS weiter.

Einschränkungen

Derzeit unterstützt AMS Firewalls der Serien VM-300 oder VM-500. Konfigurationen finden Sie hier: [Modelle der VM-Serie auf EC2 AWS-Instances](#),

Note

Die AMS-Lösung wird im Active-Active-Modus ausgeführt, da jede PA-Instance in ihrer AZ den ausgehenden Datenverkehr für ihre jeweilige AZ abwickelt. Bei zwei AZs Instanzen verarbeitet jede PA-Instance also ausgehenden Datenverkehr mit bis zu 5 Gbit/s und bietet effektiv einen Gesamtdurchsatz von 10 Gbit/s über zwei. AZs Das Gleiche gilt für alle Grenzwerte in jeder AZ. Sollte die AMS-Zustandsprüfung fehlschlagen, verlagern wir den

Verkehr von der AZ mit der fehlerhaften PA auf eine andere AZ, und beim Austausch der Instance wird die Kapazität auf die verbleibenden AZs Grenzwerte reduziert.

AMS unterstützt derzeit keine anderen Palo Alto-Pakete, die auf dem AWS Marketplace erhältlich sind. Sie können beispielsweise nicht nach dem „VM-Series Next-Generation Firewall Bundle 2“ fragen. Beachten Sie, dass die AMS Managed Firewall-Lösung, die Palo Alto verwendet, derzeit nur ein Angebot zur Filterung des ausgehenden Datenverkehrs bietet, sodass die Verwendung erweiterter Pakete der VM-Serie keine zusätzlichen Funktionen oder Vorteile bieten würde.

Anforderungen für das Onboarding

- Sie müssen die Allgemeinen Geschäftsbedingungen der VM-Series Next-Generation Firewall von Palo Alto im AWS Marketplace lesen und akzeptieren.
- Sie müssen die Instance-Größe, die Sie verwenden möchten, auf der Grundlage Ihrer erwarteten Arbeitslast bestätigen.
- Sie müssen einen /24-CIDR-Block angeben, der nicht zu Konflikten mit Netzwerken in Ihrer Multi-Account-Landing Zone-Umgebung oder vor Ort führt. Sie muss derselben Klasse angehören wie die Egress-VPC (die Lösung stellt eine /24-VPC-Erweiterung für die Egress-VPC VPC).

Preise

Die Basiskosten für die Infrastruktur von AMS Managed Firewall sind in drei Hauptfaktoren aufgeteilt: die EC2 Instanz, die die Palo Alto-Firewall hostet, die Softwarelizenz, die Lizenzen der Palo Alto VM-Serie und Integrationen. CloudWatch

Die folgenden Preise basieren auf der Firewall der Serie VM-300.

- EC2 Instanzen: Die Palo Alto-Firewall wird in einem Hochverfügbarkeitsmodell mit 2-3 EC2 Instanzen ausgeführt, wobei die Instanz auf den erwarteten Workloads basiert. Die Kosten für die Instanz hängen von der Region und der Anzahl der ab AZs
 - Bsp. us-east-1, m5.xlarge, 3 AZs
 - $0,192\$ \cdot 24 \cdot 30 \cdot 3 = 414,72\$$
 - <https://aws.amazon.com/ec2/Preise/auf Abfrage/>
- Palo Alto-Lizenzen: Die Softwarelizenzkosten einer Palo Alto VM-300-Firewall der nächsten Generation hängen von der Anzahl der AZ sowie vom Instanztyp ab.

- Bsp. us-east-1, m5.xlarge, 3 AZs
 - $0,87\$ * 24 * 30 * 3 = 1879,20\$$
 - https://aws.amazon.com/marketplace/PP/B083M7JPKB?ref_=srh_res_product_title#pdp - Preisgestaltung
- CloudWatch Integration von Protokollen: Die Protokollintegration nutzt SysLog Server (-t3.medium), NLB und CloudWatch Protokolle. EC2 CloudWatch Die Kosten für die Server hängen von der Region und der Anzahl der Server ab AZs, und die Kosten für die NLB/CloudWatch Protokolle variieren je nach Auslastung des Datenverkehrs.
- Bsp. us-east-1, t3.medium, 3AZ
 - $0,0416\$ * 24 * 30 * 3 = 89,86\$$
 - <https://aws.amazon.com/ec2/Preise/auf Abfrage/>
 - <https://aws.amazon.com/cloudwatch/Preisgestaltung/>

Umkreis (DMZ) VPC

Die Perimeter- oder DMZ-VPC enthält die Ressourcen, die AMS-Betriebsingenieure für den Zugriff auf AMS-Netzwerke benötigen. Es enthält öffentliche Subnetze in 2-3 AZs Bereichen mit SSH-Bastions-Hosts in einer Auto Scaling Scaling-Gruppe (ASG), in die sich die Techniker von AMS Operations einloggen oder einen Tunnel durchqueren können. Die Sicherheitsgruppen, die den DMZ-Bastionen zugeordnet sind, enthalten Port-22-Regeln für eingehenden Datenverkehr von Amazon Corp Networks.

DMZ-VPC-CIDR-Bereich: Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 Adressbereich für die VPC in Form eines CIDR-Blocks (Classless Inter-Domain Routing) angeben, z. B. 10.0.16.0/24. Dies ist der primäre CIDR-Block für Ihre VPC.

Note

Das AMS-Team empfiehlt den Bereich von 24 (mit mehr IP-Adressen), um einen gewissen Puffer für den Fall bereitzustellen, dass in future andere Ressourcen, wie z. B. eine Firewall, bereitgestellt werden.

AWS Transit Gateway

AWS Transit Gateway (TGW) ist ein Service, mit dem Sie Ihre Amazon Virtual Private Clouds (VPCs) und Ihre lokalen Netzwerke mit einem einzigen Gateway verbinden können. Transit Gateway ist das

Netzwerk-Backbone, das das Routing zwischen AMS-Kontonetzwerken und externen Netzwerken abwickelt. Informationen zu Transit Gateway finden Sie unter [AWS Transit Gateway](#).

Geben Sie die folgenden Eingaben ein, um diese Ressource zu erstellen:

- Transit Gateway-ASN-Nummer *: Geben Sie die private Autonome Systemnummer (ASN) für Ihr Transit Gateway an. Dabei sollte es sich um die ASN für die AWS-Seite einer BGP-Sitzung (Border Gateway Protocol) handeln. Der Bereich liegt zwischen 64512 und 65534 für 16-Bit. ASNs

Shared Services-Konto

Das Shared Services-Konto dient als zentraler Knotenpunkt für die meisten AMS-Datenebenendienste. Das Konto enthält die Infrastruktur und die Ressourcen, die für Access Management (AD) und Endpoint Security Management (Trend Micro) erforderlich sind, und es enthält die Kundenbastionen (SSH/RDP). Die folgende Grafik bietet einen allgemeinen Überblick über die im Shared Services-Konto enthaltenen Ressourcen.

Die Shared Services-VPC besteht aus dem AD-Subnetz, dem EPS-Subnetz und dem Customer-Bastions-Subnetz in den drei Verfügbarkeitszonen (). AZs Die in der Shared Services-VPC erstellten Ressourcen sind unten aufgeführt und erfordern Ihre Eingabe.

- Shared Services VPC CIDR-Bereich: Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 Adressbereich für die VPC in Form eines CIDR-Blocks (Classless Inter-Domain Routing) angeben, z. B. 10.0.1.0/24. Dies ist der primäre CIDR-Block für Ihre VPC.

Note

Das AMS-Team empfiehlt den Bereich /23.

- Active Directory-Details: Microsoft Active Directory (AD) wird für user/resource Verwaltung, Authentifizierung/Autorisierung und DNS für all Ihre AMS-Landingzone-Konten mit mehreren Konten verwendet. AMS AD ist außerdem mit einer unidirektionalen Vertrauensstellung für Ihr Active Directory für eine vertrauensbasierte Authentifizierung konfiguriert. Die folgende Eingabe ist erforderlich, um das AD zu erstellen:
 - Domain Fully Qualified Domain Name (FQDN): Der vollqualifizierte Domainname für das AWS Managed Microsoft AD-Verzeichnis. Die Domain sollte keine bestehende Domain oder untergeordnete Domain einer bestehenden Domain in Ihrem Netzwerk sein.

- **Domain-NetBIOS-Name:** Wenn Sie keinen NetBIOS-Namen angeben, verwendet AMS standardmäßig den ersten Teil Ihres Verzeichnis-DNS als Namen. Zum Beispiel corp für das Verzeichnis DNS corp.example.com.
- **Trend Micro — Endpoint Protection Security (EPS):** Trend Micro Endpoint Protection (EPS) ist die Hauptkomponente von AMS für die Betriebssystemsicherheit. Das System besteht aus Deep Security Manager (DSM), EC2 Instanzen, EC2 Relay-Instanzen und einem Agenten, der auf allen Datenebenen und EC2 Kundeninstanzen präsent ist.

Sie müssen das `EPSMarketplaceSubscriptionRole` im Shared Services-Konto verwenden und entweder das Trend Micro Deep Security (BYOL) AMI oder Trend Micro Deep Security (Marketplace) abonnieren.

Die folgenden Standardeingaben sind erforderlich, um EPS zu erstellen (falls Sie die Standardwerte ändern möchten):

- **Relay-Instanztyp:** Standardwert — m5.large
- **DSM-Instanztyp:** Standardwert — m5.xlarge
- **DB-Instance-Größe:** Standardwert — 200 GB
- **RDS-Instance-Typ:** Standardwert — db.m5.large
- **Kundenbastionen:** Im Shared Services-Konto stehen Ihnen SSH- oder RDP-Bastionen (oder beide) zur Verfügung, um auf andere Hosts in Ihrer AMS-Umgebung zugreifen zu können. Um als Benutzer auf das AMS-Netzwerk zuzugreifen (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPN zum Transit Gateway (TGW)) und wird dann zur Shared Services-VPC weitergeleitet. Sobald Sie auf die Bastion zugreifen können, können Sie zu anderen Hosts in der AMS-Umgebung springen, sofern die Zugriffsanfrage genehmigt wurde.
- Die folgenden Eingaben sind für SSH-Bastionen erforderlich.
 - **Gewünschte Instanzkapazität von SSH Bastion:** Standardwert: 2.
 - **Maximale Anzahl an SSH Bastion-Instanzen:** Standardwert: 4.
 - **Minimale Anzahl an SSH-Bastion-Instanzen:** Standardwert -2.
 - **SSH Bastion-Instanztyp:** Standardwert — m5.large (kann geändert werden, um Kosten zu sparen; zum Beispiel ein t3.medium).

- SSH Bastion Ingress CIDRs: IP-Adressbereiche, von denen aus Benutzer in Ihrem Netzwerk auf SSH Bastions zugreifen.
- Die folgenden Eingaben sind für Windows RDP-Bastionen erforderlich.
 - RDP-Bastion-Instanztyp: Standardwert — t3.medium.
 - Gewünschte Mindestanzahl an Sitzungen für RDP Bastion: Standardwert: 2.
 - Maximale Anzahl an RDP-Sitzungen: Standardwert -10.
 - RDP Bastion-Konfigurationstyp: Sie können eine der folgenden Konfigurationen wählen
 - SecureStandard = Ein Benutzer erhält eine Bastion und nur ein Benutzer kann sich mit der Bastion verbinden.
 - SecureHA = Ein Benutzer erhält zwei Bastionen in zwei verschiedenen AZs, mit denen er sich verbinden kann, und nur ein Benutzer kann sich mit der Bastion verbinden.
 - SharedStandard = Ein Benutzer erhält eine Bastion, mit der er sich verbinden kann, und zwei Benutzer können sich gleichzeitig mit derselben Bastion verbinden.
 - shareDHA = Ein Benutzer erhält zwei Bastionen in zwei verschiedenen AZs, mit denen er sich verbinden kann, und zwei Benutzer können sich gleichzeitig mit derselben Bastion verbinden.
- Kunden-RDP-Eingang CIDRs: IP-Adressbereiche, von denen aus Benutzer in Ihrem Netzwerk auf RDP Bastions zugreifen.

Aktualisierungen für gemeinsame Dienste: Landing Zone für mehrere Konten

AMS wendet auf monatlicher Basis und ohne vorherige Ankündigung Datenebenen-Releases auf verwaltete Konten an.

AMS verwendet die zentrale Organisationseinheit, um gemeinsam genutzte Dienste wie Zugriff, Netzwerk, EPS, Protokollspeicherung und Alert-Aggregation in Ihrer Multi-Account-Landing Zone bereitzustellen. AMS ist für die Behebung von Sicherheitslücken, das Patchen und die Bereitstellung dieser gemeinsamen Dienste verantwortlich. AMS aktualisiert regelmäßig die Ressourcen, die für die Bereitstellung dieser gemeinsamen Dienste verwendet werden, sodass Benutzer Zugriff auf die neuesten Funktionen und Sicherheitsupdates haben. Die Updates erfolgen in der Regel monatlich. Zu den Ressourcen, die Teil dieser Updates sind, gehören:

- Konten, die Teil der Kernorganisationseinheit sind.

Das Verwaltungskonto, das Shared Services-Konto, das Netzwerkkonto, das Sicherheitskonto und das Protokollarchivkonto verfügen über Ressourcen für RDP- und SSH-Bastionen, Proxys,

Management-Hosts und Endpoint Security (EPS), die normalerweise jeden Monat aktualisiert werden. AMS verwendet unveränderliche EC2 Bereitstellungen als Teil der Shared Services-Infrastruktur.

- Neues AMS AMIs mit den neuesten Updates.

Note

AMS-Operatoren verwenden bei der Ausführung von Änderungen an der Datenebene einen internen Alarmunterdrückungsänderungstyp (CT), und der RFC für diesen CT wird in Ihrer RFC-Liste angezeigt. Dies liegt daran, dass bei der Bereitstellung der Datenebenenversion verschiedene Infrastrukturen heruntergefahren, neu gestartet oder offline geschaltet werden können oder dass CPU-Spitzen oder andere Auswirkungen der Bereitstellung auftreten können, die Alarmer auslösen, die während der Bereitstellung der Datenebene irrelevant sind. Sobald die Bereitstellung abgeschlossen ist, wird überprüft, ob die gesamte Infrastruktur ordnungsgemäß funktioniert, und die Alarmer werden wieder aktiviert.

Konto protokollieren und archivieren

Das Log Archive-Konto dient als zentrale Anlaufstelle für die Archivierung von Protokollen in Ihrer AMS-Landingzone-Umgebung mit mehreren Konten. Das Konto enthält einen S3-Bucket, der Kopien der AWS CloudTrail - und AWS Config-Protokolldateien von jedem der AMS-Landingzone-Umgebungskonten mit mehreren Konten enthält. Sie könnten dieses Konto für Ihre zentralisierte Logging-Lösung mit AWS Firehose oder Splunk usw. verwenden. Der Zugriff von AMS auf dieses Konto ist auf einige wenige Benutzer beschränkt. Der Zugriff ist auf Prüfer und Sicherheitsteams beschränkt, die für Compliance-Untersuchungen und forensische Untersuchungen im Zusammenhang mit Kontoaktivitäten zuständig sind.

Sicherheitskonto

Das Sicherheitskonto ist die zentrale Anlaufstelle für Operationen im Zusammenhang mit der Wohnungssicherheit und die zentrale Anlaufstelle für die Weiterleitung von Benachrichtigungen und Warnmeldungen an die AMS-Steuerflugzeugdienste. Darüber hinaus beherbergt das Sicherheitskonto das Amazon Guard Duty-Verwaltungskonto und den AWS Config-Aggregator.

Arten von Anwendungskonten

Anwendungskonten sind AWS-Konten innerhalb der von AMS verwalteten landing zone Zone-Architektur, die Sie zum Hosten Ihrer Workloads verwenden. AMS bietet drei Arten von Anwendungskonten an:

- [Von AMS verwaltete Anwendungskonten](#)
- [AMS Accelerate-Konten](#)
- [Vom Kunden verwaltete Anwendungskonten](#)

Anwendungskonten werden OUs in AWS Organizations je nach Art des Anwendungskontos unterschiedlich gruppiert:

- Stamm-OU:
 1. Anwendungen (OU)
 - Verwaltete Organisationseinheit: Von AMS verwaltete Konten
 - Entwicklungs-OU: Von AMS verwaltete Konten mit aktiviertem Entwicklermodus
 2. Accelerate OU: AMS Accelerate Application-Konten
 3. Kundenverwaltete Organisationseinheit: Vom Kunden verwaltete Anwendungskonten

Anwendungskonten werden über einen RFC bereitgestellt, der vom Verwaltungskonto aus übermittelt wird:

- [Anwendungskonto mit VPC erstellen ct-1zdasmc2ewzrs](#)
- [Accelerate-Konto erstellen ct-2p93tyd5angmi](#)
- [Erstellen Sie ein vom Kunden verwaltetes Anwendungskonto ct-3pwbixz27n3tn](#)

Von AMS verwaltete Anwendungskonten

Anwendungskonten, die vollständig von AMS verwaltet werden, werden als AMS-verwaltete Anwendungskonten bezeichnet, bei denen einige oder alle betrieblichen Aufgaben, wie z. B. Verwaltung von Serviceanfragen, Vorfallmanagement, Sicherheitsmanagement, Kontinuitätsmanagement (Backup), Patchmanagement, Kostenoptimierung oder Überwachung und Eventmanagement der Infrastruktur, von AMS ausgeführt werden.

Die Anzahl der von AMS ausgeführten Aufgaben hängt vom ausgewählten Change-Management-Modus ab. Von AMS verwaltete Konten unterstützen verschiedene Modi für das Änderungsmanagement:

- [RFC-Modus](#)
- [Direkter Änderungsmodus in AMS](#)
- [AMS- und AWS Service Catalog](#)
- [AMS Advanced-Entwicklermodus](#)
- [Self-Service-Bereitstellungsmodus in AMS](#)

Weitere Informationen zum Änderungsmanagement und zu den verschiedenen Modi finden Sie unter [Verwaltungsmodi ändern](#)

Es gibt einige AWS-Services, die Sie in Ihrem AMS-verwalteten Konto ohne AMS-Management verwenden können. Die Liste dieser AWS-Services und wie Sie sie Ihrem AMS-Konto hinzufügen können, finden Sie im Abschnitt [Self-Service-Bereitstellung](#).

AMS Accelerate-Konten

AMS Accelerate ist der AMS-Betriebsplan, mit dem die AWS-Infrastruktur betrieben werden kann, die Workloads unterstützt. Sie können von den Betriebsservices von AMS Accelerate wie Überwachung und Warnung, Incident Management, Sicherheitsmanagement und Backup-Management profitieren, ohne eine neue Migration durchführen zu müssen, Ausfallzeiten zu erleben oder Ihre Nutzung von AWS zu ändern. AMS Accelerate bietet auch ein optionales Patch-Add-on für EC2 basierte Workloads, die regelmäßig gepatcht werden müssen.

Mit AMS Accelerate haben Sie die Freiheit, alle AWS-Services nativ oder mit Ihren bevorzugten Tools zu verwenden, zu konfigurieren und bereitzustellen. Sie verwenden Ihre bevorzugten Zugriffs- und Änderungsmechanismen, während AMS konsequent bewährte Verfahren anwendet, die Ihnen helfen, Ihr Team zu skalieren, Kosten zu optimieren, Sicherheit und Effizienz zu erhöhen und die Ausfallsicherheit zu verbessern.

Note

AMS Accelerate-Konten in AMS Advanced verfügen weder über AMS Change Management (RFCs) noch über die AMS Advanced-Konsole. Stattdessen verfügen sie über die AMS Accelerate-Konsole und Funktionen.

Accelerate-Konten können nur über Ihr AMS-Landing landing zone Management-Konto mit mehreren Konten bereitgestellt werden. Accelerate bietet verschiedene betriebliche Funktionen. Weitere Informationen finden Sie in der [Leistungsbeschreibung von Accelerate](#).

- Sie werden weiterhin einige der Funktionen der Kernkonten mit mehreren Konten (MALZ) nutzen können, z. B. zentrale Protokollierung, Einzelabrechnung, Config Aggregator im Sicherheitskonto und. SCPs
- AMS Accelerate bietet einige AMS Advanced-Dienste wie EPS, Access Management, Change Management und Provisioning nicht an. Wir empfehlen Ihnen, die nächsten Schritte zu befolgen, um Zugriff auf das Transit Gateway (TGW) zu erhalten und es zu konfigurieren.

Weitere Informationen zu Accelerate finden Sie unter [Was ist Accelerate](#).

Erstellen Sie Ihr Accelerate-Konto

Gehen Sie wie folgt vor, um ein Accelerate-Konto zu [erstellen: Accelerate-Konto erstellen](#).

Zugriff auf Ihr Accelerate-Konto

Nachdem Sie ein Accelerate-Konto in Ihrem MALZ-Konto (Multi-Account landing zone) bereitgestellt haben, können Sie in dem Konto eine Rolle mit [administrativen Zugriffsberechtigungen](#) übernehmen.
`AccelerateDefaultAdminRole`

So greifen Sie auf das neue Accelerate-Konto zu:

1. Melden Sie sich bei der IAM-Konsole für das Verwaltungskonto mit der `CustomerDefaultAssumeRole` Rolle an.
2. Wählen Sie in der IAM-Konsole in der Navigationsleiste Ihren Benutzernamen aus.
3. Wählen Sie Switch Role. Wenn Sie diese Option erstmalig auswählen, wird eine Seite mit weiteren Informationen angezeigt. Lesen Sie sich diese Informationen durch und klicken Sie dann auf Switch Role (Rolle wechseln). Wenn Sie die Cookies Ihres Browsers löschen, kann die Seite erneut angezeigt werden.
4. Geben Sie auf der Seite „Rolle wechseln“ die Accelerate-Konto-ID und den Namen der Rolle ein, die Sie annehmen möchten:`AccelerateDefaultAdminRole`.

Nachdem Sie nun Zugriff haben, können Sie neue IAM-Rollen erstellen, um weiterhin auf Ihre Umgebung zuzugreifen. Wenn Sie SAML Federation für Ihr Accelerate-Konto nutzen möchten, finden

Sie weitere Informationen unter [Aktivieren des Zugriffs auf die AWS-Managementkonsole für SAML 2.0-Verbundbenutzer](#).

Ihr Accelerate-Konto mit Transit Gateway verbinden

AMS verwaltet die Netzwerkeinrichtung eines Accelerate-Kontos nicht. Sie haben die Möglichkeit, Ihr eigenes Netzwerk mit AWS zu verwalten APIs (siehe [Netzwerklösungen](#)) oder eine Verbindung zum von AMS verwalteten MALZ-Netzwerk herzustellen, indem Sie das bestehende Transit Gateway (TGW) verwenden, das in AMS MALZ bereitgestellt wird.

 Note

Sie können nur dann eine VPC mit dem TGW verbinden, wenn sich das Accelerate-Konto in derselben AWS-Region befindet. Weitere Informationen finden Sie unter [Transit-Gateways](#).

Um Ihr Accelerate-Konto zu Transit Gateway hinzuzufügen, fordern Sie mithilfe des Änderungstyps [Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Statische Route hinzufügen \(ct-3r2ckznmt0a59\) eine neue Route](#) an. Geben Sie folgende Informationen an:

- **Blackhole:** True bedeutet, dass das Ziel der Route nicht verfügbar ist. Tun Sie dies, wenn der Verkehr für die statische Route vom Transit Gateway unterbrochen werden soll. False, um den Verkehr an die angegebene TGW-Anhangs-ID weiterzuleiten. Der Standardwert ist „false“.
- **DestinationCidrBlock:** Der IPV4 CIDR-Bereich, der für Zielübereinstimmungen verwendet wird. Routing-Entscheidungen basieren auf der genauesten Übereinstimmung. Beispiel: 10.0.2.0/24.
- **TransitGatewayAttachmentId:** Die TGW-Anhangs-ID, die als Ziel für die Routentabelle dient. Wenn Blackhole den Wert false hat, ist dieser Parameter erforderlich, andernfalls lassen Sie diesen Parameter leer. Beispiel: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId:** Die ID der TGW-Routentabelle. Beispiel: tgw-rtb-06ddc751c0c0c881c.

Erstellen Sie Routen in den TGW-Routentabellen, um eine Verbindung zu dieser VPC herzustellen:

1. Standardmäßig kann diese VPC mit keiner anderen VPCs in Ihrem MALZ-Netzwerk kommunizieren.
2. Entscheiden Sie mit Ihrem Lösungsarchitekten, mit was VPCs diese Accelerate-VPC kommunizieren soll.

3. [Bereitstellung einreichen](#) | [Verwaltete landing zone](#) | [Netzwerkkonto](#) | [Änderungstyp für statische Route \(ct-3r2ckznmt0a59\) hinzufügen](#), geben Sie folgende Informationen an:

- **Blackhole:** True bedeutet, dass das Ziel der Route nicht verfügbar ist. Tun Sie dies, wenn der Verkehr für die statische Route vom Transit Gateway unterbrochen werden soll. False, um den Verkehr an die angegebene TGW-Anhangs-ID weiterzuleiten. Der Standardwert ist „false“.
- **DestinationCidrBlock:** Der IPV4 CIDR-Bereich, der für Zielübereinstimmungen verwendet wird. Routing-Entscheidungen basieren auf der genauesten Übereinstimmung. Beispiel: 10.0.2.0/24.
- **TransitGatewayAttachmentId:** Die TGW-Anhangs-ID, die als Ziel für die Routentabelle dient. Wenn Blackhole den Wert false hat, ist dieser Parameter erforderlich, andernfalls lassen Sie diesen Parameter leer. Beispiel: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId:** Die ID der TGW-Routentabelle. Beispiel: tgw-rtb-06ddc751c0c0c881c.

Eine neue Accelerate-Account-VPC mit dem AMS Multi-Account Landing Zone-Netzwerk verbinden (einen TGW-VPC-Anhang erstellen):

1. Öffnen Sie in Ihrem landing zone Networking-Konto mit mehreren Konten die [Amazon VPC-Konsole](#).
2. Klicken Sie im Navigationsbereich auf Transit Gateways. Notieren Sie sich die TGW-ID des Transit-Gateways, das Sie sehen.
3. Öffnen Sie in Ihrem Accelerate-Konto die [Amazon VPC-Konsole](#).
4. Wählen Sie im Navigationsbereich Transit Gateway Gateway-Anlagen > Transit Gateway Gateway-Anlage erstellen. Treffen Sie diese Entscheidungen:
 - Wählen Sie für die Transit Gateway Gateway-ID die Transit-Gateway-ID aus, die Sie in Schritt 2 aufgezeichnet haben.
 - Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.
 - Geben Sie unter VPC Attachment (VPC-Anfügung) optional einen Namen für Attachment name tag (Anfügungs-Namens-Tag) ein.
 - Wählen Sie aus, ob DNS-Support und IPv6 Support aktiviert werden sollen.
 - Wählen Sie für VPC ID die VPC aus, die dem Transit-Gateway angefügt werden soll. Dieser VPC muss mindestens ein Subnetz zugeordnet sein.
 - Wählen Sie unter Subnetz ein Subnetz für jede Availability Zone aus IDs, das vom Transit-Gateway zur Weiterleitung des Datenverkehrs verwendet werden soll. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.

5. Wählen Sie **Create attachment** (Anhang erstellen) aus. Notieren Sie sich die ID des neu erstellten TGW-Anhangs.

Zuordnen des TGW-Anhangs zu einer Routentabelle:

1. Entscheiden Sie, welcher TGW-Routentabelle Sie die VPC zuordnen möchten. Wir empfehlen, eine neue Anwendungsroutentabelle für das Accelerate-Konto VPCs mithilfe des Änderungstyps **Deployment | Managed landing zone | Netzwerkkonto | Transit-Gateway-Routentabelle erstellen** (ct-3dscwaeyi6cup) zu erstellen.
2. Reichen Sie einen RFC [Management | Managed landing zone | Networking Account | TGW-Attachment \(ct-3nmhh0qr338q6\)](#) für das Netzwerkkonto ein, um den VPC- oder TGW-Anhang der ausgewählten Routentabelle zuzuordnen.

Erstellen Sie Routen in den TGW-Routentabellen, um eine Verbindung zu dieser VPC herzustellen:

1. Standardmäßig kann diese VPC mit keiner anderen VPCs in Ihrem Landingzone-Netzwerk mit mehreren Konten kommunizieren.
2. Entscheiden VPCs Sie mit Ihrem Lösungsarchitekten, mit was diese Accelerate-Account-VPC kommunizieren soll.
3. [Bereitstellung einreichen | Verwaltete landing zone | Netzwerkkonto | Fügen Sie statische Route](#) (ct-3r2ckznmt0a59) RFC für das Netzwerkkonto hinzu, um die benötigten TGW-Routen zu erstellen.

Konfiguration Ihrer VPC-Routing-Tabellen so, dass sie auf das AMS landing zone Transit Gateway für mehrere Konten verweisen:

1. Entscheiden Sie gemeinsam mit Ihrem Lösungsarchitekten, welchen Verkehr Sie an das AMS Multi-Account Landing Zone-Transit-Gateway senden möchten.
2. [Bereitstellung einreichen | Verwaltete landing zone | Netzwerkkonto | Fügen Sie statische Route](#) (ct-3r2ckznmt0a59) RFC für das Netzwerkkonto hinzu, um die benötigten TGW-Routen zu erstellen.

Vom Kunden verwaltete Anwendungskonten

Sie können Konten erstellen, die AMS nicht standardmäßig verwaltet. Diese Konten werden als vom Kunden verwaltete Konten bezeichnet und geben Ihnen die volle Kontrolle über den Eigenbetrieb der

Infrastruktur innerhalb der Konten, während Sie gleichzeitig die Vorteile der zentralisierten Architektur nutzen können, die von AMS verwaltet wird.

Kundenverwaltete Konten haben keinen Zugriff auf die AMS-Konsole oder einen der von uns angebotenen Dienste (Patch, Backup usw.).

Kundenverwaltete Konten können nur über Ihr AMS-Landingzone-Verwaltungskonto mit mehreren Konten bereitgestellt werden.

Verschiedene AMS-Modi funktionieren unterschiedlich mit Anwendungskonten. Weitere Informationen zu den Modi finden Sie unter [AWS Managed Services Services-Modi](#).

Informationen zur Erstellung Ihres kundenverwalteten Anwendungskontos finden Sie unter [Verwaltungskonto | Kundenverwaltetes Anwendungskonto erstellen](#).

Um ein vom Kunden verwaltetes Anwendungskonto zu löschen, verwenden Sie [Verwaltungskonto | Offboard-Anwendungskonto](#). (Das [Confirm Offboarding](#) CT gilt nicht für vom Kunden verwaltete Anwendungskonten.)

Zugriff auf Ihr vom Kunden verwaltetes Konto

Nachdem Sie ein vom Kunden verwaltetes Konto (CMA) in der landing zone mit mehreren Konten (MALZ) bereitgestellt haben, befindet sich im Konto eine Administratorrolle `CustomerDefaultAdminRole`, die Sie über den SAML-Verbund übernehmen müssen, um das Konto zu konfigurieren.

So greifen Sie auf die CMA zu:

1. Melden Sie sich bei der IAM-Konsole für das Verwaltungskonto mit der Rolle an `CustomerDefaultAssumeRole`.
2. Wählen Sie in der IAM-Konsole in der Navigationsleiste Ihren Benutzernamen aus.
3. Wählen Sie Switch Role. Wenn Sie diese Option erstmalig auswählen, wird eine Seite mit weiteren Informationen angezeigt. Lesen Sie sich diese Informationen durch und klicken Sie dann auf Switch Role (Rolle wechseln). Wenn Sie die Cookies Ihres Browsers löschen, kann die Seite erneut angezeigt werden.
4. Geben Sie auf der Seite „Rolle wechseln“ die ID des vom Kunden verwalteten Kontos und den Namen der Rolle ein, die Sie übernehmen möchten: `CustomerDefaultAdminRole`.

Nachdem Sie nun Zugriff haben, können Sie neue IAM-Rollen erstellen, um weiterhin auf Ihre Umgebung zuzugreifen. Wenn Sie SAML Federation für Ihr CMA-Konto nutzen möchten, finden Sie

weitere Informationen unter [Aktivieren des Zugriffs auf die AWS-Managementkonsole für SAML 2.0-Verbundbenutzer](#).

Verbinden Sie Ihre CMA mit Transit Gateway

AMS verwaltet nicht die Netzwerkeinrichtung von vom Kunden verwalteten Konten (CMAs). Sie haben die Möglichkeit, Ihr eigenes Netzwerk mit AWS zu verwalten APIs (siehe [Networking Solutions](#)) oder eine Verbindung zu dem von AMS verwalteten Mehrkonto-Landingzone-Netzwerk herzustellen, indem Sie das bestehende Transit Gateway (TGW) verwenden, das in AMS MALZ bereitgestellt wird.

Note

Sie können nur dann eine VPC mit dem TGW verbinden, wenn sich die CMA in derselben AWS-Region befindet. [Weitere Informationen finden Sie unter Transit-Gateways](#).

Um Ihre CMA zu Transit Gateway hinzuzufügen, fordern Sie eine neue Route mit dem Änderungstyp [Netzwerkkonto | Statische Route hinzufügen \(ct-3r2ckznmt0a59\)](#) an und geben Sie folgende Informationen an:

- **Blackhole:** True bedeutet, dass das Ziel der Route nicht verfügbar ist. Tun Sie dies, wenn der Verkehr für die statische Route vom Transit Gateway unterbrochen werden soll. False, um den Verkehr an die angegebene TGW-Anhangs-ID weiterzuleiten. Der Standardwert ist „false“.
- **DestinationCidrBlock:** Der IPV4 CIDR-Bereich, der für Zielübereinstimmungen verwendet wird. Routing-Entscheidungen basieren auf der genauesten Übereinstimmung. Beispiel: 10.0.2.0/24.
- **TransitGatewayAttachmentId:** Die TGW-Anhangs-ID, die als Ziel für die Routentabelle dient. Wenn Blackhole den Wert false hat, ist dieser Parameter erforderlich, andernfalls lassen Sie diesen Parameter leer. Beispiel: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId:** Die ID der TGW-Routentabelle. Beispiel: tgw-rtb-06ddc751c0c0c881c.

Verbindung einer neuen kundenverwalteten VPC mit dem AMS Multi-Account Landing Zone-Netzwerk (Erstellen eines TGW-VPC-Anhangs):

1. Öffnen Sie in Ihrem landing zone Networking-Konto mit mehreren Konten die [Amazon VPC-Konsole](#).

2. Wählen Sie im Navigationsbereich Transit Gateways aus. Notieren Sie sich die TGW-ID des Transit-Gateways, das Sie sehen.
3. Öffnen Sie in Ihrem vom Kunden verwalteten Konto die [Amazon VPC-Konsole](#).
4. Wählen Sie im Navigationsbereich Transit Gateway Gateway-Anlagen > Transit Gateway Gateway-Anlage erstellen. Treffen Sie diese Entscheidungen:
 - a. Wählen Sie für die Transit Gateway Gateway-ID die Transit-Gateway-ID aus, die Sie in Schritt 2 aufgezeichnet haben.
 - b. Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.
 - c. Geben Sie unter VPC Attachment (VPC-Anfügung) optional einen Namen für Attachment name tag (Anfügungs-Namens-Tag) ein.
 - d. Wählen Sie aus, ob DNS-Support und IPv6 Support aktiviert werden sollen.
 - e. Wählen Sie für VPC ID die VPC aus, die dem Transit-Gateway angefügt werden soll. Dieser VPC muss mindestens ein Subnetz zugeordnet sein.
 - f. Wählen Sie unter Subnetz ein Subnetz für jede Availability Zone aus IDs, das vom Transit-Gateway zur Weiterleitung des Datenverkehrs verwendet werden soll. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.
5. Wählen Sie Create attachment (Anhang erstellen) aus. Notieren Sie sich die ID des neu erstellten TGW-Anhangs.

Zuordnen des TGW-Anhangs zu einer Routentabelle:

Entscheiden Sie, mit welcher TGW-Routentabelle Sie die VPC verknüpfen möchten. Wir empfehlen, eine neue Anwendungsroutentabelle für Customer Managed zu erstellen, VPCs indem Sie einen RFC für Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Transit-Gateway-Routentabelle erstellen (ct-3dscwaeyi6cup) einreichen. Um die VPC- oder TGW-Anlage der ausgewählten Routing-Tabelle zuzuordnen, reichen Sie einen RFC Deployment | Managed landing zone | Networking Account | Associate TGW Attachment (ct-3nmhh0qr338q6) für das Netzwerkkonto ein.

Erstellen Sie Routen in den TGW-Routentabellen, um eine Verbindung zu dieser VPC herzustellen:

1. Standardmäßig kann diese VPC mit keiner anderen VPCs in Ihrem Multi-Account-Landingzone-Netzwerk kommunizieren.
2. Entscheiden Sie mit Ihrem Lösungsarchitekten, mit was VPCs diese vom Kunden verwaltete VPC kommunizieren soll. Bereitstellung einreichen | Verwaltete landing zone | Netzwerkkonto | Fügen Sie statische Route (ct-3r2ckznmt0a59) RFC für das Netzwerkkonto hinzu, um die benötigten TGW-Routen zu erstellen.

 Note

Dieses CT (ct-3r2ckznmt0a59) erlaubt es nicht EgressRouteDomain, statische Routen zur Core-Routentabelle hinzuzufügen. Wenn Ihre CMA ausgehenden Verkehr zulassen muss, reichen Sie einen Management | Other | Other (MOO) -RFC mit ct-0xdawir96cy7k ein.

Konfiguration Ihrer VPC-Routentabellen so, dass sie auf das AMS Multi-Account Landing Zone-Transit-Gateway verweisen:

Entscheiden Sie gemeinsam mit Ihrem Lösungsarchitekten, welchen Verkehr Sie an das AMS Multi-Account Landing Zone-Transit-Gateway senden möchten. Aktualisieren Sie Ihre VPC-Routentabellen, um Traffic an den zuvor erstellten TGW-Anhang zu senden

Holen Sie sich operative Hilfe mit Ihren vom Kunden verwalteten Konten

AMS kann Ihnen helfen, die Workloads zu verwalten, die Sie in Ihren vom Kunden verwalteten Konten bereitgestellt haben, indem das Konto in AMS Accelerate integriert wird. Mit AMS Accelerate können Sie von operativen Services wie Überwachung und Alarmierung, Incident Management, Sicherheitsmanagement und Backup-Management profitieren, ohne eine neue Migration durchführen zu müssen, Ausfallzeiten zu haben oder Ihre Nutzung zu ändern. AWS AMS Accelerate bietet auch ein optionales Patch-Add-on für EC2 basierte Workloads, die regelmäßig gepatcht werden müssen. Mit AMS Accelerate nutzen, konfigurieren und implementieren Sie weiterhin alle AWS Dienste nativ oder mit Ihren bevorzugten Tools, wie Sie es mit AMS Advanced Customer Managed Accounts tun. Sie verwenden Ihre bevorzugten Zugriffs- und Änderungsmechanismen, während AMS bewährte Methoden anwendet, die Ihnen helfen, Ihr Team zu skalieren, Kosten zu optimieren, Sicherheit und Effizienz zu erhöhen und die Ausfallsicherheit zu verbessern. Weitere Informationen finden Sie in der [Leistungsbeschreibung von Accelerate](#).

Um Ihr kundenverwaltetes Konto in Accelerate einzubinden, wenden Sie sich an Ihren CSDM und folgen Sie den Schritten unter [Erste Schritte mit AMS Accelerate](#).

Note

AMS Accelerate-Konten in AMS Advanced verfügen weder über das AMS-Änderungsmanagement (Änderungsanträge oder RFCs) noch über die AMS Advanced-Konsole. Stattdessen verfügen sie über die AMS Accelerate-Konsole und -Funktionalität.

AMS Tools-Konto (Workloads migrieren)

Ihr Konto für Landing Zone-Tools mit mehreren Konten (mit VPC) beschleunigt die Migration, verbessert Ihre Sicherheitsposition, reduziert Kosten und Komplexität und standardisiert Ihr Nutzungsmuster.

Ein Tools-Konto bietet Folgendes:

- Eine klar definierte Grenze für den Zugriff auf Replikationsinstanzen für Systemintegratoren außerhalb Ihrer Produktions-Workloads.
- Ermöglicht die Einrichtung einer isolierten Kammer, um einen Workload auf Malware oder unbekannte Netzwerkrouen zu überprüfen, bevor er einem Konto mit anderen Workloads zugeordnet wird.
- Da es sich um ein definiertes Konto handelt, bietet es eine schnellere Einarbeitung und Einrichtung für die Migration von Workloads.
- Isolierte Netzwerkrouen zur Sicherung des Datenverkehrs vor Ort -> -> Tools-Konto CloudEndure -> AMS-aufgenommenes Image. Sobald ein Image aufgenommen wurde, können Sie es über einen AMS Management | Advanced Stack Components | AMI | Share (ct-1eiczxw8ihc18) -RFC für das Zielkonto freigeben.

Übergeordnetes Architekturdiagramm:

Verwenden Sie den Änderungstyp Deployment | Managed landing zone | Management account | Tools account (with VPC) erstellen (ct-2j7q1hgf26x5c), um schnell ein Tools-Konto bereitzustellen und einen Workload Ingestion-Prozess in einer Multi-Account-Landingzone-Umgebung zu instanziiieren. Siehe [Verwaltungskonto, Tools-Konto: Erstellen \(mit VPC\)](#).

 Note

Wir empfehlen, zwei Verfügbarkeitszonen (AZs) einzurichten, da es sich um einen Migrationshub handelt.

Standardmäßig erstellt AMS die folgenden zwei Sicherheitsgruppen (SGs) in jedem Konto. Vergewissern Sie sich, dass diese beiden vorhanden SGs sind. Wenn sie nicht vorhanden sind, öffnen Sie bitte eine neue Serviceanfrage beim AMS-Team, um sie anzufordern.

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

Stellen Sie sicher, dass CloudEndure Replikationsinstanzen im privaten Subnetz erstellt werden, in dem es Routen zurück zum Standort gibt. Sie können dies überprüfen, indem Sie sicherstellen, dass die Routing-Tabellen für das private Subnetz über eine Standardroute zurück zu TGW verfügen. Bei einem CloudEndure Computer-Cutover sollte jedoch das „isolierte“ private Subnetz verwendet werden, in dem es keine Route zurück zum lokalen Standort gibt, sondern nur ausgehender Internetverkehr zulässig ist. Es ist wichtig sicherzustellen, dass die Umstellung im isolierten Subnetz erfolgt, um mögliche Probleme mit den Ressourcen vor Ort zu vermeiden.

Voraussetzungen:

1. Entweder Plus - oder Premium-Supportstufe.
2. Das Anwendungskonto IDs für den KMS-Schlüssel, auf dem AMIs sie bereitgestellt werden.
3. Das Tools-Konto, das wie zuvor beschrieben erstellt wurde.

AWS Service zur Anwendungsmigration (AWS MGN)

AWS Der [Application Migration Service](#) (AWS MGN) kann in Ihrem MALZ Tools-Konto über die `AWSToolsServicesMigrationRole` IAM-Rolle verwendet werden, die bei der Bereitstellung des Tools-Kontos automatisch erstellt wird. [Sie können AWS MGN verwenden, um Anwendungen und Datenbanken zu migrieren, die auf unterstützten Versionen von Windows- und Linux-Betriebssystemen laufen.](#)

Die meisten up-to-date Informationen zum AWS-Region Support finden Sie in der [Liste der AWS regionalen Dienste](#).

Falls Ihr bevorzugtes AWS-Region Produkt derzeit nicht von AWS MGN unterstützt wird oder das Betriebssystem, auf dem Ihre Anwendungen ausgeführt werden, derzeit nicht von AWS MGN unterstützt wird, sollten Sie in Erwägung ziehen, stattdessen die [CloudEndure Migration](#) in Ihrem Tools-Konto zu verwenden.

Beantragen Sie die MGN-Initialisierung AWS

AWS MGN muss vor der ersten Verwendung von AMS [initialisiert](#) werden. Um dies für ein neues Tools-Konto zu beantragen, reichen Sie einen RFC Management | Other | Other aus dem Tools-Konto mit den folgenden Angaben ein:

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

https://console.aws.amazon.com/mgn/home?region=MALZ\_PRIMARY\_REGION#/welcome using
all default values
to 'Create template' and complete the initialization process.
```

Sobald AMS den RFC erfolgreich abgeschlossen und AWS MGN in Ihrem Tools-Konto initialisiert hat, können Sie die Standardvorlage `AWSManagedServicesMigrationRole` für Ihre Anforderungen bearbeiten.

Zugriff auf das neue AMS Tools-Konto aktivieren

Sobald das Tools-Konto erstellt wurde, stellt AMS Ihnen eine Konto-ID zur Verfügung. Ihr nächster Schritt besteht darin, den Zugriff auf das neue Konto zu konfigurieren. Dazu gehen Sie wie folgt vor:

1. Aktualisieren Sie die entsprechenden Active Directory-Gruppen auf das entsprechende Konto IDs.

Neuen, von AMS erstellten Konten wird die `ReadOnly` Rollenrichtlinie sowie eine Rolle zugewiesen, über die Benutzer Dateien ablegen können. RFCs

Für das Tools-Konto stehen außerdem eine zusätzliche IAM-Rolle und ein zusätzlicher Benutzer zur Verfügung:

- IAM-Rolle: `AWSManagedServicesMigrationRole`
- IAM-Benutzer: `customer_cloud_endure_user`

2. Fordern Sie Richtlinien und Rollen an, damit die Mitglieder des Serviceintegrationsteams Tools der nächsten Generation einrichten können.

Navigieren Sie zur AMS-Konsole und legen Sie Folgendes ab RFCs:

- a. KMS-Schlüssel erstellen. Verwenden Sie entweder [KMS-Schlüssel erstellen \(auto\)](#) oder [KMS-Schlüssel erstellen \(Überprüfung erforderlich\)](#).

Wenn Sie KMS zum Verschlüsseln aufgenommener Ressourcen verwenden, bietet die Verwendung eines einzigen KMS-Schlüssels, der mit den übrigen Landingzone-Anwendungskonten für mehrere Konten gemeinsam genutzt wird, Sicherheit für aufgenommene Bilder, sodass sie im Zielkonto entschlüsselt werden können.

- b. Teilen Sie den KMS-Schlüssel.

Verwenden Sie den Änderungstyp Verwaltung | Erweiterte Stack-Komponenten | KMS-Schlüssel | Teilen (Überprüfung erforderlich) (ct-05yb337abq3x5), um anzufordern, dass der neue KMS-Schlüssel für Ihre Anwendungskonten freigegeben wird, in denen die Daten gespeichert werden. AMIs

Beispielgrafik einer endgültigen Kontoeinrichtung:

Beispiel für eine vorab genehmigte IAM-Richtlinie von CloudEndure AMS

Um eine vorab von AMS genehmigte CloudEndure IAM-Richtlinie einzusehen:

Entpacken Sie die [WIGS Cloud Endure Landing Zone-Beispieldatei](#) und öffnen Sie die. `customer_cloud_endure_policy.json`

Testen der Konnektivität und end-to-end Einrichtung des AMS Tools-Kontos

1. Beginnen Sie mit der Konfiguration CloudEndure und Installation des CloudEndure Agenten auf einem Server, der auf AMS repliziert wird.
2. Erstellen Sie ein Projekt in CloudEndure.
3. Geben Sie die AWS Anmeldeinformationen ein, die Sie bei der Erfüllung der Voraussetzungen über den Secrets Manager gemeinsam genutzt haben.
4. In den Replikationseinstellungen:
 - a. Wählen Sie für die Option Wählen Sie die Sicherheitsgruppen aus, die auf die Replikationsserver angewendet werden sollen, beide AMS- „Sentinel“ -Sicherheitsgruppen (Nur privat und EgressAll) aus.

- b. Definieren Sie Umtauschoptionen für die Maschinen (Instanzen). Weitere Informationen finden Sie in [Schritt 5. Überschneiden](#)
 - c. Subnetz: Privates Subnetz.
5. Sicherheitsgruppe:
- a. Wählen Sie beide AMS-Sicherheitsgruppen „Sentinel“ aus (Nur privat und EgressAll).
 - b. Cutover-Instanzen müssen mit dem von AMS verwalteten Active Directory (MAD) und mit öffentlichen Endpunkten kommunizieren: AWS
 - i. Elastische IP: Keine
 - ii. Öffentliche IP: nein
 - iii. IAM-Rolle: customer-mc-ec 2-Instanzen-Profil
 - c. Legen Sie Tags gemäß Ihrer internen Tagging-Konvention fest.
6. Installieren Sie den CloudEndure Agenten auf dem Computer und suchen Sie in der EC2 Konsole nach der Replikationsinstanz, die in Ihrem AMS-Konto angezeigt werden soll.

Der AMS-Aufnahmeprozess:

AMS Tools Kontohygiene

Sie sollten aufräumen, nachdem Sie mit dem Konto fertig sind, das AMI gemeinsam genutzt haben und die replizierten Instances nicht mehr benötigen:

- Nach der Inanspruchnahme der WIGs Instance:
 - Cutover-Instance: Stoppen oder beenden Sie diese Instanz mindestens, nachdem die Arbeit abgeschlossen ist, über die AWS-Konsole
 - AMI-Backups vor der Ingestion: Wird entfernt, sobald die Instance aufgenommen und die On-Premise-Instance beendet wurde
 - AMS-Ingested Instances: Schalten Sie den Stack aus oder beenden Sie ihn, sobald das AMI gemeinsam genutzt wurde
 - AMS-Ingested AMIs: Wird gelöscht, sobald die gemeinsame Nutzung mit dem Zielkonto abgeschlossen ist
- Bereinigung am Ende der Migration: Dokumentieren Sie die Ressourcen, die im Entwicklermodus bereitgestellt wurden, um sicherzustellen, dass die Bereinigung regelmäßig erfolgt, zum Beispiel:
 - Sicherheitsgruppen

- Ressourcen, die über Cloud-Formation erstellt wurden
- Netzwerk ACK
- Subnetz
- VPC
- Routing-Tabelle
- Rollen
- Benutzer und Konten

Migration im großen Maßstab - Migration Factory

Weitere Informationen finden Sie unter [Einführung in die AWS CloudEndure Migration Factory-Lösung](#).

SALZ Netzwerkarchitektur

Das folgende Diagramm zeigt das VPC-Netzwerklayout von AWS Managed Services (AMS) für Einzelkonten (SALZ) und ist ein Beispiel für die Einrichtung mit hoher Verfügbarkeit.

AMS konfiguriert alle Netzwerkaspekte für Sie auf der Grundlage unserer Standardvorlagen und Ihrer ausgewählten Optionen, die Sie beim Onboarding ausgewählt haben. Ein standardmäßiges AWS-Netzwerkdesign wird auf Ihr AWS-Konto angewendet, und eine virtuelle private Cloud (VPC) wird für Sie erstellt und entweder über VPN oder Direct Connect mit AMS verbunden. Erfahren Sie mehr über Direct Connect bei [AWS Direct Connect](#). Zum Standard VPCs gehören die DMZ, Shared Services und ein Anwendungssubnetz. Während des Onboarding-Prozesses VPCs können zusätzliche Informationen angefordert und erstellt werden, die Ihren Anforderungen entsprechen (z. B. Kundenabteilungen, Partner). Nach dem Onboarding erhalten Sie ein Netzwerkdiagramm, ein Umgebungsdokument, in dem erklärt wird, wie Ihr Netzwerk eingerichtet wurde.

Note

Informationen zu den standardmäßigen Service-Limits und Einschränkungen für alle aktiven Services finden Sie in der Dokumentation zu [AWS-Servicelimits](#).

Unser Netzwerkdesign basiert auf dem „[Prinzip der geringsten Rechte](#)“ von Amazon. Um dies zu erreichen, leiten wir den gesamten eingehenden und ausgehenden Datenverkehr über Gateways weiter, mit Ausnahme des Datenverkehrs, der von einem vertrauenswürdigen Netzwerk stammt. Das einzige vertrauenswürdige Netzwerk ist das, das zwischen Ihrer lokalen Umgebung und der VPC mithilfe and/or eines VPN und AWS Direct Connect (DX) konfiguriert wurde. Der Zugriff wird durch die Verwendung von Bastion-Instances gewährt, wodurch ein direkter Zugriff auf Produktionsressourcen verhindert wird. Alle Ihre Anwendungen und Ressourcen befinden sich in privaten Subnetzen, die über öffentliche Load Balancer erreichbar sind. Öffentlicher Ausgangsverkehr fließt über unsere Forward-Proxys zum Internet Gateway und dann zum Internet. Alternativ kann der Datenverkehr über Ihr VPN oder Direct Connect in Ihre lokale Umgebung fließen.

AMS landing zone Shared Services mit einem Konto

Shared Services-Subnetze enthalten AMS Directory Services, den Management-Host, der die Bereitstellung und allgemeine Aufgaben automatisiert, den Antivirus (TrendMicro) -Management-Server und interne Bastion-Hosts:

- AMS Directory Services = AD-Domänencontroller

Erstellt ein Active Directory in AMS-Konten, erstellt die AMS-Domäne und verbindet verwaltete Stacks beim Start mit der Domäne.

- Management-Hosts = AMS Management Host (automatische Bereitstellung und allgemeine Aufgaben)

Fungiert als API-Endpunkt Directory Service, um Directory Service Domänencontroller zu modifizieren und mit ihnen zu interagieren.

- Sicherheitsdienste: Antivirus (TrendMicro) -Managementserver = EPS DSM + EPS Relay

Nutzt die Trend Micro™ Deep Security Software (DSM), arbeitet in einem Client-Server-Modell und verfügt über eine Back-End-Datenbank mit Deep Security Managern, -Agenten und Relays.

- Interne Bastion-Hosts = Bastionen der Kunden

Spezialserver, die als primärer Zugriffspunkt für das Internet konzipiert sind und als Proxy für Ihre anderen EC2 Amazon-Instances fungieren.

AMS einrichten

Themen

- [AMS-StandardEinstellungen verstehen](#)
- [Verwendung der AMS-Konsolen](#)
- [Verwenden der AMS-API und CLI](#)
- [AMS bring dein eigenes EPS mit](#)
- [Empfangen von AMS-Benachrichtigungen](#)
- [Privates und öffentliches DNS einrichten](#)
- [Verwaltung des Ausgangsverkehrs mit AMS](#)
- [Bereitstellung von IAM-Ressourcen in AMS Advanced](#)
- [Berechtigungen in AMS mit IAM-Rollen und -Profilen einrichten](#)
- [AD FS-Anspruchsregel und SAML-Einstellungen](#)
- [Mit Netzwerk-ACL einschränken](#)
- [AMS auf Outposts](#)
- [Verwenden von Tags in AMS](#)
- [Ressourcenplaner für AWS Managed Services](#)
- [AWS Systems Manager in AMS Advanced](#)
- [Offboard-AMS-Konten](#)

Einige AMS-Setup-Aufgaben können beim Onboarding abgeschlossen werden.

Eine vollständige Beschreibung der Rollen und Zuständigkeiten, einschließlich des AMS [Unterstützte AWS Dienste](#), finden Sie unter [AMS-Verantwortungsmatrix \(RACI\)](#).

Note

Um AMS mit der Bereitstellung eines zusätzlichen AWS Dienstes zu beauftragen, reichen Sie eine Serviceanfrage ein. Informationen darüber, wie Sie diese Anfrage stellen können, finden Sie unter [Verwaltung von Serviceanfragen](#).

AMS-StandardEinstellungen verstehen

Ihr AWS Managed Services (AMS) -Netzwerk hat eine standardisierte Konfiguration mit Standardeinstellungen für die meisten Services.

In diesem Abschnitt werden die Standardeinstellungen beschrieben, die AMS für Zugriff, Überwachung, Protokollierung und Verwaltung verwendet.

Ein Beispiel für Infrastrukturkosten für eine landing zone mit mehreren Konten oder für eine landing zone mit einem Konto finden Sie unter. [Grundkomponenten der AMS-Umgebung](#)

Themen

- [Standardeinstellungen für die DNS-Auflösung \(MALZ\)](#)
- [EC2 IAM-Instanzprofil](#)
- [Warnmeldungen aus der Basisüberwachung in AMS](#)
- [Standardeinstellungen für die Aufbewahrung und Rotation von Protokollen](#)

Standardeinstellungen für die DNS-Auflösung (MALZ)

AWS Managed Services (AMS) -Landing landing zone für mehrere Konten: In AWS-Umgebungen kann die DNS-Auflösung (Domain Name System) zwischen Route 53 Resolver und DNS-Resolvern in einer VPC integriert werden, indem Resolver-Weiterleitungsregeln konfiguriert werden. Bevor diese Regeln für die Weiterleitung von DNS-Abfragen verwendet werden können, müssen Resolver-Endpunkte für eingehende und ausgehende Anfragen eingerichtet werden, an die diese Anfragen weitergeleitet werden können.

Standardmäßig werden DNS-Abfragen innerhalb des Anwendungskontos VPCs in den Einstellungen für mehrere Konten in AMS an die bedingten Weiterleitungen der Domäne AWS Directory Service for Microsoft Active Directory (auch bekannt als Managed AD) weitergeleitet, die im Shared Services-Konto vorhanden sind. AMS ermöglicht es Ihnen optional, das AmazonProvided DNS zu verwenden, z. B. AmazonProvided DNS, um DNS-Anfragen weiterzuleiten. Auf diese Weise können Sie VPC-Endpunkte nutzen, die derzeit nur von Amazon bereitgestelltes DNS über Amazon Route 53 unterstützen. Dementsprechend werden Resolver-Regeln auch automatisch für allgemeine VPC-Endpunkte eingerichtet, die standardmäßig im Shared Services-Konto bereitgestellt werden. Weitere Informationen zu diesen gängigen VPC-Endpunkten finden Sie unter. [AMS VPC-Endpunkte](#)

Um DHCP-Optionssätze (Dynamic Host Configuration Protocol) in Ihrem gesamten Anwendungskonto so VPCs zu konfigurieren, dass von Amazon bereitgestelltes DNS für VPC-

Endpunkte verwendet wird und Route53-Resolver-Regeln auf die gemeinsamen VPC-Endpunkte in Ihren Shared Services-Konten verweisen (mit einer optionalen Resolver-Regel für lokale Domänen), erstellen Sie eine Verwaltung | Andere | Andere | Änderungsanforderung (RFC) erstellen, in der Sie das Shared Services-Konto angeben und die Aktivierung des Anwendungskontos beantragen Lokale VPC-DNS- und Route 53 53-Resolver-Regeln für VPC-Endpunkte.

EC2 IAM-Instanzprofil

Ein Instanzprofil ist ein Container für eine IAM-Rolle, den Sie verwenden können, um Rolleninformationen an eine EC2 Instance zu übergeben, wenn die Instance gestartet wird.

MALZ

Es gibt zwei AMS-Standard-Instanzprofile, `customer-mc-ec2-instance-profile` und `customer-mc-ec2-instance-profile-s3`. Diese Instanzprofile bieten die in der folgenden Tabelle beschriebenen Berechtigungen.

Beschreibungen der Richtlinien

Profil	Richtlinien
customer-mc-ec2-instance-profile	AmazonSSMManagedInstanceCore : Ermöglicht Ec2-Instances die Verwendung des SSM-Agenten.
	AMSInstanceProfileLoggingPolicy : Ermöglicht Ec2-Instances, Protokolle an S3 zu übertragen und. CloudWatch
	AMSInstanceProfileManagementPolicy : Ermöglicht Ec2-Instances das Ausführen von Startaktionen, z. B. den Beitritt zu Active Directory.
	AMSInstanceProfileMonitoringPolicy : Ermöglicht Ec2-Instances, Ergebnisse an die AMS-Überwachungsdienste zu melden.
	AMSInstanceProfilePatchPolicy : Ermöglicht Ec2-Instances den Empfang von Patches.

Profil	Richtlinien
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBYOEPSPolicy : Ermöglicht Ec2-Instances die Verwendung von AMS Bring Your Own EPS .
	AMSInstanceProfileLoggingPolicy : Ermöglicht Ec2-Instances, Logs an S3 zu übertragen und. CloudWatch
	AMSInstanceProfileManagementPolicy : Ermöglicht Ec2-Instances das Ausführen von Startaktionen, z. B. den Beitritt zu Active Directory.
	AMSInstanceProfileMonitoringPolicy : Ermöglicht Ec2-Instances, Ergebnisse an die AMS-Überwachungsdienste zu melden.
	AMSInstanceProfilePatchPolicy : Ermöglicht Ec2-Instances den Empfang von Patches.
	AMSInstanceProfileS3WritePolicy : Ermöglicht den Zugriff von Ec2-Instances read/write auf Kunden-S3-Buckets.

SALZ

Es gibt ein AMS-Standard-Instanzprofil `customer-mc-ec2-instance-profile`, das Berechtigungen gemäß der IAM-Instanzrichtlinie gewährt.

`customer_ec2_instance_profile_policy` Dieses Instanzprofil stellt die in der folgenden Tabelle beschriebenen Berechtigungen bereit. Das Profil gewährt den Anwendungen, die auf der Instanz ausgeführt werden, Berechtigungen, nicht den Benutzern, die sich bei der Instanz anmelden.

Richtlinien enthalten häufig mehrere Anweisungen, wobei jede Anweisung Berechtigungen für eine andere Gruppe von Ressourcen oder unter einer bestimmten Bedingung erteilt.

CW = CloudWatch. ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

EC2 Standardberechtigungen für das Profil einer IAM-Instanz

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Nachricht enaktionen	Sobald Sie die Details auf dieser Seite überprüfen, klicken Sie auf	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	Ermöglicht EC2 Systems Manager Manager-Messaging-Aktionen in Ihrem Konto.
Ec2 Beschreiben	Sobald Sie die Details auf dieser Seite überprüfen, klicken Sie auf	* (Alle)	Ermöglicht der Konsole, die Konfigurationsdetails eines EC2 in Ihrem Konto anzuzeigen.
Ich bin Get Role ID	Sobald Sie die Details auf dieser	GetRole	Ermöglicht EC2 das Abrufen Ihrer IAM-ID von <code>aws:iam::*:role/customer-*</code> und <code>aws:iam::*:role/customer_*</code>

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
	Seite überprüfen, haben, klicken Sie auf		
Instanz zum Hochladen von Protokollereignissen	Sobald Sie die Details auf dieser Seite überprüfen, haben, klicken Sie auf	Protokollgruppe erstellen	Ermöglicht das Erstellen von Protokollen in: <code>aws:logs:*:*:log-group:i-*</code>
		Log-Stream erstellen	Ermöglicht das Streamen von Protokollen nach: <code>aws:logs:*:*:log-group:i-*</code>
CW Für MMS	Sobald Sie die Details auf dieser Seite überprüfen, haben, klicken Sie auf	DescribeAlarms, PutMetricAlarm, PutMetricData	Ermöglicht das CloudWatch Abrufen von Alarmen in Ihrem Konto. Ermöglicht CW, einen Alarm zu erstellen oder zu aktualisieren und ihn der angegebenen Metrik zuzuordnen. Ermöglicht CW, metrische Datenpunkte in Ihrem Konto zu veröffentlichen.

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Ec2-Tags	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	CreateTags, DescribeTags,	Ermöglicht das Hinzufügen, Überschreiben und Beschreiben von Tags für die angegebenen Instanzen in Ihrem Konto.
CW-Protokolle explizit ablehnen	Deny	DescribeLogStreams, FilterLogEvents, GetLogEvents	Verbietet das Auflisten, Filtern oder Abrufen der Protokollstreams für: <code>aws:logs:*:*:log-group:/mc/*</code>
Amazon EC2 Simple Systems Manager (SSM)			
SSM-Aktionen	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Ermöglicht eine Vielzahl von SSM-Funktionen in Ihrem Konto.

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
SSM-Zugriff in S3	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadParts, ListBucketMultipartUploads	Ermöglicht dem SSM auf dem, Objekte abzurufen und EC2 zu aktualisieren und den Upload eines mehrteiligen Objekts zu beenden und die Ports und Buckets aufzulisten, die für mehrteilige Uploads verfügbar sind. <code>aws:s3:::mc-**-internal-*/aws/ssm*</code>

Amazon EC2 Simple Storage Service (S3)

Objekt in S3 abrufen	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	Get Auflisten	Ermöglicht EC2 Anwendungen, Objekte in S3-Buckets in Ihrem Konto abzurufen und aufzulisten.

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Verschlüsselter S3-Zugriff auf das Kundenprotokoll	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	PutObject	Ermöglicht EC2 Anwendungen das Aktualisieren von Objekten in <code>aws:s3:::mc-*-logs-*/encrypted/app/*</code>
Patch-Daten-Put-Objekt S3	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	PutObject	Ermöglicht EC2 Anwendungen das Hochladen von Patching-Daten in Ihre S3-Buckets unter <code>aws:s3:::awsms-a*-patch-data-*</code>

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Eigene Logs auf S3 hochladen	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	PutObject	Ermöglicht EC2 Anwendungen das Hochladen benutzerdefinierter Protokolle auf: <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>
MC-Namespaces3-Protokolle explizit verweigern	Deny	GetObject* Eingeben*	Verbietet EC2 Anwendungen das Abrufen oder Platzieren von Objekten von oder nach: <code>aws:s3:::mc-*-logs-*/encrypted/mc*</code> , <code>aws:s3:::mc-*-logs-*/mc/*</code> , <code>aws:s3:::mc-a*-logs-*/audit/*</code>
S3-Löschen ausdrücklich verweigern	Deny	* (alle)	Verbietet EC2 Anwendungen, Aktionen an Objekten durchzuführen in: <code>aws:s3:::mc-a*-logs-/*</code> , <code>aws:s3:::mc-a*-internal-/*</code> ,

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
S3-CFN-Bucket explizit ablehnen	Deny	Delete*	Verbietet EC2 Anwendungen das Löschen von Objekten aus: <code>aws:s3:::cf-templates-*</code>
List-Bucket S3 explizit ablehnen	Deny	ListBucket	Verbietet das Auflisten verschlüsselter Objekte, Audit-Log-Objekte oder reservierter Objekte (MC) von: <code>aws:s3:::mc-*-logs-*</code>

AWS Secrets Manager bei Amazon EC2

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Zugang zu Trend Cloud One Secrets	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	GetSecretValue	Ermöglicht Amazon EC2 den Zugriff auf geheime Daten für die Trend Cloud One-Migration: <pre>aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , arn:aws:secretsman ager:~::~secret:/ams/ eps/cloud-one-agent- activation-token* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- guid*</pre>

AWS Key Management Service bei Amazon EC2

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Trend Cloud One Entschlüsselungsschlüssel	Sobald Sie die Details auf dieser Seite überprüfen haben, klicken Sie auf	Decrypt	Erlauben EC2 Sie Amazon, den AWS KMS Schlüssel mit dem Aliasnamen/ams/eps/cloudone-migration zu entschlüsseln arn:aws:kms:*:*:alias/ams/eps/cloudone-migration

Wenn Sie mit den Amazon IAM-Richtlinien nicht vertraut sind, finden Sie wichtige Informationen unter [Überblick über die IAM-Richtlinien](#).

Note

Richtlinien enthalten oft mehrere Aussagen, wobei jede Erklärung Berechtigungen für eine andere Gruppe von Ressourcen oder unter einer bestimmten Bedingung erteilt.

Warnmeldungen aus der Basisüberwachung in AMS

Erfahren Sie mehr über die Standardeinstellungen für die AMS-Überwachung. Weitere Informationen finden Sie unter [Überwachung und Eventmanagement in AMS](#).

Die folgende Tabelle zeigt, was überwacht wird und welche Standardschwellenwerte für Warnmeldungen gelten. Sie können die Warnschwellenwerte mit einem RFC Management | Other | Other | Update (ct-0xdawir96cy7k) ändern, nachdem Sie festgelegt haben, welche Änderungen Sie wünschen, und das entsprechende Amazon SNS SNS-Thema abonniert haben. CloudWatch [Informationen zum Erstellen und Abonnieren von Themen finden Sie unter Ein Thema abonnieren](#). Allgemeine Informationen finden Sie unter [Amazon SNS FAQs](#). Um direkt benachrichtigt zu werden,

wenn Alarmer ihren Schwellenwert überschreiten, folgen Sie zusätzlich zum standardmäßigen Warnprozess von AMS diesen Anweisungen zum Überschreiben von Alarmkonfigurationen.

Empfangen von Warnmeldungen, die von AMS generiert wurden

Amazon CloudWatch bietet eine erweiterte Aufbewahrung von Metriken. Weitere Informationen finden Sie unter [CloudWatch Limits](#).

Note

AMS kalibriert seine Basisüberwachung regelmäßig. Neue Konten werden immer mit der neuesten Basisüberwachung aufgenommen, und in der Tabelle wird die Basisüberwachung für ein neu eingeführtes Konto beschrieben. AMS aktualisiert die Basisüberwachung für bestehende Konten in regelmäßigen Abständen, und es kann vorkommen, dass es zu einer gewissen Verzögerung kommt, bis die Aktualisierungen verfügbar sind. Weitere Informationen finden Sie unter [Die Überwachungskonfiguration für ein AMS-Konto anzeigen](#).

Note

Die EC2 Instanzwarnung Non-root volume usage ist standardmäßig DEAKTIVIERT. [Wenn Sie die Generierung von Warnungen auf der Grundlage dieses Alarms benötigen, müssen Sie mithilfe des RFC-Änderungstyps ct-0erkoad6uyvvg aktivieren](#)

Warnmeldungen aus der Basisüberwachung

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise

Bei Warnmeldungen mit Sternchen (*) bewertet AMS proaktiv die Auswirkungen und behebt sie, wenn möglich. Wenn eine Behebung nicht möglich ist, erstellt AMS einen Vorfall. Wenn die Automatisierung das Problem nicht behebt, informiert AMS Sie über den Vorfall und ein AMS-Techniker wird hinzugezogen. Darüber hinaus können diese Benachrichtigungen direkt an Ihre E-Mail-Adresse gesendet werden (sofern Sie sich für das Direct-Customer-Alerts SNS-Thema entschieden haben).

Application Load Balancer	Nein	RejectedConnectionCount	CloudWatch Alarm, wenn die Anzahl der Verbindungen zurückgewiesen wurde, weil der

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
(ALB) - Instanz		Summe > 0 für 1 Minute, 5 aufeinanderfolgende Male.	Load Balancer sein Maximum erreicht hat.
Ziel des Application Load Balancer (ALB)	Nein	TargetConnectionErrorCount Summe > 0 für 1 Minute, 5 aufeinanderfolgende Male.	CloudWatch Alarm, wenn die Anzahl der Verbindungen zwischen dem Load Balancer und den registrierten Instances nicht erfolgreich hergestellt wurde.
EC2 Amazon-Instanz — Windows	Nein	SecureChannelFailure > 0,0 für 10 der letzten 15 Datenpunkte.	CloudWatch Alarm auf Windows-Instanzen, um zu warnen, wenn Secure a Channel-Verbindung fehlgeschlagen ist.
Aurora-Instanz	Nein	CPUUtilization > 85% für 5 Minuten, 2 Mal hintereinander.	CloudWatch Alarm.
AWS Backup	Ja	DeleteRecoveryPoint Ein unerwarteter IAM-Rollenprinzipal oder ein IAM-Benutzerprinzipal hat einen AWS Backup Wiederherstellungspunkt gelöscht.	CloudWatch Ereignis. Wird ausgelöst, wenn ein Backup-Wiederherstellungspunkt gelöscht wird.
AWS Outposts	Ja	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% für 5 Minuten, 12 Mal hintereinander.	CloudWatch Alarm bei Verfügbarkeit der AWS Outposts Ressource durch die Instance-Familie.

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise
		AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% für 5 Minuten, 12 aufeinanderfolgende Male.	CloudWatch Alarm bei Kapazitätsverfügbarkeit der AWS Outposts Ressource vom Instanztyp.
		AMSOupostsConnectedStatusC onnectedStatus < 1 für 5 Minuten, 1 Mal hintereinander.	CloudWatch Alarm bei AWS Outposts Service Link-Verbindung, weniger als 1 Zählung ist beeinträchtigt.
		AMSOupostsCapacityExceptionCapacityExceptions 0 für 5 Minuten, 1 Mal hintereinander.	CloudWatch Alarm bei Fehlern mit unzureichender Kapazität, z. B. bei AWS Outposts Starts für eine Ressource.
EC2 Instanz - alles OSs	Nein	CPUUtilization* >= 95% für 5 Minuten, 6 aufeinanderfolgende Male.	CloudWatch Alarm. Eine hohe CPU-Auslastung ist ein Indikator für eine Änderung des Anwendungsstatus, z. B. Deadlocks, Endlosschleifen, böswillige Angriffe und andere Anomalien.
		StatusCheckFailed > 0 für 5 Minuten, dreimal hintereinander.	CloudWatch Alarm.
		Nutzung des Root-Volumes >= 95% für 5 Minuten, 6 Mal hintereinander.	

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise
EC2 Amazon-Instanz — Linux		Nutzung von Volumes ohne Root-Rechte > 85% für 5 Minuten, 2 Mal hintereinander. Standardmäßig deaktiviert; weitere Informationen finden Sie unter https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		Freier Speicher * MemoryFree < 5% für 5 Minuten, 6 Mal hintereinander.	
	Ja	EPS-Malware Auf der Instanz wurde Malware gefunden.	CloudWatch Ereignis.
	Nein	Inode-Nutzung des Root-Volumes Durchschnittlich >= 95% für 5 Minuten, 6 aufeinanderfolgende Male. Kostenlos tauschen * Speicheraustausch < 5% für 5 Minuten, 6 Mal hintereinander.	CloudWatch Alarm. Gilt nur für Linux-Instances.

Service	Sicherheitstwarnung	Name der Warnung und Auslösebedingung	Hinweise
ElastiCache Cluster	Nein	CurrConnections = 65000	Dieser Alarm informiert AMS über das maximale Verbindungslimit eines ElastiCache Hosts. CloudWatch Alarm. Wenn Sie diesen Schwellenwert aktualisieren möchten, wenden Sie sich an den AMS-Support.

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise
ElastiCache Knoten	Nein	CPUUtilization Durchschnitt > vordefinierter Wert für 15 Minuten, 2 aufeinanderfolgende Male.	CloudWatch Alarm. Die Standardeinstellung ist 90. Bei Redis verwenden Sie je nach Instanztyp einen der folgenden Werte: • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22,5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11,25% • cache.c1.xlarge: 11,25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22,5% • cache.m3.2xgroß: 11,25% • cache.r3.large: 45% • cache.r3.xlarge: 22,5% • cache.r3.2xlarge: 11,25% • cache.r3.4xgroß: 5,62% • cache.r3.8xgroß: 2.8125%

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
ElastiCache Knoten — Memcached	Nein	SwapUsage maximal > 50.000.000 Byte für 5 Minuten, 5 aufeinanderfolgende Male.	CloudWatch Alarm. Gilt nur für Memcached.
OpenSearch Cluster	Nein	ClusterStatus.red Das Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander. AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	CloudWatch Alarm. Mindestens ein primärer Shard und dessen Replikate sind keinem Knoten zugewiesen. Weitere Informationen finden Sie unter Status des roten Clusters .
OpenSearch Domäne	Nein	KMSKeyFehler >= 1 für 1 Minute, 1 Mal hintereinander.	CloudWatch Alarm. Der KMS-Verschlüsselungsschlüssel für die Verschlüsselung gespeicherter Daten in Ihrer Domäne ist deaktiviert. Reaktivieren Sie es, um den normalen Betrieb wiederherzustellen. Weitere Informationen finden Sie unter Verschlüsselung ruhender Daten für OpenSearch Service .
		ClusterStatus. gelb Das Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Mindestens ein Replikat-Shard ist nicht einem Knoten zugewiesen. Weitere Informationen finden Sie unter Gelber Clusterstatus .

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		FreeStorageSpace Der Mindestwert ist ≤ 20480 für 1 Minute, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Ein Knoten in Ihrem Cluster hat nur noch 20 GiB freien Speicherplatz. Weitere Informationen finden Sie unter Mangel an verfügbarem Speicherplatz.
		ClusterIndexWritesBlocked ≥ 1 für 5 Minuten, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu reduzieren, wenn diese Warnung ausgelöst wird.	Der Cluster blockiert Schreib Anforderungen. Weitere Informationen finden Sie unter ClusterBlockException.
		Knoten Der Mindestwert ist $< x$ für 1 Tag, 1 aufeinanderfolgende Zeit AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	x ist die Anzahl der Knoten in Ihrem Cluster. Dieser Alarm gibt an, dass mindestens ein Knoten in Ihrem Cluster für einen Tag nicht erreichbar war. Weitere Informationen finden Sie unter Fehlgeschlagene Clusterknoten.

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise
		CPUUtilization Der Durchschnitt liegt bei $\geq 80\%$ für 15 Minuten, dreimal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Eine 100-prozentige CPU-Auslastung ist üblich, aber dauerhaft hohe Durchschnittswerte sind problematisch. Ziehen Sie die Verwendung von größeren Instance-Typen oder das Hinzufügen von Instances in Betracht.
		JVMMemoryDruck Der Höchstwert liegt bei $\geq 80\%$ für 5 Minuten, dreimal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Der Cluster könnte Fehler aufgrund von unzureichendem Speicherplatz erhalten, wenn die Nutzung zunimmt. Ziehen Sie eine vertikale Skalierung in Betracht. Amazon ES verwendet die Hälfte des RAM einer Instance für den Java-Heap, bis zu einer Heap-Größe von 32 GiB. Sie können Instances bis zu 64 GiB RAM vertikal skalieren. Dann können Sie eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		Meister CPUUtilization Der Durchschnitt liegt bei $\geq 50\%$ für 15 Minuten, dreimal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Erwägen Sie die Verwendung größerer Instance-Typen für Ihre dedizierten Master-Knoten. Aufgrund ihrer Rolle bei der Clusterstabilität und blue/green -bereitstellung sollten dedizierte Masterknoten eine geringere durchschnittliche CPU-Auslastung aufweisen als Datenknoten.
		Meistern JVMMemory Sie den Druck Der Höchstwert liegt bei $\geq 80\%$ für 15 Minuten, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Erwägen Sie die Verwendung größerer Instance-Typen für Ihre dedizierten Master-Knoten. Aufgrund ihrer Rolle bei der Clusterstabilität und blue/green -bereitstellung sollten dedizierte Masterknoten eine geringere durchschnittliche CPU-Auslastung aufweisen als Datenknoten.
OpenSearch Instanz	Nein	AutomatedSnapshotFailure Das Maximum ist ≥ 1 für 1 Minute, 1 Mal hintereinander.	CloudWatch Alarm. Ein automatisierter Snapshot ist fehlgeschlagen. Dieser Fehler ist häufig das Ergebnis eines roten Cluster-Integritätsstatus. Siehe Status des roten Clusters.
Elastic Load Balancing Balancing-Instanz	Nein	SurgeQueueLength > 100 für 1 Minute, 15 aufeinanderfolgende Male.	CloudWatch Alarm, wenn zu viele Anfragen noch weitergeleitet werden müssen.

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise
		HTTPCode_ELB_5xx_Count Summe > 0 für 5 Minuten, 3 aufeinanderfolgende Male.	CloudWatch Alarm bei zu großer Anzahl von HTTP 5XX-Antworten, die vom Load Balancer stammen.
		SpilloverCount > 1 für 1 Minute, 15 aufeinanderfolgende Male.	CloudWatch Alarm bei zu vielen Anfragen, die abgelehnt wurden, weil die Surge-Warteschlange voll ist.
GuardDuty Dienst	Ja	Nicht zutreffend; alle Ergebnisse (Bedrohungszwecke) werden überwacht. Jeder Befund entspricht einer Warnung. Änderungen der GuardDuty Ergebnisse. Zu solchen Änderungen gehören beispielsweise neu generierte Ergebnisse oder alle nachfolgenden Vorkommen dieser vorhandenen Ergebnisse.	Die Liste der unterstützten GuardDuty Befundtypen befindet sich unter GuardDuty Aktive Findingtypen .
Gesundheitsswesen	Variiert	AWS Health Dashboard	Benachrichtigungen werden gesendet, wenn sich der Status von AWS Health Dashboard (AWS Health) -Ereignissen in Bezug auf die von AMS unterstützten Basisdienste ändert. Weitere Informationen finden Sie unter Unterstützte Dienste .

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
AWS Managed Microsoft AD	Nein	Active Directory-Status AWS Managed Microsoft AD Die Instanz sendet ein aktives Statusereignis.	Serviceereignis. Wird ausgegeben, wenn das Verzeichnis nach einem Ereignis normal funktioniert.
		Beeinträchtigter Verzeichnisstatus AWS Managed Microsoft AD Die Instanz sendet ein Ereignis mit dem Status eines beeinträchtigten Verzeichnisses.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis in einem heruntergestuften Zustand ausgeführt wird. Mindestens ein Problem wurde erkannt und vermutlich wird nicht bei allen Verzeichnismvorgängen die volle Leistungskapazität erreicht.
		Status des Verzeichnisses nicht funktionsfähig AWS Managed Microsoft AD Die Instanz sendet ein Statusereignis, das nicht funktioniert.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis nicht funktioniert. Alle Verzeichnispunkte haben Probleme gemeldet.
		Der Verzeichnisstatus wird gelöscht AWS Managed Microsoft AD Die Instanz sendet ein Ereignis zum Löschen des Verzeichnisstatus.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis gerade gelöscht wird.
		Verzeichnisstatus fehlgeschlagen AWS Managed Microsoft AD Die Instanz sendet ein fehlgeschlagenes Statusereignis.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis nicht erstellt werden konnte.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		RestoreFailed Status des Verzeichnisses AWS Managed Microsoft AD Die Instanz sendet ein Ereignis zum Status eines Verzeichnisses, bei dem die Wiederherstellung fehlgeschlagen ist.	Dienstereignis. Wird ausgegeben, wenn das Wiederherstellen des Verzeichnisses aus einem Snapshot fehlgeschlagen ist.
Amazon RDS-Instanz	Nein	Die Warnung „Niedriger Speicherplatz“ wird ausgelöst, wenn der zugewiesene Speicherplatz für die DB-Instance erschöpft ist.	RDS-EVENT-0007, Einzelheiten finden Sie unter Verwenden der Amazon RDS-Ereignisbenachrichtigung .
		DB-Instance schlägt fehl Die DB-Instance ist aufgrund einer inkompatiblen Konfiguration oder eines zugrunde liegenden Speicherproblems ausgefallen. Starten Sie a point-in-time-restore für die DB-Instance.	Serviceereignis. RDS-EVENT-0031, Amazon RDS-Ereigniskategorien und Ereignismeldungen .
		Es wurde kein Failover versucht Amazon RDS führt das angeforderte Failover nicht aus, da erst vor Kurzem ein Failover auf dieser DB-Instance erfolgt ist.	Serviceereignis. RDS-EVENT-0034, Amazon RDS-Ereigniskategorien und Ereignismeldungen .

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		Ungültige Parameter der DB-Instance Beispielsweise konnte MySQL nicht gestartet werden, weil ein speicherbezogener Parameter für diese Instance-Klasse zu hoch gesetzt ist. Die Kundenaktion würde also darin bestehen, den Speicherparameter zu ändern und die DB-Instance neu zu starten.	Serviceereignis. RDS-EVENT-0035, Amazon RDS-Ereigniskategorien und Ereignismeldungen .
		Ungültige IDs Subnetz-DB-Instance Die DB-Instance befindet sich in einem inkompatiblen Netzwerk. Einige der angegebenen Subnetze IDs sind ungültig oder existieren nicht.	Dienstereignis. RDS-EVENT-0036, Amazon RDS-Ereigniskategorien und Ereignismeldungen .
		Fehler beim Lesen der Replikation der DB-Instance Bei der Read-Replikation ist ein Fehler aufgetreten. Weitere Informationen finden Sie in der Ereignismeldung. Informationen zur Behebung von Read Replica-Fehlern finden Sie unter Problembehandlung bei MySQL Read Replica-Problemen.	Serviceereignis. RDS-EVENT-0045, Amazon RDS-Ereigniskategorien und Ereignismeldungen .

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		Die Lesereplikation der DB-Instance wurde beendet Die Replikation auf der Read Replica wurde beendet.	Serviceereignis. RDS-EVENT-0057, Amazon RDS-Ereigniskategorien und Ereignismeldungen .
		Fehler beim Erstellen des Statspack-Benutzerkontos Fehler beim Erstellen des Statspack-Benutzerkontos PERFSTAT. Löschen Sie das Konto, bevor Sie die Statspack-Option hinzufügen.	Serviceereignis. RDS-EVENT-0058, Amazon RDS-Ereigniskategorien und Ereignismeldungen .
		Start der Wiederherstellung der DB-Instance Die SQL Server-DB-Instance stellt ihre Spiegelung wieder her. Die Leistung ist beeinträchtigt, bis die Spiegelung wiederhergestellt ist. Datenbank mit einem anderen Wiederherstellungsmodell als FULL gefunden. Das Wiederherstellungsmodell wurde wieder auf FULL umgestellt und die Wiederherstellung mit Spiegelung wurde gestartet. (<dbname>: <recovery model found>[,...]).	Serviceveranstaltung. RDS-EVENT-0066, Amazon RDS-Ereigniskategorien und Ereignismeldungen .
		Ein Failover für das DB-Cluster ist fehlgeschlagen.	RDS-EVENT-0069, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		S3-Bucket zur Wiederherstellung ungültiger Berechtigungen Die IAM-Rolle, die Sie zum Zugriff auf den Amazon S3-Bucket für die SQL Server-nativen Backups und Wiederherstellungen verwenden, ist falsch konfiguriert. Weitere Informationen finden Sie unter Einrichtung für systemeigenes Backup und Wiederherstellung.	Serviceereignis. RDS-EVENT-0081, Amazon RDS-Ereigniskategorien und Ereignismeldungen .
		Aurora konnte die Sicherungsdaten aus einem Amazon S3-Bucket nicht kopieren.	RDS-EVENT-0082, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		Warnung bei niedrigem Speicherplatz, wenn die DB-Instance mehr als 90% des zugewiesenen Speichers verbraucht hat	RDS-EVENT-0089, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		Benachrichtigungsdienst, wenn die Skalierung für den Aurora Serverless DB-Cluster fehlgeschlagen ist.	RDS-EVENT-0143, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		Die DB-Instance hat den Status Ungültig. Es sind keine Aktionen erforderlich. Die Auto Scaling wird später erneut versucht.	RDS-EVENT-0219, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise
		Die DB-Instance hat den Schwellenwert für den Speicher vollständig erreicht, und die Datenbank wurde heruntergefahren.	RDS-EVENT-0221, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		Dieses Ereignis weist darauf hin, dass die automatische Skalierung des RDS-Instance-Speichers nicht skaliert werden kann. Es kann mehrere Gründe geben, warum die automatische Skalierung fehlgeschlagen ist.	RDS-EVENT-0223, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		Das Auto Scaling von Speicher hat eine ausstehende Skalierungsspeicheraufgabe ausgelöst, die den maximalen Speicherschwellenwert erreichen würde.	RDS-EVENT-0224, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		Der Speichertyp der DB-Instance ist der derzeit in der Availability Zone nicht verfügbar. Die Auto Scaling wird später erneut versucht.	RDS-EVENT-0237, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		RDS konnte keine Kapazität für den Proxy bereitstellen, da in Ihren Subnetzen nicht genügend IP-Adressen verfügbar sind.	RDS-EVENT-0243, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .
		Der Speicherplatz für Ihr AWS-Konto hat das zulässige Speicherkontingent überschritten.	RDS-EVENT-0254, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen .

Service	Sicherheit	Name der Warnung und Auslösebedingung	Hinweise
		CPUUtilization Durchschnittliche CPU-Auslastung > 90% für 15 Minuten, 2 aufeinanderfolgende Male. DiskQueueDepth Die Summe ist > 75 für 1 Minute, 15 aufeinanderfolgende Male. FreeStorageSpace Durchschnitt < 1.073.741.824 Byte für 5 Minuten, 2 aufeinanderfolgende Male. SwapUsage Durchschnitt = 104.857.600 Byte für 5 Minuten, 2 aufeinanderfolgende Male.	CloudWatch Alarm.
Amazon-Redshift-Cluster	Nein	RedshiftClusterStatus Der Zustand des Clusters, wenn er sich nicht im Wartungsmodus befindet, < 1 für 5 Minuten	1 steht für einen fehlerfreien Cluster.

Service	Sicherheit tswarnung	Name der Warnung und Auslösebe dingung	Hinweise
Amazon Macie	Ja	Neu generierte Warnungen und Aktualisierungen vorhandener Warnungen. Macie stellt fest, dass sich die Ergebnisse geändert haben. Zu solchen Änderungen gehören beispielsweise neu generierte Ergebnisse oder alle nachfolgenden Vorkommen dieser vorhandenen Ergebnisse.	Amazon Macie Macie-Warnung. Eine Liste der unterstützten Macie-Warnungstypen finden Sie unter Analysieren von Amazon Macie Macie-Ergebnissen. Beachten Sie, dass Macie nicht für alle Konten aktiviert ist.

AMS ergreift proaktive Maßnahmen (Skalierung des Clusters), wenn diese Warnung ausgelöst wird.

Informationen zu Abhilfemaßnahmen finden Sie unter. [Automatische AMS-Behebung von Warnmeldungen](#)

[Sehen Sie sich Andrews Video an, um mehr zu erfahren \(7:03\)](#)

Standardeinstellungen für die Aufbewahrung und Rotation von Protokollen

In diesem Abschnitt werden die Standardeinstellungen für die AMS-Protokollverwaltung beschrieben. Weitere Informationen finden Sie unter [Protokollverwaltung](#).

- Rotation = Protokollwechsel innerhalb der Instanzen
- Aufbewahrung = Zeitraum, in dem wir die Protokolle in Amazon CloudWatch Logs und Amazon Simple Storage Service (S3) aufbewahren

Die Protokolle werden nach Bedarf in CloudWatch Logs (Sie können dies konfigurieren) und in S3 aufbewahrt. Sie laufen nicht ab und werden nicht gelöscht und unterliegen der Lebensdauer des Dienstes. Detaillierte Informationen zur Haltbarkeit von S3 finden Sie unter [Datenschutz in Amazon S3](#).

Sie können eine Änderung der Protokollspeicherung für alle Protokolle beantragen, mit Ausnahme von AWS CloudTrail Protokollen, die aus Prüfungs- und Sicherheitsgründen auf unbestimmte Zeit aufbewahrt werden.

Die Protokollrotation wird innerhalb der Instanzen konfiguriert. Standardmäßig rotieren Betriebssystem- und Sicherheitsprotokolle stündlich, wenn sie mehr als 100 MB erreichen. Dadurch wird sichergestellt, dass Sie in den Instanzen nicht zu wenig Speicherplatz haben.

Der Log-Agent innerhalb der Instances lädt das Protokoll online in CloudWatch Logs hoch. Von dort aus werden die Logs in S3 archiviert.

Die Protokolle werden in CloudWatch Logs und S3 im Rohformat gespeichert, in dem sie generiert wurden. Es findet keine Vorverarbeitung statt.

Verwendung der AMS-Konsolen

Die AMS-Konsolen in der AWS Management Console stehen Ihnen zur Verfügung, um mit AMS zu interagieren und Ihre von AMS Advanced-verwalteten Ressourcen und AMS Accelerate-Ressourcen zu bedienen. Die AMS-Konsolen verhalten sich im Allgemeinen wie jede andere AWS Konsole. Da AMS jedoch eine private Organisation ist, können nur Konten, die für AMS aktiviert sind, auf die Konsole zugreifen. Sobald AMS in Ihrem Konto aktiviert ist, können Sie auf die Konsole zugreifen, indem Sie in der einheitlichen Suchleiste nach „Managed Services“ suchen.

Note

Abhängig von Ihrer Kontorolle greifen Sie auf die AMS Advanced-Konsole oder die AMS Accelerate-Konsole zu.

Beachten Sie bei der Verwendung der AMS-Konsolen die folgenden Einschränkungen:

- Die AMS-Konsole ist kontospezifisch. Wenn Sie also ein „Test“-Konto für Ihre Organisation haben, können Sie im „Prod“-Konto für diese Organisation keine Ressourcen sehen. Ebenso benötigen Sie eine AMS-Advanced-Rolle, um auf die AMS Advanced-Konsole zugreifen zu können.
- Die AMS-Konsolen wenden bei der Authentifizierung eine IAM-Richtlinie an, die festlegt, auf welche Konsole Sie zugreifen können und was Sie dort tun können. Ihr Administrator kann zusätzliche Richtlinien auf die AMS-Standardrichtlinie anwenden, um einzuschränken, was Sie in der Konsole sehen und tun können.

Die AMS Advanced-Konsole bietet die folgenden Funktionen:

- Erste Seite: Die erste Seite enthält Informationsfelder und Links, die Ihnen den Zugriff auf Ihre bestehenden Vorfälle RFCs, Serviceanfragen und Berichte erleichtern.
- Feature-Seiten, Links im linken Navigationsbereich:
 - Dashboard: Bietet einen Überblick über den aktuellen Status Ihres Kontos, einschließlich:
 - Änderungsanträge: Sehen Sie, wie RFCs viele noch auf Ihre Antwort warten, und wechseln Sie zur RFC-Listenseite mit aktivem Filter. Sehen Sie sich an, wie RFCs viele noch auf Ihre Genehmigung warten, und wechseln Sie zur RFC-Listenseite mit aktivem Filter. Sehen Sie sich an, wie viele geöffnet RFCs sind, und springen Sie zur RFC-Listenseite, auf der der Filter aktiv ist. Öffnen Sie die Listenseite für, RFCs indem Sie auf den Link Alle anzeigen klicken.
 - Vorfälle: Sehen Sie, wie viele Vorfälle noch auf Ihre Antwort warten, und wechseln Sie zur Seite mit der Liste der Vorfälle, auf der der Filter aktiv ist. Sehen Sie sich an, wie viele geöffnet sind, und wechseln Sie zur Seite mit der Liste der Vorfälle, auf der der Filter aktiv ist. Öffnen Sie die Seite mit der Liste der Vorfälle, indem Sie auf den Link Alle anzeigen klicken.
 - Serviceanfragen: Sehen Sie, wie viele Serviceanfragen noch auf Ihre Antwort warten, und wechseln Sie zur Seite mit der Liste der Serviceanfragen, auf der der Filter aktiv ist. Sehen Sie sich an, wie viele geöffnet sind, und wechseln Sie zur Seite mit der Liste der Serviceanfragen, auf der der Filter aktiv ist. Öffnen Sie die Seite mit der Liste der Serviceanfragen, indem Sie auf den Link Alle anzeigen klicken.
 - Kürzlich aktualisiert RFCs: Datum, Link zu den RFC-Details und Status
 - Kürzlich erstellte Vorfälle und Serviceanfragen: Datum, Link zu den Falldetails und Typ (Vorfall oder Serviceanfrage)
 - RFCs: Öffnet eine Liste der RFCs für das Konto vorhandenen
 - Vorfälle: Öffnet eine Liste der offenen Vorfälle für das Konto
 - Serviceanfragen: Öffnet eine Liste der offenen Serviceanfragen für das Konto
 - Berichte: Öffnet die Seite „Berichte“ und die Standardberichte „Tägliches Backup“ und „Tägliches Patch“ und „Monatliche Abrechnung“
 - Ressourcen:
 - VPCs: Öffnet eine Liste der VPCs für das Konto vorhandenen
 - Stacks: Öffnet eine Liste der vorhandenen Stacks für das Konto
 - AMIs: Öffnet eine Liste verfügbarer AMS AMIs
- Funktionen im Rampenlicht: Informationen zu den neuesten Updates für die Konsole

- Ressourcen für Entwickler: Eine Seite mit herunterladbaren Dateien, darunter das AMS Advanced Change Management SDK und mehr
- Dokumentation: Die Landingpage der AWS Managed Services Services-Dokumentation

Verwenden der AMS-API und CLI

Die AWS Managed Services (AMS) -API ähnelt der APIs für andere AWS Services. Weitere Informationen zur AMS-API finden Sie in der [AMS-API-Referenz](#).

AMS-API-HTTP-Endpunkte für REST-Aufrufe

Neben den verschiedenen SDKs bietet AMS eine CLI; Sie können auch REST-API-Aufrufe für den AMS-Endpunkt aufrufen.

Es gibt zwei AMS APIs (der Endpunkt für beide befindet sich in us-east-1):

- Change Management: Verwenden Sie diese API, um Zugriff auf oder Änderungen an Ihrer Infrastruktur anzufordern. Dazu gehören das Erstellen und Aktualisieren, Bereitstellen neuer Instances RFCs, das Aktualisieren und Löschen von Instances, das Abrufen von Informationen CTs und das Erstellen von Instances. AMIs Der HTTP-Endpunkt ist:

`https://amscm.us-east-1.amazonaws.com`

- SKMS: Verwenden Sie diese API, um Informationen über Ihre Infrastruktur abzurufen VPCs, einschließlich Stacks, Subnetze und. AMIs Der HTTP-Endpunkt ist:

`https://amsskms.us-east-1.amazonaws.com`

Installation oder Aktualisierung der AMS-CLI

Die AMS-CLI ist eine einfache Möglichkeit, mit der AMS-API zu interagieren, und wird in den Beispielen in diesem Abschnitt verwendet. Die Verwendungskonventionen für die AWS CLI und AMS CLI finden Sie [unter Verwenden der AWS Befehlszeilenschnittstelle](#).

Informationen zur Installation von SAML finden Sie unter [AD FS-Anspruchsregel und SAML-Einstellungen](#).

Gehen Sie folgendermaßen vor, um die AMS-CLI zu installieren oder zu aktualisieren:

 Note

Für dieses Verfahren benötigen Sie Administratoranmeldedaten.

Die AWS-CLI ist eine Voraussetzung für die Nutzung der AWS Managed Services (AMS) CLIs (Change Management und SKMS).

1. Informationen zur Installation der AWS-CLI finden Sie unter [Installation der AWS-Befehlszeilenschnittstelle](#) und folgen Sie den entsprechenden Anweisungen. Beachten Sie, dass sich unten auf dieser Seite Anweisungen zur Verwendung verschiedener Installationsprogramme befinden: [Linux](#), [MS Windows](#), [macOS](#), [Virtual Environment](#), [Bundled Installer \(Linux, macOS oder Unix\)](#).

Führen Sie nach der Installation den Befehl aus, `aws help` um die Installation zu überprüfen.

2. Sobald die AWS-CLI installiert ist, laden Sie zur Installation oder zum Upgrade der AMS CLI entweder die AMS CLI- oder die AMS SDK-Distributionsdatei herunter und entpacken Sie sie. Sie können auf die AMS-CLI-Distributionsdateien über den Link [Developer's Resources](#) im linken Navigationsbereich der AMS-Konsole zugreifen.
3. Die README-Datei enthält Anweisungen für jede Installation.

Öffnen Sie entweder:

- CLI zip: Stellt nur die AMS-CLI bereit.
- SDK-Zip: Stellt das gesamte AMS APIs und die AMS-CLI bereit.

Führen Sie für Windows das entsprechende Installationsprogramm aus (nur 32- oder 64-Bit-Systeme):

- 32 Bit: ManagedCloudAPI_x86.msi
- 64 Bit: ManagedCloudAPI_x64.msi

Führen Sie für Mac/Linux die Datei mit dem Namen: AWSManagedServices_InstallCLI.sh aus, indem Sie diesen Befehl ausführen: `sh AWSManagedServices_InstallCLI.sh` Beachten Sie, dass sich die Verzeichnisse amscm und amsskms und ihr Inhalt im selben Verzeichnis wie die .sh-Datei befinden müssen. AWSManagedServices_InstallCLI

4. Wenn Ihre Unternehmensanmeldedaten über den Verbund mit AWS (die AMS-Standardkonfiguration) verwendet werden, müssen Sie ein Tool zur Verwaltung von Anmeldeinformationen installieren, das auf Ihren Verbundservice zugreifen kann. Sie können beispielsweise diesen AWS-Sicherheitsblog [How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS verwenden](#), um Hilfe bei der Konfiguration Ihrer Tools zur Verwaltung Ihrer Anmeldeinformationen zu erhalten.
5. Führen Sie nach der Installation die Befehle und Optionen aus `aws amscm help` und sehen Sie `aws amsskms help` sich diese an.

 Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` z. B. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

Verwenden der AMS-API in CLI, Ruby, Python und Java

Im Folgenden finden Sie eine Liste von Codefragmenten für den `ListChangeTypeClassificationSummaries` AMS-API-Vorgang in allen verfügbaren Sprachen.

Informationen zu Python, Ruby und Java SDKs finden Sie unter [Tools for Amazon Web Services](#) und scrollen Sie nach unten zum SDKs Abschnitt. Jedes SDK-Installationsprogramm enthält eine README-Datei mit zusätzlichen Codefragmenten.

Beispiel für AMS API zu CLI

Nachdem Sie die AMS-CLI installiert haben (erfordert die AWS CLI; siehe [Installation oder Aktualisierung der AMS-CLI](#)), können Sie jeden AMS-API-Vorgang ausführen, indem Sie den Aufruf neu formieren, indem Sie zuerst angeben, welche AMS-API, `aws amscm` oder `aws amsskms`, und dann der Aktion Bindestriche anstelle von Camel case zuweisen. Geben Sie abschließend Anmeldeinformationen wie SAML ein.

Weitere Informationen finden Sie unter [Verwenden der AWS Befehlszeilenschnittstelle](#).

Beispiel:

- API: `'ChangeTypeClassificationSummaries[]'.`
`[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI: `amscm list-change-type-classification-summaries`
`--query "ChangeTypeClassificationSummaries[*].`
`[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

Note

Wenn Sie sich mit SAML authentifizieren, fügen Sie `aws --profile saml` am Anfang des Befehls etwas hinzu. Zum Beispiel

```
aws --profile saml amscm list-change-type-classification-  
summaries --query "ChangeTypeClassificationSummaries[*].  
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Beispiel für AMS API zu Python

Um die AMS-API mit Python zu verwenden, installieren Sie die AMS-CLI und installieren Sie boto3. Dazu gehen Sie wie folgt vor:

1. Installieren Sie die AMS-CLI. Siehe [Installation oder Aktualisierung der AMS-CLI](#).
2. Installieren Sie boto3, das AWS SDK für Python. Weitere Informationen finden Sie in diesem Blogbeitrag [Jetzt verfügbar — AWS SDK für Python \(Boto3\)](#).

```
import boto3
```

3. Holen Sie sich den AMS Change Management-Client:

```
cm = boto3.client('amscm')
```

4. Holen Sie sich das AMS CTs:

```
cts = cm.list_change_type_classification_summaries()  
  
print(cts)
```


Python-Beispiele

Im Folgenden finden Sie einige Beispiele für die Verwendung von Python in AMS. and/or Verwenden Sie Lambda, um EC2 Instanzen zu erstellen.

Python-Beispiel zum Erstellen eines EC2

Dieses Beispiel zeigt, wie Sie die RESTful amscm-API innerhalb von Python-Code verwenden können, um RFC-Prozesse zu archivieren und auszuführen.

1. Installieren Sie die AMS-CLI an einem Ort, auf den Sie Zugriff haben. Sie benötigen die bereitgestellten Dateien.
2. Rufen Sie Python-Bibliotheken auf und erstellen Sie die EC2 Instanz:

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
```

```
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

Python-Beispiel mit Lambda

Dieses Beispiel zeigt, wie Sie die AMS-Modelle mit Ihrem Code bündeln, sodass Sie ihn mit Lambda oder anderen EC2 Orten verwenden können, die Sie nicht installieren `awscli` wollen oder können.

Note

AMS bietet kein importierbares AMS-spezifisches Python-SDK. Das `awscli` Installationsskript installiert die AMS-Dienstdatenmodelle im normalen Pfad der CLI. Für die CLI-Verwendung und die Verwendung von System-Python ist das in Ordnung, da beide `awscli` ihre Servicemodelle von denselben Standardspeicherorten (`~/.aws/models`) `boto3` lesen. Wenn Sie jedoch AMS-Dienste über `boto3` in Lambda (oder einer anderen nicht-lokalen Laufzeit) verwenden möchten, wird dies unterbrochen, da Sie nicht mehr über

die Datenmodelle verfügen. Im Folgenden finden Sie eine Methode, um dieses Problem zu beheben, indem Sie die Datenmodelle mit der Funktion verpacken.

Es gibt einfache Schritte, die Sie unternehmen können, um Ihren AMS-integrierten Python-Code in Lambda oder einer anderen Laufzeit wie Fargate EC2 usw. auszuführen. Der folgende Workflow zeigt die Schritte, die für AMS-integrierte Lambda-Funktionen erforderlich sind.

Indem Sie die Datenmodelle zum Bereitstellungspaket des Codes hinzufügen und den SDK-Suchpfad aktualisieren, können Sie ein SDK-Erlebnis simulieren.

 Important

Dieses Beispiel und alle gezeigten Befehle, die keine Python-Befehle sind, wurden auf einem Mac-Computer getestet.

Beispiel für einen Arbeitsablauf:

1. Installieren Sie die `amsccli`. Dadurch wird ein Ordner `~/ .aws/models` auf Ihrem Computer (Mac) erstellt.
2. Kopieren Sie die Modelle in ein lokales Verzeichnis: `cp ~/ .aws/models ./models`.
3. Nehmen Sie die Modelle in das Bereitstellungspaket Ihres Codes auf.
4. Aktualisieren Sie Ihren Funktionscode, um die neuen Modelle zum SDK-Pfad hinzuzufügen. Beachten Sie, dass dieser Code ausgeführt werden muss, bevor Boto3 oder Botocore importiert werden!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

 Note

Da sich die Beispielmmodelle in einem Verzeichnis mit dem Namen `models` befinden, fügen wir sie zu `_PATH` hinzu. `./models AWS_DATA` Wenn das Verzeichnis benannt wäre `/ams/boto3models`, würden wir den folgenden Code hinzufügen:

```
import os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Ihr Code sollte die AMS-Modelle erfolgreich finden. Als konkreteres Beispiel für das Verpacken finden Sie hier den Lambda-spezifischen Workflow.

Beispiel für einen AMS Lambda-Workflow:

In diesen Schritten wird das vorherige generische Beispiel auf die Erstellung einer AWS-Lambda-Funktion angewendet.

1. Installieren Sie das `Amscli`. Dadurch wird ein Ordner `~/aws/models` auf Ihrem Computer (Mac) erstellt.
2. Kopieren Sie die Modelle in ein lokales Verzeichnis:

```
cp ~/.aws/models ./models
```

3. Fügen Sie die Modelle der Deployment-ZIP-Datei Ihrer Funktion hinzu:

```
zip -r9 function.zip ./models
```

 Important

Aktualisieren Sie Ihren Funktionscode, um die neuen Modelle zum SDK-Pfad hinzuzufügen. Beachten Sie, dass dieser Code ausgeführt werden muss, bevor Boto3 oder Botocore importiert werden!

```
# Force Python to search local directory for boto3 data models
```

```
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

Da sich die Beispielmuster in einem Verzeichnis mit dem Namen `models` befinden, fügen wir sie zu `_PATH` hinzu. `./models AWS_DATA` Wenn das Verzeichnis benannt wäre `/ams/boto3models`, würden wir den folgenden Code hinzufügen:

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Stellen Sie jetzt Ihre Funktion bereit:

1. Fügen Sie Ihren Funktionscode zur Zip-Datei für die Bereitstellung hinzu (falls Sie dies noch nicht getan haben):

```
zip -g function.zip lambda-amscm-test.py
```

2. Erstellen oder aktualisieren Sie Ihre Funktion mit der von Ihnen erstellten Zip-Datei (Konsole oder CLI):

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://function.zip --region us-east-1
```

Ihr AMS-integriertes Python-Lambda sollte jetzt funktionieren.

Note

Ihre Funktion muss über IAM-Berechtigungen für verfügen, `amscm` andernfalls wird ein Berechtigungsfehler angezeigt.

Beispiel für einen Lambda-Funktionscode zum Testen von `lambda-amscm-test amscm` (Inhalt von `py`):

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

Ergebnisse testen (erfolgreich):

Antwort der Funktion:

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

Request ID:
"1cea13c0-ed46-43b1-b102-a8ea28529c27"

Funktionsprotokolle:

START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: \$LATEST

```
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',  
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-  
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':  
  'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',  
  'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}  
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

Beispiel für eine AMS-API zu Ruby

Um die AMS-API mit Ruby zu verwenden, installieren Sie das AWS Ruby-SDK und die AMS-CLI. Dazu gehen Sie wie folgt vor:

1. Installieren Sie die AMS-CLI. Siehe [Installation oder Aktualisierung der AMS-CLI](#).
2. Installieren Sie das AWS Ruby-SDK. Siehe [Tools für Amazon Web Services](#).
3. Konfigurieren Sie Ruby mit diesen Befehlen:

```
require 'aws-sdk'  
  
config = {  
  
  region: 'us-east-1',  
  
  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. Holen Sie sich das AMS CTs:

```
ams_cm = Aws::amscm::Client.new(config)  
  
cts = ams_cm.list_change_type_classification_summaries  
  
print(cts)
```

Beispiel von AMS API zu Java

Um die AMS-API mit Java zu verwenden, installieren Sie das AWS Java-SDK und die AMS-CLI. Dazu gehen Sie wie folgt vor:

1. Installieren Sie die AMS-CLI. Siehe [Installation oder Aktualisierung der AMS-CLI](#).
2. Installieren Sie das AWS Java SDK. Siehe [Tools für Amazon Web Services](#).
3. Konfigurieren Sie Java mit diesen Befehlen:

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesRequest;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResult;

public static void getChangeTypeClassificationSummaries() {
```

4. Stellen Sie die Anmeldeinformationen ein. Wir empfehlen, dass Sie dies nicht fest codieren.

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. Erstellen Sie den AMS Change Management-Client:

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

6. Holen Sie sich das AMS CTs:

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);

}
```


AMS bring dein eigenes EPS mit

Verwenden Sie die AMS-Funktion „Bring Your Own End Point Security“ (BYOEPS), um den standardmäßigen Trend Micro Deep Security Agent durch Ihre eigene Endpunkt-Sicherheitslösung oder Trend Micro Lizenz zu ersetzen. Wenn Sie bereits über kostengünstige Lizenzen für andere Produkte als Trend Micro Deep Security verfügen oder ein Team, das Ihr EPS bereitstellt, oder wenn Sie ein bestimmtes EPS-Tool verwenden möchten, verwenden Sie BYOEPS in Ihren Instanzen.

BYOEPS funktioniert auf Kontoebene. Ihre Instances im Konto verwenden entweder BYOEPS oder das standardmäßige, von AMS verwaltete EPS:

- Multi-Account-Landingzone (MALZ): Sie legen Anwendungskonten fest, die BYOEPS oder verwaltete EPS verwenden.
- Single-Account-Landing Zone (SALZ): Ihre AMS-Konten verwenden BYOEPS oder Managed EPS.

BYOEPS reduziert Ihre AWS Rechnung um die Kosten für Trend Micro Deep Security. Für EPS fallen weiterhin Kosten an, da das vom AMS verwaltete EPS weiterhin zum Schutz der vom AMS erstellten und verwalteten EC2 Instanzen benötigt wird, die für die Zugriffsverwaltung (Bastionen und Management-Hosts) erforderlich sind. Um die Gesamtkostenauswirkung zu berechnen, müssen Sie die Lizenzkosten für Ihr neues Tool und die Kosten für die Verwaltung von EPS auf den von Ihnen benötigten Service Levels berücksichtigen.

Durch den Einsatz von BYOEPS ändern sich die Rollen und Zuständigkeiten von AMS für das Sicherheitsmanagement:

- R steht für verantwortliche Partei, die die Arbeit zur Erfüllung der Aufgabe erledigt.
- C steht für konsultiert; eine Partei, deren Meinung eingeholt wird, in der Regel als Fachexperten, und mit der bilaterale Kommunikation besteht.
- I steht für informiert, d. h. eine Partei, die über den Fortschritt informiert wird, oft erst, wenn die Aufgabe oder das Ergebnis abgeschlossen ist.

Sicherheitsmanagement	Customer	AWS Managed Services
Aufrechterhaltung gültiger Lizenzen von Managed EPS	R	C

Sicherheitsmanagement	Customer	AWS Managed Services
für EC2 Instanzen von AMS Shared Services		
Konfigurieren Sie Managed EPS für EC2 Instanzen von AMS Shared Services	I	R
Aktualisieren Sie Managed EPS für EC2 Instanzen von AMS Shared Services	I	R
Überwachung von Malware auf EC2 Instanzen von AMS Shared Services	I	R
Pflege und Aktualisierung von Virensignaturen für EC2 Instanzen von AMS Shared Services	I	R
Behebung von mit Malware infizierten EC2 Instanzen für AMS Shared Services-Instanzen	C	R

Wenn Sie BYOEPS verwenden, verlieren Sie eine der von AMS angebotenen Sicherheitskontrollen. Sie verfügen weiterhin über Sicherheitsmanagement durch Tools wie Amazon GuardDuty, Amazon Macie und Prozesskontrollen wie Überprüfungen von IAM-Konfigurationen. Die Verwendung von BYOEPS hat keinen Einfluss auf AMS-Konformitätszertifizierungen und -bescheinigungen. Viele Sicherheitsrahmen und Zertifizierungen enthalten jedoch Anforderungen zum Schutz vor Malware und bösartigem Code. Um die Sicherheit und Einhaltung der Vorschriften für Ihr Konto zu gewährleisten, sollten Sie Ihre geplanten Kontrollen überprüfen, um sicherzustellen, dass sie die Sicherheitsanforderungen für die Compliance-Zertifizierungen Ihres Workloads erfüllen.

Aktivieren Sie BYOEPS für Ihr Konto

Der Vorgang zur Aktivierung von BYOEPS besteht aus drei Schritten und umfasst mehrere. RFCs Lesen Sie die folgenden Informationen, um mehr über die drei Phasen zu erfahren, die für die Aktivierung von BYOEPS erforderlich sind. Stimmen Sie sich dann mit Ihrem CSDM ab, um BYOEPS für Ihr Konto zu aktivieren.

Themen

- [Stufe 1: Voraussetzungen](#)
- [Phase 2: Aktivieren Sie BYOEPS in Ihrem Konto](#)
- [Phase 3: Instanzmigration](#)

Stufe 1: Voraussetzungen

- Das standardmäßige EC2 Amazon-Instance-Profil ist `customer-mc-ec2-instance-profile`. Wenn Sie zusätzlich zum Standardprofil ein anderes EC2 Amazon-Instance-Profil verwenden, lassen Sie die `ssm:GetParameter` Aktion für die `/ams/end-point-security` Ressource Ihrem EC2 Instance-Profil zu.

Wenn Sie EC2 Instance-Profile nicht aktualisieren können, reichen Sie einen RFC ein, der die Instance-Profile angibt, die Sie aktualisieren müssen.

- Machen Sie sich mit dem Umfang dieser Änderung vertraut.

Bereitstellungen über einen AMS Automated Change Type (CT) ermöglichen es Ihnen, das bei der Erstellung verwendete AMI anzugeben.

Um BYOEPS mit Konten zu verwenden, die AMS-verwaltetes EPS verwenden, müssen Sie mit AMS zusammenarbeiten, um die Trend Micro Agents von diesen EC2 Instances zu deinstallieren und den AMS-Code (z. B. Boot-Skripts) auf diesen Instances zu aktualisieren. Für diese Aktionen ist möglicherweise ein Neustart erforderlich. Daher empfiehlt es sich, diese Aktionen im Rahmen eines Wartungsfensters durchzuführen. Wenden Sie sich an Ihren CSDM, um ein Wartungsfenster für diese Aktivität zu ermitteln und einen Migrationsplan zu erstellen. Beachten Sie beim Migrationsplan die folgenden Fragen:

1. Wie viele Instanzen müssen Sie migrieren? Teilen Sie die Gesamtzahl der Instanzen in kleinere, inkrementelle Batches auf.

2. Wie werden Sie die Instanzen in Batches aufteilen? Sie könnten beispielsweise nach Ressourcengruppen aufteilen und eine Liste erstellen, die Sie mit dem AMS-Betriebsteam teilen können.
 3. Wie viel Zeit wird jede Charge in Anspruch nehmen? Wie viel Gesamtzeit wird benötigt? Denken Sie daran, dass Sie Ihre bevorzugten EPS-Tools möglicherweise im selben Wartungsfenster installieren möchten. Wie viel Zeit wird das in Anspruch nehmen?
- Ihr CSDM teilt den Migrationsplan mit dem AMS Operations Team. Wenn Ihre Instance-Flotte über 50 ist, arbeiten Sie mit Ihrem CSDM zusammen, um ein geplantes Ereignis mithilfe des PEM-Prozesses (Planned Event Management) zu erstellen. Weitere Informationen finden Sie unter [Verwaltung geplanter Ereignisse in AWS Managed Services](#).

AMS Operations stimmt sich mit Ihrem CSDM ab und berät Sie anhand der Anzahl der Instances RFCs in Ihrem Konto, wie Sie Ihre Daten entsprechend Ihren Wartungsfenstern einreichen können.

- Aktualisieren Sie die Automatisierungen oder Prozesse für den EC2 Instance-Start mithilfe benutzerdefinierter Funktionen oder AMS AMIs, um AMS zu verwenden, die nach Dezember AMIs 2020 veröffentlicht wurden.

Phase 2: Aktivieren Sie BYOEPS in Ihrem Konto

Wenn Sie BYOEPS in Ihrem Konto verwenden, ändern sich die Verantwortlichkeiten von AMS für das Sicherheitsmanagement. Konsultieren Sie Ihr Sicherheits- und Cloud-Plattform-Team, bevor Sie BYOEPS aktivieren.

Um BYOEPS für Ihr Konto anzufordern, reichen Sie mit ct-0xdawir96cy7k ein „MOO“-Update-RFC (Management | Other | Other | Update) mit den folgenden Angaben ein:

Please enable BYOEPS for this account/these accounts
Account IDs: *IDs for the accounts for BYOEPS.*

AMS stellt Parameterspeicher-Updates für das Konto bereit und aktualisiert das [Amazon EC2 IAM-Instance-Profil](#).

Note

- Bei Konten mit neu gestarteten Instances, die das neueste AMS verwenden, AMIs kann die Installation des Trend Micro Agents übersprungen werden. AMIs älter als Dezember 2020

unterstützen die BYOEPS-Funktion nicht. Aktualisieren Sie Automatisierungen, die alte Versionen verwenden, AMIs um das neueste AMS AMIs mit Unterstützung für BYOEPS-Funktionen zu verwenden.

- Informationen zur Handhabung vorhandener EC2 Instanzen finden Sie unter Phase 3: Instanzmigrationen

Phase 3: Instanzmigration

Verwenden Sie je nach Anwendungsfall eine der folgenden Optionen, um Ihre Instanzen zu migrieren. Wenn Sie sich nicht sicher sind, welche Option Sie wählen sollen, wenden Sie sich an Ihre CA oder CSDM.

Konten mit EC2 Instances, die von AMS verwaltetes EPS verwenden

Während des Wartungsfensters werden in Übereinstimmung mit der Planung aus Phase 1 die folgenden Aktionen für jede Instanz ausgeführt, die in BYOEPS integriert werden muss:

- Von AMS ausgeführt: Aktualisieren Sie den AMS-Code (Boot-Skripts, Module usw.) auf die neuesten Versionen. Dies ist erforderlich, da alte AMS-Bootskripte die BYOEPS-Funktion nicht unterstützen und der Trend Micro Agent bei jedem Start neu installiert wird. Deinstallieren Sie außerdem den Trend Micro Agent.
- Von Ihnen ausgeführt: Installieren und konfigurieren Sie Ihr bevorzugtes EPS-Tool.

Important

Trend Micro Agent bietet Malware-Schutz. Stellen Sie sicher, dass Sie einen geeigneten Ersatz installieren, um Ihre Instanzen zu schützen.

Um diese Änderungen vorzunehmen, geben Sie ct-2iz9nvw8zlhst, [Trend Micro DSM | Remove Trend Micro](#) EPS Agent (Überprüfung erforderlich), stapelweise ein. RFCs

EC2 Konten ohne Instances, die von AMS verwaltetes EPS verwenden

Bei Konten, bei denen neue Instances gestartet werden, die das neueste AMS verwenden, AMIs kann die Installation des Trend Micro Agents übersprungen werden. AMIs älter als Dezember 2020 unterstützen die BYOEPS-Funktion nicht. Aktualisieren Sie Automatisierungen, die alte

Versionen verwenden, AMIs um das neueste AMS AMIs mit Unterstützung für BYOEPS-Funktionen zu verwenden.

Fügen Sie Ihren Agenten zu Instances hinzu EC2

Sie können AMS Patterns verwenden, um Agenten von Tools wie CrowdStrike Qualys einzusetzen. Senden Sie eine Serviceanfrage, um Unterstützung zu erhalten.

Empfangen von AMS-Benachrichtigungen

Die Kommunikation zwischen Ihnen und AMS erfolgt aus vielen Gründen:

- Ein von AMS erstellter RFC, der Ihre Zustimmung erfordert
- Ein AMS-Fall, der erstellt wurde, um einen von Ihnen erstellten RFC zu untersuchen, der fehlgeschlagen ist
- Ereignisse, die durch die Überwachung von Warnmeldungen erzeugt wurden
- Benachrichtigungen des Patching-Dienstes, die Sie über bevorstehende Patches informieren
- Serviceanfragen und Vorfallberichte
- Monatliche CRM-Berichte
- Gelegentlich wichtige AWS-Ankündigungen (Ihr CSDM kontaktiert Sie, falls Maßnahmen Ihrerseits erforderlich sind)

Alle diese Benachrichtigungen werden an die Standard-Kontaktinformationen (die E-Mail-Adresse des Root-Kontos) gesendet, die Sie AMS beim Onboarding angegeben haben. Da es schwierig ist, einzelne E-Mails auf dem neuesten Stand zu halten, empfehlen wir Ihnen, eine Gruppen-E-Mail zu verwenden, die auf Ihrer Seite aktualisiert werden kann. Alle an Sie gesendeten Benachrichtigungen werden ebenfalls von AMS Operations empfangen und analysiert, bevor eine Antwort erfolgt.

Der AMS-Benachrichtigungsdienst bietet zwei zusätzliche Möglichkeiten, Kontakte für Benachrichtigungen einzurichten:

- Kennzeichnen Sie Ihre Ressourcen mit Kontakt-Tags (der Schlüsselwert des Tags sind Kontaktinformationen) und geben Sie Ihrem CSDM den Tag-Schlüsselnamen an. Alarme zu diesen Ressourcen werden zusätzlich zu dem beim Onboarding erstellten Kontaktkontakt an die im Schlüsselwert angegebenen Kontakte gesendet. Dies ist besonders für Anwendungsbesitzer nützlich. Weitere Informationen finden Sie unter [Tag-basierte Warnmeldung](#).

- (Beim Onboarding erforderlich) Senden Sie benannte Kontaktlisten für Benachrichtigungen, die nicht auf Ressourcen basieren, an Ihr CSDM. Beispielsweise könnten Sie eine Liste mit dem Namen "SecurityContacts" und eine weitere mit dem Namen "OperationsContacts" usw. haben. AMS fügt die Liste dem Benachrichtigungsdienst hinzu, und Alarme, die sich auf den Kontext dieser Liste beziehen, werden an diese Kontakte gesendet. Dies ist besonders nützlich für organisatorische Angelegenheiten.

Diese erweiterte Alert-Routing-Funktion ist für die meisten wichtigen CloudWatch Alarme aktiv, z. B. bei einem Ausfall einer EC2 Amazon-Instance, bei der Volumenauslastung von Amazon Elastic Block Store (Amazon EBS) — Root-Nutzung, Amazon NonRoot EBS-Nutzung, bei hoher Speicherauslastung, bei hoher Swap-Auslastung und bei Amazon bei hoher CPU-Auslastung. EC2

Wenn Sie eine Serviceanfrage oder einen Vorfallbericht einreichen, haben Sie außerdem die Möglichkeit, „CC-E-Mails“ hinzuzufügen (dringend empfohlen), und diese E-Mail-Adressen erhalten Benachrichtigungen über die Serviceanfrage oder den Vorfall.

Important

Während die in Serviceanfragen und Vorfallberichten angegebenen CC-E-Mail-Adressen E-Mail-Benachrichtigungen über Mitteilungen erhalten, erscheinen andere Benachrichtigungen, wie z. B. Patchbenachrichtigungen, in Ihrer Serviceanforderungsliste (eine E-Mail wird auch an den Standardkontakt gesendet), ohne dass Sie ausdrücklich darüber informiert werden, dass eine Mitteilung auf Ihre Aufmerksamkeit wartet. Aus diesem Grund empfehlen wir dringend, eine CC-E-Mail-Adresse hinzuzufügen, wo Sie können, und die Standard-Kontakt-E-Mail als Gruppe einzurichten, in der jeder, der AMS verwendet, Mitglied ist.

Darüber hinaus können Sie spezielle Benachrichtigungen für neue Nachrichten AMIs, für RFC-Statusänderungen und für Konfigurationsänderungen in Ihrem AMS-Konto anfordern. Diese optionalen Benachrichtigungsdienste werden als Nächstes besprochen.

AMS AMI-Benachrichtigungen mit SNS

AMS bietet einen AMI-Benachrichtigungsdienst. Sie können es verwenden, um ein Amazon Simple Notification Service (SNS) -Thema zu abonnieren, das Sie benachrichtigt, wenn AMS-AMI-Updates veröffentlicht wurden. Sie können wählen, ob Sie nur Benachrichtigungen für das von AMIs Ihnen verwendete AMS erhalten möchten, oder Sie können sich anmelden, um

Aktualisierungsbenachrichtigungen für alle AMS zu erhalten. AMIs Weitere Informationen zu SNS-Themen finden Sie unter [Was ist Amazon Simple Notification Service?](#)

Bei jeder AMIs Veröffentlichung senden wir Benachrichtigungen an die Abonnenten des entsprechenden Themas. In diesem Abschnitt wird beschrieben, wie Sie die AMS AMI-Benachrichtigungen abonnieren können.

Beispielnachricht

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has been released. You are now able to launch new EC2 stacks from these AMIs. Please use this time to update any dependencies such as CloudFormation or Autoscaling groups. Release Notes Windows - Contains latest Windows Patches: Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004, KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091, KB4507459) Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057, KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux patches - All AMIs now force domainjoin-cli leave before domainjoin-cli join for better stability in the domain join process.\"\", \"images\": {\"images\": {\"image_name\": \"customer-ams-windows2019-2021.08-1\", \"image_id\": \"ami-05dfa45396fddaa5e\"}}, \"region\": \"us-east-1\"}}\", \"Timestamp\" : \"2021-09-03T19:05:57.882Z\", \"SignatureVersion\" : \"1\", \"Signature\" : \"example sig\", \"SigningCertURL\" : \"example url\", \"UnsubscribeURL\" : \"example url\""}"
```

Mögliche AMS AMI-Themen zum Abonnieren:

- ALLE: Verwendencustomer-ams-all-amis. Dieses Themen-Abonnement benachrichtigt Sie, wenn eines der AMS AMIs aktualisiert wird.

- AMS AWS Linux AMIs: Verwenden Sie für Amazon Linux customer-ams-amazon1 und customer-ams-amazon1-security-enhanced. Verwenden Sie für Amazon Linux 2 customer-ams-amazon2 und customer-ams-amazon2-security-enhanced.
- AMS SUSE Linux AMIs: Verwenden Sie customer-ams-sles12 oder customer-ams-sles15.
- AMS AWS RedHat AMIs: Verwenden Sie customer-ams-rhel8, customer-ams-rhel8-security-enhanced, customer-ams-rhel7, customer-ams-rhel7-security-enhanced.
- AMS AWS CentOS AMIs: Verwenden Sie customer-ams-centos7, customer-ams-centos7-security-enhanced.
- AMS Ubuntu AMIs: Verwenden Sie customer-ams-ubuntu18.
- AMS AWS Windows AMIs: Verwenden Sie customer-ams-windows2019, customer-ams-windows2019-security-enhanced, customer-ams-windows2016, customer-ams-windows2016-security-enhanced, customer-ams-windows2012, customer-ams-windows2012r2, customer-ams-windows2012r2-security-enhanced, customer-ams-windows2022.

So abonnieren Sie neue AMS-AMI-Benachrichtigungen über die Amazon SNS SNS-Konsole:

1. Öffnen Sie die Amazon SNS SNS-Konsole zum [Dashboard](#).
2. Wechseln Sie in der oberen rechten Ecke zur AWS-Region für die Region AMIs, die Sie abonnieren.
3. Wählen Sie im linken Navigationsbereich Abonnements und dann Abonnement erstellen aus.
4. Geben Sie die folgenden Informationen ein:
 - a. Thema ARN: `arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}` wobei REGION die ausgewählte AWS-Region ist (in der die SNS-Benachrichtigung erstellt wurde) und AMS_AMI_NAME das AMI ist, über das Sie Benachrichtigungen erhalten möchten.
Beispiele:
 - Um Benachrichtigungen über neue AMS Amazon Linux AMIs in der AWS-Region us-east-1 zu abonnieren, verwenden Sie dieses Thema ARN = `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`
 - Um Benachrichtigungen über den neuen AMS Window Server 2016 AMIs in der AWS-Region us-west-2 zu abonnieren, verwenden Sie dieses Thema ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.

- c. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen. Wir empfehlen eine Verteilerliste und nicht die E-Mail-Adresse einer Einzelperson.
5. Wählen Sie Create subscription (Abonnement erstellen) aus.
6. Wenn Sie eine Bestätigungs-E-Mail mit dem Betreff „AWS-Benachrichtigung — Abonnementbestätigung“ erhalten, öffnen Sie die E-Mail und wählen Sie Abonnement bestätigen, um Ihr Abonnement abzuschließen.

 Note

Sie sind nicht auf E-Mails für das Protokoll beschränkt. Informationen zu anderen akzeptablen Protokollen und deren Verwendung finden [Sie unter Abonnieren](#).

So melden Sie sich mit der AWS SNS-Konsole von AMS-Benachrichtigungen über neue AMIs ab:

1. Öffnen Sie die Amazon SNS SNS-Konsole zum [Dashboard](#).
2. Wechseln Sie in der Navigationsleiste zur AWS-Region Ihrer Wahl. Sie müssen die AWS-Region verwenden, in der Sie Benachrichtigungen für die entsprechenden Informationen erhalten möchten AMIs.
3. Wählen Sie im Navigationsbereich Abonnements, wählen Sie das Abonnement aus und klicken Sie dann auf Aktionen -> Abonnements löschen.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

So abonnieren Sie AMS New AMI-Benachrichtigungen mithilfe von Deployment | Ingestion | Stack from CloudFormation Template | Create (ct-36cn2avfrj9v):

1. Um die JSON-Datei mit Ausführungsparametern zu abonnieren AmazonLinuxSubscription, zu erstellen und zu speichern. In diesem Beispiel wird sie „.json“ genannt:
CreateSubscribeAmiParams

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription": {
      "Type" : "AWS::SNS::Subscription",
```

```

        "Properties": {
            "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
            "Protocol": "email",
            "Endpoint": "username@yourdomain.com"
        }
    }
}

```

- Erstellen und speichern Sie die JSON-Datei mit den RFC-Parametern mit dem folgenden Inhalt. In diesem Beispiel wird sie als CreateSubscribeAmiRfc JSON-Datei bezeichnet:

```

{
  "ChangeTypeId": "ct-36cn2avfrj9v",
  "ChangeTypeVersion": "1.0",
  "Title": "cfn-ingest-subscribe-ami"
}

```

- Erstellen Sie den RFC, indem Sie die CreateSubscribeAmiRfc Datei und die Datei angeben: CreateSubscribeAmiParams

```

aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --
execution-parameters file://CreateSubscribeAmiParams.json

```

Sie erhalten die ID des neuen RFC in der Antwort und können sie verwenden, um den RFC zu senden und zu überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Beispiele für die Erstellung AMIs finden Sie unter [Create AMI](#).

Informationen zur AMIs programmgesteuerten Nutzung finden Sie unter [EC2 stack: creating](#).

Servicebenachrichtigungen

AMS sendet ausgehende Serviceanfragen oder Servicebenachrichtigungen, wenn Sie auf etwas reagieren müssen oder sich dessen bewusst sein müssen, das sich auf Ihr Konto oder Ihre Ressourcen auswirken könnte, darunter:

- Auswirkungen auf die Infrastruktur: AMS sendet eine Service-Benachrichtigung, wenn sich ein zugrundeliegender AWS-Service auf Ihre Infrastruktur auswirkt und Sie vor einem bestimmten Datum Maßnahmen ergreifen müssen, andernfalls kann es zu einem Ausfall kommen.

- **EC2 Hardwareprobleme:** AMS versendet Servicemeldungen bei EC2 Hardwareproblemen, die einen Neustart einer EC2 Instance vor einem bestimmten Datum erfordern, oder teilt Ihnen mit, dass AMS die Instance für Sie neu startet. Dies ist ein wichtiger Hinweis, da ein Neustart zu einem Ausfall führen kann und Sie mit einem akzeptablen Datum antworten oder einen RFC mit `ct-09qbhy7kvtxqw` erstellen müssen, um die Instance selbst neu zu starten. Eine solche Servicebenachrichtigung wird nach fünf Tagen automatisch geschlossen, wenn Sie nicht antworten.

Benachrichtigungen über RFC-Statusänderungen

AMS bietet Benachrichtigungen über RFC-Statusänderungen per E-Mail und CloudWatch Ereignisse an:

- **E-Mails über die AMS-Konsole:** Auf der zweiten Seite des Assistenten zum Erstellen von RFC gibt es eine Option, mit der Sie bis zu fünf E-Mail-Adressen hinzufügen können, um benachrichtigt zu werden, wenn sich dieser RFC-Status ändert.
- **CloudWatch Ereignisse:** Sie können verschiedene Regeln und Ziele für CloudWatch Ereignisse konfigurieren, sodass Sie bei jeder Änderung des RFC-Status Benachrichtigungen erhalten.

E-Mail-Benachrichtigungen

Sie können E-Mail-Adressen hinzufügen, um RFC-Statusänderungen an einem RFC zu erhalten, den Sie in der AMS-Konsole oder mithilfe der AMS-API/CLI erstellen.

Verwenden Sie in der AMS-Konsole die Option E-Mail-Benachrichtigungen auf der zweiten Seite des Assistenten zum Erstellen von RFC:

Fügen Sie in der AMS API/CLI eine Zeile wie diese zum Abschnitt mit den RFC-Parametern Ihres RFC hinzu (fügen Sie die Zeile nicht dem Abschnitt mit den Ausführungsparametern hinzu):

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

Das Verhalten der Benachrichtigungen variiert je nach RFC-Scheduling-Typ:

- Geplanter RFCs Empfang von E-Mail-Benachrichtigungen für: Gesendet, Geplant, Abgeschlossen InProgress, Abgelehnt, Storniert, Automatisch abgelehnt oder Automatisch storniert.
- E-Mail-Benachrichtigung so schnell wie möglich RFCs erhalten am: „Gesendet“, „Abgeschlossen“ InProgress, „Abgelehnt“, „Storniert“ oder „Automatisch storniert“. AutoRejected

 Note

- E-Mail-Benachrichtigungen werden von dieser Adresse gesendet: `no-reply@managedservices.amazonaws.com`
- Sonderzeichen und URLs in Ihrem RFC-Titel werden in den von uns gesendeten E-Mails redigiert. Dies ist eine Sicherheitsmaßnahme.

CloudWatch Benachrichtigungen zu Ereignissen

AMS bietet Push-Benachrichtigungen für die RFC-Statusänderungen im Rahmen CloudWatch von Events an. Um diese Benachrichtigungen zu erhalten:

1. Erstellen Sie ein Thema und ein Abonnement, in das Benachrichtigungen gesendet werden. Sie können dem Thema einen beliebigen Namen geben. Informationen dazu finden Sie unter [SNS-Thema und Abonnement: Erstellen](#).
2. Reichen Sie einen RFC mit Management | Andere | Andere | Änderungstyp erstellen und das SNS-Thema und das Abonnement in die Anfrage für RFC-Statusänderungsnachrichten aufnehmen.

Wenn Sie die RFC-Anfrage Management | Other | Other für diese Funktion einreichen, können Sie angeben, über welche RFC-Statusänderungen Sie benachrichtigt werden möchten und über welche Änderungstypen Sie informiert werden möchten, und weitere Filter festlegen. Beispielsweise möchten Sie möglicherweise nur dann benachrichtigt werden, wenn die Änderungstypen für den Administratorzugriff EventType = RfcSubmitted und EventType = lauten. RfcUpdated

Dies ist eine Vorlage für CloudWatch Ereignisbenachrichtigungen, die Sie erhalten können (mit allen möglichen Werten):

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned | CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    }
  },
}
```

```

    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending
| Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired |
ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected |
RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted |
RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
        "StartTime": "null | Expected_Start_Time",
        "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
}
}

```

Die unterstützten RFC-Statusänderungen (EventType), so wie sie in der eigentlichen CloudWatch Ereignisbenachrichtigung erscheinen, sind:

- RfcActionStateUpdated (keine AMS-Konsolenoption): Der RFC in einem der später beschriebenen Zustände hat sich geändert.
- RfcApproved (keine AMS-Konsolenoption): Der RFC hat die and/or AMS-Operator-Validierung des Systems bestanden und wurde zur Fertigstellung freigegeben.
- RfcAutoRejected (Automatisch abgelehnt): Der RFC hat die Systemvalidierung oder den AMS-Operator nicht bestanden und wurde abgelehnt.
- RfcCanceled (Storniert oder Automatisch storniert): Der RFC wurde entweder vom Absender oder von einem AMS-Operator storniert.
- RfcCompleted (Abgeschlossen): Die RFC-Ausführungsparameter wurden abgeschlossen, einschließlich. UserData
- RfcCreated (keine AMS-Konsolenoption): Der RFC wurde erfolgreich erstellt (der JSON-Wert und die übermittelten Parameter waren gültig).

- `RfcInProgress` (InProgress): Der RFC-Lauf ist noch im Gange.
- `RfcRejected` (Abgelehnt): Die RFC-fehlgeschlagene System- oder AMS-Operatorvalidierung wurde zurückgewiesen.
- `RfcSubmitted` (Eingereicht): Der RFC wurde eingereicht und wird derzeit vom System validiert.
- `RfcUpdated` (keine AMS-Konsolenoption): Der RFC wurde manuell von einem AMS-Betreiber aktualisiert.

Darüber hinaus können Sie CloudWatch Ereignisbenachrichtigungen (CWE) an jedes der unterstützten Ziele senden und auf diesen automatisierten Benachrichtigungen Ihre eigenen Systeme aufbauen:

- EC2 Amazon-Instanzen
- AWS Lambda Funktionen
- Streams in Amazon Kinesis Data Streams
- Lieferströme in Amazon Data Firehose
- Gruppen in Amazon CloudWatch Logs protokollieren
- Amazon ECS-Aufgaben
- Aufrufen von Systems Manager Run Command
- Systems Manager Automation
- AWS Batch Jobs
- Step-Functions-Zustandsautomaten
- Rohrleitungen in CodePipeline
- CodeBuild projekte
- Amazon Inspector Assessment-Vorlagen
- Amazon SNS-Themen
- Amazon SQS-Warteschlangen
- Integrierte Ziele: EC2 CreateSnapshot API-Aufruf, EC2 RebootInstances API-Aufruf, EC2 StopInstances API-Aufruf und EC2 TerminateInstances API-Aufruf.
- Der Standard-Event-Bus eines anderen AWS-Kontos

Note

Wir senden nach bestem Wissen und Gewissen CloudWatch Ereignisbenachrichtigungen für RFC-Statusänderungen.

Privates und öffentliches DNS einrichten

Während des Onboardings richtet AMS einen privaten DNS-Dienst für die Kommunikation zwischen Ihren verwalteten Ressourcen und AMS ein.

Sie können AMS Route 53 verwenden, um die internen DNS-Namen für Ihre Anwendungsressourcen (Webserver, Anwendungsserver, Datenbanken usw.) zu verwalten, ohne diese Informationen dem öffentlichen Internet zugänglich zu machen. Dadurch wird eine zusätzliche Sicherheitsebene hinzugefügt und Sie können auch einen Failover von einer primären zu einer sekundären Ressource durchführen (oft auch als „Flip“ bezeichnet), indem Sie den DNS-Namen einer anderen IP-Adresse zuordnen.

Nachdem Sie private DNS-Ressourcen mithilfe von `Deployment | Advanced Stack Components | DNS (privat) | Create (ct-0c38gftq56zj6)` oder `Deployment | Advanced Stack Components | DNS (public) | Create (ct-0vzsr2nyraedl)` erstellt haben, können Sie die `Komponenten Management | Advanced Stack Components | DNS (privat) | Update (ct-1d55pi44ff21u)` und `Management | Advanced Stack Components verwenden | DNS (öffentlich) | Update (ct-1hzofpphabs3i)`, CTs um zusätzliche Datensätze zu konfigurieren oder bestehende zu aktualisieren. Bei MALZ-Konten (Multi-Account landing zone) VPCs können DNS-Ressourcen, die im Anwendungskonto erstellt wurden, mit dem Shared Services-Konto VPC gemeinsam genutzt werden, um zentralisiertes DNS mithilfe von AMS AD aufrechtzuerhalten.

MALZ

Die folgende Grafik zeigt eine mögliche DNS-Konfiguration für Multi-Account Landing Zone AMS. Sie veranschaulicht ein hybrides DNS-Setup zwischen AMS und einem typischen Kundennetzwerk. Ein Canonical Name Record (CNAME) im DNS-Server des Kundennetzwerks leitet an den AMS AD DNS im Shared Services-Konto weiter. Dabei erfolgt eine bedingte Weiterleitung, bei der der CNAME des AMS-FQDN an den A-Eintrag weitergeleitet wird.

SALZ

Die folgende Grafik zeigt eine mögliche DNS-Konfiguration für die Single-Account-Landingzone (SALZ). Sie zeigt ein hybrides DNS-Setup zwischen AMS und einem typischen Kundennetzwerk. Ein CNAME im DNS-Server des Kundennetzwerks leitet an den AMS AD DNS mit einer bedingten Weiterleitung weiter, bei der der CNAME des AMS-FQDN an den A-Eintrag weitergeleitet wird.

SALZ Route53 DNS

Die folgende Grafik zeigt eine mögliche DNS-Konfiguration für die Single-Account-Landingzone (SALZ). Sie zeigt ein hybrides DNS-Setup zwischen AMS und einem typischen Kundennetzwerk. Ein CNAME im DNS-Server des Kundennetzwerks leitet an den AMS AD DNS mit einer bedingten Weiterleitung weiter, bei der der CNAME des AMS-FQDN an den A-Eintrag weitergeleitet wird. Dabei wird Route53 auch für ausgehenden Netzwerkverkehr genutzt, sodass für jede Anwendung im Konto die DNS-Auflösung in dem Konto mit der höchsten Verfügbarkeit verfügbar ist.

Route53-aktivierte Auflösungspfade:

- Instanz versucht, AMS MAD-Namen aufzulösen --> VPC +2 (Route53/ AmazonProvided DNS) --> Conditional Forwarders evaluiert --> Route53 MAD Conditional Forwarder-Regel entspricht --> Route53 Outbound Resolver --> Managed AD DNS
- Instanz versucht, Kundenname vor Ort aufzulösen --> VPC +2 (Route53/ AmazonProvided DNS) --> Conditional Forwarders evaluiert --> Route53 On-Prem Conditional Forwarder-Regel entspricht --> Route53 Outbound Resolver --> Kunden-DNS vor Ort
- Instanz versucht, Internetname aufzulösen --> VPC +2 (AmazonProvidedRoute53/DNS) --> Bedingte Weiterleitungen ausgewertet --> Keine passende Weiterleitung --> Internet-DNS-Dienst

Weitere Informationen finden Sie unter [Verwenden von DNS mit Ihrer VPC](#) und [Arbeiten mit privaten gehosteten Zonen](#).

Verwaltung des Ausgangsverkehrs mit AMS

Standardmäßig hat die Route mit einem Ziel-CIDR von 0.0.0.0/0 für private AMS-Subnetze und Subnetze für Kundenanwendungen ein NAT-Gateway (Network Address Translation) als Ziel. AMS-

Dienste TrendMicro und Patching sind Komponenten, die ausgehenden Zugriff auf das Internet haben müssen, damit AMS seinen Dienst bereitstellen kann und Betriebssysteme Updates abrufen können. TrendMicro

AMS unterstützt die Umleitung des ausgehenden Datenverkehrs über ein vom Kunden verwaltetes Ausgangsgerät in das Internet, sofern:

- Es fungiert als impliziter (z. B. transparenter) Proxy.

and

- Es ermöglicht AMS-HTTP- und HTTPS-Abhängigkeiten (in diesem Abschnitt aufgeführt), um das kontinuierliche Patchen und die Wartung der von AMS verwalteten Infrastruktur zu ermöglichen.

Einige Beispiele sind:

- Das Transit Gateway (TGW) hat eine Standardroute, die über die AWS Direct Connect Connect-Verbindung im Multi-Account Landing Zone Networking-Konto auf die vom Kunden verwaltete, lokale Firewall verweist.
- Der TGW hat eine Standardroute, die auf einen AWS-Endpunkt in der ausgehenden Multi-Account-Landingzone-VPC verweist, der AWS nutzt PrivateLink, und auf einen vom Kunden verwalteten Proxy in einem anderen AWS-Konto verweist.
- Der TGW hat eine Standardroute, die auf eine vom Kunden verwaltete Firewall in einem anderen AWS-Konto verweist, mit einer site-to-site VPN-Verbindung als Anhang zur Multi-Account-Landing Zone TGW.

AMS hat die entsprechenden HTTP- und HTTPS-Abhängigkeiten von AMS identifiziert und entwickelt und verfeinert diese Abhängigkeiten kontinuierlich. Weitere Informationen finden Sie unter [egressMgmt.zip](#). Zusammen mit der JSON-Datei enthält die ZIP-Datei eine README-Datei.

Note

- Diese Informationen sind nicht vollständig — einige erforderliche externe Websites sind hier nicht aufgeführt.
- Verwenden Sie diese Liste nicht im Rahmen einer Ablehnungsliste oder einer Blockierungsstrategie.

- Diese Liste dient als Ausgangspunkt für einen Regelsatz zur Filterung ausgehender Zugriffe, wobei davon ausgegangen wird, dass mithilfe von Berichtstools genau ermittelt werden kann, wo der tatsächliche Datenverkehr von der Liste abweicht.

Wenn Sie Informationen zur Filterung des ausgehenden Datenverkehrs benötigen, senden Sie eine E-Mail an Ihren CSDM: ams-csdm@amazon.com.

Bereitstellung von IAM-Ressourcen in AMS Advanced

AMS stellt IAM-Ressourcen auf zwei Arten in Ihren Multi-Account-Landingzone-Anwendungs- (MALZ) -Anwendungs- und Single-Account-Landingzone-Konten (SALZ) bereit:

- **Automatisierte IAM-Bereitstellung:** Mit dieser Funktion in AMS können Sie Änderungstypen für die IAM-Rollen- oder Richtlinienbereitstellung einreichen, erstellen, aktualisieren oder löschen, ohne dass der Betreiber dies überprüfen muss und IAM- und AMS-Validierungsprüfungen automatisch ausgeführt werden.

Diese Funktion muss mit dem Änderungstyp Verwaltung | Verwaltetes Konto | AMS Automated IAM Provisioning with Lese- und Schreibberechtigungen | Enable (Überprüfung erforderlich) explizit aktiviert werden ([ct-1706xvbk6j9hf](#)). Weitere Informationen hierzu finden Sie unter [Automatisierte IAM-Bereitstellung AMS](#). Nachdem AMS Automated IAM Provisioning aktiviert wurde, haben Sie Zugriff auf die Änderungstypen Create, Update und Delete, um Ihre IAM-Ressourcen zu verwalten.

- **Erforderlicher IAM-Änderungstyp überprüfen:** Dieser Änderungstyp, Bereitstellung | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | [Entität oder Richtlinie erstellen \(Überprüfung erforderlich\)](#) ([ct-3dpd8mdd9jn1r](#)), erfordert eine Überprüfung durch den AMS-Betreiber, deren Abschluss manchmal einige Tage dauern kann, falls weitere Informationen erforderlich sind.

Note

Unabhängig davon, welche Methode verwendet wird, wird eine IAM-Rolle für das oder die entsprechenden Konten bereitgestellt. Nachdem die Rolle bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Automatisierte IAM-Bereitstellung AMS

AWS Managed Services (AMS) unterstützt die automatisierte Validierung und Bereitstellung von IAM-Ressourcen, einschließlich Rollen und Richtlinien, mithilfe von erweiterten AMS-Änderungsanforderungen (RFCs) und neuen Änderungstypen (). CTs Bisher durchliefen diese Anfragen einen halbautomatisierten Prozess, der manchmal zu langen Wartezeiten führte. Jetzt können Sie AMS Automated IAM Provisioning verwenden, um IAM-Ressourcen bereitzustellen und die Ergebnisse viel schneller zu erhalten.

So funktioniert die automatisierte IAM-Bereitstellung in AMS

Die automatisierte IAM-Bereitstellung basiert auf automatisierten Laufzeitprüfungen für IAM, um Änderungen an IAM-Ressourcen zu validieren. Diese automatisierten Prüfungen, die bei der Ausführung der Änderungstypen Create, Update oder Delete ausgeführt werden, verhindern, dass IAM-Ressourcen, die übermäßig freizügig sind oder unsichere Muster aufweisen, in Ihrem Konto bereitgestellt werden. Auf diese Weise können Sie den Grad der Genauigkeit der IAM-Überprüfungen an die Expertise Ihres Teams anpassen. Wir empfehlen Teams, die noch keine Erfahrung mit Cloud-Diensten haben und manuelle Prüfungen für alle Änderungen an IAM-Ressourcen benötigen, den vorhandenen Änderungstyp mit Überprüfungspflicht zu verwenden: Bereitstellung | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | [Entität oder Richtlinie erstellen \(Überprüfung erforderlich\)](#), ([ct-3d8mdd9jn1r](#)). Teams mit AWS Fachwissen und Kontrolle über ihre Umgebungen können Automated IAM Provisioning verwenden, um ihre Bereitstellungen zu beschleunigen. Sie können diese Funktion verwenden, um die Validierung durch automatisierte Laufzeitprüfungen durchzuführen oder um nach erfolgreicher Validierung die Validierung und Bereitstellung von IAM-Ressourcen durchzuführen.

Important

AWS Managed Services hat proaktiv eine Liste von [Validierungs-Laufzeitprüfungen](#) implementiert, die die Erstellung von IAM-Ressourcen oder -Richtlinien mit bestimmten Berechtigungen und Bedingungen verhindern. Eine Beschreibung dieser Rechte und Bedingungen finden Sie unter [Bereitstellen von IAM-Ressourcen in AMS Advanced](#). Mit den automatisierten Änderungstypen [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#) und [ct-17cj84y7632o6](#) können Benutzer, die sich mit der Verwaltung von IAM-Ressourcen auskennen, IAM-Rollen und -Richtlinien bereitstellen, die Aktionen ermöglichen, die über Nur-Lese-Rechte hinausgehen.

Darüber hinaus können Sie die Rollen verwenden, die mit den automatisierten Änderungstypen [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#) und [ct-17cj84y7632o6](#) erstellt wurden,

um die neuen Ressourcen zu erstellen. Die Ressourcen können jedoch nicht dem AMS-Benennungsstandard entsprechen und sind nicht Teil des Standard-AMS-Stacks. AMS bietet die Betriebs- und Sicherheitsunterstützung dieser spezifischen Ressourcen nach bestem Wissen und Gewissen.

Sowohl manuelle als auch automatisierte Prozesse zielen darauf ab, unsere Sicherheitsstandards aufrechtzuerhalten, es ist jedoch wichtig zu beachten, dass es Unterschiede bei den Kontrollen zwischen den beiden gibt. Die automatisierte Bereitstellung ermöglicht eine größere Flexibilität bei der Erstellung und Aktualisierung von Rollen und Richtlinien. Daher sind sie nicht identisch. Es wird empfohlen, dass Ihr Unternehmen die im AMS-Benutzerhandbuch aufgeführten [Validierungslaufzeitprüfungen](#) sorgfältig überprüft, um sicherzustellen, dass sie den Erwartungen und Anforderungen Ihres Unternehmens entsprechen.

Ablauf der Validierung

Ablauf der Validierung und Bereitstellung

Note

Diese Funktion eignet sich für Teams, die Erfahrung mit AWS IAM-Ressourcen haben. Wir empfehlen sie nicht für Teams, die noch nicht mit IAM-Ressourcen vertraut sind. AWS Der automatisierte Validierungsprozess ist darauf ausgelegt, die meisten Fehler zu erkennen, und ist hilfreich für Teams, die Änderungen an IAM schnell überprüfen können, wenn sie wissen, welche Berechtigungen sie benötigen. Um die neuen Änderungstypen sicher und effektiv nutzen zu können, empfehlen wir Ihnen, sich gut mit AWS IAM und den [Laufzeitprüfungen](#) der Änderungstypen vertraut zu machen, um festzustellen, ob sie für Ihr Team geeignet sind.

Einführung in AMS Automated IAM Provisioning in AMS

[Um die neuen Änderungstypen zu verwenden, aktivieren Sie zunächst AMS Automated IAM Provisioning, indem Sie einen RFC mit dem folgenden Änderungstyp einreichen: Verwaltung | Verwaltetes Konto | AMS Automated IAM Provisioning mit Lese- und Schreibberechtigungen | Aktivieren \(Überprüfung erforderlich\) \(ct-1706xvvk6j9hf\)](#). AWS erfordert, dass Ihr Unternehmen einen Prozess für das Kundensicherheitsrisikomanagement (CSRM) durchläuft, um sicherzustellen,

dass die Verwendung dieser Änderungstypen Ihren Unternehmensrichtlinien entspricht. Das AWS Betriebsteam arbeitet mit Ihnen zusammen, um im Rahmen der erforderlichen Überprüfung die ausdrückliche Zustimmung Ihres Ansprechpartners für das Sicherheitsteam in Form einer Risikoakzeptanz einzuholen. Weitere Informationen finden Sie im [RFC-Prozess für das Kundenrisikomanagement \(CSRM\)](#).

Nachdem der RFC zur Aktivierung der Funktion AMS Automated IAM Provisioning mit Lese- und Schreibberechtigungen erfolgreich war, aktiviert AMS die Änderungstypen für AMS Automated IAM Provisioning in dem Konto, das für die Übermittlung des Aktivierungs-RFC verwendet wurde. Um zu überprüfen, ob AMS Automated IAM Provisioning für ein Konto aktiviert ist, suchen Sie in der IAM-Konsole nach der Rolle. `AWSManagedServicesIAMProvisionAdminRole`

Im Rahmen des Onboardings stellt AMS den IAM Access Analyzer in derselben AWS-Region des Kontos bereit, um seine Access-Preview-Funktion zu nutzen. IAM Access Analyzer hilft Ihnen dabei, Ressourcen in Ihrer Organisation und Konten zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden, überprüft IAM-Richtlinien anhand der Richtliniengrammatik und der bewährten Methoden und generiert IAM-Richtlinien auf der Grundlage der Zugriffsaktivitäten in Ihren Protokollen. AWS CloudTrail [Weitere Informationen finden Sie unter Verwenden. AWS Identity and Access Management Access Analyzer](#)

Nach dem Onboarding `AWSManagedServicesIAMProvisionAdminRole` wird es für die aktivierten Konten bereitgestellt. Wenn Sie sich dafür entscheiden, diese Rolle über den SAML-Verbund zu verwenden, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Im Rahmen des Onboardings können Sie beantragen, dass die Vertrauensrichtlinie `IAMProvisionAdminRole` von `AWSManaged Services` aktualisiert wird, um einer anderen IAM-Rolle ARN zuzuweisen, mit der diese Rolle übernommen werden kann. AWS Security Token Service

Verwenden von AMS Automated IAM Provisioning in AMS

Sie können RFCs mit den folgenden AMS Automated IAM Provisioning Änderungstypen erstellen.

Note

- Es wird nur die Bereitstellung von Rollen und Richtlinien unterstützt.

Bei der Aktualisierung der Rollen ersetzt das Update CT die bestehende Liste der Amazon-Ressourcennamen (ARNs) für verwaltete Richtlinien und das Richtlinienokument „Rolle übernehmen“ durch die bereitgestellte Liste der verwalteten Richtlinien ARNs

und das Richtliniendokument „Rolle übernehmen“. Bei einer teilweisen Aktualisierung, z. B. beim Hinzufügen oder Entfernen eines ARN in der vorhandenen Liste verwalteter Richtlinien ARNs, ist das Hinzufügen oder Entfernen einzelner Richtlinienanweisungen zum Richtliniendokument „Rolle übernehmen“ nicht zulässig. In ähnlicher Weise ersetzt das Update CT bei der Aktualisierung von Richtlinien das bestehende Richtliniendokument und erlaubt es nicht, einzelne Richtlinienerklärungen in dem vorhandenen Richtliniendokument hinzuzufügen oder zu entfernen.

- Wenn die Option „Nur validieren“ ausgewählt ist, werden Laufzeitprüfungen durchgeführt, ohne dass eine IAM-Entität oder -Richtlinie bereitgestellt wird. Unabhängig von den Ergebnissen lautet der RFC-Status „erfolgreich“. Der Status „Erfolg“ weist auf eine erfolgreiche Validierung anhand der angegebenen IAM-Entität oder -Richtlinie hin.

- Bereitstellung | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | [Entität oder Richtlinie erstellen \(Lese-Schreibberechtigungen\) \(ct-1n9gfnog5x7fl\)](#): Eine neue IAM-Entität oder -Richtlinie wird automatisch validiert und bereitgestellt.
- Verwaltung | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | [Entität oder Richtlinie aktualisieren \(Lese-Schreibberechtigungen\) \(ct-1e0xmuy1diafq\)](#): Eine bestehende IAM-Entität oder -Richtlinie wird automatisch aktualisiert und validiert.
- Verwaltung | Erweiterte [Stack-Komponenten](#) | Identity and Access Management (IAM) | [Entität oder Richtlinie löschen \(Lese-/Schreibberechtigungen\) \(ct-17cj84y7632o6\)](#): Eine bestehende IAM-Entität oder Richtlinie, die mit dem automatischen Änderungstyp „Entität erstellen“ oder „Richtlinie erstellen“ bereitgestellt wurde, wird gelöscht.

Sie können die vorherigen drei nur mit einer speziellen IAM-Rolle aufrufen: CTs `AWSTManagedServicesIAMProvisionAdminRole`. Diese Rolle ist nur für Konten verfügbar, die über die Optionen Verwaltung | Verwaltetes Konto | AMS Automated IAM Provisioning Lese-/Schreibberechtigungen | [Aktivieren \(Überprüfung erforderlich\) \(ct-1706xvvk6j9hf\)](#) in die Funktion integriert wurden.

Important

Die Änderungstypen „Erstellen“, „Aktualisieren“ und „Löschen“ sind in Ihrem Konto immer sichtbar, aber standardmäßig nicht aktiviert. Wenn Sie versuchen, einen RFC mit einem

dieser Änderungstypen einzureichen, ohne zuerst die Funktion AMS Automated IAM Provisioning zu aktivieren, wird die Fehlermeldung „Nicht autorisiert“ angezeigt.

Einschränkungen:

- Mit der Option CT erstellen können Sie möglicherweise eine IAM-Rolle oder -Richtlinie mit der Berechtigung zum Erstellen von Ressourcen erstellen. AWS AWS Ressourcen, die durch diese Rollen und Richtlinien erstellt wurden, werden jedoch nicht von AMS verwaltet. Es hat sich bewährt, sich an Ihre organisatorische Kontrolle zu halten, um die Erstellung solcher Rollen oder Richtlinien einzuschränken.
- Das Update CT kann keine IAM-Rollen und -Richtlinien ändern, die mit CFN Ingest, Direct Change Mode, Developer Mode oder in einigen Fällen mit vorhandenem AMS Advanced manuell oder automatisiert erstellt wurden. CTs
- Das Delete CT kann keine vorhandenen Rollen oder Richtlinien löschen, die nicht mit dem AMS Automated IAM Provisioning Create CT erstellt wurden.
- Die Funktion AMS Automated IAM Provisioning mit Lese- und Schreibberechtigungen wird in Rollen im Direktänderungsmodus nicht unterstützt. Das bedeutet, dass Sie mit diesen Rollen keine IAM-Rollen und -Richtlinien mit Lese- und Schreibberechtigungen bereitstellen oder aktualisieren können.
- AMS Automated IAM Provisioning mit Lese- und Schreibberechtigungen Die Änderungstypen Create, Update und Delete sind nicht mit dem Connector kompatibel. ServiceNow

Laufzeitprüfungen für AMS Automated IAM Provisioning in AMS

Automated IAM Provisioning nutzt Prüfungen aus AWS Identity and Access Management Access Analyzer der AMS-Grenzrichtlinie und führt zusätzliche Prüfungen und Validierungen anhand dieser Richtlinien durch. AMS definierte die zusätzlichen Prüfungen und Validierungen auf der Grundlage von Best Practices für IAM, der Erfahrung mit der Bearbeitung von Kunden-Workloads in der Cloud und der kollektiven Erfahrung mit der manuellen Bewertung von AMS IAM.

Sie können die Ergebnisse der Überprüfung der Richtlinienlaufzeit in der RFC-Ausgabe (Request for Change) einsehen. Zu den Ergebnissen gehören die Ressourcen-ID, der Speicherort innerhalb der and/or Rollenrichtlinie, die die Ergebnisse generiert hat, und eine Meldung, in der die Prüfung beschrieben wird, dass die IAM-Entität oder -Ressource nicht bestanden hat. Diese Ergebnisse helfen Ihnen bei der Erstellung von Richtlinien, die funktionsfähig sind und den bewährten Sicherheitsmethoden entsprechen.

 Note

Bei der automatisierten IAM-Bereitstellung wird versucht, den Standort innerhalb der Entitäts- oder Richtliniendefinition, der die Prüfung nicht besteht, genau anzugeben. Je nach Typ kann der Speicherort den Ressourcennamen oder den ARN oder den Index innerhalb eines Arrays enthalten. Zum Beispiel eine Erklärung, die Ihnen hilft, die Entität oder Richtlinie so anzupassen, dass ein erfolgreiches Ergebnis erzielt wird.

Für eine reibungslose Nutzung von AMS Automated IAM Provisioning hat es sich bewährt, die Option „Nur validieren“ zu verwenden, um die Validierungsprüfungen durchzuführen, bis keine Ergebnisse der Validierungsprüfungen in den RFC-Ausgaben gemeldet werden. Wenn die Validierungsprüfungen keine Ergebnisse ergeben, wählen Sie in der AMS-Konsole die Option Kopie erstellen, um schnell eine Kopie des vorhandenen RFC zu erstellen. Wenn Sie für die Bereitstellung bereit sind, ändern Sie im Abschnitt Parameter den Wert Nur validieren von Ja auf Nein und fahren Sie dann fort.

Dies sind die Laufzeitprüfungen, die AMS Automated IAM Provisioning durchführt, um sicherzustellen, dass Ihre IAM-Ressourcen sicher sind:

 Note

Um IAM-Richtlinien bereitzustellen, die Aktionen enthalten, die durch diese automatisierten Änderungstypen verweigert wurden, müssen Sie den RFC-Prozess für das Kundensicherheitsrisikomanagement (CSRM) befolgen. Verwenden Sie den folgenden Änderungstyp: Bereitstellung | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) (ct-3dpd8mdd9jn1r).

- [Überprüfung und Validierung der IAM Access Analyzer-Richtlinien: Siehe auch Referenz zur Access Analyzer-Richtlinienprüfung und IAM Access Analyzer-Richtlinienvvalidierung.](#)
- Grenzürichtlinienprüfungen für AMS-Berechtigungen: Aktionen für eine Reihe von Diensten, die standardmäßig verweigert werden. Weitere Informationen finden Sie unter [Automatisierte Überprüfung der Zugriffsgrenzen für die IAM-Bereitstellung](#).
- Vom Kunden definierte Grenzürichtlinienprüfungen für Berechtigungen: Zusätzliche eingeschränkte Aktionen für eine Reihe von Diensten, die verweigert wurden. Weitere Informationen finden Sie unter [Automatisierte Überprüfung der Zugriffsgrenzen für die IAM-Bereitstellung](#).

- Von AMS definierte benutzerdefinierte Prüfungen: Überprüft verschiedene unsichere und übermäßig freizügige Richtlinien oder Zugriffsmuster innerhalb einer angeforderten IAM-Entität oder Richtlinie und lehnt die Anfrage ab, falls eine gefunden wird. [Weitere Informationen finden Sie unter JSON-Richtlinienelemente: Principal.AWS](#)

Erkenntnis	Beschreibung
Auf die Rolle kann von einem externen Konto aus zugegriffen werden, das sich außerhalb Ihrer Vertrauenszone befindet.	Dieses Ergebnis bezieht sich auf einen Prinzipal, der in der Vertrauensrichtlinie für Rollen aufgeführt ist und sich außerhalb Ihrer Vertrauenszone befindet. Eine Vertrauenszone ist definiert als das Konto, in dem die Rolle erstellt wird, oder als die AWS Organisation, zu der das Konto gehört. Eine Entität, die nicht zu dem Konto oder derselben AWS Organisation gehört, ist eine externe Entität. Um das Problem zu lösen, überprüfen Sie die Konto-ID im Hauptkonto ARNs und stellen Sie sicher, dass das Konto Ihnen gehört und es sich um ein integriertes AMS-Konto handelt.
Auf die Rolle kann eine externe Entität zugreifen, die einem Konto gehört <i>External_Account_ID</i> , das nicht dem AMS-Kundenkonto gehört. <i>Account_ID</i>	Dieses Ergebnis wird generiert, wenn die Rollenvertrauensrichtlinie einen Prinzipal-ARN mit einer Konto-ID, die Ihnen nicht gehört, und ein integriertes AMS-Konto enthält. Um dieses Problem zu beheben, entfernen Sie einen solchen Prinzipal aus der Rollenvertrauensrichtlinie.
Die kanonische Benutzer-ID wird in der IAM-Vertrauensrichtlinie nicht unterstützt.	Canonical Principal IDs werden in der IAM-Vertrauensrichtlinie nicht unterstützt. Um dieses Problem zu beheben, entfernen Sie einen solchen Prinzipal aus der Rollenvertrauensrichtlinie.

Erkenntnis	Beschreibung
Auf die Rolle kann über eine externe Webidentität zugegriffen werden, die sich außerhalb Ihrer Vertrauenszone befindet.	Dieses Ergebnis wird generiert, wenn die Rollenvertrauensrichtlinie einen anderen externen Web-Identitätsanbieter (IdP) als SAML-IdP zulässt. Um dieses Problem zu beheben, überprüfen Sie die Rollenvertrauensrichtlinie und entfernen Sie die Anweisungen, die den Vorgang zulassen. <code>sts:AssumeRoleWithWebIdentity</code>
Auf die Rolle kann über den SAML-Verbund zugegriffen werden. Der bereitgestellte SAML-Identitätsanbieter (IdP) ist jedoch nicht vorhanden.	Dieses Ergebnis wird generiert, wenn die Rollenvertrauensrichtlinie SAML-IdP enthält, das in Ihrem Konto nicht vorhanden ist. Um das Problem zu lösen, stellen Sie sicher, dass alle aufgelisteten SAML-IdP in Ihrem Konto vorhanden sind.
Die Richtlinie enthält privilegierte Aktionen, die dem Administrator- oder Power-User-Zugriff entsprechen. Erwägen Sie, den Umfang der Berechtigungen auf einen bestimmten Dienst, eine bestimmte Aktion oder Ressource zu reduzieren. Wenn erweiterte Richtlinienelemente wie <code>NotAction</code> oder <code>NotResource</code> verwendet werden, stellen Sie sicher, dass sie nicht mehr Zugriff gewähren, als Sie beabsichtigen, insbesondere bei Zulassungsanweisungen.	Es ist eine bewährte Sicherheitspraxis, nur die Berechtigungen AWS Identity and Access Management zu gewähren, die für die Ausführung einer Aufgabe erforderlich sind, wenn Sie Berechtigungen mit IAM-Richtlinien festlegen. Definieren Sie dazu die Aktionen, die für bestimmte Ressourcen unter bestimmten Bedingungen ausgeführt werden können, die auch als Berechtigungen mit den geringsten Rechten bezeichnet werden. Dieses Ergebnis wird generiert, wenn die Automatisierung feststellt, dass die Richtlinie weitreichende Berechtigungen gewährt und nicht dem Prinzip der geringsten Rechte entspricht. Um dieses Problem zu lösen, überprüfen und reduzieren Sie die Anzahl der Berechtigungen.

Erkenntnis	Beschreibung
Die Erklärung enthält privilegierte Aktionen für <i>Service_Name</i> . Erwägen Sie, diese Aktionen mit einer Deny-Anweisung auszuschließen. Eine Liste der privilegierten Aktionen finden Sie in der Referenz zur Grenzrichtlinie in der AMS-Dokumentation.	AMS hat bestimmte Maßnahmen für einen bestimmten Service als riskant eingestuft und bedürfen einer weiteren Risikoprüfung und Akzeptanz durch das Sicherheitsteam des Kunden. Dieses Ergebnis wird generiert, wenn die Automatisierung feststellt, dass die angegebene Richtlinie solche Berechtigungen gewährt. Um dieses Problem zu beheben, lehnen Sie diese Aktionen in Ihrer Richtlinie ab. Eine Liste der Aktionen finden Sie in der AMS-Grenzrichtlinie. Einzelheiten zur AMS-Grenzpolitik finden Sie unter Grenzüberprüfung für automatisierte IAM-Bereitstellungsberechtigungen von AMS.
Die Anweisung gewährt Zugriff auf bevorzugte RFC-Änderungstypen: ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq und ct-17cj84y7632o6 für den Service. <i>Service_Name</i> Erwägen Sie, die Berechtigungen auf bestimmte Änderungstypen zu beschränken oder diese Änderungstypen mit einer Deny-Anweisung auszuschließen.	Dieses Ergebnis wird generiert, wenn die Richtlinie Berechtigungen zur Ausführung von RFC-bezogenen Aktionen unter Verwendung von Automated IAM Provisioning Change Types () gewährt. CTs Sie CTs unterliegen der Risikobereitschaft und dürfen nur im Rahmen integrierter Rollen verwendet werden. Sie können diesen also keine Genehmigung erteilen. CTs Um dieses Problem zu beheben, verweigern Sie RFC-Aktionen, die diese CTs verwenden.

Erkenntnis	Beschreibung
Die Anweisung enthält privilegierte Aktionen, deren Ausführung nicht auf Ihre Ressourcen beschränkt ist. <i>Service_Name</i> Erwägen Sie, die Aktionen auf bestimmte Ressourcen zu beschränken oder Ressourcen mit AMS-Namespace-Präfixen auszuschließen. Wenn Platzhalter verwendet werden, stellen Sie sicher, dass sie den Geltungsbereich auf Ihre Ressourcen beschränken.	Dieses Ergebnis wird generiert, wenn die Richtlinie privilegierte Aktionen gewährt, die nicht auf Ihre Ressourcen des jeweiligen Dienstes beschränkt sind. Platzhalter führen häufig zu freizügigen Richtlinien, die eine breite Palette von Ressourcen oder Aktionen in den Geltungsbereich der Genehmigung einbeziehen. Um dieses Problem zu beheben, reduzieren Sie entweder den Umfang der Berechtigungen auf Ressourcen, die Sie besitzen, oder schließen Sie Ressourcen aus, die sich im AMS-Namespaces befinden. Eine Liste der AMS-Namespaces-Präfixe finden Sie in der AMS-Dokumentation zur Grenzrichtlinie. Beachten Sie, dass nicht alle Präfixe für alle Dienste gelten. Einzelheiten zur AMS-Grenzrichtlinie finden Sie unter Grenzüberprüfung für automatisierte IAM-Bereitstellungsberechtigungen von AMS.
Ungültige Konto-ID oder Amazon-Ressourcenname (ARN).	Dieses Ergebnis wird generiert, wenn eine in der Richtlinie oder Rollenvertrauensrichtlinie angegebene ARN oder Konto-ID ungültig ist. Informationen zu den Ressourcen einer gültigen ARN-Ressource für Dienste finden Sie in der Service Authorization Reference. Vergewissern Sie sich, dass es sich bei der Konto-ID um eine 12-stellige Zahl handelt und dass das Konto in AWS aktiv ist.

Erkenntnis	Beschreibung
Die Verwendung von Platzhaltern (*) für die Konto-ID in ARN ist eingeschränkt..	Dieser Befund wird generiert, wenn im Konto-ID-Feld eines ARN ein Platzhalter (*) angegeben wird. Ein Platzhalter in einem Konto-ID-Feld entspricht einem beliebigen Konto und gewährt möglicherweise unbeabsichtigt Zugriff auf Ressourcen. Um dieses Problem zu lösen, ersetzen Sie den Platzhalter durch eine bestimmte Konto-ID.
Das angegebene Ressourcenkonto gehört nicht demselben AMS-Kundenkonto <i>Account_ID</i> .	Dieser Befund wird generiert, wenn eine in einem Ressourcen-ARN angegebene Konto-ID Ihnen nicht gehört und nicht von AMS verwaltet wird. Um dieses Problem zu lösen, stellen Sie sicher, dass alle Ressourcen (wie in ihrem ARN in der Richtlinie angegeben) Ihren Konten gehören, die von AMS verwaltet werden.
Der Rollenname befindet sich im eingeschränkten AMS-Namespace.	Dieser Befund wird generiert, wenn Sie versuchen, eine Rolle mit einem Namen zu erstellen, der mit einem reservierten AMS-Präfix beginnt. Um dieses Problem zu lösen, verwenden Sie einen Namen für die Rolle, der für Ihren Anwendungsfall spezifisch ist. Eine Liste der reservierten AMS-Präfixe finden Sie unter Reservierte AMS-Präfixe
Der Richtlinienname befindet sich im eingeschränkten AMS-Namespace.	Dieses Ergebnis wird generiert, wenn Sie versuchen, eine Richtlinie mit einem Namen zu erstellen, der mit einem reservierten AMS-Präfix beginnt. Um dieses Problem zu beheben, verwenden Sie einen Namen für die Richtlinie, der für Ihren Anwendungsfall spezifisch ist. Eine Liste der reservierten AMS-Präfixe finden Sie unter Reservierte AMS-Präfixe .

Erkenntnis	Beschreibung
Die Ressourcen-ID im ARN befindet sich im eingeschränkten AMS-Namespace.	Dieser Befund wird generiert, wenn Sie versuchen, eine Richtlinie zu erstellen, die Zugriff auf benannte Ressourcen gewährt, die sich im AMS-Namespace befinden. Um dieses Problem zu lösen, stellen Sie sicher, dass Sie die Berechtigungen auf Ihre Ressourcen beschränken oder Berechtigungen für Ressourcen verweigern, die sich im AMS-Namespace befinden. Weitere Informationen zu AMS-Namespace finden Sie unter Eingeschränkte AMS-Namespace.
Ungültige Groß- und Kleinschreibung der Richtlinienvariablen. Aktualisieren Sie die Variable auf <i>Variable_Names</i> .	Dieses Ergebnis wird generiert, wenn versucht wird, eine Richtlinie zu erstellen, die im falschen Fall eine globale IAM-Richtlinienvariable enthält. Um dieses Problem zu beheben, verwenden Sie die richtige Groß- und Kleinschreibung für globale Variablen in Ihrer Richtlinie. Eine Liste der globalen Variablen finden Sie unter Kontextschlüssel für AWS globale Bedingungen . Weitere Informationen zu den Richtlinienvariablen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags

Erkenntnis	Beschreibung
Die Anweisung enthält privilegierte Aktionen, die nicht auf Ihre KMS-Schlüssel beschränkt sind. Erwägen Sie, diese Berechtigungen auf bestimmte Schlüssel zu beschränken oder AMS-eigene Schlüssel auszuschließen.	Dieses Ergebnis wird generiert, wenn die Richtlinie Berechtigungen enthält, die nicht auf bestimmte KMS-Schlüssel beschränkt sind, die Sie besitzen. Um dieses Problem zu lösen, beschränken Sie die Berechtigungen auf bestimmte Schlüssel oder schließen Sie die Schlüssel aus, die sich im Besitz von AMS befinden. Schlüssel, die im Besitz von AMS sind, haben spezifische Alias-Sets. Eine Liste der Schlüsselalias, die im Besitz von AMS sind, finden Sie unter Grenzüberprüfung für automatisierte IAM-Bereitstellungsberechtigungen von AMS.
Die Anweisung enthält privilegierte Aktionen, die nicht auf Ihre KMS-Schlüsselalias beschränkt sind. Erwägen Sie, diese Berechtigungen auf Ihre Schlüssel oder Aliase zu beschränken oder AMS-eigene Schlüsselalias auszuschließen.	Dieses Ergebnis wird generiert, wenn die Richtlinie Berechtigungen enthält, die nicht auf bestimmte KMS-Schlüssel-Alias beschränkt sind, deren Eigentümer Sie sind. Um dieses Problem zu lösen, beschränken Sie die Berechtigungen auf bestimmte Schlüssel oder schließen Sie die Schlüssel aus, die sich im Besitz von AMS befinden. Schlüssel, die im Besitz von AMS sind, haben spezifische Alias-Sets. Eine Liste der Schlüsselalias, die im Besitz von AMS sind, finden Sie unter Grenzüberprüfung für automatisierte IAM-Bereitstellungsberechtigungen von AMS.

Erkenntnis	Beschreibung
Die Anweisung enthält privilegierte Aktionen, die nicht ausreichend auf Ihre KMS-Schlüssel unter Verwendung von zugeschnitten sind. <code>kms:ResourceAliases condition</code> Erwägen Sie die Verwendung bestimmter Aliasnamen zusammen mit dem entsprechenden Set-Operator für den Bedingungsschlüssel. Wenn Platzhalter in den Aliasnamen verwendet werden, stellen Sie sicher, dass sie den Gültigkeitsbereich auf einen begrenzten Satz Ihrer KMS-Schlüssel beschränken.	Dieses Ergebnis wird generiert, wenn Sie den Geltungsbereich von Berechtigungen für Ihre KMS-Schlüssel anhand von Bedingungen und nicht anhand von <code>kms:ResourceAliases</code> Aliasnamen für Ihre KMS-Schlüssel einschränken. Oder wenn der <code>kms:ResourceAliases</code> Bedingungsschlüssel einen Wert hat, der auch AMS-eigene KMS-Schlüsselalias enthält. Um dieses Problem zu lösen, aktualisieren Sie die Bedingung so, dass die Berechtigungen nur auf Aliase Ihrer KMS-Schlüssel beschränkt werden oder Aliase für AMS-eigene KMS-Schlüssel ausgeschlossen werden. Eine Liste der Schlüsselalias, die sich im Besitz von AMS befinden, finden Sie unter. Grenzüberprüfung für automatisierte IAM-Bereitstellungsberechtigungen von AMS
Der Rolle muss <code>customer_deny_policy</code> angehängt sein. Nehmen Sie den Richtlinien-ARN in die Liste der verwalteten Richtlinien auf ARNs.	Dieser Befund wird generiert, wenn der Rolle, die Sie erstellen, kein <code>customer_deny_policy</code> Link zugewiesen wurde. Um dieses Problem zu beheben, nehmen Sie die <code>customer_deny_policy</code> in die ARNs Liste der verwalteten Richtlinien auf.

Erkenntnis	Beschreibung
Die AWS verwaltete Richtlinie ist übermäßig freizügig oder gewährt Berechtigungen, die durch die AMS-Grenzrichtlinie eingeschränkt sind.	Dieses Ergebnis wird generiert, wenn der ManagedPolicyArnsWert für die Rolle eine von AMS verwaltete Richtlinie enthält, die vollen Zugriff oder Zugriff auf Administratorebene auf den entsprechenden Dienst gewährt. Um dieses Problem zu lösen, überprüfen Sie die Verwendung der AWS verwalteten Richtlinie und verwenden Sie eine Richtlinie, die Zugriffsberechtigungen nach unten vorsieht, oder definieren Sie Ihre eigene Richtlinie, die dem Prinzip der geringsten Rechte folgt.
Die vom Kunden verwaltete Richtlinie befindet sich im eingeschränkten AMS-Namespace.	Dieses Ergebnis wird generiert, wenn der Rolle eine vom Kunden verwaltete Richtlinie zugewiesen wird, deren Name im AWS Namespace vorangestellt ist. Um dieses Problem zu beheben, entfernen Sie die Richtlinie aus der ManagedPolicyArnListe für die Rolle.
Die customer_deny_policy kann nicht von der Rolle getrennt werden. Nehmen Sie den Richtlinien-ARN in die Liste der verwalteten Richtlinien auf ARNs.	Dieses Ergebnis wird generiert, wenn der während eines Updates von der Rolle getrennt customer_deny_policy wird. Um dieses Problem zu beheben, fügen Sie dem customer_deny_policy ManagedPolicyArnsFeld der Rolle das hinzu und versuchen Sie es erneut.

Erkenntnis	Beschreibung
Die vom Kunden verwalteten Richtlinien wurden außerhalb des AMS Change Management Services oder ohne vorherige Überprüfung bereitgestellt.	Dieses Ergebnis wird generiert, wenn einer Rolle eine oder mehrere bestehende, vom Kunden verwaltete Richtlinien zugeordnet ARNs sind und die Richtlinien nicht über den AMS Change Management-Service (über einen RFC) bereitgestellt werden. Der Entwurfsmodus oder der Direktänderungsmodus ermöglichen es Kunden beispielsweise, IAM-Richtlinien ohne RFC bereitzustellen. Um dieses Problem zu lösen, entfernen Sie die vom Kunden verwaltete Richtlinie ARNs aus der ManagedPolicyArnsListe für die Rolle.
Die Anzahl der bereitgestellten verwalteten Richtlinien ARNs übersteigt das Kontingent der beigefügten Richtlinie pro Rolle.	Dieses Ergebnis wird generiert, wenn die Gesamtzahl der verwalteten Richtlinien, die der Rolle zugeordnet sind, das Kontingent für die Richtlinie pro Rolle überschreitet. Weitere Informationen zu IAM-Kontingenten finden Sie unter IAM- und AWS STS STS-Kontingente, Namensanforderungen und Zeichenbeschränkungen . Verwenden Sie diese Informationen, um die Anzahl der Richtlinien zu reduzieren, die Sie der Rolle zuordnen.
Die Größe der Vertrauensrichtlinie ({trust_policy}) übersteigt die angenommene Größenquote der Rollenrichtlinie von {size}.	Dieser Befund wird generiert, wenn die Größe des Dokuments mit der Richtlinie „Rolle übernehmen“ die Größenquote der Richtlinie überschreitet. Weitere Informationen zu IAM-Kontingenten finden Sie unter IAM- und AWS STS STS-Kontingente, Namensanforderungen und Zeichenbeschränkungen .

Erkenntnis	Beschreibung
Die Erklärung enthält alle mutativen Aktionen für Amazon S3. Erwägen Sie, diese Berechtigungen nur auf die erforderlichen Aktionen auszudehnen. Wenn Platzhalter verwendet werden, stellen Sie sicher, dass sie nur eine begrenzte Anzahl von mutativen Aktionen umfassen.	Dieses Ergebnis wird generiert, wenn die angegebene Richtlinie allen Amazon Simple Storage Service mutative Berechtigungen unabhängig von einer oder mehreren Ressourcen gewährt. Um dieses Problem zu lösen, schließen Sie nur die erforderlichen mutativen Amazon S3 S3-Aktionen gegen Ihre Buckets ein.
Die Anweisung enthält privilegierte Aktionen, die für keinen Bucket in Amazon S3 zulässig sind. Erwägen Sie, eine Erklärung hinzuzufügen, die diese Aktionen ablehnt.	Dieses Ergebnis wird generiert, wenn die Richtlinie privilegierte Aktionen für einen beliebigen Bucket gewährt. Eine Liste der privilegierten Aktionen finden Sie unter Grenzüberprüfung für automatisierte IAM-Bereitstellungsberechtigungen von AMS . So beheben Sie dieses Problem, entfernen oder verweigern Sie diese Aktionen in Ihrer Richtlinie.
Die Anweisung enthält privilegierte Aktionen, die nicht auf Ihre Buckets in Amazon S3 beschränkt sind. Erwägen Sie, Ihre Buckets mit AMS-Namespace-Präfixen einzubeziehen oder auszuschließen. Wenn Platzhalter verwendet werden, stellen Sie sicher, dass sie mit Buckets in Ihren Namespaces übereinstimmen.	Dieses Ergebnis wird generiert, wenn die Richtlinie Amazon S3-Aktionen gewährt, die nicht nur auf Ihre Buckets beschränkt sind. Dies ist häufig der Fall, wenn bei der Angabe von Bucket-Ressourcen Platzhalter verwendet werden. Um dieses Problem zu lösen, geben Sie Bucket-Namen an oder geben Sie an ARNs, dass Sie Eigentümer der Buckets sind, oder schließen Sie die Buckets mit AMS-Namespace-Präfixen aus.

Erkenntnis	Beschreibung
Die Anweisung enthält privilegierte Aktionen, die nicht auf Ihre Buckets in Amazon S3 beschränkt sind. Erwägen Sie, die Verwendung von Platzhaltern (*) zu vermeiden, die alle Buckets im Konto betreffen.	Dieses Ergebnis wird generiert, wenn die Richtlinie Amazon S3-Aktionen gewährt, die nicht auf Ihren Bucket beschränkt sind. Dies ist häufig der Fall, wenn bei der Angabe von Bucket-Ressourcen Platzhalter verwendet werden. Um dieses Problem zu lösen, geben Sie Bucket-Namen an oder geben Sie an ARNs, dass Sie Eigentümer der Buckets sind, oder schließen Sie die Buckets mit AMS-Namespace-Präfixen aus.
Die Anweisung enthält einen Ressourcen-Platzhalter, der für alle Amazon S3-Buckets gilt, einschließlich nicht vorhandener Buckets und Buckets, die Sie nicht besitzen. Erwägen Sie, den Geltungsbereich der Berechtigungen mithilfe einer Bedingung und eines Bedingungschlüssels festzulegen. <code>s3:ResourceAccount</code>	Dieses Ergebnis wird generiert, wenn die Richtlinie Berechtigungen für Buckets erteilt, die mit Platzhaltern angegeben wurden. Die Verwendung von Platzhaltern bringt häufig Buckets mit sich, die nicht existieren oder deren Besitzer nicht sind. Um dieses Problem zu lösen, verwenden Sie die Bedingung und den <code>aws:ResourceAccount</code> Bedingungschlüssel, um die Berechtigungen nur auf Buckets innerhalb des aktuellen Kontos zu beschränken. Weitere Informationen finden Sie unter Beschränken des Zugriffs auf Amazon S3 S3-Buckets, die bestimmten AWS Konten gehören.

Erkenntnis	Beschreibung
Die Erklärung enthält ein <code>NotResource</code> Richtlinienelement, das auf eine große Anzahl von Buckets beschränkt sein kann, einschließlich nicht vorhandener Buckets und Buckets, die Sie nicht besitzen. Erwägen Sie, den Geltungsbereich der Berechtigungen mithilfe einer Bedingung und eines Bedingungsschlüssels festzulegen. <code>s3:ResourceAccount</code>	Dieses Ergebnis wird generiert, wenn die Richtlinie das Policy-Element zur Angabe von <code>NotResources</code> Bucket-Ressourcen verwendet. Die Verwendung des <code>NotResource</code> Elements kann sich auf eine große Anzahl von Buckets erstrecken, einschließlich Buckets, die nicht existieren oder denen keine Besitzer gehören. Um dieses Problem zu lösen, verwenden Sie Bedingungen und den <code>aws:ResourceAccount</code> Bedingungsschlüssel, um die Berechtigungen auf Buckets nur innerhalb des aktuellen Kontos zu beschränken.
Die Erklärung enthält Amazon S3 S3-Aktionen für Buckets, <i>Bucket_Name</i> die entweder nicht existieren, nicht dem Konto gehören oder der Name einen Platzhalter enthält <i>Account_ID</i> , der möglicherweise auf eine große Anzahl von Buckets beschränkt ist, einschließlich nicht vorhandener Buckets und Buckets, die Ihnen nicht gehören. Erwägen Sie, den Geltungsbereich der Berechtigungen mithilfe einer Bedingung und des Bedingungsschlüssels festzulegen <code>s3:ResourceAccount</code>	Dieses Ergebnis wird generiert, wenn die Richtlinie Berechtigungen für Buckets erteilt, die entweder nicht existieren, nicht Ihnen gehören oder die Platzhalter in den Bucket-Namen enthalten, die eine große Anzahl von Buckets abdecken, und der Zugriff nicht nur auf das aktuelle Konto beschränkt ist. Um dieses Problem zu lösen, verwenden Sie die Bedingung und den <code>aws:ResourceAccount</code> Bedingungsschlüssel, um die Berechtigungen nur auf Buckets innerhalb des Girokontos zu beschränken.

Erkenntnis	Beschreibung
Die Kontoauszug enthält Amazon S3 S3-Aktionen für Buckets, <i>Bucket_Name</i> die entweder nicht existieren, nicht dem Konto gehören <i>Account_ID</i> , oder der Name enthält einen Platzhalter, der auf eine große Anzahl von Buckets beschränkt sein könnte, einschließlich nicht existierender Buckets und Buckets, die Ihnen nicht gehören. Der Zugriff ist nicht eingeschränkt, wenn Sie ein bestimmtes Ressourcenkonto verwendens3 : ResourceAccount , sofern die Bedingung nicht Ihnen gehört.	Dieses Ergebnis wird generiert, wenn die Richtlinie Berechtigungen für Buckets erteilt, die entweder nicht existieren, nicht Ihnen gehören oder die Platzhalter in den Bucket-Namen haben, die eine große Anzahl von Buckets abdecken, und der Zugriff nur auf ein bestimmtes Konto beschränkt ist. Das im aws : ResourceAccount Bedingungsschlüssel angegebene Konto gehört Ihnen jedoch nicht und wird von AMS verwaltet. Um dieses Problem zu lösen, aktualisieren Sie den aws : ResourceAccount Bedingungsschlüssel und geben Sie die entsprechende Konto-ID ein, die Ihnen gehört und von AMS verwaltet wird.
Die Erklärung enthält privilegierte Aktionen, die nicht auf Ihre Instances für Amazon beschränkt sind. EC2 Erwägen Sie, die Aktionen auf bestimmte Instances zu beschränken ARNs oder Instances auszuschließen, die einen Name-Tag-Schlüssel mit einem Wert in AMS-Namespaces-Präfixen haben. Wenn Platzhalter verwendet werden, stellen Sie sicher, dass sie mit den Namespaces übereinstimmen, deren Eigentümer Sie sind.	Dieses Ergebnis wird generiert, wenn die Richtlinie privilegierte Aktionen gegen EC2 Amazon-Instances gewährt, die AMS besitzt. AMS-Instances werden mit dem Tag-Schlüssel Name mit Werten im AMS-Namespace gekennzeichnet. Um dieses Problem zu lösen, geben Sie Ihre Ressourcen an oder schließen Sie AMS-Instances mit einer Bedingung aus, die den aws : ResourceTag/Name Schlüssel enthält, der Werte im AMS-Namespace mithilfe des Operators ausschließt StringNotLike

Erkenntnis	Beschreibung
Die Anweisung enthält privilegierte Aktionen, die nicht auf Ihre Ressourcen im Parameter Speicher beschränkt sind. AWS Systems Manager Erwägen Sie, Ihre Parameter anzugeben ARNs oder Parameter mit AMS- Namespace-Präfixen auszuschließen. Wenn Platzhalter verwendet werden, stellen Sie sicher, dass sie nur Ihre Parameter betreffen.	Dieser Befund wird generiert, wenn die Richtlinie Berechtigungen für Parameter gewährt, deren Eigentümer Sie nicht sind. Dies ist normalerweise der Fall, wenn Platzhalter verwendet werden oder Parameter mit AMS-Namespace-Präfixen in einer Richtlinienanweisung unter Ressourcen aufgeführt werden. Um dieses Problem zu lösen, geben Sie Parameter an, die sich in Ihrem Namespace befinden, oder schließen Sie AMS-Parameter mit einer Deny-Anweisung aus.
Die Anweisung enthält privilegierte Aktionen gegen Ressourcen in AWS Systems Manager. Erwägen Sie, die Berechtigungen auf nur lesbare Aktionen oder Aktionen gegen Ihre Ressourcen zu beschränken.	Dieses Ergebnis wird generiert, wenn die Richtlinie andere Berechtigungen als Parameterspeicher- oder schreibgeschützte Aktionen für Systems Manager-Ressourcen gewährt. Um dieses Problem zu beheben, reduzieren Sie die Berechtigungen auf schreibgeschützte Aktionen oder nur auf das Speichern von Parametern.
Die Anweisung enthält privilegierte Aktionen, die in <i>Service_Name</i> Ihrem Besitz nicht auf {message} beschränkt sind. Erwägen Sie, diese Berechtigungen gegebenenfalls auf bestimmte Ressourcentypen zu beschränken oder AMS-eigene Ressourcen auszuschließen. Wenn Platzhalter verwendet werden, stellen Sie sicher, dass sie übereinstimmen. <i>Resources</i>	Dieses Ergebnis wird generiert, wenn die Richtlinie privilegierte Aktionen zulässt, die nicht gegen Ihre Ressourcen gewährt werden, insbesondere für benannte Ressourcen. Um dieses Problem zu beheben, überprüfen Sie Ihre Ressourcenliste und prüfen Sie, ob sie sich nur auf Ressourcen beziehen, die sich in Ihrem Namespace befinden. Schließen Sie alternativ Ressourcen aus, die sich im AMS-Namespace befinden.

Erkenntnis	Beschreibung
Die Anweisung enthält Tagging-Aktionen von <code>{Service_Name}</code> , die nicht auf bestimmte Werte für den Namen-Tag-Schlüssel beschränkt sind. Erwägen Sie, diese Aktionen einzuschränken, indem Sie den <code>aws:RequestTag/Name</code> Bedingungsschlüssel mit Werten in Ihrem Namespace festlegen, oder schränken Sie diese Aktionen ein, indem Sie den <code>aws:RequestTag/Name</code> Bedingungsschlüssel mit dem <code>StringNotLike</code> Operator mit Werten in den AMS-Namespaces-Präfixen festlegen.	Dieses Ergebnis wird generiert, wenn die Richtlinie Tagging-Berechtigungen für einen bestimmten Dienst gewährt und die Berechtigung nicht auf bestimmte Tag-Schlüssel/Werte beschränkt ist. Verwenden Sie die Bedingung <code>,</code> um einzugrenzen, welcher Schlüssel oder Wert in Tag-Aktionen verwendet werden kann, z. B. wenn Sie eine Anfrage zur Ausführung der Aktionen stellen. <code>aws:RequestTag/tag key</code> Um dieses Problem zu lösen, verwenden Sie diesen Bedingungsschlüssel, um Schlüssel oder Werte in Ihrem Namespace einzuschränken. Oder verweigern Sie das Name Tag key (<code>aws:RequestTag/Name</code>) mit Werten im AMS-Namespaces.
Interner Fehler bei der Überprüfung der Vertrauensrichtlinie für IAM-Rollen.	Dieses Ergebnis wird generiert, wenn CT Automation bei der Validierung der IAM-Rollenvertrauensrichtlinie durch den IAM Access Analyzer-Dienst auf einen Fehler stößt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.
Interner Fehler bei der Validierung der vom Kunden verwalteten Richtlinie.	Dieses Ergebnis wird generiert, wenn CT Automation bei der Validierung der vom Kunden verwalteten Richtlinie über den IAM Access Analyzer-Service auf einen Fehler stößt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.

Erkenntnis	Beschreibung
Access Analyzer wurde nicht gefunden in AWS-Region . Die Überprüfung der Zugriffsvorschau für die Rollenvertrauensrichtlinie konnte nicht durchgeführt werden.	Dieses Ergebnis wird generiert, wenn die IAM Access Analyzer-Ressource nicht in der AWS-Region gefunden wird. Wenden Sie sich an AMS Operations, um Fehler zu beheben und eine IAM Access Analyzer-Ressource in der AWS-Region zu erstellen.
Ungültige Vertrauensrichtlinie für die Rolle Role_Name	Dieses Ergebnis wird generiert, wenn die angegebene IAM-Rolle eine ungültige Vertrauensrichtlinie enthält. Um das Problem zu lösen, überprüfen Sie die Vertrauensrichtlinie, um sicherzustellen, dass sie gültig ist.
IAM Access Analyzer ist auf einen internen Fehler gestoßen. Die Zugriffsvorschau für die Rolle konnte nicht erstellt werden Role_Name	Dieses Ergebnis wird generiert, wenn bei der Automatisierung beim Erstellen einer Zugriffsvorschau für eine Rolle mit dem IAM Access Analyzer ein Fehler auftritt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.
Die Zugriffsvorschau für die Vertrauensrichtlinie der Rolle konnte nicht erstellt werden Role_Name	Dieses Ergebnis wird generiert, wenn bei der Automatisierung beim Erstellen einer Zugriffsvorschau für eine Rolle mit dem IAM Access Analyzer ein Fehler auftritt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.

Erkenntnis	Beschreibung
Interner Fehler bei der Validierung des aufgelisteten SAML-IdP.	Dieses Ergebnis wird generiert, wenn bei der Automatisierung bei der Validierung der bereitgestellten SAML, die in der Rollenvertrauensrichtlinie IdPs aufgeführt ist, ein Fehler auftritt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.
Interner Fehler bei der Überprüfung der Berechtigungen gegen. AWS Key Management Service	Dieses Ergebnis wird generiert, wenn bei der Automatisierung bei der Überprüfung der AWS KMS Schlüsselberechtigungen in der bereitgestellten Richtlinie ein Fehler auftritt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.
Interner Fehler bei der Überprüfung der aufgelisteten verwalteten Richtlinie. ARNs	Dieses Ergebnis wird generiert, wenn bei der Automatisierung bei der Überprüfung der aufgelisteten verwalteten Richtlinie ein Fehler auftritt. ARNs Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.
Interner Fehler bei der Überprüfung des Standardanhangscustomer_deny_policy .	Dieses Ergebnis wird generiert, wenn bei der Automatisierung bei der Überprüfung, ob der an die Rolle angehängt customer_deny_policy ist, ein Fehler auftritt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.

Erkenntnis	Beschreibung
Interner Fehler bei der Überprüfung verwalteter Policy-Warnmeldungen für die Rolle <i>Role_Name</i>	Dieses Ergebnis wird generiert, wenn bei der Automatisierung bei der Validierung der verwalteten Richtlinie ARNs für die Rolle ein Fehler auftritt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.
Interner Fehler bei der Validierung <i>Policy_name</i> anhand der vom Kunden definierten Grenzrichtlinie AWSManagedServices IAMProvisionCustomerBoundaryPolicy	Dieses Ergebnis wird generiert, wenn bei der Automatisierung bei der Überprüfung der Richtlinie, die Ihre benutzerdefinierte Sperrliste enthält, ein Fehler auftritt. Um dieses Problem zu beheben, reichen Sie den RFC erneut ein. Wenn der Fehler weiterhin besteht, wenden Sie sich an AMS Operations, um den Fehler zu beheben.
Für das Konto ist eine vom Kunden definierte Grenzrichtlinie AWSManagedServices IAMProvisionCustomerBoundaryPolicy vorhanden. Die Richtlinie enthält jedoch Zulassungsanweisungen, die Berechtigungen gewähren. Die Richtlinie darf nur Verweigerungsanweisungen enthalten.	Dieses Ergebnis wird generiert, wenn die Richtlinie, die Ihre benutzerdefinierte Ablehnungsliste enthält, eine Erklärung enthält, die eine Genehmigung erteilt. Obwohl die benutzerdefinierte Ablehnungsliste in Ihrem Konto als IAM-verwaltete Richtlinie vorhanden ist, kann sie nicht für die Berechtigungsverwaltung verwendet werden. Die Richtlinie darf nur Ablehnungsaussagen enthalten, die darauf hinweisen, dass AMS Automated IAM Provisioning die Aktionen in Ihren IAM-Richtlinien, die AMS Automated IAM Provisioning erstellt, validieren und ablehnen soll.

Erkenntnis	Beschreibung
Die Erklärung enthält privilegierte Aktionen, für die Ihre Organisation definiert hat. Service_Name Erwägen Sie, diese Aktionen mit einer Deny-Anweisung auszuschließen. Die Liste der eingeschränkten Aktionen finden Sie in der in Ihrem Konto angegebenen Richtlinie.	Dieses Ergebnis wird generiert, wenn die Automatisierung eine Aktion in Ihrer Richtlinie erkennt, die Sie in der benutzerdefinierten Ablehnungsliste definiert haben. Um das Problem zu beheben, überprüfen Sie Ihre Richtlinienerklärung und entfernen Sie alle Aktionen, die in Ihrer benutzerdefinierten Ablehnungsliste definiert sind, oder fügen Sie eine Ablehnungserklärung hinzu, die diese Aktionen ablehnt.
Die Rolle muss POLICY_ARN angehängt worden sein. Nehmen Sie den Richtlinien-ARN in die Liste der verwalteten Richtlinien auf ARNs.	Dieser Befund wird generiert, wenn der Rolle, die Sie erstellen, kein POLICY_ARN Link zugeordnet ist. Um dieses Problem zu beheben, fügen Sie das POLICY_ARN in das ManagedPolicyArnsFeld der Rolle ein und versuchen Sie es erneut.
Das POLICY_ARN kann nicht von der Rolle getrennt werden. Nehmen Sie den Richtlinien-ARN in die Liste der verwalteten Richtlinien auf ARNs.	Dieses Ergebnis wird generiert, wenn der während eines Updates von der Rolle getrennt POLICY_ARN wird. Um dieses Problem zu beheben, fügen Sie dem POLICY_ARN ManagedPolicyArnsFeld der Rolle das hinzu und versuchen Sie es erneut.

Grenzüberprüfung für automatisierte IAM-Bereitstellungsberechtigungen von AMS

AMS-Berechtigungsgrenzprüfungen helfen Ihnen dabei, die von AMS bereitgestellten Standardrichtlinien für Berechtigungsgrenzen einzuhalten. Diese Richtlinie ist eine Liste von Aktionen, die von AMS Automated IAM Provisioning verweigert wurden. Bereitstellungsrichtlinien, die diese eingeschränkten Aktionen enthalten, erfordern eine zusätzliche ausdrückliche Risikoakzeptanz. Laden Sie die Richtlinie hier herunter: [boundary-policy.zip](#).

Verwenden Sie vom Kunden definierte Richtlinienprüfungen für Zugriffsgrenzen, um Ablehnungsaktionen anzupassen, die über die Standardwerte der AMS-Richtlinie für Zugriffsgrenzen

hinausgehen. Wenn Sie AMS Automated IAM Provisioning mit dem folgenden Änderungstyp nutzen: Verwaltung | Verwaltetes Konto | AMS Automated IAM Provisioning mit Lese- und Schreibberechtigungen | [Aktivieren \(Überprüfung erforderlich\) \(ct-1706xvvk6j9hf\)](#), können Sie eine Liste mit benutzerdefinierten Ablehnungsaktionen hinzufügen, die zusätzliche eingeschränkte Aktionen angeben.

Sie können die Liste der Ablehnungsaktionen mithilfe des folgenden Änderungstyps aktualisieren: Verwaltung | Verwaltetes Konto | Automatisierte IAM-Bereitstellung mit Lese- und Schreibberechtigungen | [Benutzerdefinierte Ablehnungsliste aktualisieren](#) (ct-2r9xvd3sdsic0).

Sie müssen die dedizierte IAM-Rolle verwenden, um diesen Änderungstyp auszuführen.

`AWSTransferRoleAccess`

Note

- Sie müssen für jedes Update eine umfassende Liste der Ablehnungsaktionen bereitstellen. Die vorherige Liste wird durch die neue Liste ersetzt.
- Die Liste der Ablehnungsaktionen darf nur Aktionen enthalten, die verweigert werden sollen. Aktionen zum Zulassen werden nicht unterstützt.
- Die Liste der Ablehnungsaktionen befindet sich innerhalb des Kontos als IAM-verwaltete Richtlinie mit dem Namen `AWSTransferRoleAccess`. Die Richtlinie darf keiner Rolle zugewiesen werden.
- Der Begriff „Berechtigungsgrenze“, der für verweigerter Aktionen in AMS Automated IAM Provisioning verwendet wird, hat eine andere kontextuelle Bedeutung als die IAM-Berechtigungsgrenze. Die IAM-Berechtigungsgrenze legt die maximale Berechtigung fest, die eine Richtlinie einer IAM-Entität zur Laufzeit gewähren kann. Weitere Informationen zur IAM-Berechtigungsgrenze finden Sie unter [Richtlinientypen](#) im AWS Identity and Access Management Benutzerhandbuch. Die Berechtigungsgrenze in AMS Automated IAM Provisioning verhindert, dass Sie eine IAM-Richtlinie bereitstellen, die einen bestimmten Satz von Berechtigungen enthält, z. B. eine Liste verweigerter Aktionen.

Behebung von Ergebnissen und Fehlern bei AMS Automated IAM Provisioning

Es gibt drei Möglichkeiten, wie Sie bei der Verwendung von AMS Automated IAM Provisioning auf Probleme stoßen können:

- RFC-Fehler: Diese können aus einer Vielzahl von Gründen auftreten, z. B. aufgrund falscher Eingaben. Weitere Informationen finden Sie unter [Behebung von RFC-Fehlern in AMS](#).
- SSM-Fehler: Diese können aus einer Vielzahl von Gründen auftreten, z. B. aufgrund einer schlechten Formatierung. Weitere Informationen finden Sie unter [Problembehandlung bei Systems Manager Automation](#).
- Ergebnisse der Validierungsprüfung: Diese Ergebnisse treten auf, wenn bei einer der vielen Validierungsprüfungen, die Automated IAM Provisioning ausführt, ein Problem festgestellt wird. Eine Liste der Validierungsprüfungen und empfohlene Maßnahmen zur Behebung finden Sie unter [Laufzeitprüfungen für AMS Automated IAM Provisioning in AMS](#)

Berechtigungen in AMS mit IAM-Rollen und -Profilen einrichten

AMS verwendet AWS Identity and Access Management (IAM) zur Verwaltung von Benutzern, Sicherheitsanmeldedaten wie Zugriffsschlüsseln und Berechtigungen, mit denen gesteuert wird, auf welche AWS Ressourcen Benutzer und Anwendungen zugreifen können. AMS bietet eine Standard-IAM-Benutzerrolle und ein standardmäßiges EC2 Amazon-Instance-Profil (das eine Anweisung enthält, die der Ressource den Zugriff auf die Standard-IAM-Benutzerrolle ermöglicht).

Eine neue IAM-Benutzerrolle oder ein neues Instance-Profil anfordern

AMS verwendet eine IAM-Rolle, um Benutzerberechtigungen über Ihren Verbunddienst festzulegen, und ein IAM-Instanzprofil als Container für diese IAM-Rolle.

Sie können eine benutzerdefinierte IAM-Rolle mit dem Änderungstyp Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) (ct-3dpd8mdd9jn1r) oder ein IAM-Instanzprofil mit dem Änderungstyp Management | Anwendungen | IAM-Instanzprofil erstellen | Änderungstyp erstellen (ct-0ixp4ch2tiu04) anfordern). Sehen Sie sich die jeweiligen Beschreibungen in diesem Abschnitt an.

Note

AMS hat eine IAM-Richtlinie, `customer_deny_policy` die gefährliche Namespaces und Aktionen blockiert. Diese Richtlinie ist standardmäßig allen AMS-Kundenrollen zugeordnet und stellt für Benutzer selten ein Problem dar. Ihre IAM-Benutzer- und Rollenabfragen enthalten diese Richtlinie nicht, aber die automatische Aufnahme der `customer_deny_policy` in Anfragen für IAM-Rollen hilft AMS, neue IAM-Instanzprofile schneller bereitzustellen. Sie können den Ausschluss der Richtlinie

beantragen. `customer_deny_policy` Diese Anfrage wird jedoch einer eingehenden Sicherheitsüberprüfung unterzogen und wird wahrscheinlich aus Sicherheitsgründen abgelehnt.

Beschränken Sie Berechtigungen mit IAM-Rollenrichtlinienerklärungen

AMS verwendet eine IAM-Rolle, um Benutzerberechtigungen über Ihren Verbunddienst festzulegen.

Einzelkonto Landing Zone AMS: Siehe [SALZ: Standard-IAM-Benutzerrollen](#).

Landing Zone AMS mit mehreren Konten: Siehe [MALZ: Standard-IAM-Benutzerrollen](#).

Eine IAM-Rolle ist eine IAM-Entität, die eine Reihe von Berechtigungen für das Stellen von Serviceanfragen definiert. AWS IAM-Rollen sind keinem bestimmten Benutzer oder keiner bestimmten Gruppe zugeordnet. Stattdessen übernehmen vertrauenswürdige Entitäten Rollen wie IAM-Benutzer, Anwendungen oder AWS Dienste wie Amazon EC2. Weitere Informationen finden Sie unter [IAM-Rollen](#).

Sie können die gewünschte Richtlinie für einen Benutzer, der die AMS-IAM-Benutzerrolle annimmt, mithilfe des API-Vorgangs AWS Security Token Service (STS) einschränken, [AssumeRole](#) indem Sie im Anforderungsfeld eine restriktivere IAM-Richtlinie angeben. Policy

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, mit denen Sie den CT-Zugriff einschränken können.

Mithilfe Ihrer konfigurierten Active Directory (AD) -Gruppen und der API-Operation [AssumeRole](#) AWS Security Token Service (STS) können Sie Berechtigungen für bestimmte Benutzer oder Gruppen festlegen, einschließlich der Beschränkung des Zugriffs auf bestimmte Änderungstypen (CTs). Sie können die unten aufgeführten Richtlinienerklärungen verwenden, um den CT-Zugriff auf verschiedene Arten einzuschränken.

AMS-Änderungstyp-Anweisung im Standard-IAM-Instanzprofil, die den Zugriff auf alle AMS-API-Aufrufe (`amscm` und `amsskms`) und alle Änderungstypen ermöglicht:

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
```



```

    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}

```

1. Anweisung zur Genehmigung des Zugriffs und aller Aktionen für nur zwei angegebene Benutzer CTs, wobei „Aktion“ für die AMS-API-Operationen (entweder amscm oder amsskms) und „Resource“ für den vorhandenen Änderungstyp und die Versionsnummer steht: IDs

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}

```

2. Anweisung, um den Zugriff für CreateRfc UpdateRfc, und nur für zwei SubmitRfc der angegebenen Daten zu gewähren CTs:
3. Anweisung, um den Zugriff für CreateRfc UpdateRfc, und SubmitRfc auf alle verfügbaren Daten zu gewähren CTs:
4. Erklärung zur Verweigerung des Zugriffs für alle Aktionen auf eingeschränktem CT und zur Zulassung anderer CTs:

Beschränken Sie Berechtigungen mit Amazon EC2 IAM-Instanzprofilen

Ein IAM-Instance-Profil ist ein Container für eine IAM-Rolle, den Sie verwenden können, um Rolleninformationen an eine EC2 Amazon-Instance zu übergeben, wenn die Instance gestartet wird.

Derzeit gibt es ein Standard-Instance-Profil für AWS Managed Services (AMS) `customer-mc-ec2-instance-profile`, das Berechtigungen für die Anwendungen gewährt, die auf der Instance ausgeführt werden, nicht für Benutzer, die sich bei der Instance anmelden. Möglicherweise möchten Sie das Standard-Instance-Profil ändern oder ein neues erstellen, wenn Sie einer Instance Zugriff auf etwas gewähren möchten, ohne anderen Instances ebenfalls Zugriff zu gewähren. Sie können mit dem Änderungstyp Verwaltung | Anwendungen | IAM-Instanzprofil | Änderungstyp erstellen (ct-0ixp4ch2tiu04) ein neues IAM-Instanzprofil anfordern. Wenn Sie den RFC einreichen, können Sie Ihr eigenes Instanzprofil erstellen und dieses als das angeben, oder Sie können AMS einfach (über dasselbe Feld) darüber informieren `InstanceProfileDescription`, welche Änderungen Sie wünschen. Da es sich um ein manuelles CT handelt, muss AMS die Änderung genehmigen und wird sich diesbezüglich mit Ihnen in Verbindung setzen.

Wenn Sie mit den Amazon IAM-Richtlinien nicht vertraut sind, finden Sie wichtige Informationen unter [Überblick über die IAM-Richtlinien](#). Es gibt auch einen guten Blogbeitrag, [Demystifying Amazon EC2 Resource-Level Permissions. Beachten Sie, dass AMS derzeit keine ressourcenbasierte Zugriffskontrolle unterstützt, aber Kontrollen auf Ressourcenebene mithilfe von IAM-Rollenrichtlinien unterstützt \(eine Erläuterung des Unterschieds finden Sie unter Services, die mit IAM funktionieren\).AWS](#)

Landing Zone AMS für ein Konto:

Eine Tabelle der Berechtigungen, die das standardmäßige AMS IAM-Instance-Profil gewährt, finden Sie unter [EC2 IAM-Instanzprofil](#).

AD FS-Anspruchsregel und SAML-Einstellungen

ActiveDirectory Federation Services (AD FS) -Anspruchsregel und SAML-Einstellungen für AWS Managed Services (AMS)

Ausführliche step-by-step Anweisungen zur Installation und Konfiguration von AD FS finden Sie unter [Enabling Federation to AWS Using Windows Active Directory, ADFS, and SAML 2.0](#).

Konfigurationen von ADFS-Anspruchsregeln

Wenn Sie bereits über eine ADFS-Implementierung verfügen, konfigurieren Sie Folgendes:

- Vertrauen der Parteien
- Regeln für Ansprüche

Die Schritte zur Vertrauens- und Anspruchsregeln der vertrauenden Partei werden vom [Blog Enabling Federation bis AWS Using Windows Active Directory, AD FS und SAML 2.0](#) durchgeführt

- Regeln für Ansprüche:
 - Nameid: Konfiguration pro Blogbeitrag
 - RoleSessionName: Konfigurieren Sie wie folgt
 - Name der Regel beanspruchen: **RoleSessionName**
 - Attributspeicher: **Active Directory**
 - LDAP-Attribut: **SAM-Account-Name**
 - Art des ausgehenden Anspruchs: **https://aws.amazon.com/SAML/Attributes/RoleSessionName**
 - AD-Gruppen abrufen: Konfiguration pro [Blogbeitrag](#)
 - Rollenanspruch: Konfigurieren Sie wie folgt

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^\d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([^\d]{12})-", "arn:aws:iam::$1:saml-provider/  
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Web-Konsole

Sie können auf die AWS-Webkonsole zugreifen, indem Sie den Link unten verwenden und ihn **[ADFS-FQDN]** durch den FQDN Ihrer ADFS-Implementierung ersetzen.

[https://\[ADFS-FQDN\].aspx adfs/ls/IdpInitiatedSignOn](https://[ADFS-FQDN].aspx adfs/ls/IdpInitiatedSignOn)

Ihre IT-Abteilung kann den oben genannten Link über eine Gruppenrichtlinie für die Benutzerpopulation bereitstellen.

API- und CLI-Zugriff mit SAML

So konfigurieren Sie den API- und CLI-Zugriff mit SAML.

Die Python-Pakete stammen aus den folgenden Blogbeiträgen:

- NTLM: [So implementieren Sie föderierten API- und CLI-Zugriff mit SAML 2.0 und AD FS](#)
- Formulare: [So implementieren Sie eine allgemeine Lösung für den API/CLI Verbundzugriff](#) mithilfe von SAML 2.0
- PowerShell: [So richten Sie den föderierten API-Zugriff auf AWS mithilfe von Windows](#) ein PowerShell

Skript-Konfiguration

1. Ändern Sie mit Notepad++ die Standardregion in die richtige Region
2. Deaktivieren Sie mit Notepad++ die SSL-Verifizierung für Test- und Entwicklungsumgebungen
3. Konfigurieren Sie mit Notepad++ idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?  
loginToRp=urn:amazon:webservices
```

Windows-Konfiguration

Die folgenden Anweisungen gelten für die Python-Pakete. Die generierten Anmeldeinformationen sind 1 Stunde gültig.

1. [Downloaden und installieren Sie Python \(2.7.11\)](#)
2. [Laden Sie die AWS-CLI-Tools herunter und installieren Sie sie](#)
3. Installieren Sie die AMS-CLI:
 - a. Laden Sie die ZIP-Datei für AMS-Distributionsdateien herunter, die Sie von Ihrem Cloud Service Delivery Manager (CSDM) erhalten haben, und entpacken Sie sie.

Es werden mehrere Verzeichnisse und Dateien zur Verfügung gestellt.
 - b. Öffnen Sie je nach Betriebssystem entweder das Verzeichnis Managed Cloud Distributables -> CLI -> Windows oder das Verzeichnis Managed Cloud Distributables -> CLI -> Linux/macOS und:

Führen Sie für Windows das entsprechende Installationsprogramm aus (diese Methode funktioniert nur auf Windows 32- oder 64-Bit-Systemen):

- 32 Bit: ManagedCloud API_x86.msi
- 64 Bit: ManagedCloud API_x64.msi

Führen Sie für Mac/Linux die Datei mit dem Namen MC_CLI.sh aus. Sie können dies tun, indem Sie diesen Befehl ausführen: `sh MC_CLI.sh` Beachten Sie, dass sich die Verzeichnisse amscm und amsskms sowie ihr Inhalt im selben Verzeichnis wie die Datei MC_CLI.sh befinden müssen.

- c. Wenn Ihre Unternehmensanmeldedaten über den Verbund mit AWS (die AMS-Standardkonfiguration) verwendet werden, müssen Sie ein Tool zur Verwaltung von Anmeldeinformationen installieren, das auf Ihren Verbundservice zugreifen kann. Sie können beispielsweise diesen AWS-Sicherheitsblog [How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS verwenden](#), um Hilfe bei der Konfiguration Ihrer Tools zur Verwaltung Ihrer Anmeldeinformationen zu erhalten.
- d. Führen Sie nach der Installation die Befehle und Optionen aus `aws amscm help` und sehen Sie `aws amsskms help` sich diese an.

4. Laden Sie das erforderliche SAML-Skript herunter

Laden Sie es auf `c:\aws\scripts` herunter

5. [Laden Sie PIP herunter](#)

Laden Sie es auf `c:\aws\downloads` herunter

6. Verwenden PowerShell und installieren Sie PIP

```
<pythondir>. \ python.exe c:\aws\downloads\get -pip.py
```

7. Verwenden PowerShell und installieren Sie das Boto-Modul

```
<pythondir\ scripts>Verwenden, installieren Sie das Boto-Modul ----sep----pip install boto
```

8. Verwenden Sie das Modul PowerShell Anfragen und installieren Sie es

```
<pythondir\ scripts>Verwenden des Moduls für Anfragen installieren ----sep----pip install requests
```

9. Verwenden PowerShell und installieren Sie das Sicherheitsmodul Anfragen

```
<pythondir\ scripts>Verwenden des Sicherheitsmoduls install requests ----sep----pip install requests [security]
```

10. Verwenden PowerShell und installieren Sie das BeautifulSoup-Modul

```
<pythondir\ scripts>Verwenden Sie das Modul beautifulsoup ----sep----pip install beautifulsoup4
```

11. Erstellen Sie mit Hilfe PowerShell eines Ordners namens `.aws` im Benutzerprofil (`%userprofile%\ .aws`)

```
mkdir .aws
```

12. Erstellen Sie mit PowerShell, eine Datei mit Anmeldeinformationen im Ordner „.aws“

Anmeldeinformationen für ein neues Objekt — Typ Datei —Force

Die Anmeldeinformationsdatei darf keine Dateierweiterung haben

Der Dateiname muss ausschließlich in Kleinbuchstaben geschrieben sein und die Anmeldeinformationen enthalten

13. Öffnen Sie die Anmeldeinformationsdatei mit Notepad und fügen Sie die folgenden Daten ein, wobei Sie die richtige Region angeben

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. Verwenden PowerShell des SAML-Skripts und der Anmeldung

```
<pythondir>. \ python.exe c:\aws\scripts\samlapi.py
```

Benutzername: [BENUTZERNAME] @upn

Wählen Sie die Rolle, die Sie übernehmen möchten

Linux-Konfiguration

Die generierten Anmeldeinformationen sind 1 Stunde gültig.

1. Übertragen Sie das SAML-Skript mithilfe von WinSCP
2. Übertragen Sie das Root-CA-Zertifikat mit WinSCP (ignorieren Sie es für Test und Entwicklung)
3. Fügen Sie die ROOT-CA zu den vertrauenswürdigen Root-Zertifikaten hinzu (ignorieren Sie sie für Test und Entwicklung)

\$ openssl x509 -inform der -in [certname] .cer -out certificate.pem (für Test und Entwicklung ignorieren)

Fügt den Inhalt von certificate.pem am Ende der Datei/-bundle.crt hinzu (bei Test-Entwicklung ignorieren) etc/ssl/certs/ca

4. Erstellen Sie den Ordner.aws unter home/ec2-user 5

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. Übertragen Sie die Anmeldeinformationsdatei mithilfe von WinSCP in den Ordner.aws
6. Installieren Sie das Boto-Modul

\$ sudo pip installiere Boto

7. Installieren Sie das Modul Anfragen

\$ sudo pip Installationsanfragen

8. Installieren Sie das BeautifulSoup-Modul

\$ sudo pip installiere beautifulsoup4

9. Kopieren Sie das Skript nach home/ec2-user

Stellen Sie die erforderlichen Berechtigungen ein

Führen Sie das Skript aus: samlapi.py

Mit Netzwerk-ACL einschränken

Eine Network Access Control List (NACL) ist eine optionale Sicherheitsebene für Ihre VPC, die als Firewall zur Steuerung des Datenverkehrs in und aus einem oder mehreren Subnetzen fungiert. Sie können ein Netzwerk ACLs mit Regeln einrichten, die Ihren Sicherheitsgruppen ähneln, um Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen. Weitere Informationen zu den Unterschieden zwischen Sicherheitsgruppen und Netzwerk ACLs finden Sie unter [Vergleich von Sicherheitsgruppen und Netzwerk ACLs](#).

Damit AMS die Infrastruktur effektiv verwalten und überwachen kann, NACLs ist die Verwendung von in AMS Managed Multi-Account Landing Zone jedoch auf folgenden Bereich beschränkt:

- NACLs werden in den Kernkonten für die Landing Zone mit mehreren Konten nicht unterstützt, d. h. Verwaltungskonto, Networking, Shared-Services, Protokollierung und Sicherheit.
- NACLs werden in Landing Zone-Application-Konten mit mehreren Konten unterstützt, sofern sie nur als Sperrliste verwendet werden und über die Option „Alle zulassen“ verfügen, um AMS-Überwachungs- und Verwaltungsvorgänge zu ermöglichen.

In großen Umgebungen mit mehreren Konten können Sie auch Funktionen wie zentralisierte Ausgangsfirewalls zur Steuerung des ausgehenden Datenverkehrs und/oder AWS Transit Gateway Gateway-Routingtabellen in der AMS Multi-Account Landing Zone nutzen, um den Netzwerkverkehr zwischen den einzelnen Konten zu trennen. VPCs

AMS auf Outposts

[AWS Outposts](#) ist eine verwaltete Hardwarelösung, die von AMS verwaltete Landezonen auf Kundenrechenzentren ausdehnt. Mit aktiviertem AMS-Support sind Kunden AWS Outposts, die das von AMS angebotene Cloud-Fachwissen, Kosteneinsparungen und die standardisierte Plattform suchen, nicht mehr darauf beschränkt, Ressourcen innerhalb des Unternehmens zu hosten AWS-Regionen. Wenn AMS aktiviert ist AWS Outposts, können Kunden mit On-Premise-Anforderungen nun das System modernisieren und gleichzeitig die von AMS angebotenen Services für Patching, Backup, Bereitstellung, Störungsmanagement, Geschäftskontinuität und Kostenoptimierung nutzen. AWS

Sobald ein in Ihrem AMS Multi-Account Landing Zone oder Single-Account Landing Zone Account aktiviert AWS Outposts ist, können Sie die bestehenden AMS-Change-Management-Prozesse zur Bereitstellung und Verwaltung von Ressourcen verfolgen. AWS Die von AMS gehostete Infrastruktur kann verwaltet werden, indem Sie Ihr spezifisches Subnetz angeben. AWS Outposts AWS Outposts Lebenszyklen können mithilfe der Rolle Self-Provisioning Services direkt in der AWS Outposts Konsole verwaltet werden. AWS Outposts

Informationen zur Rolle finden Sie unter. [AWS Outposts](#)

AWS Outposts Installations- und Betriebsmanagement

Der AWS Outposts Onboarding-Prozess bei AMS umfasst:

1. Planung von Outposts
2. Bestätigung der Bestellung
3. Outposts Onboarding bei AMS
4. Verwaltung des Lebenszyklus

AWS Outposts Planung

Während der AWS Outposts Planung identifizieren Sie AMS anhand von AWS Outposts Anwendungsfällen und binden wichtige Interessengruppen, einschließlich Ihres AMS-Kundenbetreuungsteams und Ihrer AWS Outposts Mitarbeiter, ein, um die Kapazitätsstrategie abzustimmen.

1. Sobald Anwendungsfälle identifiziert AWS Outposts wurden, für die AMS erforderlich ist, wenden Sie sich an Ihr AMS-Kundenbetreuungsteam, um die Kapazitätsplanung zu besprechen.
2. Sobald Ihre AWS Outposts Kapazitätsanforderungen festgelegt wurden, beauftragt Ihr AMS-Kundenbetreuungsteam das AWS Outposts Serviceteam, den AWS Outposts Onboarding-Plan, die Rollen und Verantwortlichkeiten zu besprechen. Während dieser Zeit wird AWS Outposts Ihnen ein einziger Ansprechpartner (SPOC) zugewiesen. Der AWS Outposts SPOC hilft Ihnen bei der Festlegung der Größenanforderungen. AWS Outposts

AWS Outposts Bestätigung der Bestellung

Während der Auftragsbestätigung erstellen Sie eine AWS Outposts Website und bestellen die benötigte Kapazität direkt in der AWS Outposts Konsole oder über Ihren AWS Outposts Kundenbetreuer.

Sobald Sie, das AMS-Kundenbetreuungsteam und das AWS Outposts Team sich einig sind, können Sie mithilfe der Änderungstyp-ID `ct-3qe6io8t6jtny` die AWS Outposts selbst bereitgestellte Servicrolle beantragen, um Ihre Site zu erstellen und direkt in der Konsole zu bestellen. AWS Outposts AWS Outposts

Alternativ können Sie den SPOC nutzen, um Outpost-Sites und Bestellungen zu erstellen. AWS Outposts Ihr AWS Outposts SPOC wird Sie und das AMS-Kundenbetreuungsteam während der Überprüfung der Website und der Bestellung sowie der Installation weiterhin mit Status-Updates versorgen. AWS Outposts

AWS Outposts Onboarding bei AMS

Sobald Ihr AWS Outposts Gerät in Ihrer von AMS verwalteten VPC aktiviert ist, können Sie beantragen, dass Monitore erstellt werden, um Verfügbarkeit, Kapazität, Ausnahmen und Netzwerkkonnektivität für Ihre Outposts-Hardware zu verfolgen. Wenn Sie die im Folgenden beschriebenen Schritte zur Bereitstellung der Überwachung befolgen, wird Ihre AWS Outposts Hardware aktiv von AMS überwacht.

1. Sobald Ihr System installiert und aktiviert AWS Outposts wurde, können Sie eine AWS Outposts spezifische Überwachung beantragen, indem Sie die folgende Vorlage zusammen mit einem RFC einreichen. Verwenden Sie dazu den Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76). AMS Operations stellt sicher, dass das Subnetz in den internen AMS-Tools nachverfolgt wird. AWS Outposts

- AWS Outposts ID
- Subnetz-CIDR
- Empfohlene AWS Outposts Alarme:
 - InstanceFamilyCapacityAvailabilityAlert
 - InstanceTypeCapacityAvailabilityAlert
 - EBSVolumeTypeCapacityAvailabilityAlert
 - CapacityExceptionsAlert
 - Direkte Connect ConnectionAlert
- Geben Sie für jede der oben genannten Benachrichtigungen die folgenden Parameter an:
 - Statistik („Durchschnitt“) wird empfohlen. Zu den weiteren Optionen gehören Summe, Maximum, Minimum, Stichprobenanzahl und p90)
 - Ein Zeitraum („5 Minuten“) wird empfohlen. Andere Optionen umfassen 10 und 30 Sekunden, 1, 5 und 15 Minuten, 1 und 6 Stunden und 1 Tag)
 - Der Schwellenwerttyp („Statisch“) wird empfohlen. „Anomalie“ sind ebenfalls Optionen.)
 - Bedingung („Immer wenn die Anzahl der Anrufe größer als“, „gleich“, „kleiner als“ ist, sind ebenfalls Optionen.)
 - Der Bedingungswert (“ 25% ") ist standardmäßig konfiguriert. Eine andere positive Ganzzahl ist zulässig.)
 - Thema für Benachrichtigungen (AMS-Betriebsthemen werden automatisch zugewiesen. Es kann jedoch auch jedes andere oder benutzerdefinierte Thema hinzugefügt werden.)

- AMS Operations überwacht AWS Outposts Messwerte für Netzwerkunterbrechungen oder Komponentenausfälle. AMS Operations bietet AWS Outposts Ersthelfer bei Problemen und leitet bei Bedarf an Premium-Support oder EC2 Support weiter.
 - AMS Operations steht zur Verfügung, um Probleme im Zusammenhang mit Ihrem AWS Outposts Gerät zu lösen.
3. Wenn die Überprüfung des EC2 Instance-Status oder des Systemstatus fehlschlägt, folgt AMS Operations den bestehenden Prozessen, um die Instance wieder online zu bringen. Wenn der Neustart fehlschlägt oder die AWS Outposts Kapazität nicht ausreicht, benachrichtigt Sie ein Mitglied des AMS-Betriebsteams direkt, um die nächsten Schritte festzulegen.

AWS Outposts Lebenszyklusmanagement

Sobald AWS Outposts Sie in Ihr AMS-Konto aufgenommen wurden, werden Sie benachrichtigt, wenn Verfügbarkeits-, Kapazitäts- oder Netzwerkausnahmen auftreten. Sie können die Außerbetriebnahme AWS Outposts direkt über die AWS Outposts Konsole oder den SPOC vornehmen. AWS Outposts

Sie können die Verwaltung AWS Outposts direkt in der AWS Outposts Konsole vornehmen, indem Sie die AWS Outposts Self-Service-Bereitstellungsdienstrolle oder den Entwicklermodus verwenden. Sie können die Anfrage auch AWS Outposts über Ihr CSDM (AWS Outposts Single Point of Contact, SPOC) stellen.

Eine hohe Verfügbarkeit AWS Outposts kann durch den Einsatz von zwei oder mehr erreicht werden. AWS Outposts Die Konfiguration von zwei oder mehr AWS Outposts aktiviert die Multi-Availability Zone-Option für Ihre Amazon Relational Database Service Service-Instances.

Bereitstellung von AMS-verwalteten Ressourcen auf AWS Outposts

Die Bereitstellung von AWS Ressourcen, die auf AWS Outposts (z. B. Amazon EC2, Amazon EMR, Amazon EKS, Amazon ECS, Amazon EBS und Amazon S3) in AMS-Konten (Single-Account Landing Zone, Multi-Account Landing Zone und Accelerate-Konten) gehostet werden, unterliegt denselben AMS-Supportstufen wie Ressourcen in AWS-Regionen Sie können das AMS-Änderungsmanagement, die Self-Service-Bereitstellungsdienste oder den Entwicklermodus verwenden, um die Ressourcen zu erstellen und zu ändern, die auf erstellt wurden. AWS Outposts

Derzeit sind alle Instance-Typen (m5/M5D, C5/C5D, R5/R5D, i3EN, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon EMR, Amazon Relational Database Service, Application Load Balancers und App Mesh Envoy Proxy direkt

auf verfügbar. DBs AWS Outposts Diese Ressourcen kommen für denselben AMS-Betriebssupport in Frage wie Ressourcen in bestehenden Regionen.

Einschränkungen von AMS bei AWS Outposts

- Die betriebliche Unterstützung für AWS Outposts-gehostete Ressourcen hängt von einer konsistenten Netzwerkkonnektivität ab. AWS Outposts Eine Netzwerkunterbrechung verhindert, dass AMS Operations Vorfälle oder Probleme beheben kann, die auf der getrennten AWS Outposts Einheit auftreten. Informationen zu AWS Outposts Service-Level-Eventualitäten von AMS finden Sie in den aktualisierten [AWS Service Level](#) Agreements (). SLAs
- Amazon Relational Database Service:
 - Der Änderungstyp „RDS erstellen“ (ct-2z60dyvto9g6c) aktiviert standardmäßig Multi-AZ und erfordert eine DB-Subnetzgruppe. DB-Subnetzgruppen benötigen zwei Subnetze in zwei separaten Availability Zones (AZ). Wenn Sie nur eine haben AWS Outposts, ist das Erstellen einer DB-Subnetzgruppe ein Problem, da AWS Outposts sie nur einer einzigen AZ zugewiesen sind. Gehen Sie wie folgt vor, um diese Einschränkung zu umgehen:
 1. Fordern Sie eine DB-Subnetzgruppe über einen RFC mit einem CTP Management | Other | Other an und geben Sie das Subnetz auf der an. AWS Outposts
 2. Erstellen Sie eine benutzerdefinierte CFN-Vorlage AWS Outposts, auf der RDS bereitgestellt werden soll, und geben Sie die im vorherigen Schritt erstellte Subnetzgruppe an. Weitere Informationen dazu finden Sie unter [Benutzerdefinierte](#) Ressourcen.
 3. Bitten Sie AMS, die CFN-Vorlage, die die Ziel-RDS-Instance enthält, über das AMS CFN-Ingest CT (ct-36cn2avfrj9v) bereitzustellen.
 4. Beachten Sie, dass RDS for derzeit aufgrund einer Einschränkung des RDS-Service AWS Outposts keine Metriken und Protokolle bereitstellt.
 - Workload ingest (WIGs): Linux funktioniert WIGs nur, wenn sich die WIGs EC2 Pre-Instance in einem AWS Outposts Nicht-Subnetz befindet. Der Grund dafür ist, dass Linux standardmäßig mit m4.large einen WIGs Knoten im Subnetz der ersten EC2 Instanz WIGs erstellt. AS AWS Outposts hat diesen Instance-Typ nicht und kann seinen WIGs Worker-Knoten nicht starten. Die Problemlösung hierfür besteht darin, die erste EC2 Instanz in einem AWS Outposts Nicht-Subnetz zu erstellen, auf der dann die Zielinstanz erstellt werden kann. AWS Outposts Darüber hinaus werden derzeit nur Nitro-basierte EC2 Instance-Typen wie C5, C5d, M5, M5d, R5, R5d, G4 und i3EN unterstützt. AWS Outposts

- Amazon Elastic Block Store (EBS): EBS Volume CT erstellen (ct-16xg8qguovg2w) funktioniert nicht, da Volumes in erstellt werden, AWS anstatt weil wir die AWS Outposts Amazon-Ressourcennummer (ARN) nicht AWS Outposts als Eingabeparameter für das CT angeben.
- AWS Outposts Netzwerkkonnektivität: Die Netzwerkkonnektivität liegt in Ihrer Verantwortung pro Team.
- Brownfield und Kontoübernahme: AWS Outposts Aktivierte Konten, die nicht von AMS stammen, können aufgrund der Art der AWS Outposts Abrechnung und der Anforderungen an den Unternehmenssupport nicht auf AMS übertragen werden.

AMS zur Einhaltung gesetzlicher Vorschriften AWS Outposts

AMS bei AWS Outposts Konformitätsbescheinigung

AWS Outposts Der Kontrollebene wurde die HIPAA-Zertifizierung sowie die PCI- und ISO-Konformität bescheinigt. Für AMS auf der AWS Outposts Kontrollebene wurde jedoch kein Nachweis erbracht. AWS Outposts Aus diesem Grund werden Kunden dazu angehalten, eine AMS-Konformitätsbescheinigung für Umweltfragen beantragen zu lassen. AWS Outposts

Um die Bereitstellung von Ressourcen auf der Outpost-Einheit zu kontrollieren, wird den Kunden empfohlen, den Entwicklerzugriff auf den Outpost zu trennen, um zu verhindern, dass Entwickler in standardmäßigen AMS-verwalteten Konten übermäßigen Zugriff haben.

Von AMS verwaltete Workloads, für die FedRAMP-Konformität erforderlich ist

In erster Linie müssen AMS-Verwaltungskonten zunächst auf ihre Einhaltung gesetzlicher Vorschriften hin überprüft werden, da die Daten auf der Kontrollebene aus den AWS Outposts AMS-Verwaltungskonten fließen würden.

Wenn eine FedRAMP-Zertifizierung erforderlich ist und die AMS-Kontostruktur konform ist, wird empfohlen, dass Sie entweder einen Rechenzentrumsanbieter verwenden, der bereits über die erforderliche Zertifizierung verfügt und die gesamte Service Link-Appliance besitzt (oder die Ausgangsdaten bereits verschlüsselt).

Schließlich kann zusätzlicher Datenschutz eingeführt werden, indem Sie mit Ihrem Account-Team zusammenarbeiten, um ein SCP einzurichten, das Daten auf den beschränkt AWS Outposts und die Erstellung von Ressourcen in der Region in dem Konto verhindert, auf dem der Outpost gehostet wird.

Auswirkungen auf die bestehende Compliance für AMS-Konten

Ein Konto, das ein Konto verwendet, muss AWS Outposts nicht erneut auf die Einhaltung der Vorschriften getestet werden, solange keine regulierten Daten verwendet werden und das Konto logisch getrennt ist. AMS-Verwaltungskonten können nicht regulierte und regulierte Konten verwalten, sofern kontenübergreifende Datenflüsse authentication/authorization und eingehende und ausgehende Datenflüsse voneinander getrennt werden. VPCs Obwohl sich sowohl das nicht konforme Outpost-Konto als auch die bestehenden kompatiblen Anwendungskonten in derselben Organisation befinden (einschließlich Shared Services, Networking, Logging, Master- und Sicherheits-AMS-Services), bleibt das Compliance-Anwendungskonto dennoch konform, da die Daten logisch getrennt sind.

AMS ist aktiviert AWS Outposts FAQs

In welchen Anwendungsfällen kann AMS-Support in Anspruch genommen werden AWS Outposts?

AMS on AWS Outposts kann von Unternehmen genutzt werden, die ein bewährtes Cloud-Betriebsmodell benötigen, über Workloads verfügen, die eine geringe Latenz erfordern (z. B. Verwaltung von Werksrobotern und Mainframe-Migration), Edge-Computing (z. B. Remote-Workstations und Edge-Datenoptimierung) und große Datenübertragungslasten erfordern.

Warum sollte ich diese Funktion verwenden?

AMS bietet die Überwachung der AWS Outposts Hardware und die Erstreaktion bei Hardwareproblemen. AWS Outposts Darüber hinaus stehen die folgenden Support-Funktionen für alle verwalteten Ressourcen zur Verfügung, die auf folgender Website gehostet werden AWS Outposts:

- Protokollierung, Überwachung, Guardrails und Eventmanagement
- Kontinuitätsmanagement
- Sicherheits- und Zugriffsmanagement
- Patch-Management
- Änderungsmanagement
- Automatisiertes Bereitstellungsmanagement mit Self-Service
- Vorfalls- und Problemmanagement
- Berichterstattung (Berichte für AWS Outposts Hardware werden zunächst nicht unterstützt, wenn AMS aktiviert ist AWS Outposts)

- Verwaltung von Serviceanfragen
- Entwicklermodus
- Support für Unternehmen

Wie verwende ich diese Funktion?

AWS Outposts Planung: Während der AWS Outposts Planung haben Sie AMS anhand von AWS Outposts Anwendungsfällen identifiziert und werden wichtige Interessengruppen, darunter das AMS-Kundenbetreuungsteam und AWS Outposts Vertreter, einbeziehen, um die Kapazitätsstrategie abzustimmen.

Auftragsbestätigung: Während der Auftragsvalidierung erstellen Sie eine AWS Outposts Website und bestellen die benötigte Kapazität direkt in der AWS Outposts Konsole oder über Ihren AWS Outposts Kundenbetreuer.

AWS Outposts Onboarding bei AMS: Sobald Ihre AWS Outposts Einheit in Ihrer von AMS verwalteten VPC aktiviert ist, können Sie beantragen, dass Sie in Ihr AMS-Konto aufgenommen werden, indem Sie mithilfe der Vorlage im AMS-Benutzerhandbuch () einen Änderungsantrag (RFC) einreichen. [AWS Outposts](#) AMS Operations erstellt dann ein Subnetz und überwacht Ihren Outpost mithilfe der im RFC bereitgestellten Eingaben.

Lebenszyklusmanagement: Sobald Sie Ihrem AMS-Konto hinzugefügt wurden, werden Sie AWS Outposts über alle Verfügbarkeits-, Kapazitäts- oder Netzwerkausnahmen informiert. Sie können die Inbetriebnahme AWS Outposts direkt über die AWS Outposts Konsole oder Ihren AWS Outposts zentralen Ansprechpartner (SPOC) vornehmen.

Worin bestehen die Einschränkungen von AMS? AWS Outposts

Anwendungsfälle für den Datenstandort (z. B. landesspezifische Gesetze zur Datenlokalisierung usw.) wurden für AMS am noch nicht validiert. AWS Outposts

AWS Outposts Aktivierte Konten, die nicht zu AMS gehören, können aufgrund der Art der AWS Outposts Abrechnung und der Anforderungen an den Enterprise Support nicht auf AMS übertragen werden.

AWS Outposts Die Kontrollebene wurde bescheinigt, dass sie HIPAA-fähig ist und PCI- und ISO-konform ist. Für AMS auf der AWS Outposts Kontrollebene wurde jedoch kein Nachweis erbracht. AWS Outposts Aus diesem Grund werden Kunden dazu angehalten, eine AMS-Konformitätsbescheinigung für Umweltfragen beantragen zu lassen. AWS Outposts

Kann ich diese Funktion deaktivieren?

Die Bereitstellung AWS Outposts in Ihrer AMS-Umgebung ist optional. Nach der Bereitstellung in Ihrem AMS-Konto AWS Outposts kann die Bereitstellung jederzeit über die AWS Outposts Konsole aufgehoben werden, falls sie nicht mehr benötigt wird.

Wie wird AMS on abgerechnet AWS Outposts ?

Die AWS Outposts AMS-Gebührenerhöhung wird für die Stufe Gruppe B berechnet.

Wie wird sich das AMS Service Level Agreement ändern, um dem Rechnung zu tragen? AWS Outposts

Das Incident-Management hängt von der Verfügbarkeit ab AWS Outposts . AWS Outposts Die Verfügbarkeit hängt von der Verfügbarkeit des Kundennetzwerks ab, für die der Kunde selbst verantwortlich ist. AWS Outposts Die Verfügbarkeit hängt auch von der Verfügbarkeit der AWS Outposts Hardware ab, die von AWS Outposts Service Level Agreements abhängt.

Siehe auch [AWS Outposts FAQs](#).

Verwenden von Tags in AMS

Themen

- [Automatisches Tagging der AMS-Infrastruktur](#)
- [Von AMS empfohlene Tags](#)
- [Notizen zu Massenaktualisierungen taggen](#)

Die Bereitstellung von Tags kann von großem Wert sein. Ausführliche Informationen finden Sie unter [Tagging Your Amazon EC2 Resources](#).

RFCs die Instances erstellen, wie z. B. einen Amazon S3 S3-Bucket oder einen AWS Elastic Load Balancer (ELB), bieten in der Regel ein Schema, mit dem Sie bis zu sieben Tags (Schlüssel/Wert-Paare) hinzufügen können. Sie können Ihrem S3-Bucket weitere Tags hinzufügen, indem Sie ein Management | Advanced Stack Components | Amazon S3 S3-Speicher | Update CT einreichen. Amazon EC2, Amazon EFS, Amazon RDS und die mehrstufigen Schemas (HA Two-Tiered und HA One-Tiered) ermöglichen bis zu fünfzig Tags. Tags werden im Teil des Schemas angegeben. ExecutionParameters

Wenn Sie die AMS-Konsole verwenden, müssen Sie die Ansicht Zusätzliche Konfiguration aktivieren, um Tags hinzuzufügen.

 Tip

Viele CT-Schemas haben ein Description Name UND-Feld am oberen Rand des Schemas. Diese Felder werden verwendet, um den Stack oder die Stack-Komponente zu benennen, sie benennen nicht die Ressource, die Sie erstellen. Einige Schemas bieten einen Parameter zum Benennen der Ressource, die Sie erstellen, andere nicht. Beispielsweise bietet das CT-Schema für Create Amazon EC2 Stack keinen Parameter zum Benennen der EC2 Amazon-Instance. Dazu müssen Sie ein Tag mit dem Schlüssel „Name“ und dem Wert, den der Name haben soll, erstellen. Wenn Sie kein solches Tag erstellen, wird Ihre EC2 Amazon-Instance in der EC2 Amazon-Konsole ohne ein Namensattribut angezeigt.

Gibt es Tag-Einschränkungen? Ja:

- Bei Tags muss die Groß- und Kleinschreibung beachtet werden.
- Die maximale Schlüssellänge beträgt 128 Unicode-Zeichen.
- Die maximale Wertlänge beträgt 256 Unicode-Zeichen.
- Die maximale Anzahl an Tags pro Ressource beträgt 50.
- Das reservierte Präfix ist aws : .
- Namen und Werte der von AWS generierten Tags wird automatisch das aws : -Präfix zugewiesen, das Sie nicht zuweisen können. Benutzerdefinierte Tag-Namen haben das Präfix user : im Kostenzuordnungsbericht.
- Verwenden Sie jeden Schlüssel nur einmal für jede Ressource. Wenn Sie versuchen, denselben Schlüssel zweimal für dieselbe Ressource zu verwenden, wird Ihre Anfrage abgelehnt.
- Zulässige Zeichen sind Unicode-Buchstaben, Leerzeichen, Zahlen und die folgenden Sonderzeichen: + - =. _:/

Welche AWS Ressourcentypen unterstützen Tags? Weitere Informationen finden Sie unter [Organisieren Sie jetzt Ihre AWS Ressourcen mithilfe von bis zu 50 Tags pro Ressource](#).

Automatisches Tagging der AMS-Infrastruktur

AMS kann alle Ressourcen, die von AMS zu Verwaltungszwecken erstellt wurden, in Ihren Konten mit mehreren Konten für landing zone (MALZ) und Einzelkonten für landing zone (SALZ) über einen Änderungsantrag (RFC) mit dem Änderungstyp Deployment | Advanced Stack components | Tag | Create (review required) (ct-0176f0n99vcps) taggen. Dies kann Ihnen bei der Identifizierung von Ressourcen helfen, die von AMS zu Verwaltungszwecken erstellt wurden.

AMS kann von AMS erstellte Ressourcen anhand der Benennungsstandards automatisch identifizieren und prüfen, ob die Ressource die folgenden Tag-Schlüssel und Werte hat: `AppName`: `""`, `AppId`: `""`, `AMSResource` und `EnvironmentType`. Wenn der Tag-Schlüssel nicht existiert oder der Wert leer ist, können diese Tag-Schlüssel automatisch von AMS mit dem Tag-Wert `""` erstellt werden. `AMSInfrastructure`

Sie können die gewünschten Tags für von AMS erstellte Ressourcen auf der Grundlage der Tagging-Standards Ihrer Organisation anpassen. Sie können Ihre eigenen Tag-Schlüssel und Tag-Werte angeben, wenn Sie die Anfrage an AMS senden. [Halten Sie sich an die folgenden Standards für die Benennung von AWS Tags: Bewährte Methoden für Tagging](#)

Note

Für MALZ-Konten wird das benutzerdefinierte Tagging der AMS-Infrastruktur nur für Anwendungskonten unterstützt. Benutzerdefiniertes Tagging für Kernkonten wird derzeit nicht unterstützt.

Wenn der Tag-Schlüsselname, den Sie in Ihrem RFC angeben, bereits auf der Ressource existiert, wird der Tag-Wert durch den neuen Tag-Wert ersetzt, den Sie im RFC angegeben haben.

Die Gesamtlänge der Tag-Schlüssel/Wert-Paare darf 256 Zeichen nicht überschreiten.

Nehmen Sie die folgenden Informationen mit dem Änderungstyp Deployment | Advanced stack components | Tag | Create (review erforderlich) (ct-0176f0n99vcps) zur Kennzeichnung von AMS-erstellten Ressourcen in Ihren RFC auf.

1. Liste der Landingzone-Konten mit mehreren Konten oder Landingzone-Konten mit einem Konto, für die Sie von AMS erstellte Ressourcen zu Verwaltungszwecken taggen möchten.
2. Erforderlicher Tag-Schlüsselname und Tag-Wert (falls erforderlich). Standardmäßig kann AMS Tags mit dem Tag-Schlüsselnamen `""` und dem Tag-Wert als `"EnvironmentType"` versehen.

AMSInfrastructure [Wenn Sie einen benutzerdefinierten Tag-Schlüsselnamen und einen Tag-Wert benötigen, befolgen Sie die Standards für die Tag-Benennung: Best Practices für Tagging AWS](#)

Diese Ressourcen werden derzeit von AMS Infrastructure Tagging unterstützt:

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
Elastic Load Balancing
```

* „arn:aws:s3::awsms-a*-patch-data-*“, „arn:aws:s3::ams-a*-log-management-*“, „arn:aws:s3::cf-templates-*“, „arn:aws:s3::mc-a*“, „arn:aws:s3::ams-a*-backup-reports-*“, „arn:aws:s3::ams-a*-“*, „arn:aws:s3::ams-a*-“*, „arn:aws:s3::ams-a*-“*, „arn:aws:s3::ams-a*-release-assets-*“, „arn:aws:s3:::“* patch-data-customer-reports patch-data-raw patch-data-reporting ams-cfn-drift-remediation ams-reporting-data-a

Von AMS empfohlene Tags

AMS empfiehlt die folgenden Tags für unterstützte Ressourcen. Mit einem Stern (*) markierte Tags werden dringend empfohlen.

Note

Sie können Tags verwenden, um Patches zu planen. Weitere Informationen finden Sie unter [AMS Advanced Patch Orchestrator: ein tagbasiertes Patching-Modell](#).

Reservierte AMS-Präfixe

AMS-Ressourcenattribute müssen bestimmten Mustern entsprechen. Beispielsweise dürfen Profilnamen, Namen, BackupVault Tagnamen usw. von IAM-Instanzen nicht mit reservierten AMS-Präfixen beginnen. Diese reservierten Präfixe sind:

```
*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

Von AMS empfohlene Tags

Tag-Schlüssel	Unterstützte Werte	Hinweise
AppName*	Uneingeschränkt.	Identifizieren Sie die Anwendungen, die sich auf der Ressource befinden oder Zugriff darauf benötigen. Dies erleichtert die Nachverfolgung und Kommunikation zwischen AMS und Ihnen.
AppId*		
EnvironmentType *		
OwnerTeamEmail *	E-Mail-Adresse der Verteilerliste	Identifizieren Sie die E-Mail-Adresse der Verteilerliste für das Team, das für die Ressource verantwortlich ist. Bei der E-Mail sollte es sich nicht um eine persönliche E-Mail handeln. Es muss sich um eine anonyme E-Mail wie eine Verteilerliste handeln.
ComplianceFramework	Uneingeschränkt	Identifizieren Sie, welche Kontrollen und Richtlinien auf die Ressource angewendet werden sollen.
CostCenter		Identifizieren Sie die Kostenstelle oder Geschäftseinheit, die einer Ressource zugeordnet ist (in der Regel für die Kostenzuweisung und -verfolgung).
Customer		Wird von AMS-Kunden verwendet, die über Ressourcen von mehreren Kunden verfügen (AMS-Unterkunden). Um Ressourcen in der verwalteten Umgebung dem jeweiligen Kunden zuzuordnen, für den sie zuständig sind. Identifizieren Sie einen bestimmten

Tag-Schlüssel	Unterstützte Werte	Hinweise
		Kunden für eine bestimmte Gruppe von Ressourcen oder Diensten.
DataClassification		Identifizieren Sie die spezifische Datenvertraulichkeitsstufe, die eine Ressource unterstützt. Identifizieren Sie, welche Kontrollen und Richtlinien auf die Ressource angewendet werden sollten.
HoursOfOperation		Identifizieren Sie das Datum oder die Uhrzeit, zu der eine Ressource gestartet , gestoppt, gelöscht oder rotiert werden soll.
OwnerTeam		Identifizieren Sie das Team, das für die Ressource verantwortlich ist. Erleichtert die Kommunikation mit dem für die Ressource verantwortlichen Team.

Tag-Schlüssel	Unterstützte Werte	Hinweise
Patch Group	Sie haben hierfür zwei Möglichkeiten: - Sie können eine Serviceanfrage mit den in AMS Advanced Patch Orchestra tor beschriebenen Informationen einreichen. Dabei handelt es sich um ein tagbasiertes Patch-Modell, und AMS erstellt auf Ihren angegebenen Ressourcen und unter Verwendung der von Ihnen bereitgestellten Informationen ein Patch Group Tag für Sie. - Wenn Sie bereits ein Patch Group Tag für Ihre Ressourcen erstellt haben, gelten für die unterstützten Werte keine Einschränkungen.	Welche Ressourcen sollten in ein automatisiertes Patch-Wartungsfenster aufgenommen werden?
ProjectId	Uneingeschränkt	Identifizieren Sie die Projekte, die die Ressource unterstützt.

Tag-Schlüssel	Unterstützte Werte	Hinweise
SupportPriority	Eines von sechs möglichen Akronymen für Vertraulichkeit, Integrität oder Verfügbarkeit. Die Reihenfolge der Abkürzung hat Priorität. I.C.A. würde beispielsweise bedeuten, dass die Reihenfolge Integrität, Vertraulichkeit, Verfügbarkeit lautet. Andere akzeptable Werte sind C.I.A., C.A.I., I.A.C., A.C.I. und A.I.C.	Identifizieren Sie, welche Art von Support Priorität haben sollte: Vertraulichkeit, Integrität oder Verfügbarkeit.

Notizen zu Massenaktualisierungen taggen

Diese Hinweise beziehen sich auf die exemplarischen Vorgehensweisen für den Änderungstyp [Tag | Bulk Update und Tag | Bulk Update \(Review Required\)](#).

Hinweise zu Tags für Massenaktualisierungen:

- Unterstützte Dienste:
 - Für [Schlagwort | Bulk-Update \(Überprüfung erforderlich\)](#): Alle.
 - Für [Schlagwort | Bulk-Update](#):
 - Auto Scaling
 - Amazon EC2
 - Elastic Load Balancing
 - Amazon RDS
 - Amazon-S3-Buckets
- Um die Datei mit kommagetrennten Werten (CSV) zu generieren, melden Sie sich in der AWS Konsole bei Resource Groups > Tag Editor an, suchen Sie die Ressourcen, die Sie taggen

möchten, und exportieren Sie sie dann in eine CSV-Datei. Weitere Informationen finden Sie unter [Ergebnisse nach CSV exportieren](#).

HINWEIS: Wir empfehlen die Verwendung einer vorsignierten S3-URL für die Angabe des Speicherorts des CSV-Objekts.

- Es müssen Spalten mit den Überschriften Service, Type und Identifier vorhanden sein. Diese Spalten sind Pflichtfelder.
- Benennen Sie die Spalte Identifier in ID um.
- Die Werte für die Spalten Service, Type und Identifier (geändert in ID) entsprechen den Angaben des Tag-Editors unter Resource Groups.
- Wenn eine zu markierende Ressource im Tag Editor nicht verfügbar ist, verwenden Sie den Amazon-Ressourcennamen (ARN) der Ressource für die Spalte Identifier (geändert in ID) und lassen Sie Service und Type leer.
- Die Spaltenüberschriften der Tags, die hinzugefügt oder geändert werden sollen, müssen das Format Tag: **TagKey** haben.
- Die Spaltenüberschriften der zu löschenden Tags müssen das Format Untag: haben. **TagKey**
- Jede Zeile ist für eine Ressource vorgesehen, die markiert oder nicht markiert werden soll.
- Wenn einer Ressource ein Tag hinzugefügt werden soll, geben Sie den Wert des Tags in der entsprechenden **TagKey** Spalte Tag: an.
- Wenn ein Tag aus einer Ressource gelöscht werden soll, geben Sie in der entsprechenden **TagKey** Spalte Untag: den Wert True ein.
- Wenn ein Tag: **TagKey** oder Untag: **TagKey** auf eine Ressource nicht zutrifft, fügen Sie der entsprechenden Spalte einen Bindestrich (-) hinzu oder lassen Sie das Feld leer.

HINWEIS: Das Untag hat Vorrang vor dem Tag. Das liegt daran, dass Untag im Gegensatz zu Tag manuell zur CSV-Datei hinzugefügt werden muss. Wir gehen also davon aus, dass das Tag entfernt und nicht geändert werden sollte.

- Alle zusätzlichen Spalten, die den Kriterien nicht entsprechen, werden ignoriert.

Important

Beim Export des Tag-Editors wird eine Matrix mit allen Tags für alle Ressourcen aufgefüllt. Fehlende Tags werden mit dem Wert „nicht markiert“ aufgefüllt. Die Wiederverwendung

dieser Export-CSV als Eingabe für den RFC führt dazu, dass alle zuvor fehlenden Tags mit dem Literalwert „nicht markiert“ erstellt werden.

 Note

Informationen zum Exportieren von Tags in eine CSV-Datei [finden Sie unter Ressourcen zum Taggen suchen -> Ergebnisse in CSV exportieren](#).

Ressourcenplaner für AWS Managed Services

Verwenden Sie den AWS Managed Services (AMS) Resource Scheduler, um den automatischen Start und Stopp von AutoScaling Gruppen, EC2 Amazon-Instances und RDS-Instances in Ihrem Konto zu planen. Dies trägt dazu bei, die Infrastrukturkosten dort zu senken, wo die Ressourcen nicht rund um die Uhr laufen sollen. Die Lösung baut auf [Instance Scheduler auf AWS](#), enthält jedoch zusätzliche Funktionen und Anpassungen, die speziell auf die AMS-Bedürfnisse zugeschnitten sind.

 Note

Standardmäßig interagiert AMS Resource Scheduler nicht mit Ressourcen, die nicht Teil eines Stacks sind. AWS CloudFormation Die Ressource muss Teil eines Stacks sein, der mit „stack-“, „sc-“ oder „SC-“ beginnt. Um die Ressourcen zu planen, die nicht Teil eines CloudFormation Stacks sind, können Sie den Stackparameter Resource Scheduler `ScheduleNonStackResources` auf Yes aktualisieren.

AMS Resource Scheduler verwendet Zeiträume und Zeitpläne:

- Perioden definieren die Zeiten, zu denen Resource Scheduler ausgeführt wird, z. B. Startzeit, Endzeit und Tage des Monats.
- Zeitpläne enthalten Ihre definierten Zeiträume sowie zusätzliche Konfigurationen wie SSM-Wartungsfenster, Zeitzone, Ruhezustand usw. und geben anhand der konfigurierten Periodenregeln an, wann Ressourcen ausgeführt werden sollen.

Sie können diese Zeiträume und Zeitpläne mithilfe der automatisierten Änderungstypen () von AMS Resource Scheduler konfigurieren. CTs

[Vollständige Informationen zu den für AMS Resource Scheduler verfügbaren Einstellungen finden Sie in der entsprechenden AWS Instance Scheduler-Dokumentation unter Lösungskomponenten. Eine architektonische Ansicht der Lösung finden Sie in der entsprechenden AWS Instance Scheduler-Dokumentation unter \[Architecture overview.html\]\(#\).](#)

Bereitstellung von AMS Resource Scheduler

Um AMS Resource Scheduler bereitzustellen, verwenden Sie den automatisierten Änderungstyp (CT): Deployment | AMS Resource Scheduler | Solution | Deploy (ct-0ywnhc8e5k9z5), um einen RFC auszulösen, der dann die Lösung in Ihrem Konto bereitstellt. Sobald der RFC ausgeführt wurde, wird Ihrem Konto automatisch ein CloudFormation Stack bereitgestellt, der AMS Resource Scheduler-Ressourcen mit Standardkonfiguration enthält. [Weitere Informationen zu den Änderungstypen von Resource Scheduler finden Sie unter AMS Resource Scheduler.](#)

Note

Um herauszufinden, ob AMS Resource Scheduler bereits in Ihrem Konto bereitgestellt ist, überprüfen Sie die AWS Lambda-Konsole für dieses Konto und suchen Sie nach der AMSResourceScheduler-Funktion.

Nachdem der AMS Resource Scheduler in Ihrem Konto bereitgestellt wurde, empfehlen wir Ihnen, die Standardkonfiguration zu überprüfen und bei Bedarf Konfigurationen wie Tag-Schlüssel, Zeitzone, geplante Dienste usw. an Ihre Präferenzen anzupassen. Einzelheiten zu den empfohlenen Anpassungen finden Sie unter Weiter. [AMS Resource Scheduler anpassen](#)

Um die benutzerdefinierten Konfigurationen vorzunehmen oder einfach die Resource Scheduler-Konfiguration zu bestätigen,

AMS Resource Scheduler anpassen

[Wir empfehlen Ihnen, die folgenden Eigenschaften von AMS Resource Scheduler mithilfe der aktualisierten AMS Resource Scheduler-Änderungstypen anzupassen, siehe AMS Resource Scheduler.](#)

- Tagname: Der Name des Tags, das Resource Scheduler verwendet, um Instanzpläne mit Ressourcen zu verknüpfen. Der Standardwert ist Schedule.

- **Geplante Dienste:** Eine durch Kommas getrennte Liste von Diensten, die Resource Scheduler verwalten kann. Der Standardwert ist „ec2, rds, autoscaling“. Gültige Werte sind „ec2“, „rds“ und „autoscaling“
- **Standardzeitzone:** Geben Sie die Standardzeitzone an, die der Resource Scheduler verwenden soll. Der Standardwert ist UTC.
- **Verwenden Sie CMK:** Eine durch Kommas getrennte Liste von Amazon KMS Customer Managed Key (CMK) ARNs, für die Resource Scheduler Berechtigungen erteilt werden können.
- **Verwendung LicenseManager:** Eine durch Kommas getrennte Liste der AWS Lizenzmanager, für die Resource Scheduler ARNs Berechtigungen erteilt werden können.

Note

AMS kann von Zeit zu Zeit Funktionen und Korrekturen veröffentlichen, um AMS Resource Scheduler in Ihrem Konto auf dem neuesten Stand zu halten. In diesem Fall bleiben alle Anpassungen, die Sie am AMS Resource Scheduler vornehmen, erhalten.

AMS Resource Scheduler verwenden

Um AMS Resource Scheduler nach der Bereitstellung der Lösung zu konfigurieren, verwenden Sie den automatisierten Resource Scheduler, CTs um AMS Resource Scheduler-Perioden (die Zeiten, zu denen Resource Scheduler ausgeführt wird) und Zeitpläne (die konfigurierten Zeiträume und andere Optionen) zu erstellen, zu löschen, zu aktualisieren und zu beschreiben (Details zu erhalten). [Ein Beispiel für die Verwendung der Änderungstypen des AMS Resource Scheduler finden Sie unter AMS Resource Scheduler.](#)

Um Ressourcen auszuwählen, die von AMS Resource Scheduler verwaltet werden sollen, verwenden Sie nach der Bereitstellung und Erstellung des Zeitplans das AMS-Tag Create, CTs um Auto Scaling Scaling-Gruppen, Amazon RDS-Stacks und EC2 Amazon-Ressourcen mit dem Tag-Schlüssel, den Sie bei der Bereitstellung angegeben haben, und dem definierten Zeitplan als Tag-Wert zu taggen. Nachdem die Ressourcen markiert wurden, werden die Ressourcen gemäß Ihrem definierten Resource Scheduler-Zeitplan für den Start oder Stopp geplant.

Für die Nutzung von AMS Resource Scheduler fallen keine zusätzlichen Kosten an. Die Lösung verwendet jedoch mehrere, AWS-Services und diese Ressourcen werden Ihnen je nach Nutzung in Rechnung gestellt. Weitere Informationen finden Sie unter [Überblick über die Architektur](#).

Um AMS Resource Scheduler zu deaktivieren:

- Zur vorübergehenden Deaktivierung oder Deaktivierung: Senden Sie einen RFC über den automatisierten Änderungstyp Management | AMS Resource Scheduler | State | Disable (ct-14v49adibs4db)
- Zur dauerhaften Entfernung: Reichen Sie einen RFC für Management | Sonstige | Andere | Aktualisierung (Überprüfung erforderlich) (ct-0xdawir96cy7k) ein, der die Entfernung aus dem Release-Automatisierungssystem von Resource Scheduler anfordert

Kostenschätzer für AMS Resource Scheduler

Um Kosteneinsparungen nachzuverfolgen, bietet AMS Resource Scheduler eine Komponente, die stündlich die geschätzten Kosteneinsparungen für Amazon EC2 - und RDS-Ressourcen berechnet, die vom Scheduler verwaltet werden. Diese Daten zu den Kosteneinsparungen werden dann als CloudWatch Metrik (AMS/ResourceScheduler) veröffentlicht, um Ihnen zu helfen, sie nachzuverfolgen. Der Kosteneinsparungsschätzer schätzt nur die Einsparungen bei den Betriebsstunden der Instance. Andere Kosten, wie z. B. die mit einer Ressource verbundenen Datenübertragungskosten, werden nicht berücksichtigt.

Der Kosteneinsparungsrechner ist mit Resource Scheduler aktiviert. Er läuft stündlich und ruft Kosten- und Nutzungsdaten von ab. AWS Cost Explorer Aus diesen Daten berechnet es die durchschnittlichen Kosten pro Stunde für jeden Instanztyp und prognostiziert dann die Kosten für einen ganzen Tag, wenn die Instanz ohne Zeitplan ausgeführt wurde. Die Kosteneinsparungen sind die Differenz zwischen den prognostizierten Kosten und den tatsächlich gemeldeten Kosten aus dem Cost Explorer für einen bestimmten Tag.

Wenn Instanz A beispielsweise so konfiguriert ist, dass Resource Scheduler von 9.00 Uhr bis 17.00 Uhr ausgeführt wird, sind das acht Stunden an einem bestimmten Tag. Cost Explorer meldet die Kosten mit 1\$ und die Nutzung mit 8. Die durchschnittlichen Kosten pro Stunde betragen daher 0,125\$. Wenn die Instanz nicht mit Resource Scheduler geplant wurde, würde die Instanz an diesem Tag rund um die Uhr laufen. In diesem Fall hätten die Kosten $24 \times 0,125 = 3\$$ betragen. Resource Scheduler hat Ihnen geholfen, Kosteneinsparungen von 2\$ zu erzielen.

Damit der Kosteneinsparungsschätzer Kosten und Nutzung nur für Ressourcen abrufen kann, die von Resource Scheduler aus dem Cost Explorer verwaltet werden, muss der Tag-Schlüssel, den Resource Scheduler für die Ausrichtung von Ressourcen verwendet, als Kostenzuordnungs-Tag im Fakturierungs-Dashboard aktiviert werden. Wenn das Konto zu einer Organisation gehört, muss der Tag-Schlüssel im Verwaltungskonto der Organisation aktiviert werden. Informationen dazu finden

Sie unter Benutzerdefinierte [Kostenverrechnungs-Tags und Benutzerdefinierte Kostenverrechnungs-Tags aktivieren](#)

Nachdem der Tag-Schlüssel als Cost Allocation Tag aktiviert wurde, beginnt die AWS Fakturierung mit der Erfassung der Kosten und der Nutzung der von Resource Scheduler verwalteten Ressourcen. Sobald diese Daten verfügbar sind, beginnt der Kosteneinsparungsrechner mit der Berechnung der Kosteneinsparungen und veröffentlicht die Daten unter dem AMS/ResourceScheduler Metrik-Namespace in CloudWatch

Tipps für Kostenschätzer

Der Cost Savings Estimator akzeptiert keine Rabatte wie Reserved Instances, Sparpläne usw., die bei der Berechnung berücksichtigt werden. Der Estimator verwendet die Nutzungskosten aus dem Cost Explorer und berechnet die durchschnittlichen Kosten pro Stunde für die Ressourcen. Weitere Informationen finden Sie unter [Grundlegendes zu Ihren AWS Kostendatensätzen](#): Ein Spickzettel

Damit der Kosteneinsparungsschätzer Kosten und Nutzung nur für Ressourcen abrufen kann, die von Resource Scheduler aus dem Cost Explorer verwaltet werden, muss der Tag-Schlüssel, den Resource Scheduler für die Ausrichtung von Ressourcen verwendet, im Fakturierungs-Dashboard als Cost Allocation Tag aktiviert werden. Wenn das Konto zu einer Organisation gehört, muss der Tag-Schlüssel im Verwaltungskonto der Organisation aktiviert werden. Informationen dazu finden Sie unter [Benutzerdefinierte Tags für die Kostenzuweisung](#). Wenn das Kostenzuweisungs-Tag nicht aktiviert ist, kann der Kalkulator die Einsparungen nicht berechnen und die Metrik nicht veröffentlichen, auch wenn er aktiviert ist.

Bewährte Methoden für AMS Resource Scheduler

Planung von EC2 Amazon-Instances

- Das Verhalten beim Herunterfahren der Instance muss auf stop und nicht auf eingestellt seintermiante. Dies ist stop für Instances voreingestellt, die mit dem automatisierten Änderungstyp AMS Amazon EC2 Create (ct-14027q0sjyt1h) erstellt wurden, und kann für EC2 Amazon-Instances, die mit Ingestion erstellt wurden, festgelegt werden, indem die Eigenschaft auf gesetzt wird. AWS CloudFormation InstanceInitiatedShutdownBehavior stop Wenn für Instances das Verhalten beim Herunterfahren auf eingestellt ist, werden die Instances beendetterminate, wenn der Resource Scheduler sie stoppt und der Scheduler sie nicht wieder starten kann.
- EC2 Amazon-Instances, die Teil einer Auto Scaling Scaling-Gruppe sind, werden vom AMS Resource Scheduler nicht einzeln verarbeitet, auch wenn sie markiert sind.

- Wenn das Root-Volume der Ziel-Instance mit einem KMS-Kundenhauptschlüssel (CMK) verschlüsselt ist, muss Ihrer Resource Scheduler IAM-Rolle eine zusätzliche `kms:CreateGrant` Berechtigung hinzugefügt werden, damit der Scheduler solche Instances starten kann. Diese Berechtigung wird der Rolle standardmäßig nicht hinzugefügt, um die Sicherheit zu erhöhen. Wenn Sie diese Berechtigung benötigen, reichen Sie einen RFC mit dem Änderungstyp Management | AMS Resource Scheduler | Solution | Update ein und geben Sie eine kommasetrennte ARNs KMS-Liste an. CMKs

Auto Scaling Scaling-Gruppen planen

- AMS Resource Scheduler startet oder stoppt die Auto Scaling von Auto Scaling-Gruppen, nicht von einzelnen Instances in der Gruppe. Das heißt, der Scheduler stellt die Größe der Auto Scaling Scaling-Gruppe wieder her (Start) oder setzt die Größe auf 0 (Stopp).
- Kennzeichnen Sie die AutoScaling Gruppe mit dem angegebenen Tag und nicht die Instances innerhalb der Gruppe.
- Während des Stopps speichert AMS Resource Scheduler die minimalen, gewünschten und maximalen Kapazitätswerte der Auto Scaling Scaling-Gruppe und setzt die Minimal- und Gewünschte Kapazität auf 0. Während des Starts stellt der Scheduler die Auto Scaling Scaling-Gruppengröße wieder her, wie sie beim Stopp war. Daher müssen Auto Scaling Scaling-Gruppeninstanzen eine geeignete Kapazitätskonfiguration verwenden, damit die Beendigung und der Neustart der Instances keine Auswirkungen auf Anwendungen haben, die in der Auto Scaling Scaling-Gruppe ausgeführt werden.
- Wenn die Auto Scaling Scaling-Gruppe während einer Laufzeit geändert wird (die minimale oder maximale Kapazität), speichert der Scheduler die neue Auto Scaling Scaling-Gruppengröße und verwendet sie, wenn die Gruppe am Ende eines Stopp-Zeitplans wiederhergestellt wird.

Planung von Amazon RDS-Instances

- Der Scheduler kann vor dem Stoppen der RDS-Instances einen Snapshot erstellen (gilt nicht für den Aurora-DB-Cluster). Diese Funktion ist standardmäßig aktiviert, wobei der CloudFormation Vorlagenparameter `Create RDS Instance Snapshot` auf `true` gesetzt ist. Der Snapshot wird aufbewahrt, bis die Amazon RDS-Instance das nächste Mal gestoppt und ein neuer Snapshot erstellt wird.

Scheduler kann start/stop Amazon RDS-Instances verwenden, die Teil eines Clusters oder einer Amazon RDS Aurora-Datenbank sind oder sich in einer Multi-AZone-Konfiguration (Multi-

AZ) befinden. Überprüfen Sie jedoch die Amazon RDS-Beschränkung, wenn der Scheduler die Amazon RDS-Instance, insbesondere Multi-AZ-Instances, nicht stoppen kann. Verwenden Sie den Vorlagenparameter `Schedule Aurora Clusters`, um Aurora Cluster für den Start oder Stopp zu planen (der Standardwert ist `true`). Der Aurora-Cluster (nicht die einzelnen Instances innerhalb des Clusters) muss mit dem Tag-Schlüssel, der bei der Erstkonfiguration definiert wurde, und dem Zeitplannamen als Tag-Wert für die Planung dieses Clusters gekennzeichnet werden.

Jede Amazon RDS-Instance hat ein wöchentliches Wartungsfenster, in dem alle Systemänderungen vorgenommen werden. Während des Wartungsfensters startet Amazon RDS automatisch Instances, die länger als sieben Tage angehalten wurden, um Wartungsarbeiten durchzuführen. Beachten Sie, dass Amazon RDS die Instance nicht stoppt, sobald das Wartungsereignis abgeschlossen ist.

Der Scheduler ermöglicht die Angabe, ob das bevorzugte Wartungsfenster einer Amazon RDS-Instance als Laufzeit zu ihrem Zeitplan hinzugefügt werden soll. Die Lösung startet die Instance zu Beginn des Wartungsfensters und stoppt die Instance am Ende des Wartungsfensters, wenn keine andere Laufzeit vorgibt, dass die Instance ausgeführt werden soll, und wenn das Wartungsereignis abgeschlossen ist.

Wenn das Wartungsereignis bis zum Ende des Wartungsfensters nicht abgeschlossen ist, wird die Instanz bis zum Planungsintervall nach Abschluss des Wartungsereignisses ausgeführt.

Note

Der Scheduler überprüft nicht, ob eine Ressource gestartet oder gestoppt wurde. Er ruft die API auf und fährt fort. Wenn der API-Aufruf fehlschlägt, wird der Fehler zur Untersuchung protokolliert.

AWS Systems Manager in AMS Advanced

Ein AWS Systems Manager Dokument (SSM-Dokument) definiert die Aktionen, die Systems Manager mit Ihren AWS Ressourcen durchführt. Systems Manager enthält mehr als ein Dutzend vorkonfigurierte Dokumente, die Sie verwenden können, indem Sie zur Laufzeit Parameter angeben. Dokumente verwenden JavaScript Object Notation (JSON) oder YAML und enthalten Schritte und Parameter, die Sie angeben.

AWS Managed Services (AMS) ist ein vertrauenswürdiger Herausgeber für SSM-Dokumente. SSM-Dokumente, die sich im Besitz von AMS befinden, werden nur mit integrierten AMS-Konten geteilt, beginnen immer mit einem reservierten Präfix (AWSManagedServices-*) und werden in der Systems Manager Manager-Konsole als Eigentum von angezeigt. AWS Der AMS-Prozess für die Entwicklung und Veröffentlichung von SSM-Dokumenten folgt AWS bewährten Verfahren und erfordert während des gesamten Dokumentenlebenszyklus mehrere Peer-Reviews. Weitere Informationen zu AWS bewährten Methoden für die gemeinsame Nutzung von SSM-Dokumenten finden Sie unter [Bewährte Methoden für gemeinsam genutzte SSM-Dokumente](#).

Verfügbare AMS Advanced SSM-Dokumente

AMS Advanced SSM-Dokumente stehen ausschließlich AMS Advanced-Kunden zur Verfügung und werden verwendet, um den betrieblichen Arbeitsablauf bei der Verwaltung Ihres Kontos zu automatisieren.

Die verfügbaren AMS Advanced SSM-Dokumente finden Sie unter: AWS-Managementkonsole

1. [Öffnen Sie die Systems Manager-Konsole an der Konsole.AWS Systems Manager](#)
2. Wählen Sie Mit mir geteilt.
3. Filtern Sie in der Suchleiste nach dem Präfix für den Dokumentnamen und anschließend nach „Gleich“ und setzen Sie den Wert auf AWSManagedDienste-.

Anweisungen zur AWS CLI finden Sie unter [Verwenden gemeinsam genutzter SSM-Dokumente](#).

AMS Advanced SSM-Dokumentversionen

SSM-Dokumente unterstützen die Versionierung. AMS Advanced SSM-Dokumente können nicht vom Kundenkonto aus geändert und nicht erneut geteilt werden. Sie werden von AMS Advanced zentral verwaltet und verwaltet, um das Konto zu verwalten.

Die Versionsnummern werden bei jeder Aktualisierung eines Dokuments um einen bestimmten AWS-Region Wert erhöht. Wenn neue Regionen verfügbar werden, kann derselbe Dokumentinhalt in zwei Regionen unterschiedliche Versionsnummern haben. Dies ist typisch und bedeutet nicht, dass sich ihr Verhalten unterscheidet. Wenn Sie zwei AMS Advanced SSM-Dokumente vergleichen möchten, empfehlen wir, ihre Hashes mit der AWS CLI zu vergleichen:

```
aws ssm describe-document \
```

```
--name AWSManagedServices-DOCUMENTNAME \  
--output text --query "Document.Hash"
```

Zwei SSM-Dokumente sind identisch, wenn ihre Hashes übereinstimmen.

Systems Manager Manager-Preise in AMS

Für den Zugriff auf AMS Advanced SSM-Dokumente fallen keine Kosten an. Die Laufzeitkosten variieren je nach Art des SSM-Dokuments, seinen Schritten und der Laufzeit. Weitere Informationen finden Sie unter [AWS Systems Manager Preise](#).

Offboard-AMS-Konten

AMS bietet Offboarding-Unterstützung für Landezonenkonten mit einem Konto und Landezonenkonten mit mehreren Konten.

AMS entzieht Ihnen beim Offboarding keine AMIs Daten, um Auswirkungen auf Ihre Abhängigkeiten zu vermeiden. Wenn Sie AMS AMIs aus Ihrem Konto entfernen möchten, können Sie die `cancel-image-launch-permission` API verwenden, um bestimmte Informationen zu verbergen. AMIs Sie können beispielsweise das folgende Skript verwenden, um alle AMS auszublenden AMIs , die zuvor mit Ihrem Konto geteilt wurden:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --  
query 'Images[].ImageId' --output text) ;  
do  
aws ec2 cancel-image-launch-permission --image-id $ami ;  
done
```

Sie müssen die AWS CLI v2 installiert haben, damit das Skript fehlerfrei ausgeführt werden kann. Die Installationsschritte für AWS CLI finden Sie unter [Installation oder Aktualisierung der neuesten Version der AWS-CLI](#). Einzelheiten zum `cancel-image-launch-permission` Befehl finden Sie unter [cancel-image-launch-permission](#).

Note

Das Kündigungsdatum des Dienstes ist der letzte Tag des Kalendermonats, der auf das Ende der 30-tägigen Kündigungsfrist folgt. Fällt das Ende der erforderlichen Kündigungsfrist nach dem 20. Tag des Kalendermonats, so ist das Kündigungsdatum der letzte Tag des folgenden Kalendermonats. Im Folgenden finden Sie Beispielszenarien für Kündigungstermine.

- Wenn die Kündigung am 12. April erfolgt, endet die Kündigungsfrist von 30 Tagen am 12. Mai. Das Kündigungsdatum des Dienstes ist der 31. Mai.
- Wenn am 29. April eine Kündigungsfrist erteilt wird, endet die Kündigungsfrist von 30 Tagen am 29. Mai. Das Kündigungsdatum des Dienstes ist der 30. Juni.

Themen

- [Offboard von AMS-Landingzone-Konten mit einem Konto](#)
- [Offboard von AMS-Landingzone-Konten mit mehreren Konten](#)

Offboard von AMS-Landingzone-Konten mit einem Konto

AMS bietet innerhalb von 30 Tagen vor der Kündigung von AMS Unterstützung beim Aussteigen.

Sie müssen mindestens 7 Tage, bevor diese Hilfe geleistet werden kann, um Unterstützung beim Aussteigen beantragen. Unterstützung beim Aussteigen kann auf zwei Arten angeboten werden:

- Übergabe der Kontrolle: AMS überträgt Ihnen die Kontoverwaltung zusammen mit den Zugangsdaten für alle von AMS verwalteten Anwendungen zurück, oder
- Kündigung von Ressourcen bei Schließung des Kontos: AMS löscht alle Daten in Ihrer von AMS verwalteten Umgebung und stellt die Bereitstellung aller aktiven Ressourcen im Konto ein. Beim Einreichen der Offboarding-Anfrage können Kunden AMS auffordern,
 - Löschen oder behalten Sie die Datenobjekte (einschließlich Protokolle), die in Amazon S3 S3-Buckets gespeichert sind
 - Amazon S3 S3-Buckets entfernen oder behalten
 - AWS Backup Wiederherstellungspunkte entfernen oder beibehalten

Important

Alle anderen spezifischen Anfragen (vorbehaltlich der Plausibilität) müssen AMS vor der Initialisierung des Offboardings mitgeteilt werden.

Optionale Voraussetzungen (falls erforderlich):

 Note

Vor der Offboarding-Anfrage können Kunden AMS um Unterstützung bei der Übertragung Ihrer Daten im vorhandenen Format AWS Snowball Edge oder über jedes andere Medium, mit dem eine AWS Schnittstelle besteht, anfordern.

Zusätzlich zu den Datensicherungen können die folgenden Kundendaten im Rahmen der Offboarding-Unterstützung bereitgestellt werden:

- In Speicherdiensten gespeicherte Daten, einschließlich Protokollen
- Kundenspezifische Schemas für Änderungstypen
- CloudFormation Vorlagen für Änderungstypschemas

Falls die Offboarding-Aktivitäten nach der Kündigung von AMS nicht abgeschlossen sind, übergeben wir Ihnen die Kontoverwaltung, damit Sie alle ausstehenden Aktivitäten abschließen können.

Funktion	Was wurde entfernt	Auswirkung	Erforderliche Maßnahmen
Überwachung, Protokollierung, Alarmierung	AMS-Überwachung wurde entfernt	AMS hat keinen Zugriff mehr auf oder Einblick in Ihre Ressourcen und Umgebung.	Eventualverbindlichkeiten für entfernte und abgemeldete Dienste liegen in Ihrer Verantwortung.
	MMS (Managed Monitoring System) hat sich abgemeldet		
	Resource Tagger und Alarm Manager wurden entfernt		
	CloudWatch Basiswarnungen für bestehende Ressourcen bleiben bestehen		

Funktion	Was wurde entfernt	Auswirkung	Erforderliche Maßnahmen
	GuardDuty und Macie: Das Eigentum geht wieder an Sie zurück		
Backup-Verwaltung	Die AMS Backup-Automatisierung wurde entfernt, obwohl der AWS Backup Dienst weiterhin genutzt werden kann. Backup-Tresore und Daten werden aufbewahrt, sofern nicht eine Löschung angefordert wird.	AMS überwacht die Backup-Jobs nicht mehr und führt bei Vorfällen keine Wiederherstellungsaktionen mehr durch. Alarme und Warnmeldungen sind deaktiviert. Wenn Sie die IAM-Backup-Rolle und die KMS-Schlüssel löschen, sind Ihre AMS-Backups nicht mehr funktionsfähig.	AMS-Backup-Pläne müssen neu konfiguriert werden. Die gesamte Verantwortung für Überwachung und Problembeseitigung geht an Sie zurück.
AMS-Automatisierungen für das Servicemanagement	Von AMS kuratierte AWS SSM-Automatisierungs-Runbooks, Amazon Simple Notification Service (SNS) und AWS Lambda-Funktionen sind nicht mehr verfügbar.	Kein AMS-Zugriff auf Ihre Konten. Sämtliche Automatisierungen sind deaktiviert.	Die gesamte Automatisierung, einschließlich SSM-, SNS- und Lambda-Funktionen, muss bei Bedarf neu erstellt werden.

Funktion	Was wurde entfernt	Auswirkung	Erforderliche Maßnahmen
Compliance	AMS-Übersicht und Überwachung aller GuardDuty AWS Config Regeln wurden entfernt, obwohl diese Regeln weiterhin auf den Konten verbleiben.	Alle Überwachungs-, Berichts- und Problembehebungsmaßnahmen von Amazon GuardDuty und AWS Config Rules werden nicht mehr von AMS verwaltet.	Die Überwachung und Behebung aller Sicherheits- und Compliance-Tools obliegt Ihnen.
Agenten vor Ort	Der Zugriff auf Resource Scheduler, Resource Tagger oder die automatische Instanzkonfiguration zur Installation der erforderlichen Agenten in Ihren EC2 Instanzen wurde entfernt.	CloudWatch und SSM-Agenten auf Instances bleiben mit den vorhandenen Konfigurationen bestehen, AMS unterstützt diese Konfigurationen jedoch nicht mehr.	Sie verwalten Tagging und On-Instance-CloudWatch und SSM-Agenten-Konfigurationen.

Funktion	Was wurde entfernt	Auswirkung	Erforderliche Maßnahmen
Patch- und Berichtsinfrastruktur	AMS verwaltet die Aktivitäten vor und nach dem Patchen nicht mehr, und der Zugriff auf und die Sichtbarkeit dieser Dienste sind nicht mehr verfügbar.	AMS erstellt vor dem Patchen keinen Snapshot der Instance mehr, installiert und überwacht die Patch-Installation nicht mehr und benachrichtigt Sie nicht mehr über das Ergebnis. Berichte und S3-Buckets zur Überprüfung werden auf Anfrage in Ihren Konten hinterlassen. AMS generiert keine Berichte mehr über Servicemetriken.	Sie behalten die in der Vergangenheit erstellten Patch-Baselines und Snapshots bei. Darüber hinaus bleibt die Konfiguration der Patch-Wartungsfenster erhalten, aber die Patches werden nicht mehr von AMS installiert oder repariert. Die gesamte Berichterstattung über die Betriebskennzahlen der Infrastruktur liegt jetzt in Ihrer Verantwortung.
Prozessmanagement	Alle Konten werden aus dem für Vorfälle, einschließlich Serviceanfragen, Problem- und Änderungsmanagement, bereitgestellten Servicemanagement ausgegliedert.	Alle Betriebsunterbrechungen, die zuvor von AMS durch Vorfälle und Serviceanfragen und Änderungen an der Umgebung sowie durch Ursachenuntersuchungen behoben wurden, werden heute von AMS verwaltet.	Sie übernehmen wieder die volle Verantwortung für das gesamte Prozessmanagement.

Offboard von AMS-Landingzone-Konten mit mehreren Konten

Es gibt zwei Arten von AWS Konten, die Sie aus der AMS Advanced-Landingzone für mehrere Konten auslagern können:

- Konten für Anwendungen
- Kernkonten

Um alle Konten aus Ihrer AMS-Landezone für mehrere Konten auszulagern, müssen Sie zuerst alle Anwendungskonten auslagern, bevor Sie Core-Konten auslagern.

Wenn Sie Workloads auf ausgelagerten Anwendungs- oder Core-Konten übernehmen und weiterführen möchten, stellen Sie sicher, dass Sie diese Dokumentation zusammen mit Ihrem AMS-Kundenbetreuungsteam überprüfen. In dieser Dokumentation werden die Änderungen beschrieben, die AMS während des Offboard-Prozesses vornimmt.

Aufgaben, die für den weiteren Betrieb der ausgelagerten Konten zu erledigen sind

Die folgenden Aufgaben sind für den weiteren Betrieb von Konten erforderlich, die Sie aus der AMS-Landingzone für mehrere Konten ausgebucht haben:

- Aktivieren Sie den Entwicklermodus: Um mehr Berechtigungen für Ihre Konten zu erhalten, aktivieren Sie den Entwicklermodus, bevor Sie Anwendungskonten von AMS entfernen. Wenn Sie den Entwicklermodus aktivieren, können Sie leichter die erforderlichen Änderungen vornehmen, um sich auf das Offboarding vorzubereiten. Versuchen Sie nicht, AMS-Infrastrukturressourcen zu entfernen oder zu ändern. Wenn Sie AMS-Infrastrukturressourcen löschen, kann AMS Ihr Konto möglicherweise nicht erfolgreich auslagern. Informationen zur Aktivierung des Entwicklermodus finden Sie unter [Erste Schritte mit dem AMS Advanced Developer Mode](#).

Wenn Sie die notwendigen Änderungen zur Vorbereitung auf das Offboarding nicht vornehmen können, nachdem Sie den Entwicklermodus aktiviert haben, wenden Sie sich an Ihr AMS-Kundenbetreuungsteam, um Ihre Anforderungen zu besprechen.

- Wählen Sie eine alternative Methode für den EC2 Stack-Zugriff: Nachdem Sie Anwendungskonten von AMS entfernt haben, können Sie sie nicht mehr für den RFCs Zugriff auf Ihre Stack-Ressourcen verwenden. Prüfen [Änderungen beim Offboarding](#) Sie dies und wählen Sie dann eine alternative Zugriffsmethode aus, damit Sie weiterhin Zugriff auf Ihre Stacks haben. Weitere Informationen finden Sie unter [Auf Alternativen zugreifen](#).

Externe AMS-Anwendungskonten

Um Anwendungskonten aus Ihrer Landingzone-Umgebung mit mehreren Konten zu entfernen, führen Sie für jedes Konto die folgenden Schritte aus:

1. Vergewissern Sie sich, dass das Konto keine offenen RFCs enthält. Weitere Informationen finden Sie unter [Erstellen, Klonen, Aktualisieren, Suchen und Stornieren RFCs](#).
2. Vergewissern Sie sich, dass Sie auf die E-Mail-Adresse des primären Benutzers oder des Stammbenutzers für das Konto zugreifen können.
3. Senden Sie vom Anwendungskonto aus einen RFC mit dem Änderungstyp [Anwendungskonto | Offboarding bestätigen](#) (ct-2wlfo2jxj2rkj). Geben Sie im RFC das Anwendungskonto für Offboard an.
4. Senden Sie vom Verwaltungskonto aus einen RFC mit dem Änderungstyp [Verwaltungskonto | Offboard-Anwendungskonto](#) (ct-0vdiy51oyrhbm). Geben Sie im RFC das Anwendungskonto „Offboard“ an. Geben Sie außerdem an, ob Sie die Transit-Gateway-Verbindung zur landing zone löschen oder beibehalten möchten.
5. Um sicherzustellen, dass die AMS-Abrechnung gestoppt wird, teilen Sie Ihrem CSDM mit, dass Sie das Konto ausgebucht haben.

Nach dem Offboarding des Anwendungskontos geschieht Folgendes:

- Alle Komponenten werden von den AMS-Diensten getrennt, aber Ihre erstellten Ressourcen verbleiben im Konto. Sie können wählen, ob Sie das AMS-Offboarding-Konto behalten oder schließen möchten.
- Hauptkonten und andere verbleibende Anwendungskonten funktionieren normal, nachdem ein Anwendungskonto ausgelagert wurde.
- Die AMS-Abrechnung wird gestoppt, aber die AWS Abrechnung wird erst gestoppt, wenn Sie das Konto schließen. Weitere Informationen finden Sie unter [Was Sie wissen müssen, bevor Sie Ihr Konto schließen](#).
- Wenn ein Konto geschlossen ist, ist das Konto in Ihrer Organisation im suspended Bundesstaat 90 Tage lang sichtbar. Nach 90 Tagen wird das geschlossene Konto dauerhaft entfernt und ist in Ihrer Organisation nicht mehr sichtbar.
- Nachdem das Konto geschlossen wurde, können Sie sich weiterhin anmelden und eine Support-Anfrage einreichen oder 90 Tage Support lang Kontakt aufnehmen.

- Nach 90 Tagen werden alle Inhalte, die im Konto verbleiben, dauerhaft gelöscht und die verbleibenden AWS Dienste werden beendet.

Häufig gestellte Fragen zum Offboarding von Anwendungskonten

F: Kann ich meine föderierten IAM-Rollen verwenden, um weiterhin auf ein Anwendungskonto zuzugreifen, das ich von meiner AMS-Landingzone mit mehreren Konten aus dem Offboarding genommen habe?

Ja. Von AMS erstellte [Standardrollen AWS Identity and Access Management \(IAM\)](#) bleiben auch nach dem Offboarding von AMS im Konto verfügbar. Diese Rollen und Richtlinien sind jedoch für die Verwendung mit der AMS-Zugriffsverwaltung konzipiert. Um Ihren Benutzern den erforderlichen Zugriff zu gewähren, müssen Sie möglicherweise Ihre eigenen IAM-Ressourcen bereitstellen.

F: Wie erhalte ich vollen Zugriff auf ein Anwendungskonto, das ich von meiner AMS-Landezone für mehrere Konten aus ausgebucht habe?

Konten für ausgelagerte Anwendungen werden in der Kontostruktur in die veraltete Organisationseinheit (OU) verschoben. AWS Organizations Durch diesen Schritt werden die SCP-Zugriffsbeschränkungen aufgehoben, die zuvor den Root-Benutzerzugriff blockierten. Informationen zum Zurücksetzen der Root-Benutzeranmeldedaten finden Sie unter [Ein verloren gegangenes oder vergessenes Root-Benutzerkennwort zurücksetzen](#).

F: Welche Änderungen werden beim Offboarding des Anwendungskontos vorgenommen?

Informationen zu den Maßnahmen, die AMS ergreift, wenn der Dienst Konten auslagert, finden Sie unter [Änderungen beim Offboarding](#)

F: Kann ich ein Anwendungskonto auslagern, ohne es vom Transit-Gateway zu trennen?

Ja. Verwenden Sie den [Änderungstyp Verwaltungskonto | Offboard-Anwendungskonto](#) (ct-0vdiy51oyrhbm), um den RFC zu senden, und geben Sie den Parameter als an.
`DeleteTransitGatewayAttachment False`

F: Wie lange dauert es, ein Anwendungskonto auszulagern?

Wenn Sie das [Verwaltungskonto | Offboard-Anwendungskonto](#) (ct-0vdiy51oyrhbm) verwenden, ändern Sie den Typ und schließen Sie den Vorgang innerhalb von 1 Stunde ab. RFCs

F: Muss ich das ausgelagerte Konto schließen?

Nein. Eine Kontoschließung nach dem Offboarding von AMS ist nicht verpflichtend. Während des Offboarding-Vorgangs entzieht AMS den Zugriff auf Ihr Konto und die Verwaltung Ihres AWS Kontos, Ihr Konto und Ihre Ressourcen verbleiben jedoch innerhalb des Kontos. Es ist wichtig zu beachten, dass Sie nach dem Offboarding von AMS allein für die Verwaltung und Pflege Ihres AWS Kontos und Ihrer Ressourcen verantwortlich sind. AMS ist nicht verantwortlich für Probleme, Vorfälle oder Serviceunterbrechungen, die nach Abschluss des Offboarding-Prozesses in Ihrem Konto auftreten könnten. Weitere Informationen finden Sie unter [Wie schließe ich mein Konto? AWS](#).

F: Werden alle vorhandenen Ressourcen sofort gelöscht, wenn ich eine Anfrage zur Kontoschließung einreiche?

Nein. Durch die Schließung Ihres Kontos werden Ihre Ressourcen nicht gelöscht. Ressourcen auf dem Konto werden 90 Tage nach der Anfrage zur Schließung automatisch gelöscht. Die AMS-Abrechnung wird eingestellt, aber die AWS Ressourcenabrechnung wird erst beendet, wenn Sie das Konto schließen. Weitere Informationen finden Sie unter [Was Sie wissen müssen, bevor Sie Ihr Konto schließen](#).

F: Kann ich das Offboarding eines Anwendungskontos planen?

Ja. Sie können das so planen RFCs , dass es zu einer bestimmten Zeit ausgeführt wird. Der RFC [Application Account | Confirm Offboarding](#) muss jedoch abgeschlossen sein, bevor Sie den RFC [Management Account | Offboard Application Account](#) planen können. [Weitere Informationen finden Sie unter RFC-Planung](#).

Offboarding des Anwendungskontos (RACI)

- R: Verantwortliche Partei. Die Partei, die für die Ausführung der aufgelisteten Aufgabe verantwortlich ist.
- A: Rechenschaftspflichtige Partei. Die Partei, die die abgeschlossene Aufgabe genehmigt.
- C: Konsultierte Partei. Eine Partei, deren Meinungen eingeholt werden, in der Regel als Fachexperten, und mit der bilaterale Kommunikation besteht.
- I: Informierte Partei. Eine Partei, die über den Fortschritt informiert wird, oft erst nach Abschluss der Aufgabe oder des Liefergegenstands.

Aktivität	Custom	AWS Managed Services (AMS)
Voraussetzungen		
Überprüfen Sie den Zugriff auf die Root-E-Mail-Adresse für jede AWS Konto-ID, die ausgelagert werden soll	R	C
Lesen Sie die AMS-Dokumentation zu den empfohlenen Kundenmaßnahmen und bereiten Sie Konten für das AMS-Offboarding vor	R	C
Reichen Sie bei Bedarf einen RFC ein, um den Entwicklermodus zur Vorbereitung der Konten für das AMS-Offboarding zu aktivieren	R	I
Wählen Sie bei Bedarf eine alternative Methode für den EC2 Stack-Zugriff.	R	I
Offboarding		
Abschicken RFCs , um das Offboarding von Anwendungskonten zu bestätigen und zu beantragen	R	I
Integrieren Sie AMS-Komponenten aus Anwendungskonten	I	R
Informieren Sie AMS CSDM über ausgelagerte Konten, um die AMS-Abrechnung zu beenden	R	I
Nach dem Offboarding		
Setzen Sie das Passwort für das Root-Benutzerkonto zurück und überprüfen Sie den Root-Zugriff auf externe Konten	R	C
Schließen Sie das Konto oder folgen Sie den Anweisungen von AMS zu den empfohlenen Kundenmaßnahmen in der AMS-Offboarding-Dokumentation, um die Konten weiter zu betreiben	R	C

Core-Konten außerhalb des Unternehmens

Gehen Sie wie folgt vor, um Landingzone-Core-Konten mit mehreren Konten zu offboarden:

1. Stellen Sie sicher, dass alle Anwendungskonten in der landing zone von AMS ausgegliedert wurden.
2. Vergewissern Sie sich, dass RFCs in den Konten keine offenen Konten vorhanden sind. Weitere Informationen finden Sie unter [Erstellen, Klonen, Aktualisieren, Suchen und Stornieren RFCs](#).
3. Stellen Sie sicher, dass Sie für alle Core-Konten auf die primäre E-Mail-Adresse oder die E-Mail-Adresse des Root-Benutzers zugreifen können. Weitere Informationen finden Sie unter [Landing Zone-Konten mit mehreren Konten](#).
4. Stellen Sie sicher, dass Sie auf die Primär- oder Root-Benutzer-Telefonnummer für das Verwaltungskonto zugreifen können. Verwenden Sie die `AWSManagedServicesBillingRole` IAM-Rolle, um die Telefonnummer zu aktualisieren. Weitere Informationen finden Sie unter [Wie aktualisiere ich meine Telefonnummer, die mit meinem AWS Konto verknüpft ist?](#).
5. Loggen Sie sich in Ihr AMS-Landing landing zone Management-Konto ein und reichen Sie eine AMS-Serviceanfrage ein. Geben Sie in der Serviceanfrage an, dass Sie Ihre gesamte landing zone verlassen möchten.

Nach dem Offboarding der Core-Konten geschieht Folgendes:

- Alle Komponenten werden von den AMS-Diensten getrennt, einige AWS Ressourcen verbleiben jedoch im Konto. Sie können wählen, ob Sie die ausgelagerten AMS-Core-Konten behalten oder schließen möchten.
- Die AMS-Abrechnung wird gestoppt, aber die AWS Abrechnung wird erst gestoppt, wenn Sie das Konto schließen. Weitere Informationen finden Sie unter [Was Sie wissen müssen, bevor Sie Ihr Konto schließen](#).
- Wenn ein Konto geschlossen ist, ist das Konto in Ihrer Organisation im suspended Bundesstaat 90 Tage lang sichtbar. Nach 90 Tagen wird das geschlossene Mitgliedskonto dauerhaft entfernt und ist in Ihrer Organisation nicht mehr sichtbar.
- Nachdem das Konto geschlossen wurde, können Sie sich weiterhin anmelden und eine Support-Anfrage einreichen oder 90 Tage Support lang Kontakt aufnehmen.
- Nachdem das Konto für 90 Tage geschlossen wurde, werden alle Inhalte, die im Konto verbleiben, dauerhaft gelöscht, und die verbleibenden AWS Dienste werden beendet.

Häufig gestellte Fragen zum Offboarding von Kernkonten

F: Kann ich meine föderierten IAM-Rollen verwenden, um weiterhin auf die ausgelagerten Core-Konten zuzugreifen?

Ja. Von AMS erstellte [Standardrollen AWS Identity and Access Management \(IAM\)](#) bleiben im [ausgelagerten](#) Konto verfügbar. Diese Rollen und Richtlinien sind jedoch für die Verwendung mit der AMS-Zugriffsverwaltung konzipiert. Um Ihren Benutzern den erforderlichen Zugriff zu gewähren, müssen Sie möglicherweise Ihre eigenen IAM-Ressourcen bereitstellen.

F: Wie erhalte ich vollen Zugriff auf das Management-, Shared Services-, Networking- oder ein anderes [MALZ-Konto](#) ohne Anwendung, nachdem ich von der AMS-Landingzone für mehrere Konten ausgegliedert wurde?

Folgen Sie nach dem Offboarding den Anweisungen unter [Zurücksetzen eines verlorenen oder vergessenen Root-Benutzerpassworts, um die primären \(Root-\) Benutzeranmeldedaten](#) für den Zugriff auf andere Core-Konten als das Verwaltungskonto zu verwenden. Im Gegensatz zu anderen Kontotypen behält das Verwaltungskonto ein Gerät mit Multi-Faktor-Authentifizierung (MFA), auf das nicht zugegriffen werden kann, das dem Root-Benutzer zugeordnet ist, um die Nutzung zu verhindern. Um den Root-Zugriff wiederzuerlangen, müssen Sie den [Wiederherstellungsprozess für verlorene MFA-Geräte](#) befolgen.

F: Welche Änderungen werden beim Offboarding des Core-Kontos vorgenommen?

Informationen zu den Maßnahmen, die AMS ergreift, wenn der Dienst Konten auslagert, finden Sie unter [Änderungen beim Offboarding](#)

F: Wie lange dauert es, bis das Offboarding eines Core-Kontos abgeschlossen ist?

Der Offboarding-Prozess für das Core-Konto dauert in der Regel bis zu 30 Tage. Um jedoch sicherzustellen, dass alle erforderlichen Schritte korrekt abgeschlossen wurden, müssen Sie die Offboarding-Anfrage mindestens 7 Tage vor Beginn des Offboardings stellen. Um einen einfachen Übergang zu ermöglichen, planen Sie im Voraus und reichen Sie Ihre Offboarding-Anfrage im Voraus ein.

F: Wie verwalte ich gemeinsam genutzte Komponenten nach dem Offboarding von AMS?

AMS Managed Active Directory und andere Shared Services-Infrastrukturkomponenten sind für den Zugriff durch AMS-Betreiber konzipiert. Möglicherweise müssen Sie die Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2), die AWS Organizations Service Control Policy (SCP) aktualisieren oder andere Änderungen vornehmen, um vollen Zugriff auf diese Komponenten zu behalten.

F: Kann ich ausgelagerte Core-Konten schließen?

Standardmäßig haben Anwendungskonten mehrere Abhängigkeiten von MALZ Core-Konten, z. B. AWS Organizations Mitgliedschaft, Transit-Gateway-Netzwerkonnektivität und DNS-Auflösung über AMS Managed Active Directory. Nachdem Sie diese Abhängigkeiten gelöst haben, können Sie das ausgelagerte Core-Konto außer Betrieb nehmen und schließen. Weitere Informationen finden Sie unter [Landing Zone-Konten mit mehreren Konten](#).

Das Core-Konto wird aus RACI ausgegliedert

- **R:** Verantwortliche Partei. Die Partei, die für die Ausführung der aufgelisteten Aufgabe verantwortlich ist.
- **A:** Rechenschaftspflichtige Partei. Die Partei, die die abgeschlossene Aufgabe genehmigt.
- **C:** Konsultierte Partei. Eine Partei, deren Meinungen eingeholt werden, in der Regel als Fachexperten, und mit der bilaterale Kommunikation besteht.
- **I:** Informierte Partei. Eine Partei, die über den Fortschritt informiert wird, oft erst nach Abschluss der Aufgabe oder des Liefergegenstands.

Aktivität	Custom	AWS Managed Services (AMS)
Voraussetzungen		
Überprüfen Sie den Zugriff auf die Root-E-Mail-Adresse für jede AWS-Konto-ID, die ausgelagert wird	R	C
Überprüfen Sie den Zugriff auf das Verwaltungskonto und aktualisieren Sie die Root-Benutzer-Telefonnummer	R	C
Lesen Sie die AMS-Dokumentation zu den empfohlenen Kundenmaßnahmen und bereiten Sie Konten für das AMS-Offboarding vor	R	C
Ausgliederung		

Aktivität	Custom	AWS Managed Services (AMS)
Serviceanfrage einreichen, um das Offboarding der landing zone zu beantragen	R	I
Integrieren Sie AMS-Komponenten aus Core-Konten	I	R
Nach dem Offboarding		
Setzen Sie das Passwort für das Root-Benutzerkonto zurück und überprüfen Sie den Root-Zugriff auf externe Konten	R	C
Schließen Sie die Konten oder folgen Sie den Anweisungen von AMS zu den empfohlenen Kundenmaßnahmen in der AMS-Offboarding-Dokumentation, um die Konten weiter zu verwalten	R	C

Änderungen beim Offboarding

In der folgenden Tabelle werden die Maßnahmen, die AMS beim Offboarding von landing zone mit mehreren Konten ergreift, mögliche Auswirkungen und empfohlene Maßnahmen beschrieben.

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
Zugriffsvverwaltung	Konten für Anwendungen	Nach dem Offboarding kann der Stack-Zugriff RFCs für just-in-time zeitgebundenen Zugriff nicht mehr über AMS Bastion-Hosts an EC2 Access-Stacks weitergeleitet werden	AMS-Bastionen können nicht über RFS für den Zugriff auf Instanzen verwendet werden EC2 EC2 Instanzen, die von einem anderen	Verwenden Sie alternative Methoden, um auf die EC2 Instanz zuzugreifen (siehe Auf Alternativen zugreifen)

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
		AMS verwaltet keine zugriffsbezogenen Komponenten mehr auf vorhandenen EC2 Ressourcen-Stacks (PBIS Open Agent, Domain-Join-Skripte)	Anbieter als AMS gestartet wurden, AMLs sind nicht mit der verwalteten Active Directory-Domäne verbunden Wenn sie nicht entfernt werden, können AMS-Startskripts in vorhandenen Ressourcenstapeln aufgrund fehlender AMS-Abhängigkeiten zu Fehlern führen und den erneuten Beitritt zu einer anderen Domäne verhindern	Entfernen Sie AMS-Startskripts aus vorhandenen EC2 Ressourcenstapeln (siehe Deaktivieren Sie EC2 AMS-Startskripts)
Zugriffsvverwaltung (Fortsetzung)	Kernkonten	Wenn Sie von PBIS Open zu PBIS Enterprise (AD Bridge) migriert sind, verlängert AMS die Lizenzierung nach dem Offboarding des Kernkontos nicht mehr	Wenn die PBIS Enterprise-Lizenz ablaufen darf, sind die Active Directory-Anmeldeinformationen für bestehende Linux-basierte Instance-Stacks nicht gültig EC2	Wenn Sie zu PBIS Enterprise (AD Bridge) migriert haben, entscheiden Sie, ob Sie die Lizenzierung beibehalten oder außer Betrieb nehmen möchten (siehe) PBIS Open/Enterprise (AD-Brücke)

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
Protokollierung, Überwachung, Verwaltung g Incident/Event	Anwenders- und Core-Konten	Die bereitzustellenden Warnmeldungen aus der Basisüberwachung in AMS AMS-Komponenten wurden entfernt Bestehende bereitgestellte CloudWatch Amazon-Alarme bleiben bestehen, führen aber nicht mehr zu AMS-Vorfällen AWS Config Aggregationsberechtigungen von AMS und dem MALZ Core-Sicherheitskonto werden entfernt AWS Config Regeln bleiben implementiert und Amazon GuardDuty bleibt aktiviert, erzeugt aber keine AMS-Vorfälle mehr	Bei neu erstellten Ressourcen wurden keine AMS-Basisüberwachung und Alarme angewendet Alarme und Sicherheitsereignisse aufgrund von Infrastrukturkennzahlen führen nicht mehr zu AMS-Vorfällen AWS Config wird nicht mehr in einem zentralen Konto zusammengefasst	Definieren, erfassen und analysieren Sie Betriebsmetriken, um Workload-Ereignisse einzusehen und geeignete Maßnahmen zu ergreifen. Implementieren Sie alle erforderlichen Alarm-Workflows, um weiterhin die erforderliche Betriebsüberwachung und Alarme auf neue Ressourcen anzuwenden und Sicherheitswarnungen von AWS Config und Amazon zu erhalten GuardDuty.

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
Kontinuitätsmanagement (Backup und Wiederherstellung)	Anwendungskonten	AMS überwacht keine Backup-Jobs mehr und führt keine Sicherungs- und Wiederherstellungsanfragen mehr aus Die standardmäßigen Backup-Tresore, der Backup-Verschlüsselungsschlüssel und die Backup-Rolle von AMS bleiben erhalten	Fehler beim Backup-Vorgang werden möglicherweise nicht bemerkt	Überwachen und überprüfen Sie die Konfigurationen des Backup-Plans

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
Patch-Management	Anwenders- und Core-Konten	AMS überwacht die erfolgreiche Ausführung von Patch-Vorgängen nicht mehr und führt auch keine manuellen Patches mehr durch AMS aktualisiert die AMS-Infrastrukturkomponenten nicht mehr Von AMS bereitgestellte Patch-Baselines werden beibehalten Von AMS bereitgestellte Runbooks zur AWS Systems Manager Patch-Automatisierung werden nicht gemeinsam genutzt und können nicht mehr verwendet werden	Fehler beim Patchen werden möglicherweise nicht bemerkt Bestehende Patch-Konfigurationen, die von AMS bereitgestellten Systems Manager Automation-Runbooks abhängen, müssen neu konfiguriert werden, damit sie unterbrechungsfrei weiterlaufen.	Überprüfen und konfigurieren Sie die Patching-Konfigurationen nach Bedarf neu

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
Netzwerkmanagements	Anwendungskonten	Falls angegeben, wird der Transit-Gateway-Anhang aus dem Offboarding-Anwendungskonto entfernt	Das externe Anwendungskonto kann kein Transit-Gateway mehr für den Zugriff auf gemeinsame Dienste wie verwaltetes Active Directory oder andere Anwendungskonten verwenden	Geben Sie anFalse, DeleteTransitGatewayAttachment ob die Transit-Gateway-Konnektivität beibehalten werden soll
Sicherheitsmanager	Anwendungskonten	Das Konto ist von der zentralen Trend Micro DSM-Konsole getrennt. Außerdem leiten Endpunkt-Agents keine Warnmeldungen mehr über den AMS-Incident-Prozess weiter Trend Micro Agents bleiben installiert, werden aber nicht mehr von AMS verwaltet oder aktualisiert Von AMS bereitgestellte AMI-Anpassungen, die den Trend Micro Agent einsetzen, werden von AMS nicht mehr verwaltet oder aktualisiert	EC2 Malware-Funktion auf Instanzen deaktiviert werden möglicherweise nicht bemerkt Der Trend Micro Agent wird nicht auf EC2 Instances installiert, die nicht von AMS aus gestartet werden AMIs	Erwägen Sie, ob Sie Trend Micro weiterführen oder beenden möchten (siehe Trend Micro Deep Security)

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
Sicherheitsverwaltung (Fortsetzung)	Kernkonten	Die Trend Micro DSM-Infrastruktur bleibt innerhalb der Shared Services-Konten erhalten, wird aber nicht mehr von AMS verwaltet oder aktualisiert Trend Micro DSM leitet Warnmeldungen nicht mehr über den AMS-Incident-Prozess weiter	EC2 Malware-Funde auf Instanzen dpunkten bleiben möglicherweise unbemerkt EC2 Der Endpunktschutz von Instanzen kann beeinträchtigt werden, wenn die Infrastruktur nicht gewartet wird (Definitionsupdates, Lizenzierung usw.)	Entscheiden Sie, ob Sie Trend Micro fortsetzen oder beenden möchten (siehe) Trend Micro Deep Security
Änderungsmanagement	Anwendungs- und Core-Konten	Die AMS RFC-Konsole und die API wurden entfernt Benutzerdefinierte AMS-Dienststeuerungsrichtlinien (SCPs), die Zugriffsbeschränkungen auf Kontoebene enthalten, werden beim Offboarding von Anwendungskonten getrennt und beim Offboarding von Core-Konten gelöscht	Sie müssen eine native AWS API verwenden, um neue Ressourcen zu erstellen, bestehende Ressourcen zu ändern oder bestehende Stacks zu aktualisieren CloudFormation Zugriffsbeschränkungen werden nicht mehr auf Kontoebene über das bereitgestellte AMS auferlegt SCPs	Stellen Sie sicher, dass Benutzerrollen ausreichend Zugriff für die Nutzung der Dienste bieten AWS Erstellen Sie SCPs , um Berechtigungsbeschränkungen auf Kontoebene bereitzustellen

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
AMS OS-Images und Automatisierungen für das Servicemanagement	Anwenders- und Core-Konten	AMS bietet keinen Support mehr für Anpassungen und Startskripte, die in den bereitgestellten AMS enthalten sind EC2 AMIs Von AMS bereitgestellte EC2 AMIs Dienste sind weiterhin auf Ihren ausgelagerten Konten verfügbar Von AMS bereitgestellte Systems Manager Automation-Runbooks werden nicht gemeinsam genutzt und können nicht mehr verwendet werden	Nach dem Offboarding hat AMS aufgrund fehlender Abhängigkeiten von AMS-Komponenten das CloudFormation Sende-CFN-Signal AMIs FAILURE gestartet Betriebsprozesse, die von den von AMS bereitgestellten Systems Manager Automation-Runbooks abhängen, können fehlschlagen	Überprüfen und aktualisieren Sie alle Build- oder Betriebsprozesse, die von von AMS bereitgestellten Runbooks AMIs oder Systems Manager Automation-Runbooks abhängig sind
Infrastruktur für gemeinsam genutzte Dienste	Kernkonten	Der AMS-Zugriff wurde aufgehoben und AMS verwaltet keine gemeinsam genutzten Komponenten mehr, einschließlich AMS Managed Active Directory AWS Transit Gateway, und AWS Organizations	Verlust der Verwaltung der gemeinsam genutzten Infrastruktur	Setzen Sie den Administratorzugriff auf AMS Managed Active Directory zurück und übernehmen Sie die Verwaltung der Shared Services-Komponenten

Komponente	Account type (Art des Kontos)	Maßnahmen, die für das Offboarding ergriffen wurden	Mögliche Auswirkungen	Empfohlene Maßnahmen für Kunden
Berichterstellung	Anwenders- und Core-Konten	AMS erfasst keine Daten mehr auf Konto- oder Ressourcenebene für aggregierte Berichte	Verlust des Einblicks in betriebliche und geschäftliche Kennzahlen (Umfang von Backup und Patches, Änderungsmanagement und Aktivitäten bei Zwischenfällen)	Ersetzen Sie alle erforderlichen aggregierten Datenberichte für alle Konten durch eine eigene Lösung
Das AMS-Kundenbetreuungsteam und der Service Desk	Anwenders- und Core-Konten	Das AMS Account Team (CSDM, CA) und der AMS Operations Service Desk unterstützen die ausgelagerten Konten nicht mehr	Verlust der operativen Unterstützung durch Fachwissen in der von AMS entworfenen Landezonearchitektur für mehrere Konten und verwandten Komponenten	Stellen Sie sicher, dass ausreichend Personal vorhanden ist und Sie mit der Kontostruktur und den Ressourcen vertraut sind, um den Betrieb in der Umgebung zu unterstützen

Auf Alternativen zugreifen

Im Folgenden finden Sie alternative Methoden, um auch nach dem Offboarding von AMS-Konten weiterhin Zugriff auf Ihren EC2 Stack zu haben:

- Verwenden Sie Session Manager, um auf EC2 Instanzen mit erhöhten Rechten zuzugreifen, ohne dass Bastions oder eingehender Netzwerkzugriff erforderlich sind. Weitere Informationen finden Sie unter [AWS Systems Manager Session Manager](#).

- Fügen Sie EC2 Instanzen mit neuen Domänenanmeldedaten erneut einer anderen Active Directory-Domäne hinzu. Wenn Sie dies verwenden Directory Service, finden Sie weitere Informationen unter [Eine EC2 Instanz mit Ihrem AWS Managed Microsoft AD Verzeichnis verbinden](#).
- Verwenden Sie lokale Benutzerkonten, die Sie mit einer der anderen Zugriffsmethoden oder mit [AWS Systems Manager Run Command](#) erstellt haben.

Deaktivieren Sie EC2 AMS-Startskripts

Linux-Betriebssysteme

Verwenden Sie den Paketmanager Ihrer Distribution, um das `ams-modules` Paket zu deinstallieren. Verwenden `yum remove ams-modules` Sie beispielsweise für Amazon Linux 2.

Windows-Betriebssysteme

Gehen Sie wie folgt vor, um EC2 Startskripts in Windows zu deaktivieren:

1. Windows Server 2008/2012/2012r2/2016/2019:

Deaktivieren oder entfernen Sie die geplante Aufgabe Managed Services Startup aus dem Taskplaner. Führen Sie den `Get-ScheduledTask -TaskName '*Ec2*'` Befehl aus, um geplante Aufgaben aufzulisten.

Windows Server 2022:

Entfernen Sie die [Aufgabe EC2 Launch v2](#). Diese Aufgabe wird Initialize-AMSBoot postReady stufenweise in `C:\Amazon\EC2 LaunchProgramData\config\agent-config.yml` auf der Instance ausgeführt. Das Folgende ist ein Auszug aus einem Beispiel: `agent-config.yml`

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. (Optional) Entfernen Sie den folgenden Dateiinhalt:

```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*  
C:\Windows\System32\WindowsPowerShell\v1.0\Modules  
\AWSManagedServices.Build.Utilities\*
```

PBIS Open/Enterprise (AD-Brücke)

Um festzustellen, ob Sie die PBIS Open oder die PBIS Enterprise (AD Bridge) Edition verwenden, führen Sie den folgenden Befehl in einer verwalteten EC2 Linux-Instanz aus:

```
yum info | grep pbis
```

Die folgende Beispielausgabe zeigt PBIS Enterprise (AD Bridge):

```
Name      : pbis-enterprise  
From repo : pbise  
Name      : pbis-enterprise-devel  
Repo      : pbise  
Description : The pbis-enterprise-devel package includes the development
```

PBIS Öffnen

PBIS Open ist ein veraltetes Produkt, das BeyondTrust nicht mehr unterstützt wird. [Weitere Informationen finden Sie in der Dokumentation zu pbis-openBeyondTrust](#).

AD Bridge (PBIS Enterprise)

Sie können einen der folgenden Schritte ausführen:

- Erneuern Sie die Lizenzierung und setzen Sie den Betrieb von AD Bridge fort. Kontaktieren Sie uns BeyondTrust, um Lizenzierung und Support zu besprechen.
- Stellen Sie die Verwendung von AD Bridge ein. Führen Sie den folgenden Shell-Befehl aus, um das PBIS-Enterprise-Paket aus verwalteten Linux-Instanzen zu entfernen. Weitere Informationen finden Sie in der BeyondTrust Dokumentation [Eine Domäne verlassen und den AD Bridge-Agent deinstallieren](#).

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

Verlassen Sie die von AMS verwaltete Active Directory-Domäne, ohne den PBIS-Agenten zu entfernen

Sie haben die Möglichkeit, das von AMS verwaltete Active Directory zu verlassen, ohne den PBIS-Agenten zu entfernen. Verwenden Sie je nach Betriebssystem eine der folgenden Lösungen:

Linux operating systems

Verwenden Sie PBIS aus dem von AMS verwalteten AD, um den folgenden Shell-Befehl auszuführen, um die Verbindung zu einer EC2 Linux-Instance aufzuheben. Weitere Informationen finden Sie in der Dokumentation zu [BeyondTrust pbis-open](#) oder [BeyondTrust AD Bridge](#), je nachdem, welche Version Sie verwenden.

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

Möglicherweise wird eine Fehlermeldung ähnlich der folgenden angezeigt:

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]
Cannot resolve network address for KDC in requested realm
```

Wenn dieser Fehler auftritt, führen Sie die folgenden Befehle aus, um die AD-Anbieterregistrierung zu löschen und die lwsmd Dienste neu zu starten:

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin]'
```

Verwenden Sie die Verzeichnis-ID-Ausgabe, die Sie mit dem vorherigen Befehl erhalten haben (z. **B.A123EXAMPLE.AMAZONAWS.COM**), um die folgenden Befehle auszuführen:

```
$ /opt/pbis/bin/regshell delete_tree \
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\DIRECTORID]'
```

```
$ /etc/pbis/redhat/lwsmd restart
```

```
$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:
```

```
Test-ComputerSecureChannel -verbose

# Disjoin computer from the domain:

netdom remove hostname /domain:domain name /force
```

Note

Stellen Sie sicher, dass Sie die geplante Aufgabe zum Starten von Managed Services deaktivieren oder entfernen, wie unter beschrieben [Deaktivieren Sie EC2 AMS-Startskripts](#).

Trend Micro Deep Security

Verwenden Sie eine der folgenden Optionen, um die Verwendung von Trend Micro Deep Security fortzusetzen oder zu beenden:

Nutzung fortsetzen

- (Bei Offboarding der gesamten MALZ) Verbinden Sie nach dem Core-Konto die ausgelagerten Anwendungskonten erneut mit dem vorhandenen Trend Micro Deep Security Manager (DSM) und behalten Sie die Lizenzierung im Shared Services-Konto bei. [Weitere Informationen finden Sie unter AWS Cloud-Konten hinzufügen und Lizenzinformationen überprüfen.](#)
 1. Melden Sie sich beim Shared Services-Konto an und navigieren Sie zur Secrets Manager Manager-Konsole.
 2. Rufen Sie die Administratoranmeldedaten der DSM-Konsole ab, die im `/ams/eps/` Pfad gespeichert sind.
 3. Melden Sie sich unter <https://dsm.sentinel.int> bei der DSM-Konsole an.
 4. Wählen Sie „Kontoübergreifende Rolle verwenden“ und geben Sie dann die Eingabetaste ein `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`. Ersetzen Sie ACCOUNTID durch die Konto-ID der ausgelagerten Anwendung.
 5. Wählen Sie Weiter aus.
 6. Warten Sie einige Minuten, bis DSM die Kontoermittlung durchgeführt und angezeigt hat, dass die Synchronisierung erfolgreich war.
- Verbinden Sie externe Anwendungskonten erneut mit einer neuen Trend Micro DSM-Installation. Weitere Informationen finden Sie unter [Agents aktivieren und schützen und Agent aktivieren](#).

- Verbinden Sie externe Anwendungskonten erneut mit Trend Micro Cloud One. Weitere Informationen finden Sie unter [Migration von Deep Security zu Workload Security](#) und [Migration von einem](#) lokalen DSM.

Beenden Sie die Nutzung

- Deinstallieren Sie Trend Micro Deep Security Agents von externen Anwendungskonten. Weitere Informationen finden [Sie unter Deep Security deinstallieren](#).

Verwaltungsmodi ändern

AWS Managed Services (AMS) verwendet den Änderungsverwaltungsmodus, um Änderungen in AMS Advanced zu überwachen. Die Änderungsverwaltungsmodi helfen Ihnen dabei, hohe Betriebsstandards für die Umwelt aufrechtzuerhalten, Risiken zu kontrollieren und negative Auswirkungen zu vermeiden. AMS Advanced verfügt über verschiedene Modi, die unterschiedliche Kontroll- und Risikostufen bieten. Alle Modi, mit Ausnahme des vom Kunden verwalteten Modus, werden von AMS verwaltet. Im Folgenden sind die verfügbaren Änderungsverwaltungsmodi aufgeführt:

- RFC-Modus (früher Standard-CM-Modus): Stellt ein RFC-System (Request for Change) und benutzerdefinierte AMS-Änderungstypen () bereit CTs
- Direct Change-Modus: Entspricht dem RFC-Modus, plus Verwendung von AWS APIs und Konsolen zur Erstellung von AMS-verwalteten Ressourcen
- AWS Service Catalog auf AMS: Ähnlich dem Direct Change-Modus, aber anstatt das AMS-Change-Management-System (RFCs) zu verwenden, verwenden Sie AWS Service Catalog, um Ressourcen zu erstellen, die AMS dann verwaltet.
- Entwicklermodus: Wie im Direct Change-Modus werden nur die Ressourcen, die Sie mit AWS APIs und Konsolen erstellen, nicht von AMS verwaltet — Sie sind für deren Verwaltung verantwortlich.
- Self Service Provisioning (SSP) -Modus: Entspricht dem Entwicklermodus, außer dass kein Zugriff auf das AMS-Change-Management-System besteht (nein) RFCs
- Kundenverwalteter Modus: AMS bietet Ihnen eine landing zone mit mehreren Konten, aber die gesamte Ressourcenverwaltung liegt in Ihrer Verantwortung

Das Änderungsmanagementsystem AWS Managed Services (AMS), das die Change Management (CM) -API verwendet, bietet Operationen zur Erstellung und Verwaltung von Change (RFCs) -Anfragen sowohl für Multi-Account-Landingzone-Konten (MALZ) als auch für Single-Account-Landingzone-Konten (SALZ).

Eine Änderungsanforderung (RFC) ist eine Anfrage, die entweder von Ihnen oder AMS über die AMS-Schnittstelle erstellt wird, um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen. Sie enthält eine Change Type (CT) -ID für einen bestimmten Vorgang.

Die AMS Change Management (CM) -API bietet Operationen zur Erstellung und Verwaltung von Change (RFCs) -Anfragen. Sie können sie erstellen, aktualisieren, einreichen, genehmigen, ablehnen

und stornieren RFCs. Die AMS-Operatoren können Inhalte erstellen, aktualisieren, einreichen, genehmigen, zurückweisen, stornieren und RFCs als geschlossen markieren.

Eine Liste der reservierten AMS-Präfixe, die nicht in Tags oder anderen Namen verwendet werden dürfen, finden Sie unter [Reservierte Präfixe](#).

Informationen zu den einzelnen Änderungstypen, einschließlich Schemas und Beispielen, finden Sie in der [AMS Change](#) Type Reference.

Note

Alle API-Aufrufe für das Änderungsmanagement werden in AWS aufgezeichnet CloudTrail. Weitere Informationen finden Sie unter [Zugreifen auf Ihre Protokolle](#).

Übersicht der Modi

Verwenden Sie diese Informationen, um den geeigneten AWS Managed Services (AMS) -Modus für das Hosten Ihrer Anwendungen auszuwählen, der auf Ihrer gewünschten Kombination aus Flexibilität und präskriptiver Steuerung basiert, um Ihre Geschäftsergebnisse zu erzielen.

Die Zielgruppe für diese Informationen ist:

- Kundenteams, die für die Strategie und Steuerung ihrer landing zone verantwortlich sind. Diese Informationen helfen dem Team dabei, den Grundstein für eine von AMS verwaltete landing zone mit den AMS-Modi zu legen, die es seinen internen und externen Kunden anbieten möchte.
- Geschäfts- und Anwendungsinhaber, die mit der Migration ihrer Anwendung auf AMS beauftragt sind. Diese Informationen helfen bei der Planung der Anwendungsmigration mit dem passenden AMS-Modus für migrate/host ihre Anwendung. Beachten Sie, dass dieselbe Anwendung in verschiedenen Phasen ihres Software Development Life Cycle (SDLC) -Lebenszyklus in mehr als einem AMS-Modus gehostet werden kann.
- AMS-Partner haben die Aufgabe, Kunden über die verschiedenen Optionen für die Entwicklung und Migration zu AMS zu informieren.

Diese Informationen sind in der Gründungsphase der Einrichtung Ihrer AMS-verwalteten Plattform und beim Übergang von der Grundlagen- zur Migrationsphase Ihrer Cloud-Einführung äußerst nützlich, kurz nachdem die Einführung in AMS abgeschlossen ist und Sie sich auf die Anwendungssteuerung und den Betrieb konzentrieren.

Arten von Modi und Konten in AMS

Die Modi von AWS Managed Services (AMS) können als die Art der Interaktion mit dem AMS-Service im Rahmen des spezifischen Governance-Frameworks für jeden Modus definiert werden. Die Unterschiede zwischen der landing zone, der landing zone mit mehreren Konten oder MALZ und der landing zone mit einem Konto oder SALZ, werden notiert.

 **Note**

Einzelheiten zur Anwendungsbereitstellung und zur Auswahl des richtigen AMS-Modus finden Sie unter [AMS-Modi und Anwendungen](#) oder Workloads.
Praxisnahe Anwendungsfälle der verschiedenen Modi finden Sie unter [Anwendungsfälle aus der Praxis für AMS-Modi](#)

Die folgende Tabelle enthält Beschreibungen der Modi pro AMS-Dienst.

AMS-Funktion	RFC-Modus (früher Standard-CM-Modus)/ OOD *	Direkter Änderungsmodus	AWS Service Catalog	Self-Service-Bereitstellung //Entwicklermodus	Vom Kunden verwaltet
Konfiguration der Landezone	MALZ und SALZ	MALZ und SALZ		MALZ und SALZ	
Änderungsmanagement	Planung ändern, manuelle Änderungen überprüfen und Datensatz ändern	Entspricht dem RFC-Modus für Änderungen mit hohem Risiko wie IAM oder Sicherheitsgruppen		Keine	

AMS-Funktion	RFC-Modus (früher Standard-CM-Modus)/ OOD *	Direkter Änderungsmodus	AWS Service Catalog	Self-Service-Bereitstellung //Entwicklermodus	Vom Kunden verwaltet
Protokollierung, Überwachung, Guardrails und Eventmanagement	Ja (unterstützte Ressourcen)			Nein	
Kontinuitätsmanagement	Ja (unterstützte Ressourcen)			Nicht zutreffend/Nein	Nein
Sicherheitsmanagement	Sicherheitskontrollen auf Instanzebene und Kontrollen auf Kontoebene			Kontrollen auf Kontoebene	Kontrollen auf AWS-Organisationsebene
Patch-Management	Ja			Nicht zutreffend//Nein	Nein
Vorfall- und Problemmanagement	SLA für Reaktion und Lösung für Ressourcen, die von AMS unterstützt werden			Antwort-SLA für die daraus resultierenden Ressourcen	Nein
Berichterstellung	Ja			Nein	

AMS-Funktion	RFC-Modus (früher Standard-CM-Modus)/ OOD *	Direkter Änderungsmodus	AWS Service Catalog	Self-Service-Bereitstellung //Entwicklermodus	Vom Kunden verwaltet
Verwaltung von Serviceanfragen		Ja		Nur Support-Anfragen	Nein

* Operations On Demand (OOD) bietet ein Angebot für Kunden, die den RFC-Modus verwenden, um ihre Änderungen mithilfe spezieller Ressourcen zu verwalten. Weitere Informationen finden Sie im [Angebotskatalog für Operations on Demand](#) und wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM).

Note

[Self-Service-Bereitstellungsmodus in AMS](#) und beide [AMS Advanced-Entwicklermodus](#) scheinen für eine Anwendung geeignet zu sein, deren komplexe Architektur auf nativen AWS-Services basiert. Bei der Architektur von Workloads gehen Sie je nach Ihrem Geschäftskontext Kompromisse zwischen betrieblicher Exzellenz und Agilität ein. Dies ist eine gute Möglichkeit, über die Auswahl des SSP-Modus oder des Entwicklermodus für Ihre Anwendung nachzudenken. Die Auswahl kann sich auch je nach der SDLC-Phase der Anwendung ändern. Beispiel: Wenn die Anwendung produktionsbereit ist, ist der SSP-Modus aufgrund der strengeren AMS-Richtlinien in diesem Modus möglicherweise die geeignetere Option. Die Schutzmaßnahmen werden in Form von präventiven Kontrollen wie der RFC-basierten Änderungssteuerung für IAM-Updates und auf der Ebene der Anwendungs-OU durchgesetzt. SCPs Diese Geschäftsentscheidungen können Ihre technischen Prioritäten beeinflussen. Sie könnten eine Optimierung vornehmen, um die Flexibilität der Anwendungseigentümer in der „Pre-Prod“-Phase zu erhöhen, auf Kosten der Verwaltung und des betrieblichen Supports.

MALZ-Architektur und zugehörige AMS-Modi

Die AMS Multi-Account-Landing Zone (MALZ) bietet Ihnen die Möglichkeit, Anwendungskonten (oder Ressourcenkonten) automatisch unter den standardmäßigen Organisationseinheiten (OU) bereitzustellen: vom Kunden verwaltete OU, Managed OU oder Development OU. Die Infrastruktur, die in den Anwendungskonten bereitgestellt wird, die unter diesen Konten erstellt wurden, OUs unterliegt dem spezifischen AMS-Modus, der von diesen Basiskonten angeboten wird. OUs Es ist üblich, in demselben Anwendungskonto eine Mischung aus zwei oder mehr Modi vorzufinden. Beispiel: RFC-Modus und SSP-Modus können in einem AMS-verwalteten Konto koexistieren, das eine Pipeline-Architektur hostet, die aus API Gateway und Lambda für Triggerfunktionen und S3 und SQS für EC2 Aufnahme und Orchestrierung besteht. In diesem Fall würde der SSP-Modus für Lambda und API Gateway gelten.

Abbildung 1 zeigt, wie verschiedene Modi in der Grundversion von AMS angeboten werden. OUs Wenn Sie in AMS ein neues Anwendungskonto beantragen, müssen Sie die Organisationseinheit für das Konto auswählen.

MALZ-Architektur und zugehörige AMS-Modi

AMS nutzt die Grundlagen, die auf den bewährten Methoden von AWS OUs basieren, um Konten mithilfe von Service Control Policies (SCP) logisch zu verwalten. SCPs Auf diese Weise kann das Governance-Framework in jedem AMS-Modus durchgesetzt werden. Alle Governance- und Sicherheitsvorkehrungen (in Form von SCPs), die auf das Fundament angewendet werden, werden automatisch OUs auch auf das Fundament angewendet. custom/child OUs Zusätzliche SCPs können für das Kind angefordert werden. OUs Es ist wichtig zu verstehen, dass Anwendungskonten nicht dasselbe sind wie Modi. Modi werden auf die innerhalb der Konten bereitgestellte Infrastruktur angewendet und definieren die betrieblichen Verantwortlichkeiten zwischen AMS und den Kunden.

Abbildung 1: MALZ-Architektur und zugehörige AMS-Modi

Note

„Restriktiv“ bedeutet, dass Sie für diese Programme benutzerdefinierte Richtlinien anfordern können. Diese werden von AMS genehmigt OUs, damit sichergestellt ist, dass sie die Fähigkeit von AMS, optimale Betriebsabläufe zu gewährleisten, nicht beeinträchtigen. case-

by-case Eine ausführliche Liste der AMS-Leitplanken finden Sie unter [AMS Guardrails im Benutzerhandbuch](#).

AMS-Modi und Anwendungen oder Workloads

Berücksichtigen Sie bei der Auswahl des richtigen Modus die Betriebs- und Governance-Anforderungen für Ihre Anwendungen, indem Sie entweder ein neues Anwendungskonto beantragen oder die Anwendung in einem vorhandenen Anwendungskonto hosten. Die Auswahl des geeigneten AMS-Modus für jede Anwendung oder jeden Workload hängt von den folgenden Faktoren ab:

- Die Art der SDLC-Lebenszyklusfunktion, die die Umgebung bereitstellen wird (z. B. Sandbox mit unmoderierten Änderungen, UAT mit einigen häufigen Änderungen, Produktion mit minimalen Änderungen und stark reguliert)
- Die erforderlichen Verwaltungsrichtlinien (die auf OU-Ebene durchgesetzt werden) SCPs
- Betriebsmodell (wenn Sie die operative Verantwortung übernehmen oder diese an AMS auslagern möchten)
- Die gewünschten Geschäftsergebnisse, wie die Zeit für den Betrieb in der Cloud und die Betriebskosten.

Note

Eine Beschreibung der Modustypen pro AMS-Dienst finden Sie unter [Modi- und Kontotypen in AMS](#).

Praktische Anwendungsfälle der verschiedenen Modi finden Sie unter [Anwendungsfälle aus der Praxis für AMS-Modi](#)

In der folgenden Tabelle sind die wichtigsten Überlegungen aufgeführt, die Anwendungsbesitzer bei der Entscheidung für den am besten geeigneten AMS-Modus berücksichtigen sollten. Anwendungsbesitzer sollten vor der Anwendungsmigration eine Bewertungsphase einplanen, um genau zu verstehen, welcher Modus für ihre spezifische Anwendung gilt. Beispiel: Für Anwendungen, die auf Cloud-nativen Diensten oder serverloser Architektur basieren, könnte die beste Option darin bestehen, im Entwicklermodus mit dem Aufbau und der Iteration zu beginnen und die endgültige Infrastruktur als Code mithilfe des AMS Managed — SSP-Modus bereitzustellen. In diesem Fall kann ein geringfügiges Refactoring erforderlich sein, um sicherzustellen, dass alle für die automatisierte

Bereitstellung erstellten CloudFormation Vorlagen den von AMS festgelegten Ingest-Richtlinien entsprechen. Darüber hinaus müssen alle IAM-Berechtigungen von AMS Security genehmigt werden, um sicherzustellen, dass sie dem Modell der geringsten Rechte folgen.

Der AMS-Modus, der für das Hosten der Anwendung ausgewählt wurde, kann Ihnen dabei helfen, Ihr gewünschtes Cloud-Betriebsmodell umzusetzen.

 Note

In einer einzigen AMS Managed Landing Zone kann mehr als ein Cloud-Betriebsmodell existieren, basierend auf den verschiedenen AMS-Modi, die für das Hosten der Anwendungen ausgewählt wurden.

Probleme bei der Entscheidung	Standard-CM-Modus / OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet

Betriebsbereitschaft

Protokollierung, Überwachung und Eventmanagement	AMS ist für die gesamte verwaltete Infrastruktur verantwortlich	Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	Der Kunde ist verantwortlich
Kontinuitätsmanagement	Verantwortung von AMS für die Ausführung des vom Kunden ausgewählten Backup-Plans	Der Kunde ist verantwor	Kunde, der für Ressource	

Probleme bei der Entscheidung	Standard-CM-Modus / OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
				tlich für Self-Service Provisioned Services (SSP)	n verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Zugriffsmanagement auf Instanzebene	AMS-Verwaltung über unidirektionales AD-Trust mit lokaler Domäne. Erfordert eine verwaltete Infrastruktur, um der AMS-Domäne beizutreten			Nicht zutreffend	Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Sicherheitsmanagement und Zugriffsmangement auf Kontoebenen	AMS-Verantwortung für alle verwalteten Konten			AMS ist für alle verwalteten Konten verantwortlich	Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Patch-Management	AMS-Verantwortung für alle verwalteten Konten			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	

Probleme bei der Entscheidung	Standard-CM-Modus / OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Änderungsmanagement	AMS-Verantwortung für alle verwalteten Konten			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Verwaltung der Bereitstellung	Präskriptiv und standardisiert für die in AMS angebotenen Bereitstellungsoptionen	Flexibilität bei der direkten Nutzung der AWS-Service-API für den AWS Service Catalog gemäß den vorgeschriebenen AMS-Standards	Flexibilität zur direkten Nutzung der AWS-Service-API gemäß den vorgeschriebenen AMS-Standards	Flexibilität bei der direkten Nutzung des AWS-Service APIs für SSP-Services	Flexibilität bei der direkten Nutzung der AWS-Service-API für die Bereitstellung	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Serv ice-Bereitstellung	Entwickle rmodus	Vom Kunden verwaltet
Verwaltung und Prüfung von Vorfällen	AMS ist für alle verwalteten Konten verantwortlich				Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS Change Management Systems bereitgestellt werden	
GuardRails und gemeinsam genutzte Infrastruktur (Netzwerk) und Sicherheitsframework	Präskriptive und standardisierte Nutzung von AMS Core Accounts					Flexible und maßgeschneiderte Nutzung von AMS Core Accounts
Bereitschaft zur Anwendung						

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Serv ice-Bereitstellung	Entwickle rmodus	Vom Kunden verwaltet
Refactori ng von Anwendungen	Ein leichtes Refactoring ist erforderlich				Ein leichtes Refactoring ist erforderl ich (falls es mit AMS Standard CM bereitges tellt wurde)	Ein Refactori ng ist nicht erforderlich
Support für AWS-Services	Beschränkt auf das, was von AMS unterstützt wird					Nicht begrenzt
Geschäftliche Überlegungen						
Zeit bis zur Betriebsb ereitschaft	Drei bis sechs Monate			Mehr als 6 Monate, abhängig von den Kompetenzen des Kunden im Bereich Anwendung sbetrieb		6 bis 18 Monate, abhängig von den Kompetenz en des Kunden in Bezug auf Infrastru ktur und Anwendung sbetrieb
Kosten	\$\$\$\$			\$\$\$	\$\$	\$

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Serv ice-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Anwendungsbeispiele	Webserver mit 3-Tier-Stack, Apps mit Compliance- und regulatorischen Anforderungen			Webserver mit API Gateway, containerisierte Anwendung, die ECS/EKS nutzt	Iteration/Optimierung einer Data Lake-Anwendung, die Lambda, Glue, Athena usw. verwendet	Dezentralisiert accounts/applications wie eine Sandbox, verwaltete Anwendungen von Drittanbietern

* Operations On Demand (OOD) bietet ein Angebot für Kunden, die den Standard-CM-Modus verwenden, um ihre Änderungen mithilfe spezieller Ressourcen zu verwalten. Weitere Informationen finden Sie im [Angebotskatalog für Operations on Demand](#) und wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM).

Note

Beim Preisvergleich zwischen SSP-Modus und Entwicklermodus wird davon ausgegangen, dass dieselben AWS-Services bereitgestellt werden.

Vergleich der AMS-Modi mit Geschäfts- und IT-Zielen

Wie gezeigt, sind die Modi AMS-Managed Standard Change, AWS Service Catalog oder Direct Change am besten geeignet, wenn Sie nach einem stark kontrollierten und standardisierten Governance-Modell für Ihre Anwendungen suchen. Wenn Sie ein maßgeschneidertes Governance-Modell benötigen, bei dem der Schwerpunkt auf Anwendungsinnovationen liegt, ohne dass Sie dafür betriebsbereit sein müssen, wählen Sie den Modus Customer Managed. Im vom Kunden verwalteten Modus kann die Operationalisierung Ihrer Anwendungen länger dauern, da Sie die Verantwortung für

die Einrichtung von Mitarbeitern, Prozessen und Tools zur Unterstützung betrieblicher Funktionen wie Incident Management, Configuration Management, Provisioning Management, Security Management, Patch Management usw. tragen.

Anwendungsfälle für AMS-Modi in der realen Welt

Untersuchen Sie diese, um herauszufinden, wie AMS-Modi verwendet werden können.

- Anwendungsfall 1: Geschäftliche Notwendigkeit zur Senkung der Kosten durch einen zeitkritischen Ausstieg aus dem Rechenzentrum: Ein Unternehmen mit einem wichtigen Geschäftsereignis, wie einem Ausstieg aus dem Rechenzentrum, ist daran interessiert, seine lokalen Anwendungen in der Cloud neu zu hosten. Der Großteil des lokalen Inventars besteht aus Windows- und Linux-Servern mit einer Mischung aus Betriebssystemversionen. Dabei möchte der Kunde auch die Kosteneinsparungen nutzen, die der Umstieg auf die Cloud mit sich bringt, und die technische und sicherheitstechnische Situation seiner Anwendungen verbessern. Der Kunde möchte schnell handeln, verfügt aber noch nicht über das nötige Fachwissen im Bereich Cloud-Betrieb. Der Kunde muss ein ausgewogenes Verhältnis zwischen Refactoring finden. Zu viel Refactoring kann angesichts eines engen Zeitrahmens riskant sein. Mit einigen Refaktorisierungen, wie der Aktualisierung von Betriebssystemversionen und der Optimierung von Datenbanken, können Anwendungen jedoch das nächste Leistungsniveau erreichen. In diesem Beispiel kann der Kunde den AMS-verwalteten RFC-Modus wählen, um die meisten seiner Anwendungen neu zu hosten. AMS bietet den Betrieb der Infrastruktur und berät die Betriebsteams des Kunden gleichzeitig in Bezug auf bewährte Verfahren für den sicheren Betrieb in der Cloud.

Der von AMS verwaltete AWS Service Catalog und der AMS-verwaltete Direct Change-Modus bieten dem Kunden zusätzliche Flexibilität und erreichen gleichzeitig dieselben Geschäftsergebnisse und Ziele. Darüber hinaus kann der Kunde das Angebot AMS Operations On Demand (OOD) nutzen, um über eigene AMS-Betriebstechniker zu verfügen, die die Ausführung von Änderungsanträgen priorisieren (). RFCs

Während der Kunde die undifferenzierten betrieblichen Aufgaben der Infrastruktur (Patching, Backups, Kontoverwaltung usw.) an AMS auslagern kann, kann er sich weiterhin auf die Optimierung seiner Anwendung konzentrieren und seine internen Teams auf den Cloud-Betrieb ausweiten. AMS stellt dem Kunden monatliche Berichte über Kosteneinsparungen zur Verfügung und gibt Empfehlungen zur Ressourcenoptimierung. In diesem Anwendungsfall können end-of-life Anwendungen, die auf älteren Betriebssystemversionen wie Windows 2003 und 2008 gehostet wurden und die der Kunde nicht umgestaltet hat, auch zu AMS migriert und in einem Konto gehostet werden, das den vom Kunden verwalteten Modus nutzt.

- Anwendungsfall 2, Aufbau eines Data Lake mit Lambda, Glue, Athena innerhalb der sicheren AMS-Grenzen: Ein Unternehmen möchte einen Data Lake einrichten, um die Berichtsanforderungen für mehrere AMS-Anwendungen zu erfüllen. Der Kunde möchte S3-Buckets für die Speicherung von Datensätzen und AWS Athena verwenden, um den Datensatz für jeden Bericht abzufragen. S3 und AWS Athena werden in separaten AMS Managed Accounts bereitgestellt. Das Konto bei S3 verfügt auch über andere Dienste wie Glue, Lambda und Step Functions zum Aufbau einer Datenerfassungspipeline. Glue, Lambda, Athena und Step Functions gelten in diesem Fall als Self-Service Provisioning (SSP) -Services. Der Kunde hat außerdem eine EC2 Instanz in dem Konto bereitgestellt, die als Ad-hoc-Server fungiert. tooling/scripting Der Kunde fordert AMS zunächst auf, die SSP-Dienste in seinem AMS-verwalteten Konto zu aktivieren. AMS stellt für jeden Service eine IAM-Rolle bereit, die der Kunde übernehmen kann, sobald die Rolle in die Verbundlösung des Kunden integriert ist. Zur Vereinfachung der Verwaltung kann der Kunde auch die Richtlinien für die einzelnen IAM-Rollen in einer benutzerdefinierten Rolle zusammenfassen, sodass beim Arbeiten zwischen den AWS-Services keine Rollen mehr gewechselt werden müssen. Sobald die Rolle im Konto aktiviert ist, kann der Kunde die Services gemäß seinen Anforderungen konfigurieren. Der Kunde muss jedoch mit dem AMS-Change-Management-System zusammenarbeiten, um je nach Anwendungsfall zusätzliche Berechtigungen anzufordern.

Für den Zugriff auf Glue Crawlers benötigt Glue beispielsweise zusätzliche Berechtigungen. Zusätzliche Berechtigungen sind auch erforderlich, um Ereignisquellen für Lambda zu erstellen. Der Kunde wird mit AMS zusammenarbeiten, um die IAM-Rollen zu aktualisieren, sodass Athena kontenübergreifenden Zugriff hat, um S3-Buckets abzufragen. Aktualisierungen von Servicerollen oder serviceverknüpften Rollen werden ebenfalls über das AMS Change Management benötigt, damit Lambda den Step Functions Functions-Dienst aufruft, und Glue, um in alle S3-Buckets zu lesen und in sie zu schreiben. AMS arbeitet mit Kunden zusammen, um sicherzustellen, dass das Zugriffsmodell mit den geringsten Rechten eingehalten wird und die angeforderten IAM-Änderungen nicht zu freizügig sind und die Umgebung nicht unnötigen Risiken aussetzen. Das Data Lake-Team des Kunden verbringt Zeit damit, alle IAM-Berechtigungen zu planen, die für die spezifische Architektur des Kunden erforderlich sind, und bittet AMS, diese zu aktivieren. Dies liegt daran, dass alle IAM-Änderungen manuell verarbeitet und vom AMS-Sicherheitsteam überprüft werden. Die Zeit für die Bearbeitung dieser Anfragen sollte im Zeitplan für die Anwendungsbereitstellung berücksichtigt werden.

Da die SSP-Dienste innerhalb des Accounts betriebsbereit sind, kann der Kunde über das AMS Incident Management und die Serviceanfragen Support anfordern und Probleme melden. AMS überwacht jedoch nicht aktiv die Leistungs- und Parallelitätskennzahlen für Lambda oder Job-Metriken für Glue. Es liegt in der Verantwortung des Kunden, sicherzustellen, dass für SSP-Dienste

eine angemessene Protokollierung und Überwachung aktiviert ist. Die EC2 Instance und der S3-Bucket im Konto werden vollständig von AMS verwaltet.

- Anwendungsfall 3, schnelle und flexible Einrichtung einer CICD-Bereitstellungspipeline in AMS: Ein Kunde möchte eine Jenkins-basierte CICD-Pipeline einrichten, um die Code-Pipeline für alle Anwendungskonten in AMS bereitzustellen. Für den Kunden ist es möglicherweise am geeignetsten, diese CICD-Pipeline im AMS-Managed Direct Change Mode (DCM) oder im AMS-Managed Developer-Modus zu hosten, da er so flexibel den Jenkins-Server mit der erforderlichen benutzerdefinierten Konfiguration einrichten kann EC2, mit den gewünschten IAM-Zugriffsberechtigungen CloudFormation und S3-Buckets, die das Artefakt-Repository hosten. Dies ist zwar auch im AMS-verwalteten RFC-Modus möglich, das Kundenteam müsste jedoch mehrere Handbücher RFCs für IAM-Rollen erstellen, um anhand der am wenigsten zulässigen Genehmigungen zu iterieren, die manuell von AMS überprüft werden. DCM ermöglicht es den Kunden, ihre betrieblichen Ziele auf AWS zu erreichen und gleichzeitig die Notwendigkeit zu vermeiden, mehrere Handbücher RFCs für IAM-Rollen zu erstellen, wenn der vom AMS verwaltete RFC-Modus verwendet wird, um die am wenigsten zulässigen Genehmigungen zu verwenden, die manuell von AMS überprüft werden. Dies würde sowohl Zeit als auch Schulung seitens des Kunden erfordern, um die AMS-Prozesse und -Tools auf den neuesten Stand zu bringen. Im Entwicklermodus kann der Kunde mit einer „Entwicklerrolle“ beginnen, um die Infrastruktur mithilfe von nativem AWS bereitzustellen APIs. Der schnellste und flexibelste Weg, diese Pipeline einzurichten, wäre die Verwendung des AMS Managed-Developer-Modus. Der Entwicklermodus bietet den schnellsten und einfachsten Weg, wobei er Kompromisse bei der Betriebsintegration eingeht, während DCM weniger flexibel ist, aber das gleiche Maß an Betriebsunterstützung bietet wie der RFC-Modus.
- Anwendungsfall 4, maßgeschneidertes Betriebsmodell innerhalb der AMS-Stiftung: Ein Kunde steht vor einem terminbedingten Verlassen des Rechenzentrums und eine seiner Unternehmensanwendungen wird vollständig von einem Drittanbieter-MSP verwaltet, einschließlich Anwendungsbetrieb und Infrastrukturbetrieb. Unter der Annahme, dass der Kunde im Zeitplan keine Zeit hat, diese Anwendung so umzugestalten, dass sie von AMS betrieben werden kann, ist der Modus „Kundenverwaltung“ eine geeignete Option. Der Kunde kann die Vorteile der automatisierten und schnellen Einrichtung der von AMS verwalteten Landing Zone nutzen. Sie können die zentralisierte Kontoverwaltung nutzen, die den Verkauf und die Konnektivität der Konten über das zentrale Netzwerkkonto steuert. Es vereinfacht auch ihre Abrechnung, indem die Gebühren für alle vom Kunden verwalteten Konten über das AMS Payer-Konto konsolidiert werden. Der Kunde hat die Flexibilität, sein maßgeschneidertes Zugangsmanagementmodell einzurichten, wobei der MSP von der für AMS Managed Accounts verwendeten Standardzugriffsverwaltung getrennt ist. Auf diese Weise kann der Kunde im Modus

„Kundenverwaltung“ eine von AMS verwaltete Umgebung einrichten und gleichzeitig seine Geschäftsanforderungen erfüllen, die sich aus der lokalen Umgebung ergeben. In diesem Fall ist der Kunde für die Erstellung eines Cloud-Betriebsmodells verantwortlich, wenn der Kunde auch über Windows-basierte Anwendungen verfügt, die er in die Cloud migriert, und diese in ein vom Kunden verwaltetes Konto verschieben möchte. Dies kann komplex, teuer und zeitaufwändig sein, je nachdem, ob der Kunde in der Lage ist, traditionelle IT-Prozesse zu transformieren und Mitarbeiter zu schulen. Der Kunde kann Zeit und Kosten sparen, indem er solche Workloads auf ein von AMS verwaltetes Konto überträgt und den Infrastrukturbetrieb an AMS auslagert.

Note

Kunden haben manchmal das Bedürfnis, Anwendungskonten zwischen dem Governance-Framework des RFC- oder SSP-Modus und dem Entwicklermodus zu verschieben. Beispielsweise können Kunden im Rahmen der ersten Lift-and-Shift-Migration eine Anwendung im AMS-verwalteten Modus hosten, möchten die Anwendung aber im Laufe der Zeit neu schreiben, um sie für Cloud-native AWS-Services zu optimieren. Sie könnten den Modus des Pre-Prod-Kontos von AMS-verwaltetem RFC in den AMS-verwalteten Entwicklermodus ändern, was ihnen die Flexibilität und Agilität für die Bereitstellung der Infrastruktur gibt. Sobald jedoch Änderungen an der Bereitstellung der Infrastruktur mithilfe der „Entwicklerrolle“ vorgenommen wurden, kann dieselbe Infrastruktur nicht mehr in den AMS-verwalteten RFC-Modus zurückversetzt werden. Dies liegt daran, dass AMS den Betrieb der Infrastruktur, die außerhalb des AMS-Change-Management-Systems bereitgestellt wurde, nicht garantieren kann. Kunden müssen möglicherweise ein neues Anwendungskonto erstellen, das den AMS-verwalteten RFC-Modus bietet, und dann die „optimierte“ Infrastrukturkonfiguration mithilfe von CloudFormation Vorlagen oder benutzerdefinierter Daten, die in ein von AMS verwaltetes Konto AMIs aufgenommen wurden, erneut bereitstellen. Dies ist eine saubere Methode, um eine produktionsbereite Konfiguration bereitzustellen. Nach der Bereitstellung unterliegt die Anwendung der vorgeschriebenen AMS-Verwaltung und dem Betrieb. Das Gleiche gilt für den Wechsel zwischen dem vom Kunden verwalteten Modus und dem AMS-verwalteten Modus.

RFC-Modus

Der RFC-Modus ist der Standardmodus für Kunden mit AMS Advanced Operations Plan. Er umfasst ein Change-Management-System mit Änderungsanträgen oder RFCs einen Katalog von Änderungstypen, anhand derer Sie die gewünschten Ergänzungen oder Änderungen an Ihren Konten

beantragen können. Dieses Change-Management-System bietet ein gewisses Maß an Sicherheit, indem es einschränkt, wer Änderungen an Ihren Konten vornehmen kann.

Einzelheiten zu den Änderungstypen von AMS Advanced finden Sie unter [Was sind AMS-Änderungstypen?](#).

Einzelheiten zum Onboarding bei AMS Advanced finden Sie unter Einführung in [AWS Managed Services Onboarding](#).

Exemplarische Anleitungen zum Änderungstyp finden Sie im Abschnitt „Zusätzliche Informationen“ für den entsprechenden Änderungstyp im Abschnitt AMS Advanced Change Type Reference — [Änderungstypen](#) nach Klassifizierung.

 Note

Der RFC-Modus wurde zuvor als „Change Management-Modus“ oder „Standard-CM-Modus“ bezeichnet.

Themen

- [Erfahre mehr über RFCs](#)
- [Was sind Änderungstypen?](#)
- [Behebung von RFC-Fehlern in AMS](#)

Erfahre mehr über RFCs

Änderungsanträge, oder RFCs, funktionieren auf zweierlei Weise. Erstens sind Parameter für den RFC selbst erforderlich. Dies sind die Optionen in der `CreateRfc` API. Und zweitens gibt es Parameter, die für die Aktion des RFC erforderlich sind (die Ausführungsparameter). Weitere Informationen zu den `CreateRfc` Optionen finden Sie im [CreateRfc](#) Abschnitt der AMS-API-Referenz. Diese Optionen werden normalerweise im Bereich Zusätzliche Konfigurationen der Seiten „RFC erstellen“ angezeigt.

Sie können einen RFC mit der `CreateRfc` API, `aws amscm create-rfc` CLI oder mithilfe der AMS-Konsole RFC-Seiten erstellen und einreichen. Ein Tutorial zur Erstellung eines RFC finden Sie unter. [Erstellen Sie einen RFC](#)

Themen

- [Was sind RFCs?](#)
- [Authentifizieren Sie sich, wenn Sie die AMS API/CLI CLI](#)
- [RFC-Sicherheitsüberprüfungen verstehen](#)
- [Verstehen Sie die Klassifizierungen von RFC-Änderungstypen](#)
- [RFC-Aktionen und Aktivitätsstatus verstehen](#)
- [RFC-Statuscodes verstehen](#)
- [Verstehen Sie das RFC-Update CTs und die Erkennung von CloudFormation Template-Drift](#)
- [Zeitplan RFCs](#)
- [Genehmigen oder Ablehnen RFCs](#)
- [RFC-eingeschränkte Laufzeiten anfordern](#)
- [Erstellen, Klonen, Aktualisieren, Suchen und Stornieren RFCs](#)
- [Verwenden Sie die AMS-Konsole mit RFCs](#)
- [Erfahren Sie mehr über gängige RFC-Parameter](#)
- [Melden Sie sich für die tägliche RFC-E-Mail an](#)

Was sind RFCs?

Mit einem Änderungsantrag (RFC) nehmen Sie eine Änderung in Ihrer von AMS verwalteten Umgebung vor oder bitten AMS, in Ihrem Namen eine Änderung vorzunehmen. Um einen RFC zu erstellen, wählen Sie aus AMS-Änderungstypen, wählen RFC-Parameter (z. B. Zeitplan) und reichen die Anfrage dann entweder über die AMS-Konsole oder die API-Befehle und ein. [CreateRfcSubmitRfc](#)

Ein RFC enthält zwei Spezifikationen, eine für den RFC selbst und eine für die Change Type (CT) -Parameter. In der Befehlszeile können Sie einen Inline-RFC-Befehl oder eine CreateRfc Standardvorlage im JSON-Format verwenden, die Sie zusammen mit der CT-JSON-Schemadatei ausfüllen und einreichen, die Sie erstellen (basierend auf den CT-Parametern). Der CT-Name ist eine informelle Beschreibung des CT. Ein CSIO (Kategorie, Unterkategorie, Gegenstand, Operation) ist eine formellere Beschreibung eines CT. Bei der Erstellung eines RFC muss nur die CT-ID angegeben werden.

AMS benachrichtigt Sie, wenn die Änderung erfolgreich (Success) oder erfolglos (Failure) abgeschlossen wurde.

 Note

Informationen zur Behebung von RFC-Fehlern finden Sie unter. [Behebung von RFC-Fehlern in AMS](#)

Die folgende Grafik zeigt den Arbeitsablauf eines von Ihnen eingereichten RFC.

Authentifizieren Sie sich, wenn Sie die AMS API/CLI CLI

Wenn Sie die AMS-API/CLI verwenden, müssen Sie sich mit temporären Anmeldeinformationen authentifizieren. Um temporäre Sicherheitsanmeldedaten für Verbundbenutzer anzufordern [GetFederationToken](#), rufen Sie [AssumeRole](#), [AssumeRoleWithSAML](#) oder [AssumeRoleWithWebIdentity](#) AWS Security Token Service (STS) an. APIs

Eine gängige Wahl ist SAML. Nach der Einrichtung fügen Sie jeder Operation, die Sie aufrufen, ein Argument hinzu. Beispiel: `aws --profile saml amscm list-change-type-categories`.

Eine Abkürzung für SAML 2.0-Profil besteht darin, die Profilvariable am Anfang jedes API/CLI mit zu setzen `set AWS_DEFAULT_PROFILE=saml` (für Windows; für Linux wäre das der Fallexport `AWS_DEFAULT_PROFILE=saml`). Informationen zur Einstellung von CLI-Umgebungsvariablen finden Sie unter [Konfiguration der AWS-Befehlszeilenschnittstelle, Umgebungsvariablen](#).

RFC-Sicherheitsüberprüfungen verstehen

Das Genehmigungsverfahren für das Änderungsmanagement von AWS Managed Services (AMS) stellt sicher, dass wir eine Sicherheitsüberprüfung der Änderungen durchführen, die wir an Ihren Konten vornehmen.

AMS bewertet alle Änderungsanträge (RFCs) anhand der technischen Standards von AMS. Jede Änderung, die die Sicherheitslage Ihres Kontos aufgrund einer Abweichung von den technischen Standards beeinträchtigen könnte, wird einer Sicherheitsüberprüfung unterzogen. Während der Sicherheitsüberprüfung weist AMS auf relevante Risiken hin, und in Fällen mit hohem oder sehr hohem Sicherheitsrisiko akzeptiert oder lehnt Ihr autorisiertes Sicherheitspersonal den RFC ab. Alle Änderungen werden auch daraufhin bewertet, ob sie sich negativ auf die Betriebsfähigkeit von AMS auswirken. Wenn potenzielle nachteilige Auswirkungen festgestellt werden, sind zusätzliche Prüfungen und Genehmigungen innerhalb von AMS erforderlich.

Technische Standards von AMS

Die technischen Standards von AMS definieren die Mindestsicherheitskriterien, Konfigurationen und Prozesse, um die grundlegende Sicherheit Ihrer Konten zu gewährleisten. Diese Standards müssen sowohl von AMS als auch von Ihnen befolgt werden.

Jede Änderung, die die Sicherheitslage Ihres Kontos aufgrund einer Abweichung von den technischen Standards potenziell beeinträchtigen könnte, wird einem Risikoakzeptanzprozess unterzogen, bei dem das relevante Risiko von AMS hervorgehoben und vom autorisierten Sicherheitspersonal von Ihrer Seite akzeptiert oder abgelehnt wird. All diese Änderungen werden auch bewertet, um zu beurteilen, ob sie sich negativ auf die Fähigkeit von AMS auswirken würden, das Konto zu führen. Falls ja, sind zusätzliche Prüfungen und Genehmigungen innerhalb von AMS erforderlich.

RFC-Prozess für das Kundensicherheitsrisikomanagement (CSRM)

Wenn jemand aus Ihrem Unternehmen eine Änderung an Ihrer verwalteten Umgebung anfordert, überprüft AMS die Änderung, um festzustellen, ob die Anfrage die Sicherheitslage Ihres Kontos verschlechtern könnte, weil sie nicht den technischen Standards entspricht. Wenn die Anfrage die Sicherheitslage des Kontos beeinträchtigt, informiert AMS Ihren Ansprechpartner für das Sicherheitsteam über das entsprechende Risiko und führt die Änderung durch. Oder, wenn die Änderung ein hohes oder sehr hohes Sicherheitsrisiko für die Umgebung mit sich bringt, bittet AMS um die ausdrückliche Zustimmung Ihres Ansprechpartners im Sicherheitsteam in Form einer Risikoakzeptanz (siehe unten). Der AMS-Prozess zur Risikoakzeptanz bei Kunden ist darauf ausgerichtet:

- Stellen Sie sicher, dass Risiken klar identifiziert und den richtigen Eigentümern mitgeteilt werden
- Minimieren Sie die identifizierten Risiken für Ihre Umgebung
- Lassen Sie sich von den zuständigen Sicherheitskontakten, die mit dem Risikoprofil Ihres Unternehmens vertraut sind, die Genehmigung einholen und dokumentieren
- Reduzieren Sie den laufenden Betriebsaufwand für identifizierte Risiken

Wie kann man auf technische Standards und hohe oder sehr hohe Risiken zugreifen

Wir haben die Dokumentation zu den technischen Standards von AMS als Bericht für Sie <https://console.aws.amazon.com/artifact/> als Referenz zur Verfügung gestellt. Anhand der Dokumentation zu den technischen Standards von AMS können Sie herausfinden, ob für eine Änderung die

Risikobereitschaft Ihres autorisierten Sicherheitskontakts erforderlich ist, bevor Sie einen Änderungsantrag (RFC) einreichen.

Suchen Sie den Bericht über technische Standards, indem Sie in der Suchleiste der Registerkarte AWS Artifact Berichte nach „AWS Managed Services (AMS) Technical Standards“ suchen, nachdem Sie sich mit der Standardeinstellung angemeldet haben `AWSMangedServicesChangeManagementRole`.

Note

Das technische Standarddokument von AMS ist für die Kunden_ReadOnly_Rolle in der landing zone mit einem Konto zugänglich. In der landing zone mit mehreren Konten, die `AWSManged ServicesAdminRole` von Sicherheitsadministratoren und von Anwendungsteams `AWSManged ServicesChangeManagementRole` verwendet wird, kann für den Zugriff auf das Dokument verwendet werden. Wenn Ihr Team eine benutzerdefinierte Rolle verwendet, erstellen Sie einen RFC „Andere“ | „Andere“, um Zugriff zu beantragen. Wir aktualisieren dann die angegebene benutzerdefinierte Rolle.

Verstehen Sie die Klassifizierungen von RFC-Änderungstypen

Die Änderungstypen, die Sie beim Einreichen eines RFC verwenden, sind in zwei große Kategorien unterteilt:

- **Bereitstellung:** Diese Klassifizierung dient der Erstellung von Ressourcen.
- **Verwaltung:** Diese Klassifizierung dient zum Aktualisieren oder Löschen von Ressourcen. Die Kategorie Verwaltung enthält auch Änderungstypen für den Zugriff auf Instanzen, das Verschlüsseln oder Teilen sowie das Starten AMIs, Stoppen, Neustarten oder Löschen von Stacks.

RFC-Aktionen und Aktivitätsstatus verstehen

`RfcActionState(API)/Activity State (Konsole)` helfen Ihnen dabei, den Status menschlicher Eingriffe oder Aktionen in einem RFC zu verstehen. Wird hauptsächlich für manuelle Zwecke verwendet und `RfcActionState` hilft Ihnen zu verstehen RFCs, wann entweder Sie oder AMS Operations Maßnahmen ergreifen müssen, und zeigt Ihnen, wann AMS Operations aktiv an Ihrem RFC arbeitet. Dies sorgt für mehr Transparenz in Bezug auf die Aktionen, die während des Lebenszyklus eines RFC ergriffen werden.

RfcActionStateDefinitionen für (API) /Aktivitätsstatus (Konsole):

- **AwsOperatorAssigned:** Ein AWS-Betreiber arbeitet aktiv an Ihrem RFC.
- **AwsActionPending:** Eine Antwort oder Aktion von AWS wird erwartet.
- **CustomerActionPending:** Eine Antwort oder Aktion des Kunden wird erwartet.
- **NoActionPending:** Weder von AWS noch vom Kunden sind Maßnahmen erforderlich.
- **NotApplicable:** Dieser Status kann nicht von AWS-Betreibern oder -Kunden festgelegt werden und wird nur für diejenigen verwendet RFCs , die vor der Veröffentlichung dieser Funktion erstellt wurden.

Der Status der RFC-Aktionen hängt davon ab, ob für den eingereichten Änderungstyp eine manuelle Überprüfung erforderlich ist und ob die Planung auf „ASAP“ gesetzt ist oder nicht.

- **ActionStateRFC-Änderungen während der Prüfung, Genehmigung und des Starts eines manuellen Änderungstyps mit verzögerter Planung:**
 - Nachdem Sie einen manuellen, geplanten RFC eingereicht haben, ändert sich dieser ActionState automatisch zu **AwsActionPending** zu dem Hinweis, dass ein Operator den RFC überprüfen und genehmigen muss.
 - Wenn ein Operator beginnt, Ihren RFC aktiv zu überprüfen, ändert sich der ActionState zu **AwsOperatorAssigned**
 - Wenn der Operator Ihren RFC genehmigt, ändert sich der RFC-Status in **Geplant** und der ActionState automatisch in **NoActionPending**
 - Wenn die geplante Startzeit des RFC erreicht ist, ändert sich der RFC-Status auf **InProgress** und der ActionState automatisch. Es wird angezeigt, dass ein Operator für die Überprüfung des RFC zugewiesen werden muss. **AwsActionPending**
 - Wenn ein Operator anfängt, den RFC aktiv auszuführen, ändert er den Wert in **AwsOperatorAssigned**
 - Sobald der Vorgang abgeschlossen ist, schließt der Operator den RFC. Dadurch wird der Wert automatisch auf **NoActionPending** geändert.

 Important

- Aktionsstatus können nicht von Ihnen festgelegt werden. Sie werden entweder automatisch auf der Grundlage von Änderungen im RFC oder manuell von AMS-Operatoren festgelegt.
- Wenn Sie einem RFC Korrespondenz hinzufügen, ActionState wird dieser automatisch auf gesetzt. `AwsActionPending`
- Wenn ein RFC erstellt wird, ActionState wird der automatisch auf gesetzt. `NoActionPending`
- Wenn ein RFC gesendet wird, ActionState wird der automatisch auf gesetzt. `AwsActionPending`
- Wenn ein RFC abgelehnt, storniert oder mit dem Status Erfolgreich oder Fehlgeschlagen abgeschlossen wird, ActionState wird er automatisch auf zurückgesetzt. `NoActionPending`
- Aktionsstatus sind sowohl für automatisierte als auch für manuelle Aktionen aktiviert RFCs, sind jedoch hauptsächlich für manuelle Aktionen von Bedeutung, RFCs da für diese Art von Aktionen RFCs häufig eine Kommunikation erforderlich ist.

Sehen Sie sich die Anwendungsfallbeispiele für RFC-Aktionsstatus an

Anwendungsfall: Sichtbarkeit bei manuellen RFC-Prozessen

- Sobald Sie einen manuellen RFC eingereicht haben, ändert sich der Status der RFC-Aktion automatisch in, `AwsActionPending` um anzuzeigen, dass ein Operator den RFC überprüfen und genehmigen muss. Wenn ein Operator beginnt, Ihren RFC aktiv zu überprüfen, ändert sich der RFC-Aktionsstatus auf. `AwsOperatorAssigned`
- Stellen Sie sich einen manuellen RFC vor, der genehmigt und geplant wurde und bereit ist, mit der Ausführung zu beginnen. Sobald sich der RFC-Status auf `ändertInProgress` ändert, ändert sich der RFC-Aktionsstatus automatisch auf. `AwsActionPending` Er ändert sich wieder auf, `AwsOperatorAssigned` sobald ein Operator den RFC aktiv ausführt.
- Wenn ein manueller RFC abgeschlossen ist (als „Erfolg“ oder „Fehlschlag“ geschlossen), ändert sich der Status der RFC-Aktion in, `NoActionPending` um anzuzeigen, dass weder vom Kunden noch vom Betreiber weitere Aktionen erforderlich sind.

Anwendungsfall: RFC-Korrespondenz

- Wenn es sich um einen manuellen RFC handelt, benötigt ein AMS-Operator möglicherweise weitere Informationen von Ihnen. Die Operatoren senden eine Nachricht an den RFC und ändern den RFC-Aktionsstatus auf `CustomerActionPending`. Wenn Sie antworten, indem Sie eine neue RFC-Korrespondenz hinzufügen, ändert sich der RFC-Aktionsstatus automatisch auf `AwsActionPending`.
- Wenn ein automatisierter oder manueller RFC ausgefallen ist, können Sie den RFC-Details eine Korrespondenz hinzufügen und den AMS-Operator fragen, warum der RFC fehlgeschlagen ist. Wenn Ihre Korrespondenz hinzugefügt wird, wird der RFC-Aktionsstatus automatisch auf `AwsActionPending` gesetzt. Wenn der AMS-Operator den RFC abrufen, um Ihre Korrespondenz einzusehen, ändert sich der RFC-Aktionsstatus auf `AwsOperatorAssigned`. Wenn der Operator antwortet, indem er eine neue RFC-Korrespondenz hinzufügt, kann der RFC-Aktionsstatus auf `CustomerActionPending` gesetzt werden, was bedeutet, dass eine weitere Antwort vom Kunden erwartet wird, oder auf `NoActionPending`, was bedeutet, dass keine Antwort vom Kunden erforderlich oder erwartet wird.

RFC-Statuscodes verstehen

RFC-Statuscodes helfen Ihnen dabei, Ihre Anfragen zu verfolgen. Sie können diese Statuscodes während eines RFC-Laufs in der CLI-Ausgabe oder durch Aktualisieren der RFC-Listenseite in der Konsole beobachten.

Sie können die Codes für einen RFC auch auf der Detailseite für diesen RFC sehen, die so aussehen könnte:

Möglicherweise finden Sie in Ihrer Liste einen RFC, den Sie nicht eingereicht haben. Wenn AMS-Operatoren einen CT verwenden, der nur intern verwendet wird, reichen sie ihn in einem RFC ein und er wird in Ihrer RFC-Liste angezeigt. Weitere Informationen finden Sie unter [Nur interne Änderungstypen](#).

Important

Sie können Benachrichtigungen über RFC-Statusänderungen anfordern. Einzelheiten finden Sie unter Benachrichtigungen über [RFC-Statusänderungen](#).

RFC-Statuscodes

Herzlichen Glückwunsch	Fehler
Bearbeitung: Der RFC wurde erstellt, aber nicht eingereicht PendingApproval /Eingereicht: Der RFC wurde eingereicht und das System ermittelt, ob er genehmigt werden muss, und holt diese Genehmigung, falls erforderlich, ein Genehmigt von AWS//Genehmigt vom Kunden: Der RFC wurde genehmigt. Automatisierte Geräte RFCs werden von AWS genehmigt, manuelle RFCs werden von Betreibern und manchmal auch von Kunden genehmigt Geplant: Der RFC hat die Syntax- und Anforderungsprüfungen bestanden und ist für die Ausführung geplant InProgress: Der RFC wird gerade ausgeführt. Beachten Sie, RFCs dass das Bereitstellen mehrerer Ressourcen oder die Ausführung mit langer Laufzeit UserData länger dauert Ausgeführt: Der RFC wurde ausgeführt Erfolgreich//Erfolgreich: Der RFC wurde erfolgreich abgeschlossen	Abgelehnt: RFCs werden in der Regel zurückgewiesen, weil sie nicht validiert werden können. Beispielsweise wurde eine unbrauchbare Ressource, d. h. ein Subnetz, angegeben Storniert: RFCs werden in der Regel storniert, weil sie die Validierung nicht bestehen, bevor die konfigurierte Startzeit abgelaufen ist Fehlgeschlagen: Der RFC ist ausgefallen. Die Gründe für den Fehler finden Sie StatusReason in der Ausgabe, und AMS Operations erstellt automatisch ein Trouble-Ticket und kommuniziert bei Bedarf mit Ihnen

 Note

Storniert oder abgelehnt RFCs können Sie erneut einreichen mit [UpdateRfc](#); siehe auch. [Aktualisierung RFCs](#)

Wenn der RFC alle erforderlichen Bedingungen erfüllt (z. B. wenn alle erforderlichen Parameter angegeben sind), ändert sich der Status in `PendingApproval` (auch bei automatisierter Ausführung ist CTs eine Genehmigung erforderlich, was automatisch geschieht, wenn Syntax- und Parameterprüfungen erfolgreich sind). Wenn er nicht erfolgreich ist, ändert sich der Status zu `Rejected`. Das `StatusReason` enthält Informationen zu Ablehnungen; die `ExecutionOutput` Felder enthalten Informationen zur Genehmigung und zum Abschluss. Zu den Fehlercodes gehören:

- `InvalidRfcStateException`: Der RFC befindet sich in einem Status, der die aufgerufene Operation nicht zulässt. Wenn der RFC beispielsweise in den Status `Eingereicht` übergegangen ist, kann er nicht mehr geändert werden.
- `InvalidRfcScheduleException`: Die `TimeoutInMinutes` Parameter `StartTime` `EndTime`, oder wurden verletzt.
- `InternalServerError`: Es ist ein Problem mit dem System aufgetreten.
- `InvalidArgumentException`: Ein Parameter ist falsch angegeben. Beispielsweise wird ein inakzeptabler Wert verwendet.
- `ResourceNotFoundException`: Ein Wert, z. B. die Stack-ID, kann nicht gefunden werden.

Wenn die geplanten angeforderten Start- und Endzeiten (auch bekannt als das Änderungszeitfenster) vor der Genehmigung der Änderung liegen, ändert sich der RFC-Status auf `Canceled`. Wenn die Änderung genehmigt wurde, ändert sich der RFC-Status auf `Scheduled`. Das Fenster für die Ausführung von Änderungen bei ASAP RFCs besteht aus der Zeit der Übermittlung zuzüglich des `ExpectedExecutionDuration` Werts für den CT.

Eine geplante Änderung (mit einem `RequestedStartTime` in der CLI eingereicht) kann jederzeit vor dem Eintreffen des Fensters für die Ausführung von Änderungen geändert oder storniert werden. Wenn die geplante Änderung geändert wird, muss sie erneut eingereicht werden.

Wenn die Startzeit der Änderung eintrifft (geplant oder so schnell wie möglich) und die Genehmigungen abgeschlossen sind, ändert sich der Status auf `InProgress` und es können keine Änderungen vorgenommen werden. Wenn die Änderung innerhalb des angegebenen Zeitfensters für die Ausführung von Änderungen abgeschlossen ist, ändert sich der Status in `Success`. Schlägt ein Teil der Änderung fehl oder ist die Änderung am Ende des Fensters für den Änderungsprozess noch in Bearbeitung, ändert sich der Status in `Failure`.

 Note

Während des Status „InProgressSuccess,“ oder „FailureChange“ kann der RFC nicht geändert oder abgebrochen werden.

Das folgende Diagramm zeigt den RFC-Status vom CreateRFC-Aufruf bis zur Auflösung.

Verstehen Sie das RFC-Update CTs und die Erkennung von CloudFormation Template-Drift

In AMS bereitgestellte Ressourcen verwenden eine modifizierte CloudFormation Vorlage. Wenn bei einer Ressource ein Parameter direkt über die AWS Management Console eines Dienstes geändert wurde, ist der CloudFormation Erstellungsdatensatz dieser Ressource nicht mehr synchron. Wenn dies passiert und Sie versuchen, einen AMS-Aktualisierungsänderungstyp zu verwenden, um die Ressource in AMS zu aktualisieren, verweist AMS auf die ursprüngliche Ressourcenkonfiguration und setzt möglicherweise geänderte Parameter zurück. Dieser Reset kann schädlich sein, weshalb AMS die Verwendung von RFCs Update-Änderungstypen nicht zulässt, wenn zusätzliche AMS-Konfigurationsänderungen erkannt werden.

Verwenden Sie den Konsolenfilter, um eine Liste der Arten von Update-Änderungen zu erhalten.

Behebung von Abweichungen FAQs

Fragen und Antworten zur Behebung von AMS-Abweichungen. Es gibt zwei Arten von Änderungen, mit denen Sie die Behebung von Abweichungen einleiten können: Der eine ist Ausführungsmodus=manuell oder „Überprüfung erforderlich“, der andere ist Ausführungsmodus=automatisiert.

Unterstützte Ressourcen zur Drift-Korrektur (ct-3kinq0u4l33zf)

Dies sind die Ressourcen, die vom Änderungstyp „Drift Remediation“ (ct-3kinq0u4l33zf) unterstützt werden. Verwenden Sie zur Behebung von Ressourcen stattdessen den Änderungstyp „Überprüfung erforderlich“ (ct-34sxfo53yuzah).

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
```

```
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

Änderungstypen für Drift-Korrektur

Fragen und Antworten zur Verwendung der Änderungstypen für die AMS-Drift-Korrektur

Eine Liste der unterstützten Ressourcen für die Drift-Korrekturfunktion finden Sie unter. [Unterstützte Ressourcen zur Drift-Korrektur \(ct-3king0u4l33zf\)](#)

Important

Bei der Drift-Korrektur werden die and/or Parameter der Stack-Vorlagen geändert, und es ist zwingend erforderlich, dass Sie Ihre lokalen Template-Repositorys oder alle Automatisierungen, die diese Stacks aktualisieren, aktualisieren, sodass sie die neuesten Stack-Vorlagen und -Parameter verwenden. Die Verwendung alter and/or Vorlagenparameter ohne Synchronisierung kann zu schädlichen Änderungen an den zugrunde liegenden Ressourcen führen.

Das automatisierte CT (ct-3king0u4l33zf) unterstützt die Korrektur von nur 10 Ressourcen pro RFC. Um die verbleibenden Ressourcen in Stapeln von 10 zu korrigieren, erstellen Sie neue Ressourcen, bis alle Ressourcen behoben sind. RFCs

Welchen Änderungstyp für Drift Remediation sollte ich verwenden?

Wir empfehlen, das automatisierte CT (ct-3king0u4l33zf) ohne Überprüfung zu verwenden, wenn:

- Sie versuchen, eine Aktualisierung einer vorhandenen Stack-Ressource mithilfe eines automatisierten CT durchzuführen, und der RFC wird unverändert zurückgewiesen. DRIFTED
- Sie haben in der Vergangenheit ein Update CT verwendet und es ist fehlgeschlagen, weil der Stack DRIFTED wurde. Sie müssen nicht erneut versuchen, ein Update durchzuführen, sondern können stattdessen die manuelle Überprüfung durchführen.

Wir empfehlen, das für die Überprüfung erforderliche manuelle CT (ct-34sxfo53yuzah) nur dann zu verwenden, wenn fehlerhafte Ressourcentypen von der Drift-Behebung nicht unterstützt werden (keine Überprüfung erforderlich), automatisiert, CT (ct-3king0u4l33zf) oder wenn die Drift-Korrektur (keine Überprüfung erforderlich), automatisiert, CT fehlschlägt.

Welche Änderungen werden während der Problembehebung am Stack vorgenommen?

Für die Wiederherstellung sind Aktualisierungen der and/or Parameter der Stack-Vorlage erforderlich, je nachdem, welche Eigenschaften verändert wurden. Bei der Wiederherstellung wird auch die Stack-Richtlinie des Stacks während der Wiederherstellung aktualisiert und die Stack-Richtlinie nach Abschluss der Wiederherstellung auf ihren vorherigen Wert zurückgesetzt.

Wie können wir sehen, welche Änderungen an den Parametern der Stack-Vorlage vorgenommen wurden? and/or

In der Antwort auf den RFC wird eine Zusammenfassung der Änderungen mit den folgenden Informationen bereitgestellt:

- `ChangeSummaryJson`: Enthält eine Zusammenfassung der Änderungen der and/or Stack-Vorlagenparameter als Teil der Drift-Korrektur. Die Sanierung wird in mehreren Phasen durchgeführt. Diese Änderungsübersicht besteht aus Änderungen für einzelne Phasen. Wenn die Korrektur erfolgreich ist, überprüfen Sie die Änderungen der letzten Phase. `ExecutionPlan` In der JSON-Datei finden Sie die Phasen, die der Reihe nach ausgeführt wurden. Beispielsweise wird ein `RestoreReferences` Abschnitt, wenn er vorhanden ist, immer am Ende ausgeführt und enthält JSON für Änderungen nach der Korrektur. Wenn die Wiederherstellung im `DryRun` Modus ausgeführt würde, wäre keine dieser Änderungen auf den Stack angewendet worden.
- `PreRemediationStackTemplateAndConfigurationJson`: Enthält einen Konfigurations-Snapshot des CloudFormation Stacks, einschließlich Vorlage, Parametern und Ausgaben, `StackPolicyBody` bevor die Korrektur auf dem Stack ausgelöst wurde.

Was muss ich tun, nachdem die Korrektur durchgeführt wurde?

Important

Sie müssen Ihre lokalen Vorlagen-Repositorys oder jegliche Automatisierung, die den Stack mit den Korrigierungen aktualisieren würde, mit den neuesten Vorlagen und Parametern aktualisieren, die in der RFC-Zusammenfassung enthalten sind. Dies ist sehr wichtig, da die Verwendung der alten and/or Vorlagenparameter zu weiteren zerstörerischen Änderungen an den Stack-Ressourcen führen kann.

Wird meine Anwendung während dieser Sanierung beeinträchtigt?

Die Wiederherstellung ist ein Offline-Prozess, der nur für die CloudFormation Stack-Konfiguration ausgeführt wird. An der zugrunde liegenden Ressource werden keine Aktualisierungen durchgeführt.

Kann ich weiterhin Verwaltung | Andere | Andere verwenden RFCs , um nach der Wiederherstellung Aktualisierungen an Ressourcen durchzuführen?

Wir empfehlen, dass Sie Aktualisierungen der Stack-Ressourcen immer mithilfe des verfügbaren automatisierten Updates CTs durchführen. Wenn das verfügbare Update Ihren Anwendungsfall CTs nicht unterstützt, verwenden Sie Verwaltung | Andere | Andere Anfragen.

Werden durch die Problembehebung neue Ressourcen im Stack erstellt?

Durch die Behebung werden keine neuen Ressourcen im Stack erstellt. Bei der Behebung werden jedoch neue Ausgaben erstellt und der Abschnitt mit den [Metadaten](#) der Stack-Vorlage aktualisiert, sodass die Zusammenfassung der Problembehebung als Referenz gespeichert wird.

Wird die Problembehebung immer erfolgreich sein?

Die Behebung erfordert eine sorgfältige Analyse und Validierung der Vorlagenkonfiguration, um festzustellen, ob sie durchgeführt werden kann. In Szenarien, in denen diese Validierungen fehlschlagen, wird der Behebungsprozess gestoppt und es werden keine Änderungen an der Stack-Vorlage oder den Parametern vorgenommen. Außerdem kann die Korrektur nur für unterstützte Ressourcentypen durchgeführt werden.

Wie kann ich Aktualisierungen an Stack-Ressourcen durchführen, wenn die Behebung nicht erfolgreich ist?

Sie können das Update Management | Other | Other | Update CT (ct-0xdawir96cy7k) verwenden, um Änderungen anzufordern. AMS überwacht solche Szenarien und arbeitet an der Verbesserung der Behebungslösung.

Kann ich Stacks korrigieren, die sowohl unterstützte als auch nicht unterstützte Ressourcentypen haben?

Ja. Die Wiederherstellung wird jedoch nur durchgeführt, wenn die unterstützten Ressourcentypen im Stack DRIFTED gefunden werden. Wenn nicht unterstützte Ressourcentypen DRIFTED sind, wird die Behebung nicht fortgesetzt.

Kann ich eine Problembehebung für Stacks beantragen, die durch Ingest außerhalb von CFN erstellt wurden? CTs

Ja. Die Korrektur kann für Stacks unabhängig vom Änderungstyp durchgeführt werden, der für die Erstellung des Stacks verwendet wurde.

Kann ich vor der Behebung wissen, welche Änderungen am Stack vorgenommen werden würden?

Ja. Beide Änderungstypen bieten eine DryRunOption, mit der Sie Änderungen anfordern können, die bei einer Korrektur des Stacks vorgenommen würden. Die endgültigen Korrekturänderungen können jedoch je nach der Abweichung, die zum Zeitpunkt der Korrektur auf dem Stack vorhanden war, unterschiedlich sein.

Zeitplan RFCs

Mit der Planungsfunktion können Sie eine Startzeit für RFCs auswählen. Die folgenden Optionen sind in der Planungsfunktion verfügbar:

- Führen Sie diese Änderung so schnell wie möglich aus: AMS führt den RFC aus, sobald er genehmigt wurde. Die meisten CTs werden automatisch genehmigt. Verwenden Sie diese Option, wenn der RFC nicht zu einem bestimmten Zeitpunkt starten soll.
- Planen Sie diese Änderung: Legen Sie einen Tag, eine Uhrzeit und eine Zeitzone fest, an der der RFC ausgeführt werden soll. Bei automatisierten Änderungstypen empfiehlt es sich, eine Startzeit anzufordern, die mindestens 10 Minuten nach der geplanten Einreichung des RFC liegt. Für die Überprüfung der erforderlichen Änderungstypen ist es erforderlich, dass Sie eine Startzeit beantragen, die mindestens 24 Stunden nach der geplanten Einreichung des RFC liegt. Wenn der RFC bis zur konfigurierten Startzeit nicht genehmigt wird, wird der RFC abgelehnt.

Legen Sie einen RFC-Zeitplan fest

Verwenden Sie eine der folgenden Methoden, um einen RFC zu planen:

Führen Sie diese Änderung so schnell wie möglich aus:

- Konsole: Nichts tun. Dabei wird der standardmäßige RFC-Zeitplan verwendet.
- API oder CLI: Entfernen Sie die RequestedEndTime Optionen RequestedStartTime und im Vorgang Create RFC.

ASAP „Überprüfung erforderlich“ RFCs werden automatisch abgelehnt, wenn sie nicht innerhalb von dreißig Tagen nach Einreichung genehmigt werden.

Planen Sie diese Änderung ein:

- Konsole: Wählen Sie das Optionsfeld Diese Änderung planen aus. Ein Bereich mit der Startzeit wird geöffnet. Geben Sie manuell einen Tag ein oder verwenden Sie das Kalender-Widget, um einen Tag auszuwählen. Geben Sie eine Uhrzeit in UTC ein, ausgedrückt im Format ISO 8601, und verwenden Sie die Dropdownliste, um einen Ort auszuwählen. Standardmäßig verwendet AMS das ISO 8601-Format YYYYMMDDThhmmss Z YYYY-MM-DDThh oder:MM:SSZ. Beide Formate werden akzeptiert.

Note

Die Standard-Endzeit liegt 4 Stunden nach der von Ihnen eingegebenen Startzeit. Um die Endzeit Ihrer geplanten Änderung auf mehr als 4 Stunden festzulegen, verwenden Sie die API oder CLI, um die Änderung auszuführen.

- API oder CLI: Senden Sie Werte für die RequestedEndTime Parameter RequestedStartTime und im Vorgang Create RFC. Durch die Übergabe eines konfigurierten Elements wird die Ausführung eines automatisierten Änderungstyps, der bereits gestartet wurde, RequestedEndTime nicht gestoppt. Bei einem Änderungstyp „Überprüfung erforderlich“ können Sie eine Verlängerung beantragen oder Sie werden möglicherweise aufgefordert, den RFC erneut einzureichen, wenn der Änderungstyp „Überprüfung erforderlich“ noch nicht abgeschlossen ist und Sie mit AMS in Kontakt stehen. RequestedEndTime

 Tip

Ein Beispiel für eine Anzeige der UTC-Zeit finden Sie unter [UTC](#) auf der Time-IS-Website.
Beispiel für ein ISO 8601-Format für den date/time Wert 2016-12-05 um 14:20 Uhr:
2016-12-05T 14:20:00 Z oder 20161205T142000Z.

Wenn Sie angeben...

- nur `aRequestedStartTime`, der RFC gilt als geplant und der `RequestedEndTime` wird mit dem `ExecutionDurationInMinutes` Wert gefüllt.
- nur `aRequestedEndTime`, wir werfen eine `InvalidArgumentException`.
- `RequestedStartTimes` sowohl als auch `RequestedEndTime`, wir überschreiben die `RequestedEndTime` mit der angegebenen Startzeit plus dem `ExecutionDurationInMinutes` Wert.
- `RequestedStartTime` weder noch `RequestedEndTime`, wir behalten diese Werte bei Null und der RFC wird als ASAP-RFC behandelt.

 Note

Für alle geplanten Änderungen wird eine nicht spezifizierte Endzeit angegeben RFCs, die aus der Uhrzeit des angegebenen Zeitpunkts `RequestedStartTime` plus dem `ExpectedExecutionDurationInMinutes` Attribut des übermittelten Änderungstyps besteht. Wenn der beispielsweise „60“ (Minuten) `ExpectedExecutionDurationInMinutes` ist und der angegebene Wert 2016-12-05T14:20:00Z (5. Dezember 2016 um 4:20 Uhr) `RequestedStartTime` ist, würde die tatsächliche Endzeit auf den 5. Dezember 2016 um 5:20 Uhr festgelegt. Um den `ExpectedExecutionDurationInMinutes` für einen bestimmten Änderungstyp zu finden, führen Sie diesen Befehl aus:

```
aws amscm --profile saml get-change-type-version --  
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.  
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```


Verwenden Sie die Option RFC-Priorität

Verwenden Sie die Option `Priorität` in `execution mode = manual` Änderungstypen, um AMS Operations auf die Dringlichkeit der Anfrage hinzuweisen.

Option `Priorität` in `inexecution mode = manual`:

Geben Sie die Priorität eines manuellen RFC als Hoch, Mittel oder Niedrig an. RFCs Als hoch eingestuft werden, werden geprüft und genehmigt, bevor sie als Mittel RFCs eingestuft werden. Dabei gelten die RFC-Servicelevel-Ziele (SLOs) und deren Einreichungszeiten. RFCs mit niedriger Priorität oder ohne angegebene Priorität werden in der Reihenfolge verarbeitet, in der sie eingereicht wurden.

Genehmigen oder Ablehnen RFCs

RFCs Die Vorlage mit der erforderlichen Genehmigung (manuell) CTs muss von Ihnen oder AMS genehmigt werden. Vorab genehmigte Daten werden automatisch verarbeitet CTs . Weitere Informationen finden Sie unter [Anforderungen an die CT-Zulassung](#).

Note

Wenn Sie „Überprüfung erforderlich“ verwenden CTs, empfiehlt AMS, die ASAP-Scheduling-Option zu verwenden (wählen Sie ASAP in der Konsole, lassen Sie Start- und Endzeit leer in der API/CLI), da diese einen AMS-Operator CTs erfordern, der den RFC überprüft und möglicherweise mit Ihnen kommuniziert, bevor er genehmigt und ausgeführt werden kann. Wenn Sie diese einplanen, achten Sie darauf RFCs, dass Sie mindestens 24 Stunden einplanen. Wenn die Genehmigung nicht vor der geplanten Startzeit erfolgt, wird der RFC automatisch abgelehnt.

Wenn ein für eine Genehmigung erforderlicher RFC erfolgreich von AMS eingereicht wurde, muss er von Ihnen ausdrücklich genehmigt werden. Oder wenn Sie einen RFC einreichen, für den eine Genehmigung erforderlich ist, muss dieser von AMS genehmigt werden. Wenn Sie einen von AMS eingereichten RFC genehmigen müssen, erhalten Sie eine E-Mail oder eine andere vorab festgelegte Mitteilung mit der Bitte um Genehmigung. Die Kommunikation beinhaltet die RFC-ID. Nachdem die Kommunikation gesendet wurde, führen Sie einen der folgenden Schritte aus:

- Konsole Genehmigen oder Ablehnen: Verwenden Sie die RFC-Detailseite für den entsprechenden RFC:

- API//CLI Approve: [ApproveRfc](#) markiert eine Änderung als genehmigt. Die Maßnahme muss sowohl vom Eigentümer als auch vom Betreiber ergriffen werden, falls beide erforderlich sind. Im Folgenden finden Sie ein Beispiel für einen CLI-Genehmigungsbefehl. Ersetzen Sie im folgenden Beispiel RFC_ID durch die entsprechende RFC-ID.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API//CLI Reject: [RejectRfc](#) markiert eine Änderung als abgelehnt. Im Folgenden finden Sie ein Beispiel für einen CLI-Ablehnungsbefehl. Ersetzen Sie im folgenden Beispiel RFC_ID durch die entsprechende RFC-ID.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

RFC-eingeschränkte Laufzeiten anfordern

Früher als Sperrtage bezeichnet, können Sie die Einschränkung bestimmter Zeiträume beantragen. Während dieser Zeiten können keine Änderungen vorgenommen werden.

Um einen eingeschränkten Ausführungszeitraum festzulegen, verwenden Sie die [UpdateRestrictedExecutionTimes](#) API-Operation und legen Sie einen bestimmten Zeitraum in UTC fest. Der von Ihnen angegebene Zeitraum hat Vorrang vor allen zuvor angegebenen Zeiträumen. Wenn Sie einen RFC während der angegebenen eingeschränkten Laufzeit einreichen, schlägt die Übermittlung fehl und es wird der Fehler Ungültiger RFC-Zeitplan angezeigt. Sie können bis zu 200 eingeschränkte Zeiträume angeben. Standardmäßig ist kein eingeschränkter Zeitraum festgelegt. Im Folgenden finden Sie ein Beispiel für einen Anforderungsbefehl (mit konfigurierter SAML-Authentifizierung):

```
aws amscm --profile saml update-restricted-execution-times --restricted-execution-times='[{"TimeRange":{"StartTime":"2018-01-01T12:00:00Z","EndTime":"2018-01-01T12:00:01Z"}}]'
```

Sie können Ihre aktuelle RestrictedExecutionTimes Einstellung auch anzeigen, indem Sie den [ListRestrictedExecutionTimes](#) API-Vorgang ausführen. Beispiel:

```
aws amscm --profile saml list-restricted-execution-times
```

Wenn Sie einen RFC während einer bestimmten eingeschränkten Ausführungszeit einreichen möchten, fügen Sie den RestrictedExecutionTimesOverrideId mit dem Wert von

OverrideRestrictedTimeRangeshinzu und senden Sie den RFC dann wie gewohnt weiter. Es hat sich bewährt, diese Methode nur für kritische RFCs oder Notfall-RFCs zu verwenden. Weitere Informationen finden Sie in der API-Referenz für [SubmitRfc](#).

Erstellen, Klonen, Aktualisieren, Suchen und Stornieren RFCs

Die folgenden Beispiele führen Sie durch verschiedene RFC-Operationen.

Themen

- [Erstellen Sie einen RFC](#)
- [Mit der AMS-Konsole klonen RFCs \(neu erstellen\)](#)
- [Aktualisierung RFCs](#)
- [Finden RFCs](#)
- [Stornieren RFCs](#)

Erstellen Sie einen RFC

Einen RFC mit der Konsole erstellen

Im Folgenden finden Sie die erste Seite des RFC-Erstellungsprozesses in der AMS-Konsole, auf der Quick Cards geöffnet und Browse-Änderungstypen aktiv sind:

Im Folgenden finden Sie die erste Seite des RFC-Erstellungsprozesses in der AMS-Konsole, auf der die Option Nach Kategorie auswählen aktiviert ist:

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCs zu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebigen Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
 - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebiges CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.

- Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.
3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.

4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Optional können Sie den RFC abbrechen oder eine Kopie davon mit den Optionen oben auf der Seite erstellen.

Einen RFC mit der CLI erstellen

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id ID` Befehl RFC: mit der zurückgegebenen RFC-ID ein.

Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id ID`

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter  
Attribute=ChangeTypeId,Value=CT_ID
```

Note

Sie können alle CreateRfc Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\" Eine Liste aller CreateRfc Parameter finden Sie in der [AMS Change Management API-Referenz](#).

INLINE-ERSTELLUNG:

Geben Sie den Befehl create rfc mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title  
"TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

VORLAGE ERSTELLEN:

Note

In diesem Beispiel für die Erstellung eines RFC wird der Stack-Änderungstyp Load Balancer (ELB) verwendet.

1. Suchen Sie das entsprechende CT. Der folgende Befehl durchsucht CT-Klassifizierungszusammenfassungen nach solchen, die „ELB“ im Artikelnamen enthalten, und erstellt eine Ausgabe der Kategorie, des Artikels, der Operation und der ChangeType ID in Tabellenform (Unterkategorie für beide istAdvanced stack components).

```
aws amscm list-change-type-classification-summaries --query
"ChangeTypeClassificationSummaries[?contains(Item, 'ELB')].
[Category,Item,Operation,ChangeTypeId]" --output table
```

```
-----
|                               CtSummaries                               |
+-----+-----+-----+-----+-----+-----+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7j1 |
| Management| Load balancer (ELB) stack | Update | ct-01tm873rsebx9 |
+-----+-----+-----+-----+-----+-----+

```

2. Finden Sie die aktuellste Version des CT:

ChangeTypeId und ChangeTypeVersion: Die Änderungstyp-ID für diese exemplarische Vorgehensweise lautet ct-123h45t6uz7j1 (create ELB). Um die neueste Version herauszufinden, führen Sie diesen Befehl aus:

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=ct-123h45t6uz7j1
```

3. Informieren Sie sich über die Optionen und Anforderungen. Der folgende Befehl gibt das Schema in eine JSON-Datei namens CreateElbParams.json aus.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7j1" --query
"ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. Ändern und speichern Sie die JSON-Datei mit den Ausführungsparametern. In diesem Beispiel wird die Datei „CreateElbParams.json“ genannt.

Bei einem Bereitstellungs-CT StackTemplatId ist das im Schema enthalten und muss in den Ausführungsparametern eingereicht werden.

Für die Angabe TimeoutInMinutes, wie viele Minuten für die Erstellung des Stacks vorgesehen sind, bevor der RFC fehlschlägt, verzögert diese Einstellung die RFC-Ausführung nicht, aber Sie müssen genügend Zeit einplanen (geben Sie beispielsweise nicht „5“ an). Gültige Werte sind „60“ bis „360“, für CTs Langzeitanwendungen UserData: Create und Create EC2 ASG. Wir empfehlen für alle anderen Bereitstellungen den zulässigen Höchstwert von „60“. CTs

Geben Sie die ID der VPC an, in der der Stack erstellt werden soll. Sie können die VPC-ID mit dem CLI-Befehl abrufen. `aws amsskms list-vpc-summaries`

```
{
  "Description":      "ELB-Create-RFC",
  "VpcId":            "VPC_ID",
  "StackTemplateId":  "stm-sdhopv000000000000",
  "Name":             "MyElbInstance",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "ELBSubnetIds":      ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold": 4,
    "ELBHealthCheckInterval": 5,
    "ELBHealthCheckTarget": "HTTP:80/",
    "ELBHealthCheckTimeout": 60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":         false
  }
}
```

5. Geben Sie die RFC-JSON-Vorlage in eine Datei in Ihrem aktuellen Ordner namens `.json` aus: `CreateElbRfc`

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Ändern und speichern Sie die `CreateElbRfc` JSON-Datei. Da Sie die Ausführungsparameter in einer separaten Datei erstellt haben, entfernen Sie die `ExecutionParameters` Zeile. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
{
  "ChangeTypeVersion": "2.0",
  "ChangeTypeId":      "ct-123h45t6uz7jl",
  "Title":             "Create ELB"
}
```

7. Erstellen Sie den RFC. Der folgende Befehl spezifiziert die Ausführungsparameterdatei und die RFC-Vorlagendatei:

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-parameters file://CreateElbParams.json
```

Sie erhalten die ID des neuen RFC in der Antwort und können sie verwenden, um den RFC zu senden und zu überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

Note

Sie können das AMS verwenden, um einen RFC API/CLI zu erstellen, ohne eine RFC-JSON-Datei oder eine JSON-Datei mit CT-Ausführungsparametern zu erstellen. Dazu verwenden Sie den `create-rfc` Befehl und fügen dem Befehl die erforderlichen RFC- und Ausführungsparameter hinzu. Dies wird „Inline Create“ genannt. Beachten Sie, dass alle Bereitstellungen CTs innerhalb des `execution-parameters` Blocks ein `Parameters` Array mit den Parametern für die Ressource enthielten. Die Parameter müssen Anführungszeichen enthalten, die mit einem umgekehrten Schrägstrich (\) maskiert werden. Die andere dokumentierte Methode zur Erstellung eines RFC heißt „Template Create“. Hier erstellen Sie eine JSON-Datei für die RFC-Parameter und eine weitere JSON-Datei für die Ausführungsparameter und senden die beiden Dateien mit dem `create-rfc` Befehl ab. Diese Dateien können als Vorlagen dienen und für die future wiederverwendet werden. RFCs Bei der Erstellung RFCs mit Vorlagen können Sie einen Befehl verwenden, um die JSON-Datei mit dem gewünschten Inhalt zu erstellen, indem Sie einen Befehl wie in der Abbildung gezeigt ausführen. Die Befehle erstellen eine Datei mit dem Namen „parameters.json“ mit dem angezeigten Inhalt. Sie können diese Befehle auch verwenden, um die RFC-JSON-Datei zu erstellen.

Mit der AMS-Konsole klonen RFCs (neu erstellen)

Sie können die AMS-Konsole verwenden, um einen vorhandenen RFC zu klonen.

Gehen Sie folgendermaßen vor, um einen RFC mithilfe der AMS-Konsole zu klonen oder neu zu erstellen:

1. Suchen Sie den entsprechenden RFC. Klicken Sie in der linken Navigationsleiste auf RFCs.

Das RFCs Dashboard wird geöffnet.

2. Scrollen Sie durch die Seiten, bis Sie den RFC gefunden haben, den Sie klonen möchten. Verwenden Sie die Option `Filter`, um die Liste einzugrenzen. Wählen Sie den RFC aus, den Sie klonen möchten.

Die RFC-Detailseite wird geöffnet.

3. Klicken Sie auf `Kopie erstellen`.

Die Seite „Änderungsantrag erstellen“ wird geöffnet, auf der alle Optionen wie im ursprünglichen RFC festgelegt sind.

4. Nehmen Sie die gewünschten Änderungen vor. Um zusätzliche Optionen festzulegen, ändern Sie die Option `Basic` in `Advanced`. Nachdem Sie alle Optionen festgelegt haben, wählen Sie `Absenden`.

Die aktive RFC-Detailseite wird mit einer neuen RFC-ID für den geklonten RFC geöffnet, und der geklonte RFC wird im RFC-Dashboard angezeigt.

Aktualisierung RFCs

Sie können einen zurückgewiesenen oder noch nicht eingereichten RFC erneut einreichen, indem Sie den RFC aktualisieren und ihn dann einreichen oder erneut einreichen. Beachten Sie, dass die meisten abgelehnten RFCs werden, weil der angegebene Wert vor der Einreichung bestanden `RequestedStartTime` wurde oder der angegebene Wert für die Ausführung des RFC nicht `TimeoutInMinutes` ausreicht (da ein erfolgreicher RFC `TimeoutInMinutes` nicht verlängert wird, empfehlen wir, diesen Wert immer auf mindestens „60“ und bis zu „360“ für eine Amazon- EC2 oder Amazon EC2 Auto Scaling Scaling-Gruppe mit langer Laufzeit zu setzen). `UserData` In diesem Abschnitt wird beschrieben, wie Sie die CLI-Version des `UpdateRfc` Befehls verwenden, um einen RFC mit einem neuen RFC-Parameter oder mit neuen Parametern zu aktualisieren, die entweder stringifiziertes JSON oder eine aktualisierte Parameterdatei verwenden.

Dieses Beispiel beschreibt die Verwendung der CLI-Version der `UpdateRfc` AMS-API (siehe [Update RFC](#)). Es gibt zwar Änderungstypen für die Aktualisierung einiger Ressourcen (DNS privat und öffentlich, Load Balancer-Stacks und Stack-Patching-Konfiguration), aber es gibt kein CT zur Aktualisierung eines RFC.

Wir empfehlen, dass Sie jeweils einen `UpdateRfc` Vorgang einreichen. Wenn Sie mehrere Updates einreichen, z. B. für einen DNS-Stack, schlagen die Aktualisierungen möglicherweise fehl, wenn versucht wird, den DNS gleichzeitig zu aktualisieren.

ERFORDERLICHE DATENRfcId: Der RFC, den Sie aktualisieren.

OPTIONALE DATENExecutionParameters: Sofern Sie kein nicht erforderliches Feld aktualisieren, würden Sie beispielsweise geänderte Ausführungsparameter angebenDescription, um die Probleme zu beheben, die dazu geführt haben, dass der RFC abgelehnt oder storniert wurde. Alle übermittelten Werte, die nicht Null sind, überschreiben diese Werte im ursprünglichen RFC.

1. Suchen Sie den entsprechenden abgelehnten oder stornierten RFC. Sie können diesen Befehl verwenden (Sie können den Wert durch ersetzen): Canceled

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. Sie können jeden der folgenden RFC-Parameter ändern:

```
{
  "Description": "string",
  "ExecutionParameters": "string",
  "ExpectedOutcome": "string",
  "ImplementationPlan": "string",
  "RequestedEndTime": "string",
  "RequestedStartTime": "string",
  "RfcId": "string",
  "RollbackPlan": "string",
  "Title": "string",
  "WorstCaseScenario": "string"}
```

Beispielbefehl zur Aktualisierung des Felds Beschreibung:

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
--region us-east-1
```

Beispielbefehl zur Aktualisierung des ExecutionParameters VpcId Felds:

```
aws amscm update-rfc --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
"RFC_ID" --region us-east-1
```

Beispielbefehl, der den RFC mit einer Ausführungsparameterdatei aktualisiert, die die Aktualisierungen enthält; siehe Beispiel für eine Ausführungsparameterdatei in Schritt 2 von: [EC2 stack | Create](#):

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --  
rfc-id "RFC_ID" --region us-east-1
```

3. Reichen Sie den RFC erneut ein `submit-rfc` und verwenden Sie dabei dieselbe RFC-ID, die Sie bei der ersten Erstellung des RFC haben:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Wenn der RFC erfolgreich ist, erhalten Sie in der Befehlszeile keine Bestätigungs- oder Fehlermeldungen.

4. Führen Sie den folgenden Befehl aus, um den Status der Anforderung zu überwachen und die Ausführungsausgabe anzuzeigen.

```
aws amscm get-rfc --rfc-id RFC_ID
```

Finden RFCs

Suchen Sie mit der Konsole nach einer Änderungsanforderung (RFC)

Gehen Sie folgendermaßen vor, um mithilfe der AMS-Konsole nach einem RFC zu suchen.

Note

Dieses Verfahren gilt nur für geplante RFCs Benutzer, die RFCs die ASAP-Option nicht verwendet haben.

1. Klicken Sie in der linken Navigationsleiste auf RFCs.

Das RFCs Dashboard wird geöffnet.

2. Scrollen Sie durch die Liste oder verwenden Sie die Option Filter, um die Liste zu verfeinern.

Die RFC-Liste ändert sich je nach Filterkriterium.

3. Wählen Sie den Betreff-Link für den gewünschten RFC.

Die RFC-Detailseite für diesen RFC wird mit Informationen wie der RFC-ID geöffnet.

4. Wenn das Dashboard viele enthält RFCs , können Sie die Option Filter verwenden, um nach RFC zu suchen:

- **Betreff:** Die Betreffzeile oder der Titel (in der API/CLI), der dem RFC bei seiner Erstellung gegeben wurde.
- **RFC-ID:** Die Kennung für den RFC.
- **Aktivitätsstatus:** Wenn Sie den RFC-Status kennen, können Sie wählen, ob ein Operator gerade den RFC betrachtet, `AwsOperatorAssigned` was `AwsActionPending` bedeutet, dass ein AMS-Operator etwas ausführen muss, bevor die RFC-Ausführung fortgesetzt werden kann, oder `CustomerActionPending` ob Sie eine Aktion ausführen müssen, bevor die RFC-Ausführung fortgesetzt werden kann.
- **Status:** Wenn Sie den RFC-Status kennen, können Sie wählen zwischen:
 - **Geplant:** RFCs die geplant waren.
 - **Abgesagt:** RFCs die wurden storniert.
 - **In Bearbeitung:** RFCs In Bearbeitung.
 - **Erfolgreich:** RFCs Das wurde erfolgreich ausgeführt.
 - **Abgelehnt:** RFCs die wurden abgelehnt.
 - **Bearbeitung:** RFCs die gerade bearbeitet werden.
 - **Fehl Schlag:** RFCs das ist fehlgeschlagen.
 - **Ausstehende Genehmigung:** RFCs Dies kann erst fortgesetzt werden, wenn AMS oder Sie die Genehmigung erteilt haben. In der Regel bedeutet dies, dass Sie den RFC genehmigen müssen. Sie werden in Ihrer Liste der Serviceanfragen eine entsprechende Servicebenachrichtigung erhalten haben.
- **Typ ändern:** Wählen Sie die Kategorie, Unterkategorie, Artikel und Vorgang aus, und die ID des Änderungstyps wird für Sie abgerufen.
- **Angeforderte Startzeit oder Angeforderte Endzeit:** Mit dieser Filteroption können Sie „Vorher“ oder „Nachher“ wählen und dann ein Datum und optional eine Uhrzeit (hh:mm und Zeitzone) eingeben. Dieser Filter funktioniert nur nach Zeitplan erfolgreich RFCs (nicht so schnell wie RFCs möglich).
- **Status:** Entweder geplant, Storniert, In Bearbeitung, Erfolgreich, Abgelehnt, Bearbeitung oder Fehlgeschlagen.
- **Betreff:** Der Betreff (oder Titel, wenn der RFC mit der API/CLI erstellt wurde), den Sie dem RFC gegeben haben.

Mit der Suche können Sie die Filter hinzufügen, wie im folgenden Screenshot gezeigt.

5. Klicken Sie auf den Betreff-Link für den gewünschten RFC.

Die RFC-Detailseite für diesen RFC mit Informationen, einschließlich der RFC-ID, wird geöffnet.

Einen Änderungsantrag (RFC) mit der CLI finden

Sie können mehrere Filter verwenden, um einen RFC zu finden.

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter  
Attribute=ChangeTypeId,Value=CT_ID
```

Note

Sie können alle CreateRfc Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\" Eine Liste aller CreateRfc Parameter finden Sie in der [AMS Change Management API-Referenz](#).

Wenn Sie sich die RFC-ID nicht notieren und sie später finden müssen, können Sie das AMS Change Management (CM) -System verwenden, um danach zu suchen und die Ergebnisse mit einem Filter oder einer Abfrage einzugrenzen.

1. Der [ListRfcSummaries](#)CM-API-Vorgang verfügt über Filter. Sie können Ergebnisse auf der Grundlage einer Value Kombination aus Attribute und in einer logischen UND-Operation oder basierend auf einem AttributeCondition, einem und [filtern](#)Values.

RFC-Filterung

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
ActualEndTime	Eine beliebige Zeichenfolge, die eine ISO86 01-Datetime darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
ActualStartTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
AutomationStatusId	Manuell, Automatisiert	Gleichheitszeichen	Gleichheitszeichen	Es gibt nur zwei Automatisierungsstatus

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
ChangeTypeld	Jede gültige Änderungstyp-ID, z. B. ct-123h45t6uz7jl	Gleichheitszeichen	Gleichheitszeichen	Suchen Sie nach einem Änderungstyp oder CSIO
ChangeTypeVersion	Jede gültige Änderungstyp-ID, zum Beispiel 1.0	Gleichheitszeichen	Gleichheitszeichen	Einen Änderungstyp oder CSIO finden
CreatedBy	Beliebige Zeichenfolge (die maximal zulässige Länge beträgt 2048 Zeichen)	Enthält	Enthält	Das CreatedBy Feld des RFC enthält den ARN des Benutzers, der ihn erstellt hat
CreatedTime	Jede Zeichenfolge, die eine ISO86 01 Datetime darstellt (zum Beispiel „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
LastModifiedTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
LastSubmittedTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
RequestedEndTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
RequestedStartTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
RfcStatusId	Abgebrochen, Bearbeitung, Fehlgeschlagen,, InProgress PendingApproval, Abgelehnt, Geplant, Erfolgreich	Gleichheitszeichen	Gleichheitszeichen	Aktualisieren Sie die RFC-Liste in der AMS-Konsole oder führen Sie den Befehl aus GetRfc

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
Titel	Jeder gültige RFC-Titel	Enthält	Enthält	Reguläre Ausdrücke in jedem einzelnen Feld werden nicht unterstützt. Suche ohne Berücksichtigung von Groß- und Kleinschreibung

Beispiele:

Um alle Informationen IDs zu finden, die sich auf SQS RFCs beziehen (wobei SQS im Artikelbereich des CT enthalten ist), können Sie diesen Befehl verwenden:

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Was ungefähr das Folgende zurückgibt:

```
-----
|                               ListRfcSummaries                               |
+-----+-----+-----+-----+-----+-----+
|Deployment| Advanced Stack Components      |SQS   |Create |ct-123h45t6uz7j1|
|Management| Monitoring & Notification    |SQS   |Update |ct-123h45t6uz7j1|
+-----+-----+-----+-----+-----+-----+

```

Ein weiterer verfügbarer Filter `list-rfc-summaries` ist `AutomationStatusId`, um nach RFCs automatisierten oder manuellen Filtern zu suchen:

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Ein weiterer verfügbarer Filter für `list-rfc-summaries` ist `Title` (Betreff in der Konsole):

```
Attribute=Title,Value=RFC-TITLE
```

Beispiel für die neue Anforderungsstruktur in JSON, die Folgendes zurückgibt RFCs :

- (Der Titel ENTHÄLT den Ausdruck „Windows 2012“ ODER „Amazon Linux“) UND
- (RfcStatusId ENTSPRICHT „Erfolg“ ODER „InProgress“) UND
- (20170101T000000Z <= <= 20170103T000000Z) UND (<= RequestedStartTime 20170103T000000Z) ActualEndTime

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

Note

Mit der Weiterentwicklung beabsichtigt AMS, `Filters` die folgenden Felder in einer kommenden Version nicht mehr zu unterstützen:

- Wert: Das Feld Wert ist Teil des Felds Filter. Verwenden Sie das Wertefeld, das erweiterte Funktionen unterstützt.

- **RequestedEndTimeRange:** Verwenden Sie das Feld `RequestedEndTime` innerhalb des Filters, das erweiterte Funktionen unterstützt
- **RequestedStartTimeRange:** Verwenden Sie das Feld `RequestedStartTime` innerhalb des Filters, das erweiterte Funktionen unterstützt.

Informationen zur Verwendung von CLI-Abfragen finden Sie unter [So filtern Sie die Ausgabe mit der Option --query](#) und in der Referenz zur Abfragesprache, [JMESPath Spezifikation](#).

2. Wenn Sie die AMS-Konsole verwenden:

Gehen Sie zur `RFCsListenseite`. Bei Bedarf können Sie nach dem RFC-Betreff filtern, den Sie `Title` bei der Erstellung als RFC eingegeben haben.

Tipps

Note

Dieses Verfahren gilt nur für geplante RFCs Benutzer, die die RFCs ASAP-Option nicht verwendet haben.

Stornieren RFCs

Sie können einen RFC mit der Konsole oder der AMS API/CLI stornieren.

Um einen RFC mit der Konsole zu stornieren, suchen Sie den RFC in Ihrer RFC-Liste, öffnen Sie ihn und klicken Sie auf Abbrechen.

Erforderliche Daten:

- **Reason:** Warum kündigen Sie den RFC.
- **RfcId:** Der RFC, den Sie stornieren.

1. Normalerweise würden Sie einen RFC direkt nach dem Absenden stornieren (daher sollte die RFC-ID griffbereit sein). Andernfalls können Sie ihn nur stornieren, wenn Sie ihn geplant haben und er vor der angegebenen Startzeit liegt. Wenn Sie die RFC-ID suchen müssen, können Sie

diesen Befehl verwenden (Sie können den durch einen manuell Value PendingApproval genehmigten RFC ersetzen):

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. Beispielbefehl zum Stornieren eines RFC:

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --  
region us-east-1
```

Verwenden Sie die AMS-Konsole mit RFCs

Die AMS-Konsole bietet Funktionen, die Ihnen beim erfolgreichen Erstellen und Einreichen helfen RFCs.

Verwenden Sie die RFC-Listenseite (Konsole)

Die RFCsListenseite der AMS-Konsole bietet Ihnen die folgenden Optionen:

- Erweiterte RFC-Suche mithilfe eines Filters. Weitere Informationen finden Sie unter [Finden RFCs](#).
- Finden Sie heraus, wann der RFC das letzte Mal geändert wurde. Dieser Wert steht für das letzte Mal, als der RFC-Status geändert wurde.
- RFC-Details mit dem RFC-Betreff anzeigen. Wenn Sie diesen Link wählen, wird die Detailseite für diesen RFC geöffnet.
- RFC-Status anzeigen. Weitere Informationen finden Sie unter [RFC-Statuscodes verstehen](#)

Verwenden Sie RFC Quick Create (Konsole)

Verwenden Sie die RFC-Schnellerstellungskarten oder die Listentabelle oder wählen Sie die Änderungstypen RFCs nach Klassifizierung aus.

Weitere Informationen hierzu finden Sie unter [Erstellen Sie einen RFC](#).

Fügen Sie RFC-Korrespondenz und Anlagen hinzu (Konsole)

Sie können einem RFC Korrespondenz hinzufügen, nachdem er eingereicht wurde und bevor er genehmigt wurde, z. B. solange er sich im Status "" PendingApproval befindet. Nachdem

ein RFC genehmigt wurde (im Status „Geplant“ oder „InProgress“), kann keine Korrespondenz hinzugefügt werden, da dies als Änderung der Anfrage interpretiert werden könnte. Nachdem ein RFC abgeschlossen ist (im Status „Storniert“, „Abgelehnt“, „Erfolgreich“ oder „Fehlgeschlagen“), wird die Korrespondenz wieder aktiviert, obwohl die Korrespondenz deaktiviert wird, sobald ein RFC für mehr als 30 Tage geschlossen ist.

 Note

Jede Korrespondenz ist auf 5.000 Zeichen begrenzt.

Einschränkungen für Anlagen:

- Nur drei Anlagen pro Korrespondenz.
- Beschränken Sie sich auf fünfzig Anhänge pro RFC.
- Jeder Anhang muss weniger als 5 MB groß sein.
- Es werden nur Textdateien wie Klartext (.txt), kommagetrennte Werte (.csv), JSON () oder YAML (.json) akzeptiert. .yaml Im Fall des YAML-Formats muss die Datei mit der Dateierweiterung angehängt werden. .yaml

 Note

Textdateien mit XML-Inhalt sind verboten. Wenn Sie XML-Inhalte mit AMS teilen möchten, verwenden Sie eine Serviceanfrage.

- Dateinamen sind auf 255 Zeichen begrenzt und enthalten nur Zahlen, Buchstaben, Leerzeichen, Bindestriche (-), Unterstriche (_) und Punkte (.).
- Das Aktualisieren und Löschen von Anhängen in einem RFC wird derzeit nicht unterstützt.

Gehen Sie folgendermaßen vor, um einem RFC Korrespondenz und Anlagen hinzuzufügen:

1. Suchen Sie in der AMS-Konsole auf der RFC-Detailseite für einen RFC unten auf der Seite nach dem Abschnitt Korrespondenz.

Vor jeder Korrespondenz:

Nach einiger Korrespondenz:

2. Um eine neue Korrespondenz hinzuzufügen, geben Sie Ihre Nachricht in das Textfeld Antwort ein. Um Dateien anzuhängen, die sich auf die Korrespondenz beziehen, wählen Sie Anlage hinzufügen und wählen Sie dann die gewünschten Dateien aus.
3. Wenn Sie fertig sind, wählen Sie Senden.

Die neue Korrespondenz wird zusammen mit den Links zu den angehängten Dateien in der Korrespondenzliste auf der RFC-Detailseite angezeigt.

RFC-E-Mail-Benachrichtigungen konfigurieren (Konsole)

Auf der Seite zum Erstellen von Änderungsanträgen in der AMS-Konsole haben Sie die Möglichkeit, E-Mail-Adressen hinzuzufügen, um Benachrichtigungen über RFC-Statusänderungen zu erhalten:

Darüber hinaus können Sie E-Mail-Adressen für Benachrichtigungen zu beliebigen Änderungstypen hinzufügen, zum Beispiel:

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
[\"email@example.com\"]}}"
```

Fügen Sie jeder Inline- oder Template-Anfrage vom Typ Change eine ähnliche Zeile (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) im RFC-Parameter-Teil der Anfrage hinzu, nicht im Parameter-Teil.

Erfahren Sie mehr über gängige RFC-Parameter

Im Folgenden sind die RFC-Parameter aufgeführt, die Sie einreichen müssen, sowie die Parameter, die häufig in folgenden Bereichen verwendet werden: RFCs

- Typinformationen ändern: `ChangeTypeld` und `ChangeTypeVersion`. Eine Liste der Änderungstypen IDs und Versionsnummern finden Sie unter [Referenz zum Änderungstyp](#).

Führen Sie `list-change-type-classification-summaries` in der CLI mit dem `query` Argument aus, um die Ergebnisse einzugrenzen. Grenzen Sie beispielsweise die Ergebnisse ein, um Typen zu ändern, die „Access“ im Item Namen enthalten.

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Führen Sie den `get-change-type-version` Befehl aus und geben Sie die ID des Änderungstyps an. Der folgende Befehl ruft die CT-Version für `ct-2tylseo8rxfsc` ab.

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- Titel: Ein Name für den RFC; dieser wird zum Betreff des RFC in der RFC-Liste der AMS-Konsole, und Sie können danach suchen, indem Sie den Befehl und einen Filter auf `GetRfc Title`
- Planung: Wenn Sie einen geplanten RFC wünschen, müssen Sie die `RequestedEndTime` Parameter `RequestedStartTime` und angeben oder die Konsolenoption „Diese Änderung planen“ verwenden. Bei einem ASAP-RFC (der ausgeführt wird, sobald er genehmigt wurde), wenn Sie die CLI verwenden, lassen Sie den Wert leer `RequestedStartTime` und `RequestedEndTime` null. Wenn Sie die Konsole verwenden, akzeptieren Sie die ASAP-Option.

Wenn das `RequestedStartTime` fehlt, wird der RFC zurückgewiesen.

- Bereitstellung CTs: Die Ausführungsparameter oder `Parameters` die spezifischen Einstellungen, die für die Bereitstellung der Ressource erforderlich sind. Sie sind je nach CT sehr unterschiedlich.
- Nichtbereitstellung CTs: Ressourcen CTs , die keine Ressource bereitstellen, z. B. Zugriff CTs oder Andere | Andere, oder Stapel löschen, haben nur minimale Ausführungsparameter und keinen `Parameters` Block.
- Manche verlangen RFCs auch, dass Sie `angebenTimeoutInMinutes`, wie viele Minuten für die Erstellung des Stacks vorgesehen sind, bevor der RFC fehlschlägt. Gültige Werte liegen zwischen 60 (Minuten) und 360 (bei langer `UserData` Laufzeit). Wenn die Ausführung nicht abgeschlossen werden kann, bevor der Wert überschritten `TimeoutInMinutes` wird, schlägt der RFC fehl. Diese Einstellung verzögert jedoch nicht die Ausführung des RFC.
- RFCs die Instanzen erstellen, wie z. B. einen S3-Bucket oder einen ELB, stellen im Allgemeinen ein Schema bereit, mit dem Sie bis zu sieben Tags (Schlüssel/Wert-Paare) hinzufügen können. Sie können Ihrem S3-Bucket weitere Tags hinzufügen, indem Sie über `Deployment | Advanced stack components | Tag | Create change type (ct-3cx7we852p3af)` einen RFC einreichen. EC2,

EFS, RDS und die mehrstufigen Schemas (HA Two-Tiered und HA One-Tiered) ermöglichen bis zu fünfzig Tags. Tags werden im Teil des Schemas angegeben. `ExecutionParameters` Die Bereitstellung von Tags kann von großem Wert sein. Weitere Informationen finden Sie unter [Tagging Your Amazon EC2 Resources](#).

Wenn Sie die AMS-Konsole verwenden, müssen Sie den Bereich Zusätzliche Konfiguration öffnen, um Tags hinzuzufügen.

 Tip

Viele CT-Schemas haben ein `Description Name` UND-Feld am oberen Rand des Schemas. Diese Felder werden verwendet, um den Stack oder die Stack-Komponente zu benennen, sie benennen nicht die Ressource, die Sie erstellen. Einige Schemas bieten einen Parameter zum Benennen der Ressource, die Sie erstellen, andere nicht. Das CT-Schema für `Create EC2 Stack` bietet beispielsweise keinen Parameter zum Benennen der EC2 Instanz. Dazu müssen Sie ein Tag mit dem Schlüssel „Name“ und dem Wert, den der Name haben soll, erstellen. Wenn Sie kein solches Tag erstellen, wird Ihre EC2 Instanz in der EC2 Konsole ohne ein Namensattribut angezeigt.

Verwenden Sie die Option `AWS RFC-Region`

Die AMS-API und die CLI-Endpunkte (`amscmundamsskms`) sind da. `us-east-1` Wenn Sie sich mit Security Assertion Markup Language (SAML) verbünden, werden Ihnen beim Onboarding Skripte zur Verfügung gestellt, die Ihre Region auf `us-east-1` setzen. AWS Wenn Sie SAML verwenden, müssen Sie die Option nicht angeben, wenn Sie einen Befehl ausgeben. `--region` Wenn Ihre SAML für die Verwendung von `us-east-1` konfiguriert ist, sich Ihr Konto jedoch nicht in dieser AWS Region befindet, müssen Sie Ihre kontointegrierte Region angeben, wenn Sie andere AWS Befehle ausführen (z. B.).
`aws s3`

 Note

Die meisten Befehlsbeispiele in diesem Handbuch enthalten diese Option nicht. `--region`

Melden Sie sich für die tägliche RFC-E-Mail an

Mit der RFC-Digest-Funktion können Sie sich für eine tägliche E-Mail anmelden, in der die RFC-Aktivitäten in Ihrem Konto in den letzten 24 Stunden zusammengefasst werden. Die RFC-Digest-Funktion ist ein optimierter Prozess, der die Anzahl der E-Mail-Benachrichtigungen reduziert, die Sie zu Ihrem Konto erhalten. RFCs Der RFC-Digest kann die Wahrscheinlichkeit verringern, dass Sie Aktionen verpassen, für die Ihre Antwort noch aussteht.

Um die RFC-Digest-Funktion zu aktivieren, wenden Sie sich an Ihren AMS Cloud Service Delivery Manager (CSDM). Der CSDM abonniert Sie. Sie können bis zu 20 E-Mail-Adressen (oder Aliase) anfordern, die in Ihre RFC-Digest-E-Mail-Liste aufgenommen werden sollen. Der aktuelle E-Mail-Zeitplan ist auf 09:00 Uhr UTC-8 festgelegt.

Um die RFC-Digest-Funktion zu deaktivieren, wenden Sie sich mit Ihrer Anfrage an Ihren CSDM.

Wenn Sie den RFC-Digest nicht einrichten und Benachrichtigungen zu Ihrem wünschen RFCs, oder wenn Sie detailliertere Informationen zu Ihrem wünschen, RFCs als der RFC-Digest bietet, verwenden Sie das Change Management System, um CloudWatch Ereignisbenachrichtigungen oder E-Mail-Benachrichtigungen für jeden einzelnen RFC einzurichten, zu dem Sie Informationen wünschen. [Informationen zum Einrichten von RFC-Benachrichtigungen finden Sie unter Benachrichtigungen über RFC-Statusänderungen.](#)

Der RFC-Digest enthält unter anderem folgende Themen:

- Ausstehende Genehmigung durch den Kunden: Listen RFCs , die sich im PendingApprovalStatus befinden und auf Ihre Genehmigung warten
- Ausstehende Kundenantwort: Listen RFCs , die auf Ihre Antwort zur RFC-Korrespondenz warten
- Ausstehende AWS-Genehmigung oder -Antwort: Listen RFCs , die bei AMS auf eine Antwort oder Genehmigung warten
- Abgeschlossen: Listen mit Status „ RFCs Erfolgreich“, „Fehlgeschlagen“, „Storniert“ und „Abgelehnt“

Im Folgenden finden Sie ein Beispiel für einen RFC-Digest:

Was sind Änderungstypen?

Der Änderungstyp bezieht sich auf die Aktion, die eine Änderungsanforderung (RFC) von AWS Managed Services (AMS) ausführt, und umfasst die Änderungsaktion selbst sowie die

Art der Änderung — manuell oder automatisiert. AMS verfügt über eine große Sammlung von Änderungstypen, die von anderen Amazon-Webservices nicht verwendet werden. Sie verwenden diese Änderungstypen, wenn Sie einen Änderungsantrag (RFC) einreichen, um Ressourcen bereitzustellen oder zu verwalten oder Zugriff darauf zu erhalten.

Themen

- [Automatisiert und manuell CTs](#)
- [Anforderungen an die CT-Zulassung](#)
- [Typversionen ändern](#)
- [Änderungstypen erstellen](#)
- [Änderungstypen aktualisieren](#)
- [Nur interne Änderungstypen](#)
- [Typschemas ändern](#)
- [Verwaltung von Berechtigungen für Änderungstypen](#)
- [Sensible Informationen aus Änderungstypen redigieren](#)
- [Finden eines Änderungstyps mithilfe der Abfrageoption](#)

Automatisiert und manuell CTs

Eine Einschränkung für Änderungstypen besteht darin, ob sie automatisiert oder manuell sind. Dies ist das `AutomationStatusId` Änderungstypattribut, das in der AMS-Konsole als Ausführungsmodus bezeichnet wird.

Automatisierte Änderungstypen haben erwartete Ergebnisse und Ausführungszeiten und durchlaufen das automatisierte AMS-System, in der Regel innerhalb einer Stunde oder weniger (dies hängt weitgehend davon ab, welche Ressourcen der CT bereitstellt). Manuelle Änderungstypen sind ungewöhnlich, werden aber unterschiedlich behandelt, da sie erfordern, dass ein AMS-Operator auf den RFC reagiert, bevor er ausgeführt werden kann. Das bedeutet manchmal, dass Sie mit dem RFC-Absender kommunizieren müssen, sodass manuelle Änderungstypen unterschiedlich lange dauern, bis sie abgeschlossen sind.

Für alle geplanten Änderungen RFCs wird eine nicht spezifizierte Endzeit als Uhrzeit des angegebenen Änderungstyps `RequestedStartTime` plus das `ExpectedExecutionDurationInMinutes` Attribut des übermittelten Änderungstyps angegeben. Wenn der beispielsweise „60“ (Minuten) `ExpectedExecutionDurationInMinutes` ist und der angegebene Wert `2016-12-05T14:20:00Z` (5. Dezember 2016 um 4:20 Uhr)

RequestedStartTime ist, würde die tatsächliche Endzeit auf den 5. Dezember 2016 um 5:20 Uhr festgelegt. Um den ExpectedExecutionDurationInMinutes für einen bestimmten Änderungstyp zu finden, führen Sie diesen Befehl aus:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Note

Geplant RFCs mit Ausführungsmodus = Manuell muss in der Konsole so eingestellt sein, dass sie mindestens 24 Stunden in der future ausgeführt wird. Dieser Vorbehalt gilt nicht für die AMS-API/CLI, aber es ist dennoch wichtig, die manuelle Planung RFCs mindestens 8 Stunden im Voraus vorzunehmen.

Note

Wenn Sie „Überprüfung erforderlich“ verwenden CTs, empfiehlt AMS, die ASAP-Scheduling-Option zu verwenden (wählen Sie ASAP in der Konsole, lassen Sie Start- und Endzeit leer in der API/CLI), da diese einen AMS-Operator CTs erfordern, der den RFC überprüft und möglicherweise mit Ihnen kommuniziert, bevor er genehmigt und ausgeführt werden kann. Wenn Sie diese einplanen, achten Sie darauf RFCs, dass Sie mindestens 24 Stunden einplanen. Wenn die Genehmigung nicht vor der geplanten Startzeit erfolgt, wird der RFC automatisch abgelehnt.

AMS ist bestrebt, auf ein manuelles CT innerhalb von vier Stunden zu antworten und wird sich so schnell wie möglich mit Ihnen in Verbindung setzen. Es könnte jedoch viel länger dauern, bis der RFC tatsächlich ausgeführt wird.

Eine Liste der Dateien CTs , die manuell sind und eine Überprüfung durch AMS erfordern, finden Sie in der CSV-Datei „Change Type“, die auf der Seite „Entwicklerressourcen“ der Konsole verfügbar ist.

YouTube Video: [Wie finde ich automatisierte Änderungstypen für AMS RFCs?](#)

Um den Ausführungsmodus für einen CT in der AMS-Konsole zu finden, müssen Sie die Suchoption Änderungstypen durchsuchen verwenden. Die Ergebnisse zeigen den Ausführungsmodus des entsprechenden Änderungstyps oder der entsprechenden Änderungstypen.

Führen Sie diesen Befehl aus, um die AutomationStatus für einen bestimmten Änderungstyp mithilfe der AMS-CLI zu finden:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Sie können die Änderungstypen auch in der [AMS Change Type Reference nachschlagen](#), die Informationen zu allen AMS-Änderungstypen enthält.

Note

Die AMS API/CLI sind derzeit nicht Teil von AWSAPI/CLI. To access the AMS API/CLI. Sie laden das AMS-SDK über die AMS-Konsole herunter.

Anforderungen an die CT-Zulassung

Für AMS gelten CTs immer zwei Genehmigungsbedingungen, AwsApprovalIdCustomerApprovalId angeben, ob der RFC von AMS oder von Ihnen oder einer anderen Person verlangt, die Ausführung zu genehmigen.

Die Genehmigungsbedingung hängt in gewisser Weise mit dem Ausführungsmodus zusammen. Einzelheiten finden Sie unter [Automatisiert und manuell CTs](#).

Um die Genehmigungsbedingung für ein CT herauszufinden, können Sie in der [AMS Change Type Reference](#) nachschauen oder den Befehl ausführen [GetChangeTypeVersion](#). In beiden Fällen erhalten Sie auch den CT AutomationStatusId - oder Ausführungsmodus.

Sie können die RFCs Genehmigung über die AMS-Konsole oder mit dem folgenden Befehl genehmigen:

```
aws amscm approve-rfc --rfc-id RFC_ID
```

Bedingung für die CT-Zulassung

Wenn die Bedingung für die CT-Zulassung	Es bedarf der Genehmigung von	And
<code>AwsApprovalId: Required</code>	Das AMS-System vom Typ Change,	Es ist keine Aktion erforderlich. Dieser Zustand ist typisch für automatisierte Systeme CTs.
<code>AwsApprovalId: NotRequiredIfSubmitter</code>	Das AMS-System ändert den Typ und sonst niemand, wenn der eingereichte RFC für das Konto gilt, für das er eingereicht wurde,	Es ist keine Aktion erforderlich. Dieser Zustand ist typisch für manuelle Geräte CTs , da sie stets von den AMS-Mitarbeitern überprüft werden.
<code>CustomerApprovalId: NotRequired</code>	Das AMS-System zur Änderung des Typs,	Wenn der RFC Syntax- und Parameterprüfungen besteht, wird er automatisch genehmigt.
<code>CustomerApprovalId: Required</code>	Das AMS-Change-Typsystem und Sie	Sie erhalten eine Benachrichtigung, und Sie müssen den RFC ausdrücklich genehmigen, indem Sie entweder auf die Benachrichtigung antworten oder den ApproveRfc Vorgang ausführen.
<code>CustomerApprovalId: NotRequiredIfSubmitter</code>	Das AMS-System ändert den Typ und sonst niemand, wenn Sie den RFC eingereicht haben.	Wenn der RFC Syntax- und Parameterprüfungen besteht, wird er automatisch genehmigt.

Wenn die Bedingung für die CT-Zulassung	Es bedarf der Genehmigung von	And
Dringender Sicherheitsvorfall oder Patch	AMS	Wird auto genehmigt und implementiert.

Typversionen ändern

Die Änderungstypen werden versioniert und die Version ändert sich, wenn eine größere Aktualisierung des Änderungstyps vorgenommen wird.

Nachdem Sie in der AMS-Konsole einen Änderungstyp ausgewählt haben, haben Sie die Möglichkeit, den Bereich Zusätzliche Konfiguration zu öffnen und eine Version des Änderungstyps auszuwählen. Sie können auch in der API/CLI Befehlszeile eine Version vom Typ „Change Type“ angeben. Möglicherweise möchten Sie dies aus verschiedenen Gründen tun, darunter:

- Sie wissen, dass die Version des Änderungstyps Update, die Sie möchten, mit der Version des Änderungstyps Erstellen übereinstimmen muss, mit der Sie die Ressource erstellt haben, die Sie jetzt aktualisieren möchten. Angenommen, Sie haben eine Elastic Load Balancer (ELB) -Instance, die Sie mit ELB Create Change Type Version 1 erstellt haben. Um sie zu aktualisieren, wählen Sie ELB Update Version 1.
- Sie möchten eine Version des Änderungstyps verwenden, die andere Optionen enthält als der letzte Änderungstyp. Wir empfehlen dies nicht, da AMS-Updates ihre Typen hauptsächlich aus Sicherheitsgründen ändern und wir empfehlen, dass Sie immer die neueste Version wählen.

Änderungstypen erstellen

Die Änderungstypen von Create werden version-to-version den Änderungstypen vom Typ Update zugeordnet. Das heißt, die Version des Änderungstyps, die Sie für die Bereitstellung einer Ressource verwenden, muss mit der Version des Änderungstyps Update übereinstimmen, den Sie später zum Ändern dieser Ressource verwenden würden. Wenn Sie beispielsweise einen S3-Bucket mit dem Änderungstyp Create S3 Bucket, Version 2.0, erstellen und später einen RFC zur Änderung dieses S3-Buckets einreichen möchten, müssen Sie auch den Änderungstyp Update S3-Bucket, Version 2.0, verwenden, auch wenn es einen Änderungstyp Update S3-Bucket mit Version 3.0 gibt.

Wir empfehlen, die Änderungstyp-ID und die Version aufzuzeichnen, die Sie verwenden, wenn Sie eine Ressource mit dem Änderungstyp Create bereitstellen, falls Sie später den Änderungstyp Update verwenden möchten, um sie zu ändern.

Änderungstypen aktualisieren

AMS bietet Änderungstypen aktualisieren, um Ressourcen zu aktualisieren, die mit Create Change Types erstellt wurden. Die Änderungstypen aktualisieren müssen version-to-version mit dem Änderungstyp Create übereinstimmen, der ursprünglich für die Bereitstellung der Ressource verwendet wurde.

Es wird empfohlen, die ID und Version des Änderungstyps, die Sie bei der Bereitstellung einer Ressource verwenden, aufzuzeichnen, um deren Aktualisierung zu vereinfachen.

YouTube Video: [Wie verwende ich Update CTs , um Ressourcen in einem AWS Managed Services \(AMS\) -Konto zu ändern?](#)

Nur interne Änderungstypen

Sie können Änderungstypen sehen, die nur für den internen Gebrauch bestimmt sind. Auf diese Weise wissen Sie, welche Maßnahmen AMS ergreifen kann oder tut. Wenn es einen ausschließlich internen Änderungstyp gibt, den Sie für Ihre Nutzung zur Verfügung haben möchten, reichen Sie eine Serviceanfrage ein.

Beispielsweise gibt es ein CT-System für Verwaltung | Überwachung und Benachrichtigung | CloudWatch Alarmunterdrückung | Update, das nur intern ist. AMS verwendet es, um Infrastruktur-Updates (wie Patches) bereitzustellen, um Alarmbenachrichtigungen zu deaktivieren, die durch die Updates fälschlicherweise ausgelöst werden könnten. Wenn dieses CT eingereicht wird, werden Sie den RFC für das CT in Ihrer RFC-Liste finden. Alle rein internen CTs, die in einem RFC bereitgestellt werden, werden in Ihrer RFC-Liste angezeigt.

Typschemas ändern

Alle Änderungstypen stellen ein JSON-Schema für Ihre Eingaben bei der Erstellung, Änderung oder dem Zugriff auf Ressourcen bereit. Das Schema stellt die Parameter und ihre Beschreibungen bereit, mit denen Sie einen Änderungsantrag (RFC) erstellen können.

Die erfolgreiche Ausführung eines RFC führt zu einer Ausführungsausgabe. Für die Bereitstellung RFCs enthält die Ausführungsausgabe eine „stack_id“, die den Stack darstellt CloudFormation und in der Konsole gesucht werden kann. CloudFormation Die Ausführungsausgabe beinhaltet manchmal die Ausgabe der ID der erstellten Instance, und diese ID kann verwendet werden, um in

der entsprechenden AWS-Konsole nach der Instance zu suchen. Die Ausführungsausgabe „Create ELB CT“ enthält beispielsweise eine „stack_id“, in der gesucht werden kann, CloudFormation und gibt einen Key=ELB-Wert= aus, der in der Amazon-Konsole für Elastic Load <stack-xxxx>Balancing durchsucht werden kann. EC2

Lassen Sie uns ein CT-Schema untersuchen. Dies ist das Schema für CodeDeploy Application Create, ein ziemlich kleines Schema. Einige Schemas haben sehr große Parameter Bereiche.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv000000000000",
      "type": "string",
      "enum": ["stm-sft6rv000000000000"]
    },
    "Name": {
      "description": "A name for the stack or stack component
;
this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
```

Der erste Teil des Schemas liefert AMS Informationen über den angeforderten Änderungstyp.

```

    "description": "Up to seven tags (key/value pairs) to
    categorize the resource.",
    "type": "array",
    "items": {
      "type": "object",
      "properties": {
        "Key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 127
        },
        "Value": {
          "type": "string",
          "minLength": 1,
          "maxLength": 255
        }
      },
      "additionalProperties": false,
      "required": [
        "Key",
        "Value"
      ]
    },
    "minItems": 1,
    "maxItems": 7
  },
  "TimeoutInMinutes": {
    "description": "The maximum amount of time, in minutes,
    to
    allow for execution of the change. This will not prolong
    execution,
    but the RFC fails if the change is not completed in the
    specified time.
    Valid values are 60 up to 360, for long-running
    UserData.",
    "type": "number",
    "minimum": 0,
    "maximum": 60
  },
  "Parameters": {
    "description": "Specifications for the stack.",
    "type": "object",
    "properties": {
      "CodeDeployApplicationName": {

```

Mit dem TimeoutInMinutes Parameter können Sie eine Grenzzzeit für die Ausführung des Änderungstyps angeben. Gültige Werte liegen zwischen 60 und 360 für eine lange Laufzeit UserData.

Im Abschnitt Parameter geben Sie Einstellungen für die Ressource an, die Sie erstellen, oder für die Aktion, die Sie anfordern.

In den Abschnitt en „Zusätzliche

```
        "description": "The name of an AWS CodeDeploy
application.",
        "type": "string",
        "minLength": 1,
        "maxLength": 100,
        "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
    },
    "additionalProperties": false,
    "required": [
        "CodeDeployApplicationName"
    ]
},
"additionalProperties": false,
"required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
]
}
```

Eigenschaften“
erfahren Sie, welche
Parameter erforderlich
und welche optional
sind.

Note

Dieses Schema erlaubt bis zu sieben Tags; EFS EC2, RDS und die mehrstufigen Erstellungsschemas erlauben jedoch bis zu 50 Tags.

Verwaltung von Berechtigungen für Änderungstypen

Sie können eine benutzerdefinierte Richtlinie verwenden, um einzuschränken, welche Änderungstypen (CTs) für verschiedene Gruppen oder Benutzer verfügbar sind.

Weitere Informationen dazu finden Sie im AMS-Benutzerhandbuch im Abschnitt [Berechtigungen einrichten](#).

Sensible Informationen aus Änderungstypen redigieren

AMS-Schemas für den Änderungstyp bieten ein Parameterattribut, "metadata": "ams:sensitive": "true" das für Parameter verwendet wird, die vertrauliche Informationen enthalten würden, z. B. ein Passwort. Wenn dieses Attribut gesetzt ist, ist die bereitgestellte Eingabe verdeckt. Beachten Sie, dass Sie dieses Parameterattribut nicht festlegen können. Wenn Sie jedoch mit AMS arbeiten, um einen Änderungstyp zu erstellen und einen Parameter haben, den Sie bei der Eingabe verdecken möchten, können Sie dies anfordern.

Finden eines Änderungstyps mithilfe der Abfrageoption

Dieses Beispiel zeigt, wie Sie mithilfe der AMS-Konsole den geeigneten Änderungstyp für den RFC finden, den Sie einreichen möchten.

Sie können die Konsole oder die verwenden API/CLI , um nach einer Änderungstyp-ID (CT) oder Version zu suchen. Es gibt zwei Methoden: entweder eine Suche oder die Auswahl der Klassifizierung. Für beide Auswahltypen können Sie die Suche sortieren, indem Sie entweder „Am häufigsten verwendet“, „Zuletzt verwendet“ oder „Alphabetisch“ auswählen.

YouTube Video: [Wie erstelle ich einen RFC mit der AWS Managed Services CLI und wo finde ich das CT-Schema?](#)

Gehen Sie in der AMS-Konsole auf der Seite RFCs-> RFC erstellen wie folgt vor:

- Wenn „Nach Änderungstyp suchen“ ausgewählt ist (Standardeinstellung), können Sie entweder:
 - Verwenden Sie den Bereich Schnellerstellung, um aus den beliebtesten AMS-Programmen auszuwählen CTs. Klicken Sie auf ein Label und die Seite RFC ausführen wird geöffnet, auf der die Option Betreff automatisch für Sie ausgefüllt wird. Füllen Sie die verbleibenden Optionen nach Bedarf aus und klicken Sie auf Ausführen, um den RFC einzureichen.
 - Oder scrollen Sie nach unten zum Bereich Alle Änderungstypen und beginnen Sie, einen CT-Namen in das Optionsfeld einzugeben. Sie müssen nicht den genauen oder vollständigen Namen des Änderungstyps haben. Sie können auch anhand der ID des Änderungstyps, der Klassifizierung oder des Ausführungsmodus (automatisiert oder manuell) nach einem CT suchen, indem Sie die entsprechenden Wörter eingeben.

Wenn die standardmäßige Kartenansicht ausgewählt ist, werden während der Eingabe passende CT-Karten angezeigt. Wählen Sie eine Karte aus und klicken Sie auf RFC erstellen. Wählen Sie bei ausgewählter Tabellenansicht das entsprechende CT aus und klicken Sie auf RFC erstellen. Bei beiden Methoden wird die Seite RFC ausführen geöffnet.

- Klicken Sie alternativ oben auf der Seite auf Nach Kategorie auswählen, um eine Reihe von Drop-down-Optionsfeldern zu öffnen, um eine Reihe von Auswahlmöglichkeiten für den Änderungstyp zu öffnen.
- Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Das Informationsfeld für diesen Änderungstyp wird angezeigt. Unten auf der Seite wird ein Bereich angezeigt.
- Wenn Sie bereit sind, drücken Sie die EINGABETASTE. Daraufhin wird eine Liste der passenden Änderungstypen angezeigt.
- Wählen Sie einen Änderungstyp aus der Liste aus. Das Informationsfeld für diesen Änderungstyp wird unten auf der Seite angezeigt.
- Wenn Sie den richtigen Änderungstyp gefunden haben, wählen Sie Create RFC.

Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` z. B. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

Note

Die AMS-Endpunkte API/CLI (`amscm` und `amsskms`) befinden sich in der AWS-Region Nord-Virginia, `us-east-1`. Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

So suchen Sie mit der AMS CM API (siehe [ListChangeTypeClassificationSummaries](#)) oder CLI nach einem Änderungstyp:

Sie können einen Filter oder eine Abfrage für die Suche verwenden. Der `ListChangeTypeClassificationSummaries` Vorgang verfügt über [Filteroptionen](#) für `CategorySubcategory`, `Item`, und `Operation`, aber die Werte müssen exakt mit den vorhandenen Werten übereinstimmen. Für flexiblere Ergebnisse bei der Verwendung der CLI können Sie die `--query` Option verwenden.

Ändern Sie die Typfilterung mit der AMS CM API/CLI

Attribut	Zulässige Werte	Gültige/Standardbe- dingung	Hinweise
ChangeTypeld	Jede Zeichenfolge, die a darstellt ChangeTypeld (Zum Beispiel: ct-abc123 xyz7890)	Gleichheitszeichen	Informationen zum Änderungstyp finden Sie in der Referenz zum Änderungstyp. IDs Informationen zum Änderungstyp IDs finden Sie unter Suche nach einem Änderungstyp oder CSIO.
Kategorie	Beliebiger Text in freier Form	Enthält	Reguläre Ausdrücke in jedem einzelnen Feld werden nicht unterstützt. Suche ohne Berücksic- htigung von Groß- und Kleinschreibung
Unterkategorie			
Item			
Operation			

1. Hier sind einige Beispiele für Klassifizierungen nach der Art der Angebotsänderung:

Der folgende Befehl listet alle Kategorien von Änderungstypen auf.

```
aws amscm list-change-type-categories
```

Der folgende Befehl listet die Unterkategorien auf, die zu einer bestimmten Kategorie gehören.

```
aws amscm list-change-type-subcategories --category CATEGORY
```

Der folgende Befehl listet die Elemente auf, die zu einer bestimmten Kategorie und Unterkategorie gehören.

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. Hier sind einige Beispiele für die Suche nach Änderungstypen mit CLI-Abfragen:

Der folgende Befehl durchsucht CT-Klassifikationszusammenfassungen nach solchen, die „S3“ im Elementnamen enthalten, und erstellt eine Ausgabe der Kategorie-, Unterkategorie-, Element-, Vorgangs- und Änderungstyp-ID in Tabellenform.

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-----+
|          ListChangeTypeClassificationSummaries          |
+-----+-----+-----+-----+-----+-----+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+-----+-----+-----+-----+-----+-----+-----+
```

3. Anschließend können Sie die Änderungstyp-ID verwenden, um das CT-Schema abzurufen und die Parameter zu untersuchen. Mit dem folgenden Befehl wird das Schema in eine JSON-Datei mit dem Namen CreateS3Params.schema.json ausgegeben.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
  --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
  CreateS3Params.schema.json
```

Informationen zur Verwendung von CLI-Abfragen finden Sie unter [So filtern Sie die Ausgabe mit der Option --query](#) und in der Referenz zur Abfragesprache, [JMESPath Spezifikation](#).

4. Nachdem Sie die Änderungstyp-ID erhalten haben, empfehlen wir, die Version für den Änderungstyp zu überprüfen, um sicherzustellen, dass es sich um die neueste Version handelt. Verwenden Sie diesen Befehl, um die Version für einen bestimmten Änderungstyp zu finden:

```
aws amscm list-change-type-version-summaries --filter  
Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

Um die AutomationStatus für einen bestimmten Änderungstyp zu finden, führen Sie diesen Befehl aus:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Führen Sie diesen Befehl aus, um ExpectedExecutionDurationInMinutes nach dem für einen bestimmten Änderungstyp zu suchen:

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h  
--query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Behebung von RFC-Fehlern in AMS

Viele RFC-Fehler bei der AMS-Bereitstellung können anhand der Dokumentation untersucht werden. CloudFormation Weitere Informationen finden Sie unter [AWS-Fehlerbehebung CloudFormation: Fehlerbehebung](#)

In den folgenden Abschnitten finden Sie weitere Vorschläge zur Fehlerbehebung.

RFC-Fehler im Bereich „Verwaltung“ in AMS

Mit den AMS-Kategorieänderungstypen (CTs) können Sie Zugriff auf Ressourcen beantragen und vorhandene Ressourcen verwalten. In diesem Abschnitt werden einige häufig auftretende Probleme beschrieben.

RFC-Zugriffsfehler

- Stellen Sie sicher, dass der Benutzername und der FQDN, die Sie im RFC angegeben haben, korrekt sind und in der Domäne vorhanden sind. Hilfe bei der Suche nach Ihrem FQDN finden Sie unter [Finden](#) Ihres FQDN.
- Stellen Sie sicher, dass es sich bei der Stack-ID, die Sie für den Zugriff angegeben haben, um einen verwandten Stack handelt EC2. Stacks wie ELB und Amazon Simple Storage Service (S3) sind keine RFCs Zugriffskandidaten. Verwenden Sie stattdessen Ihre Nur-Lese-Zugriffsrolle, um

auf diese Stack-Ressourcen zuzugreifen. [Hilfe bei der Suche nach einer Stack-ID finden Sie unter Stack suchen IDs](#)

- Stellen Sie sicher, dass die von Ihnen angegebene Stack-ID korrekt ist und zum entsprechenden Konto gehört.

Hilfe bei anderen RFC-Zugriffsausfällen finden Sie unter [Zugriffsverwaltung](#).

YouTube Video: [Wie stelle ich einen Request for Change \(RFC\) richtig ein, um Ablehnungen und Ausfälle zu vermeiden?](#)

RFC (manuell) CT-Planungsfehler

Die meisten Änderungstypen sind ExecutionMode =Automatisiert, aber einige sind ExecutionMode =Manuell, was sich darauf auswirkt, wie Sie sie planen sollten, um RFC-Fehler zu vermeiden.

Geplant RFCs mit ExecutionMode =Manual, muss so eingestellt sein, dass es mindestens 24 Stunden in der future ausgeführt wird, wenn Sie die AMS-Konsole verwenden, um den RFC zu erstellen. Dieser Vorbehalt gilt nicht für die AMS API/CLI, aber es ist dennoch wichtig, Manual RFCs mindestens 8 Stunden im Voraus zu planen.

AMS ist bestrebt, auf ein manuelles CT innerhalb von vier Stunden zu antworten und wird so schnell wie möglich antworten, aber es könnte viel länger dauern, bis der RFC tatsächlich ausgeführt wird.

Verwendung RFCs mit manuellem Update CTs

AMS Operations lehnt Management | Andere | Andere RFCs für Aktualisierungen von Stacks ab, wenn es für den Stacktyp, den Sie aktualisieren möchten, einen Aktualisierungstyp gibt.

RFC-Fehler beim Löschen des Stacks

RFC-Fehler beim Löschen von Stacks: Wenn Sie das CT Management | Standard Stacks | Stack | Delete verwenden, werden Ihnen in der CloudFormation Konsole die detaillierten Ereignisse für den Stack mit dem AMS-Stack-Namen angezeigt. Sie können Ihren Stack identifizieren, indem Sie ihn mit dem Namen vergleichen, den er in der AMS-Konsole hat. Die CloudFormation Konsole bietet weitere Informationen zu den Fehlerursachen.

Bevor Sie einen Stapel löschen, sollten Sie sich überlegen, wie der Stack erstellt wurde. Wenn Sie den Stack mit einem AMS-CT erstellt und die Stack-Ressourcen nicht hinzugefügt oder bearbeitet haben, können Sie davon ausgehen, dass Sie ihn problemlos löschen können. Es ist jedoch eine gute Idee, alle manuell hinzugefügten Ressourcen aus einem Stack zu entfernen, bevor Sie einen Löschstapel-RFC für diesen Stack einreichen. Wenn Sie beispielsweise einen Stack mit

dem Full-Stack-CT (HA Two Tier) erstellen, enthält er eine Sicherheitsgruppe -. SG1 Wenn Sie dann AMS verwenden, um eine weitere Sicherheitsgruppe zu erstellen - und auf die neue SG2 Sicherheitsgruppe verweisen SG2, die als Teil des vollständigen Stacks SG1 erstellt wurde, und dann den Löschstapel-CT verwenden, um den Stack zu löschen, SG1 wird nicht gelöscht, da er von referenziert wird SG2.

Important

Das Löschen von Stacks kann unerwünschte und unerwartete Folgen haben. Aus diesem Grund zieht es AMS vor, Stacks oder Stack-Ressourcen nicht im Namen von Kunden zu löschen. Beachten Sie, dass AMS in Ihrem Namen nur Ressourcen löscht (durch einen eingereichten Änderungstyp Verwaltung | Andere | Andere | Aktualisierung), die nicht mit dem entsprechenden, automatisierten Änderungstyp gelöscht werden können. Weitere Überlegungen:

- Wenn die Ressourcen für den Löschschutz aktiviert sind, kann AMS helfen, diesen zu entsperren, indem Sie den Änderungstyp Verwaltung | Andere | Andere | Aktualisierung einreichen. Nachdem der Löschschutz aufgehoben wurde, können Sie diese Ressource mit dem automatisierten CT löschen.
- Wenn ein Stack mehrere Ressourcen enthält und Sie nur eine Teilmenge der Stack-Ressourcen löschen möchten, verwenden Sie den Änderungstyp CloudFormation Update (siehe [CloudFormation Ingest Stack](#): Aktualisierung). Sie können auch den Änderungstyp Verwaltung | Andere | Andere | Aktualisierung angeben. Die AMS-Techniker können Ihnen bei Bedarf bei der Erstellung des Changesets helfen.
- Falls aufgrund von Abweichungen Probleme bei der Verwendung des CloudFormation Update CT auftreten, kann AMS helfen, indem Sie ein Management | Other | Other | Other | Update zur Behebung des Fehlers einreichen (sofern vom CloudFormation AWS-Service unterstützt) und ein Update bereitstellen ChangeSet , das Sie dann mit den automatisierten CT, Management/Custom Stack/Stack From CloudFormation Template/ Approve Changeset und Update validieren und ausführen können.

AMS hält sich an die oben genannten Einschränkungen, um sicherzustellen, dass es nicht zu unerwarteten oder unerwarteten Löschungen von Ressourcen kommt.

Weitere Informationen finden Sie unter [Fehlerbehebung bei AWS CloudFormation: Stack löschen schlägt fehl](#).

DNS-Fehler beim RFC-Update

Es kann RFCs vorkommen, dass mehrere Aktualisierungen einer DNS-Hosting-Zone fehlschlagen, manchmal auch ohne Grund. Das RFCs gleichzeitige Erstellen mehrerer Zonen zur Aktualisierung von DNS-Hosting-Zonen (privat oder öffentlich) kann dazu führen RFCs, dass einige fehlschlagen, weil sie versuchen, denselben Stack gleichzeitig zu aktualisieren. AMS Change Management lehnt ab oder schlägt fehl RFCs, wenn ein Stack nicht aktualisiert werden kann, weil der Stack bereits von einem anderen RFC aktualisiert wird. AMS empfiehlt, dass Sie jeweils einen RFC erstellen und warten, bis der RFC erfolgreich ist, bevor Sie einen neuen für denselben Stack starten.

Fehler bei RFC-IAM-Entitäten

AMS stellt eine Reihe von Standard-IAM-Rollen und -Profilen für AMS-Konten bereit, die auf Ihre Bedürfnisse zugeschnitten sind. Möglicherweise müssen Sie jedoch gelegentlich zusätzliche IAM-Ressourcen anfordern.

Das Verfahren zur Einreichung von RFCs Anfragen für benutzerdefinierte IAM-Ressourcen folgt dem Standardablauf für manuelle Anwendungen. Der Genehmigungsprozess umfasst jedoch auch eine Sicherheitsüberprüfung RFCs, um sicherzustellen, dass angemessene Sicherheitskontrollen vorhanden sind. Daher dauert der Vorgang in der Regel länger als bei anderen manuellen RFCs Vorgängen. Um die Zykluszeit bei diesen zu reduzieren RFCs, befolgen Sie bitte die folgenden Richtlinien.

Informationen darüber, was wir unter einer IAM-Überprüfung verstehen und wie sie unseren technischen Standards und unserem Prozess zur Risikoakzeptanz entspricht, finden Sie unter [RFC-Sicherheitsüberprüfungen verstehen](#).

Häufig gestellte Anfragen zu IAM-Ressourcen:

- Wenn Sie nach einer Richtlinie für eine wichtige Cloud-kompatible Anwendung fragen, wie z. B. CloudEndure, schauen Sie sich die vorab genehmigte CloudEndure IAM-Richtlinie von AMS an: Entpacken Sie die [WIGs Cloud Endure Landing Zone-Beispieldatei](#) und öffnen Sie die `customer_cloud_endure_policy.json`

Note

Wenn Sie eine restriktivere Richtlinie wünschen, besprechen Sie Ihre Bedürfnisse mit Ihrem Unternehmen und lassen Sie sich, falls erforderlich, von einem AMS Security Review

CloudArchitect/CSDM und Signoff überzeugen, bevor Sie einen RFC zur Umsetzung der Richtlinie einreichen.

- Wenn Sie eine von AMS standardmäßig in Ihrem Konto bereitgestellte Ressource ändern möchten, empfehlen wir Ihnen, anstelle von Änderungen an der vorhandenen eine modifizierte Kopie dieser Ressource anzufordern.
- Wenn Sie Berechtigungen für einen menschlichen Benutzer anfordern (anstatt die Berechtigungen dem Benutzer zuzuweisen), ordnen Sie die Berechtigungen einer Rolle zu und gewähren Sie dem Benutzer dann die Erlaubnis, diese Rolle anzunehmen. Einzelheiten dazu finden Sie unter [Temporärer Zugriff auf die AMS Advanced-Konsole](#).
- Wenn Sie außergewöhnliche Berechtigungen für eine temporäre Migration oder einen temporären Workflow benötigen, geben Sie in Ihrer Anfrage ein Enddatum für diese Berechtigungen an.
- Wenn Sie den Gegenstand Ihrer Anfrage bereits mit Ihrem Sicherheitsteam besprochen haben, legen Sie Ihrem CSDM so detailliert wie möglich einen Nachweis über deren Genehmigung vor.

Wenn AMS einen IAM-RFC ablehnt, geben wir einen klaren Grund für die Ablehnung an.

Beispielsweise könnten wir eine Anfrage zur Erstellung einer IAM-Richtlinie ablehnen und erklären, was an der Richtlinie unangemessen ist. In diesem Fall können Sie die identifizierten Änderungen vornehmen und die Anfrage erneut einreichen. Wenn weitere Informationen zum Status einer Anfrage erforderlich sind, reichen Sie eine Serviceanfrage ein oder wenden Sie sich an Ihren CSDM.

In der folgenden Liste werden die typischen Risiken beschrieben, die AMS bei der Überprüfung Ihres IAM zu minimieren versucht. RFCs Wenn Ihr IAM-RFC eines dieser Risiken birgt, kann dies zur Ablehnung des RFC führen. In Fällen, in denen Sie eine Ausnahme benötigen, bittet AMS Ihr Sicherheitsteam um die Genehmigung. Um eine solche Ausnahme zu beantragen, stimmen Sie sich mit Ihrem CSDM ab.

Note

AMS kann aus beliebigem Grund jegliche Änderung der IAM-Ressourcen innerhalb eines Kontos ablehnen. Wenn Sie Bedenken bezüglich einer RFC-Ablehnung haben, wenden Sie sich über eine Serviceanfrage an AMS Operations oder wenden Sie sich an Ihren CSDM.

- Eskalation von Rechten, z. B. Berechtigungen, die es Ihnen ermöglichen, Ihre eigenen Berechtigungen oder die Berechtigungen anderer Ressourcen innerhalb des Kontos zu ändern. Beispiele:

- Die Verwendung `iam:PassRole` mit einer anderen, privilegiierteren Rolle.
- Zugriff auf `attach/detach` IAM-Richtlinien durch eine Rolle oder einen Benutzer.
- Die Änderung der IAM-Richtlinien im Konto.
- Die Fähigkeit, API-Aufrufe im Kontext der Verwaltungsinfrastruktur zu tätigen.
- Berechtigungen zum Ändern von Ressourcen oder Anwendungen, die für die Bereitstellung von AMS-Diensten für Sie erforderlich sind. Beispiele:
 - Änderung der AMS-Infrastruktur wie der Bastions-, Management-Host- oder EPS-Infrastruktur.
 - Löschen von Protokollverwaltungsfunktionen, AWS Lambda Lambda-Funktionen oder Protokollstreams.
 - Das Löschen oder Ändern der CloudTrail Standard-Überwachungsanwendung.
 - Die Änderung des Active Directory (AD) der Verzeichnisdienste.
 - Deaktivierung CloudWatch (CW) von Alarmen.
 - Die Änderung der Principals, Richtlinien und Namespaces, die im Konto als Teil der landing zone bereitgestellt werden.
- Bereitstellung von Infrastruktur außerhalb von bewährten Verfahren, wie z. B. Genehmigungen, die den Aufbau einer Infrastruktur in einem Zustand ermöglichen, der Ihre Informationssicherheit gefährdet. Beispiele:
 - Die Erstellung von öffentlichen oder unverschlüsselten S3-Buckets oder die öffentliche gemeinsame Nutzung von EBS-Volumes.
 - Die Bereitstellung öffentlicher IP-Adressen.
 - Die Änderung von Sicherheitsgruppen, um einen breiten Zugriff zu ermöglichen.
- Zu weit gefasste Berechtigungen können Auswirkungen auf Anwendungen haben, z. B. Berechtigungen, die zu Datenverlust, Integritätsverlust, unangemessener Konfiguration oder Betriebsunterbrechungen für Ihre Infrastruktur und die Anwendungen innerhalb des Kontos führen können. Beispiele:
 - Deaktivierung oder Umleitung von Netzwerkverkehr über ähnliche oder. APIs `ModifyNetworkInterfaceAttribute UpdateRouteTable`
 - Deaktivierung der verwalteten Infrastruktur durch Trennen von Volumes von verwalteten Hosts.
- Berechtigungen für Dienste, die nicht Teil der AMS-Servicebeschreibung sind und von AMS nicht unterstützt werden.

Dienste, die nicht in der AMS-Servicebeschreibung aufgeführt sind, können nicht in AMS-Konten verwendet werden. Wenn Sie Support für eine Funktion oder einen Dienst anfordern möchten, wenden Sie sich bitte an Ihren CSDM.

- Genehmigungen, die Ihr erklärtes Ziel nicht erfüllen, da sie entweder zu großzügig oder zu konservativ sind oder auf die falschen Ressourcen angewendet werden. Beispiele:
 - Eine Anfrage nach `s3:PutObject` Berechtigungen für einen S3-Bucket mit obligatorischer KMS-Verschlüsselung ohne `KMS:Encrypt` Berechtigungen für den entsprechenden Schlüssel.
 - Berechtigungen, die sich auf Ressourcen beziehen, die im Konto nicht vorhanden sind.
 - IAM RFCs , bei dem die Beschreibung des RFC nicht mit der Anfrage zu übereinstimmen scheint.

RFC-Fehler bei der „Bereitstellung“

Mit den Änderungstypen für die Kategorie „Einsatz“ (CTs) von AMS können Sie beantragen, dass Ihrem Konto verschiedene AMS-unterstützte Ressourcen hinzugefügt werden.

Die meisten AMS CTs , die eine Ressource erstellen, basieren auf CloudFormation Vorlagen. Als Kunde haben Sie Lesezugriff auf alle AWS-Services CloudFormation, einschließlich, Sie können anhand der CloudFormation Stack-Beschreibung mithilfe der Konsole schnell den Stack identifizieren, der Ihren Stack darstellt. CloudFormation Der ausgefallene Stack wird sich wahrscheinlich im Status `DELETE_COMPLETE` befinden. Sobald Sie den CloudFormation Stack identifiziert haben, zeigen Ihnen die Ereignisse, welche spezifische Ressource nicht erstellt werden konnte und warum.

Verwenden Sie die CloudFormation Dokumentation zur Fehlerbehebung

Die meisten AMS-Bereitstellungen RFCs verwenden eine CloudFormation Vorlage, und diese Dokumentation kann bei der Fehlerbehebung hilfreich sein. Die Dokumentation zu dieser CloudFormation Vorlage finden Sie in der Dokumentation:

- Fehler beim Erstellen des Application Load Balancers:
[AWS::ElasticLoadBalancingV2::LoadBalancer \(Application Load Balancer\)](#)
- Auto Scaling Scaling-Gruppe erstellen: [AWS::AutoScaling::AutoScalingGroup \(Auto Scaling-Gruppe\)](#)
- Memcache-Cache erstellen: [AWS::ElastiCache::CacheCluster \(Cache-Cluster\)](#)
- Redis-Cache erstellen: [AWS::ElastiCache::CacheCluster \(Cache-Cluster\)](#)

- DNS-Hosted Zone erstellen (wird zusammen mit Create DNS private/public verwendet): [AWS::Route53::HostedZone](#) (R53 Hosted Zone)
- [DNS-Datensatz erstellen](#) (wird zusammen mit Create DNS private/public verwendet): [\(Ressourcendatensätze\) AWS::Route53::RecordSet](#)
- EC2 Stack erstellen: [AWS::EC2::Instance](#) (Elastic Compute Cloud)
- Elastisches Dateisystem (EFS) erstellen: [AWS::EFS::FileSystem](#) (Elastisches Dateisystem)
- Load Balancer erstellen: [AWS::ElasticLoadBalancing::LoadBalancer](#) (Elastic Load Balancer)
- RDS-Datenbank erstellen: [AWS::RDS::DBInstance](#) (Relationale Datenbank)
- Erstellen Sie Amazon S3: [AWS::S3::Bucket](#) (Simple Storage Service)
- Warteschlange erstellen: [AWS::SQS::Queue](#) (Einfacher Warteschlangendienst)

Fehler beim Erstellen von AMIs RFC

Ein Amazon Machine Image (AMI) ist eine Vorlage, die eine Softwarekonfiguration enthält (z. B. ein Betriebssystem, einen Anwendungsserver und Anwendungen). Von einem AMI aus starten Sie eine Instance, bei der es sich um eine Kopie des AMI handelt, die als virtueller Server in der Cloud ausgeführt wird. AMIs sind sehr nützlich und werden benötigt, um EC2 Instanzen oder Auto Scaling Scaling-Gruppen zu erstellen. Sie müssen jedoch einige Anforderungen beachten:

- Die Instanz, für die Sie angeben, `Ec2InstanceId` muss sich in einem gestoppten Zustand befinden, damit der RFC erfolgreich ist. Verwenden Sie für diesen Parameter keine Auto Scaling Scaling-Gruppeninstanzen (ASG), da die ASG eine gestoppte Instance beendet.
- Um ein AMS Amazon Machine Image (AMI) zu erstellen, müssen Sie mit einer AMS-Instance beginnen. Bevor Sie die Instance zum Erstellen des AMI verwenden können, müssen Sie sie vorbereiten, indem Sie sicherstellen, dass sie gestoppt und von ihrer Domäne getrennt ist. Einzelheiten finden Sie unter [Erstellen eines standardmäßigen Amazon-Computerabbilds mithilfe von Sysprep](#)
- Der Name, den Sie für das neue AMI angeben, muss innerhalb des Kontos eindeutig sein, sonst schlägt der RFC fehl. Wie das geht, ist unter [AMI | Create](#) beschrieben. Weitere Informationen finden Sie unter [AWS AMI Design](#).

Note

Weitere Informationen zur Vorbereitung der AMI-Erstellung finden Sie unter [AMI | Create](#).

RFCs Erstellen EC2s oder Fehler ASGs

Bei EC2 oder ASG-Ausfällen mit Timeouts empfiehlt AMS, zu überprüfen, ob das verwendete AMI angepasst ist. Falls ja, lesen Sie bitte die Schritte zur AMI-Erstellung in diesem Handbuch (siehe [AMI | Create](#)), um sicherzustellen, dass das AMI korrekt erstellt wurde. Ein häufiger Fehler beim Erstellen eines benutzerdefinierten AMI besteht darin, die Schritte im Handbuch zum Umbenennen oder Aufrufen von Sysprep nicht zu befolgen.

RFCs Erstellen von RDS-Fehlern

Fehler im Amazon Relational Database Service (RDS) können aus vielen verschiedenen Gründen auftreten, da Sie bei der Erstellung des RDS viele verschiedene Engines verwenden können und jede Engine ihre eigenen Anforderungen und Einschränkungen hat. Bevor Sie versuchen, einen AMS-RDS-Stack zu erstellen, überprüfen Sie die AWS-RDS-Parameterwerte sorgfältig, siehe [Erstellen DBInstance](#).

Weitere Informationen zu Amazon RDS im Allgemeinen, einschließlich Größenempfehlungen, finden Sie in der [Dokumentation zu Amazon Relational Database Service](#).

RFCs Amazon S3-Fehler erstellen

Ein häufiger Fehler beim Erstellen eines S3-Speicher-Buckets besteht darin, dass kein eindeutiger Name für den Bucket verwendet wird. Wenn Sie einen S3-Bucket Create CT mit demselben Namen wie einen zuvor eingereichten eingereicht haben, würde dies fehlschlagen, da bereits ein S3-Bucket mit diesem Bucket vorhanden wäre BucketName. Dies wird in der CloudFormation Konsole detailliert beschrieben, wo Sie sehen werden, dass das Stack-Ereignis anzeigt, dass der Bucket-Name bereits verwendet wird.

RFC-Validierung versus Ausführungsfehler

RFC-Fehler und zugehörige Meldungen unterscheiden sich in den Ausgabemeldungen auf der RFC-Detailseite der AMS-Konsole für einen ausgewählten RFC:

- Die Gründe für Validierungsfehler sind nur im Statusfeld verfügbar
- Die Gründe für Ausführungsfehler sind sowohl in den Feldern Ausführungsausgabe als auch in den Statusfeldern verfügbar.

RFC-Fehlermeldungen

Wenn Sie bei den aufgelisteten Änderungstypen (CTs) auf den folgenden Fehler stoßen, können Sie diese Lösungen verwenden, um die Ursache der Probleme zu finden und sie zu beheben.

```
{"errorMessage":"An error has occurred during RFC execution. We are investigating the issue.", "errorType":"InternalError"}
```

Wenn Sie weitere Unterstützung benötigen, nachdem Sie sich auf die folgenden Optionen zur Fehlerbehebung bezogen haben, wenden Sie sich per RFC-Korrespondenz an AMS oder stellen Sie eine Serviceanfrage. Weitere Informationen finden Sie unter [RFC-Korrespondenz und Anhang \(Konsole\)](#) und [Erstellen einer Serviceanfrage in AMS](#).

Fehler bei der Workload Ingestion (WIGS)

Note

Validierungstools für Windows und Linux können heruntergeladen und direkt auf Ihren lokalen Servern sowie auf EC2 Instanzen in AWS ausgeführt werden. Diese finden Sie im AMS Advanced Application Developer's Guide [Migrating workloads: Linux pre-ingestion validation](#) und [Migrating workloads: Windows pre-ingestion validation](#).

- EC2 Stellen Sie sicher, dass die Instanz im AMS-Zielkonto vorhanden ist. Wenn Sie beispielsweise Ihr AMI von einem Nicht-AMS-Konto für ein AMS-Konto freigegeben haben, müssen Sie in Ihrem AMS-Konto eine EC2 Instance mit dem gemeinsam genutzten AMI erstellen, bevor Sie einen Workload Ingest RFC einreichen können.
- Prüfen Sie, ob für die mit der Instance verbundenen Sicherheitsgruppen ausgehender Datenverkehr zulässig ist. Der SSM-Agent muss in der Lage sein, eine Verbindung zu seinem öffentlichen Endpunkt herzustellen.
- Überprüfen Sie, ob die Instanz über die richtigen Berechtigungen verfügt, um eine Verbindung mit dem SSM-Agenten herzustellen. Diese Berechtigungen sind im Lieferumfang `customer-mc-ec2-instance-profile` enthalten. Sie können dies in der EC2 Konsole überprüfen:

EC2 Fehler beim Stopp des Instance-Stacks

- Prüfen Sie, ob sich die Instance bereits in einem gestoppten oder beendeten Zustand befindet.

- Wenn die EC2 Instance online ist und Ihnen der `InternalError` Fehler angezeigt wird, senden Sie eine Serviceanfrage an AMS zur Untersuchung.
- Beachten Sie, dass Sie den Änderungstyp `Management | Advanced stack components | EC2 instance stack | Stop ct-3mvt2zkyvej` nicht verwenden können, um eine Auto Scaling Scaling-Gruppeninstanz (ASG) zu stoppen. Wenn Sie eine ASG-Instance beenden müssen, reichen Sie eine Serviceanfrage ein.

EC2 Fehler beim Erstellen des Instanzstapels

Die `InternalError` Nachricht stammt von CloudFormation; ein Grund für den Status `CREATION_FAILED`. Einzelheiten zum Stack-Fehler finden Sie in CloudWatch Stack-Ereignissen, indem Sie die folgenden Schritte ausführen:

- In der AWS-Managementkonsole können Sie eine Liste von Stack-Ereignissen anzeigen, während Ihr Stack erstellt, aktualisiert oder gelöscht wird. Finden Sie das Fehlerereignis in dieser Liste und sehen dann den Statusgrund für dieses Ereignis an.

Der Statusgrund kann eine Fehlermeldung von AWS CloudFormation oder von einem bestimmten Service enthalten, die Ihnen helfen kann, das Problem zu verstehen.

- Weitere Informationen zum Anzeigen von Stack-Ereignissen finden Sie unter [CloudFormation AWS-Stack-Daten und -Ressourcen in der AWS-Managementkonsole anzeigen](#).

EC2 Fehler bei der Wiederherstellung des Instance-Volumes

AMS erstellt einen internen RFC zur Fehlerbehebung, wenn die Wiederherstellung des EC2 Instance-Volumes fehlschlägt. Dies geschieht, weil die Wiederherstellung des EC2 Instance-Volumes ein wichtiger Bestandteil der Notfallwiederherstellung (DR) ist und AMS diesen internen RFC zur Fehlerbehebung automatisch für Sie erstellt.

Wenn der interne RFC zur Fehlerbehebung erstellt wurde, wird ein Banner mit Links zum RFC angezeigt. Dieser interne RFC zur Fehlerbehebung bietet Ihnen mehr Einblick in RFC-Fehler. Anstatt Wiederholungsversuche zu senden, die zu denselben Fehlern RFCs führen, oder Sie müssen sich wegen dieses Fehlers manuell an AMS wenden, können Sie Ihre Änderungen verfolgen und wissen, dass AMS an dem Fehler arbeitet. Dadurch wird auch die `time-to-recovery (TTR)` -Metrik für ihre Änderung reduziert, da AMS-Operatoren proaktiv an dem RFC-Fehler arbeiten, anstatt auf Ihre Anfrage zu warten.

Wie erhalte ich Hilfe bei einem RFC

Sie können sich an AMS wenden, um die Ursache Ihres Fehlers zu ermitteln. Die AMS-Geschäftszeiten sind 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr.

AMS bietet Ihnen verschiedene Möglichkeiten, um Hilfe zu bitten oder Serviceanfragen zu stellen.

- Verwenden Sie die AMS-Konsole und senden Sie eine Serviceanfrage, um Informationen oder Beratung oder um Zugriff auf einen von AMS verwalteten IT-Service zu erhalten oder um einen zusätzlichen Service von AMS anzufordern. Einzelheiten finden Sie unter [Serviceanfrage erstellen](#). Allgemeine Informationen zu AMS-Serviceanfragen finden Sie unter [Verwaltung von Serviceanfragen](#).
- Um ein Leistungsproblem mit dem AWS- oder AMS-Service zu melden, das sich auf Ihre verwaltete Umgebung auswirkt, verwenden Sie die AMS-Konsole und reichen Sie einen Vorfallbericht ein. Einzelheiten finden Sie unter [Einen Vorfall melden](#). Allgemeine Informationen zum AMS Incident Management finden Sie unter [Reaktion auf Vorfälle](#).
- Wenn Sie spezielle Fragen dazu haben, wie Sie oder Ihre Ressourcen oder Anwendungen mit AMS zusammenarbeiten, oder um einen Vorfall zu eskalieren, senden Sie eine E-Mail an eine oder mehrere der folgenden Adressen:
 1. Wenn Sie mit der Serviceanfrage oder der Antwort auf den Vorfallbericht nicht zufrieden sind, senden Sie zunächst eine E-Mail an Ihren CSDM: ams-csdm@amazon.com
 2. Als Nächstes können Sie, falls eine Eskalation erforderlich ist, eine E-Mail an den AMS Operations Manager senden (aber Ihr CSDM wird das wahrscheinlich tun): ams-opsmanager@amazon.com
 3. Eine weitere Eskalation erfolgt an den AMS-Direktor: ams-director@amazon.com
 4. Schließlich sind Sie immer in der Lage, den AMS VP zu erreichen: ams-vp@amazon.com

Direkter Änderungsmodus in AMS

Themen

- [Erste Schritte mit dem Direct Change-Modus](#)
- [Sicherheit und Compliance](#)
- [Änderungsmanagement im Direct Change-Modus](#)
- [Stapel im Direct Change-Modus erstellen](#)
- [Anwendungsfälle für den Direct Change Mode](#)

Der Direct Change Mode (DCM) von AWS Managed Services (AMS) erweitert das AMS Advanced Change Management um systemeigenen AWS Zugriff auf AMS Advanced Plus- und Premium-Konten zur Bereitstellung und Aktualisierung von AWS Ressourcen. Mit DCM haben Sie die Möglichkeit, native AWS API (Konsole oder CLI/SDK) oder AMS Advanced Change Management Requests for change (RFCs) zu verwenden. In beiden Fällen werden die Ressourcen und Änderungen daran vollständig von AMS unterstützt, einschließlich Überwachung, Patch, Backup und Incident Response Management. Über DCM bereitgestellte Ressourcen werden im AMS Service Knowledge Management System (SKMS) registriert, der von AMS verwalteten Active Directory-Domäne (falls zutreffend) hinzugefügt und führen AMS-Management-Agenten aus. Verwenden Sie vorhandene Tools (z. B. AWS SDK und CDK) CloudFormation, um AMS-verwaltete Stacks zu entwickeln und bereitzustellen. CloudFormation

 Note

Durch den Direct Change-Modus wird das AMS-Änderungsmanagement nicht entfernt. RFCs
RFCs Mit DCM haben Sie vollen Zugriff auf AMS.

[Sehen Sie sich das Video von Akash an, um mehr zu erfahren \(6:30\)](#)

Erste Schritte mit dem Direct Change-Modus

Überprüfen Sie zunächst die Voraussetzungen und reichen Sie dann einen Änderungsantrag (RFC) in Ihrem berechtigten AMS Advanced-Konto ein.

1. Vergewissern Sie sich, dass das Konto, das Sie mit DCM verwenden möchten, die Anforderungen erfüllt:
 - Das Konto ist AMS Advanced Plus oder Premium.
 - Für das Konto ist Service Catalog nicht aktiviert. Wir unterstützen derzeit nicht das gleichzeitige Onboarding von Konten für DCM und Service Catalog. Wenn Sie bereits bei Service Catalog angemeldet sind, aber an DCM interessiert sind, besprechen Sie Ihre Anforderungen mit Ihrem Cloud Service Delivery Manager (CSDM). Wenn Sie sich dazu entschließen, von Service Catalog zu DCM, Offboard Service Catalog, zu wechseln, fügen Sie die Anfrage in die unten stehende Änderungsanfrage ein. Einzelheiten zum Service Catalog in AMS finden Sie unter [AMS und Service Catalog](#).

2. Senden Sie eine Änderungsanforderung (RFC) über die Optionen Verwaltung | Verwaltetes Konto | Direkter Änderungsmodus | Änderungstyp aktivieren (ct-3rd4781c2nnhp). [Ein Beispiel für eine exemplarische Vorgehensweise finden Sie unter Direkter Änderungsmodus | Aktivieren.](#)

Nach der Verarbeitung des CT werden die vordefinierten IAM-Rollen `AWSManagedServicesCloudFormationAdminRole` und `AWSManagedServicesUpdateRole` im angegebenen Konto bereitgestellt.

3. Weisen Sie den Benutzern, die DCM-Zugriff benötigen, mithilfe Ihres internen Verbundprozesses die entsprechende Rolle zu.

Note

Sie können eine beliebige Anzahl von SAMLIdentity Anbietern, AWS Diensten und IAM-Entitäten (Rollen, Benutzer usw.) angeben, um die Rollen zu übernehmen. Sie müssen mindestens ein: `SAMLIdentityProviderARNsIAMEntityARNs`, oder `AWSServicePrincipals` angeben. Weitere Informationen erhalten Sie von der IAM-Abteilung Ihres Unternehmens oder von Ihrem AMS Cloud Architect (CA).

IAM-Rollen und -Richtlinien im Direktänderungsmodus

Wenn der Direct Change-Modus in einem Konto aktiviert ist, werden diese neuen IAM-Entitäten bereitgestellt:

`AWSManagedServicesCloudFormationAdminRole`: Diese Rolle gewährt Zugriff auf die CloudFormation Konsole, das Erstellen und Aktualisieren von CloudFormation Stacks, das Anzeigen von Drift-Berichten sowie das Erstellen und Ausführen. CloudFormation ChangeSets Der Zugriff auf diese Rolle wird über Ihren SAML-Anbieter verwaltet.

Folgende verwaltete Richtlinien werden bereitgestellt und der Rolle `AWSManagedServicesCloudFormationAdminRole` zugewiesen:

- AMS Advanced-Anwendungskonto für mehrere Konten (MALZ)
 - `AWSManagedServices_CloudFormationAdminPolicy1`
 - `AWSManagedServices_CloudFormationAdminPolicy2`
 - Diese Richtlinie stellt die Berechtigungen dar, die dem gewährt wurden.
- `AWSManagedServicesCloudFormationAdminRole` Sie und Ihre Partner verwenden diese

Richtlinie, um Zugriff auf eine bestehende Rolle im Konto zu gewähren und dieser Rolle das Starten und Aktualisieren von CloudFormation Stacks im Konto zu ermöglichen. Dies kann zusätzliche Aktualisierungen der AMS Service Control Policy (SCP) erfordern, damit andere IAM-Entitäten Stacks starten können. CloudFormation

- AMS Advanced-Landingzone-Konto (SALZ) mit einem Konto
 - AWSManagedServices_CloudFormationAdminPolicy1
 - AWSManagedServices_CloudFormationAdminPolicy2
 - cdk-legacy-mode-s[Inline-Richtlinie] mit 3 Zugriffen
 - AWS ReadOnlyAccess Richtlinie

AWSManagedServicesUpdateRole: Diese Rolle gewährt eingeschränkten Zugriff auf nachgelagerte AWS Dienste APIs. Die Rolle wird mit verwalteten Richtlinien bereitgestellt, die mutierende und nicht mutierende API-Operationen bereitstellen, aber im Allgemeinen mutierende Operationen (wie Create/Delete/PUT) für bestimmte Dienste wie IAM, KMS, VPC, AMS-Infrastrukturressourcen und -konfiguration usw. einschränken. GuardDuty Der Zugriff auf diese Rolle wird über Ihren SAML-Anbieter verwaltet.

Folgende verwaltete Richtlinien werden bereitgestellt und der Rolle **AWSManagedServicesUpdateRole** zugewiesen:

- AMS Advanced landing zone Anwendungskonto für mehrere Konten
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyPolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2Und RDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitik
- AMS Advanced-Landingzone-Konto mit einem Konto
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2Und RDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSInfraRichtlinie 1
 - AWSManagedServicesUpdateDenyActionsOnAMSInfraRichtlinie 2

Darüber hinaus ist der `AWSManagedServicesUpdateRole` Rolle „Verwaltete Richtlinie“ auch die AWS verwaltete Richtlinie `ViewOnlyAccess` zugeordnet.

Sicherheit und Compliance

Für Sicherheit und Compliance sind AMS Advanced und Sie als unser Kunde gemeinsam verantwortlich. Der AMS Advanced Direct Change-Modus ändert nichts an dieser gemeinsamen Verantwortung.

Sicherheit im Direct Change-Modus

AMS Advanced bietet zusätzlichen Mehrwert mit einer präskriptiven landing zone, einem Change-Management-System und einer Zugriffsverwaltung. Bei Verwendung des Direct Change-Modus ändert sich dieses Verantwortungsmodell nicht. Sie sollten sich jedoch zusätzlicher Risiken bewusst sein.

Die Rolle „Update“ im Direktänderungsmodus (siehe [IAM-Rollen und -Richtlinien im Direktänderungsmodus](#)) bietet erweiterte Berechtigungen, sodass die Entität, die Zugriff darauf hat, Änderungen an den Infrastrukturressourcen der von AMS unterstützten Dienste in Ihrem Konto vornehmen kann. Bei erhöhten Berechtigungen bestehen je nach Ressource, Service und Aktion unterschiedliche Risiken, insbesondere in Situationen, in denen aufgrund eines Versehens, eines Fehlers oder der mangelnden Einhaltung Ihres internen Prozess- und Kontrollrahmens eine falsche Änderung vorgenommen wird.

Gemäß den technischen Standards von AMS wurden die folgenden Risiken identifiziert, und es werden folgende Empfehlungen ausgesprochen. Detaillierte Informationen zu den technischen Standards von AMS finden Sie unter AWS Artifact. Um darauf zuzugreifen AWS Artifact, wenden Sie sich an Ihren CSDM, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS Artifact](#).

AMS-STD-001: Taggen

Normen	Geht es kaputt	Risiken	Empfehlungen
Alle AMS-eigenen Ressourcen müssen das folgende Schlüssel-Wert-Paar haben	Ja. Unterbrechungen für CloudFormation, CloudTrail, EFS, OpenSearch, CloudWatch	Eine falsche Kennzeichnung von AMS-Ressourcen kann sich nachteilig auf die Berichts-	Der Zugriff muss eingeschränkt werden, um Änderungen an den standardmäßigen

Normen	Geht es kaputt	Risiken	Empfehlungen
Alle AMS-eigenen Tags, mit Ausnahme der oben aufgeführten, müssen Präfixe wie oder in case haben. AMS* MC* upper/lower/mix	Logs, SQS, SSM, Tagging-API — da diese Dienste die <code>aws:TagsKey</code> Bedingung, das Tagging für den AMS-Namespace einzuschränken, nicht unterstützen. Der in der folgenden Tabelle AMS-STD-003 angegebene Standard besagt, dass Sie die Umgebung und ändern Appld können, aber nicht für AMS-eigene Ressourcen. AppName Mit IAM-Berechtigungen nicht erreichbar.	, Warnungs- und Patching-Vorgänge Ihrer Ressourcen auf AMS-Seite auswirken.	AMS-Tagging-Anforderungen für andere Personen als AMS-Teams vorzunehmen.
Alle Tags in AMS-eigenen Stacks dürfen aufgrund Ihrer Änderungsanforderungen nicht gelöscht werden.	Ja. CloudFormation unterstützt nicht die <code>aws:TagsKey</code> Bedingung, Tags für den AMS-Namespace einzuschränken.		

Normen	Geht es kaputt	Risiken	Empfehlungen
Es ist Ihnen nicht gestattet, die AMS-Tag-Namenskonvention in Ihrer Infrastruktur zu verwenden, wie in Tabelle AMS-STD-002, weiter unten beschrieben.	Ja. Unterbrechungen für CloudFormation, CloudTrail, Amazon Elastic File System (EFS), OpenSearch, CloudWatch Logs, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM), Tagging API; diese Dienste unterstützen nicht die <code>aws:TagsKey</code> Bedingung, das Tagging für den AMS-Namespace einzuschränken.		

AMS-STD-002: Identity and Access Management (IAM)

Normen	Geht es kaputt	Risiken	Empfehlungen
4.7 Aktionen, die den Change Management Process (RFC) umgehen, dürfen nicht erlaubt sein, wie z. B. das Starten oder Stoppen einer Instance, das Erstellen von S3-Buckets oder RDS-Instances	Ja. Der Zweck von Self-Service-Aktionen ermöglicht es Ihnen, Aktionen unter Umgehung des AMS-RFC-Systems durchzuführen.	Das Modell des sicheren Zugriffs ist ein zentraler technischer Aspekt von AMS, und ein IAM-Benutzer für Konsolen- oder programmatischen Zugriff umgeht diese Zugriffskontrolle. Der Zugriff der	Der IAM-Benutzer sollte zeitlich begrenzt sein und ihm sollten Berechtigungen auf der Grundlage der geringsten Rechte und erteilt werden. need-to-know

Normen	Geht es kaputt	Risiken	Empfehlungen
usw. Konten im Entwicklermodus und Dienste im Self-Service Provisioned Mode (SSPS) sind ausgenommen, solange die Aktionen innerhalb der Grenzen der zugewiesenen Rolle ausgeführt werden.		IAM-Benutzer wird nicht vom AMS Change Management überwacht. Der Zugriff ist CloudTrail nur angemeldet.	

AMS-STD-003: Netzwerksicherheit

Standards	Geht es kaputt	Risiken	Empfehlungen
S2. Elastic IP auf EC2 Instances darf nur mit einer formellen Risikoakzeptanzvereinbarung oder mit einem gültigen Anwendungsfall durch interne Teams verwendet werden.	Ja. Self-Service-Aktionen ermöglichen es Ihnen, Elastic IP-Adressen (EIP) zuzuordnen und die Zuordnung aufzuheben.	Durch das Hinzufügen einer Elastic IP zu einer Instance wird sie dem Internet zugänglich gemacht. Dies erhöht das Risiko der Offenlegung von Informationen und unberechtigter Aktivitäten.	Blockieren Sie jeglichen unnötigen Datenverkehr zu dieser Instance über Sicherheitsgruppen und stellen Sie sicher, dass Ihre Sicherheitsgruppen mit der Instance verknüpft sind, um sicherzustellen, dass der Datenverkehr nur dann zugelassen wird, wenn er aus geschäftlichen Gründen benötigt wird.
S14. VPC-Peering und Endpunkt	Ja. Dies ist im Rahmen der IAM-	Der Datenverkehr, der Ihr AMS-Konto	Wir empfehlen, nur mit AMS-Konten

Standards	Geht es kaputt	Risiken	Empfehlungen
Verbindungen zwischen Konten, die demselben Kunden gehören, können zugelassen werden.	Richtlinie nicht möglich.	verlässt, wird nicht überwacht, sobald er die Kontogrenze überschreitet.	zu peeren, die Sie besitzen. Wenn Ihr Anwendungsfall dies erfordert, verwenden Sie Sicherheitsgruppen und Routingtabellen, um zu begrenzen, welche Datenverkehrsbereiche, Ressourcen und Typen über die entsprechende Verbindung abfließen können.
Die AMS-Basis AMIs kann von AMS-verwalteten und nicht verwalteten Konten gemeinsam genutzt werden, sofern wir überprüfen können, ob sie derselben Organisation gehören. AWS		AMIs kann sensible Daten enthalten und unbeabsichtigten Konten ausgesetzt sein.	Teilen Sie die Daten nur mit AMIs mit dem Konto, das Ihrer Organisation gehört, oder überprüfen Sie den Anwendungsfall und die Kontoinformationen, bevor Sie sie an Dritte weitergeben.

AMS-STD-007: Protokollierung

Normen	Geht es kaputt	Risiken	Empfehlungen
19. Jedes Protokoll kann von einem AMS-Konto an ein anderes AMS-Konto desselben	Ja. Mögliche Unsicherheiten in Bezug auf Kundenprotokolle, da die Überprüfung, ob sich	Protokolle können vertrauliche Daten enthalten und sie können unbefugten	Teilen Sie Protokolle nur mit Konten, die von Ihrer AWS Organisation verwaltet werden, oder

Normen	Geht es kaputt	Risiken	Empfehlungen
Kunden weitergeleitet werden. 20. Jedes Protokoll kann nur dann von AMS an ein Nicht-AMS-Konto weitergeleitet werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain mit dem Firmennamen des Kunden und dem mit PAYER verknüpften Konto abgeglichen wird). Dabei werden interne Tools verwendet.	die Kundenkonten in derselben Organisation befinden, nicht durch die IAM-Richtlinie erreicht werden kann.	Konten zugänglich gemacht werden.	überprüfen Sie den Anwendungsfall und die Kontoinformationen, bevor Sie sie an Dritte weitergeben. Wir können dies auf verschiedene Weise überprüfen. Erkundigen Sie sich bei Ihrem Cloud Service Delivery Manager (CSDM).

Arbeiten Sie mit Ihrem internen Autorisierungs- und Authentifizierungsteam zusammen, um die Berechtigungen für die Rollen im Direct Change-Modus entsprechend zu kontrollieren.

Einhaltung der Vorschriften im Modus „Direkter Wandel“

Der Direct Change-Modus ist sowohl mit produktiven als auch mit produktionsfremden Workloads kompatibel. Es liegt in Ihrer Verantwortung, die Einhaltung aller Compliance-Standards (z. B. PHI, HIPAA, PCI) sicherzustellen und sicherzustellen, dass die Verwendung des Direct Change-Modus Ihren internen Kontrollrahmen und Standards entspricht.

Änderungsmanagement im Direct Change-Modus

Änderungsmanagement ist der Prozess, den AMS Advanced verwendet, um Änderungsanträge zu implementieren. Eine Änderungsanforderung (RFC) ist eine Anfrage, die entweder von Ihnen oder AMS Advanced über die AMS Advanced-Schnittstelle erstellt wird, um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen. Sie enthält eine AMS Advanced-Änderungstyp-ID (CT) für einen bestimmten Vorgang. Weitere Informationen finden Sie unter [Change Management](#).

Note

Durch den Direct Change-Modus wird das AMS-Änderungsmanagement RFCs nicht entfernt. RFCs Mit DCM haben Sie weiterhin vollen Zugriff auf AMS.

Der AMS Direct Change-Modus (DCM) erweitert das AMS Advanced Change Management, indem er systemeigenen AWS Zugriff auf AMS Advanced Plus- und Premium-Konten ermöglicht, um Ressourcen bereitzustellen und zu aktualisieren AWS . Benutzer, denen über die IAM-Rollen die Berechtigung zum Direct Change-Modus erteilt wurde, können den systemeigenen AWS API-Zugriff verwenden, um Ressourcen in ihren AMS Advanced-Konten bereitzustellen und zu ändern. Die Benutzer können AMS Advanced Change Management weiterhin RFCs mit denselben IAM-Rollen verwenden. In beiden Fällen werden die Ressourcen und deren Änderungen vollständig von AMS unterstützt, einschließlich Überwachung, Patch, Backup und Incident Response Management. Benutzer, die nicht über die entsprechende Rolle in diesen Konten verfügen, müssen den RFC-Prozess AMS Advanced Change Management verwenden, um Änderungen vorzunehmen.

Anwendungsfälle des Change-Managements

Aus Sicherheitsgründen können einige Änderungen in AMS Advanced nur über den RFC-Prozess (Change Management Request for Change) vorgenommen werden. Der `AWSManagedServicesCloudFormationAdminRole` ist auf Aktionen beschränkt, die durch CloudFormation (CFN) ergriffen wurden. Weitere Informationen zum Erstellen von Stacks mit DCM finden Sie unter [Erstellen von Stacks im Direct Change-Modus](#). Der `AWSManagedServicesUpdateRole` ist auf die folgenden Aktionen beschränkt.

[Exemplarische Vorgehensweisen für jeden Änderungstyp, einschließlich des Änderungstyps Verwaltung | Verwaltetes Konto | Direkter Änderungsmodus | Aktivieren \(ct-3rd4781c2nnhp\)](#), finden Sie im Abschnitt „Zusätzliche Informationen“ für den entsprechenden Änderungstyp im Abschnitt [AMS Advanced Change Type Reference — Änderungstypen nach Klassifizierung](#).

Service	Aktion
AWS Key Management Service (AWS KMS)	Aktualisierung
AWS Certificate Manager	Erstellen
AWS Identity and Access Management (IAM)	Any
Site-to-Site VPN	Any
AMS-Ressourcenplaner	
AWS Backup	Backup-Plan erstellen
Aufnahme von AMS-Workloads () WIGs	Any
AMS-Ausgangsfilterung (verwaltetes Palo Alto)	
Änderungen am AMS Advanced MALZ-Konto	
Amazon GuardDuty	
Erweiterter AMS-Stack-Zugriff	Any
Volumen von Amazon Elastic Block Store (EBS)	Löschen
Standardverschlüsselung für Amazon Elastic Block Store (EBS)	Aktivieren Sie die Standardverschlüsselung
Amazon Elastic Compute Cloud (Amazon EC2)	Hostnamen ändern
Amazon Machine Images (AMI)	Löschen, teilen
EC2 Amazon-Sicherheitsgruppe	Any
AMS Advanced SSPS	
AWS Verwaltetes Microsoft AD	
AMS Advanced-Entwicklermodus	

Service	Aktion
Amazon Simple Storage Service (Amazon-S3)	Erstellen Sie S3-Bucket-Richtlinien
AWS Systems Manager	Erstellen

Stapel im Direct Change-Modus erstellen

Beim Starten von Stacks CloudFormation mit dem müssen zwei Voraussetzungen erfüllt sein `AWSManagedServicesCloudFormationAdminRole`, damit der Stack von AMS verwaltet werden kann:

- Die Vorlage muss eine `AmsStackTransform` enthalten.
- Der Stackname muss mit dem Präfix beginnen, `stack-` gefolgt von einer 17-stelligen alphanumerischen Zeichenfolge.

Note

Um den erfolgreich verwenden zu können `AmsStackTransform`, müssen Sie bestätigen, dass Ihre Stack-Vorlage die `CAPABILITY_AUTO_EXPAND` Fähigkeit enthält, mit der CloudFormation (CFN) den Stack erstellen oder aktualisieren kann. Sie tun dies, indem Sie das `CAPABILITY_AUTO_EXPAND` als Teil Ihrer Create-Stack-Anfrage übergeben. CFN lehnt die Anfrage ab, wenn diese Funktion nicht bestätigt wird, wenn sie in der Vorlage enthalten `AmsStackTransform` ist. Die CFN-Konsole stellt sicher, dass Sie diese Funktion übergeben, wenn Sie die Transformation in Ihrer Vorlage haben. Dies kann jedoch übersehen werden, wenn Sie über deren Funktion mit CFN interagieren. APIs Sie müssen diese Funktion immer dann weitergeben, wenn Sie die folgenden CFN-API-Aufrufe verwenden:

- [CreateChangeSet](#)
- [CreateStack](#)
- [UpdateStack](#)

Beim Erstellen oder Aktualisieren eines Stacks mit DCM werden dieselben Validierungen und Erweiterungen von CFN Ingest und Stack Update CTs auf dem Stack durchgeführt. Weitere

Informationen finden Sie unter [CloudFormation Ingest-Richtlinien](#), bewährte Methoden und Einschränkungen. Die Ausnahme besteht darin, dass die AMS-Standardsicherheitsgruppen (SGs) nicht an eigenständige EC2 Instances oder EC2 Instances in Auto Scaling Scaling-Gruppen (ASGs) angehängt werden. Wenn Sie Ihre CloudFormation Vorlage mit eigenständigen EC2 Instances oder erstellen ASGs, können Sie die Standardinstanz anhängen. SGs

Note

IAM-Rollen können jetzt mit dem erstellt und verwaltet werden.
`AWSTManagedServicesCloudFormationAdminRole`

Die AMS-Standardeinstellungen SGs verfügen über Eingangs- und Ausgangsregeln, die es ermöglichen, dass die Instances erfolgreich gestartet werden und dass AMS-Operationen und Sie später über SSH oder RDP darauf zugreifen können. Wenn Sie der Meinung sind, dass die AMS-Standardsicherheitsgruppen zu freizügig sind, können Sie Ihre eigenen Regeln SGs mit restriktiveren Regeln erstellen und diese an Ihre Instance anhängen, sofern Sie und AMS-Operationen dadurch weiterhin bei Vorfällen auf die Instance zugreifen können.

Die AMS-Standardsicherheitsgruppen sind die folgenden:

- `SentinelDefaultSecurityGroupPrivateOnly`: Kann in der CFN-Vorlage über diesen SSM-Parameter aufgerufen werden `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- `SentinelDefaultSecurityGroupPrivateOnlyEgressAll`: Kann in der CFN-Vorlage über diesen SSM-Parameter aufgerufen werden `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS-Transformation

Fügen Sie Ihrer CloudFormation Vorlage eine Transform Erklärung hinzu. Dadurch wird ein CloudFormation Makro hinzugefügt, das den Stack beim Start validiert und bei AMS registriert.

JSON-Beispiel

```
"Transform": {  
  "Name": "AmsStackTransform",  
  "Parameters": {  
    "StackId": {"Ref" : "AWS::StackId"}  
  }  
}
```



```
}
```

YAML-Beispiel

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

Fügen Sie die Transform Anweisung auch hinzu, wenn Sie die Vorlage eines vorhandenen Stacks aktualisieren.

JSON-Beispiel

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
  "Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML-Beispiel

```
AWSTemplateFormatVersion: '2010-09-09'
```

```

Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName

```

Stack name

Der Stackname muss mit dem Präfix beginnen, `stack-` gefolgt von einer 17-stelligen alphanumerischen Zeichenfolge. Dies dient der Aufrechterhaltung der Kompatibilität mit anderen AMS-Systemen, die auf dem AMS-Stack IDs arbeiten.

Im Folgenden finden Sie Beispiele für Möglichkeiten, einen kompatiblen Stack zu generieren IDs:

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```

import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))

```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17 | %
{[char]$_}) )
```

Anwendungsfälle für den Direct Change Mode

Im Folgenden sind Anwendungsfälle für den Direct Change Mode aufgeführt:

Bereitstellung und Verwaltung von Ressourcen durch CloudFormation

- Integrieren CloudFormation Sie bestehende Tools und Prozesse.

Kontinuierliches Ressourcenmanagement und Updates

- Kleine atomare Veränderungen mit geringem Risiko.
- Änderungen, die sonst über einen manuellen oder automatisierten RFC laufen würden.
- Tools, für die systemeigener AWS API-Zugriff erforderlich ist.
- Die DCM-Rolle kann verwendet werden, wenn Sie sich in der Migrationsphase befinden.
Migrationsteams nutzen die Berechtigungen auf dem DCM, um Stacks zu erstellen oder zu ändern.
- DCM-Rollen können in der CI/CD Pipeline verwendet werden, um neue Aufgaben zu erstellen
AMIs, Amazon ECS-Aufgaben zu erstellen usw.

AMS Advanced-Entwicklermodus

Themen

- [Erste Schritte mit dem AMS Advanced Developer Mode](#)
- [Sicherheit und Compliance im Entwicklermodus](#)
- [Änderungsmanagement im Entwicklermodus](#)
- [Infrastruktur im AMS-Entwicklermodus bereitstellen](#)
- [Detective Controls im AMS-Entwicklermodus](#)
- [Protokollierung, Überwachung und Ereignisverwaltung im AMS-Entwicklermodus](#)
- [Vorfalmanagement im AMS-Entwicklermodus](#)
- [Patch-Management im AMS-Entwicklermodus](#)
- [Kontinuitätsmanagement im AMS-Entwicklermodus](#)
- [Sicherheits- und Zugriffsmanagement im AMS-Entwicklermodus](#)

Der Entwicklermodus von AWS Managed Services (AMS) verwendet erhöhte Berechtigungen in AMS Advanced Plus- und Premium-Konten, um AWS-Ressourcen außerhalb des AMS Advanced-Change-Management-Prozesses bereitzustellen und zu aktualisieren. Im AMS Advanced Developer-Modus werden dazu native AWS-API-Aufrufe innerhalb der AMS Advanced Virtual Private Cloud (VPC)

genutzt, sodass Sie Infrastruktur und Anwendungen in Ihrer verwalteten Umgebung entwerfen und implementieren können.

Wenn Sie ein Konto verwenden, für das der Entwicklermodus aktiviert ist, werden Continuity Management, Patch Management und Change Management für Ressourcen bereitgestellt, die über den AMS Advanced Change Management-Prozess oder mithilfe eines AMS Amazon Machine Image (AMI) bereitgestellt wurden. Diese AMS-Verwaltungsfunktionen werden jedoch nicht für Ressourcen angeboten, die über native Ressourcen bereitgestellt werden. AWS APIs

Sie sind für die Überwachung der Infrastrukturressourcen verantwortlich, die außerhalb des AMS Advanced Change Management-Prozesses bereitgestellt werden. Der Entwicklermodus ist sowohl mit Produktionsworkloads als auch mit Workloads außerhalb der Produktion kompatibel. Mit erweiterten Berechtigungen tragen Sie eine größere Verantwortung dafür, dass die internen Kontrollen eingehalten werden.

 Important

Ressourcen, die Sie im Entwicklermodus erstellen, können nur dann von AMS Advanced verwaltet werden, wenn sie mithilfe von AMS Advanced-Change-Management-Prozessen erstellt wurden.

Der Entwicklermodus ist einer der AMS-Advanced-Modi, die Sie verwenden können. Weitere Informationen finden Sie unter [Übersicht der Modi](#).

Erste Schritte mit dem AMS Advanced Developer Mode

Lernen Sie die verschiedenen AMS Advanced-Konten im AMS Advanced-Entwicklermodus kennen und erfahren Sie, wie Sie den Entwicklermodus erfolgreich implementieren.

Themen

- [Bevor Sie mit dem AMS-Entwicklermodus beginnen](#)
- [Voraussetzungen für den AMS-Entwicklermodus](#)
- [Wie implementiert man den AMS Advanced Developer-Modus](#)
- [Berechtigungen für den AMS Advanced-Entwicklermodus](#)

Bevor Sie mit dem AMS-Entwicklermodus beginnen

Bevor Sie den Entwicklermodus implementieren, sollten Sie einige Dinge wissen.

AMS Advanced kann keine vorhandenen Stacks oder Ressourcen in einem DevMode Konto verwalten, die außerhalb des AMS Advanced-Änderungsverwaltungsprozesses durch Änderungsanforderungen (RFCs) erstellt wurden. Solange das Konto aktiv ist, verwaltet AMS Advanced jedoch weiterhin die Ressourcen DevMode, die im Rahmen des AMS Advanced-Change-Management-Prozesses mit bereitgestellt wurden. RFCs

Sie können nicht mit einem DevMode Konto beginnen und es später in ein von AMS Advanced verwaltetes Anwendungskonto umwandeln.

Voraussetzungen für den AMS-Entwicklermodus

Im Folgenden sind die Voraussetzungen für die Implementierung des Entwicklermodus aufgeführt:

- Sie müssen ein AMS Advanced-Kunde mit mindestens einem integrierten AMS Advanced Plus- oder Premium-Konto sein.
- Jedes Konto, das Sie verwenden, muss ein AMS Advanced Plus- oder Premium-Konto sein.
- Multi-Account Landing Zone (MALZ): Sie müssen die `AWSManagedServicesDevelopmentRole` vordefinierte Rolle AWS Identity and Access Management (IAM) verwenden. Sie fordern diese Rolle an. Im nächsten Abschnitt wird beschrieben, wie Sie Berechtigungen für den Entwicklermodus erwerben.
- Single-Account Landing Zone (SALZ): Sie müssen die `customer_developer_role` vordefinierte Rolle AWS Identity and Access Management (IAM) verwenden. Sie fordern diese Rolle an. Im nächsten Abschnitt wird beschrieben, wie Sie Berechtigungen für den Entwicklermodus erwerben.

Wie implementiert man den AMS Advanced Developer-Modus

Sie implementieren den Entwicklermodus, indem Sie beantragen, dass Ihrem berechtigten AMS Advanced-Konto die vordefinierte IAM-Rolle zugewiesen wird:

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALZ: `customer_developer_role`

Anschließend weisen Sie die Rolle den entsprechenden Benutzern in Ihrem Verbundnetzwerk zu.

AMS Advanced empfiehlt, dass Sie sicherstellen, dass Ihre Verwendung des Entwicklermodus Ihren internen Kontrollrahmen und Standards entspricht, da der Entwicklermodus zwei Arten von Änderungen bewirkt: AMS Advanced Change Management für von AMS Advanced verwaltete Ressourcen und kundenverwalteter Rollenverbund für Ressourcen, die Sie als unser Kunde verwalten. Die Prozesse von AMS Advanced entsprechen zwar weiterhin unseren Erklärungen, aber die Kundenprozesse und Kontrollrahmen müssen möglicherweise aktualisiert werden.

Um den Entwicklermodus in Ihrem AMS Advanced-Konto zu implementieren

1. Vergewissern Sie sich, dass das Konto, das Sie im Entwicklermodus verwenden möchten, die unter aufgeführten Anforderungen erfüllt [Voraussetzungen für den AMS-Entwicklermodus](#).
2. Reichen Sie eine Änderungsanforderung (RFC) ein, indem Sie den Änderungstyp (CT) Management | Verwaltetes Konto | Entwicklermodus | Aktivieren (Überprüfung erforderlich) verwenden. Ein Beispiel für die Verwendung dieses CT finden Sie unter [Entwicklermodus | Aktivieren \(Überprüfung erforderlich\)](#).

Nach der Verarbeitung des CT wird die vordefinierte IAM-Rolle (AWSManagedServicesDevelopmentRole für MALZ, customer_developer_role für SALZ) im angeforderten Konto bereitgestellt.

3. Weisen Sie den Benutzern, die Zugriff auf den Entwicklermodus benötigen, mithilfe Ihres internen Verbundprozesses die entsprechende Rolle zu.

AMS Advanced empfiehlt, den Zugriff einzuschränken, um eine ungewollte oder nicht genehmigte Bereitstellung oder Änderung von Ressourcen zu verhindern.

Berechtigungen für den AMS Advanced-Entwicklermodus

Die vordefinierte Rolle (AWSManagedServicesDevelopmentRole für MALZ, customer_developer_role für SALZ) gewährt die Berechtigung zur Erstellung von Anwendungsinfrastrukturressourcen innerhalb der AMS Advanced VPC, einschließlich IAM-Rollen, und schränkt gleichzeitig den Zugriff auf Shared Service-Komponenten ein, die von AMS Advanced betrieben werden (z. B. Management-Hosts, Domain-Controller, Trend Micro EPS, Bastions und nicht unterstützte AWS-Services). Die Rolle schränkt auch den Zugriff auf Folgendes ein AWS-Services: Amazon- GuardDuty, AWS Organizations AWS Directory Service APIs, und AMS Advanced-Protokolle.

Mit der Rolle können Sie zwar zusätzliche IAM-Rollen erstellen, aber die gleichen Berechtigungsgrenzen, die im Zugriff im Entwicklermodus enthalten sind, gelten auch für alle IAM-Rollen, die von der erstellt wurden. `AWSManagedServicesDevelopmentRole`

Sicherheit und Compliance im Entwicklermodus

Für Sicherheit und Compliance sind AMS Advanced und Sie als Kunde gemeinsam verantwortlich. Im erweiterten Entwicklermodus von AMS wird Ihnen die gemeinsame Verantwortung für Ressourcen übertragen, die außerhalb des Change-Management-Prozesses oder im Rahmen des Change-Managements bereitgestellt, aber mit den Berechtigungen im Entwicklermodus aktualisiert wurden. Weitere Informationen zur gemeinsamen Verantwortung finden Sie unter [AWS Managed Services](#).

Vorsichtsmaßnahmen:

- DevMode ermöglicht es Ihnen und Ihrem autorisierten Team, die deny-by-default Prinzipien zu umgehen, die den Kern der AMS-Sicherheit bilden. Die Vorteile, Self-Service und weniger Wartezeit auf AMS, müssen gegen die Nachteile abgewogen werden. Jeder kann unerwartete und zerstörerische Aktionen durchführen, ohne das Wissen seines Sicherheitsteams zu haben. Automatisierte Änderungstypen zur Aktivierung des Dev-Modus und des Direct Change-Modus sind verfügbar, und jede autorisierte Person in Ihrer Organisation kann diese Änderungen ausführen CTs und diese Modi aktivieren.
- Sie sind dafür verantwortlich, die Berechtigungen für die CT-Ausführung von Ihrer Benutzerbasis aus zu verwalten.
- AMS verwaltet keine CT-Ausführungsberechtigungen

Empfehlungen:

- Schützen
 - Kunden können den Zugriff auf dieses CT mithilfe von Zugriffsberechtigungen verhindern. Weitere Informationen finden Sie unter [Einschränken von Berechtigungen mithilfe von IAM-Rollenrichtlinienerklärungen](#)
 - Verhindern Sie den Zugriff auf dieses CT, indem Sie einen Proxy, z. B. ein ITSM-System, implementieren
 - Verwenden Sie Richtlinien zur Servicesteuerung (SCPs), die bei Bedarf Richtlinien und Verhaltensweisen verhindern, siehe [AMS Preventative and Detective Controls Library](#)
- Erkennen

- Überwachen Sie Ihre RFCs darauf, dass diese ausgeführt werden CTs (Entwicklermodus aktivieren ct-1opjmhuddw194 und Direktänderungsmodus, Aktivieren Sie ct-3rd4781c2nnhp) und reagieren Sie entsprechend
- Prüfen Sie, überprüfen Sie Ihre Konten auf das Vorhandensein der and/or IAM-Ressourcen, um die Konten zu identifizieren, für die der Entwicklermodus oder der Direktänderungsmodus bereitgestellt wurden
- Reagieren Sie
 - Entfernen Sie nach Bedarf Konten im Entwicklermodus

Sicherheit im Entwicklermodus

AMS Advanced bietet zusätzlichen Mehrwert mit einer präskriptiven landing zone, einem Change-Management-System und einer Zugriffsverwaltung. Bei Verwendung des Entwicklermodus wird der Sicherheitswert von AMS Advanced beibehalten, indem dieselbe Kontokonfiguration wie die standardmäßigen AMS Advanced-Konten verwendet wird, mit der das standardmäßige, sicherheitsverstärkte AMS Advanced-Netzwerk eingerichtet wird. Das Netzwerk ist durch die in der Rolle festgelegten Berechtigungsgrenzen geschützt (AWSManagedServicesDevelopmentRole für MALZ, customer_developer_role für SALZ). Dadurch wird verhindert, dass der Benutzer den bei der Einrichtung des Kontos festgelegten Parameterschutz aufhebt.

Benutzer mit dieser Rolle können beispielsweise auf Amazon Route 53 zugreifen, aber die interne Hosting-Zone von AMS Advanced ist eingeschränkt. Dieselben Berechtigungsgrenzen werden für eine IAM-Rolle durchgesetzt AWSManagedServicesDevelopmentRole, die von der erstellt wurde. Dadurch wird verhindert, AWSManagedServicesDevelopmentRole dass der Benutzer den Parameterschutz aufhebt, der beim Onboarding des Kontos in AMS Advanced eingerichtet wurde.

Einhaltung von Vorschriften im Entwicklermodus

Der Entwicklermodus ist sowohl mit Produktionsworkloads als auch mit Workloads außerhalb der Produktion kompatibel. Es liegt in Ihrer Verantwortung, die Einhaltung aller Compliance-Standards (z. B. PHI, HIPAA, PCI) sicherzustellen und sicherzustellen, dass die Verwendung des Entwicklermodus Ihren internen Kontrollrahmen und Standards entspricht.

Änderungsmanagement im Entwicklermodus

Change Management ist der Prozess, den der AMS Advanced-Service verwendet, um Änderungsanforderungen zu implementieren. Eine Änderungsanforderung (RFC) ist eine Anfrage, die

entweder von Ihnen oder AMS Advanced über die AMS Advanced-Schnittstelle erstellt wird, um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen. Sie enthält eine Change Type (CT) -ID für einen bestimmten Vorgang. Weitere Informationen finden Sie unter [Verwaltungsmodi ändern](#).

Die Änderungsverwaltung wird bei AMS Advanced-Konten, für die Berechtigungen im Entwicklermodus gewährt werden, nicht durchgesetzt. Benutzer, denen die Berechtigung für den Entwicklermodus mit der IAM-Rolle (AWSManagedServicesDevelopmentRole für MALZ, `customer_developer_role` für SALZ) erteilt wurde, können den systemeigenen AWS API-Zugriff verwenden, um Ressourcen in ihren AMS Advanced-Konten bereitzustellen und zu ändern. Benutzer, die nicht über die entsprechende Rolle in diesen Konten verfügen, müssen den AMS-Advanced-Change-Management-Prozess verwenden, um Änderungen vorzunehmen.

Important

Ressourcen, die Sie im Entwicklermodus erstellen, können nur dann von AMS Advanced verwaltet werden, wenn sie mithilfe von AMS Advanced-Change-Management-Prozessen erstellt wurden. An AMS Advanced eingereichte Änderungsanträge für Ressourcen, die außerhalb des AMS Advanced-Change-Management-Prozesses erstellt wurden, werden von AMS Advanced abgelehnt, da sie von Ihnen bearbeitet werden müssen.

API-Einschränkungen für Self-Service-Bereitstellungsdienste

Alle selbst bereitgestellten AMS Advanced-Dienste werden im Entwicklermodus unterstützt. Der Zugriff auf selbst bereitgestellte Dienste unterliegt den Einschränkungen, die in den jeweiligen Abschnitten des Benutzerhandbuchs beschrieben sind. Wenn ein selbst bereitgestellter Dienst mit Ihrer Rolle im Entwicklermodus nicht verfügbar ist, können Sie über den Änderungstyp Entwicklermodus eine aktualisierte Rolle anfordern.

Die folgenden Dienste bieten keinen vollen Zugriff auf den Dienst: APIs

Self-Provisioned Services: Eingeschränkt im Entwicklermodus

Service	Hinweise
Amazon API Gateway	Alle APIs Gateway-Aufrufe sind zulässig, außer SetWebACL

Service	Hinweise
Application Auto Scaling	Es können nur skalierbare Ziele registriert oder deregistriert und eine Skalierungsrichtlinie hinzugefügt oder gelöscht werden.
AWS CloudFormation	Es kann nicht auf CloudFormation Stacks zugegriffen oder diese geändert werden, denen ein Name als Präfix vorangestellt ist. mc -
AWS CloudTrail	Es kann nicht auf CloudTrail Ressourcen zugegriffen oder diese geändert werden, denen ein Name als Präfix vorangestellt ist. ams - and/ or mc -
Amazon Cognito (Benutzerpools)	Softwaretoken können nicht verknüpft werden. Benutzerpools, Benutzerimportaufträge, Ressourcenserver oder Identitätsanbieter können nicht erstellt werden.

Service	Hinweise
AWS Directory Service	Nur die folgenden Directory Service Aktionen sind für die Connect WorkSpaces Dienste erforderlich. Alle anderen Verzeichnisdienst-Aktionen werden durch die Berechtigungsgrenzrichtlinie für den Entwicklermodus verweigert: • <code>ds:AuthorizeApplication</code> • <code>ds:CreateAlias</code> • <code>ds:CreateIdentityPoolDirectory</code> • <code>ds>DeleteDirectory</code> • <code>ds:DescribeDirectories</code> • <code>ds:GetAuthorizedApplicationDetails</code> • <code>ds:ListAuthorizedApplications</code> • <code>ds:UnauthorizeApplication</code> Bei landing zone Zone-Konten mit einem Konto verweigert die Boundary-Policy ausdrücklich den Zugriff auf das verwaltete AMS Advanced-Verzeichnis, das von AMS Advanced zur Aufrechterhaltung des Zugriffs auf Konten mit aktiviertem Dev-Modus verwendet wird.
Amazon Elastic Compute Cloud	Es kann nicht auf Amazon EC2 APIs zugegriffen werden, die die Zeichenfolge: <code>DhcpOptions</code> Gateway,Subnet,VPC, und enthaltenVPN. Es kann nicht auf EC2 Amazon-Ressourcen zugegriffen oder diese geändert werden, denen ein Tag mit dem PräfixAMS,, mcManagemen tHostASG , and/or sentinel vorangestellt ist.

Service	Hinweise
Amazon EC2 (Berichte)	Es wird nur Lesezugriff gewährt (kann nicht geändert werden). Hinweis: Amazon EC2 Reports zieht um. Der Menüpunkt Berichte wird aus dem Navigationsmenü der EC2 Amazon-Konsole entfernt. Um Ihre EC2 Amazon-Nutzungsberichte nach der Entfernung einzusehen, verwenden Sie die AWS Billing und Cost Management-Konsole.
AWS Identity and Access Management (IAM)	Bestehende Berechtigungsgrenzen können nicht gelöscht oder die Kennwortrichtlinien für IAM-Benutzer geändert werden. IAM-Ressourcen können nur erstellt oder geändert werden, wenn Sie die richtige IAM-Rolle (AWSManagedServicesDevelopmentRole für MALZ, customer_developer_role für SALZ) verwenden. IAM-Ressourcen mit dem Prefix:,, können nicht geändert werden. <code>ams mc customer_deny_policy</code> and/or <code>sentinel</code> Beim Erstellen einer neuen IAM-Ressource (Rolle, Benutzer oder Gruppe) muss die Berechtigungsgrenze (MALZ:AWSManagedServicesDevelopmentRolePermissionsBoundary , SALZ:ams-app-infra-permissions-boundary) angehängt werden.
AWS Key Management Service (AWS KMS)	Auf von AMS Advanced verwaltete KMS-Schlüssel kann nicht zugegriffen oder diese geändert werden.

Service	Hinweise
AWS Lambda	Es kann nicht auf AWS Lambda Funktionen zugegriffen oder diese geändert werden, denen das Präfix vorangestellt ist. AMS
CloudWatch Logs	Auf CloudWatch Protokollstreams mit dem Präfix:.,mc, awsLambda, and/or AMS kann nicht zugegriffen werden.
Amazon Relational Database Service (Amazon RDS)	Auf Amazon Relational Database Service (Amazon RDS) -Datenbanken (DBs) mit dem Präfix: kann nicht zugegriffen oder diese geändert werden. mc -
AWS -Ressourcengruppen	Kann nur auf Get API-Aktionen List und Search Resource Group zugreifen.
Amazon Route 53	Auf die von Route53 AMS Advanced verwaltet en Ressourcen kann nicht zugegriffen oder diese geändert werden.
Amazon S3	Es kann nicht auf Amazon S3 S3-Buckets zugegriffen werden, denen ein Name mit dem Präfix:ams - *, amsms - a, oder vorangestellt ist. mc - a
AWS Security Token Service	Die einzige zulässige Sicherheitstoken-Dienst-API ist. DecodeAuthorizationMessage
Amazon SNS	Es kann nicht auf SNS-Themen zugegriff en werden, denen ein Name mit dem Präfix: AMS-Energon-Topic , oder vorangestellt ist. MMS-Topic

Service	Hinweise
AWS Systems Manager Manager (SSM)	SSM-Parameter mit <code>ams</code> dem Präfix, oder können nicht geändert werden. <code>mc svc</code> Die SSM-API <code>SendCommand</code> kann nicht für EC2 Amazon-Instances verwendet werden, denen ein Tag mit <code>ams</code> dem Präfix oder vorangestellt ist. <code>mc</code>
AWS Taggen	Sie haben nur Zugriff auf AWS Tagging-API-Aktionen, denen das Präfix vorangestellt ist. <code>Get</code>
AWS Lake Formation	Die folgenden AWS Lake Formation API-Aktionen werden verweigert: • <code>lakeformation:DescribeResource</code> • <code>lakeformation:GetDataLakeSettings</code> • <code>lakeformation:DeregisterResource</code> • <code>lakeformation:RegisterResource</code> • <code>lakeformation:UpdateResource</code> • <code>lakeformation:PutDataLakeSettings</code>
Amazon Elastic Inference	Sie können nur die Elastic Inference API-Aktion <code>elastic-inference:Connect</code> aufrufen. Diese Berechtigung ist in der Datei enthalten <code>customer_sagemaker_admin_policy</code>, die dem <code>customer_sagemaker_admin_role</code> beigefügt ist. Mit dieser Aktion erhalten Sie Zugriff auf den Elastic Inference Accelerator.

Service	Hinweise
AWS Shield	Kein Zugriff auf einen dieser Dienste APIs oder Konsolen.
Amazon Simple Workflow Service	Kein Zugriff auf diese Dienste APIs oder Konsolen.

Infrastruktur im AMS-Entwicklermodus bereitstellen

Benutzer, die nicht über die IAM-Rolle im Entwicklermodus verfügen, müssen in `KontenAWSManagedServicesDevelopmentRole`, in denen der Entwicklermodus aktiviert ist, den AMS-Advanced-Change-Management-Prozess befolgen, der AMS Advanced nutzt. AMIs Benutzer mit der richtigen Rolle (`MALZ:AWSManagedServicesDevelopmentRole`, `SALZ:customer_developer_role`) können das AMS Advanced Change Management System und AMS Advanced verwenden, sind AMIs aber nicht dazu verpflichtet.

Note

Ein AWS AMI, das nicht über AMS Advanced Workload Ingestion verarbeitet oder in einem AMS Advanced-Konto erstellt wurde, enthält keine für AMS Advanced erforderlichen Konfigurationen.

Detective Controls im AMS-Entwicklermodus

Dieser Abschnitt wurde redigiert, da er sensible sicherheitsrelevante AMS-Informationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

Protokollierung, Überwachung und Ereignisverwaltung im AMS-Entwicklermodus

Protokollierung, Überwachung und Ereignisverwaltung sind nicht für Ressourcen verfügbar, die außerhalb des AMS Advanced Change Management-Prozesses bereitgestellt wurden, oder für

Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden.

Vorfallmanagement im AMS-Entwicklermodus

Keine Änderung der Reaktionszeiten bei Vorfällen. Für Ressourcen, die außerhalb des Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit den Berechtigungen im Entwicklermodus geändert wurden, ist die Lösung eines Vorfalls nach bestem Wissen möglich.

Note

Das AMS Service Level Agreement (SLA) gilt nicht für Ressourcen, die außerhalb des AMS-Change-Management-Systems erstellt oder aktualisiert wurden (Änderungsanforderungen oder RFCs), einschließlich des Entwicklermodus. Daher werden Ressourcen, die im Entwicklermodus aktualisiert oder erstellt wurden, automatisch auf P3 heruntergestuft, und AMS-Support ist nach bestem Bemühen möglich.

Patch-Management im AMS-Entwicklermodus

Patch-Management ist nicht für Ressourcen verfügbar, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden. Zeiten für Patches:

- Für ein wichtiges Sicherheitsupdate: Innerhalb von 10 Werktagen nach der Veröffentlichung durch den Anbieter für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden.
- Für ein wichtiges Update: Innerhalb von 2 Monaten nach der Veröffentlichung durch den Anbieter für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann über ein Konto mit Berechtigungen im Entwicklermodus geändert wurden.

Kontinuitätsmanagement im AMS-Entwicklermodus

Continuity Management ist nicht für Ressourcen verfügbar, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das

Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden.

Bei Ressourcen, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder bei Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden, kann die Initiierungszeit für die Wiederherstellung der Umgebung bis zu 12 Stunden in Anspruch nehmen.

Sicherheits- und Zugriffsmanagement im AMS-Entwicklermodus

Für den Schutz vor Schadsoftware sind Sie für Ressourcen verantwortlich, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden. Der Zugriff auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, die nicht über AMS Advanced Change Management bereitgestellt werden, kann durch Schlüsselpaare gesteuert werden, anstatt einen Verbundzugriff bereitzustellen.

Self-Service-Bereitstellungsmodus in AMS

Der Self-Service Provisioning (SSP) -Modus von AWS Managed Services (AMS) bietet vollen Zugriff auf native AWS Service- und API-Funktionen in AMS-verwalteten Konten. Sie greifen über standardisierte, auf bestimmte Bereiche zugeschnittene Rollen auf Services zu. AWS Identity and Access Management AMS bietet Serviceanfragen und das Management von Vorfällen. Warnmeldungen, Überwachung, Protokollierung, Patches, Backups und Änderungsmanagement liegen in Ihrer Verantwortung. In vielen Fällen werden Self-Service Provisioning Services (SSPS) selbst oder serverlos verwaltet und erfordern keine Verwaltung bestimmter betrieblicher Aufgaben wie das Patchen. Sie profitieren von der Nutzung dieser Services innerhalb der durch AMS-Guardrails definierten Umgebungsgrenzen. Alle IAM-Änderungen (einschließlich serviceverknüpfter Rollen, Servicerollen, kontoübergreifender Rollen oder Richtlinienaktualisierungen) müssen von AMS Operations genehmigt werden, um die grundlegende Sicherheit der Plattform aufrechtzuerhalten. Sie können CloudFormation Vorlagen verwenden, um die Bereitstellung dieser Dienste zu automatisieren. Dies wird jedoch nicht für alle SSP-Dienste unterstützt.

Important

Verwenden Sie den SSP-Modus in Ihren AWS Managed Services (AMS) -Konten, um auf AWS Services zuzugreifen und diese zu nutzen, mit den angegebenen Einschränkungen.

Es gibt einige AWS-Services, die Sie ohne AMS-Verwaltung in Ihrem AMS-Konto verwenden können. Die Dienste im Self-Service Provisioning-Modus, kurz SSPS, werden im Abschnitt beschrieben, wie Sie sie zu Ihrem AMS-Konto hinzufügen können und FAQs für welche Dienste.

Self-Service Provisioning Services werden so angeboten, wie sie sind, und Sie sind für deren Verwaltung verantwortlich. AMS bietet keine Benachrichtigungen, Überwachungs-, Protokollierungs- oder Patching-Funktionen für die Ressourcen, die mit diesen Diensten verknüpft sind. AMS bietet IAM-Rollen, mit denen Sie den Dienst in Ihrem AMS-Konto sicher nutzen können. AMS gelten SLAs nicht.

Für Ressourcen, die Sie über Self-Service bereitstellen, bietet AMS Vorfallmanagement, detektive Kontrollen und Leitplanken, Berichterstattung, zugewiesene Ressourcen (Cloud Service Delivery Manager und Cloud Architect), Sicherheit und Zugriff sowie technischen Support bei Serviceanfragen. Darüber hinaus übernehmen Sie gegebenenfalls die Verantwortung für das Kontinuitätsmanagement, das Patch-Management, die Infrastrukturüberwachung und das Änderungsmanagement für Ressourcen, die außerhalb des AMS-Change-Management-Systems bereitgestellt oder konfiguriert wurden.

Erste Schritte mit dem SSP-Modus in AMS

Self-Service Provisioning ist einer der AMS-Modi für die Multi-Account-Landing landing zone (MALZ), die Sie verwenden können. Weitere Informationen finden Sie unter [Übersicht der Modi](#).

Um Funktionen zur Self-Service-Bereitstellung bereitzustellen, hat AMS erweiterte IAM-Rollen mit Rechtegrenzen eingerichtet, um unbeabsichtigte Änderungen durch direkten Zugriff zu verhindern. AWS-Service Die Rollen verhindern nicht alle Änderungen, und Sie müssen Ihre internen Kontrollen und Compliance-Richtlinien einhalten und sicherstellen, dass alle AWS-Services verwendeten Rollen die erforderlichen Zertifizierungen erfüllen. Dies ist der Self-Service-Bereitstellungsmodus. [Einzelheiten zu den AWS Compliance-Anforderungen finden Sie unter AWS Compliance](#).

Um Ihrem Landingzone-Anwendungskonto mit mehreren Konten einen Self-Service Provisioning Service hinzuzufügen, verwenden Sie den Befehl Verwaltung | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (CT), entweder den für die Prüfung erforderlichen CT oder den automatisierten CT, wie für den Service angegeben.

Note

Um zu beantragen, dass AMS einen zusätzlichen Self-Service-Bereitstellungsservice anbietet, reichen Sie eine Serviceanfrage ein.

Verwenden Sie AMS SSP, um Amazon API Gateway in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon API Gateway zuzugreifen. [Amazon API Gateway](#) ist ein vollständig verwalteter Service, der Entwicklern die Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung APIs in jeder Größenordnung erleichtert. Mithilfe von können AWS-Managementkonsole Sie REST erstellen WebSocket APIs , die als Eingangstür für Anwendungen dienen, um auf Daten, Geschäftslogik oder Funktionen aus Ihren Back-End-Services zuzugreifen, z. B. Workloads, die auf Amazon Elastic Compute Cloud ([Amazon EC2](#)) ausgeführt werden, Code, der auf [AWS Lambda](#) beliebigen Webanwendungen ausgeführt wird, oder Echtzeitkommunikationsanwendungen.

API Gateway übernimmt alle Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind, einschließlich Verkehrsmanagement, Autorisierung und Zugriffskontrolle, Überwachung und API-Versionsverwaltung. Für API Gateway fallen keine Mindestgebühren oder Startkosten an. Sie zahlen nur für die API-Aufrufe, die Sie erhalten, und die Menge der übertragenen Daten. Mit dem gestaffelten Preismodell von API Gateway können Sie Ihre Kosten senken, wenn Ihre API-Nutzung steigt. Weitere Informationen finden Sie unter [Amazon API Gateway](#).

Häufig gestellte Fragen: API Gateway in AMS

F: Wie beantrage ich Zugriff auf Amazon API Gateway in meinem AMS-Konto?

Fordern Sie Zugriff auf API Gateway an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem customer_apigateway_author_role customer_apigateway_cloudwatch_role Konto die folgenden IAM-Rollen zur Verfügung: und. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon API Gateway in meinem AMS-Konto?

- Die API-Gateway-Konfiguration ist auf Ressourcen ohne AMS- MC- Präfixe beschränkt, um Änderungen an der AMS-Infrastruktur zu verhindern.
- CREATEDie Rechte für VPCLink sind deaktiviert, um die unregulierte Erstellung von Elastic Load Balancers zu verhindern. Falls VPCLinks erforderlich, finden Sie weitere Informationen unter [Application Load Balancer | Erstellen](#).

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon API Gateway in meinem AMS-Konto?

Dies hängt von der Art des API Gateway ab, das Sie bereitstellen möchten. Es kann sich um einen eigenständigen Dienst handeln, er kann aber auch Zugriff auf bestehende Dienste (z. B. Network Load Balancer) anfordern.

Verwenden Sie AMS SSP, um Alexa for Business in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen von Alexa for Business zuzugreifen. Alexa for Business ist ein Dienst, der es Ihrem Unternehmen und Ihren Mitarbeitern ermöglicht, Alexa zu verwenden, um mehr Arbeit zu erledigen. Mit Alexa for Business können Sie Alexa als intelligenten Assistenten verwenden, um in Besprechungsräumen, an Ihrem Schreibtisch und sogar mit den Alexa-Geräten, die Sie bereits zu Hause oder unterwegs verwenden, produktiver zu sein. IT- und Facility-Manager können Alexa for Business verwenden, um die Auslastung der vorhandenen Besprechungsräume an ihrem Arbeitsplatz zu messen und zu erhöhen.

Weitere Informationen finden Sie unter [Alexa for Business](#).

Häufig gestellte Fragen zu Alexa for Business in AWS Managed Services

F: Wie beantrage ich Zugriff auf Alexa for Business in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_alex_console_role` Konto die folgende IAM-Rolle zur Verfügung: `customer_alex_device_setup_user` wird auch für das von Alexa for Business bereitgestellte Geräteeinrichtungstool erstellt. Dieses Geräteeinrichtungstool kann dann zur Einrichtung Ihrer Geräte verwendet werden. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Mit dem Alexa for Business-Gateway können Sie Alexa for Business mit Ihren Endpunkten der Cisco Webex- und Poly Group-Serie verbinden, um Besprechungen mit Ihrer Stimme zu steuern. Die Gateway-Software läuft auf Ihrer lokalen Hardware und leitet Konferenzanweisungen von Alexa for Business sicher an Ihren Cisco-Endpunkt weiter. Das Gateway benötigt zwei Paare von AWS Anmeldeinformationen, um mit Alexa for Business zu kommunizieren. Wir bieten zwei IAM-Benutzer mit beschränktem Zugriff: `customer_alex_gateway_installer_user` und

`customer_alexagateway_execution_user` für Ihre Alexa for Business-Gateways einen für die Installation des Gateways und einen für den Betrieb des Gateways. Diese können angefordert werden, indem Sie einen RFC mit dem Änderungstyp `Deployment | Advanced Stack components | Identity and Access Management (IAM) | Entität oder Richtlinie` erstellen (Überprüfung erforderlich) einreichen (ct-3d8pd8mdd9jn1r).

 Note

Um Nutzungsberichte zu generieren und an Amazon S3 zu senden, geben Sie den Amazon S3 S3-Bucket-Namen im RFC für den selbst bereitgestellten Service an.

F: Welche Einschränkungen gelten für die Nutzung von Alexa for Business in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Alexa for Business ist mit der selbst bereitgestellten Servicerolle `Alexa for Business` verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Alexa for Business in meinem AMS-Konto?

- Wenn Sie WPA2 Enterprise Wi-Fi verwenden möchten, um Ihre gemeinsam genutzten Geräte einzurichten, geben Sie diesen Netzwerksicherheitstyp im Geräte-Setup-Tool an, wofür ein erforderlich AWS Private Certificate Authority ist.
- AMS erstellt nur geheime Schlüssel, die mit dem Namespace „A4B“ beginnen. Dies ist nur auf diesen Namespace beschränkt.

F: Welche Funktionen von Alexa for Business sind separat erforderlich RFCs?

Um ein Alexa Voice Service (AVS) -Gerät bei Alexa for Business zu registrieren, gewähren Sie Zugriff auf den integrierten Gerätehersteller von Alexa. Dazu muss in der Alexa for Business Business-Konsole eine IAM-Rolle erstellt werden, die mit dem Änderungstyp `Management | Other | Other` bereitgestellt werden kann. Auf diese Weise kann der AVS-Gerätehersteller Geräte in Ihrem Namen bei Alexa for Business registrieren und verwalten.

Verwenden Sie AMS SSP, um Amazon AppStream 2.0 in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen von Amazon AppStream AppStream 2.0 (2.0) zuzugreifen.

AppStream 2.0 ermöglicht es Ihnen, Ihre Desktop-Anwendungen zu verschieben AWS, ohne sie neu schreiben zu müssen. Sie können Ihre Anwendungen auf AppStream Version 2.0 installieren, Startkonfigurationen festlegen und Ihre Anwendungen Benutzern zur Verfügung stellen. AppStream 2.0 bietet eine große Auswahl an Optionen für virtuelle Maschinen, sodass Sie den Instanztyp auswählen können, der Ihren Anwendungsanforderungen am besten entspricht, und die Parameter für die automatische Skalierung so einstellen können, dass Sie die Anforderungen Ihrer Endbenutzer problemlos erfüllen können. AppStream 2.0 ermöglicht es Ihnen, Anwendungen in Ihrem eigenen Netzwerk zu starten, was bedeutet, dass Ihre Anwendungen mit Ihren vorhandenen AWS Ressourcen interagieren können.

Mit Amazon AppStream 2.0 können Sie Ihre Anwendungen mithilfe des Image Builders schnell und einfach installieren, testen und aktualisieren. Jede Anwendung, die auf Microsoft Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019 ausgeführt wird, wird unterstützt, und Sie müssen keine Änderungen vornehmen. Wenn Ihre Tests abgeschlossen sind, können Sie Konfigurationen für den Anwendungsstart und Standardbenutzereinstellungen festlegen und Ihr Image veröffentlichen, damit Benutzer darauf zugreifen können.

Weitere Informationen finden Sie unter [AppStream 2.0](#).

AppStream 2.0 in AWS Managed Services — Häufig gestellte Fragen

F: Wie beantrage ich Zugriff auf AppStream 2.0 in meinem AMS-Konto?

Beantragen Sie Zugriff auf AppStream 2.0, indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt `customer_appstream_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:

A `customer_appstream_stream_role` wird auch zum Streamen von Anwendungen eingesetzt, bei denen Benutzer mit ihren Active Directory-Anmeldeinformationen authentifiziert werden müssen.

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von AppStream 2.0 in meinem AMS-Konto?

- Die folgenden Funktionen müssen vom AMS-Supportteam konfiguriert werden und erfordern spezielle Funktionen RFCs. Anweisungen zur Anforderung zusätzlicher Funktionen finden Sie in Abschnitt 4.
- Erstellen und Streamen von Schnittstellen-VPC-Endpunkten.

- Support für Amazon S3 S3-Endpunkte für Basisordner und Persistenz von Anwendungseinstellungen in einem privaten Netzwerk.
- Erstellung und Auswahl der IAM-Rolle, die auf allen Fleet-Streaming-Instances verfügbar sein wird.
- Beitritt zu AppStream 2.0-Flotten und Image Builder-Microsoft-Active-Directory-Domänen
- Erstellen von benutzerdefinierten AppStream 2.0-Nutzungsberichten.
- Benutzerdefiniertes Branding wird derzeit nicht unterstützt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von AppStream 2.0 in meinem AMS-Konto?

Geben Sie bei der Übermittlung des RFC an Onboard AppStream 2.0 den Namen des Amazon S3 S3-Buckets an, der für den AppStream 2.0-Nutzungsbericht verwendet werden soll. Der Bucket-Name wird zu dem hinzugefügt `customer-appstream-usagereports-policy`, der beim Onboarding von AppStream 2.0 erstellt wurde.

F: Für welche AppStream 2.0-Funktionalität ist eine separate Version erforderlich? RFCs

- Um einen VPC-Schnittstellen-Endpunkt für AppStream 2.0 auszuwählen, reichen Sie einen RFC vom Typ Management | Other | Other | Update ein, um einen VPC-Endpunkt in Ihrem Konto zu erstellen. Schritte zum Erstellen benutzerdefinierter Endpoints für AppStream 2.0 finden Sie unter [Creating and Streaming from Interface VPC Endpoints](#) im AppStream 2.0-Benutzerhandbuch.
- Die Support von Amazon S3 S3-Endpunkten für Basisordner und die Persistenz von Anwendungseinstellungen in einem privaten Netzwerk kann konfiguriert werden, indem Amazon S3 S3-VPC-Endpunkte mit einem RFC vom Typ Management | Other | Other | Create change type angefordert werden. Der RFC muss den Amazon S3 S3-Ziel-Bucket, der den Inhalt des Home-Ordners hostet, bzw. die Amazon S3 S3-Buckets für Anwendungseinstellungen enthalten. Dieser RFC stellt AppStream 2.0 die Berechtigungen bereit, die für den Zugriff auf Amazon S3 S3-VPC-Endpunkte erforderlich sind. Schritte zum Erstellen benutzerdefinierter Endpunkte für Streams finden Sie unter [Using Amazon S3 VPC Endpoints for Home Folders and Application Settings Persistence im AppStream 2.0-Benutzerhandbuch](#).
- Um eine IAM-Rolle zu erstellen und auszuwählen, die auf allen Fleet-Streaming-Instances verfügbar sein wird, reichen Sie einen RFC vom Typ Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) (ct-3dpg8mdd9jn1r) ein und fordern Sie die IAM-Rolle mit der erforderlichen Richtlinie an. Der Name der IAM-Rolle sollte immer mit dem Präfix „customer_appstream“ beginnen.

- Amazon AppStream 2.0-Flotten und Image Builder können mit Domains in Microsoft Active Directory verknüpft werden, indem ein RFC vom Typ Management | Other | Other | Update für die Erstellung eines Dienstkontos in Active Directory (AD) eingereicht wird. Die Mindestberechtigungen, die für den Beitritt zu Microsoft Active Directory erforderlich sind, sind in der AppStream 2.0-Dokumentation unter [Gewähren von Berechtigungen zum Erstellen und Verwalten von Active Directory-Computerobjekten](#) definiert.
- Um benutzerdefinierte AppStream 2.0-Nutzungsberichte zu erstellen, reichen Sie einen RFC für Management | Other | Other | Create Change Type RFC ein und fordern Sie Folgendes an:
 - "AppStreamUsageReports" Erstellung eines CFN-Stacks
 - „customer_appstream_usagereports_role“ muss im Konto bereitgestellt werden
 - Geben Sie außerdem die folgenden Details an:
 - Geben Sie den CRON-Ausdruck an, um die Ausführung des Crawlers zu planen. Standardmäßig ist es jeden Tag 23:00 UTC.
 - Amazon S3 S3-Bucket-ARN, der für Athena-Abfrageergebnisse verwendet werden soll. Dieser Bucket sollte das Präfix haben: `aws-athena-query-results`
 - Amazon S3 S3-Bucket ARN für AppStream 2.0-Nutzungsberichte, Protokolle.

Nachdem die Rolle bereitgestellt wurde, integrieren Sie die Rolle in Ihre Verbundlösung und melden Sie sich an. Greifen Sie dann auf AWS GlueAWS Glue Athena zu, um mithilfe der Nutzungsbericht-Rolle benutzerdefinierte Berichte zu generieren. Einzelheiten zur Verwendung von AppStream 2.0-Nutzungsberichten finden Sie in der 2.0-Dokumentation unter [Benutzerdefinierte Berichte erstellen und AppStream 2.0-Nutzungsdaten analysieren](#). AppStream

Verwenden Sie AMS SSP, um Amazon Athena in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Athena (Athena) zuzugreifen. Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten in Amazon S3 mithilfe von Standard-SQL analysieren können. Athena ist Serverless, weshalb auch keine Infrastruktur eingerichtet oder verwaltet werden muss – und Sie zahlen nur für tatsächlich ausgeführte Abfragen. Sie verweisen auf Ihre Daten in Amazon S3, definieren das Schema und beginnen mit der Abfrage mithilfe von Standard-SQL. Die meisten Ergebnisse werden innerhalb von Sekunden geliefert. Mit Athena sind keine komplexen extract-transform-load (ETL-) Jobs erforderlich, um Ihre Daten für die Analyse vorzubereiten. Dies

macht es für jeden mit SQL-Kenntnissen einfach, große Datensätze schnell zu analysieren. Weitere Informationen finden Sie unter [Amazon Athena](#).

Häufig gestellte Fragen: Athena in AMS

F: Wie beantrage ich Zugriff auf Amazon Athena in meinem AMS-Konto?

Beantragen Sie Zugriff auf Athena, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_athena_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Athena in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Athena ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Athena in meinem AMS-Konto?

Athena ist stark vom AWS Glue Dienst abhängig, da er die mit catalog/metastore AWS Glue erstellten Daten verwendet. Daher sind AWS Glue Berechtigungen im erfolgreichen Athena RFC enthalten.

Die Rolle `customer_athena_console_role` ist Voraussetzung für einen Amazon S3 S3-Bucket. Verwenden Sie das automatisierte CT `ct-1a68ck03fn98r` (Deployment | Advanced Stack Components | S3 storage | Create), um einen neuen Bucket zu erstellen. Wenn Sie dieses automatisierte CT verwenden, um einen S3-Bucket für Athena zu erstellen, muss der Bucket-Name mit einem Präfix `athena-query-results-*` beginnen.

Verwenden Sie AMS SSP, um Amazon Bedrock in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Bedrock zuzugreifen. Amazon Bedrock ist ein vollständig verwalteter Service, der leistungsstarke Basismodelle (FMs) von führenden KI-Startups bereitstellt und AWS Ihnen über eine einheitliche API zur Verfügung stellt. Sie können aus einer Vielzahl von Basismodellen wählen, um das Modell zu finden, das für Ihren Anwendungsfall am besten geeignet ist. Amazon Bedrock bietet außerdem eine breite Palette von Funktionen zur Entwicklung generativer KI-Anwendungen mit Sicherheits- und Datenschutzfunktionen und

verantwortungsvoller KI. Mit Amazon Bedrock können Sie auf einfache Weise mit den wichtigsten Basismodellen für Ihre Anwendungsfälle experimentieren und diese evaluieren, sie mithilfe von Techniken wie Feinabstimmung und Retrieval Augmented Generation (RAG) privat an Ihre Daten anpassen und Agenten erstellen, die Aufgaben mithilfe Ihrer Unternehmenssysteme und Datenquellen ausführen.

Mit der serverlosen Erfahrung von Amazon Bedrock können Sie schnell loslegen, Foundation-Modelle privat mit Ihren eigenen Daten anpassen und sie mithilfe von AWS-Tools einfach und sicher in Ihre Anwendungen integrieren und bereitstellen, ohne eine Infrastruktur verwalten zu müssen. Weitere Informationen finden Sie unter [Amazon Bedrock](#).

Häufig gestellte Fragen: Amazon Bedrock in AMS

F: Wie beantrage ich Zugriff auf Amazon Bedrock in meinem AMS-Konto?

Um Zugriff auf Amazon Bedrock zu beantragen, reichen Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (review erforderlich) (ct-3qe6io8t6jtny) ein. Dieser RFC stellt `customer_bedrock_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Bedrock in meinem AMS-Konto?

- Amazon Bedrock Knowledge Bases werden standardmäßig nicht als Teil der SSPS-Rolle unterstützt, da sie von Amazon OpenSearch Service Serverless abhängig sind, das derzeit nicht von AMS unterstützt wird.
- Bedrock Studio wird nicht unterstützt, da es von nicht unterstützten Diensten wie Amazon abhängig ist. DataZone

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Bedrock in meinem AMS-Konto?

- Modellabonnements von Drittanbietern, für die AWS Marketplace Berechtigungen erforderlich sind, müssen über die Standardrolle (`AWSManagedServicesAdminRole` auf MALZ und `Customer_ReadOnly_Role` auf SALZ) ausgeführt werden. Das liegt daran, dass die Standardrolle AWS Marketplace Berechtigungen beinhaltet.
- Wenn Datenverschlüsselung verwendet wird, müssen Sie den AWS KMS Schlüssel-ARN angeben, wenn Sie die Erstellung der Konsolenrolle anfordern. Außerdem muss der Amazon S3 S3-Bucket „Bedrock“ im Namen haben.

Verwenden Sie AMS SSP, um Amazon CloudSearch in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf CloudSearch Amazon-Funktionen zuzugreifen. Amazon CloudSearch ist ein verwalteter Service in der AWS Cloud, mit dem Sie kostengünstig eine Suchlösung für Ihre Website oder Anwendung einrichten, verwalten und skalieren können. Amazon CloudSearch unterstützt 34 Sprachen und beliebte Suchfunktionen wie Hervorhebung, automatische Vervollständigung und Geodatenuche. Weitere Informationen finden Sie auf [Amazon CloudSearch](#).

Note

AWS hat mit Wirkung zum 25. Juli 2024 den Zugang für Neukunden zu Amazon CloudSearch geschlossen. CloudSearch Amazon-Bestandskunden können den Service weiterhin wie gewohnt nutzen. AWS investiert weiterhin in Sicherheits-, Verfügbarkeits- und Leistungsverbesserungen für Amazon CloudSearch, aber wir planen nicht, neue Funktionen einzuführen.

Um mehr über die Unterschiede zwischen Amazon CloudSearch und Amazon OpenSearch Service zu erfahren und zu erfahren, wie Sie zu OpenSearch Service wechseln können, wenden Sie sich an Ihren Cloud-Architekten (CA). Weitere Informationen zur Umstellung auf OpenSearch Service finden Sie unter [Übergang von Amazon CloudSearch zu Amazon OpenSearch Service](#).

Häufig gestellte Fragen zu Amazon CloudSearch in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon CloudSearch in meinem AMS-Konto?

Beantragen Sie Zugriff auf Amazon, CloudSearch indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem customer_csearch_admin_role Konto customer_csearch_dev_role die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon CloudSearch in meinem AMS-Konto?

Die volle Funktionalität von Amazon CloudSearch ist in Ihrem AMS-Konto verfügbar. Alle von AMS unterstützten Datenbanklösungen werden derzeit auf Amazon unterstützt. CloudSearch Beachten

Sie, dass DynamoDB derzeit die einzige verwaltete AWS Datenbanklösung ist, die nicht indexiert werden kann.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon CloudSearch in meinem AMS-Konto?

Amazon ist CloudSearch darauf angewiesen, dass Amazon S3 mit Identitätsanbietern zusammenarbeitet, um Eingabedaten automatisch zu analysieren und die Tabellenfelder zu bestimmen. Der Zugriff auf Amazon S3 ist in diesem RFC nicht enthalten und muss separat in einer Serviceanfrage angefordert werden.

Verwenden Sie AMS SSP, um Amazon CloudWatch Synthetics in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon CloudWatch Synthetics zuzugreifen. Sie können Amazon CloudWatch Synthetics verwenden, um „Kanarien“ zur Überwachung Ihrer Endgeräte zu erstellen und APIs

Canaries sind konfigurierbare Skripte, die in Node.js oder Python geschrieben sind und nach einem Zeitplan ausgeführt werden. Sie legen Lambda-Funktionen in Ihrem Konto an, die Node.js oder Python als Framework verwenden. Canaries arbeiten über HTTP- und HTTPS-Protokolle. Canaries überprüfen die Verfügbarkeit und Latenz Ihrer Endgeräte und können Ladezeitdaten und UI-Screenshots speichern. Sie überwachen Ihre REST APIs - und Website-Inhalte und können nach unbefugten Änderungen durch Phishing, Code-Injection und Cross-Site-Scripting suchen. URLs

Canaries verfolgen dieselben Wege und führen dieselben Aktionen aus wie ein Kunde, sodass Sie Ihr Kundenerlebnis kontinuierlich überprüfen können, auch wenn Sie keinen Kundenverkehr mit Ihren Anwendungen haben. Durch den Einsatz von Canaries können Sie Probleme entdecken, bevor Ihre Kunden sie entdecken. Weitere Informationen finden Sie unter [Amazon CloudWatch: Synthetisches Monitoring verwenden](#).

Häufig gestellte Fragen zu Amazon CloudWatch Synthetics in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon CloudWatch Synthetics in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon CloudWatch Synthetics an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur Verfügung:

„customer_cw_synthetics_console_role“ und „customer_cw_synthetics_canary_lambda_role“. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle „customer_cw_synthetics_console_role“ in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon CloudWatch Synthetics in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von Amazon CloudWatch Synthetics in Ihrem AMS-Konto. Das Erstellen von Rollen für Canaries außerhalb der von AMS bereitgestellten Servicerolle 'customer_cw_synthetics_canary_lambda_role' ist verboten.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon CloudWatch Synthetics in meinem AMS-Konto?

Die Kanaren erstellen und verwenden einen standardmäßigen Amazon CloudWatch Synthetics S3-Bucket: "cw-syn-results- *-\${accountnumber}* *-\${default-region}*"

Verwenden Sie AMS SSP, um Amazon Cognito Cognito-Benutzerpools in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Cognito Cognito-Benutzerpools zuzugreifen. Amazon Cognito Cognito-Benutzerpools bieten ein sicheres Benutzerverzeichnis, das auf Hunderte von Millionen von Benutzern skaliert werden kann. Als vollständig verwalteter Service können Amazon Cognito Cognito-Benutzerpools eingerichtet werden, ohne sich Gedanken über die Einrichtung der Serverinfrastruktur machen zu müssen. Mit diesem Service können Sie einen Pool von Endbenutzern verwalten, den Sie für die Integration in Ihre internen Anwendungen verwenden können. Dieser Service bietet Ihnen eine Alternative zu einer benutzerdefinierten Datenbank oder einem Verzeichnis von Endbenutzern für Web- oder Mobilanwendungen. Gleichzeitig bieten Amazon Cognito Cognito-Benutzerpools den vollen Funktionsumfang eines Verzeichnisdienstes wie Kennwortrichtlinien, Multi-Faktor-Authentifizierung, Kennwortwiederherstellung und Selbstanmeldung bei Diensten. Es ermöglicht der Anwendung auch, den Zugriff in anderen beliebigen öffentlichen Diensten wie OpenID, Facebook, Amazon oder Google zu bündeln.

Amazon Cognito ist in zwei Hauptprodukte unterteilt. Amazon Cognito-Benutzerpools und Amazon Cognito Identity Provider. Dieser Abschnitt konzentriert sich auf Amazon Cognito Cognito-Benutzerpools, die Zugriff auf andere AWS Dienste wie Amazon S3 oder DynamoDB bieten. Mit diesem Service können Sie Amazon Cognito Cognito-Benutzerpools oder einen externen

Identitätsanbieter verwenden, um Zugriff auf AWS Dienste zu gewähren. Er ermöglicht auch den Zugriff auf AWS Dienste mithilfe eines anonymen Gastzugriffs. Aufgrund der Leistungsfähigkeit von Amazon Cognito Cognito-Benutzerpools würden sie manuell als Service case-by-case für Betriebsanleitungen verwaltet werden, um mögliche Sicherheitslücken im Konto zu vermeiden. Weitere Informationen finden Sie unter [Amazon Cognito User Pools](#).

Häufig gestellte Fragen zu Amazon Cognito Cognito-Benutzerpools in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Cognito Cognito-Benutzerpools in meinem AMS-Konto?

Die Implementierung von Amazon Cognito Cognito-Benutzerpools in AMS erfolgt in zwei Schritten:

1. Reichen Sie den Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) ein und fordern Sie die Erstellung der Amazon Cognito Cognito-Benutzerpools in Ihrem AMS-Konto an. Schließen Sie die folgenden Informationen ein:
 - AWS Region.
 - Name für den Cognito-Benutzerpool.
 - Wenn Sie anstelle des standardmäßigen internen Cognito-Mail-Service den Amazon Simple Email Service (Amazon SES) zum Senden von Nachrichten und Benachrichtigungen verwenden möchten, sollte der Kunde im Konto eine bereits validierte E-Mail-Adresse für den Amazon SES-Service angeben. Diese Adresse wird für die Felder „Von“ und „ANTWORT-TO“ der Nachricht verwendet. Sie müssen auch die Region angeben, in der Amazon SES aktiviert wurde (us-east-1, eu-west-1 oder us-west-2).
 - Wenn Sie SMS-Nachrichten für Einmalpasswörter und zur Bestätigung verwenden möchten, sollte der Kunde dies angeben.
2. Fordern Sie den Benutzerzugriff an, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung: und. `customer_cognito_admin_role` `customer_cognito_importjob_role` Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren. Mit diesen Rollen können Sie die Amazon Cognito Cognito-Benutzerpools verwalten, Ihre Benutzer und Gruppen im Pool verwalten, Importjobs für Benutzer erstellen, die Benachrichtigungen und Abonnementnachrichten ändern, Anwendungen dem Benutzerpool zuordnen, das Hinzufügen von Verbunddiensten zum Pool selbst verwalten und bereits erstellte Pools löschen.

F: Was sind die Einschränkungen bei der Verwendung von Amazon Cognito Cognito-Benutzerpools in meinem AMS-Konto?

Sie können die Amazon Cognito Cognito-Benutzerpools nicht erstellen. Diese Aktion erfordert die Erstellung von IAM-Rollen, um die von Amazon Cognito verwendeten Dienste wie Amazon SES und Amazon Simple Notification Service (Amazon SNS) nutzen zu können.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Cognito Cognito-Benutzerpools in meinem AMS-Konto?

Wenn Sie Amazon SES verwenden möchten, um Nachrichten und Benachrichtigungen per E-Mail an Ihre Benutzerpools zu senden, sollten diese den Amazon SES SES-Service bereits im Konto aktivieren und die E-Mail-Adresse, die in den Feldern „FROM“ und „REPLY-TO“ der gesendeten E-Mails verwendet werden soll, bereits validieren. Weitere Informationen zur Validierung von E-Mail-Adressen mit Amazon SES finden Sie unter [Verifizieren von E-Mail-Adressen in Amazon SES](#).

Verwenden Sie AMS SSP, um Amazon Comprehend in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Comprehend zuzugreifen. Amazon Comprehend ist ein Service zur Verarbeitung natürlicher Sprache (NLP), der maschinelles Lernen nutzt, um Erkenntnisse und Zusammenhänge im Text zu finden. Es sind keine Erfahrungen mit maschinellem Lernen erforderlich. Amazon Comprehend verwendet maschinelles Lernen, um Ihnen zu helfen, die Erkenntnisse und Zusammenhänge in Ihren unstrukturierten Daten aufzudecken. Der Service identifiziert die Sprache des Textes, extrahiert wichtige Phrasen, Orte, Personen, Marken oder Ereignisse, versteht, wie positiv oder negativ der Text ist, analysiert Text mithilfe von Tokenisierung und Wortarten und organisiert automatisch eine Sammlung von Textdateien nach Themen. Sie können auch die AutoML-Funktionen in Amazon Comprehend verwenden, um einen benutzerdefinierten Satz von Entitäten oder Textklassifizierungsmodellen zu erstellen, die speziell auf die Bedürfnisse Ihres Unternehmens zugeschnitten sind. Weitere Informationen finden Sie unter [Amazon Comprehend](#).

Häufig gestellte Fragen zu Amazon Comprehend in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Comprehend in meinem AMS-Konto?

Die Konsolen- und Datenzugriffsrollen von Amazon Comprehend können durch Einreichung von zwei AMS-Services angefordert werden: RFCs

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem customer_comprehend_console_role Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Comprehend in meinem AMS-Konto?

Die Funktion „Neue IAM-Rolle erstellen“ über die Amazon Comprehend Comprehend-Konsole ist eingeschränkt. Andernfalls ist der volle Funktionsumfang von Amazon Comprehend in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Comprehend in meinem AMS-Konto?

Amazon S3 und AWS Key Management Service (AWS KMS) sind für die Verwendung von Amazon Comprehend erforderlich, wenn Amazon S3 S3-Buckets mit Schlüsseln verschlüsselt sind. AWS KMS

Verwenden Sie AMS SSP, um Amazon Connect in Ihrem AMS-Konto bereitzustellen

Note

Nach reiflicher Überlegung haben wir beschlossen, den Support für Amazon Connect Voice ID mit Wirkung zum 20. Mai 2026 einzustellen. Amazon Connect Voice ID akzeptiert ab dem 20. Mai 2025 keine Neukunden mehr. Als Bestandskunde mit einem Konto, das vor dem 20. Mai 2025 für den Service registriert wurde, können Sie die Amazon Connect Voice ID-Funktionen weiterhin nutzen. Nach dem 20. Mai 2026 können Sie Amazon Connect Voice ID nicht mehr verwenden.

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon Connect Connect-Funktionen zuzugreifen. Amazon Connect ist ein Omnichannel-Cloud-Kontaktzentrum, das Unternehmen dabei unterstützt, erstklassigen Kundenservice zu geringeren Kosten anzubieten. Amazon Connect bietet Kunden und Mitarbeitern ein nahtloses Sprach- und Chat-Erlebnis. Dazu gehören eine Reihe von Tools für kompetenzbasiertes Routing, leistungsstarke Echtzeit- und Verlaufsanalysen sowie easy-to-use intuitive Verwaltungstools — alles mit pay-as-you-go Preisgestaltung.

Sie können eine oder mehrere Instanzen der virtuellen Contact Center-Instanzen entweder in AMS-Landingzone-Konten mit mehreren Konten oder Landingzone-Konten mit nur einem Konto erstellen. Sie können bestehende SAML 2.0-Identitätsanbieter für den Agentenzugriff verwenden oder die native Unterstützung von Amazon Connect für das Benutzerlebenszyklusmanagement verwenden.

Darüber hinaus können Sie von der Amazon free/direct Connect-Konsole aus gebührenpflichtige Telefonnummern für jede Amazon Connect Connect-Instanz anfordern. Mithilfe einer easy-to-use grafischen Benutzeroberfläche können Sie umfangreiche Kontaktabläufe erstellen, um das gewünschte Kundenerlebnis und die gewünschte Weiterleitung zu erreichen. Die Kontaktflüsse können AWS Lambda Funktionen zur Integration in lokale Datenspeicher und APIs nutzen. Sie können Datenstreaming auch mit Kinesis Streams und Firehose aktivieren.

Die Anrufaufzeichnungen, Chat-Transkripte und Berichte werden in einem Amazon S3 S3-Bucket gespeichert, der mit einem AWS KMS Schlüssel verschlüsselt ist. Die Kontaktflussprotokolle können in CloudWatch Protokollgruppen gespeichert werden.

Weitere Informationen finden Sie unter [Amazon Connect](#).

Häufig gestellte Fragen zu Amazon Connect in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Connect in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem customer_connect_console_role Konto customer_connect_user_role die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Connect in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Connect ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Connect in meinem AMS-Konto?

- Sie müssen einen AWS KMS Schlüssel und einen Amazon S3 S3-Bucket mit Standard-AMS RFCs erstellen. Der Amazon S3 S3-Bucket ist zum Speichern von Anrufaufzeichnungen und Chat-Transkripten erforderlich.
- Wenn Sie eine Integration mit Active Directory (AD) durchführen möchten, ist ein AD Connector für die Integration zwischen AMS-gehosteten Amazon Connect Connect-Instances und Ihren lokalen

Verzeichnisdiensten erforderlich. AD Connector kann in Ihrem Konto konfiguriert werden, indem Sie einen RFC „Management | Other | Other“ anfordern.

- Sie können die folgenden optionalen, selbst bereitgestellten Dienste auf der Grundlage Ihrer Anforderungen an den Kontaktablauf aktivieren.
 - AWS Lambda: Sie können Lambda-Funktionen verwenden, um die Kontaktflüsse zu erweitern, um vorhandene lokale Datenspeicher zu nutzen oder. APIs Sie können den selbst bereitgestellten Lambda-Dienst verwenden, um die Lambda-Funktionen zu erstellen.
 - Amazon Kinesis Data Streams: Sie können Datenstreams erstellen, um Datenstreaming zu externen Anwendungen zu ermöglichen. Sie können Kontaktnachverfolgungsdatensätze oder Agentenereignisse streamen.
 - Amazon Kinesis Data Firehose: Sie können Data Firehose erstellen, um umfangreiche Kontaktverfolgungsdatensätze an externe Anwendungen zu streamen.
 - Amazon Lex: Sie können Amazon Lex Chatbots nutzen, um intelligente Kontaktabläufe zu erstellen und dabei die Amazon Alexa-Services für ein umfassendes Kundenerlebnis und Automatisierung zu nutzen.
- F: Wie beantrage ich das Hinzufügen einer Länderliste für ausgehende oder eingehende Anrufe?

Um eine Länderliste für ausgehende oder eingehende Anrufe hinzuzufügen, reichen Sie eine Serviceanfrage an AMS ein.

Verwenden Sie AMS SSP, um Amazon Data Firehose in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Data Firehose zuzugreifen. Firehose ist der einfachste Weg, Streaming-Daten zuverlässig in Data Lakes, Datenspeicher und Analysetools zu laden. Es kann Streaming-Daten erfassen, transformieren und in Amazon S3, Amazon Redshift, Amazon OpenSearch Service und [Splunk](#) laden und ermöglicht so Analysen nahezu in Echtzeit mit vorhandenen Business Intelligence-Tools und Dashboards, die Sie bereits heute verwenden. Es handelt sich um einen vollständig verwalteten Service, der sich automatisch an den Durchsatz Ihrer Daten anpasst und für den keine laufende Verwaltung erforderlich ist. Außerdem können die Daten vor dem Laden gebündelt, komprimiert, transformiert und verschlüsselt werden, wodurch der Speicherverbrauch am Zielort minimiert und die Sicherheit erhöht wird. Weitere Informationen finden Sie unter [Was ist Amazon Data Firehose?](#)

Häufig gestellte Fragen zu Firehose in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Data Firehose in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_kinesis_firehose_user_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Firehose in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Data Firehose ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Firehose in meinem AMS-Konto?

Für jeden Delivery-Stream müssen neue serviceverknüpfte IAM-Rollen angefordert werden. Sie können auch eine einzelne dienstverknüpfte Rolle für alle Streams wiederverwenden, indem Sie die Rollenrichtlinie mit den erforderlichen Ressourcenberechtigungen aktualisieren (einschließlich S3-Buckets/KMS-Schlüsseln/Lambda-Funktionen/Kinesis-Streams).

Nachdem Sie den RFC zum Hinzufügen von Firehose eingereicht haben, wird sich ein AMS Operations Engineer mit einer Serviceanfrage für die Ressourcen, die ARNs Sie mit Data Firehose verbinden möchten (z. B. S3, Lambda und Kinesis Streams) AWS KMS, mit Ihnen in Verbindung setzen.

Verwenden Sie AMS SSP, um Amazon DevOps Guru in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon DevOps Guru zuzugreifen. Amazon DevOps Guru ist ein vollständig verwalteter Betriebsservice, der es Entwicklern und Betreibern leicht macht, die Leistung und Verfügbarkeit ihrer Anwendungen zu verbessern. DevOpsMit Guru können Sie die mit der Identifizierung betrieblicher Probleme verbundenen administrativen Aufgaben auslagern, sodass Sie schnell Empfehlungen zur Verbesserung Ihrer Anwendung umsetzen können. DevOpsGuru

liefert reaktive Erkenntnisse, die Sie nutzen können, um Ihre Anwendung jetzt zu verbessern. Es bietet auch proaktive Einblicke, mit denen Sie betriebliche Probleme vermeiden können, die sich in future auf Ihre Anwendung auswirken könnten. DevOpsGuru nutzt maschinelles Lernen, um Ihre Betriebsdaten sowie Anwendungsmetriken und Ereignisse zu analysieren und Verhaltensweisen zu identifizieren, die von normalen Betriebsmustern abweichen. Sie werden benachrichtigt, wenn DevOps Guru ein betriebliches Problem oder Risiko feststellt. Für jedes Problem präsentiert DevOps Guru intelligente Empfehlungen zur Lösung aktueller und prognostizierter future betrieblicher Probleme.

Weitere Informationen finden Sie unter [Was ist Amazon DevOps Guru](#).

Häufig gestellte Fragen zu Amazon DevOps Guru in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon DevOps Guru in meinem AMS-Konto?

Um Zugriff zu beantragen, reichen Sie den Änderungstyp Verwaltung | AWS Service | Selbstbereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) ein. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur `customer_devopsguru_role` Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon DevOps Guru in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon DevOps Guru ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon DevOps Guru in meinem AMS-Konto?

Es gibt keine Voraussetzungen. DevOpsGuru nutzt die folgenden AWS Dienste: Amazon CloudWatch Logs, RDS Insights, AWS X-Ray AWS Lambda, und AWS CloudTrail.

Verwenden Sie AMS SSP, um Amazon DocumentDB (mit MongoDB-Kompatibilität) in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen von Amazon DocumentDB (mit MongoDB-Kompatibilität) zuzugreifen. Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein schneller, skalierbarer, hochverfügbarer und vollständig verwalteter Dokumentendatenbankservice, der MongoDB-Workloads

unterstützt. Amazon DocumentDB bietet Ihnen die Leistung, Skalierbarkeit und Verfügbarkeit, die Sie für den skalierbaren Betrieb geschäftskritischer MongoDB-Workloads benötigen. Amazon DocumentDB implementiert die Apache 2.0-Open-Source-API MongoDB 3.6, indem es die Antworten emuliert, die ein MongoDB-Client von einem MongoDB-Server erwartet, sodass Sie Ihre vorhandenen MongoDB-Treiber und -Tools mit Amazon DocumentDB verwenden können. In Amazon DocumentDB sind Speicher und Datenverarbeitung entkoppelt, sodass beide unabhängig voneinander skaliert werden können. Sie können die Lesekapazität auf Millionen von Anfragen pro Sekunde erhöhen, indem Sie bis zu 15 Read Replicas mit niedriger Latenz hinzufügen, unabhängig von der Größe Ihrer Daten. Amazon DocumentDB ist für eine Verfügbarkeit von 99,99% konzipiert und repliziert sechs Kopien Ihrer Daten in drei AWS Availability Zones (). AZs Sie können AWS Database Migration Service (DMS) kostenlos (für sechs Monate) verwenden, um Ihre lokalen oder Amazon Elastic Compute Cloud (Amazon EC2) MongoDB-Datenbanken praktisch ohne Ausfallzeiten zu Amazon DocumentDB zu migrieren. Weitere Informationen finden Sie unter [Amazon DocumentDB \(mit MongoDB-Kompatibilität\)](#).

Häufig gestellte Fragen zu Amazon DocumentDB in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon DocumentDB in meinem AMS-Konto?

Amazon DocumentDB DocumentDB-Konsolen- und Datenzugriffsrollen können durch die Einreichung von zwei AMS RFCs, Konsolenzugriff und Datenzugriff, beantragt werden:

Fordern Sie Zugriff auf Amazon DocumentDB an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem customer_documentdb_role Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon DocumentDB in meinem AMS-Konto?

Amazon DocumentDB erfordert Amazon RDS-spezifische Berechtigungen. Da AMS Amazon RDS vollständig verwaltet, beinhaltet die IAM-Rolle für Amazon DocumentDB einige Einschränkungen für Aktionen auf Amazon RDS. Beachten Sie die folgenden Einschränkungen:

- Der Zugriff auf DeleteDBInstance und wurde DeleteDBCluster APIs eingeschränkt. Um diese Löschungen zu verwenden APIs, reichen Sie einen RFC mit dem Änderungstyp Management | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie aktualisieren (Überprüfung erforderlich) ein (ct-27tuth19k52b4).

- Sie können keine Tags zu Amazon RDS-Instances hinzufügen oder daraus entfernen.
- Sie können Ihre Amazon DocumentDB DocumentDB-Instance nicht öffentlich machen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon DocumentDB in meinem AMS-Konto?

Amazon S3 und AWS KMS sind für die Verwendung von Amazon DocumentDB erforderlich, wenn Amazon S3 S3-Buckets mit AWS KMS Schlüsseln verschlüsselt sind.

Verwenden Sie AMS SSP, um Amazon DynamoDB in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon DynamoDB (DynamoDB) zuzugreifen. Amazon DynamoDB ist eine Schlüsselwert- und Dokumentendatenbank, die in jeder Größenordnung eine Leistung im einstelligen Millisekundenbereich bietet. Es handelt sich um eine vollständig verwaltete, multiaktive Datenbank mit mehreren Regionen und integrierter Sicherheit, Sicherung und Wiederherstellung sowie In-Memory-Caching für Anwendungen im Internet. Weitere Informationen hierzu finden Sie unter [Amazon DynamoDB](#).

Amazon DynamoDB Accelerator (DAX) ist ein Write-Through-Cache-Service, der das Hinzufügen eines Caches zu DynamoDB-Tabellen vereinfachen soll. DAX ist für Anwendungen konzipiert, die Lesevorgänge mit hoher Leistung erfordern.

Häufig gestellte Fragen zu DynamoDB in AWS Managed Services

F: Wie beantrage ich Zugriff auf DynamoDB und DAX in meinem AMS-Konto?

Fordern Sie Zugriff auf DynamoDB und DAX an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen und -Richtlinien zur Verfügung:

- DynamoDB-Rollenname: `customer_dynamodb_role`

Name der DAX-Dienstrolle: `customer_dax_service_role`

- Name der DynamoDB-Richtlinie: `customer_dynamodb_policy`

DAX-Dienstrichtlinie: `customer_dax_service_policy`

Nach der Bereitstellung in Ihrem Konto müssen Sie die Lösung `customer_dynamodb_role` in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von DynamoDB in meinem AMS-Konto?

Alle DynamoDB-Funktionen werden unterstützt, einschließlich DynamoDB Accelerator (DAX).

Beim Erstellen von Alarmen für eine bestimmte Tabelle muss dem Alarmnamen das Präfix „customer*“ vorangestellt werden, zum Beispiel. `customer-employee-table-high-put-latency`

Wenn Sie ein Amazon SNS SNS-Thema für DynamoDB erstellen, muss es den Namen haben: `dynamodb`

Um das von DynamoDB erstellte Amazon SNS SNS-Thema zu löschen, reichen Sie einen RFC vom Änderungstyp Management | Other | Other | Update ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von DynamoDB in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von DynamoDB in Ihrem AMS-Konto.

Verwenden Sie AMS SSP, um Amazon Elastic Container Registry in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Elastic Container Registry (Amazon ECR) zuzugreifen. Amazon Elastic Container Registry ist eine vollständig verwaltete [Docker-Container-Registry](#), die Entwicklern das Speichern, Verwalten und Bereitstellen von Docker-Container-Images erleichtert. Amazon ECR ist in [Amazon Elastic Container Service \(Amazon ECS\)](#) integriert und vereinfacht so Ihren Arbeitsablauf von der Entwicklung bis zur Produktion. Mit Amazon ECR müssen Sie keine eigenen Container-Repositorys betreiben oder sich Gedanken über die Skalierung der zugrunde liegenden Infrastruktur machen. Amazon ECS hostet Ihre Images in einer hochverfügbaren und skalierbaren Architektur, sodass Sie Container für Ihre Anwendungen zuverlässig bereitstellen können. Die Integration mit AWS Identity and Access Management (IAM) ermöglicht die Kontrolle jedes Repositorys auf Ressourcenebene. Bei Amazon ECR fallen keine Vorabgebühren oder Verpflichtungen an. Sie zahlen nur für die Datenmenge, die Sie in Ihren Repositorys speichern, und für die Datenmenge, die ins Internet übertragen wird.

Weitere Informationen finden Sie unter [Amazon Elastic Container Registry](#).

Häufig gestellte Fragen zu Amazon Elastic Container Registry in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon ECR in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon ECR an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:, und mit den zugehörigen IAM-Richtlinien bzw. `customer_ecr_console_role` `customer_ecr_poweruser_instance_profile` `customer_ecr_console_policy` `customer_ecr_poweruser_instance_profile_policy`. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon ECR in meinem AMS-Konto?

Es gibt Einschränkungen in Bezug auf AMS-Namespaces für die Verwendung von Amazon ECR in Ihrem AMS-Konto. Container-Images dürfen nicht das Präfix „AMS-“ oder „Sentinel-“ haben.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon ECR in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon ECR in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP, um EC2 Image Builder in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf EC2 Image Builder Builder-Funktionen zuzugreifen. EC2 Image Builder ist ein vollständig verwalteter AWS Service, der es einfacher macht, die Erstellung, Verwaltung und Bereitstellung von benutzerdefinierten, sicheren und up-to-date „goldenen“ Server-Images zu automatisieren, die vorinstalliert und mit Software und Einstellungen vorkonfiguriert sind, um bestimmte IT-Standards zu erfüllen.

Sie können die AWS-Managementkonsole AWS CLI oder verwenden, APIs um benutzerdefinierte Images in Ihrem AWS Konto zu erstellen. Wenn Sie den verwenden AWS-Managementkonsole, führt Sie der Amazon EC2 Image Builder Builder-Assistent durch die folgenden Schritte:

- Stellen Sie Startartefakte bereit

- Software hinzufügen und entfernen
- Passen Sie Einstellungen und Skripts an
- Führen Sie ausgewählte Tests aus
- Verteilen Sie Bilder nach AWS Regionen

Die von Ihnen erstellten Images werden in Ihrem Konto erstellt und können fortlaufend für Betriebssystem-Patches konfiguriert werden. Weitere Informationen finden Sie unter [EC2 Image Builder](#).

EC2 Häufig gestellte Fragen zu Image Builder in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf EC2 Image Builder in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Über diesen RFC wird die folgende IAM-Rolle in Ihrem Konto bereitgestellt: `customer_ec2_imagebuilder_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen für EC2 Image Builder?

AMS unterstützt die Verwendung von Service Defaults für die Infrastrukturkonfiguration nicht. Sie können eine neue Infrastrukturkonfiguration erstellen oder eine bestehende verwenden.

AMS unterstützt derzeit nicht die Erstellung von Container-Rezepten.

F: Was sind die Voraussetzungen oder Abhängigkeiten, um EC2 Image Builder zu aktivieren?

- EC2 Serviceverknüpfte Image Builder Builder-Rolle: Sie müssen eine dienstverknüpfte Rolle nicht manuell erstellen. Wenn Sie Ihre erste Image Builder-Ressource in der AWS-Managementkonsole, der AWS CLI oder der AWS API erstellen, erstellt Image Builder die serviceverknüpfte Rolle für Sie.
- Instanzen, die zum Erstellen von Images und zum Ausführen von Tests mit Image Builder verwendet werden, müssen Zugriff auf den Systems Manager Manager-Dienst haben. Der SSM-Agent wird auf dem Quell-Image installiert, sofern er noch nicht vorhanden ist, und er wird entfernt, bevor das Image erstellt wird.
- AWS IAM: Die IAM-Rolle, die Sie Ihrem Instanzprofil zuordnen, muss über Berechtigungen zum Ausführen der in Ihrem Image enthaltenen Build- und Testkomponenten verfügen. Die folgenden

IAM-Rollenrichtlinien müssen der IAM-Rolle angehängt werden, die den Instanzprofilen zugeordnet ist: und. `EC2InstanceProfileForImageBuilder` `AmazonSSMManagedInstanceCore` Der Name der IAM-Rolle sollte das Schlüsselwort enthalten. `*imagebuilder*`

- Wenn Sie die Protokollierung konfigurieren, muss das in Ihrer Infrastrukturkonfiguration angegebene Instanzprofil über `s3:PutObject` Berechtigungen für den Ziel-Bucket (`arn:aws:s3:::{bucket-name}/*`) verfügen. Beispiel:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::{bucket-name}/*"
    }
  ]
}
```

- Erstellen Sie ein SNS-Thema mit dem Namen „imagebuilder“, um alle Benachrichtigungen und Benachrichtigungen von EC2 Image Builder zu erhalten.

Verwenden Sie AMS SSP, um Amazon ECS AWS Fargate in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Fargate Funktionen von Amazon ECS zuzugreifen. AWS Fargate ist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen (siehe [Container on AWS](#)), ohne Server oder Cluster von EC2 Amazon-Instances verwalten zu müssen. Damit AWS Fargate müssen Sie keine Cluster von virtuellen Maschinen mehr bereitstellen, konfigurieren oder skalieren, um Container auszuführen. Auf diese Weise müssen keine Servertypen mehr ausgewählt werden, es muss nicht entschieden werden, wann die Cluster skaliert werden oder das Cluster-Packing optimiert werden.

Weitere Informationen finden Sie unter [Amazon ECS auf AWS Fargate](#).

Häufig gestellte Fragen zu Amazon ECS on Fargate in AWS Managed Services

F: Wie beantrage ich in meinem AMS-Konto Zugriff auf Amazon ECS on Fargate?

Beantragen Sie Zugriff auf Amazon ECS auf Fargate, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung: `customer_ecs_fargate_console_role` (falls keine vorhandene IAM-Rolle bereitgestellt wird, der die ECS-Richtlinie zugeordnet werden kann),,, und. `customer_ecs_fargate_events_service_role`
`customer_ecs_task_execution_service_role`
`customer_ecs_codedeploy_service_role`
`AWSServiceRoleForApplicationAutoScaling_ECSService` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon ECS auf Fargate in meinem AMS-Konto?

- Die Überwachung und Protokollierung von Amazon ECS-Aufgaben liegt in Ihrer Verantwortung, da Aktivitäten auf Containerebene oberhalb des Hypervisors stattfinden und die Protokollierungsmöglichkeiten von Amazon ECS auf Fargate eingeschränkt sind. Als Benutzer von Amazon ECS auf Fargate empfehlen wir Ihnen, die notwendigen Schritte zu unternehmen, um die Protokollierung Ihrer Amazon ECS-Aufgaben zu aktivieren. Weitere Informationen finden Sie unter [Aktivieren des awslogs-Protokolltreibers für Ihre Container](#).
- Für Sicherheit und Malware-Schutz auf Container-Ebene sind Sie ebenfalls verantwortlich. Amazon ECS on Fargate enthält weder Trend Micro noch vorkonfigurierte Netzwerksicherheitskomponenten.
- Dieser Service ist sowohl für Landingzone-Konten mit mehreren Konten als auch für AMS-Konten mit Einzelkonten verfügbar.
- Amazon ECS [Service Discovery](#) ist standardmäßig in der Rolle „Self-Provisioned“ eingeschränkt, da erhöhte Berechtigungen erforderlich sind, um private gehostete Route 53 53-Zonen zu erstellen. Um Service Discovery für einen Service zu aktivieren, reichen Sie den Änderungstyp Management | Other | Other | Update ein. Die Informationen, die zur Aktivierung von Service Discovery für Ihren Amazon ECS-Service erforderlich sind, finden Sie im [Service Discovery-Handbuch](#).
- AMS verwaltet oder beschränkt derzeit keine Images, die für die Bereitstellung in Containern auf Amazon ECS Fargate verwendet werden. Sie können Images aus Amazon ECR, Docker Hub oder einem anderen privaten Image-Repository bereitstellen. Aus diesem Grund haben wir empfohlen,

öffentliche oder ungesicherte Images nicht bereitzustellen, da sie zu böswilligen Aktivitäten auf dem Konto führen können.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon ECS auf Fargate in meinem AMS-Konto?

- Im Folgenden sind Abhängigkeiten von Amazon ECS von Fargate aufgeführt. Es sind jedoch keine zusätzlichen Maßnahmen erforderlich, um diese Dienste mit Ihrer selbst bereitgestellten Rolle zu aktivieren:
 - CloudWatch Logs
 - CloudWatch Ereignisse
 - CloudWatch Alarme
 - CodeDeploy
 - App Mesh
 - Cloud Map
 - Route 53
- Abhängig von Ihrem Anwendungsfall stützt sich Amazon ECS auf die folgenden Ressourcen, die Sie möglicherweise benötigen, bevor Sie Amazon ECS on Fargate in Ihrem Konto verwenden können:
 - Sicherheitsgruppe, die mit dem Amazon ECS-Service verwendet werden soll. Sie können Deployment | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Create (auto) (ct-3pc215bnwb6p7) verwenden oder, falls Ihre Sicherheitsgruppe spezielle Regeln erfordert, Deployment | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Erstellen (Überprüfung erforderlich) verwenden (ct-1oxx2g2d7hc90). Hinweis: Die Sicherheitsgruppe, die Sie mit Amazon ECS auswählen, muss speziell für Amazon ECS erstellt werden, wo sich der Amazon ECS-Service oder -Cluster befindet. Weitere Informationen finden Sie im Abschnitt Sicherheitsgruppe unter [Einrichtung mit Amazon ECS](#) und [Sicherheit in Amazon Elastic Container Service](#).
 - Application Load Balancer (ALB), Network Load Balancer (NLB), Classic Load Balancer (ELB) für den Lastenausgleich zwischen Aufgaben.
 - Zielgruppen für ALBs
 - App-Mesh-Ressourcen (z. B. virtuelle Router, virtuelle Dienste, virtuelle Knoten) zur Integration in Ihren Amazon ECS-Cluster.

- Derzeit gibt es für AMS keine Möglichkeit, das Risiko, das mit der Unterstützung von Berechtigungen von Sicherheitsgruppen verbunden ist, automatisch zu minimieren, wenn diese außerhalb der standardmäßigen AMS-Änderungstypen erstellt werden. Wir empfehlen Ihnen, eine bestimmte Sicherheitsgruppe für die Verwendung mit Ihrem Fargate-Cluster anzufordern, um die Möglichkeit der Verwendung einer Sicherheitsgruppe einzuschränken, die nicht für die Verwendung mit Amazon ECS vorgesehen ist.

Verwenden Sie AMS SSP, um Amazon EKS AWS Fargate in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Fargate Funktionen von Amazon EKS zuzugreifen. AWS Fargate [ist eine Technologie, die bedarfsgerecht dimensionierte Rechenkapazität für Container bereitstellt \(Informationen zu Containern finden Sie unter Was sind Container?\)](#). Mit AWS Fargate müssen Sie keine Gruppen von virtuellen Maschinen mehr bereitstellen, konfigurieren oder skalieren, um Container auszuführen. Auf diese Weise müssen keine Servertypen mehr ausgewählt werden, es muss nicht entschieden werden, wann die Knotengruppen skaliert werden oder das Cluster-Packing optimiert werden.

Amazon Elastic Kubernetes Service (Amazon EKS) integriert Kubernetes mithilfe AWS Fargate von Controllern, die mithilfe des erweiterbaren AWS Upstream-Modells von Kubernetes erstellt wurden. Diese Controller werden als Teil der von Amazon EKS verwalteten Kubernetes-Steuerebene ausgeführt und sind für die Planung nativer Kubernetes-Pods auf Fargate verantwortlich. Die Fargate-Controller enthalten einen neuen Scheduler, der neben dem Standard-Kubernetes-Scheduler und zusätzlich zu mehreren mutierenden und validierenden Zugangscontrollern ausgeführt wird. Wenn Sie einen Pod starten, der die Kriterien für die Ausführung auf Fargate erfüllt, erkennen, aktualisieren und planen die im Cluster ausgeführten Fargate-Controller den Pod auf Fargate.

Weitere Informationen finden Sie unter [Amazon EKS ab AWS Fargate sofort allgemein verfügbar](#) und im [Amazon EKS Best Practices Guide for Security](#) (enthält „Empfehlungen“ wie „Unnötigen anonymen Zugriff überprüfen und widerrufen“ und mehr).

Tip

AMS hat einen Änderungstyp, Deployment | Advanced Stack Components | Identity and Access Management (IAM) | OpenID Connect-Anbieter erstellen (ct-30ecvfi3tq4k3), den

Sie mit Amazon EKS verwenden können. Ein Beispiel finden Sie unter [Identity and Access Management \(IAM\) | OpenID Connect Provider erstellen](#).

Häufig gestellte Fragen zu Amazon EKS on AWS Fargate in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon EKS on Fargate in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur Verfügung.

- `customer_eks_fargate_console_role`.

Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

- Diese Servicerollen geben Amazon EKS on Fargate die Erlaubnis, andere AWS Dienste in Ihrem Namen anzurufen:
 - `customer_eks_pod_execution_role`
 - `customer_eks_cluster_service_role`

F: Welche Einschränkungen gelten für die Nutzung von Amazon EKS auf Fargate in meinem AMS-Konto?

- Das Erstellen von [verwalteten](#) oder [EC2 selbstverwalteten](#) Knotengruppen wird in AMS nicht unterstützt. Wenn Sie EC2 Worker Nodes verwenden möchten, wenden Sie sich an Ihren AMS Cloud Service Delivery Manager (CSDM) oder Cloud Architect (CA).
- AMS enthält keine Trend Micro- oder vorkonfigurierten Netzwerksicherheitskomponenten für Container-Images. Es wird von Ihnen erwartet, dass Sie vor der Verteilung Ihre eigenen Image-Suchdienste verwalten, um bösartige Container-Images zu erkennen.
- EKCTL wird aufgrund von Interdependenzen nicht unterstützt. CloudFormation
- Während der Clustererstellung sind Sie berechtigt, die Protokollierung der Cluster-Steuerungsebene zu deaktivieren. Weitere Informationen finden Sie unter [Amazon-EKS-Steuerungsebenen-Protokollierung](#). Wir empfehlen Ihnen, alle wichtigen API-, Authentifizierungs- und Audit-Logging bei der Clustererstellung zu aktivieren.
- Während der Cluster-Erstellung ist der Cluster-Endpointzugriff für Amazon EKS-Cluster standardmäßig öffentlich. Weitere Informationen finden Sie unter [Amazon EKS-Cluster-](#)

[Endpunktzugriffskontrolle](#). Wir empfehlen, Amazon EKS-Endpunkte auf privat zu setzen. Wenn Endgeräte für den öffentlichen Zugriff erforderlich sind, empfiehlt es sich, sie nur für bestimmte CIDR-Bereiche auf öffentlich zu setzen.

- AMS verfügt nicht über eine Methode, um Bilder, die für die Bereitstellung in Containern auf Amazon EKS Fargate verwendet werden, zu erzwingen oder einzuschränken. Sie können Images aus Amazon ECR, Docker Hub oder einem anderen privaten Image-Repository bereitstellen. Daher besteht das Risiko, dass ein öffentliches Image bereitgestellt wird, das böswillige Aktivitäten auf dem Konto ausführen könnte.
- Die Bereitstellung von EKS-Clustern über das Cloud Development Kit (CDK) oder CloudFormation Ingest wird in AMS nicht unterstützt.
- Sie müssen die erforderliche Sicherheitsgruppe mithilfe von [ct-3pc215bnwb6p7 Deployment | Advanced Stack Components | Security Group | Create erstellen und in der Manifestdatei für die Erstellung von Ingresses](#) referenzieren. Das liegt daran, dass die Rolle nicht autorisiert ist, Sicherheitsgruppen zu erstellen. `customer-eks-alb-ingress-controller-role`

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon EKS auf Fargate in meinem AMS-Konto?

Um den Service nutzen zu können, müssen die folgenden Abhängigkeiten konfiguriert werden:

- Für die Authentifizierung gegenüber dem Dienst `aws-iam-authenticator` müssen sowohl KUBECTL als auch installiert sein. Weitere Informationen finden Sie unter Clusterauthentifizierung [verwalten](#).
- Kubernetes basiert auf einem Konzept, das als „Dienstkonten“ bezeichnet wird. Um die Funktionalität der Dienstkonten innerhalb eines Kubernetes-Clusters auf EKS nutzen zu können, ist ein RFC Management | Other | Other | Update mit den folgenden Eingaben erforderlich:
 - [Erforderlich] Name des Amazon EKS-Clusters
 - [Erforderlich] Amazon EKS-Cluster-Namespace, in dem das Servicekonto (SA) bereitgestellt wird.
 - [Erforderlich] Name der Amazon EKS-Cluster-SA.
 - [Erforderlich] Name der IAM-Richtlinie, der permissions/document zugeordnet werden muss.
 - [Erforderlich] Der Name der IAM-Rolle wird angefordert.
 - [Optional] OpenID Connect-Provider-URL. Weitere Informationen finden Sie unter
 - [Aktivierung von IAM-Rollen für Dienstkonten auf Ihrem Cluster](#)
 - [Einführung detaillierter IAM-Rollen für Dienstkonten](#)

- Wir empfehlen, dass Config-Regeln konfiguriert und überwacht werden
 - Öffentliche Cluster-Endpunkte
 - API-Protokollierung deaktiviert

Es liegt in Ihrer Verantwortung, diese Konfigurationsregeln zu überwachen und zu korrigieren.

Wenn Sie einen [ALB-Ingress-Controller](#) bereitstellen möchten, reichen Sie einen RFC für das Update Management | Other | Other ein, um die erforderliche IAM-Rolle für die Verwendung mit dem ALB Ingress Controller-Pod bereitzustellen. Die folgenden Eingaben sind erforderlich, um IAM-Ressourcen zu erstellen, die dem ALB Ingress Controller zugeordnet werden sollen (schließen Sie diese in Ihren RFC ein):

- [Erforderlich] Name des Amazon EKS-Clusters
- [Optional] URL des OpenID Connect-Anbieters
- [Optional] Amazon EKS-Cluster-Namespace, in dem der Application Load Balancer (ALB) -Ingress Controller-Service bereitgestellt wird. [Standard: kube-system]
- [Optional] Name des Amazon EKS-Cluster-Servicekontos (SA). [Standard: aws-load-balancer-controller]

Wenn Sie die Verschlüsselung von Envelope Secrets in Ihrem Cluster aktivieren möchten (was wir empfehlen), geben Sie den KMS-Schlüssel, den IDs Sie verwenden möchten, im Beschreibungsfeld des RFC an, um den Dienst hinzuzufügen (Management | Service | Self-provisioned AWS service | Add (ct-1w8z66n899dct)). Weitere Informationen zur Umschlagverschlüsselung finden Sie unter [Amazon EKS fügt Umschlagverschlüsselung für geheime Daten mit AWS KMS](#) hinzu.

Verwenden Sie AMS SSP, um Amazon EMR in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon EMR-Funktionen zuzugreifen. Amazon EMR ist die branchenführende Cloud-Big-Data-Plattform für die Verarbeitung riesiger Datenmengen mithilfe von Open-Source-Tools wie Apache Spark, Apache Hive, Apache, Apache Flink HBase, Apache Hudi und Presto. Mit Amazon EMR können Sie Analysen im Petabyte-Bereich zu weniger als der Hälfte der Kosten herkömmlicher On-Premises-Lösungen und mehr als dreimal schneller als Apache Spark-Standardlösungen durchführen. Für Aufträge mit kurzer Laufzeit können Sie Cluster hoch- und herunterfahren und pro Sekunde für die verwendeten Instances zahlen. Für Workloads mit langer

Laufzeit können Sie hochverfügbare Cluster erstellen, die automatisch skaliert werden, um der Nachfrage gerecht zu werden.

Sie können eine oder mehrere Instances der Amazon EMR-Cluster entweder in AMS-Landingzone-Konten mit mehreren Konten oder Landingzone-Konten mit einem Konto erstellen, um sowohl transiente als auch persistente Amazon EMR-Cluster zu unterstützen. Sie können auch die Kerberos-Authentifizierung aktivieren, um Benutzer aus einer lokalen Active Directory-Domäne zu authentifizieren.

Sie können mehrere Datenspeicher mit den Amazon EMR-Clustern nutzen, um anwendungsspezifische Hadoop-Tools und -Bibliotheken zu unterstützen. Die Amazon EMR-Cluster können mithilfe von OnDemand Spot-Instances erstellt und Autoscaling konfiguriert werden, um die Kapazität zu verwalten und die Kosten zu senken.

Die Cluster-Protokolldateien können zum Protokollieren und Debuggen in einem Amazon S3 S3-Bucket archiviert werden. Sie können auch auf die im Amazon EMR-Cluster gehosteten Weboberflächen zugreifen, um Hadoop-Administrationsanforderungen oder Notizbucheinträge für Kunden zu unterstützen.

Weitere Informationen finden Sie unter [Amazon EMR](#).

Häufig gestellte Fragen zu Amazon EMR in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon EMR in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Nachdem es in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer_emr_console_role` in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon EMR in meinem AMS-Konto?

Wir empfehlen Ihnen, bei der Erstellung von Amazon EMR auf einem EC2 Cluster von der AWS-Konsole aus die Option Create Cluster — Advanced zu verwenden. Amazon EMR-Cluster müssen erstellt werden, indem das Tag mit dem Schlüssel "for-use-with-amazon-emr-managed-policies" mit dem Wert „true“ hinzugefügt wird. Wählen Sie in den Sicherheitsoptionen die folgenden Konfigurationen aus:

- Wählen Sie benutzerdefinierte Rollen für Ihren Cluster aus:
 - EMR-Rolle: `customer_emr_cluster_service_role`
 - EC2 Instanzprofil: `customer_emr_cluster_instance_profile`
 - Auto Scaling Scaling-Rolle: `customer_emr_cluster_autoscaling_role`
- EC2 Sicherheitsgruppen:
 - Master: `ams-emr-master-security` -Gruppe
 - Kern und Aufgabe: -Gruppe `ams-emr-worker-security`
 - Servicezugriff: -group `ams-emr-serviceaccess-security`

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon EMR in meinem AMS-Konto?

AMS erstellt Standardsicherheitsgruppen für die Master-, Worker- und Services-Knoten von Amazon EMR.

Die Startvorlagen und Sicherheitsgruppen, die mit Amazon EMR-Clustern verwendet werden sollen, müssen den Tag-Schlüssel "for-use-with-amazon-emr-managed-policies" mit dem Wert „true“ haben.

Das standardmäßige Amazon EMR-Cluster-Instance-Profil ermöglicht den Zugriff auf Ressourcen wie S3-Buckets und Dynamodb-Tabellen, deren Namen „emr“ enthalten. Sie können zusätzliche IAM-Richtlinien anfordern, um zusätzliche Ressourcen für Amazon EMR zu nutzen. Die folgenden Ressourcen-ARNs können mit Amazon EMR-Jobs unter Verwendung des `customer_emr_cluster_instance_profile` verwendet werden:

- `arn:aws:dynamodb: *: *: table/*emr*`
- `arn:aws:kinesis: *: *: stream/*emr*`
- `arn:aws:sns: *: *: *emr*` `arn:aws:sqs: *: *: *emr*`
- `arn:aws:sqs: *: *: *emr*`
- `arn:aws:sqs: *: *: AWS-* ElasticMapReduce`
- `arn:aws:sdb: *: *: domäne: *emr*`

- `arn:aws:s3: ::*emr*`

Wenn Kerberos-Authentifizierung für den Amazon EMR-Cluster erforderlich ist:

- Geben Sie den Bereichsnamen an, der für jeden kerberisierten Amazon EMR-Cluster verwendet werden soll, und die lokalen Active Directory-IP-Adressen.
- Anforderungen an die Infrastruktur:

Multi-Account Landing Zone (MALZ): Reichen Sie einen RFC ein, um ein neues verwaltetes Anwendungskonto oder eine neue VPC in einem vorhandenen Anwendungskonto zu erstellen.

Single-Account Landing Zone (SALZ): Reichen Sie einen RFC ein, um ein neues Subnetz in Ihrer VPC zu erstellen.

- Konfigurieren Sie die eingehende Vertrauensstellung für den Bereich des Clusters im lokalen Active Directory.
- Reichen Sie einen RFC ein, um DNS-Zonen für den Bereich im Managed AD zu konfigurieren.
- Konfiguration des Bereichs:

MALZ: Senden Sie einen Management | Other | Other | Update (ct-0xdawir96cy7k) -RFC, um den VPC-DHCP-Optionssatz so zu aktualisieren, dass er den Realmnamen als Domainnamensuffix verwendet.

SALZ: Reichen Sie einen RFC für Management | Other | Other | Update (ct-0xdawir96cy7k) ein, um ein neues Amazon EMR-AMI zu generieren, das den spezifischen Bereich für das Domainnamensuffix verwendet.

Für die Bereitstellung von Amazon EMR Studio ist für die Rolle `customer_emr_cluster_service_role` eine Voraussetzung für einen Amazon Simple Storage Service-Bucket erforderlich. Um den Bucket zu erstellen, verwenden Sie das automatisierte CT `ct-1a68ck03fn98r` (Deployment | Advanced Stack Components | S3 storage | Create). Wenn Sie dieses automatisierte CT verwenden, um einen Amazon S3 S3-Bucket für Amazon EMR zu erstellen, muss der Bucket-Name mit dem Präfix `customer-emr-*` beginnen. Außerdem müssen Sie den Bucket in derselben AWS Region wie der Amazon EMR-Cluster erstellen.

Verwenden Sie AMS SSP, um Amazon EventBridge in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf EventBridge Amazon-Funktionen zuzugreifen. Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software-as-a-Service (SaaS) -Anwendungen und AWS Diensten und leitet diese Daten an Ziele weiter, wie AWS Lambda z. Sie können Routing-Regeln einrichten, um festzulegen, wohin Ihre Daten gesendet werden sollen, um Anwendungsarchitekturen zu erstellen, die in Echtzeit auf alle Ihre Datenquellen reagieren. Mit EventBridge können Sie ereignisgesteuerte Architekturen erstellen, die lose gekoppelt und verteilt sind.

Weitere Informationen finden Sie auf [Amazon EventBridge](#).

EventBridge in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf EventBridge in meinem AMS-Konto?

Beantragen Sie den Zugriff auf EventBridge indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_eventbridge_role` Konto `customer_eventbridge_scheduler_execution_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Die Ausführungsrolle `customer_eventbridge_scheduler_execution_role` ist eine IAM-Rolle, von der EventBridge Scheduler annimmt, um in Ihrem Namen mit anderen AWS-Services zu interagieren. Die mit dieser Rolle verknüpften Berechtigungsrichtlinien gewähren dem EventBridge Scheduler Zugriff auf das Aufrufen von Zielen.

Note

Standardmäßig verwendet EventBridge Scheduler AWS eigene Schlüssel EventBridge zum Verschlüsseln der Daten. Um einen vom Kunden verwalteten Schlüssel für die Verschlüsselung der Daten EventBridge zu verwenden, reichen Sie den RFC über den

Änderungstyp Management | AWS-Service | Self-provisioned service | [Add \(review required\)](#)
[Change Type \(ct-3qe6io8t6jtny\)](#) für die Servicebereitstellung ein.

F: Welche Einschränkungen gelten für die Nutzung in meinem AMS-Konto? EventBridge

Sie müssen AMS einreichen RFCs und die folgenden Ressourcen erstellen: Servicerollen zum Auslösen des Batch-Jobs, SQS-Warteschlange, CodeBuild CodePipeline, und SSM-Befehle.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung EventBridge in meinem AMS-Konto?

Sie müssen mithilfe des Änderungstyps Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) (ct-3dpg8mdd9jn1r) eine EventBridge Servicerolle mit einem RFC anfordern, bevor Sie andere AWS Ressourcen wie AWS Batch Lambda-, Amazon SNS-, Amazon SQS- oder Amazon Logs-Ressourcen EventBridge zum Auslösen verwenden. CloudWatch Geben Sie die Dienste an, die aufgerufen werden sollen, wenn Sie Ihre Servicerolle anfordern. Informationen zu den Berechtigungen, die zum Aufrufen von Zielen erforderlich sind, finden Sie unter [Verwenden ressourcenbasierter Richtlinien](#) für EventBridge

EventBridge ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem Mitglied ausgeführt wurden. AWS-Service EventBridge CloudTrail muss aktiviert sein und darf die Protokolldateien in S3-Buckets speichern. Hinweis: Alle AMS-Konten wurden CloudTrail aktiviert, sodass keine Maßnahmen erforderlich sind.

F: Für die Rolle customer_eventbridge_scheduler_execution_role ist ein Schlüssel erforderlich (optional, falls er für die Verschlüsselung verwendet wird). AWS Key Management Service Wie AWS KMS CMKs setze ich die Verschlüsselung von Daten im Ruhe/bei der Übertragung ein?

Standardmäßig verschlüsselt EventBridge Scheduler Ereignismetadaten und Nachrichtendaten, die er unter einem AWS eigenen Schlüssel speichert (Verschlüsselung im Ruhezustand). EventBridge Scheduler verschlüsselt auch Daten, die zwischen EventBridge Scheduler und anderen Diensten übertragen werden, mithilfe von Transport Layer Security (TLS) (Verschlüsselung bei der Übertragung).

Wenn Ihr spezieller Anwendungsfall erfordert, dass Sie die Verschlüsselungsschlüssel, die Ihre Daten auf EventBridge Scheduler schützen, kontrollieren und prüfen, können Sie einen vom Kunden verwalteten Schlüssel verwenden.

Sie müssen einen RFC mit dem Änderungstyp Verwaltung | AWS-Service | Self-provisioned Service | Add (review required) anfordern, bevor Sie Amazon EventBridge für die Aktivierung der Genehmigung verwenden. AWS KMS

Verwenden Sie AMS SSP, um Amazon Forecast in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Forecast (Forecast) zuzugreifen. Amazon Forecast ist ein vollständig verwalteter Service, der maschinelles Lernen nutzt, um hochgenaue Prognosen zu liefern.

Note

AWS hat mit Wirkung zum 29. Juli 2024 den Zugang für Neukunden zu Amazon Forecast geschlossen. Bestandskunden von Amazon Forecast können den Service weiterhin wie gewohnt nutzen. AWS investiert weiterhin in Sicherheits-, Verfügbarkeits- und Leistungsverbesserungen für Amazon Forecast, plant jedoch AWS nicht, neue Funktionen einzuführen.

Wenn Sie Amazon Forecast verwenden möchten, wenden Sie sich an Ihren CSDM, damit dieser Ihnen weiterhelfen kann, wie Sie [Ihre Nutzung von Amazon Forecast auf Amazon SageMaker Canvas umstellen](#) können.

Forecast basiert auf derselben Technologie, die auch bei Amazon.com verwendet wird, und verwendet maschinelles Lernen, um Zeitreihendaten mit zusätzlichen Variablen zu kombinieren, um Prognosen zu erstellen. Forecast erfordert keine Erfahrung mit maschinellem Lernen, um loszulegen. Sie müssen nur historische Daten sowie alle zusätzlichen Daten angeben, von denen Sie glauben, dass sie sich auf Ihre Prognosen auswirken könnten. Beispielsweise kann sich die Nachfrage nach einer bestimmten Hemdfarbe mit den Jahreszeiten und dem Standort des Geschäfts ändern. Dieser komplexe Zusammenhang ist für sich genommen schwer zu ermitteln, aber maschinelles Lernen eignet sich hervorragend, um ihn zu erkennen. Sobald Sie Ihre Daten bereitgestellt haben, untersucht Forecast sie automatisch, ermittelt, was aussagekräftig ist, und erstellt ein Prognosemodell, mit dem Prognosen getroffen werden können, die bis zu 50% genauer sind als die alleinige Betrachtung von Zeitreihendaten.

Weitere Informationen finden Sie unter [Amazon Forecast](#).

Häufig gestellte Fragen zu Amazon Forecast in AWS Managed Services

F: Wie beantrage ich Zugriff auf Forecast in meinem AMS-Konto?

Beantragen Sie Zugriff auf, AWS Firewall Manager indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_forecast_admin_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Forecast in meinem AMS-Konto?

Der standardmäßige S3-Bucket-Zugriff ermöglicht Ihnen nur den Zugriff auf Buckets mit dem Benennungsmuster „customer-forecast-*“. Wenn Sie Ihre eigene Benennungskonvention für Daten-Buckets haben, besprechen Sie die Benennung von Buckets und die damit verbundene Einrichtung des Zugriffs mit Ihrem Cloud Architect (CA). Beispiel:

- Sie könnten Ihre spezifische Amazon Forecast-Servicerolle mit einer Benennung wie 'AmazonForecast- ExecutionRole -*' und dem zugehörigen richtigen S3-Bucket-Zugriff definieren. Weitere Informationen finden Sie in der IAM-Konsole unter AmazonForecast-ExecutionRole-Admin Servicerolle und IAM-Richtlinie `customer_forecast_default_s3_access_policy`.
- Möglicherweise müssen Sie den zugehörigen S3-Buckets-Zugriff der IAM-Verbundrolle zuordnen. Weitere Informationen finden Sie in der IAM-Richtlinie `customer_forecast_default_s3_access_policy` in der IAM-Konsole.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Forecast in meinem AMS-Konto?

- Vor der Verwendung von Forecast müssen die richtigen Amazon S3 S3-Buckets erstellt werden. Insbesondere erfolgt der Standardzugriff auf S3-Buckets nach dem Benennungsmuster „customer-forecast-*“
- Wenn Sie für S3-Buckets andere Benennungsmuster als „customer-forecast-*“ verwenden möchten, müssen Sie eine neue Servicerolle mit S3-Zugriffsberechtigungen für die Buckets erstellen:
 1. Es muss eine neue Servicerolle mit der Benennung 'AmazonForecast- - ExecutionRole {suffix}' erstellt werden.
 2. Es muss eine neue IAM-Richtlinie erstellt werden, die `customer_forecast_default_s3_access_policy` ähnelt und der neuen Servicerolle und der

zugehörigen Verbundadministratorrolle (z. B. 'customer_forecast_admin_role') zugeordnet werden soll

F: Wie kann ich die Datensicherheit bei der Nutzung von Amazon Forecast verbessern?

- Für die Datenverschlüsselung im Ruhezustand können AWS KMS Sie ein vom Kunden verwaltetes CMK bereitstellen, um den Datenspeicher auf dem Amazon S3 S3-Service zu schützen:
 - Aktivieren Sie die Standardverschlüsselung für den Bucket mit dem Bereitstellungsschlüssel und richten Sie die Bucket-Richtlinie so ein, dass die AWS KMS Datenverschlüsselung beim Eingeben von Daten akzeptiert wird.
 - Aktivieren Sie die Amazon Forecast-Servicerolle 'AmazonForecast- ExecutionRole -*' und die Verbundadministratorrolle (z. B. 'customer_forecast_admin_role') als Hauptbenutzer. AWS KMS
- Für die Datenverschlüsselung während der Übertragung können Sie das HTTPS-Protokoll einrichten, das bei der Übertragung von Objekten gemäß der Amazon S3 S3-Bucket-Richtlinie erforderlich ist.
- Weitere Einschränkungen der Zugriffskontrolle: Aktivieren Sie eine Bucket-Richtlinie für den genehmigten Zugriff für die Amazon Forecast-Servicerolle 'AmazonForecast- ExecutionRole -*' und die Administratorrolle (z. B. 'customer_forecast_admin_role').

F: Was sind die Best Practices bei der Verwendung von Amazon Forecast?

- Sie sollten ein gutes Verständnis Ihrer Datenklassifizierungspraktiken haben und die damit verbundenen Datensicherheitsanforderungen bei der Verwendung von S3-Buckets mit Amazon Forecast abbilden.
- Für die Amazon S3 S3-Bucket-Konfiguration empfehlen wir Ihnen dringend, die HTTPS-Durchsetzung in Ihrer S3-Bucket-Richtlinie zu aktivieren.
- Sie müssen wissen, dass die Admin-Rolle „customer_forecast_admin_role“ den permissiven Zugriff (Get/Delete/PutS3-Objekte) auf Amazon S3 S3-Buckets mit dem Namen „customer-forecast-*“ unterstützt. HINWEIS: Wenn Sie eine detaillierte Zugriffskontrolle für mehrere Teams benötigen, gehen Sie wie folgt vor:
 - Definieren Sie Ihre IAM-Identität für den teambasierten Zugriff (Rolle/Benutzer) mit geringsten Zugriffsrechten auf zugehörige Amazon S3 S3-Buckets.
 - Erstellen Sie team/project basierend AWS KMS CMKs und gewähren Sie den entsprechenden IAM-Identitäten den richtigen Zugriff. (Benutzerzugriff und 'AmazonForecast- ExecutionRole - {team/project}').

- Richten Sie die S3-Bucket-Standardverschlüsselung mit der erstellten ein. AWS KMS CMKs
- Erzwingen Sie S3-API-Verkehr mit dem HTTPS-Protokoll in der S3-Bucket-Richtlinie.
- Erzwingen Sie die S3-Bucket-Konfiguration für den genehmigten Zugriff für verwandte IAM-Identitäten (Benutzerzugriff und 'AmazonForecast- ExecutionRole - {team/project}') auf die Buckets.
- Wenn Sie die 'customer_forecast_admin_role' für allgemeine Zwecke verwenden möchten, sollten Sie die zuvor aufgeführten Punkte berücksichtigen, um S3-Buckets zu schützen.

F: Wo sind Compliance-Informationen zu Amazon Forecast?

Weitere Informationen finden Sie im [Compliance-Programm für AWS Dienste](#).

Verwenden Sie AMS SSP, um Amazon FSx in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf FSx Amazon-Funktionen zuzugreifen. Amazon FSx bietet vollständig verwaltete Dateisysteme von Drittanbietern. Amazon FSx bietet Ihnen die native Kompatibilität von Dateisystemen von Drittanbietern mit Funktionen für Workloads wie Windows-basierten Speicher, Hochleistungsrechnen (HPC), maschinelles Lernen und Electronic Design Automation (EDA). Amazon FSx automatisiert zeitaufwändige Verwaltungsaufgaben wie Hardwarebereitstellung, Softwarekonfiguration, Patching und Backups. Amazon FSx integriert die Dateisysteme mit Cloud-nativen AWS Diensten, wodurch sie für eine breitere Palette von Workloads noch nützlicher werden.

Amazon FSx stellt Ihnen zwei Dateisysteme zur Auswahl: Amazon FSx für Windows File Server für Windows-basierte Anwendungen und Amazon for Lustre FSx für rechenintensive Workloads. Weitere Informationen finden Sie auf [Amazon FSx](#).

Häufig gestellte Fragen zu Amazon FSx in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon FSx in meinem AMS-Konto?

Beantragen Sie Zugriff auf Amazon, FSx indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt customer_fsx_admin_role Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon FSx in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität des Dienstes ist verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon FSx in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Für erweiterte Konfigurationen wie Multi-AZ müssen Sie jedoch die Dienste DFS-Replikation und DFS-Namespaces installieren und verwalten. [Weitere Informationen finden Sie unter Bereitstellen von Multi-AZ-Dateisystemen.](#)

F: Wie integriere ich mein FSx Amazon-Dateisystem in mein Managed AD für mehrere Konten in der landing zone?

Wenn Sie ein FSx Amazon-Dateisystem erstellen, können Sie Ihr MALZ Managed AD als „AWS Managed Microsoft Active Directory“ für die Windows-Authentifizierung angeben. Weitere Informationen finden Sie [unter Amazon FSx mit AWS Directory Service für Microsoft Active Directory](#) verwenden

Außerdem müssen Sie das Managed AD zuerst für das Anwendungskonto freigeben. Senden Sie dazu einen RFC mit dem Änderungstyp Management | Directory Service | Directory | Share directory (ct-369odosk0pd9w).

F: Welche Benutzer gehören zur Gruppe der Delegierten FSx Administratoren von AWS?

Nur IT-Dateiserveradministratoren. Diese Gruppe verfügt über Vollzugriffsrechte für alle Dateifreigaben.

F: Sollte ich die Standard-Dateifreigabe Share verwenden, die bei der Bereitstellung des FSx Systems erstellt wird?

Nein, wir empfehlen nicht, die standardmäßige Dateifreigabe Share wie bereitgestellt zu verwenden. Es gewährt allen Benutzern vollen Zugriff, was gegen das Prinzip der geringsten Rechte verstößt. Erstellen Sie stattdessen kleinere, benutzerdefinierte Dateifreigaben, die Ihren Geschäftsanforderungen entsprechen.

F: Wie kann ich benutzerdefinierte Dateifreigaben für bestimmte Organisationen in meinem Unternehmen erstellen?

Anweisungen zum Erstellen benutzerdefinierter [Dateifreigaben](#) finden Sie unter Dateifreigaben. Beschränken Sie den Zugriff auf jede Dateifreigabe nach dem Prinzip der geringsten Rechte.

Verwenden Sie AMS SSP, um Amazon FSx für OpenZFS in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon FSx for OpenZFS zuzugreifen. FSx for OpenZFS ist ein vollständig verwalteter Dateispeicherservice, der es einfach macht, Daten, die sich auf lokalen ZFS- oder anderen Linux-basierten Dateiservern befinden, nach AWS zu verschieben, ohne Ihren Anwendungscode oder die Art und Weise, wie Sie Daten verwalten, zu ändern. Es bietet einen äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher, der auf dem Open-Source-OpenZFS-Dateisystem basiert und die vertrauten Funktionen und Fähigkeiten von OpenZFS-Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten AWS Dienstes bietet. Für Entwickler, die Cloud-native Anwendungen entwickeln, bietet es einfachen, leistungsstarken Speicher mit umfangreichen Funktionen für die Arbeit mit Daten.

FSx für OpenZFS sind Dateisysteme von Linux-, Windows- und macOS-Recheninstanzen und Containern aus breit zugänglich, die das branchenübliche NFS-Protokoll (v3, v4.0, v4.1, v4.2) verwenden. OpenZFS basiert AWS auf Graviton-Prozessoren und den neuesten AWS Festplatten- und Netzwerktechnologien (einschließlich AWS Scalable Reliable Datagram Networking und dem AWS Nitro-System) und bietet bis zu 1 Million IOPS mit FSx Latenzen von Hunderten von Mikrosekunden. Durch die vollständige Unterstützung von OpenZFS-Funktionen wie Instant point-in-time Snapshots und Datenklonen können Sie mit OpenZFS Ihre lokalen Dateiserver ganz einfach durch AWS Speicher ersetzen, der vertraute Dateisystemfunktionen bietet und die Notwendigkeit, langwierige Qualifizierungen durchzuführen und bestehende Anwendungen oder Tools zu ändern oder neu zu gestalten, überflüssig macht. FSx Und durch die Kombination der leistungsstarken Datenverwaltungsfunktionen von OpenZFS mit der hohen Leistung und Kosteneffizienz der neuesten AWS-Technologien ermöglicht OpenZFS Ihnen, FSx leistungsstarke, datenintensive Anwendungen zu erstellen und auszuführen.

Als vollständig verwalteter Service macht es OpenZFS einfach, FSx vollständig verwaltete Dateisysteme zu starten, auszuführen und zu skalieren, die die Dateiserver ersetzen AWS , die Sie vor Ort betreiben, und gleichzeitig für mehr Flexibilität und geringere Kosten sorgen. Mit FSx OpenZFS müssen Sie sich nicht mehr um die Einrichtung und Bereitstellung von Dateiservern und Speichervolumes, die Replikation von Daten, die Installation und das Patchen von Dateiserversoftware, die Erkennung und Behebung von Hardwarefehlern und die manuelle Durchführung von Backups kümmern. Es bietet auch eine umfassende Integration mit anderen AWS Diensten wie AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS) CloudWatch, Amazon und AWS CloudTrail.

Amazon FSx stellt Ihnen zwei Dateisysteme zur Auswahl: Amazon FSx für Windows File Server für Windows-basierte Anwendungen und Amazon for Lustre FSx für rechenintensive Workloads. Weitere Informationen finden Sie auf [Amazon FSx](#).

Häufig gestellte FSx Fragen zu Amazon für OpenZFS in AWS Managed Services

F: Wie beantrage ich Zugriff FSx zur Nutzung von OpenZFS in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon FSx OpenZFS an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem customer_fsx_ontap_admin_role Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten FSx für die Nutzung von OpenZFS in meinem AMS-Konto?

Um die Sicherheitsgruppe auf den Amazon FSx Elastic Network Interfaces (ENIs) zu ersetzen, müssen Sie Management | Other | Other | Update einreichen, RFCs da Sicherheitsgruppen ein kritischer Perimeter für die AMS-Umgebung sind. Das ist die einzige Einschränkung.

F: Was sind die Voraussetzungen oder Abhängigkeiten FSx für die Nutzung von OpenZFS in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Sie müssen es jedoch [Verwenden Sie AMS SSP, um Amazon FSx in Ihrem AMS-Konto bereitzustellen](#) installiert haben.

Verwenden Sie AMS SSP, um Amazon FSx für NetApp ONTAP in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon FSx for NetApp ONTAP zuzugreifen. Amazon FSx for NetApp ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässige, skalierbare, leistungsstarke und funktionsreiche Dateispeicherung bietet, die auf dem beliebten NetApp ONTAP-Dateisystem basiert. Er bietet die vertrauten Funktionen, Leistungen und Fähigkeiten APIs von NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten Systems. AWS-Service

Amazon FSx for NetApp ONTAP bietet funktionsreichen, schnellen und flexiblen gemeinsamen Dateispeicher, auf den von Linux-, Windows- und macOS-Recheninstanzen aus, die vor Ort

AWS oder vor Ort ausgeführt werden, umfassend zugegriffen werden kann. FSx for ONTAP bietet leistungsstarken SSD-Speicher mit Latenzen unter einer Millisekunde und ermöglicht eine schnelle und einfache Verwaltung Ihrer Daten, indem Sie Ihre Dateien mit einem Klick auf eine Schaltfläche speichern, klonen und replizieren können. Außerdem werden Ihre Daten automatisch auf kostengünstigeren, elastischen Speicher aufgeteilt, sodass Sie keine Kapazität bereitstellen oder verwalten müssen. So können Sie SSD-Leistung für Ihren Workload erreichen, während Sie nur für einen kleinen Teil Ihrer Daten für SSD-Speicher bezahlen. Es bietet hochverfügbaren und langlebigen Speicher mit vollständig verwalteten Backups und Unterstützung für regionsübergreifende Notfallwiederherstellung. Außerdem unterstützt es beliebte Datensicherheits- und Antivirenanwendungen, die den Schutz und die Sicherung Ihrer Daten noch einfacher machen. Für Kunden, die NetApp ONTAP vor Ort verwenden, FSx ist ONTAP eine ideale Lösung, um Ihre dateibasierten Anwendungen von lokalen zu migrieren, zu sichern oder zu beschleunigen, AWS ohne dass Sie Ihren Anwendungscode oder die Art und Weise, wie Sie Ihre Daten verwalten, ändern müssen.

Als vollständig verwalteter Service macht es Amazon FSx for NetApp ONTAP einfach, zuverlässigen, leistungsstarken und sicheren gemeinsamen Dateispeicher in der Cloud zu starten und zu skalieren. Mit Amazon FSx for NetApp ONTAP müssen Sie sich keine Gedanken mehr über die Einrichtung und Bereitstellung von Dateiservern und Speichervolumes, die Replikation von Daten, die Installation und das Patchen von Dateiserversoftware, die Erkennung und Behebung von Hardwarefehlern, die Verwaltung von Failover und Failback sowie die manuelle Durchführung von Backups machen. Es bietet auch eine umfassende Integration mit anderen AWS-Services Anbietern wie Amazon AWS Identity and Access Management WorkSpaces AWS Key Management Service, und AWS CloudTrail.

Amazon FSx stellt Ihnen zwei Dateisysteme zur Auswahl: Amazon FSx für Windows File Server für Windows-basierte Anwendungen und Amazon für Lustre FSx für rechenintensive Workloads. Weitere Informationen finden Sie auf [Amazon FSx](#).

Häufig gestellte FSx Fragen zu Amazon für NetApp ONTAP in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon FSx for NetApp ONTAP in meinem AMS-Konto?

Beantragen Sie Zugriff auf Amazon FSx for NetApp ONTAP, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto `customer_fsx_ontap_admin_role` die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon FSx for NetApp ONTAP in meinem AMS-Konto?

Um die Sicherheitsgruppe auf den elastischen Netzwerkschnittstellen von Amazon FSx for NetApp ONTAP (ENIs) zu ersetzen, müssen Sie Management | Other | Other | Update einreichen, RFCs da Sicherheitsgruppen ein kritischer Perimeter für die AMS-Umgebung sind. Das ist die einzige Einschränkung.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon FSx for NetApp ONTAP in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Sie müssen es jedoch [Verwenden Sie AMS SSP, um Amazon FSx in Ihrem AMS-Konto bereitzustellen](#) installiert haben.

Verwenden Sie AMS SSP, um Amazon Inspector Classic in Ihrem AMS-Konto bereitzustellen

Note

Hinweis zum Ende des Supports: Am 20. Mai 2026 AWS wird der Support für Amazon Inspector Classic eingestellt. Nach dem 20. Mai 2026 können Sie nicht mehr auf die Amazon Inspector Classic-Konsole oder die Amazon Inspector Classic-Ressourcen zugreifen. Amazon Inspector Classic ist nicht mehr für neue Konten und Konten verfügbar, die in den letzten sechs Monaten keine Bewertung abgeschlossen haben. Für alle anderen Konten bleibt der Zugriff bis zum 20. Mai 2026 gültig. Danach können Sie nicht mehr auf die Amazon Inspector Classic-Konsole oder die Amazon Inspector Classic-Ressourcen zugreifen. Weitere Informationen finden Sie unter [Ende des Supports für Amazon Inspector Classic](#).

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Inspector Classic zuzugreifen. Amazon Inspector Classic ist ein automatisierter Sicherheitsbewertungsservice, der dazu beiträgt, die Sicherheit und Konformität von Anwendungen zu verbessern, auf denen bereitgestellt wird AWS. Amazon Inspector Classic bewertet Anwendungen automatisch auf Sicherheitslücken, Sicherheitslücken und Abweichungen von bewährten Methoden. Nach der Durchführung einer Bewertung erstellt Amazon Inspector Classic eine detaillierte Liste der Sicherheitsergebnisse, die nach Schweregrad priorisiert sind. Diese Ergebnisse können direkt oder als Teil detaillierter Bewertungsberichte überprüft werden,

die über die Amazon Inspector Classic-Konsole oder API verfügbar sind. Weitere Informationen finden Sie unter [Amazon Inspector Classic](#).

Häufig gestellte Fragen zu Amazon Inspector in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Inspector Classic in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon Inspector Classic an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die IAM-Rolle zur Verfügung. `customer_inspector_admin_role` Die Rolle umfasst die AWS `AmazonInspectorFullAccess` -verwaltete Richtlinie. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Inspector Classic in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Inspector Classic ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Inspector Classic in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon Inspector Classic in Ihrem AMS-Konto zu verwenden.

Verwenden Sie den neuen Amazon Inspector in AMS

Sie können den neuen Amazon Inspector jetzt in Ihrem AMS-Konto verwenden.

Für Amazon Inspector Classic `AmazonInspectorFullAccess` waren die `customer-inspector-admin-role-ssm-inspector-agent-policy` und erforderlich. Es wurde jedoch ein Update für die SSPS-Rolle vorgenommen `customer-inspector-admin-role`, das nun eine zusätzliche Rolle beinhaltet. `policyAmazonInspector2FullAccess` Diese neue Richtlinie ermöglicht API-Berechtigungen für die neue Version von Amazon Inspector.

Verwenden Sie AMS SSP, um Amazon Kendra in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Kendra zuzugreifen. Amazon Kendra ist ein

intelligenter Suchdienst, der natürliche Sprachverarbeitung und fortschrittliche Algorithmen für maschinelles Lernen verwendet, um spezifische Antworten auf Suchfragen aus Ihren Daten zurückzugeben. Im Gegensatz zur herkömmlichen schlüsselwortbasierten Suche verwendet Amazon Kendra seine Funktionen für semantisches und kontextuelles Verständnis, um festzustellen, ob ein Dokument für eine Suchabfrage relevant ist. Amazon Kendra gibt spezifische Antworten auf Fragen zurück, sodass Ihre Erfahrung der Interaktion mit einem menschlichen Experten sehr nahe kommt. Amazon Kendra ist hochgradig skalierbar, in der Lage, Leistungsanforderungen zu erfüllen, ist eng in andere AWS Dienste wie Amazon S3 und Amazon Lex integriert und bietet Sicherheit auf Unternehmensniveau. Weitere Informationen finden Sie unter [Amazon Kendra](#).

Häufig gestellte Fragen zu Amazon Kendra in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Kendra in meinem AMS-Konto?

Um Zugriff auf Amazon Inspector Classic zu beantragen, reichen Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) ein. Dieser RFC stellt Ihrem Konto die IAM-Rolle zur Verfügung. `customer_kendra_console_role`. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Kendra in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Kendra ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Kendra in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um mit Amazon Kendra zu beginnen. Abhängig von Ihrem spezifischen Anwendungsfall benötigen Sie jedoch möglicherweise Zugriff auf andere AWS Dienste.

Verwenden Sie AMS SSP, um Amazon Kinesis Data Streams in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Kinesis Data Streams (KDS) zuzugreifen. Amazon Kinesis Data Streams ist ein hoch skalierbarer und langlebiger Echtzeit-Datenstreaming-Service. KDS kann kontinuierlich Gigabytes an Daten pro Sekunde aus Hunderttausenden von Quellen wie Website-Clickstreams, Datenbankereignisströmen, Finanztransaktionen, Social-Media-Feeds, IT-

Protokollen und Ereignissen zur Standortverfolgung erfassen. Die gesammelten Daten sind innerhalb von Millisekunden verfügbar, um Anwendungsfälle für Echtzeitanalysen wie Echtzeit-Dashboards, Erkennung von Anomalien in Echtzeit, dynamische Preisgestaltung und mehr zu ermöglichen. Weitere Informationen finden Sie unter [Amazon Kinesis Data Streams](#).

Häufig gestellte Fragen zu Kinesis Data Streams in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Kinesis Data Streams in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon Kinesis Data Streams an, indem Sie einen RFC mit dem Management | AWS-Service | Self-provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_kinesis_data_streaming_user_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Kinesis Data Streams in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Kinesis Data Streams ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Data Streams in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Data Streams in Ihrem AMS-Konto.

Verwenden Sie AMS SSP, um Amazon Kinesis Video Streams in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Kinesis Video Streams (KVS) zuzugreifen. Amazon Kinesis Video Streams unterstützt Sie beim sicheren Streamen von Videos von verbundenen Geräten AWS für Analysen, maschinelles Lernen (ML), Wiedergabe und andere Verarbeitungszwecke. Kinesis Video Streams stellt automatisch die gesamte Infrastruktur bereit, die für die Aufnahme von Streaming-Videodaten von Millionen von Geräten erforderlich ist, und

skaliert sie elastisch. Außerdem speichert, verschlüsselt und indexiert es dauerhaft Videodaten in Ihren Streams und ermöglicht Ihnen den Zugriff auf Ihre Daten über easy-to-use APIs. Kinesis Video Streams ermöglicht Ihnen die Wiedergabe von Videos für die Live- und On-Demand-Anzeige und die schnelle Erstellung von Anwendungen, die durch die Integration mit Amazon Rekognition Video und Bibliotheken für ML-Frameworks wie Apache MxNet TensorFlow, und OpenCV die Vorteile von Computer Vision und Videoanalyse nutzen. Weitere Informationen finden Sie unter [Amazon Kinesis Video Streams](#).

Häufig gestellte Fragen zu Amazon Kinesis Video Streams in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Kinesis Video Streams in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon Kinesis Video Streams an, indem Sie einen RFC mit dem Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_kinesis_video_streaming_user_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Kinesis Video Streams in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Kinesis Video Streams ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Video Streams in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Video Streams in Ihrem AMS-Konto.

Verwenden Sie AMS SSP, um Amazon Lex in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon Lex Lex-Funktionen zuzugreifen. Amazon Lex ist ein Service zum Integrieren von Konversationsschnittstellen in jede Anwendung, die Sprache und Text verwendet.

Amazon Lex bietet fortschrittliche Deep-Learning-Funktionen wie automatische Spracherkennung (ASR) zur Umwandlung von Sprache in Text und Natural Language Understanding (NLU), um die Absicht des Textes zu erkennen, sodass Sie Anwendungen mit äußerst ansprechenden Benutzererlebnissen und lebensechten Konversationsinteraktionen entwickeln können. Mit Amazon Lex stehen dieselben Deep-Learning-Technologien, die Amazon Alexa unterstützen, jetzt allen Entwicklern zur Verfügung, sodass Sie schnell und einfach anspruchsvolle Konversationsbots oder Chatbots in natürlicher Sprache erstellen können. Weitere Informationen finden Sie unter [Amazon Lex](#).

Häufig gestellte Fragen zu Amazon Lex in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Lex in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_lex_author_role` die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Lex in meinem AMS-Konto?

Die Amazon Lex Lex-Integration mit Lambda ist auf Lambda-Funktionen ohne „AMS-“ -Präfix beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Lex in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon Lex in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP, um Amazon MQ in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon MQ MQ-Funktionen zuzugreifen. Amazon MQ ist ein verwalteter Message Broker-Service für Apache ActiveMQ, der Sie bei der Einrichtung und dem Betrieb von Message Brokern in der Cloud unterstützt. Message Broker ermöglichen es verschiedenen Softwaresystemen, die häufig unterschiedliche Programmiersprachen und auf unterschiedlichen

Plattformen verwenden, zu kommunizieren und Informationen auszutauschen. Amazon MQ reduziert Ihre Betriebslast, indem es die Bereitstellung, Einrichtung und Wartung von ActiveMQ, einem beliebten Open-Source-Nachrichtenbroker, verwaltet. Wenn Sie Ihre aktuellen Anwendungen mit Amazon MQ verbinden, werden Industriestandards APIs und Protokolle für das Messaging verwendet, darunter JMS, NMS, AMQP, STOMP, MQTT und. WebSocket Die Verwendung von Standards bedeutet, dass in den meisten Fällen kein Messaging-Code neu geschrieben werden muss, wenn Sie zu migrieren. AWS Weitere Informationen finden Sie unter [Was ist Amazon MQ?](#)

Häufig gestellte Fragen zu Amazon MQ in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon MQ in meinem AMS-Konto?

Die Nutzung von Amazon MQ in Ihrem AMS-Konto erfolgt in zwei Schritten:

1. Stellen Sie den Amazon MQ Broker bereit. Reichen Sie dazu eine CFN-Vorlage mit dem Amazon MQ Broker über einen RFC mit Deployment | Ingestion | Stack from CloudFormation Template | Create change type (ct-36cn2avfrj9v) ein, oder reichen Sie einen RFC mit dem Änderungstyp Management | Other | Other | Other | Create change type (ct-1e1xtak34nx76) ein und fordern Sie die Bereitstellung von Amazon MQ Broker in Ihrem Konto an.
2. Greifen Sie auf die Amazon MQ MQ-Konsole zu. Nachdem der Amazon MQ Broker bereitgestellt wurde, erhalten Sie Zugriff auf die Amazon MQ MQ-Konsole, indem Sie einen RFC mit Management | AWS service | Self-provisioned service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur Verfügung: `customer_mq_console_role`

Nachdem die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie sie in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon MQ in meinem AMS-Konto?

Die volle Funktionalität von Amazon MQ ist in Ihrem AMS-Konto verfügbar. Die Bereitstellung von Amazon MQ Broker ist jedoch aufgrund der erforderlichen erhöhten Berechtigungen nicht im Rahmen der Richtlinie verfügbar. Einzelheiten zur Bereitstellung von Amazon MQ Broker in Ihren Konten finden Sie oben.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon MQ in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon MQ in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP, um Amazon Managed Service für Apache Flink in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Managed Service für Apache Flink zuzugreifen. Managed Service für Apache Flink ist der einfachste Weg, Streaming-Daten zu analysieren, umsetzbare Erkenntnisse zu gewinnen und auf Ihre Geschäfts- und Kundenanforderungen in Echtzeit zu reagieren. Amazon Managed Service für Apache Flink reduziert die Komplexität beim Erstellen, Verwalten und Integrieren von Streaming-Anwendungen mit anderen AWS Services. SQL-Benutzer können mithilfe von Vorlagen und einem interaktiven SQL-Editor problemlos Streaming-Daten abfragen oder ganze Streaming-Anwendungen erstellen. Java-Entwickler können mithilfe von Open-Source-Java-Bibliotheken und AWS -Integrationen schnell anspruchsvolle Streaming-Anwendungen erstellen, um Daten in Echtzeit zu transformieren und zu analysieren. Amazon Managed Service für Apache Flink kümmert sich um alles, was für die kontinuierliche Ausführung Ihrer Echtzeitanwendungen erforderlich ist, und skaliert automatisch, um dem Volumen und dem Durchsatz Ihrer eingehenden Daten zu entsprechen. Mit Amazon Managed Service für Apache Flink zahlen Sie nur für die Ressourcen, die Ihre Streaming-Anwendungen verbrauchen. Es gibt keine Mindestgebühr oder Einrichtungskosten. Weitere Informationen finden Sie unter [Amazon Managed Service für Apache Flink](#).

Häufig gestellte Fragen zu Managed Service für Apache Flink in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Managed Service für Apache Flink in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_kinesis_analytics_application_role` Konto die folgende IAM-Rolle zur Verfügung:.. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Managed Service für Apache Flink in meinem AMS-Konto?

- Konfigurationen sind auf Ressourcen ohne „AMS-“ oder „MC-“ -Präfixe beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.
- Die Erlaubnis, Kinesis Data Streams oder Firehose zu löschen oder neue zu erstellen, wurde aus der Richtlinie entfernt. Wir haben eine andere Richtlinie, die das ermöglicht.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Data Streams in meinem AMS-Konto?

Es gibt einige Abhängigkeiten:

- Amazon Managed Service für Apache Flink erfordert, dass Kinesis Data Streams oder Firehose erstellt werden müssen, bevor eine Anwendung mit Managed Service für Apache Flink konfiguriert werden kann.
- Die ressourcenbasierten Richtlinienberechtigungen sollten auf eine bestimmte Eingabedatenquelle hinweisen.

Verwenden Sie AMS SSP, um Amazon Managed Streaming for Apache Kafka in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Managed Streaming for Apache Kafka (Amazon MSK) zuzugreifen. Amazon Managed Streaming for Apache Kafka ist ein vollständig verwalteter AWS Streaming-Datenservice, mit dem Sie ganz einfach Anwendungen erstellen und ausführen können, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden, ohne dass Sie Experte für den Betrieb von Apache Kafka-Clustern werden müssen. Amazon MSK verwaltet die Bereitstellung, Konfiguration und Wartung von Apache Kafka-Clustern und ZooKeeper Apache-Knoten für Sie. Amazon MSK zeigt auch wichtige Leistungskennzahlen von Apache Kafka in der AWS Konsole an.

Amazon MSK bietet mehrere Sicherheitsstufen für Ihre Apache Kafka-Cluster, darunter VPC-Netzwerkisolierung, AWS IAM für die API-Autorisierung auf Kontrollebene, Verschlüsselung im Ruhezustand, TLS-Verschlüsselung bei der Übertragung, TLS-basierte Zertifikatsauthentifizierung und Authentifizierung gesichert durch SASL/SCRAM AWS Secrets Manager Weitere Informationen finden Sie unter [Amazon MSK](#).

Häufig gestellte Fragen zu Amazon MSK in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon MSK in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbstbereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt die folgenden IAM-Richtlinien und Rollen für Ihr Konto bereit:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon MSK?

Damit Amazon MSK Brokerprotokolle an die von Ihnen konfigurierten Ziele senden kann, stellen Sie sicher, dass die `AmazonMSKFullAccess` Richtlinie mit Ihrer IAM-Rolle verknüpft ist. Es sind also bereits vollständige Zugriffsberechtigungen vorhanden.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon MSK?

Bevor Sie Ihren MSK-Cluster erstellen, müssen Sie über eine VPC und Subnetze innerhalb dieser VPC verfügen. Standardmäßig deckt AMS dies im Rahmen der standardmäßigen [AMS-VPC-Erstellung ab](#).

Weitere Informationen zu den Einschränkungen von Amazon MSK finden Sie unter [Amazon MSK Limits](#).

Verwenden Sie AMS SSP, um Amazon Managed Service für Prometheus in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Managed Service für Prometheus (AMP) zuzugreifen. Amazon Managed Service für Prometheus ist ein serverloser, Prometheus-kompatibler Service zur Überwachung von Containermetriken, der es einfacher macht, Containerumgebungen im großen Maßstab sicher zu überwachen. Mit Amazon Managed Service für Prometheus können Sie dasselbe Open-Source-Prometheus-Datenmodell und dieselbe Abfragesprache verwenden, die Sie heute verwenden, um die Leistung Ihrer containerisierten Workloads zu überwachen, und außerdem von verbesserter Skalierbarkeit, Verfügbarkeit und Sicherheit profitieren, ohne die zugrunde liegende Infrastruktur verwalten zu müssen.

Amazon Managed Service for Prometheus skaliert automatisch die Erfassung, Speicherung und Abfrage von Betriebsmetriken, wenn Workloads nach oben oder unten skaliert werden. Es lässt sich in AWS Sicherheitsdienste integrieren, um einen schnellen und sicheren Zugriff auf Daten zu ermöglichen. Weitere Informationen finden Sie unter [Was ist Amazon Managed Service for Prometheus?](#)

Häufig gestellte Fragen zu Amazon Managed Service für Prometheus in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Managed Service for Prometheus in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem customer-prometheus-console-role Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die customer-prometheus-console-role Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Managed Service for Prometheus in meinem AMS-Konto?

Alle Funktionen werden unterstützt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Managed Service for Prometheus in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um mit Amazon Managed Service for Prometheus zu beginnen. Abhängig von Ihrem spezifischen Anwendungsfall benötigen Sie jedoch möglicherweise Zugriff auf andere AWS Dienste.

Verwenden Sie AMS SSP, um Amazon Personalize in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Personalize zuzugreifen. Amazon Personalize ist ein Service für maschinelles Lernen, mit dem Entwickler auf einfache Weise individuelle Empfehlungen für Kunden erstellen können, die ihre Anwendungen verwenden.

Maschinelles Lernen wird zunehmend zur Verbesserung der Kundenbindung eingesetzt, indem personalisierte Produkt- und Inhaltsempfehlungen, maßgeschneiderte Suchergebnisse und gezielte

Marketingaktionen bereitgestellt werden. Die Entwicklung der Funktionen für maschinelles Lernen, die zur Erstellung dieser ausgeklügelten Empfehlungssysteme erforderlich sind, war für die meisten Unternehmen heute aufgrund der Komplexität jedoch unerreichbar. Amazon Personalize ermöglicht es Entwicklern, die noch keine Erfahrung mit maschinellem Lernen haben, mithilfe von Machine-Learning-Technologie, die durch jahrelangen Einsatz auf Amazon.com perfektioniert wurde, mühelos anspruchsvolle Personalisierungsfunktionen in ihre Anwendungen zu integrieren.

Mit Amazon Personalize stellen Sie einen Aktivitätsstream aus Ihrer Anwendung bereit — Klicks, Seitenaufrufe, Anmeldungen, Käufe usw. — sowie ein Inventar der Artikel, die Sie empfehlen möchten, wie Artikel, Produkte, Videos oder Musik. Sie können Amazon Personalize auch zusätzliche demografische Informationen von Ihren Benutzern wie Alter oder geografischer Standort zur Verfügung stellen. Amazon Personalize verarbeitet und untersucht die Daten, ermittelt, was sinnvoll ist, wählt die richtigen Algorithmen aus und trainiert und optimiert ein Personalisierungsmodell, das auf Ihre Daten zugeschnitten ist. Alle von Amazon Personalize analysierten Daten werden vertraulich und sicher behandelt und nur für Ihre individuellen Empfehlungen verwendet. Sie können mit der Bereitstellung personalisierter Empfehlungen über einen einfachen API-Aufruf beginnen. Sie zahlen nur für das, was Sie tatsächlich nutzen, und es fallen keine Mindestgebühren und keine Vorabverpflichtungen an.

Weitere Informationen finden Sie unter [Amazon Personalize](#).

Häufig gestellte Fragen zu Amazon Personalize in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Personalize in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (review erforderlich) (ct-3qe6io8t6jtny) einreichen. Sie müssen dann angeben, welcher S3-Bucket die Daten enthält, die von personalize zur Generierung der Empfehlungen verwendet werden sollen. AWS Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung `customer_personalize_console_role`: und `customer_personalize_service_role`

- Sobald die in Ihrem Konto `customer_personalize_console_role` bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren. Sie können die `customer_personalize_console_policy` auch einer anderen vorhandenen Rolle zuordnen als `Customer_ReadOnly_Role`.
- Nachdem der `customer_personalize_service_role` Ihrem Konto zur Verfügung gestellt wurde, können Sie seinen ARN angeben, wenn Sie eine neue Datensatzgruppe erstellen.

Zu diesem Zeitpunkt wird AMS Operations diese Servicrolle auch in Ihrem Konto bereitstellen: `aws_code_pipeline_service_role_policy`.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Personalize in meinem AMS-Konto?

Die Amazon Personalize Personalize-Konfiguration ist auf Ressourcen ohne „ams-“ oder „mc-“ - Präfixe beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Personalize in meinem AMS-Konto?

- Wenn der S3-Bucket, in dem Daten gespeichert sind, verschlüsselt ist, muss die KMS-Schlüssel-ID angegeben werden, damit wir der von Amazon Personalize verwendeten Rolle erlauben können, den Bucket zu entschlüsseln.

Amazon Personalize unterstützt den KMS S3-Standardschlüssel nicht. Falls für die Verwendung von KMS erforderlich, erstellen Sie einen benutzerdefinierten Schlüssel und fügen Sie ihm die folgende Richtlinie hinzu, indem Sie einen RFC mit dem Änderungstyp KMS Key | Create (Überprüfung erforderlich) öffnen:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```

- Ein S3-Bucket muss mit der folgenden Bucket-Richtlinie erstellt werden. Reichen Sie dazu einen RFC mit dem Änderungstyp S3 Storage | Create Policy ein. Diese Richtlinie ermöglicht Amazon Personalize den Zugriff auf Daten. Dieser Bucket enthält die Daten, die von Amazon Personalize verwendet werden sollen.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PersonalizeS3BucketAccessPolicy",
  "Statement": [
    {
      "Sid": "PersonalizeS3BucketAccessPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

Verwenden Sie AMS SSP, um Amazon QuickSight in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf QuickSight Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. QuickSight ist ein schneller, cloudgestützter Business Intelligence-Service, der allen Mitarbeitern Ihres Unternehmens Einblicke bietet. Da es sich um einen vollständig verwalteten Service handelt, QuickSight können Sie auf einfache Weise interaktive Dashboards erstellen und veröffentlichen, die Erkenntnisse aus maschinellem Lernen (ML) enthalten. Weitere Informationen finden Sie auf [Amazon QuickSight](#).

QuickSight in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff QuickSight auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_quicksight_console_admin_role` die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung QuickSight in meinem AMS-Konto?

- AWS Sie können aufgrund der Abhängigkeit von den IAM-Richtlinien QuickSight nicht auf die Ressourceneinstellungen zugreifen. Das AMS-Team aktiviert jedoch jede Ressource für Sie als Antwort auf Ihre Anfrage zur Aktivierung des Dienstes.
- Der Ressourcenzugriff für einzelne Benutzer und Gruppen wird in diesem Modell nicht unterstützt, da diese Funktion es Benutzern ermöglicht, IAM-Berechtigungen zu ändern, was die AMS-Infrastruktur gefährden könnte.
- Die Möglichkeit, IAM-Identitäten von innen einzuladen, QuickSight wird aufgrund des Risikos, das mit der Änderung von IAM-Objekten verbunden ist, nicht unterstützt.
- QuickSight Der Service bietet zwei Editionen: Enterprise und Standard. Beide bieten eine Single Sign-On-Option (SSO), die von AMS unterstützt wird. Die Enterprise Edition bietet jedoch eine Option zur QuickSight Integration in Active Directory (AD). QuickSight on AMS unterstützt aufgrund von Inkompatibilitäten zwischen der AMS-Kontostruktur und den QuickSight Vertrauensanforderungen keine Integration mit AD.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung QuickSight in meinem AMS-Konto?

- Wenn AMS diesen RFC zum Hinzufügen erhält QuickSight, erhalten Sie eine Serviceanfrage mit zusätzlichen Informationen. Geben Sie dem Kunden folgende Informationen:
 - QuickSight Kontoname (zum Beispiel *CustomerName*-quicksight)
 - QuickSight Edition (Standard oder Enterprise)
 - Die AWS Region, in der der QuickSight Service aktiviert werden soll (standardmäßig Ihre AWS AMS-Region).
 - Eine Benachrichtigungs-E-Mail-Adresse für das QuickSight Konto.
 - (Optional) Der S3-Bucket, in dem sich die zu analysierenden Datendateien befinden.

- Die VPC und das Subnetz IDs , mit denen eine Verbindung hergestellt wird, QuickSight unterstützen eine Funktion zum Hinzufügen einer VPC-Verbindung, die private Konnektivität zwischen QuickSight und Ressourcen innerhalb des Kontos ermöglicht.

Ein AMS-Betreiber führt den Anmeldevorgang in Ihrem Namen durch und konfiguriert zwei Funktionen: QuickSight

- [Automatische Erkennung](#) von Datenquellen.
- [VPC-Verbindungen](#).

 Note

Diese Aktionen müssen von einem AMS-Betreiber ausgeführt werden, da während des Anmeldevorgangs erhöhte IAM- und VPC-Berechtigungen erforderlich sind.

Verwenden Sie AMS SSP, um Amazon Rekognition in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Rekognition zuzugreifen. Amazon Rekognition macht es einfach, Bild- und Videoanalysen zu Ihren Anwendungen hinzuzufügen, und zwar mithilfe bewährter, hochgradig skalierbarer Deep-Learning-Technologie, für deren Verwendung kein Fachwissen im Bereich maschinelles Lernen erforderlich ist. Mit Amazon Rekognition können Sie Objekte, Personen, Text, Szenen und Aktivitäten in Bildern und Videos identifizieren und unangemessene Inhalte erkennen. Amazon Rekognition bietet außerdem hochgenaue Funktionen zur Gesichtsanalyse und Gesichtssuche, mit denen Sie Gesichter erkennen, analysieren und vergleichen können, und zwar für eine Vielzahl von Anwendungsfällen zur Benutzerverifizierung, Personenzählung und zur öffentlichen Sicherheit.

Mit Amazon Rekognition Custom Labels können Sie Objekte und Szenen in Bildern identifizieren, die speziell auf Ihre Geschäftsanforderungen zugeschnitten sind. Sie können beispielsweise ein Modell erstellen, um bestimmte Maschinenteile an Ihrer Montagelinie zu klassifizieren oder um ungesunde Pflanzen zu erkennen. Amazon Rekognition Custom Labels nimmt Ihnen die schwere Arbeit bei der Modellentwicklung ab, sodass keine Erfahrung mit maschinellem Lernen erforderlich ist. Sie

müssen lediglich Bilder von Objekten oder Szenen bereitstellen, die Sie identifizieren möchten, und der Service erledigt den Rest.

Weitere Informationen finden Sie unter [Amazon Rekognition](#).

Häufig gestellte Fragen zu Amazon Rekognition in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Rekognition in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_rekognition_console_role` & `customer_rekognition_service_role` Konto die folgende IAM-Rolle zur Verfügung: Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Rekognition in meinem AMS-Konto?

Der volle Funktionsumfang von Amazon Rekognition ist mit der selbst bereitgestellten Servicerolle Amazon Rekognition verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Rekognition in meinem AMS-Konto?

Wenn Sie Kinesis Video Streams verwenden, die das Quell-Streaming-Video für einen Amazon Rekognition Video Video-Stream-Prozessor oder einen Datenstream als Ziel zum Schreiben von Daten in Kinesis Data Streams bereitstellen, geben Sie AMS bitte `kinesisStreamName` bei der Erstellung des RFC eine an.

Verwenden Sie AMS SSP, um Amazon SageMaker AI in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon SageMaker AI zuzugreifen. SageMaker KI bietet jedem Entwickler und Datenwissenschaftler die Möglichkeit, Modelle für maschinelles Lernen schnell zu erstellen, zu trainieren und einzusetzen. Amazon SageMaker AI ist ein vollständig verwalteter Service, der den gesamten Workflow für maschinelles Lernen abdeckt, um Ihre Daten zu kennzeichnen und aufzubereiten, einen Algorithmus auszuwählen, das Modell zu trainieren, es für die Bereitstellung abzustimmen und zu optimieren, Vorhersagen zu treffen und Maßnahmen zu ergreifen.

Ihre Modelle werden schneller, mit viel weniger Aufwand und geringeren Kosten in Produktion gehen. Weitere Informationen finden Sie unter [Amazon SageMaker AI](#).

SageMaker Häufig gestellte Fragen zu KI in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf SageMaker KI in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen und die Servicerolle zur Verfügung. `customer_sagemaker_admin_role` `AmazonSageMaker-ExecutionRole-Admin` Nachdem SageMaker KI in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer_sagemaker_admin_role` Rolle in Ihre Verbundlösung integrieren. Sie können nicht direkt auf die Servicerolle zugreifen. Der SageMaker KI-Dienst verwendet sie bei der Ausführung verschiedener Aktionen, wie hier beschrieben: [Rollen übergeben](#).

F: Was sind die Einschränkungen bei der Nutzung von SageMaker KI in meinem AMS-Konto?

- Die folgenden Anwendungsfälle werden von der AMS Amazon SageMaker AI IAM-Rolle nicht unterstützt:
 - SageMaker AI Studio wird derzeit nicht unterstützt.
 - SageMaker KI Ground Truth zur Verwaltung privater Belegschaften wird nicht unterstützt, da diese Funktion einen übermäßigen Zugriff auf Amazon Cognito Cognito-Ressourcen erfordert. Wenn die Verwaltung einer privaten Belegschaft erforderlich ist, können Sie eine benutzerdefinierte IAM-Rolle mit kombinierten SageMaker KI- und Amazon Cognito Cognito-Berechtigungen anfordern. Andernfalls empfehlen wir, Mitarbeiter der öffentlichen Hand (unterstützt von Amazon Mechanical Turk) oder AWS Marketplace Dienstleister für die Datenkennzeichnung zu beauftragen.
- Erstellung von VPC-Endpunkten zur Unterstützung von API-Aufrufen an SageMaker KI-Dienste (`aws.sagemaker`). `{region}.notebook`, `com.amazonaws.{region}.sagemaker.api` und `com.amazonaws.{region}.sagemaker.runtime`) wird nicht unterstützt, da Berechtigungen nicht nur auf KI-bezogene Dienste beschränkt werden können. SageMaker Um diesen Anwendungsfall zu unterstützen, reichen Sie einen RFC Management | Other | Other ein, um zugehörige VPC-Endpoints zu erstellen.
- SageMaker Die auto Skalierung von KI-Endpunkten wird nicht unterstützt, da SageMaker KI `DeleteAlarm` Berechtigungen für jede („*“) Ressource benötigt. Um Endpoint Auto Scaling zu

unterstützen, reichen Sie einen RFC Management | Other | Other ein, um Auto Scaling für einen SageMaker KI-Endpoint einzurichten.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von SageMaker KI in meinem AMS-Konto?

- Die folgenden Anwendungsfälle erfordern vor der Verwendung eine spezielle Konfiguration:
 - Wenn ein S3-Bucket zum Speichern von Modellartefakten und Daten verwendet werden soll, müssen Sie einen S3-Bucket mit den erforderlichen Schlüsselwörtern („SageMaker“, „Sagemaker“, „sagemaker“ oder „aws-glue“) mit einem Deployment | Advanced stack components | S3 storage | Create RFC anfordern.
 - Wenn Elastic File Store (EFS) verwendet wird, muss der EFS-Speicher im selben Subnetz konfiguriert und von Sicherheitsgruppen zugelassen werden.
 - Wenn andere Ressourcen direkten Zugriff auf SageMaker KI-Dienste (Notebooks, API, Runtime usw.) benötigen, muss die Konfiguration wie folgt angefordert werden:
 - Senden eines RFC zur Erstellung einer Sicherheitsgruppe für den Endpoint (Deployment | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Create (auto)).
 - Verwaltung einreichen | Andere | Andere | RFC erstellen, um zugehörige VPC-Endpoints einzurichten.

F: Welche Benennungskonventionen werden für Ressourcen unterstützt, auf die sie direkt zugreifen **customer_sagemaker_admin_role** können? (Im Folgenden finden Sie Informationen zu Aktualisierungs- und Löschberechtigungen. Wenn Sie zusätzliche unterstützte Namenskonventionen für Ihre Ressourcen benötigen, wenden Sie sich zur Beratung an einen AMS Cloud Architect.)

- Ressource: AmazonSageMaker-ExecutionRole-* Rolle übergeben
 - Berechtigungen: Die selbst bereitgestellte SageMaker AI-Servicerolle unterstützt Ihre Verwendung der SageMaker AI-Servicerolle (AmazonSageMaker-ExecutionRole-*) mit AWS Glue AWS RoboMaker, und. AWS Step Functions
- Ressource: Secrets auf AWS Secrets Manager
 - Berechtigungen: Beschreiben, Erstellen, Abrufen und Aktualisieren von Geheimnissen mit einem AmazonSageMaker-* Präfix.
 - Berechtigungen: Beschreiben, Geheimnisse abrufen, wenn das SageMaker Ressourcen-Tag auf gesetzt ist true.

- Ressource: Repositorien aktiviert AWS CodeCommit
 - Berechtigungen: Repositorys mit einem Präfix erstellen/löschen. `AmazonSageMaker-`*
 - Berechtigungen: Git Pull/Push auf Repositorys mit den folgenden Präfixen, `*sagemaker*``*SageMaker*`, und. `*Sagemaker*`
- Ressource: Amazon ECR-Repositorys (Amazon Elastic Container Registry)
 - Berechtigungen: Berechtigungen: Legen Sie Repository-Richtlinien fest, löschen Sie sie und laden Sie Container-Images hoch, wenn die folgende Benennungskonvention für Ressourcen verwendet wird. `*sagemaker*`
- Ressource: Amazon S3 S3-Buckets
 - Berechtigungen: Objekt abrufen, speichern, löschen, mehrteiliges Hochladen von S3-Objekten abbrechen, wenn Ressourcen die folgenden Präfixe haben: `*SageMaker*`, und. `*Sagemaker*` `*sagemaker*` `aws-glue`
 - Berechtigungen: Ruft S3-Objekte ab, wenn das SageMaker Tag auf gesetzt ist. `true`
- Ressource: Amazon CloudWatch Log Group
 - Berechtigungen: Protokollgruppe oder Stream erstellen, Protokollereignis speichern, Auflisten, Aktualisieren, Erstellen, Löschen der Protokollzustellung mit dem folgenden Präfix: `/aws/sagemaker/*`.
- Ressource: Amazon CloudWatch Metric
 - Berechtigungen: Geben Sie Metrikdaten ein, wenn die folgenden Präfixe verwendet werden: `AWS/SageMaker` `AWS/SageMaker/aws/SageMaker`, `aws/SageMaker/`, `aws/sagemaker`, `aws/sagemaker/`, und `/aws/sagemaker/..`
- Ressource: Amazon CloudWatch Dashboard
 - Berechtigungen: Create/Delete Dashboards, wenn die folgenden Präfixe verwendet werden: `customer_*`
- Ressource: Thema Amazon SNS (Simple Notification Service)
 - Berechtigungen: Subscribe/Create Thema, wenn die folgenden Präfixe verwendet werden: `*sagemaker*``*SageMaker*`, und. `*Sagemaker*`

F: Was ist der Unterschied zwischen **AmazonSageMakerFullAccess** und **customer_sagemaker_admin_role**?

Das `customer_sagemaker_admin_role` `customer_sagemaker_admin_policy` bietet fast die gleichen Berechtigungen wie mit der `AmazonSageMakerFullAccess` Ausnahme:

- Erlaubnis zur Verbindung mit AWS RoboMaker Amazon Cognito und AWS Glue Ressourcen.
- SageMaker Automatische Skalierung von KI-Endpunkten. Sie müssen einen RFC mit dem Änderungstyp Management | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie aktualisieren (Überprüfung erforderlich) (ct-27tuth19k52b4) einreichen, um Autoscaling-Berechtigungen vorübergehend oder dauerhaft zu erhöhen, da Autoscaling einen permissiven Zugriff auf den Service erfordert. CloudWatch

F: Wie verwende ich einen vom Kunden verwalteten Schlüssel bei der Datenverschlüsselung im Ruhezustand? AWS KMS

Sie müssen sicherstellen, dass die Schlüsselrichtlinie für die vom Kunden verwalteten Schlüssel ordnungsgemäß eingerichtet wurde, sodass zugehörige IAM-Benutzer oder -Rollen die Schlüssel verwenden können. Weitere Informationen finden Sie im [Dokument mit den AWS KMS wichtigsten Richtlinien](#).

Verwenden Sie AMS SSP, um Amazon Simple Email Service in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Simple Email Service (Amazon SES) zuzugreifen. Amazon Simple Email Service ist ein Cloud-basierter E-Mail-Versandservice, der digitale Vermarkter und Anwendungsentwickler beim Versand von Marketing-, Benachrichtigungs- und Transaktions-E-Mails unterstützt.

Sie können die SMTP-Schnittstelle oder eine der Schnittstellen verwenden AWS SDKs , um Amazon SES direkt in Ihre vorhandenen Anwendungen zu integrieren. Sie können die E-Mail-Versandfunktionen von Amazon SES auch in die Software integrieren, die Sie bereits verwenden, z. B. Ticketsysteme und E-Mail-Clients.

Weitere Informationen finden Sie unter [Amazon Simple Email Service](#).

Häufig gestellte Fragen zu Amazon SES in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon SES in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon SES an, indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_ses_admin_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon SES in meinem AMS-Konto?

- Sie müssen eine S3-Bucket-Richtlinie konfigurieren, damit Amazon SES Ereignisse im Bucket veröffentlichen kann.
- Sie müssen einen Standardschlüssel (AWS SES) verwenden oder einen CMK-Schlüssel konfigurieren, damit Amazon SES E-Mails verschlüsseln und Ereignisse an andere Serviceressourcen wie Amazon S3, Amazon SNS, Lambda und Firehose weiterleiten kann, die zum Konto gehören.

F: Welche Einschränkungen gelten für die Nutzung von Amazon SES in meinem AMS-Konto?

Sie müssen Spenden sammeln RFCs , um die folgenden Ressourcen zu erstellen:

- Ein SMTP-Benutzer und eine IAM-Servicerolle mit PutEvents Genehmigung für einen Kinesis Firehose-Stream.
- Sie müssen mithilfe von AMS-Änderungstypen neue AWS Ressourcen wie S3-Bucket, Firehose-Stream und SNS-Thema erstellen, damit die Ziele Ihrer Amazon SES SES-Regeln und Konfigurationssätze mit diesen Ressourcen funktionieren.
- SMTP-Anmeldeinformationen. Um neue SMTP-Anmeldeinformationen anzufordern, verwenden Sie den Change Type (Management | Other | Other | Create). AMS erstellt die Anmeldeinformationen und fügt sie für Sie zu Secrets Manager hinzu.

Verwenden Sie AMS SSP, um Amazon Simple Workflow Service in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Simple Workflow Service (Amazon SWF) zuzugreifen. Amazon Simple Workflow Service unterstützt Entwickler beim Erstellen, Ausführen und Skalieren von Hintergrundjobs mit parallel oder sequentiellen Schritten. Sie können sich Amazon SWF als vollständig verwalteten Status-Tracker und Aufgabenkoordinator in der Cloud vorstellen. Wenn die Ausführung der Schritte Ihrer Anwendung mehr als 500 Millisekunden in Anspruch nimmt, Sie den Status der Verarbeitung verfolgen müssen oder wenn Sie eine Aufgabe wiederherstellen oder erneut versuchen müssen, wenn eine Aufgabe fehlschlägt, kann Amazon SWF Ihnen helfen. Weitere Informationen finden Sie unter [Amazon Simple Workflow Service](#).

Häufig gestellte Fragen zu Amazon SWF in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon SWF in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_swf_role` die folgende IAM-Rolle zur Verfügung: Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon SWF in meinem AMS-Konto?

Die `InvokeFunction` Lambda-Berechtigungen wurden in diesen Service aufgenommen. Das `AMScustomer_deny_policy`, das allen AMS-Kundenrollen hinzugefügt wird, verweigert jedoch ausdrücklich den Zugriff auf AMS-Lambda-Funktionen und AMS-eigene Ressourcen. Um Ressourcen in Amazon SWF zu kennzeichnen oder die Markierung aufzuheben, reichen Sie einen Änderungstyp `Management | Andere | Andere` ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon SWF in meinem AMS-Konto?

Amazon SWF ist vom AWS Lambda Service abhängig, daher wurden im Rahmen dieser Rolle Berechtigungen zum Aufrufen von Lambda bereitgestellt, und es sind keine zusätzlichen Berechtigungen erforderlich, um Lambda von Amazon SWF aufzurufen. Andernfalls gibt es keine Voraussetzungen für die Verwendung von Amazon SWF.

Verwenden Sie AMS SSP, um Amazon Textract in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Textract zuzugreifen. Amazon Textract ist ein vollständig verwalteter Service für maschinelles Lernen, der automatisch gedruckten Text, Handschriften und andere Daten aus gescannten Dokumenten extrahiert. Er geht über die einfache optische Zeichenerkennung (OCR) hinaus, um Daten aus Formularen und Tabellen zu identifizieren, zu verstehen und zu extrahieren. Weitere Informationen finden Sie unter [Amazon Textract](#).

Häufig gestellte Fragen zu Amazon Textract in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich die Einrichtung von Amazon Textract in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung: `customer_textract_console_role`, `customer_textract_human_review_execution_role`, `customer_ec2_textract_instance_profile`. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle `customer_textract_console_role` in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Textract in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von Amazon Textract in Ihrem AMS-Konto.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Textract in meinem AMS-Konto?

Sie müssen die Erstellung eines S3-Buckets beantragen, indem Sie die folgenden Felder einreichen: RFC Deployment | Advanced Stack Components | S3 storage | Create (ct-1a68ck03fn98r).

Verwenden Sie AMS SSP, um Amazon Transcribe in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Transcribe zuzugreifen. Amazon Transcribe ist ein vollständig verwalteter und kontinuierlich geschulter automatischer Spracherkennungsdienst, der automatisch Texttranskripte mit Zeitstempel aus Audiodateien generiert. Amazon Transcribe macht es Entwicklern leicht, ihren Anwendungen speech-to-text Funktionen hinzuzufügen. Es ist für Computer praktisch unmöglich, Audiodaten zu suchen und zu analysieren. Daher muss aufgezeichnete Sprache in Text umgewandelt werden, bevor sie in Anwendungen verwendet werden kann. In der Vergangenheit mussten Kunden mit Transkriptionsanbietern zusammenarbeiten, bei denen sie teure Verträge unterzeichnen mussten, und es war schwierig, sie in ihre Technologie-Stacks zu integrieren, um diese Aufgabe zu erfüllen. Viele dieser Anbieter verwenden veraltete Technologien, die sich nicht gut an verschiedene Szenarien anpassen lassen, wie z. B. Telefonaudio mit niedriger Klangqualität, das in Kontaktzentren üblich ist, was zu einer schlechten Genauigkeit führt.

Amazon Transcribe verwendet einen Deep-Learning-Prozess namens automatische Spracherkennung (ASR), um Sprache schnell und präzise in Text umzuwandeln. Amazon Transcribe kann verwendet werden, um Kundendienstanrufe zu transkribieren, Untertitelung und Untertitelung

zu automatisieren und Metadaten für Medienressourcen zu generieren, um ein vollständig durchsuchbares Archiv zu erstellen. Sie können Amazon Transcribe Medical verwenden, um medizinische speech-to-text Funktionen zu klinischen Dokumentationsanwendungen hinzuzufügen. Weitere Informationen finden Sie unter [Amazon Transcribe](#).

Häufig gestellte Fragen zu Amazon Transcribe in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich die Einrichtung von Amazon Transcribe in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_transcribe_role` Konto die folgende IAM-Rolle zur Verfügung: Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Transcribe in meinem AMS-Konto?

Wenn Sie mit Transcribe arbeiten, müssen Sie „customer-transcribe“ als Präfix für Ihre Buckets verwenden, sofern RA nicht anders angegeben.

Sie können keine IAM-Rolle in Amazon Transcribe erstellen.

Sie können keinen vom Service verwalteten S3-Bucket für Ausgabedaten in Standard-SSPS verwenden (falls dies erforderlich ist, wenden Sie sich bitte an Ihre Konto-zertifizierungsstelle).

Sie müssen die Risikoakzeptanz einreichen, wenn Sie vom Kunden verwaltete KMS-Schlüssel verwenden möchten, die nicht unter den AMS-Namespaces fallen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Transcribe in meinem AMS-Konto?

S3 muss Zugriff auf die Buckets mit dem Namen „customer-transcribe“ haben. KMS ist für die Verwendung von Amazon Transcribe erforderlich, wenn Ihre S3-Buckets mit KMS-Schlüsseln verschlüsselt sind. Wenn ein Bucket nicht verschlüsselt werden muss, kann "KMStranscribeAllow" entfernt werden.

Verwenden Sie AMS SSP, um Amazon WorkSpaces in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf WorkSpaces Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. WorkSpaces ermöglicht Ihnen die

Bereitstellung virtueller, cloudbasierter Microsoft Windows- oder Amazon Linux-Desktops für Ihre Benutzer, bekannt als WorkSpaces. WorkSpaces macht die Beschaffung und Bereitstellung von Hardware oder die Installation komplexer Software überflüssig. Sie können nach Ihren Bedürfnissen Benutzer schnell und bequem hinzufügen oder entfernen. Benutzer greifen auf sie zu, WorkSpaces indem sie eine Client-Anwendung von einem unterstützten Gerät oder, für Windows WorkSpaces, einen Webbrowser verwenden, und melden sich mit ihren vorhandenen lokalen Active Directory (AD) -Anmeldeinformationen an.

Weitere Informationen finden Sie auf [Amazon WorkSpaces](#).

WorkSpaces in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff WorkSpaces auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_workspaces_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung WorkSpaces in meinem AMS-Konto?

Die volle Funktionalität von Workspaces ist mit der von Amazon WorkSpaces selbst bereitgestellten Servicerolle verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung WorkSpaces in meinem AMS-Konto?

- WorkSpaces sind AWS regional begrenzt; daher muss der AD Connector in derselben AWS Region konfiguriert werden, in der die WorkSpaces Instanzen gehostet werden.

Kunden können mit einer der folgenden beiden Methoden eine Verbindung WorkSpaces zum Kunden-AD herstellen:

1. Verwenden des AD-Connectors zur Proxyauthentifizierung für den lokalen Active Directory-Dienst (bevorzugt):

Konfigurieren Sie den Active Directory (AD) Connector in Ihrem AMS-Konto, bevor Sie Ihre WorkSpaces Instanz in Ihren lokalen Verzeichnisdienst integrieren. Der AD Connector fungiert als Proxy für Ihre vorhandenen AD-Benutzer (aus Ihrer Domain), mit denen Sie WorkSpaces

mithilfe vorhandener lokaler AD-Anmeldeinformationen eine Verbindung herstellen können. Dies wird bevorzugt, da sie direkt mit der lokalen Domäne des Kunden verknüpft WorkSpaces sind, die sowohl als Ressourcen- als auch als Benutzergesamtstruktur fungiert, was zu mehr Kontrolle auf Kundenseite führt.

Weitere Informationen finden Sie unter [Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces \(Szenario 1\)](#).

2. Verwenden von AD Connector mit AWS Microsoft AD, Shared Services VPC und einer unidirektionalen Vertrauensstellung für lokale Umgebungen:

Sie können Benutzer auch mit Ihrem lokalen Verzeichnis authentifizieren, indem Sie zunächst eine unidirektionale ausgehende Vertrauensstellung von AMS-verwaltetem AD zu Ihrem lokalen AD einrichten. WorkSpaces tritt AMS-verwaltetem AD über einen AD Connector bei. WorkSpaces Die Zugriffsberechtigungen werden dann über das von AMS verwaltete AD an die WorkSpaces Instanzen delegiert, ohne dass Sie eine wechselseitige Vertrauensstellung mit Ihrer lokalen Umgebung aufbauen müssen. In diesem Szenario befindet sich die Benutzergesamtstruktur im Kunden-AD und die Ressourcengesamtstruktur im AMS-verwalteten AD (Änderungen am AMS-verwalteten AD können über RFC angefordert werden). Beachten Sie, dass die Konnektivität zwischen WorkSpaces VPC und der MALZ Shared Services VPC, auf der AMS-verwaltetes AD ausgeführt wird, über Transit Gateway hergestellt wird.

Weitere Informationen finden Sie unter [Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces \(Szenario 6\)](#).

Note

Der AD Connector kann konfiguriert werden, indem ein RFC vom Typ Management | Other | Other | Create Change Type mit den erforderlichen AD-Konfigurationsdetails eingereicht wird. Weitere Informationen finden [Sie unter AD Connector erstellen](#). Wenn Methode 2 verwendet wird, um eine Ressourcengesamtstruktur in AMS-verwaltetem AD zu erstellen, reichen Sie ein weiteres Management | Other | Other | Other | Create Change Type RFC in AMS Shared-Services-Konto ein, indem Sie das von AMS verwaltete AD ausführen.

Verwenden Sie AMS SSP, um AMS Code-Dienste in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem von AMS verwalteten Konto auf die Funktionen der AMS Code-Dienste zuzugreifen. AMS Code Services ist ein firmeneigenes Bündel von AWS-Code-Management-Services, wie im Folgenden beschrieben wird. Sie können wählen, ob Sie alle Services in AMS mit AMS Code-Services oder einzeln in AMS bereitstellen möchten.

Die AMS Code-Dienste umfassen die folgenden Dienste:

- **AWS CodeCommit:** Ein vollständig verwalteter [Quellcodeverwaltungsdienst](#), der sichere Git-basierte Repositories hostet. Dadurch können Teams in einem sicheren und hoch skalierbaren Ökosystem gemeinsam an Code arbeiten. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen. Sie können CodeCommit auch zum sicheren Aufbewahren beliebiger Objekte von Quellcode bis hin zu Binärdateien verwenden. Außerdem wird das reibungslose Arbeiten mit vorhandenen Git-basierten Tools ermöglicht. Weitere Informationen hierzu finden Sie unter [AWS CodeCommit](#).

Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unter [Verwenden Sie AMS SSP zur Bereitstellung AWS CodeCommit in Ihrem AMS-Konto](#).

- **AWS CodeBuild:** Ein vollständig verwalteter Dienst für kontinuierliche Integration, der Quellcode kompiliert, Tests durchführt und Softwarepakete erstellt, die sofort einsatzbereit sind. Mit CodeBuild müssen Sie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in einer Warteschlange warten müssen. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen. Mit CodeBuild werden Ihnen die von Ihnen genutzten Rechenressourcen minutengenau berechnet. Weitere Informationen hierzu finden Sie unter [AWS CodeBuild](#).

Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unter [Verwenden Sie AMS SSP zur Bereitstellung AWS CodeBuild in Ihrem AMS-Konto](#).

- **AWS CodeDeploy:** Ein vollständig verwalteter Bereitstellungsservice, der Softwarebereitstellungen für eine Vielzahl von Rechendiensten wie Amazon EC2 und Ihren lokalen Servern automatisiert.

AWS CodeDeploy unterstützt Sie bei der schnellen Veröffentlichung neuer Funktionen, hilft Ihnen, Ausfallzeiten bei der Anwendungsbereitstellung zu vermeiden, und bewältigt die Komplexität der Aktualisierung Ihrer Anwendungen. Sie können AWS CodeDeploy verwenden, um Softwarebereitstellungen zu automatisieren, sodass fehleranfällige manuelle Operationen überflüssig werden. Der Service lässt sich an Ihre Bereitstellungsanforderungen anpassen. Weitere Informationen hierzu finden Sie unter [AWS CodeDeploy](#).

Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unter [Verwenden Sie AMS SSP zur Bereitstellung AWS CodeDeploy in Ihrem AMS-Konto](#).

- AWS CodePipeline: Ein vollständig verwalteter [Continuous Delivery-Service](#), der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses bei jeder Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells. Auf diese Weise können Sie Funktionen und Updates schnell und zuverlässig bereitstellen. Sie können problemlos Dienste von Drittanbietern wie GitHub oder Ihr eigenes benutzerdefiniertes Plugin integrieren AWS CodePipeline. Mit zahlen Sie nur für das AWS CodePipeline, was Sie nutzen. Es fallen keine Vorausleistungen an und Sie gehen keine langfristigen Verpflichtungen ein. Weitere Informationen hierzu finden Sie unter [AWS CodePipeline](#).

Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unter [Verwenden Sie AMS SSP zur Bereitstellung AWS CodePipeline in Ihrem AMS-Konto](#).

Häufig gestellte Fragen zu AMS-Code-Services in AWS Managed Services

F: Wie beantrage ich Zugriff auf AMS Code-Services in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_code_suite_console_role` Konto die folgende IAM-Rolle zur Verfügung: Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren. Zu diesem Zeitpunkt wird AMS Operations auch die `customer_codebuild_service_role`, `customer_codedeploy_service_role`, `aws_code_pipeline_service_role` Servicerollen in Ihrem Konto für CodeBuild CodeDeploy und CodePipeline Services bereitstellen. Wenn zusätzliche IAM-Berechtigungen für die erforderlich sind, reichen Sie eine AMS-Serviceanfrage ein. `customer_codebuild_service_role`

 Note

Sie können diese Dienste auch separat hinzufügen. Weitere Informationen finden Sie unter [Verwenden Sie AMS SSP zur Bereitstellung AWS CodeBuild in Ihrem AMS-Konto](#) [Verwenden Sie AMS SSP zur Bereitstellung AWS CodeDeploy in Ihrem AMS-Konto](#) [Verwenden Sie AMS SSP zur Bereitstellung AWS CodePipeline in Ihrem AMS-Konto](#), bzw..

F: Welche Einschränkungen gelten für die Nutzung der AMS Code-Dienste in meinem AMS-Konto?

- AWS CodeCommit: Die Trigger-Funktion CodeCommit ist aufgrund der damit verbundenen Rechte zum Erstellen von SNS-Themen deaktiviert. Die direkte Authentifizierung gegen CodeCommit ist eingeschränkt. Benutzer sollten sich mit Credential Helper authentifizieren. Einige KMS-Befehle sind ebenfalls eingeschränkt: kms: Encrypt, kms: Decrypt,, und kms:ReEncrypt. kms: GenerateDataKey kms: GenerateDataKeyWithoutPlaintext kms: DescribeKey
- CodeBuild: Für den Zugriff auf AWS CodeBuild Konsolenadministratoren sind die Berechtigungen auf Ressourcenebene beschränkt. CloudWatch Aktionen sind beispielsweise auf bestimmte Ressourcen beschränkt und die iam:PassRole Berechtigungen werden kontrolliert.
- CodeDeploy: CodeDeploy Unterstützt derzeit nur Bereitstellungen auf Amazon EC2 /On-Premises. Bereitstellungen auf ECS und Lambda werden nicht CodeDeploy unterstützt.
- CodePipeline: CodePipeline Funktionen, Stufen und Anbieter sind auf Folgendes beschränkt:
 - Bereitstellungsphase: Amazon S3 und AWS CodeDeploy
 - Quellstufe: Amazon S3 AWS CodeCommit, Bit Bucket und GitHub
 - Build-Phase: AWS CodeBuild und Jenkins
 - Genehmigungsphase: Amazon SNS
 - Testphase: Jenkins AWS CodeBuild, Ghost Inspector UI-Tests BlazeMeter, Micro Focus StormRunner Load, Runscope API-Überwachung
 - Invoke Stage: Step Functions und Lambda

 Note

AMS Operations stellt das `customer_code_pipeline_lambda_policy` in Ihrem Konto bereit. Es muss mit der Lambda-Ausführungsrolle für die Lambda-Aufrufphase verknüpft werden. Geben Sie den service/execution Lambda-Rollenamen an, mit dem Sie diese Richtlinie hinzufügen möchten. Wenn es keine

benutzerdefinierte service/execution Lambda-Rolle gibt, erstellt AMS eine neue Rolle mit dem Namen `customer_code_pipeline_lambda_execution_role`, das ist eine Kopie von `customer_lambda_basic_execution_role` zusammen mit `customer_code_pipeline_lambda_policy`.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung der AMS Code-Dienste in meinem AMS-Konto?

- CodeCommit: Wenn S3-Buckets mit AWS KMS Schlüsseln verschlüsselt AWS KMS sind, müssen S3 verwendet AWS CodeCommit werden.
- CodeBuild: Wenn zusätzliche IAM-Berechtigungen für die definierte AWS CodeBuild Servicerolle erforderlich sind, fordern Sie diese über eine AMS-Serviceanfrage an.
- CodeDeploy: Keine.
- CodePipeline: Keine. AWS unterstützte Dienste—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—müssen vor oder zusammen mit dem Start von CodePipeline gestartet werden. Dies wird jedoch von einem AMS-Techniker durchgeführt.

Verwenden Sie AMS SSP zur Bereitstellung AWS Amplify in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Amplify Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. Dabei AWS Amplify handelt es sich um eine Komplettlösung, mit der Frontend-Web- und Mobilentwickler auf einfache Weise Full-Stack-Anwendungen erstellen, verbinden und hosten können. Amplify bietet Flexibilität, um die Bandbreite der AWS Dienste zu nutzen, wenn sich Ihre Anwendungsfälle weiterentwickeln. Amplify bietet Produkte zur Erstellung von Fullstack-Apps für iOS, Android, Flutter, Web und React Native. Weitere Informationen hierzu finden Sie unter [AWS Amplify](#).

AWS Amplify in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS Amplify die Einrichtung in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen.

Dieser RFC stellt Ihrem `customer_amplify_console_role` Konto die folgende IAM-Rolle zur Verfügung: Nach der Bereitstellung für Ihr Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Darüber hinaus müssen Sie eine Risikoakzeptanz angeben, da es AWS Amplify über Berechtigungen verfügt, die die Infrastruktur verändern. Arbeiten Sie dazu mit Ihrem Cloud Service Delivery Manager (CSDM) zusammen.

F: Welche Einschränkungen gelten für die Nutzung AWS Amplify in meinem AMS-Konto?

Sie müssen es `'amplify*'` als Präfix für Ihre Buckets verwenden, wenn Sie mit Amplify arbeiten, sofern RA nicht anders angegeben.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Amplify in meinem AMS-Konto?

Es gibt keine Voraussetzungen für die Nutzung von AWS Amplify in Ihrem AMS-Konto.

Nur Malz-Umgebungen: Die integrierte Standardrolle für Amplify ist „`customer_amplify_console_role`“. Um eine benutzerdefinierte Rolle zu verwenden, stellen Sie zunächst die IAM-Entitäten bereit. Erstellen Sie dann einen zusätzlichen RFC, um Ihre benutzerdefinierte Rolle zur Zulassungsliste der Service Control-Richtlinie für Anwendungskonten hinzuzufügen.

Verwenden Sie AMS SSP für die Bereitstellung AWS AppSync

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS AppSync Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS AppSync vereinfacht die Anwendungsentwicklung, indem Sie eine flexible API erstellen können, mit der Sie sicher auf Daten aus einer oder mehreren Datenquellen zugreifen, diese bearbeiten und kombinieren können. AWS AppSync ist ein verwalteter Dienst, der GraphQL verwendet, um es Anwendungen zu erleichtern, genau die Daten zu erhalten, die sie benötigen.

Mit AWS AppSync können Sie skalierbare Anwendungen, einschließlich solcher, die Aktualisierungen in Echtzeit erfordern, auf einer Reihe von Datenquellen wie NoSQL-Datenspeichern, relationalen Datenbanken APIs, HTTP und Ihren benutzerdefinierten Datenquellen erstellen. AWS Lambda Für mobile Apps und Web-Apps bietet es AWS AppSync zusätzlich lokalen Datenzugriff, wenn Geräte offline gehen, und Datensynchronisierung mit anpassbarer Konfliktlösung, wenn sie wieder online sind. Weitere Informationen hierzu finden Sie unter [AWS AppSync](#).

AWS AppSync in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS AppSync auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung: und. `customer_appsync_service_role` `customer_appsync_author_role` Nach der Bereitstellung in Ihrem Konto müssen Sie sie `customer_appsync_author_role` in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der AWS AppSync Nutzung von?

- Beim Erstellen einer Datenquelle für AppSync den Kunden muss die zuvor erstellte Servicerolle angegeben werden. Die Erstellung einer neuen Rolle ist nicht zulässig. Daher wird der Zugriff verweigert zurückgegeben
- AppSync Rollen sind so konfiguriert, dass Berechtigungen auf Ressourcen beschränkt werden, die die Präfixe „AMS-“ oder „MC-“ enthalten, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS AppSync?

Der Dienst ermöglicht die Verwendung mehrerer anderer Dienste als Datenquelle.

Die Grundberechtigungen, sie als solche zu verwenden, sind in der Dienstrolle (`customer_appsync_service_role`) enthalten, aber Sie müssen die Servicerolle manuell auswählen, wenn Sie den Dienst verwenden.

Verwenden Sie AMS SSP zur Bereitstellung AWS App Mesh in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS App Mesh Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS App Mesh bietet Netzwerke auf Anwendungsebene, sodass Ihre Dienste über verschiedene Arten von Computerinfrastrukturen hinweg einfach miteinander kommunizieren können. App Mesh standardisiert die Art und Weise, wie Ihre Dienste kommunizieren, bietet Ihnen end-to-end Transparenz und gewährleistet eine hohe Verfügbarkeit Ihrer Anwendungen.

AWS App Mesh macht es einfach, Dienste auszuführen, indem es konsistente Transparenz und Netzwerkverkehrskontrollen für Dienste bietet, die auf mehreren Arten von Computerinfrastrukturen basieren. App Mesh macht es überflüssig, den Anwendungscode zu aktualisieren, um zu ändern, wie Überwachungsdaten gesammelt oder der Datenverkehr zwischen Diensten weitergeleitet wird. App Mesh konfiguriert jeden Dienst für den Export von Überwachungsdaten und implementiert eine konsistente Kommunikationssteuerungslogik in Ihrer gesamten Anwendung. Dies macht es einfach, schnell den genauen Ort von Fehlern zu lokalisieren und den Netzwerkverkehr automatisch umzuleiten, wenn es zu Ausfällen kommt oder wenn Codeänderungen implementiert werden müssen. Weitere Informationen hierzu finden Sie unter [AWS App Mesh](#).

AWS App Mesh in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS App Mesh auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_app_mesh_console_role` die folgende IAM-Rolle zur Verfügung:.. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der AWS App Mesh Nutzung von?

Die volle Funktionalität von AWS App Mesh ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS App Mesh?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung AWS App Mesh in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Audit Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Audit Manager zuzugreifen. Audit Manager hilft Ihnen dabei, Ihre AWS Nutzung kontinuierlich zu überprüfen, um die Bewertung von Risiken und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen. Audit Manager automatisiert die Sammlung von Beweisen, um die Bewertung zu erleichtern, ob Ihre Richtlinien, Verfahren und Aktivitäten effektiv funktionieren. Wenn es Zeit für ein Audit ist, hilft Ihnen Audit Manager dabei, die

Überprüfung Ihrer Kontrollen durch Interessengruppen zu verwalten und revisionstaugliche Berichte mit deutlich weniger manuellem Aufwand zu erstellen. Weitere Informationen finden Sie unter [Audit Manager](#).

AWS Audit Manager in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Audit Manager auf mein AMS-Konto?

Sie können den Zugriff beantragen, indem Sie die folgenden Felder einreichen: AWS Services RFC Management | AWS-Service | Self-Provisioned Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny). Dieser RFC `customer-audit-manager-admin-Role` stellt die folgende IAM-Rolle in Ihrem Konto bereit. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

F: Welche Einschränkungen gibt es bei der Nutzung AWS Audit Manager?

Es gibt keine Einschränkungen für die Verwendung von AWS Audit Manager in Ihrem AMS-Konto. Die volle Funktionalität für AWS Audit Manager wird bereitgestellt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS Audit Manager?

1. Sie müssen AMS den S3-Bucket zur Verfügung stellen, in dem Sie sich befinden reports/assessments möchten.
2. Wenn Sie den Dienst verschlüsseln möchten, müssen Sie AMS den zu verwendenden KMS-CMK-ARN zur Verfügung stellen.
3. Wenn Sie eine SNS-Benachrichtigung an ein Thema senden möchten, müssen Sie den Namen des Themas oder ARN angeben.
4. (Optional) Wenn Sie Organizations als Teil Ihrer Multi-Account-Landingzone in Audit Manager aktivieren möchten und ein delegiertes Administratorkonto wünschen, gibt es eine zusätzliche Voraussetzung: Geben Sie im Beschreibungsfeld für RFC (Management | AWS Service | Compatible Service| Add) an, dass Sie das delegierte Administratorkonto als Teil des Audit Manager Manager-Setups verwenden möchten, und geben Sie die folgenden Details an:
 - KMS CMK ARN (ursprünglich zur Einrichtung von Audit Manager verwendet)
 - Delegierte Administratorkonto-ID für Audit Manager zur Verwendung als Teil dieser landing zone mit mehreren Konten (kann ein MALZ-Anwendungskonto sein)

Verwenden Sie AMS SSP zur Bereitstellung AWS Batch in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Batch Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Batch ermöglicht Entwicklern, Wissenschaftlern und Ingenieuren die einfache und effiziente Ausführung von Hunderttausenden von Batch-Computing-Jobs. AWS Batch stellt dynamisch die optimale Menge und Art der Rechenressourcen (wie CPU- oder speicheroptimierte Instances) bereit, basierend auf dem Volumen und den spezifischen Ressourcenanforderungen der eingereichten Batch-Jobs. Mit müssen Sie keine Batch-Computing-Software oder Servercluster AWS Batch, die Sie für die Ausführung Ihrer Jobs verwenden, installieren und verwalten, sodass Sie sich auf die Analyse der Ergebnisse und die Lösung von Problemen konzentrieren können. Weitere Informationen hierzu finden Sie unter [AWS Batch](#).

AWS Batch in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Batch auf mein AMS-Konto?

1. Um Zugriff auf zu beantragen AWS Batch, reichen Sie RFC Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) ein. Dieser RFC stellt die folgenden IAM-Rollen und -Richtlinien in Ihrem Konto bereit:

IAM-Rollen:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Richtlinien:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`

- `customer_batch_events_service_role_policy`

2. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle `customer_batch_console_role` in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gibt es bei der Nutzung AWS Batch?

Bei der Erstellung der Compute-Umgebung sollten Sie EC2 Instanzen als „customer_batch“ oder „customer-batch“ kennzeichnen. Wenn die Instanzen nicht markiert sind, werden die Instanzen nicht per Batch beendet, wenn der Job abgeschlossen ist.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS Batch?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung AWS Batch in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Certificate Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf die Funktionen AWS Certificate Manager (ACM) in Ihrem verwalteten AMS-Konto zuzugreifen. AWS Certificate Manager ist ein Dienst, mit dem Sie öffentliche und private Secure Sockets Layer/Transport Layer Security (SSL/TLS) -Zertifikate zur Verwendung mit AWS Diensten und Ihren internen verbundenen Ressourcen bereitstellen, verwalten und bereitstellen können. SSL/TLS Zertifikate werden verwendet, um die Netzwerkkommunikation zu sichern und die Identität von Websites im Internet sowie von Ressourcen in privaten Netzwerken nachzuweisen. AWS Certificate Manager macht den zeitaufwändigen manuellen Prozess des Kaufs, Hochladens und SSL/TLS Erneuerns von Zertifikaten überflüssig.

Mit AWS Certificate Manager können Sie ein Zertifikat anfordern, es auf ACM-integrierten AWS Ressourcen wie Elastic Load Balancers, CloudFront Amazon-Distributionen und APIs auf API Gateway bereitstellen und die Verlängerung von Zertifikaten übernehmen lassen AWS Certificate Manager . Außerdem können Sie damit private Zertifikate für Ihre internen Ressourcen erstellen und den Lebenszyklus von Zertifikaten zentral verwalten. Öffentliche und private Zertifikate, die AWS Certificate Manager für die Verwendung mit ACM-integrierten Diensten bereitgestellt werden, sind kostenlos. Sie zahlen nur für die AWS Ressourcen, die Sie für die Ausführung Ihrer Anwendung erstellen. Mit [AWS Private Certificate Authority](#) zahlen Sie monatlich für den Betrieb der AWS Private CA und für die privaten Zertifikate, die Sie ausstellen. Weitere Informationen finden Sie unter [AWS Certificate Manager — AWS Dokumentation](#).

Häufig gestellte Fragen zu ACM in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Certificate Manager auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_acm_create_role` die folgende IAM-Rolle zur Verfügung: Sie können diese Rolle verwenden, um ACM-Zertifikate zu erstellen und zu verwalten. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

ACM-Zertifikate können mit den folgenden Änderungstypen erstellt werden, auch wenn Sie die `customer_acm_create_role` IAM-Rolle nicht hinzugefügt haben:

- [ACM | Öffentliches Zertifikat erstellen](#)
- [ACM | Privates Zertifikat erstellen](#)
- [ACM-Zertifikat mit zusätzlichem | Erstellen SANs](#)

F: Was sind die Einschränkungen bei der AWS Certificate Manager Verwendung von?

Sie müssen eine Änderungsanforderung (Request for Change, RFC) an AMS senden, um bestehende Zertifikate zu löschen oder zu ändern, da diese Aktionen vollen Administratorzugriff erfordern (verwenden Sie den Änderungstyp Verwaltung | Andere | Andere | Aktualisierung (ct-0xdawir96cy7k). Beachten Sie, dass die IAM-Richtlinie Rechte, die auf Tagnamen (mc*, ams* usw.) basieren, nicht ausschließen kann. Für Zertifikate fallen keine Kosten an, daher ist das Löschen unbenutzter Zertifikate nicht zeitaufwändig.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Certificate Manager?

Bestehender öffentlicher DNS-Name und Zugriff zum Erstellen von DNS-CNAME-Einträgen, diese müssen jedoch nicht im verwalteten Konto gehostet werden.

Verwenden Sie AMS SSP zur Bereitstellung AWS Private Certificate Authority in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Private Certificate Authority Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. Private Zertifikate werden zur Identifizierung und Sicherung der Kommunikation zwischen verbundenen Ressourcen

in privaten Netzwerken wie Servern, Mobil- und IoT-Geräten und -Anwendungen verwendet. AWS Private CA ist ein verwalteter privater CA-Dienst, mit dem Sie den Lebenszyklus Ihrer privaten Zertifikate einfach und sicher verwalten können. AWS Private CA bietet Ihnen einen hochverfügbaren Service für private Zertifizierungsstellen ohne die Vorabinvestitionen und laufenden Wartungskosten für den Betrieb Ihrer eigenen privaten Zertifizierungsstelle. AWS Private CA erweitert die Zertifikatsverwaltungsfunktionen von ACM auf private Zertifikate, sodass Sie öffentliche und private Zertifikate zentral erstellen und verwalten können. Mithilfe der AWS Management Console oder der ACM-API können Sie ganz einfach private Zertifikate für Ihre AWS Ressourcen erstellen und bereitstellen. Für EC2 Instances, Container, IoT-Geräte und lokale Ressourcen können Sie ganz einfach private Zertifikate erstellen und verfolgen und sie mit Ihrem eigenen clientseitigen Automatisierungscode bereitstellen. Sie haben auch die Flexibilität, private Zertifikate zu erstellen und diese für Anwendungen, die benutzerdefinierte Gültigkeitsdauer von Zertifikaten, Schlüsselalgorithmen oder Ressourcennamen erfordern, selbst zu verwalten. Weitere Informationen finden Sie unter. [AWS Private CA](#)

AWS Private CA in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Private CA auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den AWS Services-RFC (Management | AWS Service | Compatible Service) einreichen. Über diesen RFC wird Ihrem Konto die folgende IAM-Rolle zugewiesen: `customer_acm_pca_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der AWS Private CA Nutzung von?

Derzeit kann AWS Resource Access Manager (AWS RAM) nicht verwendet werden, um Ihr AWS Private CA Cross-Konto zu teilen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Private CA?

1. Wenn Sie eine CRL erstellen möchten, benötigen Sie einen S3-Bucket, in dem Sie sie speichern können. AWS Private CA hinterlegt die CRL automatisch in dem von Ihnen Amazon S3 S3-Bucket und aktualisiert sie regelmäßig. Es ist eine Voraussetzung, dass für den S3-Bucket die unten angegebene Bucket-Richtlinie gilt, bevor Sie eine CRL einrichten können. Um mit dieser Anfrage fortzufahren, erstellen Sie einen RFC mit `ct-0fpj1xa808sh2` (Verwaltung | Erweiterte Stack-Komponenten | S3-Speicher | Aktualisierungsrichtlinie) wie folgt:

- Geben Sie den S3-Bucket-Namen oder den ARN an.
- Kopieren Sie die folgende Richtlinie auf RFC und bucket -name ersetzen Sie sie durch den gewünschten S3-Bucket-Namen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "acm-pca.amazonaws.com"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*",
        "arn:aws:s3:::bucket-name"
      ]
    }
  ]
}
```

2. Wenn der obige S3-Bucket verschlüsselt ist, benötigt der Service Principal acm-pca.amazonaws.com Berechtigungen zum Entschlüsseln. Um mit dieser Anfrage fortzufahren, erstellen Sie einen RFC mit ct-3ovo7px2vsa6n (Management | Erweiterte Stack-Komponenten | KMS-Schlüssel | Update) wie folgt:

- Geben Sie den KMS-Schlüssel-ARN an, für den die Richtlinie aktualisiert werden muss.
- Kopieren Sie die folgende Richtlinie auf RFC und bucket -name ersetzen Sie sie durch den gewünschten S3-Bucket-Namen.

```
{
```

```

{
  "Sid": "Allow ACM-PCA use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "acm-pca.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
        "arn:aws:s3:::bucket_name/audit-report/*",
        "arn:aws:s3:::bucket_name/crl/*"
      ]
    }
  }
}

```

3. AWS Private CA CRLs unterstützt die S3-Einstellung „Öffentlichen Zugriff auf Buckets und Objekte blockieren, die über neue Zugriffskontrolllisten gewährt wurden (ACLs)“ nicht. Sie müssen diese Einstellung für das S3-Konto und den AWS Private CA Bucket deaktivieren, damit sie schreiben können, CRLs wie unter [So erstellen und speichern Sie Ihre CRL für ACM Private CA sicher](#) beschrieben. Wenn Sie deaktivieren möchten, erstellen Sie einen neuen RFC mit ct-0xdawir96cy7k (Verwaltung | Andere | Andere | Update) und fügen Sie eine Risikoakzeptanz hinzu. Wenn Sie Fragen zur Risikoakzeptanz haben, wenden Sie sich an Ihren Cloud Architect.

Verwenden Sie AMS SSP zur Bereitstellung AWS CloudEndure in Ihrem AMS-Konto

Note

Nach dem erfolgreichen Start von AWS Application Migration Service ist der CloudEndure Migrationsdienst nun in allen AWS Regionen nicht mehr verfügbar. Wir empfehlen unseren Kunden, ihn AWS Application Migration Service für Lift-and-Shift-Migrationen in GovCloud Regionen und in kommerzielle Regionen zu nutzen. Weitere Informationen finden Sie unter [Was ist? AWS Application Migration Service](#).

Wenn Sie die verwenden möchten AWS Application Migration Service, wenden Sie sich an Ihre CA, damit sie Ihnen weiterhelfen kann.

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CloudEndure Funktionen in Ihrem AMS-verwalteten Konto zuzugreifen. AWS CloudEndure Die Migration vereinfacht, beschleunigt und automatisiert umfangreiche Migrationen von physischer, virtueller und cloudbasierter Infrastruktur zu. AWS CloudEndure Disaster Recovery (DR) schützt vor Ausfallzeiten und Datenverlust aufgrund beliebiger Bedrohungen, einschließlich Ransomware und Serverbeschädigung.

AWS CloudEndure in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CloudEndure in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_cloud_endure_user` Konto den folgenden IAM-Benutzer zur Verfügung: Nach dem es in Ihrem Konto bereitgestellt wurde, werden der Zugriffsschlüssel und der geheime Schlüssel für den Benutzer in AWS Secrets Manager geteilt.

Diese Richtlinien werden auch für das Konto bereitgestellt: `customer_cloud_endure_policy` und `customer_cloud_endure_deny_policy`

Darüber hinaus müssen Sie eine Risikoakzeptanz angeben, da die CloudEndure DR-Lösung für die Anwendungsintegration über Berechtigungen verfügt, die die Infrastruktur verändern. Arbeiten Sie dazu mit Ihrem Cloud Service Delivery Manager (CSDM) zusammen.

F: Welche Einschränkungen gelten für die Nutzung CloudEndure in meinem AMS-Konto?

Die Cloud-fähigen Replikations- und Konvertierungsinstanzen können nur in dem von Ihnen angegebenen Subnetz gestartet werden.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CloudEndure in meinem AMS-Konto? Teilen Sie Folgendes über die bidirektionale RFC-Korrespondenz mit:

- VPC-Subnetzdetails für Replikations- und Konvertierungsinstanzen, die gestartet werden sollen.
- Der KMS-Schlüssel Amazon Resource Name (ARN), wenn die EBS-Volumes verschlüsselt sind.

Verwenden Sie AMS SSP zur Bereitstellung AWS CloudHSM in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CloudHSM Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CloudHSM hilft Ihnen dabei, die unternehmensinternen, vertraglichen und behördlichen Compliance-Anforderungen an die Datensicherheit zu erfüllen, indem spezielle Hardware Security Module (HSM) -Instanzen in der Cloud verwendet werden. AWS AWS, und AWS Marketplace-Partner bieten eine Vielzahl von Lösungen zum Schutz sensibler Daten innerhalb der AWS Plattform an. Für einige Anwendungen und Daten, die vertraglichen oder behördlichen Vorschriften zur Verwaltung kryptografischer Schlüssel unterliegen, kann jedoch zusätzlicher Schutz erforderlich sein. AWS CloudHSM ergänzt bestehende Datenschutzlösungen und ermöglicht es Ihnen, Ihre darin enthaltenen Verschlüsselungscodes zu schützen HSMs , die nach staatlichen Standards für sicheres Schlüsselmanagement entwickelt und validiert wurden. AWS CloudHSM ermöglicht es Ihnen, kryptografische Schlüssel, die für die Datenverschlüsselung verwendet werden, sicher zu generieren, zu speichern und zu verwalten, sodass nur Sie auf die Schlüssel zugreifen können. Weitere Informationen hierzu finden Sie unter [AWS CloudHSM](#).

AWS CloudHSM in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS CloudHSM auf mein AMS-Konto?

Die Nutzung von in Ihrem AMS-Konto erfolgt in zwei Schritten:

1. Fordern Sie einen AWS CloudHSM Cluster an. Reichen Sie dazu einen RFC mit dem Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) ein. Geben Sie die folgenden Details an:
 - AWS Region.
 - ID/ARN. Provide a VPC ID/VPCVPC-ARN, der sich in demselben Konto befindet wie der RFC, den Sie einreichen.
 - Geben Sie mindestens zwei Availability Zones für den Cluster an.
 - EC2 Amazon-Instance-ID, die eine Verbindung zum HSM-Cluster herstellt.
2. Greifen Sie auf die AWS CloudHSM Konsole zu. Senden Sie dazu einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct).

Dieser RFC stellt Ihrem `customer_cloudhsm_console_role` Konto die folgende IAM-Rolle zur Verfügung:.

Nachdem die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie sie in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS CloudHSM in meinem AMS-Konto?

Der Zugriff auf die AWS CloudHSM Konsole bietet Ihnen nicht die Möglichkeit, Ihren Cluster zu erstellen, zu beenden oder wiederherzustellen. Um diese Dinge zu tun, reichen Sie den Änderungstyp Management | Andere | Andere | Änderungstyp erstellen (ct-1e1xtak34nx76) ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung in meinem AMS-Konto? AWS CloudHSM

Sie müssen TCP-Verkehr über Port 2225 über eine EC2 Amazon-Client-Instance innerhalb einer VPC zulassen oder Direct Connect VPN für lokale Server verwenden, die auf den HSM-Cluster zugreifen möchten. AWS CloudHSM ist in Bezug auf Sicherheitsgruppen und Netzwerkschnittstellen von Amazon EC2 abhängig. Für die Überwachung oder Prüfung von Protokollen stützt sich HSM auf CloudTrail (AWS API-Operationen) und CloudWatch Protokolle für alle lokalen HSM-Geräteaktivitäten.

F: Wer installiert Updates für den AWS CloudHSM Client und die zugehörigen Softwarebibliotheken?

Sie sind für die Installation der Bibliotheks- und Client-Updates verantwortlich. Sie sollten die Seite mit dem [Versionsverlauf von CloudHSM](#) auf Releases überprüfen und dann Updates mithilfe des [CloudHSM-Client-Upgrades](#) anwenden.

 Note

Software-Patches für die HSM-Appliance werden vom Service immer automatisch angewendet. AWS CloudHSM

Verwenden Sie AMS SSP zur Bereitstellung AWS CodeBuild in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodeBuild Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CodeBuild ist ein vollständig

verwalteter Continuous Integration Service, der Quellcode kompiliert, Tests durchführt und Softwarepakete erstellt, die sofort einsatzbereit sind. Mit CodeBuild müssen Sie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in einer Warteschlange warten müssen. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen. Mit CodeBuild werden Ihnen die von Ihnen genutzten Rechenressourcen minutengenau berechnet. Weitere Informationen hierzu finden Sie unter [AWS CodeBuild](#).

Note

Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Services an:, und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen,, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

CodeBuild in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS CodeBuild auf mein AMS-Konto?

Die Nutzung von AWS CodeBuild in Ihrem AMS-Konto erfolgt in zwei Schritten:

1. Bereitstellung des CodeBuild Service Role For-Build-Prozesses zur Koordination mit AWS S3-Buckets, Amazon CloudWatch und Log-Gruppen
2. Fordern Sie Zugriff auf die Konsole an CodeBuild

Sie können beantragen, dass beide in Ihrem AMS-Konto eingerichtet werden, indem Sie einen RFC an Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen senden (ct-1w8z66n899dct). Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS CodeBuild in meinem AMS-Konto?

Für den Zugriff auf AWS CodeBuild Konsolenadministratoren sind die Berechtigungen auf Ressourcenebene beschränkt. CloudWatch Aktionen sind beispielsweise auf bestimmte Ressourcen beschränkt und die `iam:PassRole` Berechtigungen werden kontrolliert.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CodeBuild in meinem AMS-Konto?

Wenn zusätzliche IAM-Berechtigungen für die definierte AWS CodeBuild Servicerolle erforderlich sind, fordern Sie diese über eine AMS-Serviceanfrage an.

Verwenden Sie AMS SSP zur Bereitstellung AWS CodeCommit in Ihrem AMS-Konto

Note

AWS hat mit Wirkung zum 25. Juli 2024 den AWS CodeCommit Zugang für Neukunden geschlossen. AWS CodeCommit Bestandskunden können den Service weiterhin wie gewohnt nutzen. AWS investiert weiterhin in Sicherheit, Verfügbarkeit und Leistungsverbesserungen für AWS CodeCommit, aber wir haben nicht vor, neue Funktionen einzuführen.

Wenn Sie CodeCommit AWS-Git-Repositorys zu anderen Git-Anbietern migrieren möchten, wenden Sie sich an Ihren Cloud-Architekten (CA). Weitere Informationen zur Migration Ihrer Git-Repositorys finden Sie unter [So migrieren Sie Ihr CodeCommit AWS-Repository zu einem anderen Git-Anbieter](#).

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodeCommit Funktionen in Ihrem AMS-verwalteten Konto zuzugreifen. AWS CodeCommit ist ein vollständig verwalteter [Quellcodeverwaltungsdienst](#), der sichere Git-basierte Repositorys hostet. Er hilft Teams bei der Zusammenarbeit an Code in einem sicheren und hoch skalierbaren Ökosystem. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen. Sie können damit alles CodeCommit , vom Quellcode bis hin zu Binärdateien, sicher speichern und es funktioniert nahtlos mit Ihren vorhandenen Git-Tools. Weitere Informationen hierzu finden Sie unter [AWS CodeCommit](#).

Note

Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-

provisioned service | Add (review required) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Services an: und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

CodeCommit in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CodeCommit in meinem AMS-Konto?

AWS CodeCommit Konsolen- und Datenzugriffsrollen können beantragt werden, indem zwei AWS Dienste RFCs, Konsolenzugriff und Datenzugriff eingereicht werden:

- Beantragen Sie den Zugriff auf, AWS CodeCommit indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_codecommit_console_role` Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Für den Datenzugriff (z. B. für Trainings- und Entitätslisten) ist CTs für jede Datenquelle eine separate Angabe der S3-Datenquelle (verpflichtend), des Ausgabe-Buckets (verpflichtend) und des KMS (optional) erforderlich. Es gibt keine Einschränkungen bei der Schaffung von AWS CodeCommit Arbeitsplätzen, solange allen Datenquellen Zugriffsrollen gewährt wurden. Um Datenzugriff zu beantragen, reichen Sie einen RFC bei Management | Other | Other | Create (ct-1e1xtak34nx76) ein.

F: Welche Einschränkungen gelten für die Nutzung in meinem AMS-Konto? AWS CodeCommit

Die aktivierte CodeCommit Trigger-Funktion ist aufgrund der damit verbundenen Rechte zum Erstellen von SNS-Themen deaktiviert. Die direkte Authentifizierung gegen CodeCommit ist eingeschränkt. Benutzer sollten sich mit Credential Helper authentifizieren. Einige KMS-Befehle sind ebenfalls eingeschränkt: `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenerateDataKey`, `kms:GenerateDataKeyWithoutPlaintext` und `kms:DescribeKey`

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS CodeCommit in meinem AMS-Konto?

Wenn S3-Buckets mit KMS-Schlüsseln verschlüsselt sind, müssen S3 und KMS verwendet AWS CodeCommit werden.

Verwenden Sie AMS SSP zur Bereitstellung AWS CodeDeploy in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodeDeploy Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CodeDeploy ist ein vollständig verwalteter Bereitstellungsservice, der Softwarebereitstellungen für eine Vielzahl von Rechendiensten wie Amazon EC2, AWS Fargate AWS Lambda, und Ihren lokalen Servern automatisiert. AWS CodeDeploy unterstützt Sie bei der schnellen Veröffentlichung neuer Funktionen, hilft Ihnen, Ausfallzeiten bei der Anwendungsbereitstellung zu vermeiden, und bewältigt die Komplexität der Aktualisierung Ihrer Anwendungen. Sie können AWS CodeDeploy damit Softwarebereitstellungen automatisieren, sodass fehleranfällige manuelle Operationen überflüssig werden. Der Service lässt sich an Ihre Bereitstellungsanforderungen anpassen. Weitere Informationen hierzu finden Sie unter [AWS CodeDeploy](#).

Note

Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Services an: und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

CodeDeploy in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CodeDeploy in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, CodeDeploy indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_codedeploy_console_role` Konto `customer_codedeploy_service_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer_codedeploy_console_role` Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung CodeDeploy in meinem AMS-Konto?

Derzeit unterstützen wir Compute Platform nur als — Amazon EC2 /On-Premises. Blue/Green Bereitstellungen werden nicht unterstützt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CodeDeploy in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung CodeDeploy in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS CodePipeline in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodePipeline Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CodePipeline ist ein vollständig verwalteter [Continuous Delivery](#) Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses bei jeder Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells. Auf diese Weise können Sie Funktionen und Updates schnell und zuverlässig bereitstellen. Sie können problemlos Dienste von Drittanbietern wie GitHub oder Ihr eigenes benutzerdefiniertes Plugin integrieren AWS CodePipeline . Mit zahlen Sie nur für das AWS CodePipeline, was Sie nutzen. Es fallen keine Vorausleistungen an und Sie gehen keine langfristigen Verpflichtungen ein. Weitere Informationen hierzu finden Sie unter [AWS CodePipeline](#).

Note

Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Dienste an:, und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen,, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren. CodePipeline in AMS unterstützt „Amazon CloudWatch Events“ für Source Stage nicht, da für die Erstellung der Servicerolle und -richtlinie erweiterte Berechtigungen erforderlich sind,

wodurch das Modell mit den geringsten Rechten und der AMS-Change-Management-Prozess umgangen werden.

CodePipeline in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CodePipeline in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, CodePipeline indem Sie eine Serviceanfrage für das `customer_code_pipeline_console_role` entsprechende Konto einreichen. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Zu diesem Zeitpunkt wird AMS Operations diese Servicerolle auch in Ihrem Konto bereitstellen: `aws_code_pipeline_service_role_policy`.

F: Welche Einschränkungen gelten für die Nutzung CodePipeline in meinem AMS-Konto?

Ja. CodePipeline Funktionen, Stufen und Anbieter sind auf Folgendes beschränkt:

1. Bereitstellungsphase: Beschränkt auf Amazon S3 und AWS CodeDeploy
2. Source Stage: Beschränkt auf Amazon S3 AWS CodeCommit, BitBucket, und GitHub
3. Build-Phase: Beschränkt auf AWS CodeBuild, und Jenkins
4. Genehmigungsphase: Beschränkt auf Amazon SNS
5. Testphase: Beschränkt auf Jenkins AWS CodeBuild BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load und Runscope API-Überwachung
6. Invoke Stage: Beschränkt auf Step-Funktionen und Lambda

Note

AMS Operations wird `customer_code_pipeline_lambda_policy` in Ihrem Konto bereitgestellt. Es muss mit der Lambda-Ausführungsrolle für die Lambda-Aufrufphase verknüpft sein. Bitte geben Sie den service/execution Lambda-Rollenamen an, mit dem Sie diese Richtlinie hinzufügen möchten. Wenn es keine benutzerdefinierte service/execution Lambda-Rolle gibt, erstellt AMS eine neue Rolle mit dem Namen `customer_code_pipeline_lambda_execution_role`, bei der es sich um eine Kopie von `customer_lambda_basic_execution_role` zusammen mit `customer_code_pipeline_lambda_policy` handelt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CodePipeline in meinem AMS-Konto?

AWS unterstützte Dienste AWS CodeCommit AWS CodeDeploy müssen vor oder zusammen mit dem Start von gestartet werden CodePipeline. AWS CodeBuild

Verwenden Sie AMS SSP zur Bereitstellung AWS Compute Optimizer in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Compute Optimizer Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Compute Optimizer empfiehlt optimale AWS Rechenressourcen für Ihre Workloads, um Kosten zu senken und die Leistung zu verbessern, indem maschinelles Lernen zur Analyse historischer Nutzungskennzahlen verwendet wird. Eine übermäßige Bereitstellung von Rechenleistung (Amazon EC2 und ASGs) kann zu unnötigen Infrastrukturkosten führen, und eine unzureichende Bereitstellung von Rechenleistung kann zu einer schlechten Anwendungsleistung führen. Compute Optimizer hilft Ihnen bei der Auswahl der optimalen EC2 Amazon-Instance-Typen, einschließlich derer, die Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe sind, basierend auf Ihren Nutzungsdaten. Weitere Informationen hierzu finden Sie unter [AWS Compute Optimizer](#).

Häufig gestellte Fragen zu Compute Optimizer in AWS Managed Services

F: Wie beantrage ich Zugriff auf Compute Optimizer in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem customer_compute_optimizer_readonly_role Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von Compute Optimizer in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von AWS Compute Optimizer ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Compute Optimizer in meinem AMS-Konto?

- Sie müssen einen RFC (Management | Other | Other | Update) einreichen, mit dem AMS Ops autorisiert wird, den Dienst in dem Konto zu aktivieren. Während der Bereitstellung wird eine Service Linked Role (SLR) erstellt, um die Erfassung von Metriken und die Generierung von Berichten zu ermöglichen. Die Spiegelreflexkamera trägt die Bezeichnung ""AWSServiceRoleForComputeOptimizer. Weitere Informationen finden Sie unter [Verwenden von dienstverknüpften Rollen](#) für AWS Compute Optimizer
- CloudWatch Metriken müssen für die folgenden Metriken aktiviert sein:
 - CPU-Auslastung: Der Prozentsatz der zugewiesenen EC2 Amazon-Recheneinheiten, die auf der Instance verwendet werden. Diese Metrik identifiziert die Rechenleistung, die zum Ausführen einer Anwendung auf einer ausgewählten Instance erforderlich ist.
 - Speicherauslastung: Die Speichermenge, die während des Probenahmezeitraums auf irgendeine Weise genutzt wurde. Diese Metrik identifiziert den Arbeitsspeicher, der für die Ausführung einer Anwendung auf einer ausgewählten Instanz erforderlich ist. Die Speicherauslastung wird nur für Ressourcen analysiert, auf denen der Unified CloudWatch Agent installiert ist. Weitere Informationen finden Sie unter Aktivieren der Speicherauslastung mit dem CloudWatch Agenten (S. 10).
 - Netzwerkeingang: Die Anzahl der Byte, die von der Instance auf allen Netzwerkschnittstellen empfangen wurden. Diese Metrik identifiziert das Volumen des eingehenden Netzwerkverkehrs zu einer einzelnen Instance.
 - Netzwerkausgang: Die Anzahl der Byte, die von der Instance an alle Netzwerkschnittstellen gesendet wurden. Diese Metrik identifiziert das Volumen des ausgehenden Netzwerkverkehrs von einer einzelnen Instance.
 - Lokales Laufwerk input/output (I/O): Die Anzahl der input/output Operationen für das lokale Laufwerk. Diese Metrik identifiziert die Leistung des Root-Volumes einer Instance

Verwenden Sie AMS SSP zur Bereitstellung AWS DataSync in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS DataSync Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS DataSync verschiebt große Datenmengen online zwischen lokalem Speicher und Amazon S3, Amazon Elastic File System (Amazon Elastic File System) oder Amazon FSx. Manuelle Aufgaben im Zusammenhang mit Datenübertragungen können Migrationen verlangsamen und den IT-Betrieb belasten. DataSync macht viele dieser Aufgaben überflüssig oder erledigt sie automatisch, darunter die Erstellung von Skripten, die Planung und Überwachung von Übertragungen, die Validierung von Daten und die

Optimierung der Netzwerkauslastung. Der DataSync Software-Agent stellt eine Verbindung zu Ihrem Network File System (NFS) und Server Message Block (SMB) -Speicher her, sodass Sie Ihre Anwendungen nicht ändern müssen. DataSync kann Hunderte von Terabyte und Millionen von Dateien mit Geschwindigkeiten übertragen, die bis zu zehnmal schneller sind als Open-Source-Tools, über das Internet oder über Links. AWS Direct Connect Sie können DataSync damit aktive Datensätze oder Archive in die Cloud migrieren AWS, Daten zur zeitnahen Analyse und Verarbeitung in die Cloud übertragen oder Daten replizieren, um die Geschäftskontinuität zu AWS gewährleisten.

Weitere Informationen hierzu finden Sie unter [AWS DataSync](#).

DataSync in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf DataSync in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_datasync_console_role` Konto die folgende IAM-Rolle zur Verfügung:.

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Die CloudWatch Protokollgruppe, die zum Streamen von Aufgabenprotokollen verwendet werden soll, ist „/aws/datasync“.

F: Welche Einschränkungen gelten für die Nutzung DataSync in meinem AMS-Konto?

Die volle Funktionalität von AWS DataSync ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung DataSync in meinem AMS-Konto?

- Amazon S3 ARNs (Amazon Resource Names) sind für alle S3-Buckets erforderlich, die mit DataSync Aufgaben verknüpft sind, die mithilfe der DataSync Service-Rolle `customer_datasync_service_role` ausgeführt werden.
- VPC-Endpunkte und Sicherheitsgruppen für DataSync Agenten müssen vor der Verwendung von VPC-Endpunkten mit einem RFC mit dem Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) angefordert werden.
- AWS DataSync Agenten werden in AMS als Appliance ausgeführt. Der AWS DataSync Agent wird vom Service gepatcht und aktualisiert. Einzelheiten finden Sie in den [AWS DataSync häufig gestellten Fragen](#).

- Um einen AWS DataSync Agenten zu starten, reichen Sie einen RFC mit dem Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) ein und fordern Sie die Bereitstellung des Agenten an. Geben Sie die AWS DataSync Amazon EC2 AMI-ID, den Instance-Typ, das Subnetz und die Sicherheitsgruppe an und verweisen Sie entweder auf ein vorhandenes EC2 Amazon-Schlüsselpaar oder fordern Sie die Erstellung eines neuen Schlüsselpaars an.

 Note

AMS stellt den AWS DataSync Agenten manuell im Namen des Kunden bereit und benötigt den WIGS-Aufnahmeprozess auf dem AWS DataSync Amazon AMI nicht. EC2

Verwenden Sie AMS SSP zur Bereitstellung AWS Device Farm in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Device Farm Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Device Farm ist ein Service zum Testen von Anwendungen, mit dem Sie die Qualität Ihrer Web- und mobilen Apps verbessern können, indem Sie sie mit einer Vielzahl von Desktop-Browsern und echten Mobilgeräten testen, ohne eine Testinfrastruktur bereitstellen und verwalten zu müssen. Der Dienst ermöglicht es Ihnen, Ihre Tests gleichzeitig auf mehreren Desktop-Browsern oder realen Geräten auszuführen, um die Ausführung Ihrer Testsuite zu beschleunigen, und generiert Videos und Protokolle, mit denen Sie Probleme mit Ihrer App schnell identifizieren können.

Weitere Informationen hierzu finden Sie unter [AWS Device Farm](#).

AWS Device Farm in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Device Farm in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_devicefarm_role` Konto die folgende IAM-Rolle zur Verfügung:

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Device Farm in meinem AMS-Konto?

Vollzugriff auf den AWS Device Farm Service ist möglich, mit Ausnahme der Verwendung des AMS-Namespace im Tag „Name“.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Device Farm in meinem AMS-Konto?

Keine.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elastic Disaster Recovery in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elastic Disaster Recovery Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elastic Disaster Recovery minimiert Ausfallzeiten und Datenverluste durch schnelle, zuverlässige Wiederherstellung von lokalen und cloudbasierten Anwendungen mit erschwinglichem Speicher, minimalem Rechenaufwand und minimaler Wiederherstellung. point-in-time Sie können die IT-Resilienz erhöhen, wenn Sie AWS Elastic Disaster Recovery lokale oder cloudbasierte Anwendungen replizieren, die auf unterstützten Betriebssystemen ausgeführt werden. Verwenden Sie den AWS-Managementkonsole , um Replikations- und Starteinstellungen zu konfigurieren, die Datenreplikation zu überwachen und Instanzen für Drills oder Recovery zu starten.

Weitere Informationen hierzu finden Sie unter [AWS Elastic Disaster Recovery](#).

AWS Elastic Disaster Recovery in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Elastic Disaster Recovery in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem customer_drs_console_role Konto die folgende IAM-Rolle zur Verfügung:

Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Elastic Disaster Recovery in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Nutzung AWS Elastic Disaster Recovery in Ihrem AMS-Konto.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Elastic Disaster Recovery in meinem AMS-Konto?

- Nachdem Sie Zugriff auf die Konsolenrolle haben, müssen Sie den Elastic Disaster Recovery-Dienst initialisieren, um die erforderlichen IAM-Rollen innerhalb des Kontos zu erstellen.

- Sie müssen den Änderungstyp Verwaltung | Anwendungen | IAM-Instanzprofil | Create (Überprüfung erforderlich) Change Type ct-0ixp4ch2tiu04 RFC einreichen, um einen Klon des Instance-Profils zu erstellen und die Richtlinie anzuhängen. `customer-mc-ec2-instance-profile AWSElasticDisasterRecoveryEc2InstancePolicy` Sie müssen angeben, an welche Computer die neue Richtlinie angehängt werden soll.
- Wenn die Instanz nicht das Standard-Instanzprofil verwendet, kann AMS die Verbindung `AWSElasticDisasterRecoveryEc2InstancePolicy` durch Automatisierung herstellen.
- Für die kontoübergreifende Wiederherstellung müssen Sie einen kundeneigenen KMS-Schlüssel verwenden. Der KMS-Schlüssel des Quellkontos muss gemäß der Richtlinie aktualisiert werden, um den Zugriff auf das Zielkonto zu ermöglichen. Weitere Informationen finden Sie unter [Teilen des EBS-Verschlüsselungsschlüssels mit dem Zielkonto](#).
- Die KMS-Schlüsselrichtlinie muss aktualisiert werden, damit der `customer_drs_console_role` Benutzer die Richtlinie einsehen kann, wenn Sie nicht zwischen den Rollen wechseln möchten.
- Für die konto- und regionsübergreifende Notfallwiederherstellung muss AMS das Quell - und das Zielkonto als vertrauenswürdige Konten einrichten und die Rollen Failback und In-Right-Sizing über [bereitstellen AWS](#) . CloudFormation

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaConvert in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaConvert Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaConvert ist ein dateibasierter Videotranskodierungsdienst mit Funktionen in Broadcast-Qualität. Damit können Sie video-on-demand (VOD) -Inhalte für die Übertragung und die Übertragung auf mehreren Bildschirmen in großem Maßstab erstellen. Der Service kombiniert erweiterte Video- und Audiofunktionen mit einer einfachen Webservice-Oberfläche und pay-as-you-go Preisgestaltung. Mit AWS Elemental MediaConvert können Sie sich auf die Bereitstellung überzeugender Medienerlebnisse konzentrieren, ohne sich Gedanken über die Komplexität des Aufbaus und Betriebs Ihrer eigenen Videoverarbeitungsinfrastruktur machen zu müssen.

Weitere Informationen hierzu finden Sie unter [AWS Elemental MediaConvert](#).

MediaConvert in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaConvert in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem customer_mediaconvert_author_role Konto die folgende IAM-Rolle zur Verfügung: Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Es wird eine zweite Rolle bereitgestellt customer_MediaConvert_Default_Role, die von verwendet wird, um aus dem S3-Quell-Bucket zu lesen und die Ausgabe MediaConvert in den S3-Ziel-Bucket zu schreiben sowie das API-Gateway aufzurufen, falls Sie Digital Rights Management (DRM) benötigen.

F: Welche Einschränkungen gelten für die Nutzung MediaConvert in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaConvert in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaConvert in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaConvert in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaLive in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaLive Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaLive ist ein Dienst zur Live-Videoverarbeitung in Rundfunkqualität. Damit können Sie hochwertige Videostreams für die Übertragung auf Fernsehgeräten und mit dem Internet verbundene Multiscreen-Geräte wie Tablets TVs, Smartphones und Set-Top-Boxen erstellen. Der Dienst kodiert Ihre Live-Videostreams in Echtzeit, verwendet eine größere Live-Videoquelle und komprimiert sie in kleinere Versionen, um sie an Ihre Zuschauer zu verteilen. Mit AWS Elemental MediaLive können Sie ganz einfach Streams sowohl für Live-Events als auch für Rund-um-die-Uhr-Kanäle mit erweiterten Übertragungsfunktionen, hoher Verfügbarkeit und Preisgestaltung einrichten. pay-as-you-go AWS Elemental MediaLive ermöglicht es Ihnen, sich darauf zu konzentrieren, überzeugende Live-Videoerlebnisse für Ihre Zuschauer zu schaffen, ohne die Komplexität des Aufbaus und Betriebs einer Videoverarbeitungsinfrastruktur in Sendequalität.

Weitere Informationen hierzu finden Sie unter [AWS Elemental MediaLive](#).

MediaLive in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaLive in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_medialive_author_role` Konto die folgende IAM-Rolle zur Verfügung:

Im Rahmen dieses RFC wird Ihrem Konto eine zweite Rolle zugewiesen. Diese `customer_medialive_service_role` Rolle kann Ihren Media Live-Kanälen und Eingaben zugewiesen werden, um mit anderen Diensten wie Amazon S3 und CloudWatch Logs zu interagieren. MediaStore

Nachdem die Rollen in Ihrem Konto bereitgestellt wurden, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung MediaLive in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaLive in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaLive in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaLive in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaPackage in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaPackage Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaPackage bereitet Ihr Video zuverlässig für die Übertragung über das Internet vor und schützt es. AWS Elemental MediaPackage Erstellt aus einem einzigen Videoeingang Videostreams, die für die Wiedergabe auf verbundenen Mobiltelefonen TVs, Computern, Tablets und Spielekonsolen formatiert sind. Es macht es einfach, beliebte Videofunktionen für Zuschauer (Start, Pause, Rücklauf usw.) zu implementieren, wie sie häufig auf zu finden sind. DVRs AWS Elemental MediaPackage kann Ihre Inhalte auch mithilfe von Digital Rights Management (DRM) schützen. AWS Elemental MediaPackage skaliert automatisch als Reaktion auf die Auslastung, sodass Ihre Zuschauer immer ein großartiges Erlebnis haben, ohne dass Sie im Voraus genau vorhersagen müssen, wie viel Kapazität Sie benötigen.

Weitere Informationen hierzu finden Sie unter [AWS Elemental MediaPackage](#).

MediaPackage in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Elemental MediaPackage in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_mediapackage_author_role` Konto die folgende IAM-Rolle zur Verfügung: Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Eine zweite Rolle wird bereitgestellt `customer_mediapackage_service_role`, die Ihren Media Live-Kanälen und -Eingängen zugewiesen werden kann, um mit anderen Diensten wie S3 und Secrets Manager zu interagieren.

F: Welche Einschränkungen gelten für die Nutzung MediaPackage in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaPackage in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaPackage in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaPackage in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaStore in Ihrem AMS-Konto

Note

AWS Hat nach reiflicher Überlegung die Entscheidung getroffen MediaStore, das Unternehmen mit Wirkung zum 13. November 2025 einzustellen. Wenn Sie ein aktiver Kunde von sind MediaStore, können Sie den Service bis zum 13. November 2025 MediaStore wie gewohnt nutzen. Dann endet der Support für den Service. Nach diesem Datum können Sie keine der Funktionen dieses Dienstes mehr nutzen MediaStore .

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaStore Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental

MediaStore ist ein für Medien optimierter AWS Speicherdienst. Er bietet Ihnen die Leistung, Konsistenz und geringe Latenz, die für die Bereitstellung von Live-Streaming-Videoinhalten erforderlich sind. AWS Elemental MediaStore fungiert als Ursprungsspeicher in Ihrem Video-Workflow. Seine hohen Leistungsfähigkeiten erfüllen die Anforderungen der anspruchsvollsten Workloads für die Medienbereitstellung in Kombination mit langfristiger, kostengünstiger Speicherung. Weitere Informationen hierzu finden Sie unter [AWS Elemental MediaStore](#).

MediaStore in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaStore in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, MediaStore indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_mediastore_author_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung: Als Teil dieses RFC wird eine zweite Rolle in Ihrem Konto bereitgestellt, eine `MediaStoreAccessLogs` Rolle, die vom MediaStore Dienst zur Anmeldung von Aktivitäten verwendet wird CloudWatch, sofern Sie diese Funktion aktivieren. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Zu diesem Zeitpunkt wird AMS Operations diese Servicerolle auch in Ihrem Konto bereitstellen: `aws_code_pipeline_service_role_policy`.

F: Welche Einschränkungen gelten für die Nutzung MediaStore in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaStore in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaStore in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaStore in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaTailor in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaTailor Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaTailor ermöglicht es Videoanbietern, individuell zugeschnittene Werbung in ihre Videostreams einzufügen, ohne dabei Abstriche bei der Übertragungsqualität machen zu müssen. `quality-of-service`

Mit AWS Elemental MediaTailor erhalten die Zuschauer Ihres Live- oder On-Demand-Videos jeweils einen Stream, der Ihre Inhalte mit auf sie personalisierten Anzeigen kombiniert. Im Gegensatz zu anderen personalisierten Werbelösungen wird AWS Elemental MediaTailor Ihr gesamter Stream — Video und Werbung — jedoch in sendegerechter Videoqualität geliefert, um das Erlebnis für Ihre Zuschauer zu verbessern. AWS Elemental MediaTailor bietet automatisierte Berichte, die sowohl auf kunden- als auch auf serverseitigen Kennzahlen zur Anzeigenbereitstellung basieren, um Werbeimpressionen und Zuschauerverhalten genau zu messen. Sie können unerwartete, stark nachgefragte Zuschauerereignisse ganz einfach monetarisieren, ohne dass Vorabkosten anfallen. AWS Elemental MediaTailor Es verbessert auch die Anzeigenbereitstellungsraten, sodass Sie mit jedem Video mehr Geld verdienen können, und es funktioniert mit einer Vielzahl von Netzwerken zur Inhaltsbereitstellung, Anzeigenentscheidungsservern und Client-Geräten.

Weitere Informationen hierzu finden Sie unter [AWS Elemental MediaTailor](#).

MediaTailor in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaTailor in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, MediaTailor indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer-mediatailor-role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung MediaTailor in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaTailor in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaTailor in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaTailor in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Global Accelerator in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Global Accelerator zuzugreifen. Global Accelerator ist ein

Service auf Netzwerkebene, mit dem Sie Beschleuniger erstellen, um die Verfügbarkeit und Leistung von Internetanwendungen zu verbessern, die von einem globalen Publikum verwendet werden. Weitere Informationen finden Sie unter [Global Accelerator](#).

Häufig gestellte Fragen zu Global Accelerator in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich die Einrichtung von Global Accelerator in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den AWS Services-RFC (Management | AWS Service | Self-Provisioned Service) einreichen. Über diesen RFC werden die folgenden IAM-Rollen in Ihrem Konto bereitgestellt: `customer_global_accelerator_console_role`. Nach der Bereitstellung in Ihrem Konto müssen Sie die Konsolenrolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Global Accelerator in meinem AMS-Konto?

Global Accelerator ist ein globaler Service, der Endgeräte in mehreren AWS Regionen unterstützt, die in der [AWS Regionentabelle](#) aufgeführt sind.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Global Accelerator in meinem AMS-Konto?

Wenn Sie Ihren Accelerator mit Global Accelerator einrichten, ordnen Sie die statischen IP-Adressen regionalen Endpunkten in einer oder mehreren AWS Regionen zu. Bei Standardbeschleunigern sind die Endpunkte Network Load Balancers, Application Load Balancers, EC2 Amazon-Instances oder Elastic IP-Adressen. Bei benutzerdefinierten Routing-Beschleunigern sind Endpunkte Virtual Private Cloud (VPC) -Subnetze mit einer oder mehreren Instanzen. EC2

Verwenden Sie AMS SSP zur Bereitstellung AWS Glue in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Glue Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Glue ist ein vollständig verwalteter ETL-Service (Extrahieren, Transformieren und Laden), mit dem Sie Ihre Daten für Analysen vorbereiten und laden können. Sie können einen ETL-Job mit ein paar Klicks in der erstellen und ausführen AWS-Managementkonsole. Sie zeigen AWS Glue auf Ihre Daten, die auf gespeichert sind AWS, AWS Glue und entdecken Ihre Daten und speichern die zugehörigen Metadaten (z. B. Tabellendefinition und Schema) im AWS Glue Data Catalog. Nach der Katalogisierung sind Ihre Daten sofort durchsuchbar, abfragbar und für ETL-Aktionen verfügbar. Weitere Informationen hierzu finden Sie unter [AWS Glue](#).

AWS Glue in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS Glue die Einrichtung in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Glue indem Sie einen RFC mit dem Management | AWS-Service | Selbstbereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:

- `customer_glue_console_role`
- `customer_glue_service_role`

Zu den vorherigen Rollen gehören die folgenden beigefügten Richtlinien:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Nachdem die Rollen in Ihrem Konto bereitgestellt wurden, müssen Sie sie in Ihre Verbundlösung integrieren.

Für den Zugriff auf Crawler-, Jobs- und Entwicklungsendpunkte (Rollen, die für bestimmte Anwendungsfälle benötigt werden), reichen Sie einen RFC mit Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (ct-3dpd8mdd9jn1r) ein.

F: Welche Einschränkungen gelten für die Nutzung in meinem AMS-Konto? AWS Glue

Es gibt keine Einschränkungen. Die volle Funktionalität von AWS Glue ist in Ihrem AMS-Konto verfügbar. Für eine interaktive Umgebung, in der Sie ETL-Skripts erstellen und testen können, verwenden Sie Notebooks on AWS Glue Studio. AWS Glue Interaktive Sitzungen und Job Notebooks sind serverlose Funktionen AWS Glue , die Sie in der AWS Glue Servicerolle verwenden können AWS Glue und die diese nutzen.

AWS Glue vor 2.0: AWS Glue Notebooks sind eine nicht verwaltete Ressource, die EC2 Amazon-Instances in einem Konto startet. Es hat sich bewährt, Ihre eigenen EC2 Amazon-Instances zu starten und die Software zu installieren, die zur Unterstützung einer Notebook-Umgebung und -Entwicklung erforderlich ist. Weitere Informationen finden Sie unter [Tutorial: Einrichten eines lokalen](#)

[Apache Zeppelin-Notebooks zum Testen und Debuggen von ETL-Skripts und Verwenden von Entwicklungsendpunkten für die Entwicklung von Skripts.](#)

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Glue in meinem AMS-Konto?

AWS Glue ist von Amazon S3, CloudWatch, und CloudWatch Logs abhängig. Transitive Abhängigkeiten variieren je nach Datenquelle, und andere AWS Glue Servicefunktionen können miteinander interagieren (Beispiel: Amazon Redshift, Amazon RDS, Athena).

Verwenden Sie AMS SSP zur Bereitstellung AWS Lake Formation in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Lake Formation Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Lake Formation ist ein Service, der es einfach macht, innerhalb weniger Tage einen sicheren Data Lake einzurichten. Ein Data Lake ist ein zentralisiertes, kuratiertes und gesichertes Repository, in dem alle Ihre Daten gespeichert werden, sowohl in seiner ursprünglichen Form als auch für die Analyse vorbereitet. Mit einem Data Lake können Sie Datensilos aufschlüsseln und verschiedene Arten von Analysen kombinieren, um Erkenntnisse zu gewinnen und bessere Geschäftsentscheidungen zu leiten.

Das Erstellen eines Data Lake mit Lake Formation ist so einfach wie das Definieren von Datenquellen und die Datenzugriffs- und Sicherheitsrichtlinien, die Sie anwenden möchten. Lake Formation hilft Ihnen dann, Daten aus Datenbanken und Objektspeicher zu sammeln und zu katalogisieren, die Daten in Ihren neuen Amazon S3-Data Lake zu verschieben, Ihre Daten mithilfe von Algorithmen für Machine Learning zu bereinigen und zu klassifizieren und den sicheren Zugriff auf Ihre sensiblen Daten zu sichern. Ihre Benutzer können auf einen zentralen Datenkatalog zugreifen (Einzelheiten finden Sie in den [AWS Glue häufig gestellten Fragen](#)), in dem die verfügbaren Datensätze und ihre entsprechende Verwendung beschrieben werden. Ihre Benutzer nutzen diese Datensätze dann mit Analyse- und Machine-Learning-Diensten ihrer Wahl, wie [Amazon Redshift](#), [Amazon Athena](#) und (in der Betaversion) [Amazon EMR](#) für Apache Spark. Lake Formation baut auf den Funktionen auf, die in verfügbar sind [AWS Glue](#).

Weitere Informationen hierzu finden Sie unter [AWS Lake Formation](#).

Häufig gestellte Fragen zu Lake Formation in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Lake Formation in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem customer_lakeformation_data_analyst_role Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Darüber hinaus sind die folgenden zwei Rollen optional:

- customer_lakeformation_admin_role
- customer_lakeformation_workflow_role

Bei Administratorberechtigungen können Sie wählen, ob Sie die Rolle customer_lakeformation_admin_role als Teil desselben SSPS-Änderungstyps (ct-3qe6io8t6jtny) integrieren möchten.

Wenn Sie Blueprints in der AWS Lake Formation Konsole erstellen möchten, müssen Sie den RFC Management | Other | Other (ct-1e1xtak34nx76) einreichen, um den bereitzustellen. customer_lakeformation_workflow_role Im RFC müssen Sie den S3-Bucket-Namen angeben, wenn der Bucket bei der Erstellung von Blueprints eine Quelle ist. Der S3-Bucket ist anwendbar AWS CloudTrail, wenn der Blueprint-Typ Classic Load Balancer Logs oder Application Load Balancer Logs ist.

F: Welche Einschränkungen gelten für die Nutzung AWS Lake Formation in meinem AMS-Konto?

Die volle Funktionalität von Lake Formation ist in AMS verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Lake Formation in meinem AMS-Konto?

Lake Formation ist in den AWS Glue Dienst integriert, sodass AWS Glue Benutzer nur auf die Datenbanken und Tabellen zugreifen können, für die sie Lake Formation Formation-Berechtigungen haben. Darüber hinaus können AWS Athena- und Amazon Redshift Redshift-Benutzer nur die AWS Glue Datenbanken und Tabellen abfragen, für die sie Lake Formation Formation-Berechtigungen haben.

Verwenden Sie AMS SSP zur Bereitstellung AWS Lambda in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Lambda Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Lambda ermöglicht es Ihnen, Code auszuführen, ohne Server bereitzustellen oder zu verwalten. Sie zahlen nur für die Rechenzeit, die Sie verbrauchen. Es fallen keine Gebühren an, wenn Ihr Code nicht ausgeführt wird. Mit Lambda können Sie Code für praktisch jede Art von Anwendung oder Back-End-Dienst ausführen, und das alles ohne Verwaltungsaufwand. Laden Sie Ihren Code hoch und Lambda kümmert sich um alles, was für die Ausführung und Skalierung Ihres Codes mit hoher Verfügbarkeit erforderlich ist. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS Diensten ausgelöst wird, oder ihn direkt von einer beliebigen Web- oder mobilen App aus aufrufen. Weitere Informationen hierzu finden Sie unter [AWS Lambda](#).

Häufig gestellte Fragen zu Lambda in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Lambda in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_lambda_admin_role` Konto `customer_lambda_basic_execution_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem es in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Lambda in meinem AMS-Konto?

- Eine Lambda-Funktion ist so konzipiert, dass sie von Ereignisquellen aufgerufen wird. Eine Liste der Dienste, die als Lambda-Ereignisquelle verwendet werden können, finden Sie unter [AWS Lambda Mit anderen Diensten verwenden](#). Derzeit sind nicht alle diese Dienste in AMS-Konten verfügbar. Wenn Sie einen Dienst benötigen, der nicht verfügbar ist, arbeiten Sie mit Ihrem AMS CSDM zusammen, um eine Ausnahme einzureichen.
- Standardmäßig stellt Ihnen AMS eine grundlegende Lambda-Initiierungsrolle zur Verfügung, die die `AWSXrayWriteOnlyAccess` Berechtigungen `AWSLambdaBasicExecutionRole` und enthält. Weitere Informationen finden Sie unter [AWS Lambda Initiation Role](#). Wenn Sie zusätzliche Berechtigungen benötigen, z. B. die Möglichkeit, Lambda-Funktionen in Ihrer AMS-VPC bereitzustellen, reichen Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung in meinem AMS-Konto? AWS Lambda

Für den Einstieg gibt es keine Voraussetzungen oder Abhängigkeiten. Abhängig von Ihrem spezifischen Anwendungsfall benötigen Sie jedoch möglicherweise Zugriff auf andere AWS Dienste, um Ereignisquellen zu erstellen, oder zusätzliche Berechtigungen für Ihre Funktion, um verschiedene Aktionen auszuführen. AWS Lambda Wenn zusätzliche Berechtigungen erforderlich sind, reichen Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (review required) ein (Überprüfung erforderlich) (ct-3qe6io8t6jtny).

F: Was muss ich tun, um eine Lambda-Funktion in einem meiner Konten auszuführen?

Verwenden Sie die folgenden Richtlinien, um eine Lambda-Funktion in einem Core-Konto bereitzustellen:

- Stellen Sie sicher, dass SSPS for AWS Lambda integriert ist.
- Es gibt keine spezifischen Einschränkungen, die diese Bereitstellung im Rahmen der AMS-Verantwortlichkeiten verbieten, solange Ihre AMS-Ressourcen geschützt und gesetzeskonform sind.
- Wenn Sie möchten, dass AMS die Lambda-Funktion erstellt, müssen Sie zuerst die dafür vorgesehene SSPS-Rolle verwenden. AWS Lambda Wenn Sie dann weiterhin AMS-Unterstützung bei der Bereitstellung oder Unterstützung der Funktion benötigen, wenden Sie sich an Ihre Zertifizierungsstelle und starten Sie den Out-of-Scope-Prozess (OOS).

Verwenden Sie AMS SSP zur Bereitstellung AWS License Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS License Manager Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS License Manager lässt sich in AWS Services integrieren, um die Verwaltung von Lizenzen für mehrere AWS Konten, IT-Kataloge und lokale Lizenzen über ein einziges Konto zu vereinfachen. AWS AWS License Manager ermöglicht es Administratoren, benutzerdefinierte Lizenzregeln zu erstellen, die die Bedingungen ihrer Lizenzvereinbarungen emulieren, und setzt diese Regeln dann durch, wenn eine Amazon-Instance gestartet EC2 wird. Mit diesen Regeln können Sie Lizenzverstöße einschränken, indem Sie den Start der Instance physisch unterbinden oder Administratoren über den Verstoß informieren. AWS License Manager Weitere Informationen hierzu finden Sie unter [AWS License Manager](#).

Häufig gestellte Fragen zum License Manager in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS License Manager die Einrichtung in meinem AMS-Konto?

Beantragen Sie Zugriff auf, AWS License Manager indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_license_manager_role` Konto die folgende IAM-Rolle zur Verfügung:.. Sobald die IAM-Rolle License Manager in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS License Manager in meinem AMS-Konto?

Sie können AWS License Manager Regeln mit Ihren eigenen verknüpfen (gefiltert unter „Mein Eigentum“). AMIs Wenn Sie sich dafür entscheiden, eine Limit-Zuordnung zu einem AMI zu erzwingen (Beispiel: kann nur 100 vCPUs dieses AMI unterstützen) und das Limit ausschöpfen, werden future Starts mit diesem AMI blockiert und es wird die Fehlermeldung „Keine Lizenzen verfügbar“ zurückgegeben. Dies ist das beabsichtigte Verhalten dieses Dienstes (die Lizenzerschöpfung wird nicht zugelassen). Falls Sie das Limit ausgeschöpft haben, das AMI aber erneut starten müssen, müssen Sie die in konfigurierte Regel ändern AWS License Manager.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS License Manager in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS License Manager in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Migration Hub in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Migration Hub Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Migration Hub bietet einen zentralen Ort, an dem Sie den Fortschritt der Anwendungsmigrationen für mehrere Lösungen und Partnerlösungen verfolgen können. AWS Mithilfe von Migration Hub können Sie die Migrationstools AWS und Partner-Migrationstools auswählen, die Ihren Anforderungen am besten entsprechen, und gleichzeitig einen Überblick über den Status der Migrationen in Ihrem gesamten Anwendungsportfolio erhalten. Migration Hub bietet auch wichtige Kennzahlen und Fortschritte für einzelne Anwendungen, unabhängig davon, welche Tools für die Migration verwendet werden. Auf diese Weise können Sie schnell über den Fortschritt all Ihrer Migrationen informiert werden, Probleme einfach identifizieren

und beheben und den Gesamtzeit- und Arbeitsaufwand für Ihre Migrationsprojekte reduzieren. Weitere Informationen hierzu finden Sie unter [AWS Migration Hub](#).

Häufig gestellte Fragen zu Migration Hub in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Migration Hub in meinem AMS-Konto?

Fordern Sie Zugriff auf Migration Hub an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_migrationhub_author_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen für Migration Hub?

Keine.

F: Was sind die Voraussetzungen für die Aktivierung von Migration Hub?

Es gibt keine Voraussetzungen, um mit der Nutzung von Migration Hub in Ihrem AMS-Konto zu beginnen. Während der Verwaltung des Service sind jedoch möglicherweise Berechtigungen außerhalb von Migration Hub erforderlich, z. B. Schreibberechtigungen für Amazon S3 zum Hochladen von Serverinformationen.

Verwenden Sie AMS SSP zur Bereitstellung AWS Outposts in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Outposts Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, AWS Dienste und Tools auf praktisch jedes Rechenzentrum APIs, jeden Colocation-Bereich oder jede lokale Einrichtung ausdehnt und so für ein einheitliches Hybrid-Erlebnis sorgt. AWS Outposts eignet sich gut für Workloads, die einen Zugriff auf lokale Systeme mit geringer Latenz, lokale Datenverarbeitung oder lokalen Datenspeicher erfordern. Weitere Informationen hierzu finden Sie unter [AWS Outposts](#).

AWS Outposts in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS Outposts die Einrichtung in meinem AMS-Konto?

Beantragen Sie Zugriff auf, AWS Outposts indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_outposts_role` Konto die folgende IAM-Rolle zur Verfügung:.. Sobald die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie sie in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Outposts in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung AWS Outposts in Ihrem AMS-Konto.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Outposts in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Outposts in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Resilience Hub in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Resilience Hub Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Resilience Hub hilft Ihnen dabei, Ihre AWS Anwendungen proaktiv vorzubereiten und vor Störungen zu schützen. Der Resilience Hub bietet Resilienzbeurteilungen und -validierungen, die in Ihren Softwareentwicklungszyklus integriert werden können, um Schwachstellen bei der Ausfallsicherheit aufzudecken. Resilience Hub hilft Ihnen bei der Einschätzung, ob Ihre Anwendungen die Ziele für die Wiederherstellungszeit (RTO) und die Zielvorgaben für den Wiederherstellungspunkt (Recovery Point Objective, RPO) erfüllen können, und hilft Ihnen, Probleme zu lösen, bevor sie in Betrieb genommen werden. Nachdem Sie eine AWS Anwendung in der Produktion bereitgestellt haben, können Sie Resilience Hub verwenden, um die Ausfallsicherheit Ihrer Anwendung weiter zu verfolgen. Wenn ein Ausfall auftritt, sendet Resilience Hub eine Benachrichtigung an den Betreiber, um den zugehörigen Wiederherstellungsprozess zu starten.

AWS Resilience Hub in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Resilience Hub auf mein AMS-Konto?

Beantragen Sie Zugriff auf Resilience Hub, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen und -Richtlinien zur Verfügung:

IAM roles

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Richtlinien

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Nachdem die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle `customer_resiliencehub_console_role` in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Resilience Hub in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Resilience Hub ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Resilience Hub in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von Resilience Hub in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Secrets Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Secrets Manager Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Secrets Manager hilft Ihnen beim Schutz von Geheimnissen, die Sie für den Zugriff auf Ihre Anwendungen, Dienste und IT-Ressourcen benötigen. Mit diesem Service können Sie Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse während ihres gesamten Lebenszyklus problemlos rotieren, verwalten und abrufen. Benutzer und Anwendungen rufen Geheimnisse mit einem Aufruf des Secrets Manager ab APIs, sodass sensible Informationen nicht mehr im Klartext hartcodiert werden müssen. Secrets Manager bietet geheime Rotation mit integrierter Integration für Amazon RDS, Amazon Redshift und Amazon DocumentDB. Der Service ist auch auf andere Arten von Geheimnissen erweiterbar, einschließlich API-Schlüsseln und Tokens. OAuth Weitere Informationen hierzu finden Sie unter [AWS Secrets Manager](#).

 Note

Standardmäßig können AMS-Betreiber auf Geheimnisse zugreifen AWS Secrets Manager , die mit dem AWS KMS Standardschlüssel (CMK) des Kontos verschlüsselt wurden. Wenn Sie möchten, dass AMS Operations nicht auf Ihre Geheimnisse zugreifen kann, verwenden Sie ein benutzerdefiniertes CMK mit einer AWS Key Management Service (AWS KMS) - Schlüsselrichtlinie, die Berechtigungen definiert, die den im Secret gespeicherten Daten entsprechen.

Häufig gestellte Fragen zu Secrets Manager in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Secrets Manager in meinem AMS-Konto?

Fordern Sie Zugriff auf Secrets Manager an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_secrets_manager_console_role` `customer-rotate-secrets-lambda-role` Konto die folgenden IAM-Rollen zur Verfügung: und. Die `customer_secrets_manager_console_role` wird als Admin-Rolle für die Bereitstellung und Verwaltung der Secrets verwendet und `customer-rotate-secrets-lambda-role` wird als Lambda-Ausführungsrolle für die Lambda-Funktionen verwendet, die die Secrets rotieren. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer_secrets_manager_console_role` Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Secrets Manager in meinem AMS-Konto?

Der volle Funktionsumfang von AWS Secrets Manager ist in Ihrem AMS-Konto verfügbar, ebenso wie die automatische Rotation von Geheimnissen. Beachten Sie jedoch, dass das Einrichten Ihrer Rotation mithilfe von „Create a new Lambda function to perform rotation“ nicht unterstützt wird, da für die Erstellung des CloudFormation Stacks erhöhte Berechtigungen erforderlich sind (Erstellung der IAM-Rolle und Lambda-Funktion), wodurch der Change-Management-Prozess umgangen wird. AMS Advanced unterstützt nur „Eine bestehende Lambda-Funktion zur Rotation verwenden“, bei der Sie Ihre Lambda-Funktionen so verwalten, dass Geheimnisse mithilfe der Lambda-SSPS-Admin-Rolle rotiert werden. AWS AMS Advanced erstellt oder verwaltet Lambda nicht, um die Geheimnisse rotieren zu lassen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Secrets Manager in meinem AMS-Konto?

Die folgenden Namespaces sind für AMS reserviert und im Rahmen des direkten Zugriffs auf nicht verfügbar: AWS Secrets Manager

- `arn:aws:secretsmanager: *:secret:ams-shared/*`
- `arn:aws:secretsmanager: *:secret:customer-shared/*`
- `arn:aws:secretsmanager: *:secret:ams/*`

Schlüssel mit Secrets Manager (AMS SSPS) teilen

Die Weitergabe von Geheimnissen an AMS im Klartext eines RFC, einer Serviceanfrage oder eines Vorfallberichts führt zu einem Vorfall mit der Offenlegung von Informationen. AMS löscht diese Informationen aus dem Fall und fordert Sie auf, die Schlüssel neu zu generieren.

Sie können [AWS Secrets Manager](#) (Secrets Manager) unter diesem Namespace verwenden, `customer-shared`.

Häufig gestellte Fragen zum Teilen von Schlüsseln mit Secrets Manager

F: Welche Arten von Geheimnissen müssen mit Secrets Manager geteilt werden?

Einige Beispiele sind vorab genutzte Schlüssel für die VPN-Erstellung, vertrauliche Schlüssel wie Authentifizierungsschlüssel (IAM, SSH), Lizenzschlüssel und Passwörter.

F: Wie kann ich die Schlüssel mithilfe von Secrets Manager mit AMS teilen?

1. Melden Sie sich mit Ihrem Verbundzugriff und der entsprechenden Rolle bei der AWS Management-Konsole an:

für SALZ, das `Customer_ReadOnly_Role`

für MALZ, `AWSManagedServicesChangeManagementRole`.
2. Navigieren Sie zur [AWS Secrets Manager Konsole](#) und klicken Sie auf Neues Geheimnis speichern.
3. Wählen Sie Andere Art von Secrets aus.
4. Geben Sie den geheimen Wert als Klartext ein und verwenden Sie die standardmäßige KMS-Verschlüsselung. Klicken Sie auf Weiter.
5. Geben Sie den geheimen Namen und die Beschreibung ein. Der Name beginnt immer mit `customer-shared/`. Zum Beispiel `customer-shared/mykey2022`. Klicken Sie auf Weiter.

6. Lassen Sie die automatische Rotation deaktiviert und klicken Sie auf Weiter.
7. Überprüfen Sie es und klicken Sie auf Speichern, um das Geheimnis zu speichern.
8. Antworten Sie uns über die Serviceanfrage, den RFC oder den Vorfallbericht mit dem geheimen Namen, damit wir das Geheimnis identifizieren und abrufen können.

F: Welche Berechtigungen sind für die gemeinsame Nutzung der Schlüssel mit Secrets Manager erforderlich?

SALZ: Suchen Sie nach der `customer_secrets_manager_shared_policy` verwalteten IAM-Richtlinie und stellen Sie sicher, dass das Richtliniendokument mit dem Dokument übereinstimmt, das in den folgenden Erstellungsschritten angehängt wurde. Vergewissern Sie sich, dass die Richtlinie den folgenden IAM-Rollen zugeordnet ist: `Customer_ReadOnly_Role`

MALZ: Stellen Sie sicher `AMSSecretsManagerSharedPolicy`, dass der `AWSTransientCacheChangeManagementRole` Rolle, zugeordnet ist, die Ihnen die `GetSecretValue` Aktion im `ams-shared` Namespace ermöglicht.

Beispiel:

```
{
  "Action": "secretsmanager:*",
  "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  ],
  "Effect": "Allow",
  "Sid": "AllowAccessToSharedNameSpaces"
}
```

Note

Die erforderlichen Berechtigungen werden erteilt, wenn Sie einen AWS Secrets Manager als Self-Service bereitgestellten Dienst hinzufügen.

Verwenden Sie AMS SSP zur Bereitstellung AWS Security Hub CSPM in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Security Hub CSPM Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Security Hub CSPM bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und Ihre Einhaltung der Sicherheitsstandards und Best Practices der Sicherheitsbranche. Security Hub zentralisiert und priorisiert Sicherheits- und Compliance-Erkenntnisse aus AWS Konten, Diensten und unterstützten Drittanbietern, um Sie bei der Analyse Ihrer Sicherheitstrends und der Identifizierung der Sicherheitsprobleme mit der höchsten Priorität zu unterstützen. Weitere Informationen hierzu finden Sie unter [AWS Security Hub CSPM](#).

Häufig gestellte Fragen zu Security Hub in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Security Hub CSPM in meinem AMS-Konto?

Fordern Sie Zugriff auf Security Hub an, indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_securityhub_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:.. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Security Hub in meinem AMS-Konto?

Die Archivierungsfunktion wurde als potenzielles Sicherheits- und Betriebsrisiko eingestuft und im Rahmen der Sicherheitsfunktion des selbst bereitgestellten Dienstes eingeschränkt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Security Hub CSPM in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Security Hub CSPM in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Service Catalog AppRegistry in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AppRegistry Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AppRegistry ermöglicht die Anwendungssuche, Berichterstattung und Verwaltungsaktionen von einem zentralen Ort aus. Entwickler erstellen selten Anwendungen in einem einzigen AWS Konto. In der Regel trennen

sie Anwendungsressourcen nach Lebenszyklusphasen wie Entwicklung, Test und Produktion. AppRegistry ermöglicht es Ihnen, all Ihre Ressourcensammlungen in den von Ihnen definierten AWS Konten zu gruppieren und anzuzeigen.

Mit AppRegistry können Sie Ihre AWS Anwendungen, die Sammlung von Ressourcen, die Ihren Anwendungen zugeordnet sind, und Anwendungsattributgruppen speichern. Weitere Informationen finden Sie unter [Was ist AppRegistry](#).

Häufig gestellte Fragen: AWS Service Catalog AppRegistry im AMS

F: Wie beantrage ich Zugriff AWS Service Catalog AppRegistry auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AppRegistry indem Sie einen RFC mit dem Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt `customer-appregistry-console-role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Service Catalog AppRegistry in meinem AMS-Konto?

Der volle Zugriff auf den AppRegistry Dienst wird gewährt, mit Ausnahme der Verwendung des AMS-Namespaces im 'Name' Tag.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Service Catalog AppRegistry in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AppRegistry in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Shield Advanced in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Shield Advanced Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Shield Advanced ist ein verwalteter Service zum Schutz vor verteilten Denial of Service (DDoS), der Anwendungen schützt, auf denen ausgeführt wird. AWS Shield Advanced bietet eine ständig aktive Erkennung und automatische Inline-Abwehrmaßnahmen, die Ausfallzeiten und Latenz von Anwendungen minimieren, sodass Sie nicht den AWS Support in Anspruch nehmen müssen, um vom DDo S-Schutz

zu profitieren. Es gibt zwei Stufen: AWS Shield Standard und Advanced; AMS bietet Shield Advanced an. Weitere Informationen finden Sie unter [Shield Advanced](#).

Alle AWS Kunden profitieren ohne zusätzliche Kosten vom automatischen Schutz von AWS Shield Standard. AWS Shield Standard schützt vor den häufigsten, häufig auftretenden Netzwerk- und DDoS-Transport-Layer-S-Angriffen, die auf Ihre Website oder Anwendungen abzielen. Wenn Sie Amazon CloudFront und Amazon Route 53 verwenden AWS Shield Standard, erhalten Sie umfassenden Verfügbarkeitsschutz vor allen bekannten Infrastrukturangriffen (Layer 3 und 4).

Für einen besseren Schutz vor Angriffen auf Ihre Anwendungen, die auf Ressourcen von Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB) CloudFront AWS Global Accelerator, Amazon und Amazon Route 53 ausgeführt werden, können Sie abonnieren AWS Shield Advanced.

Zusätzlich zu den mitgelieferten Schutz auf Netzwerk- und Transportebene AWS Shield Advanced bietet es zusätzliche Erkennung und Abwehr großer und ausgeklügelter DDoS-Angriffe, Einblicke in Angriffe nahezu in Echtzeit und die Integration mit AWS WAF einer Firewall für Webanwendungen. AWS Shield Standard AWS Shield Advanced bietet Ihnen außerdem rund um die Uhr Zugriff auf das AWS Shield Response Team (SRT) und Schutz vor DDoS-bedingten Spitzen in Ihren Gebühren für Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (Elastic Load Balancing) CloudFront AWS Global Accelerator, Amazon und Amazon Route 53.

Häufig gestellte Fragen zu Shield Advanced in AWS Managed Services

F: Wie beantrage ich Zugriff auf Shield Advanced in meinem AMS-Konto?

Fordern Sie Zugriff auf Shield Advanced an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_shield_role` `aws_drt_shield_role` Konto die folgenden IAM-Rollen zur Verfügung: und. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Nachdem die Rollen in Ihrem Konto bereitgestellt wurden, können Sie sie verwenden, `customer_shield_role` um Ihr Abonnement AWS Shield Advanced in Ihrem Konto zu bestätigen.

Note

Beachten Sie, dass mit der Nutzung von eine monatliche Gebühr und eine einjährige Verpflichtung verbunden sind. AWS Shield Advanced Darüber hinaus berechtigt die Verwendung AWS Shield Advanced in AMS AMS zur Eskalation an den AWS Shield (SRT),

der bei eskalierten Distributed-Denial-of-Service (S) -Vorfällen Änderungen an den Firewall-Regeln (AWS WAF) Ihrer Webanwendung vornehmen kann. DDo Diese Änderungen werden in Abstimmung mit AMS vorgenommen.

F: Welche Einschränkungen gelten für die Nutzung von Shield Advanced in meinem AMS-Konto?

Dies ist zwar keine Einschränkung, Sie sollten sich jedoch darüber im Klaren sein, dass bei Verwendung von Shield Advanced die bereitgestellt wird `aws_drt_shield_role`, sodass AWS Shield Teams (SRT) bei eskalierten DDo S-Vorfällen Notfalländerungen an AWS WAF Regeln innerhalb von AMS-Konten vornehmen können. Dies wird von AMS für die schnellste Behebung von S-Angriffen empfohlen und würde nach einer DDo AMS-Eskalation an das SRT erfolgen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Shield Advanced in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Shield Advanced in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP zur Bereitstellung AWS Snowball Edge in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Snowball Edge-Funktionen zuzugreifen. Snowball Edge ist eine Datentransportlösung im Petabyte-Bereich, die Geräte verwendet, die so konzipiert sind, dass sie sicher sind, um große Datenmengen in die und aus der Cloud zu übertragen. AWS Snowball Edge bewältigt häufig auftretende Herausforderungen im Zusammenhang mit umfangreichen Datenübertragungen, darunter hohe Netzwerkkosten, lange Übertragungszeiten und Sicherheitsbedenken. Sie können Snowball Edge verwenden, um Analysedaten, Genomikdaten, Videobibliotheken, Bildrepositorys und Backups zu migrieren und Teile von Rechenzentrumsabschaltungen, Bandaustauschprojekten oder Anwendungsmigrationsprojekten zu archivieren. Die Übertragung von Daten mit Snowball Edge ist einfach, schnell, sicherer und kann nur ein Fünftel der Kosten für die Übertragung von Daten über Highspeed-Internet kosten.

Mit Snowball Edge müssen Sie keinen Code schreiben oder Hardware kaufen, um Ihre Daten zu übertragen. Verwenden Sie zunächst die AWS Management Console, um [einen Importauftrag für Snowball zu erstellen](#), und ein Snowball-Gerät wird Ihnen automatisch zugeschickt. Sobald es ankommt, schließen Sie das Gerät an Ihr lokales Netzwerk an, laden Sie den Snowball-Client („Client“) herunter und führen Sie ihn aus, um eine Verbindung herzustellen, und wählen Sie dann

mit dem Client die Dateiverzeichnisse aus, die Sie auf das Gerät übertragen möchten. Der Client verschlüsselt dann die Dateien und überträgt sie mit hoher Geschwindigkeit auf das Gerät. Sobald die Übertragung abgeschlossen ist und das Gerät zur Rücksendung bereit ist, wird das E Ink-Versandetikett automatisch aktualisiert und Sie können den Auftragsstatus mit Amazon Simple Notification Service (Amazon SNS), Textnachrichten oder direkt in der Konsole verfolgen. Weitere Informationen hierzu finden Sie unter [AWS Snowball Edge](#).

Häufig gestellte Fragen zu Snowball Edge in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Snowball Edge auf mein AMS-Konto?

Die Implementierung von Snowball Edge in AMS erfolgt in zwei Schritten:

1. Reichen Sie einen Änderungstyp Management | Andere | Andere | Erstellen Sie einen (ct-1e1xtak34nx76) -Änderungstyp und fordern Sie eine Servicerolle für Snowball Edge für Ihr AMS-Konto an.
2. Beantragen Sie Benutzerzugriff, indem Sie die folgenden Optionen einreichen: Verwaltung | AWS Dienst | Selbst bereitgestellter Dienst | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:, und. `customer_snowball_console_role` `customer_snowball_export_role` `customer_snowball_import_role` Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Snowball Edge in meinem AMS-Konto?

Die volle Funktionalität von AWS Snowball Edge ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Snowball Edge in meinem AMS-Konto?

Sie müssen über das oben angegebene Servicerollenkonto verfügen.

Verwenden Sie AMS SSP zur Bereitstellung AWS Step Functions in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Step Functions Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Step Functions ist

ein Webservice, mit dem Sie die Komponenten verteilter Anwendungen und Microservices mithilfe visueller Workflows koordinieren können. Sie erstellen Anwendungen aus einzelnen Komponenten, die jeweils eine diskrete Funktion oder Aufgabe ausführen, sodass Sie Anwendungen schnell skalieren und verändern können. Step Functions bietet eine zuverlässige Möglichkeit, Komponenten zu koordinieren und die Funktionen Ihrer Anwendung Schritt für Schritt durchzugehen. Step Functions bietet eine grafische Konsole, mit der Sie die Komponenten Ihrer Anwendung als eine Reihe von Schritten visualisieren können. Sie löst jeden Schritt automatisch aus, verfolgt ihn und versucht es erneut, wenn Fehler auftreten, sodass Ihre Anwendung jedes Mal in der richtigen Reihenfolge und wie erwartet ausgeführt wird. Step Functions protokolliert den Status jedes Schritts, sodass Sie Probleme schnell diagnostizieren und debuggen können, wenn etwas schief geht. Weitere Informationen hierzu finden Sie unter [AWS Step Functions](#).

Häufig gestellte Fragen zu Step Functions in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Step Functions auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Step Functions indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_step_functions_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Step Functions in meinem AMS-Konto?

Die volle Funktionalität von AWS Step Functions ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Step Functions in meinem AMS-Konto?

Zur Laufzeit muss die von Step Functions verwendete Rolle Zugriff auf die von der Step-Funktion verwendeten Dienste haben. Beispielsweise könnte eine Schrittfunktion von Lambda-Funktionen abhängen. Jemand, der eine Step-Funktion erstellt, erstellt wahrscheinlich gleichzeitig Lambda-Funktionen und müsste auch Zugriff auf diesen Dienst anfordern.

Verwenden Sie AMS SSP, um AWS Systems Manager Parameter Store in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Systems Manager Parameter Store-Funktionen zuzugreifen.

AWS Systems Manager Der Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen. Sie können Daten wie Passwörter, Datenbankzeichenfolgen und Lizenzcodes als Parameterwerte speichern. Sie können Werte als Klartext oder als verschlüsselte Daten speichern. Anschließend können Sie anhand des eindeutigen Namens, den Sie beim Erstellen des Parameters angegeben haben, auf die Werte verweisen. Parameter Store ist hochgradig skalierbar, verfügbar und langlebig und wird von der AWS Cloud unterstützt. Weitere Informationen finden Sie unter [AWS Systems Manager Parameter Store](#).

Note

Wenn Sie einen dedizierten Geheimspeicher mit Lebenszyklusmanagement wünschen, verwenden Sie [Verwenden Sie AMS SSP zur Bereitstellung AWS Secrets Manager in Ihrem AMS-Konto](#) anstelle von Parameter Store. Secrets Manager hilft Ihnen dabei, Ihre Sicherheits- und Compliance-Anforderungen zu erfüllen, indem Sie Secrets automatisch rotieren lassen können. Secrets Manager bietet eine integrierte Integration für MySQL, PostgreSQL und Amazon Aurora auf Amazon RDS, die durch die Anpassung von Lambda-Funktionen auf andere Arten von Geheimnissen erweiterbar ist.

AWS Systems Manager Häufig gestellte Fragen zum Speichern von Parametern in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Systems Manager Parameter Store in meinem AMS-Konto?

Beantragen Sie den Zugriff auf den AWS Systems Manager Parameterspeicher, indem Sie einen RFC an folgende Adresse senden: Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt `customer_systemsmanager_parameterstore_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von AWS Systems Manager Parameter Store in meinem AMS-Konto?

Sie müssen AWS verwaltete Schlüssel verwenden. Der Zugriff ist auf die Erstellung benutzerdefinierter KMS-Schlüssel beschränkt. Wenn jedoch ein benutzerdefinierter Schlüssel

erforderlich ist, reichen Sie einen RFC ein, um einen vom Kunden verwalteten Schlüssel (CMK) zu erstellen. Verwenden Sie dabei Deployment | Advanced Stack Components | KMS-Schlüssel | Änderungstyp erstellen (ct-1d84keiri1jhg) mit dieser IAM-Rolle als Wert für die Parameter und. `customer_systemsmanager_parameterstore_console_role`
`IAMPrincipalsRequiringDecryptPermissions`
`IAMPrincipalsRequiringEncryptPermissionsPrincipal` Nachdem der KMS-Schlüssel erstellt wurde, können Sie damit eine sichere Zeichenfolge erstellen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von AWS Systems Manager Parameter Store in meinem AMS-Konto?

Es gibt keine Voraussetzungen. SSM Parameter Store ist jedoch darauf angewiesen, dass KMS eine sichere Zeichenfolge erstellt, sodass Sie die im Parameter Store gespeicherten Werte ver- und entschlüsseln können.

Verwenden Sie AMS SSP, um AWS Systems Manager Automation in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Systems Manager Automatisierungsfunktionen zuzugreifen.

AWS Systems Manager Die Automatisierung vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von Amazon Elastic Compute Cloud-Instances und anderen AWS Ressourcen mithilfe von Runbooks, Aktionen und Servicekontingenten. Sie ermöglicht es Ihnen, Automatisierungen in großem Umfang zu erstellen, auszuführen und zu überwachen. Eine Systems Manager-Automatisierung ist eine Art von Systems Manager Manager-Dokument, das die Aktionen definiert, die Systems Manager auf Ihren verwalteten Instanzen ausführt. Ein Runbook, mit dem Sie allgemeine Wartungs- und Bereitstellungsaufgaben wie das Ausführen von Befehlen oder Automatisierungsskripten in Ihren verwalteten Instanzen ausführen. Systems Manager umfasst Funktionen, mit denen Sie mithilfe von Amazon Elastic Compute Cloud-Tags auf große Gruppen von Instances abzielen können, sowie Geschwindigkeitssteuerungen, mit denen Sie Änderungen gemäß den von Ihnen definierten Grenzwerten implementieren können. Die Runbooks werden mit JavaScript Object Notation (JSON) oder YAML geschrieben. Mit dem Document Builder in der Systems Manager-Automation-Konsole können Sie jedoch ein Runbook erstellen, ohne nativen JSON- oder YAML-Code erstellen zu müssen. Alternativ können Sie von Systems Manager bereitgestellte Runbooks mit vordefinierten Schritten verwenden, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie in der Dokumentation unter [Arbeiten mit Runbooks](#). AWS Systems Manager

 Note

Systems Manager Automation unterstützt zwar 20 Aktionstypen, die im Runbook verwendet werden können, aber eine begrenzte Anzahl von Aktionen, die Sie beim Erstellen von Runbooks verwenden können, können Sie in Ihrem AMS Advanced-Konto verwenden. Ebenso kann eine begrenzte Anzahl von Runbooks, die von Systems Manager bereitgestellt werden, entweder direkt oder in Ihrem eigenen Runbook verwendet werden. Einzelheiten finden Sie in den folgenden häufig gestellten Fragen zu den Einschränkungen.

AWS Systems Manager Häufig gestellte Fragen zur Automatisierung in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Systems Manager Automation in meinem AMS-Konto?

Beantragen Sie Zugriff auf AWS Systems Manager Automation, indem Sie einen RFC über Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_systemsmanager_automation_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von AWS Systems Manager Automation in meinem AMS-Konto?

Sie müssen Ihr Runbook mit einer begrenzten Anzahl von von Systems Manager unterstützten Aktionen zur Automatisierung nur verfassen, um and/or Befehlsskripts innerhalb Ihrer verwalteten Instanzen auszuführen. Die Aktionen, die Ihnen zur Verfügung stehen, sowie etwaige Einschränkungen werden im Folgenden beschrieben.

AWS Systems Manager Einschränkungen der Automatisierung

Aktion	Beschreibung	Einschränkung
aws: assertAwsResource Eigentum —	Bestätigen Sie einen AWS Ressourcen- oder Ereigniss tatus	Nur EC2 Instanzen

Aktion	Beschreibung	Einschränkung
aws:aws:branch —	Führen Sie bedingte Automatisierungsschritte aus	Keine Einschränkung
AWS: CreateTags —	Tags für Ressourcen erstellen AWS	Nur für SSM-Automatisierungs-Runbooks, die Sie erstellen
AWS: ExecuteAutomation —	Führen Sie eine weitere Automatisierung aus	Nur das Automatisierungs-Runbook, das Sie erstellen
aws:ExecuteScript —	Führen Sie ein Skript aus	Das einzige Skript, das keine API-Aufrufe an Dienste tätigt
aws:pause —	Eine Automatisierung pausieren	Keine Einschränkung
aws:RunCommand —	Führen Sie einen Befehl auf einer verwalteten Instanz aus	Verwenden Sie nur das vom System Manager bereitgestellte Dokument - AWS-RunShellScript und AWS-RunPowerShellScript
aws:sleep —	Eine Automatisierung verzögern	Keine Einschränkung
aws:waitForAwsResourceProperty —	Warte auf eine AWS Ressourceneigenschaft	Nur EC2 Instanzen

Sie können sich auch dafür entscheiden, Befehle oder Skripte direkt mit dem von Systems Manager bereitgestellten Runbook AWS RunShellScript und AWS auszuführen, RunPowerShellScript indem Sie die Funktion „Befehl ausführen“ in der Systems Manager Manager-Konsole verwenden. Sie können diese Runbooks auch in Ihrem Runbook verschachteln, um zusätzliche Prüfungen vor der Nachbearbeitung oder eine komplexe Automatisierungslogik zu and/or ermöglichen.

Die Rolle folgt dem Prinzip der geringsten Rechte und gewährt nur die erforderlichen Berechtigungen zum Verfassen, Ausführen und Abrufen von Ausführungsdetails von Runbooks, die auf die Ausführung von and/or Befehlsskripten in Ihren verwalteten Instances abzielen. Sie gewährt keine

Genehmigung für andere Funktionen, die der AWS Systems Manager Dienst bereitstellt. Mit dieser Funktion können Sie Automatisierungs-Runbooks erstellen, die Ausführung der Runbooks kann jedoch nicht auf AMS-eigene Ressourcen ausgerichtet werden.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von AWS Systems Manager Automation in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Sie müssen jedoch sicherstellen, dass Ihre internen and/or Compliance-Kontrollen bei der Erstellung von Runbooks eingehalten werden. Wir empfehlen außerdem, Runbooks gründlich zu testen, bevor Sie sie mit Produktionsressourcen ausführen.

F: Kann die Systems Manager Manager-Richtlinie mit anderen IAM-Rollen verknüpft **customer_systemsmanager_automation_policy** werden?

Nein, im Gegensatz zu anderen Self-Provision-fähigen Diensten kann diese Richtlinie nur der bereitgestellten Standardrolle zugewiesen werden.
`customer_systemsmanager_automation_console_role`

Im Gegensatz zu den Richtlinien anderer SSPS-Rollen kann diese SSM-SSPS-Richtlinie nicht mit anderen benutzerdefinierten IAM-Rollen gemeinsam genutzt werden, da dieser AMS-Dienst nur zum Ausführen von Befehlen oder Automatisierungsskripten innerhalb Ihrer verwalteten Instanzen dient. Wenn diese Berechtigungen mit anderen benutzerdefinierten IAM-Rollen verknüpft werden könnten, möglicherweise mit Berechtigungen für andere Dienste, könnte sich der Umfang der zulässigen Aktionen auf verwaltete Dienste erstrecken und die Sicherheitslage Ihres Kontos potenziell beeinträchtigen.

Wenden Sie sich an Ihren jeweiligen Cloud-Architekten oder Service Delivery Manager, um alle Änderungsanträge (RFCs) anhand unserer technischen AMS-Standards zu bewerten. Weitere Informationen finden Sie unter [RFC-Sicherheitsüberprüfungen](#).

Note

AWS Systems Manager ermöglicht es Ihnen, Runbooks zu verwenden, die mit Ihrem Konto geteilt werden. Wir empfehlen Ihnen, Vorsicht walten zu lassen und eine Due-Diligence-Prüfung durchzuführen, wenn Sie gemeinsam genutzte Runbooks verwenden. Stellen Sie außerdem sicher, dass Sie vor der Ausführung der Runbooks den Inhalt überprüfen, um zu verstehen, welche Runbooks ausgeführt command/scripts werden. Einzelheiten finden Sie unter Bewährte [Methoden für gemeinsam genutzte SSM-Dokumente](#).

Verwenden Sie AMS SSP zur Bereitstellung AWS Transfer Family in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen AWS Transfer Family (Transfer Family) zuzugreifen. AWS Transfer Family ist ein vollständig verwalteter AWS Service, mit dem Sie Dateien über das Secure File Transfer Protocol (SFTP) in den und aus dem Amazon Simple Storage Service (Amazon S3) -Speicher übertragen können. SFTP wird auch als Secure Shell (SSH) File Transfer Protocol bezeichnet. SFTP wird für den Datenaustausch zwischen unterschiedlichen Branchen wie Finanzdienstleistungen, Gesundheitswesen, Werbung, Einzelhandel usw. eingesetzt.

Mit AWS SFTP erhalten Sie Zugriff auf einen SFTP-Server, AWS ohne eine Serverinfrastruktur betreiben zu müssen. Sie können diesen Service verwenden, um Ihre SFTP-basierten Workflows zu migrieren und AWS gleichzeitig die Clients und Konfigurationen Ihrer Endbenutzer unverändert beizubehalten. Sie verknüpfen Ihren Hostnamen zunächst mit dem SFTP-Serverendpunkt, fügen dann Ihre Benutzer hinzu und gewähren ihnen die richtige Zugriffsebene. Danach werden die Übertragungsanfragen Ihrer Benutzer direkt von Ihrem AWS SFTP-Serverendpunkt aus bearbeitet. Weitere Informationen finden Sie unter [Einen AWS Transfer for SFTPSFTP-fähigen Server erstellen](#).

AWS Transfer for SFTP in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Transfer for SFTP auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Transfer for SFTP indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Über diesen RFC werden die folgenden IAM-Rollen und eine Richtlinie in Ihrem Konto bereitgestellt:

- `customer_transfer_author_role`. Mit dieser Rolle können Sie den SFTP-Dienst über die Konsole verwalten.
- `customer_transfer_sftp_server_logging_role`. Diese Rolle ist so konzipiert, dass sie an den SFTP-Server angehängt werden kann. Sie ermöglicht dem SFTP-Server das Abrufen von Protokollen. CloudWatch
- `customer_transfer_sftp_user_role`. Diese Rolle ist so konzipiert, dass sie den SFTP-Benutzern zugewiesen werden kann. Sie ermöglicht den SFTP-Benutzern die Interaktion mit dem S3-Bucket.

- `policy_customer_transfer_scope_down_policy`. Bei dieser Richtlinie handelt es sich um eine Scopedown-Richtlinie, die auf den SFTP-Benutzer angewendet werden kann, um seinen Zugriff auf den S3-Bucket auf seine Home-Ordner zu beschränken.
- `customer_transfer_sftp_efs_user_role`. Diese Rolle ist so konzipiert, dass sie den SFTP-Benutzern zugewiesen werden kann. Es ermöglicht den SFTP-Benutzern die Interaktion mit dem EFS-Dateisystem.

Nachdem es in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Transfer for SFTP in meinem AMS-Konto?

AWS Die Übertragung für die SFTP-Konfiguration ist auf Ressourcen ohne „AMS-“ oder „MC-“ - Präfixe beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Transfer for SFTP in meinem AMS-Konto?

- Sie benötigen einen Amazon S3 S3-Bucket mit einem Namen, der das Schlüsselwort „transfer“ enthält, bevor Sie den AWS Transfer for SFTP Server und die Benutzer erstellen können.
- Um einen „Customer Identify Provider“ zu verwenden, müssen Sie das API Gateway, die Lambda-Funktion und Ihr Benutzer-Repository (AD, Secrets Manager usw.) bereitstellen. Weitere Informationen finden Sie unter [Aktivieren der Kennwortauthentifizierung für die AWS Transfer for SFTP Verwendung von AWS Secrets Manager](#) und die [Arbeit mit Identitätsanbietern](#).

Verwenden Sie AMS SSP zur Bereitstellung AWS Transit Gateway in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Transit Gateway Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Transit Gateway ist ein Service, mit dem Sie Ihre Amazon Virtual Private Cloud (VPCs) und Ihre lokalen Netzwerke mit einem einzigen Gateway verbinden können. Wenn Sie die Anzahl der Workloads erhöhen AWS, auf denen ausgeführt wird, müssen Sie in der Lage sein, Ihre Netzwerke auf mehrere Konten zu skalieren, und Amazon VPCs muss mit dem Wachstum Schritt halten können. Heute können Sie Amazon-Paare VPCs mithilfe von Peering verbinden. Die Verwaltung der point-to-point Konnektivität in vielen Amazon-Ländern ohne die Möglichkeit VPCs, die Konnektivitätsrichtlinien zentral zu verwalten, kann jedoch betrieblich kostspielig und umständlich sein. Für lokale Konnektivität müssen Sie Ihr AWS

VPN mit jeder einzelnen Amazon-VPC verbinden. Die Entwicklung dieser Lösung kann zeitaufwändig und schwierig zu verwalten sein, wenn die Anzahl der Lösungen auf Hunderte VPCs ansteigt. Weitere Informationen hierzu finden Sie unter [AWS Transit Gateway](#).

AWS Transit Gateway in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Transit Gateway auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Transit Gateway indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem customer_tgw_console_role Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Transit Gateway in meinem AMS-Konto?

Die volle Funktionalität von AWS Transit Gateway ist in Ihrem AMS-Landezone-Konto mit einem Konto verfügbar, mit Ausnahme von Änderungen der Routentabelle für das Transit Gateway Gateway-Routing. Fordern Sie Änderungen an der Routentabelle an, indem Sie Folgendes einreichen: Management | Sonstige | Änderungstyp erstellen (ct-1e1xtak34nx76).

Note

Dieser Dienst wird nur für die landing zone mit einem Konto (SALZ) unterstützt, nicht für die landing zone mit mehreren Konten (MALZ).

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Transit Gateway in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Transit Gateway in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung von AWS WAF Web Application Firewall in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS WAF Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS WAF ist eine Firewall für

Webanwendungen (AWS WAF), mit der Sie Ihre Webanwendungen vor häufigen Web-Exploits schützen können, die die Verfügbarkeit von Anwendungen beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen könnten. AWS WAF gibt Ihnen die Kontrolle darüber, welcher Datenverkehr zu Ihren Webanwendungen zugelassen oder blockiert werden soll, indem Sie anpassbare Websicherheitsregeln definieren. Sie können AWS WAF damit benutzerdefinierte Regeln erstellen, die gängige Angriffsmuster wie SQL-Injection oder Cross-Site-Scripting blockieren, sowie Regeln, die auf Ihre spezifische Anwendung zugeschnitten sind.

Weitere Informationen finden Sie unter [AWS WAF — Web Application Firewall](#).

AMS unterstützt keine Überwachung (CloudWatch Alarme/Ereignisse/MMS-Warnungen) für AWS WAF. Es liegt in der Natur des AWS WAF Systems, dass Sie benutzerdefinierte Regeln für Ihre Anwendungen erstellen müssen. AMS kann Alarme nicht quantifizieren und für Sie erstellen, ohne den Kontext Ihrer Anwendung zu berücksichtigen. Weitere Informationen finden Sie unter [AWS WAF — Web Application Firewall](#).

AWS WAF in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS WAF die Einrichtung in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, AWS WAF indem Sie einen RFC mit dem Management | AWS-Service | Selbstbereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_waf_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem die AWS WAF IAM-Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gibt es bei der Nutzung? AWS WAF

Nachdem die Berechtigungen bereitgestellt wurden, steht Ihnen der volle Funktionsumfang von AWS WAF zur Verfügung.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS WAF?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung AWS WAF in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Well-Architected Tool in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Well-Architected Tool Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. Auf diese AWS Well-Architected Tool Weise können Sie den Status Ihrer Workloads überprüfen und sie mit den neuesten AWS Best Practices für die Architektur vergleichen. Das Tool basiert auf dem [AWS Well-Architected Framework](#), das Cloud-Architekten beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Anwendungsinfrastruktur unterstützt. Dieses Framework bietet Ihnen einen konsistenten Ansatz zur Bewertung von Architekturen, wurde in Zehntausenden von Workload-Überprüfungen verwendet, die vom AWS Lösungsarchitekturteam durchgeführt wurden, und bietet Anleitungen zur Implementierung von Designs, die im Laufe der Zeit an die Anwendungsanforderungen angepasst werden. Weitere Informationen hierzu finden Sie unter [AWS Well-Architected Tool](#).

AWS WA Tool in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Well-Architected Tool auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Well-Architected Tool indem Sie einen RFC mit dem Management | AWS-Service | Selbstbereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_well_architected_tool_console_admin_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Well-Architected Tool in meinem AMS-Konto?

Die volle Funktionalität von AWS Well-Architected Tool ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Well-Architected Tool in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Well-Architected Tool in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS X-Ray in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS X-Ray (X-Ray) -Funktionen in Ihrem verwalteten AMS-Konto zuzugreifen. AWS X-Ray hilft Entwicklern dabei, verteilte Produktionsanwendungen zu analysieren und zu debuggen, z. B. solche, die mit einer Microservices-Architektur erstellt wurden. Mit X-Ray können Sie die Leistung Ihrer Anwendung und der zugrunde liegenden Dienste nachvollziehen, um die Hauptursache von Leistungsproblemen und Fehlern zu identifizieren und zu beheben. X-Ray bietet eine end-to-end Übersicht der Anfragen, während sie Ihre Anwendung durchlaufen, und zeigt eine Übersicht der Ihrer Anwendung zugrunde liegenden Komponenten. Mit X-Ray können Sie sowohl Anwendungen in der Entwicklung als auch in der Produktion analysieren, von einfachen dreistufigen Anwendungen bis hin zu komplexen Microservices-Anwendungen, die aus Tausenden von Diensten bestehen. Weitere Informationen hierzu finden Sie unter [AWS X-Ray](#).

Häufig gestellte Fragen zu X-Ray in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS X-Ray auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto `customer_xray_console_role` die folgende IAM-Rolle zur Verfügung: Nach dem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren. Darüber hinaus müssen Sie über die `customer_xray_daemon_write_instance_profile` Möglichkeit verfügen, Daten von Ihren EC2 Amazon-Instances an X-Ray zu übertragen. Dieses Instance-Profil wird erstellt, wenn Sie das erhalten `customer_xray_console_role`.

Sie können eine Serviceanfrage an AMS Operations senden, um sie dem `customer_xray_daemon_write_policy` vorhandenen Instance-Profil zuzuweisen, oder Sie können das Instance-Profil verwenden, das erstellt wird, wenn AMS Operations X-Ray für Sie aktiviert.

F: Welche Einschränkungen gelten für die Nutzung AWS X-Ray in meinem AMS-Konto?

Die volle Funktionalität von AWS X-Ray ist in Ihrem AMS-Konto verfügbar, mit Ausnahme der Verschlüsselung mit dem AWS KMS-Schlüssel (KMS-Schlüssel). AWS X-Ray verschlüsselt standardmäßig alle Trace-Daten. Standardmäßig verschlüsselt X-Ray Traces und zugehörige Daten

im Ruhezustand. Wenn Sie Daten im Ruhezustand mit einem Schlüssel verschlüsseln müssen, können Sie entweder einen verwalteten AWS KMS-Schlüssel (aws/xray) oder einen vom Kunden verwalteten KMS-Schlüssel wählen. Reichen Sie für KMS Customer-Managed Key for X-Ray Encryption Folgendes ein: Management | Other | Other | Create change type (ct-1e1xtak34nx76).

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung in meinem AMS-Konto? AWS X-Ray

AWS X-Ray ist von Amazon S3 und CloudWatch Logs abhängig CloudWatch, die bereits in AMS-Konten implementiert sind. Transitive Abhängigkeiten variieren je nach Datenquellen und anderen AWS Diensten AWS X-Ray , mit denen Funktionen interagieren können (z. B. Amazon Redshift, Amazon RDS, Athena).

Verwenden Sie AMS SSP, um VM Import/Export in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um Import/Exportcapabilities direkt in Ihrem AMS-verwalteten Konto auf VM zuzugreifen. Import/Export Mit VM können Sie auf einfache Weise VM-Images aus Ihrer vorhandenen Umgebung in EC2 Amazon-Instances importieren und sie zurück in Ihre lokale Umgebung exportieren. Dieses Angebot ermöglicht es Ihnen, Ihre bestehenden Investitionen in die virtuellen Maschinen, die Sie zur Erfüllung Ihrer Anforderungen an IT-Sicherheit, Konfigurationsmanagement und Compliance entwickelt haben, zu nutzen, indem Sie diese virtuellen Maschinen EC2 als ready-to-use Instances zu Amazon bringen. Sie können importierte Instances auch zurück in Ihre lokale Virtualisierungsinfrastruktur exportieren, sodass Sie Workloads in Ihrer gesamten IT-Infrastruktur bereitstellen können. Weitere Informationen finden Sie unter [VM Import/Export](#).

Häufig gestellte Fragen Import/Export zu virtuellen Maschinen in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf virtuelle Maschinen Import/Export in meinem AMS-Konto?

Beantragen Sie den Zugriff auf die VM, Import/Export indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt customer_vmimport_policy die folgende IAM-Richtlinie für Ihr Konto bereit:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Eine zusätzliche Rolle, die Import/Export VM-Dienstrolle, ist erforderlich, damit der Dienst Aktionen in Ihrem Konto ausführen kann.

F: Was sind die Einschränkungen bei der Verwendung von VM Import/Export in meinem AMS-Konto?

- Funktionen zum Importieren von benutzerdefinierten Maschinenabbildern und Datenvolumen sind beide in AMS VM Import/Export verfügbar. Die Berechtigungen für S3 wurden jedoch so eingeschränkt, dass Aktionen auf Buckets beschränkt werden, die dem Namen entsprechen, um den Zugriff auf `customer-vmimport-*` Informationen innerhalb des Kontos einzuschränken.
- Der Import von Images und Snapshots wird in AMS VM Import/Export unterstützt. Die Funktionen für den Instanzimport und den Instanzexport sind jedoch aus Sicherheitsgründen nicht verfügbar.
- Darüber hinaus wurde die Exportfunktion deaktiviert, um das Risiko des Exports eingeschränkter und sensibler Daten zu minimieren.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von VM Import/Export in meinem AMS-Konto?

- Sie müssen ein unterstütztes Festplatten-Image für den Import in die AWS Umgebung bereitstellen. Weitere Informationen finden Sie unter [Import/Export VM-Anforderungen](#).
- Auf die VM kann Import/Export nicht über die AWS Konsole zugegriffen werden. Sie müssen über AWS CLI, AWS -Tools für PowerShell oder den auf diesen Dienst zugreifen AWS SDKs. Oder Sie können ein Instanzprofil anfordern, indem Sie den Änderungstyp `ct-117rmp64d5mnb` einreichen: Bereitstellung | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | Instanzprofil erstellen. EC2 Dieses Instanzprofil ermöglicht es den Tools, Befehle von einer Instanz aus auszuführen.

Vom Kunden verwalteter Modus

Der kundenverwaltete Modus von AWS Managed Services (AMS) bietet ein flexibles Governance-Modell, das an Ihre Anforderungen angepasst werden kann. Dies kann als Ausweichoption für Dienste und Anwendungen angesehen werden, die AMS nicht für Sie ausführen kann. AMS betreibt keine Infrastruktur, die in Konten gehostet wird, die in diesem Modus erstellt wurden. In diesem Modus können Sie jedoch die zentralisierte Verwaltung mehrerer Konten nutzen. In diesem Modus können die folgenden Funktionen der Landing Zone für mehrere Konten genutzt werden:

- Automatisierte Kontobereitstellung

- Konnektivität über Transit Gateway im Netzwerkkonto
- Bibliothek mit AMS-Konfigurationsregeln
- Speichern Sie Kopien der Protokolle im Protokollkonto
- Zusammenfassung der vom Kunden verwalteten Guard Duty-Benachrichtigungen im Sicherheitskonto
- Konsolidierte Fakturierung
- Aktivierung benutzerdefinierter Service Control-Richtlinien.

Beispiel: Wenn Sie Workloads auf Ubuntu Pro ausführen möchten, bei dem es sich nicht um ein von AMS verwaltetes Betriebssystem handelt, können Sie ein vom Kunden verwaltetes Konto zum Hosten verwenden. Sie können Workloads auch über vom Kunden verwaltete Konten konsolidieren, um den Mengenrabatt auf reservierte Instances/Sharing Pläne zu nutzen, der durch gemeinsame Nutzung innerhalb einer AWS-Organisation verfügbar ist.

Erste Schritte mit dem vom Kunden verwalteten Modus

Der AMS-Modus „Customer Managed“ ist über ein spezielles Anwendungskonto mit mehreren Konten für die landing zone verfügbar.

Einzelheiten, einschließlich der Erstellung eines vom Kunden verwalteten Anwendungskontos, finden Sie unter [Kundenverwaltete Anwendungskonten](#).

AMS- und AWS Service Catalog

Service Catalog in AWS Managed Services (AMS) ermöglicht es Unternehmen, Kataloge von AWS-Informationstechnologie (IT) -Services zu erstellen und zu verwalten. IT-Administratoren können Kataloge mit zugelassenen Produkten in ihren Konten erstellen, verwalten und an Endbenutzer verteilen, die dann in einem personalisierten Serviceportal auf die Produkte zugreifen können, die sie benötigen. Administratoren können kontrollieren, welche Benutzer Zugriff auf jedes Produkt haben, um die Einhaltung der Unternehmensrichtlinien durchzusetzen. Administratoren können auch Rollen einrichten, sodass Endbenutzer nur IAM-Zugriff auf Service Catalog benötigen, um genehmigte Ressourcen bereitzustellen. Service Catalog ermöglicht es Ihrem Unternehmen, von mehr Flexibilität und geringeren Kosten zu profitieren, da Endbenutzer in einem Katalog, den Sie kontrollieren, nur die Produkte finden und auf den Markt bringen können, die sie benötigen.

Service Catalog bietet Ihnen eine Alternative zum AMS Request for Change (RFC) -Prozess für die Bereitstellung und Aktualisierung von Ressourcen in Ihren AMS-verwalteten Konten. AMS verwaltet

alle Aufgaben des Infrastrukturbetriebs, die für den skalierbaren Betrieb von AWS für alle über Service Catalog bereitgestellten Infrastrukturressourcen erforderlich sind, einschließlich Sicherheit, Compliance, Bereitstellung, Verfügbarkeit, Patch, Überwachung, Warnung, Berichterstattung, Reaktion auf Vorfälle und Kostenoptimierung. Die Verwendung von Service Catalog in Ihrem AMS-verwalteten Konto bietet Ihnen einen Mechanismus zur zentralen Verwaltung häufig bereitgestellter IT-Services und hilft Ihnen dabei, eine konsistente Governance zu erreichen, während Benutzer schnell nur die genehmigten IT-Services bereitstellen können, die sie in ihren verwalteten Umgebungen benötigen.

Erste Schritte mit Service Catalog

Um mit Service Catalog in AMS zu beginnen, reichen Sie eine Serviceanfrage über die AMS-Konsole ein, um Zugriff auf Service Catalog anzufordern. Nach dem Absenden der Anfrage werden drei IAM-Rollen zusammen mit einem AMS-verwalteten Stack, der das CloudFormation Makro enthält, das das AMS aufruft `Transform` (zuvor beschrieben), in Ihren Konten bereitgestellt, sodass wir die Produkte in unseren Systemen registrieren und Operationen mit der über Service Catalog bereitgestellten Infrastruktur ausführen können. Zu den drei bereitgestellten IAM-Rollen gehören eine Rolle für IT-Administratoren zur Verwaltung von Produkten als Service Catalog-Administratoren, eine Rolle für Anwendungsbesitzer und Endbenutzer zum Konfigurieren, Starten und Verwalten von Produkten sowie eine Rolle, die als Starteinschränkung verwendet wird und die Berechtigungen definiert, die Service Catalog beim Starten oder Aktualisieren Ihres Produkts verwendet.

Service Catalog in AMS, bevor Sie beginnen

Ersetzt Service Catalog den bestehenden AMS Request for Change (RFC) -Prozess?

In Konten, für die Service Catalog aktiviert ist, fungiert er als Change-Management-System, in dem Sie IT-Services in Ihrem AMS-Konto über Ihren vordefinierten Produktkatalog bereitstellen und aktualisieren. AMS stellt einen portfolio/product Standardkatalog bereit, und Ihre IT-Administratoren können Ihren eigenen erstellen und konfigurieren. Service Catalog bestätigt nur Stacks, die über Service Catalog bereitgestellt wurden. Ebenso können Dienste, die über Service Catalog bereitgestellt werden, nicht über den AMS RFC-Prozess geändert werden, da Änderungen außerhalb von Service Catalog dazu führen, dass der Stack von der genehmigten Produktkonfiguration abweicht.

Kann ich die über den Service Catalog bereitgestellten Stacks in der AMS-Konsole sehen?

Ja. Sie können alle über den Servicekatalog bereitgestellten Stacks in der AMS-Konsole einsehen. Stacks, die über Service Catalog bereitgestellt werden, sind leicht anhand der Stack-

ID „SC-“ zu identifizieren. Stacks sind zwar in der AMS-Konsole sichtbar, sie können jedoch nicht über den AMS-RFC-Prozess aktualisiert werden. Der Zugriff auf das AMS-Change-Management-System (RFCs) ist ausschließlich auf Zugriffsanforderungen, Patch-Orchestrierung und Datensicherung beschränkt. RFCs

Wenn ich einen Stack über Service Catalog and/or aktualisiere, gibt es dann einen entsprechenden RFC in der AMS-Konsole?

Der einzige RFC, der in der AMS-Konsole angezeigt wird, ist ein RFC zur Registrierung des Stacks bei AMS, wenn ein Stack zum ersten Mal bereitgestellt wird. Dieser RFC wird automatisch durch den AMS-Validierungsprozess abgelegt, der ausgelöst wird, wenn ein Stack über Service Catalog gestartet wird. Alle anderen Bereitstellungen und Änderungen werden direkt in Service Catalog verfolgt und sind in der Service Catalog-Konsole sichtbar. Darüber hinaus können Sie die Funktion „Bereitgestellter Produktplan“ in Service Catalog verwenden, um die Liste der Änderungen anzuzeigen, die vor der Bereitstellung oder Aktualisierung des Produkts an den Ressourcen vorgenommen werden.

Muss ich etwas Spezielles für die Bereitstellung von Produkten in meinem AMS-verwalteten Konto tun?

Ja. Alle Service Catalog-Produkte, die in AMS-Konten bereitgestellt werden, müssen diese JSON-Zeile in der CFN-Vorlage enthalten, die dieses Produkt definiert:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}}
```

Dieser Codeausschnitt löst die AMS-Validierungen aus, die erforderlich sind, bevor die Ressource in Ihrem AMS-verwalteten Konto bereitgestellt werden kann. CloudFormation Es liegt in Ihrer Verantwortung, diese Codezeile als Teil der Produktdefinition aufzunehmen. Wenn es nicht enthalten ist, schlägt die Bereitstellung fehl und die folgende Fehlermeldung wird angezeigt: „Produkt konnte nicht erstellt werden. Dieses Konto wird von AMS verwaltet. Alle Produkte in AMS-Konten müssen den Transform AMS-Code in der Vorlage enthalten.“

Gibt es Service Catalog-Funktionen, die AMS-Kunden bei der Markteinführung nicht and/or eingeschränkt zur Verfügung stehen?

Ja, die folgenden SC-Funktionen sind für AMS-Kunden bei der ersten Markteinführung nicht verfügbar:

- Kontoerstellung über Service Catalog

- Möglichkeit, alle AWS-Services über Service Catalog auf einem von AMS verwalteten Konto zu starten. Die Verfügbarkeit von AWS-Services ist auf AMS-unterstützte Services (verwaltet und selbst bereitgestellt) beschränkt. Weitere Informationen zu AMS-unterstützten Services finden Sie in der AMS-Servicebeschreibung.
- Service Catalog IT Service Manager (ITSM) -Konnektoren kommunizieren nicht mit AMS-Vorfallberichten und Serviceanfragen.
- Möglichkeit, Service Catalog-Schnellstarts und Referenzarchitekturen ohne Änderungen zu nutzen. Denken Sie daran, dass Service Catalog-Produkte für AMS-Konten diese JSON-Codezeile enthalten müssen:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":  
{"Ref":"AWS::StackId"}}}
```

in der CNF-Vorlage. Beachten Sie, dass diese Zeile nicht Teil einer typischen CloudFormation AWS-Vorlage ist und explizit hinzugefügt werden muss.

- Terraform wird derzeit von AMS nicht für die Bereitstellung von Service Catalog-Produkten unterstützt.
- AWS-CFN-Stacksets werden in AMS nicht unterstützt.
- Sie können keine benutzerdefinierten IAM-Rollen erstellen.
- Serviceaktionen sind beschränkt auf:
 - [AWS- RebootRdsInstance](#)
 - [AWS-Neustart-Instanz EC2](#)
 - [AWS-Startinstanz EC2](#)
 - [AWS- StartRdsInstance](#)
 - [AWS-Stopp-Instanz EC2](#)
 - [AWS- StopRdsInstance](#)
 - [AWS- CreateImage](#)
 - [AWS- CreateRdsSnapshot](#)
 - [AWS- CreateSnapshot](#)

 Note

Bei der Erstellung von Serviceaktionen können Sie die Ausführungsrolle so konfigurieren, dass sie die Berechtigungen des Endbenutzers, die Startrolle oder

eine benutzerdefinierte IAM-Rolle Ihrer Wahl ist. Die ausgewählte Ausführungsrolle muss über ausreichende Berechtigungen verfügen, um die Dienstaktion auszuführen, und sie muss über eine Berechtigung verfügen TrustPolicy , mit der sie von Service Catalog übernommen werden kann. Andernfalls schlägt die Dienstaktion zur Ausführungszeit fehl. Wir empfehlen die Verwendung von `AWSManagedServicesServiceCatalogLaunchRole`, die über die richtigen Berechtigungen und die richtige Vertrauensrichtlinie für die Verwendung als Serviceaktion verfügt.

Wofür muss ich das AMS RFC-System weiterhin verwenden?

Bei allgemeiner Verfügbarkeit (GA) müssen Sie weiterhin RFCS verwenden, um die folgenden Aktionen auszuführen:

- Patch Orchestrator konfigurieren
- Konfiguration von Backup-Richtlinien
- Instanzzugriff anfordern
- Erstellung und Zuweisung von Sicherheitsgruppen, die nicht den AMS-Richtlinien entsprechen.
- Workload Ingest (WIGS) durchführen
- Erstellen von IAM-Rollen

Kann ich die Service Catalog-CLI verwenden, um in meinem AMS-verwalteten Konto auf Service Catalog zuzugreifen?

Ja, Service Catalog APIs ist über die CLI verfügbar und aktiviert. Aktionen von der Verwaltung von Service Catalog-Artefakten bis hin zur Bereitstellung und Beendigung dieser Artefakte sind verfügbar. Weitere Informationen finden Sie unter [AWS Service Catalog Resources](#) oder laden Sie das neueste AWS-SDK oder CLI herunter.

Wer erstellt, verwaltet und verteilt Kundenkataloge mit zugelassenen Produkten?

Der Katalogadministrator, der and/or IT-Administrator oder die zugewiesene Ressource des Kunden, ist für die Verwaltung Ihrer Servicecatalog-Kataloge und genehmigten Produkte verantwortlich.

Kann ich AMS verwenden? AMIs

AMS, AMIs die nach März 2020 verkauft wurden, können über den AWS Service Catalog bereitgestellt werden.

Wie migriere ich mithilfe von Service Catalog zu AMS?

Um Ihren Workload mithilfe von Service Catalog zu AMS zu migrieren, folgen Sie zunächst dem [Workload Ingest](#) (WIGs) -Prozess, um ein AMI in AMS zu erstellen. Sie verwenden das von WIGS erstellte AMI, um ein Produkt im Service Catalog zu erstellen. Eine Anleitung dazu finden Sie unter [AWS Service Catalog — Erste Schritte](#).

Finden der benötigten Daten (SKMS), AMS

Um die Daten zu finden, die Sie für die Nutzung Ihrer AWS Managed Services (AMS) -Konten benötigen, wird das AMS Service Knowledge Management- oder SKMS-System verwendet. AMS.

SKMS steht für Service Knowledge Management System und bezieht sich auf alle Informationen, die sich auf den AWS Managed Services (AMS) -Service für einen Kunden beziehen. AMS verfügt über eine SKMS-API zum Auffinden von Daten.

Themen

- [Was ist Service-Wissensmanagement?](#)
- [VPC IDs in AMS finden](#)
- [Subnetz IDs in AMS finden](#)
- [Finde AMI IDs, AMS](#)
- [Finden Sie die Sicherheitsgruppe \(SG\) IDs, AMS](#)
- [Suchen Sie nach IAM-Entitäten in AMS](#)
- [Finden Sie den Stack IDs in AMS](#)
- [Suchen Sie nach Instanzen IDs oder IP-Adressen in AMS](#)
- [Suchen Sie Amazon-Ressourcennamen \(ARNs\) in AMS](#)
- [Finden Sie Ressourcen nach ARN in AMS](#)
- [Finden Sie die AMS-Kontoeinstellungen](#)

Was ist Service-Wissensmanagement?

Service Knowledge Management ist der Speicher aller Informationen auf Ihrem AMS-Konto.

Informationen zu den folgenden Themen werden vom AMS Service Knowledge Management System (SKMS), über die AMS SKMS-API oder über die AMS-Konsole abgerufen:

- VPCs
- Verwaltete Subnetze
- Stacks und Stack-Komponenten, einschließlich EC2 Amazon-Instances und anderer Ressourcen
- Amazon-Maschinenbilder (AMIs)

Sie können Informationen aus dem SKMS verwenden, um sich ein Bild von der verwalteten Infrastruktur zu machen und als Grundlage für das Änderungsmanagement und für Serviceanfragen zur Erstellung, Änderung oder Entfernung der Infrastruktur dienen.

 Note

Alle AMS SKMS API-Aufrufe werden in aufgezeichnet. AWS CloudTrail

Greifen Sie über die AMS SKMS-API auf das SKMS zu, die Operationen zum Auffinden von Informationen über eine Umgebung (VPCs und Subnetze) und die Anwendungsressourcen (Stacks, EC2 Amazon-Instances und Instance-Images oder AMIs) bereitstellt, die dort bereitgestellt werden können.

VPCs und Instance-Images werden beim Onboarding in einem Konto mit den erforderlichen Zugriffsberechtigungen eingerichtet. Nachdem sie eingerichtet wurden, können Sie das Change-Management-System verwenden, um sie VPCs mit funktionierenden Stacks zu füllen.

VPC IDs in AMS finden

Eine Virtual Private Cloud (VPC) hat ein oder mehrere Subnetze. In AMS befindet sich Ihre VPC in einem AWS-Region und Sie haben private und öffentliche Subnetze.

Siehe auch [Subnetz IDs in AMS finden](#).

Einige CTs benötigen die. VpcId Um eine VPC-ID zu finden, können Sie entweder die AMS-Konsole oder API/CLI verwenden.

AMS-Konsole:

Wählen Sie im Navigationsbereich die VPCsentsprechende VPC aus. Die VPC-Detailseite für die ausgewählte VPC wird mit Informationen wie der VPC-ID geöffnet.

AMS SKMS API ListVpcSummaries oder CLI:

 Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-

Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` z. B.. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

Note

Die AMS-Endpunkte API/CLI (`amscm` und `amsskms`) befinden sich in der AWS-Region Nord-Virginia. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

1. In den folgenden Beispielen fordert der erste Befehl eine Liste mit Zusammenfassungen für alle Benutzer des Kontos VPCs an. Der zweite Befehl fordert die Liste von an VPCs, wobei ein Abfragefilter nur diejenigen auflistet, die 2016 VPCs erstellt wurden, und gibt den Namen `CreatedTime` `VpcId`, und aus.

Note

Sie können die AMS SKMS-CLI über die Seite Entwicklerressourcen in der AMS-Konsole abrufen.

```
aws amsskms list-vpc-summaries --output table
```

```
-----
|                               ListVPCSummaries                               |
+-----+-----+-----+-----+-----+-----+
|                               VPCSummaries                               |
|+-----+-----+-----+-----+-----+-----+|
| CreatedTime | 2016-01-15T18:50:11Z |
| VpcId       | vpc-01234567890abcdef |
| LastModifiedTime | 2016-01-15T18:50:11Z |
```

Name	952444781316-initial-vpc

Visibility	

Id	PrivateAndPublic
Name	PrivateAndPublic

2. Diesmal mit einer Abfrage:

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
table
```

----- ListVPCSummaries -----		
+-----+-----+-----+		
2016-01-15T18:50:11Z	vpc-01234567890abcdef	952444781316-initial-VPC
+-----+-----+-----+		

Subnetz IDs in AMS finden

Für mehrere Ressourcen müssen Sie bei der Konfiguration ein Subnetz oder eine Liste von Subnetzen angeben. Um Subnetze zu finden, können Sie entweder die AMS-Konsole verwenden oder AMS SKMS API/CLI. Note that the AMS SKMS API/CLI ist privat und muss installiert werden, bevor Sie es verwenden können.

AMS-Konsole:

1. Wählen Sie im Navigationsbereich die VPCsentsprechende VPC aus. Die VPC-Detailseite für die ausgewählte VPC wird mit einer Tabelle mit Subnetzen geöffnet. Klicken Sie auf eine Subnetz-ID, um die Detailseite zu öffnen und die ID zu finden.

AMS SKMS API ListSubnetSummaries oder CLI:

Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf.

Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` z. B.. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

Note

Die AMS-Endpunkte API/CLI (`amscm` und `amsskms`) befinden sich in der AWS-Region Nord-Virginia. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Um die Subnetze für Ihre VPC zu finden, können Sie wie in der Abbildung gezeigt mit dem `list-subnet-summaries` Befehl suchen.

Note

Wenn Sie nach Subnetzen suchen, die sich nicht in einem AMS-Konto befinden, können Sie es versuchen. `aws ec2 describe-subnets --region us-west-2`

1. Der SKMS-Vorgang API/CLI ListSubnetSummaries :

Eine einfache Liste:

```
aws amsskms list-subnet-summaries
```

Ausgabe in eine Tabelle:

```
aws amsskms list-subnet-summaries --output table
```

2. Der ListSubnetSummaries SKMS-API-Vorgang verfügt über Parameter, mit denen die Ergebnisse je nach Sichtbarkeit eingegrenzt werden können. Darüber hinaus können Sie Ergebnisse nach Namen [filtern](#). Wenn Sie die CLI verwenden, können Sie die `--query` Option auch verwenden, um die Ausgabe einzuschränken oder nach einem Teil eines Werts zu suchen. Um beispielsweise alle Subnetze für eine bestimmte VPC zu finden, können Sie diesen Befehl verwenden:

```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

Was etwa Folgendes zurückgibt:

```
-----
|                               ListSubnetSummaries                               |
+-----+-----+-----+-----+
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
+-----+-----+-----+-----+
```

Informationen zur Verwendung von CLI-Abfragen finden Sie unter [So filtern Sie die Ausgabe mit der Option --query](#) und in der Referenz zur Abfragesprache, [JMESPath Spezifikation](#).

3. Wenn Sie mehrere haben VPCs, fügen Sie einen VPC-Filter in den Befehl ein und führen Sie dann den Befehl für jede VPC aus. Beispiel:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

4. Verwenden Sie in AWS [describe-subnets](#).

Informationen zur Verwendung von CLI-Abfragen finden Sie unter [So filtern Sie die Ausgabe mit der Option --query](#) und in der Referenz zur Abfragesprache, [JMESPath Spezifikation](#).

Subnetznamen

Ihre AMS-Subnetze werden automatisch erstellt, nachdem Eingaben von Ihnen gesammelt und dem System hinzugefügt wurden. AMS verwendet eine Formel, um Ihre Subnetznamen zu erstellen: A *ACCOUNT_ID* - -*SUBNET-TYPE*. *AZ-IDENTIFIER* Der Subnetztyp wäre entweder *dmzshared-services*, oder *customer-application* Falls Sie mehr als ein Subnetz für Kundenanwendungen haben, kann dem Subnetznamen nach der Konto-ID eine optionale Kennung hinzugefügt werden, um anzugeben, dass es sich bei dem Subnetz um ein „zusätzliches“ oder „reserviertes“ Subnetz handelt.

Finde AMI IDs, AMS

Ein Amazon Machine Image oder AMI ist eine Vorlage für EC2 Amazon-Instances, die aus einer EC2 Amazon-Instance erstellt wurde. AWS stellt jeden Monat aktualisierte AMIs (z. B. mit Patches) bereit. AWS Managed Services (AMS) setzt jedoch voraus AMIs, dass diese für die AMS-Nutzung modifiziert wurden. AMS veröffentlicht jeden Monat AMIs etwas Neues, das Sie kurz nach dem Patch Tuesday verwenden können.

Amazon Machine Images (AMIs) sind Instanzkonfigurationsvorlagen, die zur Erstellung von EC2 Instanzen in AWS verwendet werden. AMS erfordert, dass dieses spezielle AMIs für AMS-verwaltete Ressourcen verwendet wird. Die Änderungstypen für die Erstellung von EC2 Instances und EC2 Auto Scaling Scaling-Gruppen erfordern, dass Sie ein AMI angeben, das AMS als Grundlage für die Instances verwenden soll, die der Änderungstyp erstellt. AMS empfiehlt, immer das neueste AMI auszuwählen, das Ihnen zur Verfügung steht.

Weitere Informationen finden Sie AWS AMIs unter [AWS AMI Design](#).

Wenn Sie einen EC2 Amazon-Stack oder eine Amazon EC2 Auto Scaling Scaling-Gruppe für Ihr AMS-Konto erstellen, müssen Sie ein AMI von angeben Amild. Sie sind auf AMIs das beschränkt, was mit „Kunde-“ beginnt, und wir empfehlen Ihnen, immer das neueste AMI zu wählen.

Um das neueste AMI für Ihr Konto zu finden, können Sie mit einem AMS SKMS CLI-Befehl suchen oder die Detailseite der AMS-Konsole für die entsprechende VPC verwenden:

- Verwenden Sie die AMS-Konsole: Die verfügbaren AMIs sind auf der AMI-Seite in der AMS-Konsole aufgeführt. Wählen Sie aus, deren Namen AMIs mit „Kunde-“ beginnen.
- Verwenden Sie den AMS API/CLI ListAmis SKMS-Vorgang.

 Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` zum Beispiel. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

Hier ist ein CLI-Beispiel mit einer `query` Option, die die Ergebnisse auf den Kunden AMIs beschränkt:

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

In diesem Beispiel wird die `filter` Option mit der `query` Option verwendet, um Windows zu finden AMIs , die mit „Kunde“ beginnen:

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- Informationen zur Verwendung von CLI-Abfragen finden Sie unter [So filtern Sie die Ausgabe mit der Option --query](#) und in der Referenz zur Abfragesprache, [JMESPath Spezifikation](#).

Finden Sie die Sicherheitsgruppe (SG) IDs, AMS

Amazon EC2 Create und OpenSearch Create Domain CTs erfordert eine Sicherheitsgruppen-ID. Dies wird in der Form `seinsg-02ce123456e7893c7`. Ihr Konto hat mindestens zwei Standardsicherheitsgruppen [Sicherheitsgruppen](#). Weitere Informationen finden Sie unter. Darüber hinaus verfügen Sie möglicherweise über Sicherheitsgruppen, die Sie für bestimmte Zwecke erstellt haben. Gehen Sie wie folgt vor, um Ihre Sicherheitsgruppen zu ermitteln:

- AWS-Konsole: Verwenden Sie die EC2 oder VPC-Konsole, um alle Sicherheitsgruppen für die ausgewählte VPC anzuzeigen.
- API/CLI (wenn Sie in Ihrem AMS-Konto angemeldet sind):

Listen Sie Ihre Sicherheitsgruppen auf:

```
aws ec2 describe-security-groups
```

Suchen Sie nach IAM-Entitäten in AMS

Ihr Konto verfügt über standardmäßige IAM-Rollen und -Richtlinien; siehe [IAM-Benutzerrolle in AMS](#) und Standard-IAM-Instance-Profile; siehe [EC2 IAM-Instanzprofil](#) mit Standardrichtlinien. So finden Sie Ihre IAM-Rollen und -Richtlinien heraus:

- Konsole: Verwenden Sie die IAM-Konsole, um alle IAM-Richtlinien und -Rollen für Ihr Konto anzuzeigen.
- API/CLI (wenn Sie in Ihrem AMS-Konto angemeldet sind):

Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` z. B. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

Listen Sie Ihre Rollen auf:

```
aws --profile saml iam list-roles
```

Listen Sie Ihre Richtlinien auf:

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

Finden Sie den Stack IDs in AMS

Um eine Stack-ID zu finden, können Sie entweder die EC2 Amazon-Konsole, die AMS-Konsole oder die AMS SKMS-API/CLI verwenden.

AMS-Konsole:

- Wählen Sie im Navigationsbereich den RFC aus RFCs, der den Stack erstellt hat, und klicken Sie dann darauf. Verwenden Sie die Filteroption oben, um die Liste zu reduzieren. Die RFC-Detailseite wird geöffnet und enthält die Run-Ausgabe mit der Stack-ID.
- Alternativ können Sie im Navigationsbereich Stacks auswählen, um die Seite mit der Stack-Liste zu öffnen, und dann durch die Stack-Liste zu dem Stack blättern, der Sie interessiert. Diese Methode ist nützlicher, wenn Sie das Thema des Stacks kennen, nach dem Sie suchen.

EC2 Amazon-Konsole:

Wählen Sie im Navigationsbereich Instances oder Load Balancers oder Auto Scaling Groups aus.

AMS SKMS API ListStackSummaries oder CLI:

Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` z. B. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

Note

Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia, `us-east-1`. Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile sam1`, ob dies Ihre Authentifizierungsmethode ist.

Um eine Liste der Stacks im aktuellen Konto anzuzeigen, führen Sie den `ListStackSummaries` Betrieb der SKMS-API (CLI: `list-stack-summaries`) aus. Um vollständige Informationen über eine bestimmte Stack-Instance zu erhalten, führen Sie den Befehl `StackId` aus. `GetStack`

- In den folgenden Beispielen fordert der erste Befehl eine Liste mit Zusammenfassungen für alle Stack-Instances im Konto an. Der zweite Befehl fordert die Liste der Stack-Instances mit einem Abfragefilter an, um nur die Instanzen einer bestimmten Stack-Vorlage aufzulisten, und gibt den VpcId Namen und StackId aus.

```
aws amsskms list-stack-summaries --output table
```

```
-----
|                                     ListStackSummaries                                     |
|                                     StackSummaries                                       |
|-----+-----+-----+-----+
| VpcId | StackId | StackTemplateId | Name |
|-----+-----+-----+-----+
| vpc-0123abcd | stack-1fb7fe2212345678 | stm-sdhopvbb123456789 | Test ELB |
| vpc-0123abcd | stack-8323cc0e12345678 | stm-s2b72beb123456789 | S3 store |
| vpc-0123abcd | stack-2309fa0712345678 | stm-sdhopvbb123456789 | ELB      |
| vpc-0123abcd | stack-5e61a70512345678 | stm-sdpabqbb123456789 | PatchSim |
| vpc-0123abcd | stack-bd0e080d12345678 | stm-s2b72beb123456789 | CLI demo |
|-----+-----+-----+-----+
```

Informationen zur Verwendung von CLI-Abfragen finden Sie unter [So filtern Sie die Ausgabe mit der Option --query](#) und in der Referenz zur Abfragesprache, [JMESPath Spezifikation](#).

 Note

Informationen zur Verwendung einer Instanz IDs für den Zugriff finden Sie auch [Zugreifen auf Instanzen mithilfe von Bastionen](#) unter.

Suchen Sie nach Instanzen IDs oder IP-Adressen in AMS

- Um Zugriff auf eine Instance anzufordern, sich bei einer Instance anzumelden oder ein AMI zu erstellen, benötigen Sie die Instance-ID. Für eine EC2 Instance (entweder eine eigenständige Instance oder ein Teil eines Stacks) oder eine Datenbank-Instance können Sie die ID auf verschiedene Arten finden:
 - Die AMS-Konsole für eine Instance in einem ASG-Stack: Suchen Sie auf der RFC-Detailseite nach dem RFC, der den Stack erstellt hat. Im Abschnitt Execution Output finden Sie die Stack-ID für den ASG-Stack. Sie können dann auf der Seite EC2 Console Auto Scaling Groups nach dieser Stack-ID suchen und Instances dafür finden. Wenn Sie die Instance gefunden haben, wählen Sie sie aus und unten auf der Seite öffnet sich ein Bereich mit Details, einschließlich der IP-Adresse.
 - Die AMS-Konsole für eine Standalone EC2 - oder Datenbank-Instance (DB): Suchen Sie auf der RFC-Detailseite nach dem RFC, der den EC2 Stack oder die DB-Instance erstellt hat. Im Abschnitt Execution Output finden Sie die Instance-ID und die IP-Adresse.
 - EC2 AWS-Konsole:
 1. Wählen Sie im Navigationsbereich Instances aus. Die Seite „Instances“ wird geöffnet.
 2. Klicken Sie auf die Instance, für die Sie die ID benötigen. Die Seite mit den Instanzdetails wird geöffnet und zeigt die ID und die IP-Adresse an.
 - AWS-Datenbankkonsole:
 1. Wählen Sie auf der Startseite DB-Instances aus. Die Seite Instances wird geöffnet.
 2. Filtern Sie nach der DB-Instance, für die Sie die ID benötigen. Die Seite mit den Instance-Details wird geöffnet und die ID wird angezeigt.
 - AMS CLI/API.

 Note

Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole

auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms ams-cli-command --profile SAML` zum Beispiel. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise `us-east-1` ausgeht. `aws amscm ams-cli-command --region=us-east-1`

 Note

Die AMS-Endpunkte API/CLI (`amscm` und `amsskms`) befinden sich in der AWS-Region Nord-Virginia, `us-east-1`. Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Führen Sie den folgenden Befehl aus, um die Ausgabedetails zur Stack-Ausführung abzurufen:

```
aws amsskms get-stack --stack-id STACK_ID
```

Die Ausgabe sieht in etwa so aus, Instanceld dass sie unten unter angezeigt wird Outputs (die angegebenen Werte sind Beispiele):

```
{
  "Stack": {
    "StackId": "stack-7fa52bd5eb8240123",
    "Status": {
      "Id": "CreateCompleted",
      "Name": "CreateCompleted"
    },
    "VpcId": "vpc-01234567890abcdef",
    "Description": "Amazon",
    "Parameters": [
      {
        "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
        "Key": "SecurityGroups"
      }
    ]
  }
}
```

```

    },
    {
      "Value": "subnet-01234567890abcdef",
      "Key": "InstanceSubnetId"
    },
    {
      "Value": "t2.large",
      "Key": "InstanceType"
    },
    {
      "Value": "ami-01234567890abcdef",
      "Key": "InstanceAmiId"
    }
  ],
  "Tags": [],
  "Outputs": [
    {
      "Value": "i-0b22a22eec53b9321",
      "Key": "InstanceId"
    },
    {
      "Value": "10.0.5.000",
      "Key": "InstancePrivateIP"
    }
  ],
  "StackTemplateId": "stm-s6xvs0000000000000",
  "CreatedTime": "1486584508416",
  "Name": "Amazon"
}
}

```

Suchen Sie Amazon-Ressourcennamen (ARNs) in AMS

Ein Amazon-Ressourcenname (ARN) ist eine Zeichenfolge, die eine AWS Ressource eindeutig identifiziert, z. B. EC2 Instances, S3-Buckets, Konten, Lambda-Funktionen usw. AWS erfordert einen ARN, wenn Sie eine Ressource für alle eindeutig angeben möchten AWS, z. B. in IAM-Richtlinien, Amazon Relational Database Service (Amazon RDS) -Tags und API-Aufrufen. ARNs bestehen aus Kennungen, die den Service, die Region, das Konto und andere Informationen angeben. Es gibt drei ARN-Formate:

```
arn:aws:service:region:account-id:resource-id
```

```
arn:aws:service:region:account-id:resource-type/resource-id  
arn:aws:service:region:account-id:resource-type:resource-id
```

Note

Das genaue Format eines ARN hängt vom Service- und Ressourcentyp ab. [Weitere Informationen ARNs finden Sie unter Amazon Resource Names \(ARNs\) und AWS Service Namespaces and ARN Formats.](#)

Beispiele für ARN-Format nach Ressourcen finden Sie in der [Tabelle mit den Ressourcentypen](#) der AWS Service Authorization Reference.

Es kann schwierig sein, den ARN eines AWS-Objekts zu finden. Es gibt drei Möglichkeiten, es auszuprobieren:

- AWS-Servicekonsole: Rufen Sie die entsprechende AWS-Servicekonsole auf, suchen Sie die Ressource und suchen Sie den ARN in den Details für die Ressource.
- AWS API/CLI (Sie müssen zuerst die AWS-CLI installieren): Suchen Sie in der [AWS CLI Command Reference](#) nach dem entsprechenden Service und suchen Sie dann, je nach AWS-Service, nach dem entsprechenden Vorgang `describe`, `list`, oder `get`. Beispielsweise können Sie für alle IAM-Rollen, -Richtlinien und -Benutzer den ARN in der Ausgabe von der CLI abrufen mit:

```
aws iam get-role --role-name EMR_DefaultRole
```

- Konstruieren Sie den ARN auf der Grundlage des entsprechenden Formats: Suchen Sie das ARN-Format für die Ressource, [indem Sie auf der Seite Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Services](#) suchen, den entsprechenden Service und dann die entsprechende Aktion suchen und bis zum ARN-Format der Ressource aufschlüsseln. Sobald Sie das Format haben, ersetzen Sie die Variablen durch die entsprechenden Einstellungen.

Sie können den ARN selbst erstellen, indem Sie dem entsprechenden Format folgen (die Formate ändern sich je nach Dienst und Ressourcentyp) und die Informationen eingeben. Hier sind einige ARN-Beispiele:

- Ein AWS-Konto ARN hat die folgende Syntax:

```
arn:aws:iam::ACCOUNT-ID:root
```

- Ein S3-ARN hat eine flache Hierarchie von Buckets und zugehörigen Objekten:

```
arn:aws:s3:::ams-bucket
```

- Ein EC2 ARN hat Unterressourcentypen wie Image, Sicherheitsgruppen, Instanz usw. Dieses Beispiel beinhaltet die Instanz-ID am Ende:

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Ein Lambda-ARN hat den Funktionsnamen für den Resource-ID-Teil, und Sie müssen möglicherweise die Versionsnummer am Ende angeben, wie in diesem Beispiel gezeigt:

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

Der AWS Key Management Service Dienst stellt folgende Informationen bereit: [Ermitteln der Schlüssel-ID und des Schlüssel-ARN](#).

[Um den ARN einer DynamoDB-Tabelle zu ermitteln, verwenden Sie die DynamoDB-CLI Describe-Table.](#)

Informationen zu Ergebnissen für Außenstehende finden AWS ARNs Sie unter [AWS ARN Explained: Amazon Resource Name Guide](#).

Finden Sie Ressourcen nach ARN in AMS

Amazon Resource Names (ARNs) identifizieren AWS Ressourcen eindeutig. [Weitere Informationen ARNs zu ARN-Formaten finden Sie unter Amazon Resource Names \(ARNs\) und AWS Service Namespaces and ARN Formats.](#)

Note

Um Details zu einer Ressource aus ihrem ARN abzurufen, müssen Sie Zugriff auf das Konto haben, mit dem die Ressource erstellt wurde.

Es gibt keinen direkten Pfad AWS , um alle Ressourcendetails aus dem Ressourcen-ARN abzurufen, da Dienste über mehrere Ressourcentypen mit verschiedenen verwandten Informationen verfügen. Wenn Sie den ARN für eine Ressource haben, können Sie Folgendes bestimmen:

- Der zugehörige AWS Service (das dritte ARN-Segment) teilt Ihnen mit, auf welcher AWS-Konsole Sie suchen müssen, um die Ressource zu finden
- Die Ressourcen-ID (das sechste oder siebte ARN-Segment) bestätigt, dass Sie die richtige Ressource gefunden haben

Sie können auch in der AWS [CLI-Befehlsreferenz nach den für diesen Dienst verfügbaren AWS CLI-Befehlen](#) suchen, um Informationen zum Abrufen von Details zu der Ressource zu erhalten.

Anhand des folgenden ARN können Sie beispielsweise ermitteln, dass der Dienst `lambda`, das Konto `123456789012`, der Ressourcentyp und der Name der Funktion lauten `TestFunction`.

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

Auf dieser Grundlage können Sie in der [AWS CLI-Dokumentation für den Lambda-Service nachlesen](#), wie weitere Details mit verschiedenen Befehlen abgerufen werden können, z. B. `get-function` und `get-function-configuration`.

Sie können beispielsweise die folgenden Befehle verwenden, um weitere Informationen zu einer Lambda-Funktion zu erhalten, wenn Sie ihren Namen oder ARN haben:

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

Finden Sie die AMS-Kontoeinstellungen

Kontoeinstellungen, die verwendet werden, um AMS zu erstellen RFCs, Zeitpläne festzulegen und festzulegen, wer Benachrichtigungen erhält.

Einige Einstellungen werden beim Onboarding erstellt und erfordern eine Serviceanfrage, um sie zu ändern. Sie sollten sich diese Kontodaten notieren, da Sie sie für die Kommunikation mit AMS verwenden werden:

- **Anmeldeinformationen:** Wenn Sie Ihren AMS-Benutzernamen oder Ihr AMS-Passwort abrufen müssen, wenden Sie sich an Ihren lokalen IT-Administrator. AMS verwendet das Active Directory Ihres Unternehmens.

- **Cloud Service Delivery Manager (CSDM):** Diese Person ist Ihr Ansprechpartner bei AMS und steht Ihnen für Servicefragen zur Verfügung. Sie erhalten die Kontaktinformationen dieser Person beim Onboarding und sollten sie allen Mitarbeitern Ihrer Organisation zur Verfügung stellen, die mit AMS interagieren. Sie können davon ausgehen, dass Sie von dieser Person monatliche Berichte über Ihren AMS-Service erhalten.
- **Konsolenzugriff:** Sie greifen über eine URL auf die AMS-Konsole zu, die speziell für Ihr Konto eingerichtet wurde. Sie können die URL von Ihrem CSDM abrufen.
- **AMS-CLI:** Sie können die AMS-CLI über die Entwicklerressourcenseite der AMS-Konsole oder über das Distributions-Paket, das Sie von Ihrem CSDM erhalten, abrufen. Nachdem Sie das Paket für die Distributionsdateien erhalten haben, folgen Sie den unter [Installation oder Upgrade der AMS-CLI](#) beschriebenen Schritte.
- **Wartungsfenster:** Ihr Wartungsfenster bestimmt, wann das Patchen für Ihre EC2 Instances erfolgt. Das AWS Managed Services Maintenance Window (oder Maintenance Window) führt Wartungsaktivitäten für AWS Managed Services (AMS) durch und findet jeden zweiten Donnerstag im Monat von 15:00 Uhr bis 16:00 Uhr pazifischer Zeit statt. AMS kann das Wartungsfenster 48 Stunden im Voraus ändern. Möglicherweise haben Sie beim Onboarding ein anderes Fenster gewählt. Notieren Sie sich das von Ihnen gewählte Wartungsfenster.
- **Überwachung:** AMS stellt standardmäßig eine Reihe von CloudWatch Metriken bereit, aber Sie können auch zusätzliche Metriken anfordern. Wenn Sie dies tun, zeichnen Sie diese auf.
- **Logs:** Standardmäßig werden Ihre Logs unter `ams-a-ACCOUNT_ID-log-management-` gespeichert. Dabei **REGION** handelt es sich um die Region **REGION**, in der das Protokoll generiert wurde.
- **Schadensbegrenzung:** Beim Onboarding zeichnet AMS die Abhilfemaßnahmen Ihrer Wahl auf, falls ein Malware-Angriff auf Ihre Ressourcen erkannt wird. Nehmen Sie beispielsweise Kontakt mit bestimmten Personen auf. Halten Sie diese Informationen für alle Personen in Ihrer Organisation verfügbar, die mit AMS interagieren.
- **Region:** Sie können sich die VPC-Detailseite in der AMS-Konsole ansehen. Sie können diesen Befehl auch ausführen, nachdem Sie die AMS SKMS-CLI installiert haben (dieser Befehl verwendet ein SAML-Profil, entfernen Sie es, wenn Ihre Authentifizierungsmethode anders ist):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

 Important Note

Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia, `us-east-1`. Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile sam1`, ob dies Ihre Authentifizierungsmethode ist.

FQDNs In AMS suchen

Für die Zugriffsänderungstypen () von AWS Managed Services (AMSCTs) ist der vollqualifizierte Domainname oder FQDN Ihrer von AMS vertrauenswürdigen Domain in der Form von erforderlich. `C844273800838.amazonaws.com` Gehen Sie wie folgt vor, um Ihren AWS FQDN zu ermitteln:

- AWS-Konsole: Suchen Sie in der AWS Directory Service-Konsole in der Spalte Verzeichnisname nach.
- CLI: Verwenden Sie diese Befehle, während Sie in Ihrer Domain angemeldet sind:

Windows (gibt Benutzer und FQDN zurück):

```
whoami /upn
```

oder (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux:

```
hostname --fqdn
```

 Note

Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia, `us-east-1`. Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Finden Sie Verfügbarkeitszonen (AZs) in AMS

Availability Zone: Alle Konten haben mindestens zwei Availability Zones. Um die Namen Ihrer Verfügbarkeitszonen genau zu ermitteln, müssen Sie zunächst die zugehörige Subnetz-ID kennen.

- **AMS-Konsole:** Klicken Sie im Navigationsbereich auf VPCs und klicken Sie dann gegebenenfalls auf die entsprechende VPC. Wählen Sie auf der VPCs Detailseite das entsprechende Subnetz in der Tabelle der Subnetze aus, um die Seite mit den Subnetzdetails mit dem Namen der zugehörigen Availability Zone zu öffnen.
- **AMS SMS-API/CLI:**

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

 Note

Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia, `us-east-1`. Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Suchen Sie nach SNS-Themen in AMS

Ihre SNS-Themen bestimmen, wer unter verschiedenen Umständen benachrichtigt wird. AMS bietet SNS-Themen für AMI-Benachrichtigungen (siehe [AMS-AMI-Benachrichtigungen mit SNS](#)), CloudWatch Alarme und EC2 Ressourcen (siehe [Empfangen von Warnmeldungen, die von AMS generiert wurden](#)) und mehr. Um mehr über Ihre bestehenden SNS-Themen zu erfahren:

- AWS-Konsole: Verwenden Sie die SNS-Konsole, um alle Themen, Anwendungen und Abonnements sowie eine grafische Darstellung der Nachrichten anzuzeigen. Außerdem können Sie Themen erstellen, löschen, abonnieren und veröffentlichen.
- API/CLI (wenn Sie bei Ihrem AMS-Konto angemeldet sind, ist die AWS-CLI erforderlich):

Listen Sie Ihre SNS-Themen auf:

```
aws sns list-topics
```

Listen Sie Ihre SNS-Abonnements auf:

```
aws sns list-subscriptions
```

Note

Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia, us-east-1. Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben `--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Finden Sie die Backup-Einstellungen in AMS

Backups und Snapshots werden von AMS über den systemeigenen [AWS Backup](#) Service verwaltet.

Die Konfiguration wird über AWS Backup Pläne verwaltet. Sie können mehrere AWS Backup Pläne haben, die markierte Ressourcen mit Backup-Zeitplänen und Aufbewahrungsrichtlinien verknüpfen. Um Ihre AWS Backup AMS-Kontoeinstellungen zu finden, verwenden Sie die <https://>

console.aws.amazon.com/backup-Konsole oder die AWS CLI Command Reference für [Backup-Befehle](#).

Weitere Informationen zu AMS und AWS Backup finden Sie unter [Continuity Management](#).

Zugriffsverwaltung in AMS

Erfahren Sie, wie Sie mithilfe von SSH oder Remote Desktop Protocol (RDP) auf Ressourcen zugreifen und wie Sie Bastionen verwenden.

Das Zugriffsverwaltungssystem AWS Managed Services (AMS) wird beim Onboarding konfiguriert. Nur Benutzer mit der AMS IAM-Benutzerrolle, die über AMS verbunden sind, können auf AMS-Ressourcen im Konto zugreifen.

Neben dem im Folgenden beschriebenen Verbundvertrauen sind AMS-Sicherheitsgruppen ein wichtiges Element beim Zugriff auf private und öffentliche Anwendungen. Informationen zu AMS-Sicherheitsgruppen und deren Änderung finden Sie unter [Sicherheitsgruppen](#).

Themen

- [Was ist Access Management?](#)
- [Wie und wann benutzt man das Root-Benutzerkonto in AMS](#)
- [AMS Advanced-Konsole und EC2 Amazon-Zugriff](#)
- [Zugriff auf die AWS Management-Konsole und die AMS-Konsole](#)
- [Zugreifen auf Instanzen mithilfe von Bastionen](#)

Was ist Access Management?

Mit der Zugriffsverwaltung schützt AMS Ihre Ressourcen, indem es nur autorisierten und authentifizierten Zugriff gewährt. AMS verwendet eine standardmäßige IAM-Benutzerrolle und ein Instanzprofil sowie Multi-Faktor-Authentifizierung, Sicherheitsgruppen, DNS-freundliche Bastionsnamen und mehr, um Ihre Ressourcen zu schützen.

AMS konzentriert sich auf drei Zugriffsarten, die verwaltet werden müssen:

- **Konsolenzugriff:** Mithilfe des Verbunds können Benutzer im Active Directory des Kontos über Single Sign-On (SSO) auf die Konsole zugreifen. Wenn Sie die Multi-Faktor-Authentifizierung für diese Konten konfiguriert haben, können Sie weiterhin MFA benötigen, um Zugriff auf die Konsole zu erhalten.
- **Instanzzugriff mit RDP oder SSH:** Mithilfe einer Active Directory-Vertrauensstellung können Benutzer im vorhandenen Active Directory des Kontos Zugriff auf eine Instanz beantragen und sich dann mit ihren vorhandenen Unternehmensanmeldedaten erfolgreich bei einer Bastion und der

Instance authentifizieren. Wenn Sie die Multi-Faktor-Authentifizierung für diese Konten konfiguriert haben, können Sie weiterhin MFA vorschreiben, um Zugriff auf eine Instance anzufordern. AMS verwendet eine eigene MFA-Lösung, um den Zugriff von AMS-Technikern auf Instances zu beschränken.

- Anwendungszugriff: Variiert je nach Anwendungsfall.

Themen

- [Warum und wann AMS auf Ihr Konto zugreift](#)

Warum und wann AMS auf Ihr Konto zugreift

AWS Managed Services (AMS) verwaltet Ihre AWS-Infrastruktur, und manchmal greifen AMS-Betreiber und -Administratoren aus bestimmten Gründen auf Ihr Konto zu. Diese Zugriffseignisse sind in Ihren AWS CloudTrail (CloudTrail) -Protokollen dokumentiert.

Warum, wann und wie AMS auf Ihr Konto zugreift, wird in den folgenden Themen erklärt.

Auslöser für den Zugriff auf das AMS-Kundenkonto

Die Aktivität beim Zugriff auf AMS-Kundenkonten wird durch Auslöser gesteuert. Die Auslöser sind heute die AWS Tickets, die in unserem Problemmanagementsystem als Reaktion auf Alarme und Ereignisse von Amazon CloudWatch (CloudWatch) erstellt wurden, sowie auf von Ihnen eingereichte Vorfälle oder Serviceanfragen. Für jeden Zugriff können mehrere Serviceanrufe und Aktivitäten auf Host-Ebene durchgeführt werden.

Die Begründung des Zugriffs, die Auslöser und der Initiator des Triggers sind in der folgenden Tabelle aufgeführt.

Auslöser für den Zugriff

Zugriff	Initiator	Auslöser
Patchen	AMS	Problem mit dem Patch
Infrastrukturbereitstellungen	AMS	Problem mit der Bereitstellung
Untersuchung interner Probleme	AMS	Problemproblem (ein Problem, das als systemisch eingestuft wurde)

Zugriff	Initiator	Auslöser
Untersuchung und Behebung von Warnmeldungen	AMS	Operative Arbeitselemente (SSM OpsItems) von AWS Systems Manager
Manuelle RFC-Ausführung	Sie	Problem mit dem Änderungsantrag (RFC). (Nicht automatisiertes System erfordert RFCs möglicherweise AMS-Zugriff auf Ihre Ressourcen)
Untersuchung und Behebung von Vorfällen	Sie	Eingehender Support-Fall (ein Vorfall oder eine Serviceanfrage, die Sie einreichen)
Bearbeitung eingehender Serviceanfragen	Sie	

Zugriff auf das AMS-Kundenkonto (IAM-Rollen)

Bei Aktivierung greift AMS mithilfe von AWS Identity and Access Management (IAM-) Rollen auf Kundenkonten zu. Wie alle Aktivitäten in Ihrem Konto sind auch die Rollen und ihre Nutzung angemeldet. CloudTrail

Important

Ändern oder löschen Sie diese Rollen nicht.

IAM-Rollen für den AMS-Zugriff auf Kundenkonten

Name der Rolle	Kontotyp (SALZ, MALZ-Management, MALZ-Anwendung usw.)	Beschreibung
ams-service-admin	SALZ, MALZ	Automatischer Zugriff auf AMS-Services und automatisierte Infrastrukturbereitstellungen, z. B. Patch, Backup, Automated Remediation.

Name der Rolle	Kontotyp (SALZ, MALZ-Management, MALZ-Anwendung usw.)	Beschreibung
ams-application-infra-read-nur	SALZ, MALZ-Anwendung, MALZ-Tools-Anwendung	Nur lesender Zugriff für den Bediener
ams-application-infra-operations		Bedienerzugriff für incidents/service Anfragen
ams-application-infra-admin		AD-Admin-Zugriff
ams-primary-read-only	MALZ-Verwaltung	Nur lesender Zugriff für den Bediener
ams-primary-operations		Bedienerzugriff für incidents/service Anfragen
ams-primary-admin		AD-Admin-Zugriff
ams-logging-read-only	MALZ-Protokollierung	Nur lesender Zugriff durch den Betreiber
ams-logging-operations		Bedienerzugriff für incidents/service Anfragen
ams-logging-admin		AD-Admin-Zugriff
ams-networking-read-only	MALZ Networking	Nur lesender Zugriff durch den Betreiber
ams-networking-operations		Bedienerzugriff für incidents/service Anfragen
ams-networking-admin		AD-Admin-Zugriff
ams-shared-services-read-nur	Gemeinsame Dienste von MALZ	Nur lesender Zugriff durch den Betreiber
ams-shared-services-operations		Bedienerzugriff für incidents/service Anfragen

Name der Rolle	Kontotyp (SALZ, MALZ-Management, MALZ-Anwendung usw.)	Beschreibung
ams-shared-services-admin		AD-Admin-Zugriff
ams-security-read-only		Nur lesender Zugriff durch den Bediener
ams-security-operations	MALZ-Sicherheit	Bedienerzugriff für incidents/service Anfragen
ams-security-admin		AD-Admin-Zugriff
ams-access-security-analyst	SALZ, MALZ-Anwendung,	AMS-Sicherheitszugriff
ams-access-security-analyst-nur lesbar	MALZ Tools-Anwendung, MALZ Core	AMS-Sicherheit, Nur-Lese-Zugriff
Sentinel_ _Role_ 0 MBHe AdminUser PXHaz RQadu PVc CDc	SALZ	[BreakGlassRole] Wird verwendet, um Glass in die Kundenkonten einzuschleusen
PowerUserSentinel_ _Role_ S0 0 wZuPu ROOI lazDb RI9		Poweruser-Zugriff auf Kundenkonten für die RFC-Ausführung
Sentinel_ _Role_PD4 L6RW9RD0LNLKD5 ReadOnlyUser JOo	SALZ, MALZ	ReadOnly Zugriff auf Kundenkonten für die RFC-Ausführung
ams_admin_role		Administratorzugriff auf Kundenkonten für die RFC-Ausführung
AWSManagedServices _Provisioning_CustomerStacksRole		Wird verwendet, um CFN-Stacks im Namen von Kunden über Ingest zu starten und zu aktualisieren CloudFormation

Name der Rolle	Kontotyp (SALZ, MALZ-Management, MALZ-Anwendung usw.)	Beschreibung
customer_ssm_automation_role		Die Rolle wurde von CT-Ausführungen zur Runbook-Ausführung an SSM Automation übergeben
ams_ssm_automation_role	SALZ, MALZ-Anwendung, MALZ-Kern	Die Rolle wurde von den AMS-Diensten zur Runbook-Ausführung an SSM Automation übergeben
ams_ssm_iam_deployment_role	MALZ-Anwendung	Vom IAM-Katalog verwendete Rolle
ams_ssm_shared_services_intermediary_role	Gemeinsame Dienste von MALZ	Rolle, die von der Anwendung ams_ssm_automation_role verwendet wird, um bestimmte SSM-Dokumente im Shared Services-Konto auszuführen
AmsOpsCenterRole		Wird zum Erstellen und Aktualisieren von OpsItems Kundenkonten verwendet
AMSOpsItemAutoExecutionRole	SALZ, MALZ	Wird verwendet, um SSM-Dokumente abzurufen, Ressourcen-Tags zu beschreiben, zu aktualisieren OpsItems und die Automatisierung zu starten
customer-mc-ec2-Instanzen-Profil		EC2 Standard-Kundeninstanzprofil (Rolle)

Instanzzugriff anfordern

Um auf eine Ressource zuzugreifen, müssen Sie zunächst einen Änderungsantrag (RFC) für diesen Zugriff einreichen. Es gibt zwei Zugriffsarten, die Sie anfordern können: admin (Lese-/

Schreibberechtigungen) und schreibgeschützt (Standardbenutzerzugriff). Der Zugriff dauert standardmäßig acht Stunden. Diese Information ist erforderlich:

- Stack-ID oder Stack-Set für die Instance oder die Instances IDs, auf die Sie zugreifen möchten.
- Der vollqualifizierte Domainname Ihrer vertrauenswürdigen AMS-Domäne.
- Der Active Directory-Benutzername der Person, die Zugriff wünscht.
- Die ID der VPC, in der sich die Stacks befinden, auf die Sie zugreifen möchten.

Sobald Ihnen der Zugriff gewährt wurde, können Sie die Anfrage nach Bedarf aktualisieren.

Beispiele dafür, wie Sie Zugriff beantragen können, finden Sie unter [Stack Admin Access | Grant](#) oder [Stack Read-only Access | Grant](#).

Wie und wann benutzt man das Root-Benutzerkonto in AMS

Der [Root-Benutzer](#) ist der Superuser in Ihrem AWS Konto. AMS überwacht die Root-Nutzung. Wir empfehlen Ihnen, Root nur für die wenigen Aufgaben zu verwenden, für die es erforderlich ist, z. B.: Änderung Ihrer Kontoeinstellungen, Aktivierung des AWS Identity and Access Management (IAM-) Zugriffs auf Abrechnung und Kostenmanagement, Änderung Ihres Root-Passworts und Aktivierung der Multi-Faktor-Authentifizierung (MFA). Weitere Informationen finden Sie im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich](#) sind AWS Identity and Access Management .

Note

MFA ist während des AMS Advanced-Onboardings aktiviert, um den Root-Benutzerzugriff ausdrücklich zu verbieten. Der Root-Zugriff in AMS-verwalteten Konten unterscheidet sich von anderen AWS Konten und ist für die Sicherheit Ihrer gesamten AMS-verwalteten Umgebung von entscheidender Bedeutung. Die konfigurierte MFA ist eine virtuelle MFA und wird mit einem AMS-eigenen Gerät ausgeführt. Nachdem das virtuelle MFA mit Unterstützung von AMS konfiguriert wurde, wird das virtuelle Token sofort gelöscht. Dadurch wird sichergestellt, dass weder Sie noch AMS die Möglichkeit haben, sich als Root-Benutzer bei dem Konto anzumelden. Die Root-Anmeldung kann nur auf speziellen Anfragen wieder aktiviert werden (wird weiter unten erklärt), und AMS geht davon aus, dass solche Zugänge nur dann verwendet werden, wenn dies unbedingt erforderlich ist. Informationen zu MFA finden Sie unter [Sicheres neues Konto mit Multi-Faktor-Authentifizierung](#).

Der Root-Zugriff löst immer eine Antwort des AMS Security and Operations Teams aus. AMS überwacht API-Aufrufe für den Root-Zugriff und es werden Alarme ausgelöst, wenn ein solcher Zugriff erkannt wird.

Das Anfordern von Root-Zugriff unterscheidet sich zwischen den AMS-Kontotypen geringfügig.

Root-Zugriff mit AMS Advanced-Landezone für ein einzelnes Konto:

Wenn Sie eine landing zone mit einem einzigen Konto haben, wenden Sie sich an Ihren Cloud Service Deliver Manager (CSDM) und Ihre Cloud-Architekten (CAs), um sie über die erforderlichen Root-Zugriffsarbeiten zu informieren. Am besten geben Sie uns vierundzwanzig Stunden vor der geplanten Aktivität Bescheid.

Root-Zugriff mit AMS Advanced-Landezone für mehrere Konten:

Verwenden Sie für Landingzone-Konten mit mehreren Konten für Anwendungs-, Shared Services-, Sicherheits- oder Netzwerkkonten den Änderungstyp Verwaltung | Andere | Andere (ct-1e1xtak34nx76). Geben Sie das Datum, die Uhrzeit und den Zweck der Verwendung der Root-Benutzeranmeldeinformationen an und planen Sie den RFC so, dass er vierundzwanzig Stunden vor der geplanten Aktivität informiert wird. Verwenden Sie Ihr landing zone Management-Konto mit mehreren Konten, um den RFC einzureichen.

Wenden Sie sich außerdem CAs vierundzwanzig Stunden im Voraus an Ihren CSDM und teilen Sie ihm mit, welche Root-Zugriffsarbeiten Sie benötigen.

AMS-Betrieb und Sicherheitsreaktion bei Root-Nutzung:

AMS erhält einen Alarm, wenn das Root-Benutzerkonto verwendet wird. Wenn die Verwendung der Root-Anmeldeinformationen außerplanmäßig erfolgt, wenden sie sich an das AMS-Sicherheitsteam und Ihr Account-Team, um zu überprüfen, ob es sich um eine erwartete Aktivität handelt. Wenn es sich nicht um eine erwartete Aktivität handelt, arbeitet AMS mit Ihrem Sicherheitsteam zusammen, um das Problem zu untersuchen.

AMS Advanced-Konsole und EC2 Amazon-Zugriff

Zugriff auf die AMS Advanced-Konsole.

Zugriff auf Ihre EC2 Amazon-Instances.

Zugriffsanfrage einreichen:

Melden Sie sich bei Ihren AMS EC2 Amazon-Instances an:

Zugriff auf die AWS Management-Konsole und die AMS-Konsole

Während des Onboarding-Vorgangs erhalten Sie einen Anmeldenamen für die AWS Management-Konsole (mit eingeschränkten Rechten: Sie können in die AMS-Konsole und in einige Felder auf Ihrer Kundeninformationsseite schreiben). Sie können auf die AMS-Konsole zugreifen, indem Sie in der AWS Management-Konsole auf den Link Managed Services klicken. Je nach Absprache mit Ihrem IT-Administrationsteam werden entweder Verbundzugriff oder gemeinsame Anmeldeinformationen (Benutzername/Passwort) vorbereitet. Wenn Sie weitere Konten oder Gruppen erstellen möchten, senden Sie eine Serviceanfrage an AMS.

Informationen zum Zugriff auf die AWS Managementkonsole finden Sie unter [Arbeiten mit der AWS Managementkonsole](#).

Einige Tipps zur Verwendung der AMS-Konsole finden Sie unter [Verwenden der AMS-Konsole](#).

Temporärer Zugriff auf die AMS-Konsole

Wenn Sie noch keinen Identitätsanbieter (z. B. SAML) für die Authentifizierung bei AMS eingerichtet haben, können Sie temporären Zugriff auf die AMS-Konsole erhalten. Wenden Sie sich an Ihren CSDM, um in Ihrem Namen einen Antrag auf Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Create Entity or Policy Change Request (ct-3dpd8mdd9jn1r) mit den folgenden Werten einreichen zu lassen:

- **UserName:** Ein Name für die IAM-Benutzerentität, die Sie erstellen
- **AccessType:** „Konsolenzugriff“
- **UserPermissions:** „Temporärer Zugriff auf die AMS-Konsole für **USERNAME** (die Person, für die Sie temporären Zugriff wünschen)“
- **E-Mail-Benachrichtigungen:** Ihre E-Mail-Adresse, damit Sie die Anfrage genehmigen können, wenn AMS Sie dazu auffordert

 Note

Dieser RFC für den temporären Zugriff auf die AMS-Konsole erfordert eine Sicherheitsüberprüfung und Zustimmung sowohl durch Ihr internes Sicherheitsteam als auch durch AMS Global Security.

Nachdem diese Anfrage abgeschlossen ist und Sie sich anmelden können, müssen Sie den erstellten RFC genehmigen, die Genehmigung verfolgen und dem AMS-Team den Abschluss der Arbeit ermöglichen. Um den RFC zu genehmigen, suchen Sie ihn auf der Listenseite des RFC (neben dem RFC wird das Kennzeichen „Ausstehende Genehmigung“ angezeigt), wählen Sie ihn aus, um die RFC-Detailseite für diesen RFC zu öffnen, und klicken Sie dann auf Genehmigen. Beachten Sie, dass Sie AMS erst verwenden können, wenn der RFC genehmigt wurde.

Wenn der RFC erfolgreich abgeschlossen wurde, erhalten Sie von AMS Operations den neuen IAM-Benutzer und ein Passwort. Gehen Sie dann wie folgt vor:

1. Gehen Sie zur AWS Management-Konsole und melden Sie sich mit den angegebenen Anmeldeinformationen an. Sie werden aufgefordert, ein neues Passwort zu erstellen. Außerdem müssen Sie bei der Anmeldung die Multi-Faktor-Authentifizierung (MFA) einrichten. Weitere Informationen dazu finden Sie unter [Verwenden der Multi-Factor Authentication \(MFA\)](#) unter AWS.
2. Wechseln Sie in der AWS Managementkonsole zur angegebenen IAM-Rolle ().
`customer_CustomerCode_readonly_user_role`
3. Öffnen Sie die AMS Managed Services Console.

 Note

Der temporäre Zugriff ist standardmäßig auf sechzig Tage eingestellt. Sie können jedoch eine Verlängerung um dreißig Tage beantragen, indem Sie sich an Ihren CSDM wenden.

Zugreifen auf Instanzen mithilfe von Bastionen

Der gesamte Zugriff auf Ressourcen innerhalb von AMS-verwalteten Konten, sowohl für Kunden als auch für AMS-Betreiber, ist durch die Verwendung von Bastion-Hosts begrenzt. Wir verwalten sowohl Linux- als auch Windows-RDP-Bastionen für den Zugriff sowohl für Multi-Account landing zone (MALZ) als auch für Single-Account landing zone (SALZ) AMS Advanced-Konten.

Ihre Bastionen sind nur über Ihre private Verbindung (VPN oder) DX zugänglich. Direct Connect
Zusätzlich zum Firewalling zur Verhinderung von eingehendem Datenverkehr werden Bastionen
regelmäßig (mit vorhandenen Anmeldeinformationen) nach einem festen Zeitplan neu bereitgestellt.

Note

Informationen zum Verschieben von Dateien in eine EC2 Instance finden Sie unter
[Dateiübertragung: Lokaler Windows- oder MAC-PC auf Linux Amazon EC2](#).

MALZ

Sie greifen auf Ihre Account-Instances zu, indem Sie sich mit Ihren Active Directory (AD) -
Anmeldeinformationen bei einer Bastion-Instance anmelden. Amazon verwendet Bastionen,
die sich in der VPC (Netzwerkkonto) des Umkreisnetzwerks befinden, und Sie verwenden Ihre
Kundenbastionen, die sich in Ihrem Kundenbastions-Subnetz im Shared Services-Konto befinden.

Wenn Ihre AMS-Umgebung zum ersten Mal integriert ist, haben Sie je nach Ihrer Wahl zwei SSH-
Bastionen und zwei RDP-Bastionen.

SALZ

Sie greifen auf Ihre Kontoinstanzen zu, indem Sie sich mit Ihren Active Directory (AD) -
Anmeldeinformationen bei einer Bastion-Instance anmelden. AMS verwendet Bastionen, die sich
in den Subnetzen des Umkreisnetzwerks befinden, und Sie verwenden Bastionen, die sich in
Ihren privaten Subnetzen befinden.

Wenn Ihr Konto zum ersten Mal eingerichtet ist, haben Sie standardmäßig zwei RDP- und zwei
SSH-Bastionen.

Note

Als Teil der Single-Account-Landingzone stellt AMS sowohl RDP- (Windows) als auch
SSH-Bastionen (Linux) für den Zugriff auf Ihre Stacks bereit. Sie können jedoch wählen,
ob Sie nur RDP-Bastionen oder nur SSH-Bastionen verwenden möchten. Wenn Sie
beantragen möchten, dass nur RDP- oder nur SSH-Bastionen verwaltet werden, reichen
Sie eine Serviceanfrage ein.

Um auf eine Instanz zuzugreifen, benötigen Sie:

- Zugriff auf den Stack gewährt. Um Zugriff auf einen Stack zu erhalten, siehe [Stack Admin Access | Grant](#) oder [Stack Read-Only Access | Grant](#).
- Die Stack-ID, auf die Sie zugreifen möchten, damit Ihnen Zugriff auf die Instance gewährt werden kann. Informationen zur Suche nach einer Stack-ID finden Sie unter [Finden Sie den Stack IDs in AMS](#).
- Die Instanz-IP, auf die Sie zugreifen möchten. Informationen zur Suche nach einer Instanz-IP finden Sie unter [Suchen Sie nach Instanzen IDs oder IP-Adressen in AMS](#).
- Der DNS-freundliche Bastion-Name oder die Bastion-IP. Im Folgenden wird beschrieben, wie Sie DNS-freundliche Bastionsnamen verwenden und wie Sie eine Bastion-IP finden.

DNS-freundliche Bastionsnamen

AWS Managed Services (AMS) verwendet DNS-freundliche Bastionsnamen.

MALZ

Für die Multi-Account-Landingzone (MALZ) werden DNS-Einträge für die Bastionen im FQDN des von AMS verwalteten Active Directory erstellt. AMS ersetzt bei Bedarf Linux- und Windows-Bastionen. Wenn beispielsweise ein neues Bastion-AMI bereitgestellt werden muss, werden die Bastion-DNS-Einträge dynamisch aktualisiert, sodass sie auf neue, gültige Bastionen verweisen.

1. Verwenden Sie DNS-Einträge wie folgt, um auf SSH-Bastionen (Linux) zuzugreifen:
`sshbastion(1-4).Your_Domain.com`

Zum Beispiel, wo die Domain ist: Your_Domain

- `sshbastion1.Your_Domain.com`
- `sshbastion2.Your_Domain.com`
- `sshbastion3.Your_Domain.com`
- `sshbastion4.Your_Domain.com`

2. Verwenden Sie DNS-Einträge wie folgt, um auf RDP-Bastionen (Windows) zuzugreifen:.
`rdp-Username.Your_Domain.com`

Beispiel: Der Benutzername ist alex,, oder test demobob, und die Domäne lautet:
`Your_Domain.com`

- `rdp-alex.Your_Domain.com`

- `rdp-test.Your_Domain.com`
- `rdp-demo.Your_Domain.com`
- `rdp-bob.Your_Domain.com`

SALZ

Die Single-Account-Landingzone (SALZ) ersetzt bei Bedarf die Linux- und Windows-Bastionen. Wenn beispielsweise ein neues Bastion-AMI bereitgestellt werden muss, werden die Bastion-DNS-Einträge dynamisch aktualisiert, sodass sie auf neue, gültige Bastionen verweisen.

1. Verwenden Sie DNS-Einträge wie folgt, um auf SSH-Bastionen (Linux) zuzugreifen:
`sshbastion(1-4).AccountNumber.amazonaws.com`.

Wo 123456789012 ist zum Beispiel die Kontonummer:

- `sshbastion1.A123456789012.amazonaws.com`
- `sshbastion2.A123456789012.amazonaws.com`
- `sshbastion3.A123456789012.amazonaws.com`
- `sshbastion4.A123456789012.amazonaws.com`

2. Verwenden Sie DNS-Einträge wie folgt, um auf RDP-Bastionen (Windows) zuzugreifen:
`rdpbastion(1-4).ACCOUNT_NUMBER.amazonaws.com`

Wo 123456789012 ist zum Beispiel die Kontonummer:

- `rdpbastion1.A123456789012.amazonaws.com`
- `rdpbastion2.A123456789012.amazonaws.com`
- `rdpbastion3.A123456789012.amazonaws.com`
- `rdpbastion4.A123456789012.amazonaws.com`

Kosteneinsparung bei Bastionen in der Single-Account-Landezone (SALZ)

AMS bietet in der Standardkonfiguration zwei SSH-Bastionen und zwei RDP-Bastionen, damit Sie eine Verbindung zu Ihren EC2 Amazon-Instances herstellen können, und stellt in der Standardkonfiguration auch zwei DMZ-Bastionen für den Servicebetrieb bereit. Die Bastionen verwenden standardmäßig m4. große EC2 Amazon-Instances. Sie haben die Möglichkeit, die für Bastionen verwendeten EC2 Amazon-Instances auf t3.small umzustellen und so Kosten zu sparen.

Wenn Sie On-Demand-Instances, Spot-Instances oder einen Sparplan verwenden, sollten Sie diese Funktion in Betracht ziehen und Kosten sparen. Wenn Sie Reserved Instances verwenden, sollten Sie in Betracht ziehen, ob die Verwendung von t3.small-Instances Ihre Kosten senken könnte. Um den Instance-Typ zu ändern, reichen Sie einen RFC mit Management | Advanced Stack Components | EC2 Instance Stack | Resize (ct-15mazjj88xc69) CT von Ihrem AMS-Konto aus ein.

Wenden Sie sich bei weiteren Fragen an Ihren Cloud Service Delivery Manager (CSDM) oder um zu prüfen, ob Sie von dieser Funktion profitieren können.

Verwendung von Bastion-IP-Adressen

AMS-Kunden können SSH- und RDP-Bastionen, entweder die zuvor [DNS-freundliche Bastionsnamen](#) beschriebenen, oder Bastion-IP-Adressen verwenden.

So finden Sie Bastion-IP-Adressen, SSH und RDP, für Ihr Konto:

1. Nur für landing zone mit mehreren Konten: Melden Sie sich beim Shared Services-Konto an.
2. Öffnen Sie die EC2 Konsole und wählen Sie Running Instances.

Die Seite „Instances“ wird geöffnet.

3. Geben Sie im Filterfeld oben entweder ssh-bastion oder rdp-bastion ein.

Geben Sie im Filterfeld oben entweder customer-ssh oder customer-rdp ein.

Die and/or SSH-RDP-Bastionen für Ihr Konto werden angezeigt.

Beachten Sie, dass Sie zusätzlich zu Ihren SSH-Bastionen möglicherweise auch AMS-Perimeter-Netzwerkbastionen in der Liste sehen, die dafür nicht verfügbar sind.

4. Wählen Sie eine SSH- oder RDP-Bastion aus. Wenn Sie einen Windows-Computer verwenden und sich bei einer Linux-Instanz anmelden möchten, verwenden Sie eine SSH-Bastion. Wenn Sie sich bei einer Windows-Instanz anmelden möchten, verwenden Sie eine RDP-Bastion. Wenn Sie ein Linux-Betriebssystem verwenden und sich bei einer Windows-Instanz anmelden möchten, verwenden Sie eine SSH-Bastion über einen RDP-Tunnel (so können Sie auf den Windows-Desktop zugreifen). Um von einem Linux-Betriebssystem aus auf eine Linux-Instanz zuzugreifen, verwenden Sie eine SSH-Bastion.

Beispiele für den Instanzzugriff in AMS

Diese Beispiele zeigen, wie Sie sich mithilfe einer Bastion bei einer Instance in Ihrem AMS-Konto anmelden, nachdem Ihnen der Zugriff über einen RFC gewährt wurde. Informationen zur Gewährung von Zugriff finden Sie unter. [Instanzzugriff anfordern](#)

Note

Informationen zum Verschieben von Dateien in eine EC2 Instance finden Sie unter [Dateiübertragung: Lokaler Windows- oder MAC-PC auf Linux Amazon EC2](#).

Erforderliche Daten:

- DNS-freundlicher Name oder IP-Adresse von Bastion: Verwenden Sie einen DNS-freundlichen Namen, wie unter beschrieben, [DNS-freundliche Bastionsnamen](#) oder suchen Sie nach Bastion-IP-Adressen, wie unter beschrieben. [Verwendung von Bastion-IP-Adressen](#)

Note

Eine EC2 Amazon-Instance, die über eine Amazon EC2 Auto Scaling Scaling-Gruppe erstellt wurde, hat eine IP-Adresse, die hin und her wechselt, und Sie müssen Ihre EC2 Amazon-Konsole verwenden, um diese IP-Adresse zu finden.

- Benutzername (zum Beispiel `DOMAIN_FQDN\USERNAME`) und Passwort: Anmeldeinformationen für das Konto. Das `USERNAME` muss Ihr Active Directory-Benutzername sein.

Beachten Sie, dass ein Benutzername im Format `username@customerdomain.com` verwendet werden kann, aber Probleme mit Ihrer PBIS-Einrichtung verursachen kann.

- Stack-IP-Adresse: Finden Sie diese, indem Sie sich die Run-Ausgabe für den RFC ansehen, den Sie zum Starten des Stacks eingereicht haben, oder suchen Sie in der EC2 Amazon-Konsole nach der IP-Adresse der EC2 Amazon-Instance. Für eine einzelne EC2 Amazon-Instance können Sie auch den AMS SKMS-Befehl `ListStackSummaries`, um die Stack-ID und dann die Stack-IP-Adresse `GetStack` zu ermitteln. Die AMS SKMS API-Referenz finden Sie auf der Registerkarte Berichte in der AWS Artifact Console.

Greifen Sie auf die Bastion-IP-Adresse zu, entweder SSH oder RDP, je nach Bedarf, und melden Sie sich mit einem der folgenden Verfahren an.

 Note

RDP-Bastionen erlauben nur zwei gleichzeitige Verbindungen. Im besten Fall können also nur 4 Administratoren gleichzeitig eine Verbindung zu Windows-Stacks herstellen. Wenn Sie mehr Verbindungen für RDP benötigen, finden Sie im AMS-Onboarding-Leitfaden weitere Informationen unter [AMS Bastion-Optionen bei Anwendungsmigrationen/Onboarding](#).

Linux-Computer zu Linux-Instanz

Verwenden Sie SSH, um eine Verbindung zur SSH-Bastion und dann zur Linux-Instanz herzustellen.

MALZ

[Weitere Informationen zu den Friendly Bastion Names finden Sie unter DNS-Bastionen.](#)

Um eine Verbindung zur Linux-Instanz herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

1. Öffnen Sie ein Shell-Fenster und geben Sie ein:

```
ssh Domain_FQDN\\Username@SSH_bastion_name  
or SSH_bastion_IP
```

Das würde so aussehen, wenn Ihr Domain_FQDN „corp.domain.com“ lautet, Ihre Kontonummer „123456789123“ lautet, Ihre Domain „amazonaws.com“ lautet, Sie Bastion „4“ wählen und Ihr Benutzername „JoeSmith“ lautet:

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Melden Sie sich mit den Active Directory-Anmeldeinformationen Ihres Unternehmens an.
3. Wenn Sie eine Bash-Eingabeaufforderung erhalten, melden Sie sich per SSH bei der Instanz an und geben Sie dann Folgendes ein:

```
ssh Domain_FQDN\\Username@Instance_IP
```

Sie können auch das Login-Flag (-l) verwenden:

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

Weitere Informationen zu den Friendly Bastion Names finden Sie unter [DNS-Bastionen](#).

Um eine Verbindung zur Linux-Instance herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

1. Öffnen Sie ein Shell-Fenster und geben Sie ein:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name  
or SSH_BASTION_IP
```

Das würde so aussehen, wenn Ihre Kontonummer 123456789123 lautet, Sie Bastion 4 wählen und Ihr Benutzername lautet: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Melden Sie sich mit den Active Directory-Anmeldeinformationen Ihres Unternehmens an.
3. Wenn Sie eine Bash-Eingabeaufforderung erhalten, melden Sie sich per SSH bei der Instanz an und geben Sie dann Folgendes ein:

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Sie können auch das Login-Flag (-l) verwenden:

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux-Computer zur Windows-Instanz

Verwenden Sie einen SSH-Tunnel und einen RDP-Client, um von Ihrem Linux-Computer aus eine Verbindung zu einer Windows-Instanz herzustellen.

MALZ

Für dieses Verfahren ist ein Remote Desktop Connection-Client für Linux erforderlich. Das Beispiel verwendet Microsoft Remote Desktop (ein Open-Source-UNIX-Client für die Verbindung mit Windows Remote Desktop Services). Rdesktop ist eine Alternative.

 Note

Die Art und Weise, wie Sie sich bei Windows-Instanzen anmelden, kann sich je nach verwendetem Remote-Desktop-Client ändern.

Zuerst richten Sie einen SSH-Tunnel ein und melden sich dann an.

Weitere Informationen zu den Namen der freundlichen Bastion finden Sie unter [DNS-freundliche Bastionsnamen](#)

Bevor Sie beginnen:

- Fordern Sie Zugriff auf die Instance an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter [Zugriffsanforderungen](#).
- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

```
sshbastion(1-4).Your_Domain
```

Das würde so aussehen, wenn Ihr Domain_FQDN „corp.domain.com“ lautet, Ihre AMS-verwaltete Your_Domain „amazonaws.com“ lautet, Sie Bastion „4“ wählen und Ihr Benutzername „lautet: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- [Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Instance-ID oder IP-Adresse suchen.](#)

1. Richten Sie RDP über einen SSH-Tunnel von einem Linux-Desktop zu einer Windows-Instanz ein. Um den ssh Befehl mit den richtigen Werten auszugeben, gibt es mehrere Möglichkeiten, vorzugehen:

- Stellen Sie in der Linux-Shell die Variablen ein und geben Sie dann den SSH-Verbindungsbefehl ein:

```
BASTION="sshbastion(1-4).Your_Domain"  
WINDOWS="Windows_Instance_Private_IP"
```



```
AD="AD_Account_Number"  
USER="AD_Username"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

Beispiel, wenn die folgenden Werte verwendet werden:

BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"

- Fügen Sie die Variablenwerte direkt zum ssh Befehl hinzu.

In beiden Fällen würde die gerenderte Anfrage wie folgt aussehen (unter der Annahme desselben Satzes von Variablenwerten):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. Entweder: Öffnen Sie Ihren Remote Desktop Client, geben Sie die Loopback-Adresse und den Port 127.0.0.1:3389 ein und öffnen Sie dann die Verbindung.

Oder melden Sie sich über eine neue Linux-Desktop-Shell bei der Windows-Instanz an. Wenn Sie verwenden RDesktop, sieht der Befehl wie folgt aus:

```
rdesktop 127.0.0.1:3389
```

Ein Remote-Desktop-Fenster für die Windows-Instanz wird auf Ihrem Linux-Desktop angezeigt.

Tip

Wenn die Remote-Desktop-Sitzung nicht gestartet werden kann, überprüfen Sie in Schritt 1, ob die Netzwerkkonnektivität zur Windows-Instanz von der SSH-Bastion auf Port 3389 von der Shell aus zulässig ist (ersetzen Sie `private_ip_address_of_windows_instance` sie entsprechend):

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Erfolgreich:

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

SALZ

Dieses Verfahren für eine landing zone mit einem Konto erfordert einen Remote Desktop Connection-Client für Linux. Das Beispiel verwendet Microsoft Remote Desktop (ein Open-Source-UNIX-Client für die Verbindung mit Windows Remote Desktop Services). Rdesktop ist eine Alternative.

 Note

Die Art und Weise, wie Sie sich bei Windows-Instanzen anmelden, kann sich je nach verwendetem Remote-Desktop-Client ändern.

Zuerst richten Sie einen SSH-Tunnel ein und melden sich dann an.

Weitere Informationen zu den Namen der freundlichen Bastion finden Sie unter [DNS-freundliche Bastionsnamen](#)

Bevor Sie beginnen:

- Fordern Sie Zugriff auf die Instance an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter [Zugriffsanforderungen](#).
- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

Das würde so aussehen, wenn deine Kontonummer 123456789123 lautet und du Bastion 4 wählst:

```
sshbastion4.A123456789123.amazonaws.com
```

- Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter [Instanz-ID oder IP-Adresse finden](#).

1. Richten Sie RDP über einen SSH-Tunnel von einem Linux-Desktop zu einer Windows-Instanz ein. Um den ssh Befehl mit den richtigen Werten auszugeben, gibt es mehrere Möglichkeiten, vorzugehen:

- Stellen Sie in der Linux-Shell die Variablen ein und geben Sie dann den SSH-Verbindungsbefehl ein:

```
BASTION="sshbastion(1-4).AMSAccountNumber.amazonaws.com"  
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"  
AD="AD_ACCOUNT_NUMBER"  
USER="AD_USERNAME"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\"$USER@$BASTION
```

Beispiel, wenn die folgenden Werte verwendet werden:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- Fügen Sie die Variablenwerte direkt zum ssh Befehl hinzu.

In beiden Fällen würde die gerenderte Anfrage wie folgt aussehen (unter der Annahme desselben Satzes von Variablenwerten):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\njohn.doe@sshbastion4.A123456789123.amazonaws.com
```

2. Entweder: Öffnen Sie Ihren Remote Desktop Client, geben Sie die Loopback-Adresse und den Port 127.0.0.1:3389 ein und öffnen Sie dann die Verbindung.

Oder melden Sie sich über eine neue Linux-Desktop-Shell bei der Windows-Instanz an. Wenn Sie verwenden RDesktop, sieht der Befehl wie folgt aus:

```
rdesktop 127.0.0.1:3389
```

Ein Remote-Desktop-Fenster für die Windows-Instanz wird auf Ihrem Linux-Desktop angezeigt.

 Tip

Wenn die Remote-Desktop-Sitzung nicht gestartet werden kann, überprüfen Sie in Schritt 1, ob die Netzwerkkonnektivität zur Windows-Instanz von der SSH-Bastion auf Port 3389 von der Shell aus zulässig ist (ersetzen Sie `private_ip_address_of_windows_instance` sie entsprechend):

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Erfolgreich:

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp      0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Windows-Computer zur Windows-Instanz

Verwenden Sie den Windows Remote Desktop Connection Client, um von Ihrem Windows-Computer aus eine Verbindung zu einer Windows-Instanz herzustellen.

MALZ

Weitere Informationen zu den Namen der freundlichen Bastion finden Sie unter [DNS-freundliche Bastionsnamen](#).

1. Öffnen Sie das Programm Remote Desktop Connection, ein Windows-Standardprogramm, und geben Sie den freundlichen DNS-Namen der Windows-Bastion in das Feld Hostname ein.

2. Wählen Sie Connect aus. Die Remotedesktopverbindung versucht, eine RDP-Verbindung zur Bastion herzustellen.

Bei Erfolg wird ein Dialogfeld mit den Anmeldeinformationen geöffnet. Um Zugriff zu erhalten, verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens, wie Sie es für die Windows-Instanz tun würden.

3. Öffnen Sie das Remote Desktop Connection-Programm auf der Bastion und geben Sie die IP-Adresse der Windows-Instanz ein, zu der Sie eine Verbindung herstellen möchten (z. B. 10.0.0.100), und wählen Sie dann Connect. Ihre Active Directory-Anmeldeinformationen für Ihr Unternehmen sind erneut erforderlich, bevor Sie eine Verbindung mit der Windows-Instanz herstellen.

SALZ

Weitere Informationen zu den Friendly Bastion-Namen finden Sie unter [DNS-freundliche Bastionsnamen](#).

1. Öffnen Sie das Programm Remote Desktop Connection, ein Windows-Standardprogramm, und geben Sie den freundlichen DNS-Namen der Windows-Bastion in das Feld Hostname ein. Das würde beispielsweise so aussehen `rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`, wenn Ihre Kontonummer 123456789123 lautet und Sie Bastion 4 wählen, `rdpbastion4.A123456789123.amazonaws.com`
2. Wählen Sie Connect aus. Die Remotedesktopverbindung versucht, eine RDP-Verbindung zur Bastion herzustellen.

Bei Erfolg wird ein Dialogfeld mit den Anmeldeinformationen geöffnet. Um Zugriff zu erhalten, verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens, wie Sie es für die Windows-Instanz tun würden.

3. Öffnen Sie das Remote Desktop Connection-Programm auf der Bastion und geben Sie die IP-Adresse der Windows-Instanz ein, zu der Sie eine Verbindung herstellen möchten (z. B. 10.0.0.100), und wählen Sie dann Connect. Ihre Active Directory-Anmeldeinformationen

für Ihr Unternehmen sind erneut erforderlich, bevor Sie eine Verbindung mit der Windows-Instanz herstellen.

Windows-Computer zur Linux-Instanz

Gehen Sie wie folgt vor, um von einer Windows-Umgebung aus per RDP zu einer SSH-Bastion zu gelangen.

MALZ

Bevor Sie beginnen:

- [Fordern Sie Zugriff auf die Instanz an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Zugriffsanforderungen.](#)
- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

```
sshbastion(1-4).YOUR_DOMAIN
```

Das würde so aussehen, wenn YOUR_DOMAIN „myamsaddomain.com“ lautet und Sie Bastion 4 wählen:

```
sshbastion4.myamsaddomain.com
```

- Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen [finden](#) Sie unter Instanz-ID oder IP-Adresse suchen.

Um von Ihrem Windows-Computer aus eine Verbindung zur Linux-Instance herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

Verwenden Sie den nativen Windows [OpenSSH-Client](#) oder installieren Sie [PuTTY](#) auf Ihrem lokalen Computer. Weitere Informationen zu OpenSSH finden Sie unter [OpenSSH](#) in Windows.

1. Verwenden Sie das native Windows oder öffnen Sie PuTTY und geben Sie den SSH-Bastion-Hostnamen oder die IP-Adresse der SSH-Bastion ein. Zum Beispiel 10.65.2.214 (22 ist der Port, der für SSH verwendet wird; er wird standardmäßig festgelegt).

2. OpenSSH oder PuTTY versucht, eine SSH-Verbindung zur Bastion herzustellen und ein Shell-Fenster zu öffnen.
3. Verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens wie bei den RDP-Hosts, um Zugriff zu erhalten.
4. Wenn Sie eine Bash-Eingabeaufforderung erhalten, greifen Sie per SSH auf die Instanz zu. Geben Sie ein:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

Bevor Sie beginnen:

- Fordern Sie Zugriff auf die Instance an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter [Zugriffsanforderungen](#).
- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

Das würde so aussehen, wenn deine Kontonummer 123456789123 lautet und du Bastion 4 wählst:

```
sshbastion4.A123456789123.amazonaws.com
```

- Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter [Instanz-ID oder IP-Adresse finden](#).

Um von Ihrem Windows-Computer aus eine Verbindung zur Linux-Instance herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

Verwenden Sie den nativen Windows [OpenSSH-Client](#) oder installieren Sie [PuTTY](#) auf Ihrem lokalen Computer. Weitere Informationen zu OpenSSH finden Sie unter [OpenSSH](#) in Windows.

1. Verwenden Sie das native Windows oder öffnen Sie PuTTY und geben Sie den SSH-Bastion-Hostnamen oder die IP-Adresse der SSH-Bastion ein. Zum Beispiel 10.65.2.214 (22 ist der Port, der für SSH verwendet wird; er wird standardmäßig festgelegt).

2. OpenSSH oder PuTTY versucht, eine SSH-Verbindung zur Bastion herzustellen und ein Shell-Fenster zu öffnen.
3. Verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens wie bei den RDP-Hosts, um Zugriff zu erhalten.
4. Wenn Sie eine Bash-Eingabeaufforderung erhalten, greifen Sie per SSH auf die Instanz zu. Geben Sie ein:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Team- oder rollenbasierte Zugriffskontrolle in einem AMS-Konto

Szenario: Zwei Anwendungsteams A und B verwenden ein einziges AMS-Konto für ihre Apps „AA“ bzw. „BB“. Team A möchte nur auf Ressourcen für App „AA“ zugreifen, und Team B möchte nur auf Ressourcen für App „BB“ zugreifen. Wie richte ich das ein?

Verwenden Sie die ITSM-Tools des Unternehmens, um teambasierte Zugriffskontrollen (TBAC) zu implementieren. Sie könnten beispielsweise die AMS ServiceNow Connector App für die Integration mit AMS verwenden. APIs Wenden Sie sich an Ihren CSDM, um eine umfassende Anleitung zu dieser Implementierung zu erhalten.

Automatisierte Instanzkonfiguration in AMS Advanced

Der automatisierte Instanzkonfigurationsdienst AMS Advanced wird täglich ausgeführt und scannt und aktualisiert automatisch den SSM sowie die CloudWatch Agenten und Konfigurationsdateien auf Ihren verwalteten EC2 Instances. Die Updates gelten je nach Bedarf für:

- SSM und Agenten CloudWatch
- CloudWatch Konfigurationsdateien

Mit diesen Updates kann AMS auf Ihre vom AMS verwalteten EC2 Instances zugreifen und Ihre Instances so konfigurieren, dass sie entsprechende [Logs](#) und Metriken ausgeben.

Themen

- [Voraussetzungen für die automatisierte Instanzkonfiguration](#)
- [Automatische Installation des SSM-Agenten](#)
- [Automatisierte Änderungen](#)

Voraussetzungen für die automatisierte Instanzkonfiguration

Für AMS Advanced-Kunden, die Instances mit Change Management bereitstellen, müssen die folgenden Voraussetzungen erfüllt sein:

- Der SSM-Agent ist installiert und befindet sich in einem verwalteten Zustand.
- Die Instanz ist als verwaltete Instanz gekennzeichnet. (Das `aws:cloudformation:stack-name` Tag hat einen Wert, der mit `stack-` oder `beginntsc-`.)

Wenn der SSM-Agent noch nicht auf Ihrer Instance installiert ist, können Sie ihn mithilfe der auto Installationsfunktion des AMS SSM-Agenten installieren. Weitere Informationen finden Sie unter [Automatische Installation des SSM-Agenten](#).

Sie können den SSM Agent auch manuell installieren. Weitere Informationen finden Sie hier:

- Linux: [Manuelles Installieren des SSM-Agenten auf EC2 Instances für Linux - AWS Systems Manager](#)

- Windows: [Manuelles Installieren des SSM-Agenten auf EC2 Instances für Windows Server - AWS Systems Manager](#)

Weitere Informationen zum SSM-Agent finden Sie in der AWS-Dokumentation [Working with SSM Agent](#).

Automatische Installation des SSM-Agenten

Damit AMS Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwaltet, müssen Sie AWS Systems Manager SSM Agent auf jeder Instance installieren. Wenn auf Ihren Instances kein SSM Agent installiert ist, können Sie die Funktion zur automatischen Installation von AMS SSM Agent verwenden.

Note

- Diese Funktion ist nur für EC2 Instances verfügbar, die nicht zu einer Auto Scaling Scaling-Gruppe gehören und auf denen von AMS unterstützte Linux-Betriebssysteme ausgeführt werden.
- Die automatische Installationsfunktion des AMS SSM-Agenten ist standardmäßig deaktiviert. Um sie zu aktivieren, wenden Sie sich an Ihre CA oder CSDM.

Voraussetzungen für die Verwendung des SSM-Agenten

- Stellen Sie sicher, dass das mit den Ziel-Instances verknüpfte Instanzprofil über eine der folgenden Richtlinien verfügt (oder über gleichwertige Berechtigungen, die in den Zielinstanzen aufgeführt sind):
 - Amazon SSMManged EC2 InstanceDefaultPolicy
 - Amazon SSMManged InstanceCore
- Stellen Sie sicher, dass es keine Service Control-Richtlinie auf der AWS Organizations Ebene gibt, die die in den vorherigen Richtlinien aufgeführten Berechtigungen ausdrücklich verweigert.

Weitere Informationen finden Sie unter [Erforderliche Instance-Berechtigungen für Systems Manager konfigurieren](#).

- Um ausgehenden Datenverkehr zu blockieren, stellen Sie sicher, dass die folgenden Schnittstellenendpunkte auf der VPC aktiviert sind, auf der sich die Ziel-Instances befinden (ersetzen Sie „Region“ in der URL entsprechend):
 - ssm.<region>.amazonaws.com
 - ssmmessages.<region>.amazonaws.com
 - ec2-Nachrichten. <region>.amazonaws.com

Weitere Informationen finden Sie unter [Verbessern der Sicherheit von EC2 Instances mithilfe von VPC-Endpunkten für Systems Manager](#).

Allgemeine Tipps zur Aktivierung oder Fehlerbehebung bei der Verfügbarkeit verwalteter Knoten finden Sie unter [Lösung 2: Stellen Sie sicher, dass ein IAM-Instanzprofil für die Instanz angegeben wurde \(nur EC2 Instanzen\)](#).

Note

AMS stoppt und startet jede Instanz im Rahmen der automatischen Installation. Wenn eine Instance gestoppt wird, gehen die auf den Instance-Speicher-Volumes gespeicherten Daten und die im RAM gespeicherten Daten verloren. Weitere Informationen finden Sie unter [Was passiert, wenn Sie eine Instance beenden](#).

Fordern Sie die automatische Installation des SSM-Agenten auf Ihren Instances an

Wenn Ihre Konten in das AMS Accelerate Patch Add-On integriert sind, konfigurieren Sie ein Patch-Wartungsfenster (MW) für die Instances. Ein funktionierender SSM-Agent ist erforderlich, um den Patch-Vorgang abzuschließen. Wenn der SSM-Agent auf einer Instanz fehlt, versucht AMS, ihn während des Patch-Wartungsfensters automatisch zu installieren.

Note

AMS stoppt und startet jede Instanz im Rahmen der automatischen Installation. Wenn eine Instance gestoppt wird, gehen die auf den Instance-Speicher-Volumes gespeicherten Daten und die im RAM gespeicherten Daten verloren. Weitere Informationen finden Sie unter [Was passiert, wenn Sie eine Instance beenden](#).

So funktioniert die automatische Installation des SSM-Agenten

AMS verwendet EC2 Benutzerdaten, um das Installationsskript auf Ihren Instances auszuführen. Um das Benutzerdatenskript hinzuzufügen und es auf Ihren Instances auszuführen, muss AMS jede Instance beenden und starten.

Wenn Ihre Instance bereits über ein Benutzerdatenskript verfügt, führt AMS während des auto Installationsvorgangs die folgenden Schritte aus:

1. Erstellt eine Sicherungskopie des vorhandenen Benutzerdatenskripts.
2. Ersetzt das vorhandene Benutzerdatenskript durch das SSM-Agent-Installationsskript.
3. Startet die Instanz neu, um den SSM Agent zu installieren.
4. Stoppt die Instanz und stellt das ursprüngliche Skript wieder her.
5. Startet die Instanz mit dem Originalskript neu.

Automatisierte Änderungen

Der automatisierte Instance-Konfigurationsservice AMS Advanced nimmt bei Bedarf Änderungen an Ihren EC2 Instances vor.

Welche Änderungen:

- [Automatisches Aktualisieren von Code auf Linux-Instances](#)
- [Automatisches Aktualisieren von PBIS auf Linux-Instances](#)
- [Automatisches Aktualisieren der Mindestversion von SSM und Agenten CloudWatch](#)
- [CloudWatch Konfigurationsdateien, Aktualisierungsdetails](#)
- [Automatisch konfigurierte Protokolle](#)

Automatisches Aktualisieren von Code auf Linux-Instances

AMS aktualisiert automatisch den Instanzcode auf Linux-Instances. Dies trägt dazu bei, die Betriebsstabilität und Sicherheit der AMS-Komponenten und der AMS-Umgebung insgesamt zu verbessern.

Häufig gestellte Fragen:

Was ist im On Instance Code (OIC) unter Linux enthalten?

OIC enthält das AMS-Toolkit-Paket zusammen mit einigen Konfigurationsdateien und Cron-Jobs. AMS benötigt diese Dateien und Pakete für die Integration (Active Directory und andere Abhängigkeiten). CloudFormation Wir bereiten diese Dateien in das von AMS bereitgestellte System vor AMIs oder installieren sie während der Workload-Aufnahme auf Ihrer Instance.

Wann aktualisiert AMS OIC?

AMS aktualisiert OIC, wenn wir eine neue Version mit Fehlerkorrekturen oder anderen Verbesserungen veröffentlichen. Der Workflow zur Überprüfung der OIC-Version und des Updates wird täglich ausgeführt.

Automatisches Aktualisieren von PBIS auf Linux-Instances

AMS verwendet das Power Broker Identity Service (PBIS) -Modul, um Linux-Instanzen mit dem von AMS verwalteten Active Directory zu verbinden.

AMS aktualisiert PBIS auf Linux-Instances automatisch.

Häufig gestellte Fragen:

Wann aktualisiert AMS PBIS?

AMS aktiviert das PBIS-Update beim Neustart. Wenn eine neue PBIS-Version verfügbar ist, versucht AMS, die neue Version beim nächsten Instance-Neustart zu installieren.

Kann das PBIS-Update ausgeschaltet werden?

Sie können das PBIS-Update auf Instanz- oder Kontoebene deaktivieren:

- Kontoebene: Erstellen Sie einen Parameter im SSM-Parameterspeicher: Name: `/ams/skip-pbis-update`, Wert: `true` (in jedem Fall).

Note

Das Instanzprofil muss über Berechtigungen zum Lesen von SSM-Parametern verfügen. Wenn das Flag fehlt, besteht das Standardverhalten darin, das Update auszuführen.

- Instanzebene:

- Tag-basiert: Fügen Sie der Instanz das folgende Tag hinzu: Schlüssel: `skip_pbis_update`, Wert: `true` (in jedem Fall).
- Konfigurationsdatei: Fügen Sie der `/opt/aws/ams/etc/ams.conf.d/state.ini` Datei das folgende Flag hinzu: `skip_pbis_update = true`.

Note

Das Tag hat eine höhere Priorität als der SSM-Parameter. Sie können das PBIS-Update auf Kontoebene über den Parameter deaktivieren, es aber für eine einzelne (oder mehrere) Instanz (en) aktivieren, indem Sie ein Tag `Key: skip_pbis_update` hinzufügen. `Value: false`

Um eine der beschriebenen Optionen zu konfigurieren, folgen Sie dem standardmäßigen Change-Management-Prozess in Ihrer AMS-Umgebung.

Automatisches Aktualisieren der Mindestversion von SSM und Agenten CloudWatch

Die AMS Advanced-Mindestversion (des SSM oder der CloudWatch Agenten) ist die Version, die vom AMS-Serviceteam getestet und für Ihr Betriebssystem vorab genehmigt wurde. Wir versuchen, proaktiv zu bleiben und die neueste stabile und kompatible Version auszuführen, sodass sich die Versionsnummer im Laufe der Zeit ändert. Sie können die aktuelle Mindestversion finden, indem Sie eine Serviceanfrage an AMS stellen.

- SSM-Agentenverwaltung

Der Amazon SSM-Agent ist für die Ausführung von Remote-Befehlen auf der Instance verantwortlich. Die Automatisierung der Instance-Konfiguration stellt sicher, dass der SSM-Agent die Mindestversion ausführt.

- Cloudwatch Agentenverwaltung

Der CloudWatch Amazon-Agent ist für die Ausgabe von Betriebssystemprotokollen und Metriken verantwortlich. Bei der automatisierten Instance-Konfiguration wird Folgendes ausgeführt:

- Deaktiviert bei Bedarf den alten CloudWatch Log-Agenten und migriert die Konfiguration auf den neuen Unified Agent CloudWatch

- Wenn auf Ihrer Instance der CloudWatch Legacy-Log Agent ausgeführt wird, deaktiviert die automatische Instanzkonfiguration den alten CloudWatch Log Agent-Dienst und migriert seine Konfiguration auf den Unified Agent. CloudWatch
- Passt Ihre CloudWatch Konfiguration so an, dass entsprechende Protokolle und Metriken ausgegeben werden.

Betroffene Dateien und Verzeichnisse:

- Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\
- Linux
 - /opt/aws/amazon-cloudwatch-agent/etc/
 - /-cloudwatch-agent.d/ opt/aws/amazon-cloudwatch-agent/etc/amazon
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch Konfigurationsdateien, Aktualisierungsdetails

Wir lesen Ihre benutzerdefinierten CloudWatch Konfigurationen (nur JSON) aus den folgenden CloudWatch Verzeichnissen (siehe [empfohlene Verzeichnisse](#)) und führen sie mit der CloudWatch AMS-Standardkonfiguration zusammen:

- CloudWatch Dateien
 - Auf der Instanz:
 - Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\
 - %ProgramFiles%\ ModulesWindowsPowerShell\ AWSManaged Services.Logging.Utilities\ Files\ Config.json
 - Linux
 - opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon/-cloudwatch-agent.json
 - Auf Amazon S3:
 - Windows:
 - [https://ams-configuration-artifacts-**REGION_NAME**.s3.**REGION_NAME**.amazon.aws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json](https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazon.aws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json)

- Linux:
 - https://s3.amazonaws.com/ams-configuration-artifacts/REGION_NAME/REGION_NAME/amazon.aws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json

Automatisch konfigurierte Protokolle

Wir konfigurieren Ihre Instanz so, dass sie die folgenden Protokolle schreibt.

- Windows:
 - SSMAgentAmazon-Protokoll
 - AmazonCloudWatchAgentLog
 - SSMErrorAmazon-Protokoll
 - AmazonCloudFormationLog
 - ApplicationEventLog
 - EC2ConfigServiceEventLog
 - MicrosoftWindowsAppLockerEXEAndDLLEventLoggen
 - MicrosoftWindowsAppLockerMSIAndScriptEventLog
 - MicrosoftWindowsGroupPolicyOperationalEventLog
 - SecurityEventLog
 - SystemEventLog
- Linux:
 - /var/log/amazon/ssm/amazon-ssm-agent.log
 - /var/log/amazon/ssm/errors.log
 - /var/log/audit/audit
 - /var/log/cloud-init-output.log
 - /var/log/cloud-init.log
 - /var/log/cron
 - /var/log/dpkg.log
 - /var/log/maillog
 - /var/log/messages
 - /var/log/secure
 - /var/log/spooler

- `/var/log/syslog`
- `/.log var/log/yum`
- `/.log var/log/zypper`

Überwachung und Eventmanagement in AMS

Themen

- [Was ist Überwachung?](#)
- [Was überwacht das AMS-Überwachungssystem?](#)
- [So funktioniert die Überwachung](#)
- [Die Überwachungskonfiguration für ein AMS-Konto anzeigen](#)
- [Änderung der Überwachungskonfiguration für ein AMS-Konto](#)
- [Benachrichtigungen über anwendungsbezogene Vorfälle in AMS](#)
- [Verwendung OpsCenter in AMS](#)
- [Warnmeldungen von AMS](#)
- [Zusätzliche CloudWatch Alarme in AMS erstellen](#)
- [Benutzerdefinierte CloudWatch Metriken und Alarme in AMS erstellen](#)
- [Verwenden von CloudWatch Application Insights für .Net und SQL Server in AMS](#)
- [Verwenden von Amazon EventBridge Managed Rules in AMS](#)
- [Vertrauenswürdiger Remediator in AMS](#)

Das Überwachungssystem AWS Managed Services (AMS) überwacht Ihre AMS-Ressourcen auf Ausfälle, Leistungseinbußen und Sicherheitsprobleme. Das AMS-Überwachungssystem stützt sich auf AWS-Services wie Amazon CloudWatch (CloudWatch), Amazon GuardDuty, Amazon Macie und AWS Health. Zusätzlich zum Überwachungssystem bietet AMS auch Schutz vor Malware auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Informationen zu den Standardeinstellungen für Endpoint Security (EPS) finden Sie unter [TrendMicro DeepSecurity Endpunktsicherheit \(EPS\)](#)

Die AMS-Überwachung bietet folgende Vorteile:

- Eine Überwachungsbasis, sodass Sie über ein Standardschutzniveau verfügen, auch wenn Sie keine andere Überwachung für Ihre verwalteten Konten konfigurieren. Weitere Informationen finden Sie unter [Warnmeldungen aus der Basisüberwachung in AMS](#).
- Ermittlungswarnungen, um die geeignete Maßnahme zu ermitteln. Wenn beispielsweise Aktivitäten GuardDuty gefunden werden, die auf Brute-Forcing-Versuche gegen eine EC2 Amazon-Instance

hinweisen, analysiert AMS VPC-Flowlogs, um den Ursprung und den Kontext der Aktivität zu verstehen.

- Behebung von Warnmeldungen, sofern möglich, um die Auswirkungen auf Ihre Anwendungen zu verhindern oder zu reduzieren. Wenn Sie beispielsweise eine eigenständige EC2 Amazon-Instance verwenden und diese die Systemintegritätsprüfung nicht besteht, versucht AMS, die Instance wiederherzustellen, indem sie gestoppt und neu gestartet wird. Weitere Informationen finden Sie unter [Automatische AMS-Behebung von Warnmeldungen](#).
- Transparenz über aktive und zuvor behobene Warnmeldungen mithilfe von OpsCenter. Wenn Sie beispielsweise eine unerwartet hohe CPU-Auslastung auf einer EC2 Amazon-Instance haben, können Sie Zugriff auf die AWS Systems Manager Manager-Konsole anfordern (einschließlich Zugriff auf die OpsCenter Konsole) und diese OpsItem direkt in der OpsCenter Konsole anzeigen.

Was ist Überwachung?

Das AMS-Überwachungssystem überwacht Ihre AWS Ressourcen auf Ausfälle, Leistungseinbußen und Sicherheitsprobleme. Als verwaltetes Konto konfiguriert und implementiert AMS Alarme für die entsprechenden AWS Ressourcen, überwacht sie und führt gegebenenfalls Abhilfemaßnahmen durch.

Das AMS-Überwachungssystem generiert Warnmeldungen auf der Grundlage der Überwachungskonfiguration in Ihrem Konto. Die Überwachungskonfiguration eines Kontos bezieht sich auf alle Ressourcenparameter im Konto, die eine Warnung auslösen. Informationen zu den Ressourcenparametern finden Sie unter [Warnmeldungen aus der Basisüberwachung in AMS](#). Die Überwachungskonfiguration eines Kontos umfasst CloudWatch Alarmdefinitionen und CloudWatch Ereignisregeln, die die Warnung (Alarm oder Ereignis) generieren.

Die grundlegende Überwachungskonfiguration besteht aus einer Reihe von Alarmdefinitionen ([Warnmeldungen aus der Basisüberwachung in AMS](#)), die von AMS für die Überwachung der Ressourcen in Ihrem verwalteten Konto zusammengestellt wurden. Die Überwachungskonfiguration eines Kontos kann aufgrund von Änderungen, die Sie angefordert haben, von der Basiskonfiguration abweichen.

Eine Benachrichtigung über bevorstehende, andauernde, sich zurückziehende oder potenzielle Ausfälle, Leistungseinbußen oder Sicherheitsprobleme, die durch die in einem Konto konfigurierte Basisüberwachung verursacht werden, wird als Warnung bezeichnet. Beispiele für Warnmeldungen sind ein CloudWatch Amazon-Alarm, ein CloudWatch Amazon-Ereignis, ein Ereignis oder ein Finding

from AWS-Service wie Amazon GuardDuty und ein Ereignis oder eine Warnung von Trend Micro Deep Security.

Warnmeldungen von sicherheitsrelevanten AWS-Services wie Amazon GuardDuty, Amazon Macie oder Trend Micro Deep Security werden als Sicherheitswarnungen bezeichnet, um sie von anderen Warnungstypen zu unterscheiden.

Die AMS-Überwachung bietet folgende Vorteile:

- Die Möglichkeit, die grundlegenden Ressourcenalarme an Ihre Anforderungen anzupassen.
- Automatische Behebung von Warnmeldungen, wenn möglich, um die Auswirkungen auf Ihre Anwendungen zu verhindern oder zu verringern. Wenn Sie beispielsweise eine eigenständige EC2 Amazon-Instance verwenden und diese die Systemintegritätsprüfung nicht besteht, versucht AMS, die Instance wiederherzustellen, indem sie gestoppt und neu gestartet wird. Weitere Informationen finden Sie unter [Automatische AMS-Behebung von Warnmeldungen](#).
- Transparenz über aktive und zuvor behobene Warnmeldungen mithilfe von OpsCenter. Wenn Sie beispielsweise eine unerwartet hohe CPU-Auslastung auf einer EC2 Amazon-Instance haben, können Sie Zugriff auf die AWS Systems Manager Konsole anfordern (einschließlich Zugriff auf die OpsCenter Konsole) und diese OpsItem direkt in der OpsCenter Konsole anzeigen.
- Untersuchung von Warnmeldungen, um die geeigneten Maßnahmen zu ermitteln.
- Benachrichtigungen, die auf der Grundlage der Konfiguration in Ihrem Konto und der unterstützten AWS Dienste generiert werden. Die Überwachungskonfiguration eines Kontos bezieht sich auf alle Ressourcenparameter im Konto, die eine Warnung auslösen. Die Überwachungskonfiguration eines Kontos umfasst CloudWatch Alarmdefinitionen und EventBridge (früher als CloudWatch Ereignisse bezeichnet), die die Warnung auslösen (Alarm oder Ereignis). Weitere Hinweise zu Ressourcenparametern finden Sie unter [Warnmeldungen aus der Basisüberwachung in AMS](#).
- Benachrichtigung über drohende, andauernde, sich wiederholende oder potenzielle Ausfälle, Leistungseinbußen oder Sicherheitsprobleme, die durch die in einem Konto konfigurierte Basisüberwachung verursacht werden (auch als Warnung bezeichnet). Beispiele für Warnmeldungen sind ein CloudWatch Alarm, ein Ereignis oder ein Ergebnis aus einem AWS-Service, z. B. GuardDuty oder AWS Health.

Was überwacht das AMS-Überwachungssystem?

Gemäß dem Modell der gemeinsamen Verantwortung von AWS Managed Services (AMS) überwacht das AMS-Überwachungssystem Ihre AWS-Infrastruktur. Einzelheiten zur Basisüberwachung in AMS,

einschließlich der überwachten AWS-Ressourcen und der Art der Warnungen für jede Ressource, finden Sie unter [Warnmeldungen aus der Basisüberwachung in AMS](#). Bei EC2 Amazon-Instances überwacht AMS das Betriebssystem und bietet eine Basisüberwachung auf der Grundlage von Betriebssystemmetriken wie CPU-Auslastung und Root-Volume-Nutzung.

Wir empfehlen, die AMS-Überwachung durch zusätzliche Überwachung mithilfe von AWS-Services zu ergänzen, die auf Ihre Anwendung zugeschnitten sind. [Anleitungen zur Überwachung der Verfügbarkeit finden Sie im Abschnitt „Überwachung und Alarmierung“ in diesem Whitepaper Reliability Pillar](#). Sie können Ihre eigene Überwachung so konfigurieren, dass sie Ihren betrieblichen Anforderungen entspricht. Wie das geht, erfahren Sie unter und. [Zusätzliche CloudWatch Alarmer in AMS erstellen](#) [Benutzerdefinierte CloudWatch Metriken und Alarmer in AMS erstellen](#)

Proaktive Überwachung des Active Directory-Vertrauens in AMS durch die Landing Zone mit einem einzigen Konto

Die AMS Single Account landing zone (SALZ) überwacht den Status der unidirektionalen Vertrauensstellung (en) zwischen dem Managed Active Directory (AD) in Ihrem AMS-verwalteten Konto und Ihrer Unternehmensdomain. Die unidirektionale Vertrauensstellung mit Managed AD ist für Zugriffs- und Instanzanmeldeanfragen von entscheidender Bedeutung. Mit dieser neuen Überwachung reagiert AMS nun proaktiv auf vertrauensbezogene Probleme und reduziert die durchschnittliche Zeit für die Erkennung von zugriffsbezogenen Vorfällen.

Diese Funktion wird automatisch in Ihren AWS Managed Services (AMS) -Konten aktiviert.

Es gibt geringfügige Auswirkungen auf die Kosten. Die Funktion verwendet vier CloudWatch AWS-Metriken und zwei CloudWatch AWS-Alarmer für eine Vertrauensstellung.

So funktioniert die Überwachung

Sehen Sie sich die folgenden Grafiken zur Überwachungsarchitektur in AWS Managed Services (AMS) an.

Das folgende Diagramm bietet einen allgemeinen Überblick über den Workflow zur Überwachung der AMS-Landzone mit mehreren Konten und der AMS-Landzone mit einem Konto.

- **Generierung:** Zum Zeitpunkt der Kontoeröffnung konfiguriert AMS die Basisüberwachung (eine Kombination aus CloudWatch (CW-) Alarmen und CW-Ereignisregeln) für all Ihre Ressourcen, die

in einem verwalteten Konto erstellt wurden. Die Basisüberwachungskonfiguration generiert eine Warnung, wenn ein CW-Alarm ausgelöst oder ein CW-Ereignis ausgelöst wird.

- **Aggregation:**
 - Landezone für mehrere Konten: Benachrichtigungen werden von Ihren Ressourcen in den Konten der Anwendung und der zentralen Organisationseinheit generiert und an das AMS-Überwachungssystem gesendet, indem sie über das Sicherheitskonto weitergeleitet werden.
 - Landing Zone für ein einzelnes Konto: Alle von Ihren Ressourcen generierten Benachrichtigungen werden an das AMS-Überwachungssystem gesendet, indem sie an ein SNS-Thema im Konto weitergeleitet werden.
 - Sie können auch konfigurieren, wie AMS Warnmeldungen EC2 gruppiert. AMS gruppiert entweder alle Warnungen, die sich auf dieselbe EC2 Instanz beziehen, zu einem einzigen Vorfall oder erstellt je nach Wunsch einen Vorfall pro Warnung. Sie können diese Konfiguration jederzeit ändern, indem Sie mit Ihrem Cloud Service Delivery Manager oder Cloud Architect zusammenarbeiten. Dies funktioniert auf die gleiche Weise, unabhängig davon, ob Sie die Landing Zone mit mehreren Konten oder die Landing Zone mit einem Konto verwenden.
- **Verarbeitung:** AMS analysiert die Warnmeldungen und verarbeitet sie auf der Grundlage ihres Auswirkungspotenzials. Warnmeldungen werden wie im Folgenden beschrieben verarbeitet.
 - Warnmeldungen mit bekannten Auswirkungen auf den Kunden: Diese führen zur Erstellung eines neuen Vorfallberichts, und AMS folgt dem Incident-Management-Prozess. Informationen zum Incident-Management finden Sie unter [Reaktion auf AMS-Vorfälle](#).

Beispielwarnung: Eine EC2 Amazon-Instance besteht eine Systemintegritätsprüfung nicht. AMS versucht, die Instance wiederherzustellen, indem sie gestoppt und neu gestartet wird.

- Benachrichtigungen mit ungewisser Auswirkung auf den Kunden: Für diese Art von Benachrichtigungen sendet AMS einen Vorfallbericht, in dem Sie in vielen Fällen aufgefordert werden, die Auswirkungen zu überprüfen, bevor AMS Maßnahmen ergreift. Wenn die infrastrukturbezogenen Prüfungen jedoch bestanden werden, sendet AMS Ihnen keinen Vorfallbericht.

Beispiel: Eine Warnung für eine CPU-Auslastung von > 85% für mehr als 10 Minuten auf einer EC2 Amazon-Instance kann nicht sofort als Vorfall eingestuft werden, da dieses Verhalten je nach Nutzung zu erwarten sein könnte. In diesem Beispiel führt AMS Automation infrastrukturbezogene Prüfungen der Ressource durch. Wenn diese Prüfungen erfolgreich sind, sendet AMS keine Warnmeldung, auch wenn die CPU-Auslastung 99% überschritten hat. Wenn Automation feststellt, dass infrastrukturbezogene Prüfungen an der Ressource fehlschlagen, sendet AMS eine Warnmeldung und prüft, ob Abhilfemaßnahmen erforderlich

sind. Warnmeldungen werden in diesem Abschnitt ausführlich behandelt. AMS bietet in der Benachrichtigung Optionen zur Risikominderung. Wenn Sie auf die Benachrichtigung antworten, in der bestätigt wird, dass es sich bei der Warnung um einen Vorfall handelt, erstellt AMS einen neuen Vorfallbericht und der AMS-Incident-Management-Prozess beginnt. Servicebenachrichtigungen, bei denen die Antwort „keine Auswirkungen auf den Kunden“ oder drei Tage lang überhaupt keine Antwort erhalten, werden als gelöst markiert, und die entsprechende Warnung wird als gelöst markiert.

- Benachrichtigungen ohne Auswirkungen auf den Kunden: Wenn AMS nach der Auswertung feststellt, dass die Warnung keine Auswirkungen auf den Kunden hat, wird die Warnung geschlossen.

AWS Health Benachrichtigt beispielsweise über eine EC2 Instanz, die ersetzt werden muss, diese Instanz aber inzwischen beendet wurde.

EC2 Benachrichtigungen, gruppiert nach Instanzen

Sie können die AMS-Überwachung so konfigurieren, dass Warnmeldungen derselben EC2 Instanz zu einem einzigen Vorfall zusammengefasst werden. Ihr Cloud Service Delivery Manager oder Cloud Architect kann dies für Sie konfigurieren. Es gibt vier Parameter, die Sie für jedes von AMS verwaltete Konto konfigurieren können.

1. Umfang: Wählen Sie entweder kontoweit oder tagbasiert.

- Um eine Konfiguration anzugeben, die für jede EC2 Instanz in diesem Konto gilt, wählen Sie scope = account-wide.
- Um eine Konfiguration anzugeben, die nur für EC2 Instanzen in diesem Konto mit einem bestimmten Tag gilt, wählen Sie scope = tag-based.

2. Gruppierungsregel: Wählen Sie entweder „klassisch“ oder „Instanz“.

- Um die Gruppierung auf Instanzebene für jede Ressource in Ihrem Konto zu konfigurieren, wählen Sie Bereich = Kontoweit und Gruppierungsregel = Instanz.
- Um bestimmte Ressourcen in Ihrem Konto für die Gruppierung auf Instanzebene zu konfigurieren, taggen Sie diese Instanzen und wählen Sie dann Bereich = Tag-basiert und Gruppierungsregel = Instanzebene.
- Um die Instanzgruppierung nicht für Benachrichtigungen in Ihrem Konto zu verwenden, wählen Sie Gruppierungsregel = klassisch.

3. Interaktionsoption: Wählen Sie entweder „Keine“, „Nur Bericht“ oder „Standard“.

- Damit AMS während der aktiven Konfiguration keine Vorfälle erstellt oder Automatisierungen für Alarme von diesen Ressourcen aus durchführt, wählen Sie „Keine“.
 - Damit AMS keine Vorfälle erstellt oder Automatisierungen für Alarme aus diesen Ressourcen ausführt, solange die Konfiguration aktiv ist, und keine automatisierten Systems Manager Manager-Dokumente ausführt, sondern Aufzeichnungen dieser Ereignisse in Ihre Berichterstattung einbezieht, wählen Sie Nur Bericht. Dies kann nützlich sein, wenn Sie die Anzahl der Support-Anfragen reduzieren möchten, mit denen Sie zu tun haben, und wenn einige Vorfälle, die von einigen Ressourcen stammen, nicht sofort bearbeitet werden müssen, z. B. wenn es sich um Vorfälle handelt, bei denen es sich nicht um ein produktives Konto handelt.
 - Wählen Sie Standard, damit AMS Ihre Benachrichtigungen verarbeiten, Automatisierungen ausführen und bei Bedarf Incident-Fälle erstellen kann.
4. Lösung nach: Wählen Sie entweder 24 Stunden, 48 Stunden oder 72 Stunden. Stellen Sie abschließend ein, wann Vorfälle automatisch geschlossen werden. Wenn die Zeit seit der letzten Fallkorrespondenz den konfigurierten Wert „Nach lösen“ erreicht, wird der Vorfall geschlossen.

Warnungsbenachrichtigung

Als Teil der Alert-Verarbeitung erstellt AWS Managed Services (AMS) auf der Grundlage der Auswirkungsanalyse einen Vorfall und leitet den Incident-Management-Prozess zur Behebung ein, sobald die Auswirkungen festgestellt werden können. Wenn die Auswirkung nicht festgestellt werden kann, sendet AMS im Rahmen einer Servicemeldung eine Warnmeldung an die mit Ihrem Konto verknüpfte E-Mail-Adresse. In einigen Szenarien wird diese Warnmeldung nicht gesendet. Wenn die infrastrukturbezogenen Prüfungen beispielsweise aufgrund einer Warnung bei hoher CPU-Auslastung erfolgreich sind, wird keine Warnmeldung an Sie gesendet. Weitere Informationen finden Sie im Diagramm zur AMS-Überwachungsarchitektur für den Prozess zur Behandlung von Warnmeldungen unter: [So funktioniert die Überwachung](#)

Tag-basierte Warnmeldung

Verwenden Sie Tags, um Warnmeldungen für Ihre Ressourcen an verschiedene E-Mail-Adressen zu senden. Es hat sich bewährt, tagbasierte Warnmeldungen zu verwenden, da Benachrichtigungen, die an eine einzige E-Mail-Adresse gesendet werden, zu Verwirrung führen können, wenn mehrere Entwicklerteams dasselbe Konto verwenden. Tag-basierte Warnmeldungen werden von den von Ihnen ausgewählten [EC2 Benachrichtigungen, gruppiert nach Instanzen](#) Einstellungen nicht beeinflusst.

Mit tagbasierten Warnmeldungen können Sie:

- Benachrichtigungen an eine bestimmte E-Mail-Adresse senden: Taggen Sie Ressourcen mit Benachrichtigungen, die an eine bestimmte E-Mail-Adresse gesendet werden müssen, mit demkey = `OwnerTeamEmail`, value = `EMAIL_ADDRESS`.
- Benachrichtigungen an mehrere E-Mail-Adressen senden: Um mehrere E-Mail-Adressen zu verwenden, geben Sie eine durch Kommas getrennte Werteliste an. Zum Beispiel key = `OwnerTeamEmail`, value = `EMAIL_ADDRESS_1`, `EMAIL_ADDRESS_2`, `EMAIL_ADDRESS_3`, ... Die Gesamtzahl der Zeichen für das Wertfeld darf 260 nicht überschreiten.
- Verwenden Sie einen benutzerdefinierten Tag-Schlüssel: Um einen benutzerdefinierten Tag-Schlüssel zu verwenden, geben Sie Ihrem CSDM den Namen des benutzerdefinierten Tag-Schlüssels in einer E-Mail an, in der ausdrücklich Ihre Zustimmung zur Aktivierung automatisierter Benachrichtigungen für die tagbasierte Kommunikation erteilt wird. Es hat sich bewährt, für alle Ihre Instances und Ressourcen dieselbe Tagging-Strategie für Kontakt-Tags zu verwenden.

Note

Der Schlüsselwert `OwnerTeamEmail` muss nicht in Camel Case angegeben werden. Bei Tags wird jedoch zwischen Groß- und Kleinschreibung unterschieden, und es empfiehlt sich, das empfohlene Format zu verwenden.

Die E-Mail-Adresse muss vollständig angegeben werden, mit dem „at“-Zeichen (@), um den lokalen Teil von der Domain zu trennen. Beispiele für ungültige E-Mail-Adressen:

`Team.AppATabc.xyz` oder `john.doe`. Allgemeine Hinweise zu Ihrer Tagging-Strategie finden Sie unter [Tagging-Ressourcen AWS](#). Fügen Sie Ihren Tags keine persönlich identifizierbaren Informationen (PII) hinzu. Verwenden Sie nach Möglichkeit Verteilerlisten oder Aliase.

Tag-basierte Warnmeldungen werden für Ressourcen der folgenden Amazon Services unterstützt: EC2, Elastic Block Store (EBS), Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS) OpenSearch, Elastic File System (EFS) und VPN. FSx Site-to-Site

Die Überwachungskonfiguration für ein AMS-Konto anzeigen

Die Überwachungskonfiguration eines Kontos besteht aus zwei wichtigen Teilen, die Sie einsehen können:

- CloudWatch Alarme: Sie können alle CW-Alarme im Konto einsehen, indem Sie auf der CloudWatch Konsole verschiedene Dienste auswählen, die Sie interessieren.
- CloudWatch Ereignisse:
 - Landezone für mehrere Konten: CloudWatch Ereignisse, die im Konto überwacht wurden, können gefunden werden, indem nach allen CW-Ereignisregeln mit der Zeichenfolge gefiltert wird. "ams -"
 - Landing Zone für ein einzelnes Konto: Die im Konto überwachten CloudWatch Ereignisse können gefunden werden, indem nach allen CW-Ereignisregeln mit der Zeichenfolge gefiltert wird. "mc -"

Änderung der Überwachungskonfiguration für ein AMS-Konto

Sie können Ihre grundlegende Überwachungskonfiguration für EC2 Amazon-Ressourcen ändern. Informationen zu den Warnmeldungen, die konfiguriert werden können, finden Sie unter [Warnmeldungen aus der Basisüberwachung in AMS](#). Sie können die Alarmdefinition und das Alarmziel ändern oder die Alarmbenachrichtigung für die Basismonitore deaktivieren, sodass die Warnmeldungen den Betriebsanforderungen Ihrer Anwendung entsprechen. Sie können einige oder alle der zuvor genannten Änderungen beantragen, indem Sie ein CT (ct-0xdawir96cy7k) mit den folgenden Angaben einreichen.

- Instanz IDs [optional, falls nicht erwähnt, fallen alle Instanzen im Konto in den Geltungsbereich]
- CloudWatch Metrikname, zum Beispiel CPU-Auslastung/swap-free/ IOwait
- Ziel — E-Mail-ID//Telefonnummer für SMS/SNS-Thema

Weitere Informationen zu den Änderungen, die Sie in der Basiskonfiguration der Überwachung beantragen können, finden Sie in der [CloudWatch Amazon-Dokumentation](#).

Benachrichtigungen über anwendungsbezogene Vorfälle in AMS

Verwenden Sie anwendungsorientierte automatische Benachrichtigungen zu Vorfällen, um Ihr Kommunikationserlebnis für Supportfälle, die AMS in Ihrem Namen erstellt, individuell zu gestalten. Wenn Sie diese Funktion verwenden, ruft AMS benutzerdefinierte Workload-Einstellungen von ab, [AWS Service Catalog AppRegistry](#) um Ihre AMS-Incident-Kommunikation mit Metadaten zu Ihren Anwendungen anzureichern und den Schweregrad der von AMS in Ihrem Namen erstellten

Support-Fälle individuell anzupassen. Um diese Funktion nutzen zu können, müssen Sie zunächst die Bereitstellung AWS Service Catalog AppRegistry in Ihrem AMS-Konto vornehmen.

Weitere Informationen zu den Standardeinstellungen für die AMS-Überwachung finden Sie unter [Überwachung und Eventmanagement in AMS](#).

Bereitstellung AppRegistry in Ihrem AMS-Konto und Erstellung von Anwendungen

Der AppRegistry Service ist im Self-Service Provisioning (SSP) -Modus für Ihr AMS-Konto verfügbar. Anweisungen, wie Sie Zugriff beantragen, finden Sie unter [Verwenden von AMS SSP zur Bereitstellung AWS Service Catalog AppRegistry in](#) Ihrem AMS-Konto.

Verwenden Sie nach der Bereitstellung eine der folgenden Methoden AppRegistry, um Anwendungen zu erstellen:

1. AWS Konsole: Weitere Informationen zum Erstellen einer Anwendung AppRegistry über die AWS-Konsole finden Sie unter [Creating Applications](#) im AWS Service Catalog AppRegistry Administratorhandbuch.
2. CloudFormation: Sie können Ihre AppRegistry Anwendung genauso definieren wie jede andere Ressource. Weitere Informationen finden Sie unter [AWS Service Catalog AppRegistry Ressourcentyp-Referenz](#) im CloudFormation -Benutzerhandbuch.

Erstellen Sie Tags, um die Anreicherung von Kundenvorgängen zu ermöglichen

Sie müssen Ihre Anwendungen taggen, bevor AMS auf Anwendungsmetadaten zugreifen kann. In der folgenden Tabelle sind die erforderlichen Tags aufgeführt.

Tag-Schlüssel	Tag-Wert
ams-verwaltet	true

Passen Sie den Schweregrad der AMS-Supportfälle für Ihre Anwendungen an

Sie können den Schweregrad der von AMS erstellten Supportfälle anpassen, indem Sie angeben, wie wichtig Ihre Anwendung für Ihr Unternehmen ist. Diese Einstellung wird durch eine Attributgruppe gesteuert, die Ihrer Anwendung in zugeordnet ist AppRegistry. Der Name der Attributgruppe muss dem folgenden Muster entsprechen:

```
AMS.<ApplicationName>.CommunicationOptions
```

Im vorherigen Muster `ApplicationName` muss der mit dem Namen übereinstimmen, der AppRegistry bei der Erstellung der Anwendung verwendet wurde.

Beispielinhalt:

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

SchemaVersion

Dies bestimmt die Schemaversion, die Sie verwenden, und die Teilmenge der verfügbaren Funktionen.

Schemaversion	Funktion
1,0	Maßgeschneiderter Schweregrad für Supportfälle basierend auf dem Kritikalitätswert

Kritikalität

Die Wichtigkeit dieser Anwendung bestimmt den Schweregrad der von den automatisierten AMS-Systemen erstellten Supportfälle.

Zulässige Werte:

```
low|normal|high|urgent|critical
```

Weitere Informationen zu Schweregraden finden Sie [SeverityLevel](#) in der AWS -Support API-Referenz.

Erforderlich: Ja

Überprüfen Sie die erforderlichen Berechtigungen

Um diese Funktion nutzen zu können, benötigt AMS Zugriff auf die folgenden Berechtigungen: AWS Identity and Access Management

- Ich bin: ListRoleTags
- ich bin: ListUserTags
- Ressourcengruppen, die API taggen: GetResources
- Servicekatalog-App-Registrierung: GetApplication
- Servicekatalog-App-Registrierung: ListAssociatedAttributeGroups
- Servicekatalog-App-Registrierung: GetAttributeGroup

Important

Stellen Sie sicher, dass es keine IAM-Richtlinie oder Service Control Policy (SCP) gibt, die die vorherigen Aktionen ablehnt.

Die API-Aufrufe werden von der Rolle ausgeführt. `ams-access-admin` Das Folgende ist ein Beispiel dafür, was Sie sehen könnten:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

Verwendung OpsCenter in AMS

Das Betriebsteam von AWS Managed Services (AMS) verwendet [AWS Systems Manager OpsCenter](#) für die Diagnose und Behebung vieler Alarme im Zusammenhang mit Ihren Ressourcen.

Die Verwendung OpsCenter reduziert die mittlere Zeit bis zur Problemlösung (MTTR) und bietet gleichzeitig einen transparenten Einblick in die betrieblichen Warteschlangen der AMS-Betriebsteams.

Mit OpsCenter AMS erhalten Sie zusätzlich zu automatisierten Lösungen einen transparenten Überblick über betriebliche Arbeitsaufgaben [OpsItems](#), auch bekannt als, an denen AMS-Teams aktiv arbeiten.

Weitere Informationen zu OpsCenter und finden OpsItems Sie unter [AWS Systems Manager OpsCenter](#). Informationen zum Zugriff auf die AWS Management Console finden Sie unter [Arbeiten mit der AWS-Managementkonsole](#). Von der AWS-Managementkonsole aus können Sie zur AWS Systems Manager-Konsole navigieren OpsCenter. Weitere Informationen finden Sie unter [AWS Systems Manager Session Manager](#). OpsCenter bietet auch eine API, die Sie verwenden können. Weitere Informationen finden [Sie unter Erfahren Sie mehr über OpsCenter](#).

OpsCenter ist eine kostenpflichtige Funktion mit ~1000 € OpsItems , die weniger als 10\$ kostet. Weitere Informationen finden Sie unter [AWS Systems Manager -Preise](#).

Warnmeldungen von AMS

Als Teil der Alert-Verarbeitung erstellt AWS Managed Services (AMS) auf der Grundlage der Auswirkungsanalyse einen Vorfall und leitet den Incident-Management-Prozess zur Behebung ein, sobald die Auswirkungen festgestellt werden können. Falls die Auswirkungen nicht festgestellt werden können, sendet AMS über eine Servicemeldung eine Warnmeldung an die mit Ihrem Konto verknüpfte E-Mail-Adresse. Weitere Informationen finden Sie im Diagramm zur AMS-Monitoring-Architektur für den Alert-Handling-Prozess unter. [So funktioniert die Überwachung](#)

Empfangen von Warnmeldungen, die von AMS generiert wurden

Mit AWS Managed Services (AMS) können Sie Warnmeldungen für EC2 Amazon-Ressourcen direkt erhalten, um Kommunikationsverzögerungen zu reduzieren. Um EC2 Amazon-Benachrichtigungen direkt zu erhalten, abonnieren Sie Ihr Ziel (bevorzugte E-Mail-Adresse) für das Amazon SNS-Thema Direct-Customer-Alerts mithilfe der Änderungsart Verwaltung | Überwachung und Benachrichtigung | SNS | Abonnieren (ct-3rc19u1k017wu).

Note

Nicht alle Basiswarnungen werden standardmäßig an das Thema Direct-Customer-Alerts gesendet. Um alle vom AMS-Überwachungssystem generierten Warnmeldungen zu sehen, abonnieren Sie das Amazon SNS SNS-Thema für das AMS-Überwachungssystem. Fragen Sie in der Anfrage nach dem „AMS-Monitoring-Thema“, geben Sie einen Abonnementkanal für den Empfang der Benachrichtigungen an (Lambda, Amazon SQS, HTTP/S, E-Mail oder

SMS) und geben Sie die Endpunkte an (z. B. E-Mail-Adressen, wenn Sie das E-Mail-Protokoll wählen), die die Benachrichtigungen erhalten sollen.

Das AMS-Monitoring-Thema empfängt Warnmeldungen, die von AMS Shared Services verwendet werden, sodass es zu Störungen kommen kann.

Weitere Informationen finden Sie im Abschnitt [Abonnieren](#) in der Amazon Simple Notification Service Abonnement-API-Referenz.

Eine Liste der Basiswarnungen, die AMS bereitstellt, finden Sie unter [Warnmeldungen aus der Basisüberwachung in AMS](#).

Tag-basierte Warnmeldungen in AMS

Verwenden Sie Tags, um Warnmeldungen für Ihre Ressourcen an verschiedene E-Mail-Adressen zu senden. Es hat sich bewährt, tagbasierte Warnmeldungen zu verwenden, da Benachrichtigungen, die an eine einzige E-Mail-Adresse gesendet werden, zu Verwirrung führen können, wenn mehrere Entwicklerteams dasselbe Konto verwenden.

Important

Tag-basierte Warnmeldungen funktionieren nur für Benachrichtigungen im Zusammenhang mit Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift und. OpenSearch
Fügen Sie Ihren Tags keine personenbezogenen Daten (PII) hinzu.

Senden Sie Benachrichtigungen an eine bestimmte E-Mail-Adresse

Taggen Sie Ressourcen mit Benachrichtigungen, die an eine bestimmte E-Mail-Adresse gesendet werden müssen, mit `demkey = OwnerTeamEmail,value = EMAIL_ADDRESS`.

Senden Sie Benachrichtigungen an mehrere E-Mail-Adressen

Um mehrere E-Mail-Adressen zu verwenden, geben Sie eine durch Kommas getrennte Werteliste an. Zum Beispiel `key = OwnerTeamEmail,value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, . . .`. Die Gesamtzahl der Zeichen für das Wertfeld darf 260 nicht überschreiten.

Verwenden Sie einen benutzerdefinierten Tag-Schlüssel

Um einen benutzerdefinierten Tag-Schlüssel zu verwenden, geben Sie Ihrem CSDM den Namen des benutzerdefinierten Tag-Schlüssels in einer E-Mail an, in der Sie Ihre Zustimmung zur Aktivierung der automatischen Benachrichtigung für die tagbasierte Kommunikation geben. Es hat sich bewährt, für alle Ihre Instances und Ressourcen dieselbe Tagging-Strategie für Kontakt-Tags zu verwenden.

Die E-Mail-Adresse muss vollständig angegeben werden, mit dem „at“ -Zeichen (@), um den lokalen Teil von der Domain zu trennen. Beispiele für ungültige E-Mail-Adressen: *Team.AppATabc.xyz* oder *john.doe*. Allgemeine Hinweise zu Ihrer Tagging-Strategie finden Sie unter [Verwenden von Tags](#). Um eine vorhandene Ressource zu taggen, reichen Sie einen RFC mit dem Änderungstyp Deployment | Advanced stack components | Tag | Create (auto) (ct-3cx7we852p3af) ein.

 Note

Der Schlüsselwert muss nicht in Camel Case angegeben werden. *OwnerTeamEmail* Bei Tags wird jedoch zwischen Groß- und Kleinschreibung unterschieden, und es empfiehlt sich, das empfohlene Format zu verwenden.

Automatische AMS-Behebung von Warnmeldungen

Nach der Überprüfung behebt AWS Managed Services (AMS) automatisch bestimmte Warnmeldungen gemäß den in diesem Abschnitt beschriebenen Bedingungen und Prozessen.

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
Defekter sicherer Kanal	Der Alarm für defekte sichere Kanäle wird auf EC2 Windows-Instances ausgelöst, wenn die Instance die Verbindung zum AD-Domänencontroller verliert.	Der Schwellenwert lag in den letzten 15 Minuten zehnmal über dem definierten Wert.	Die automatische AMS-Wiederherstellung überprüft, ob die Instanz in SSM online ist, dass der Hostname nicht doppelt vorhanden ist und dass das AD-Computerobjekt auf den Stack abgestimmt ist. CloudFormation

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
			Die Behebung repariert die sichere Kanalverbindung, um den Zugriff auf die Instanz wiederherzustellen.
Statusprüfung fehlgeschlagen	Mögliche Hardwarefehler oder ein Fehlerstatus der Instanz.	Das System hat in den letzten 15 Minuten mindestens einmal einen ausgefallenen Status erkannt.	Die automatische AMS-Problembehebung überprüft zunächst, ob auf die Instanz zugegriffen werden kann. Wenn auf die Instanz nicht zugegriffen werden kann, wird die Instanz gestoppt und neu gestartet. Das Stop-and-Start-Verfahren ermöglicht es der Instanz, auf neue zugrunde liegende Hardware zu migrieren. Weitere Informationen finden Sie im folgenden Abschnitt „Automatisierung der EC2 Fehlerkorrektur bei der Statusprüfung“.

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
AMSLinuxDiskUsage	Wird ausgelöst, wenn die Festplattenbelegung eines Bereitstellungspunkts (zugewiesener Speicherplatz auf einem Volume) auf Ihrer EC2 Instance voll ausgelastet ist.	Der Schwellenwert lag in den letzten 30 Minuten sechsmal über dem definierten Wert.	Die automatische AMS-Wiederherstellung löscht zunächst temporäre Dateien. Wenn dadurch nicht genügend Festplattenspeicher frei wird, wird das Volume erweitert, um Ausfallzeiten zu vermeiden, wenn das Volume voll wird.
AMSWindowsDiskUsage	Wenn die Festplattenbelegung eines Bereitstellungspunkts (zugewiesener Speicherplatz auf einem Volume) auf Ihrer EC2 Instance aufgebraucht ist.	Der Schwellenwert lag in den letzten 30 Minuten sechsmal über dem definierten Wert.	Die automatische AMS-Wiederherstellung löscht zunächst temporäre Dateien. Wenn dadurch nicht genügend Festplattenspeicher frei wird, wird das Volume erweitert, um Ausfallzeiten zu vermeiden, wenn das Volume voll wird.

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-EVENT-0089	Die DB-Instance hat mehr als 90% ihres zugewiesenen Speichers verbraucht.	Der Speicher ist zu mehr als 90% zugewiesen.	Die automatische AMS-Problembehebung überprüft zunächst, ob sich die Datenbank in einem modifizierbaren und verfügbaren Zustand befindet oder ob der Speicher voll ist. Anschließend wird versucht, den zugewiesenen Speicher, die IOPS und den Speicherdurchsatz mithilfe eines Changesets zu erhöhen. CloudFormation Wenn eine Stack-Drift bereits erkannt wird, wird sie auf die RDS-API zurückgegriffen, um Ausfallzeiten zu vermeiden. Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-EVENT-0007	Der der DB-Instance zugewiesene Speicherplatz ist erschöpft. Um das Problem zu lösen, weisen Sie zusätzlichen Speicher zu.	Der Speicherplatz ist zu 100% zugewiesen.	Die automatische AMS-Problembehebung überprüft zunächst, ob sich die Datenbank in einem modifizierbaren und verfügbaren Zustand befindet oder ob der Speicherplatz voll ist. Anschließend wird versucht, den zugewiesenen Speicher, die IOPS und den Speicherdrucksatz mithilfe eines Changesets zu erhöhen. CloudFormation Wenn eine Stack-Drift bereits erkannt wird, wird sie auf die RDS-API zurückgegriffen, um Ausfallzeiten zu vermeiden. Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-EVENT-0224	Der angeforderte zugewiesene Speicher erreicht oder überschreitet den konfigurierten maximalen Speicherschwellenwert.	Der maximale Speicherschwellenwert für die DB-Instance wurde ausgeschöpft oder ist größer oder gleich dem angeforderten zugewiesenen Speicher.	Die automatische AMS-Problembehebung überprüft zunächst, ob die angeforderte Menge an RDS-Speicher den maximalen Speicherschwellenwert überschreitet. Falls bestätigt, versucht AMS, den maximalen Speicherschwellenwert mit einem CloudFormation Changeset oder einer direkten RDS-API, falls Ressourcen nicht bereitgestellt werden, um 30% zu erhöhen. CloudFormation Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-Speicherkapazität	Im zugewiesenen Speicher für die DB-Instance verbleiben weniger als 1 GB.	Der Speicherplatz ist zu 99% zugewiesen.	Die automatische AMS-Problembehebung überprüft zunächst, ob sich die Datenbank in einem modifizierbaren und verfügbaren Zustand befindet oder ob der Speicherplatz voll ist. Anschließend wird versucht, den zugewiesenen Speicher, die IOPS und den Speicherdurchsatz mithilfe eines Changesets zu erhöhen. CloudFormation Wenn eine Stack-Drift bereits erkannt wird, wird sie auf die RDS-API zurückgegriffen, um Ausfallzeiten zu vermeiden. Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Amazon EC2 Broken Secure Channel: Hinweis zur Automatisierung der Problembehebung

Bevor die automatische Behebung durch AWS Managed Services (AMS) Probleme mit dem Amazon EC2 Windows Broken Secure Channel behebt, führt die Automatisierung die folgenden Vorabprüfungen durch und erstellt einen Vorfallbericht zur weiteren Untersuchung:

- Überprüft, ob der SSM-Status der EC2 Amazon-Instance „Online“ lautet.
- Überprüft, ob die EC2 Amazon-Instance Teil einer Auto Scaling Scaling-Gruppe ist und ob alle Instances in der Auto Scaling Scaling-Gruppe denselben Hostnamen haben.
- Prüft, ob die EC2 Amazon-Instance Teil des CloudFormation Stacks ist, mit dem sie bereitgestellt wurde. Wenn die Instance aus dem CloudFormation Stack entfernt wurde, überprüft die Automatisierung, ob die zugehörige Active Directory-Organisationseinheit (OU) immer noch auf den Stack verweist.

Nachdem die oben genannten Validierungen bestanden wurden, fährt die Automatisierung mit der Behebung des defekten sicheren Kanals fort.

Schritte zur Behebung:

- Bei der automatischen Problembehebung wird versucht, den sicheren Kanal zwischen der EC2 Instanz und der AD-Domäne zu reparieren und den Zugriff auf die Instanz wiederherzustellen.
- Nach der Behebung überprüft die Automatisierung, ob der sichere Kanal eingerichtet ist. Gelingt das nicht, erstellt AMS einen Vorfall und beauftragt den AMS-Betrieb mit der Untersuchung.

EC2 Fehler bei der Statusüberprüfung: Hinweise zur Automatisierung der Problembehebung

So funktioniert die automatische AMS-Problembehebung bei EC2 fehlgeschlagenen Statusprüfungen:

- Wenn Ihre EC2 Amazon-Instance nicht mehr erreichbar ist, muss die Instance gestoppt und erneut gestartet werden, damit sie auf neue Hardware migriert und wiederhergestellt werden kann.
- Wenn die Ursache des Problems im Betriebssystem liegt (fehlende Geräte in fstab, Kernelfehler usw.), kann die Automatisierung Ihre Instance nicht wiederherstellen.
- Wenn Ihre Instance zu einer Auto Scaling Scaling-Gruppe gehört, ergreift die Automatisierung keine Aktion — die AutoScalingGroup Skalierungsaktion ersetzt die Instance.

- Wenn für Ihre Instance EC2 Auto Recovery aktiviert ist, werden bei der Behebung keine Maßnahmen ergriffen.

EC2 Automatisierung der Behebung der Volumennutzung

So funktioniert die automatische Behebung von Problemen mit der EC2 Volumennutzung durch AWS Managed Services (AMS):

- Die Automatisierung überprüft zunächst, ob die Volumenerweiterung erforderlich ist und ob sie durchgeführt werden kann. Wenn die Erweiterung als angemessen erachtet wird, kann die Automatisierung die Volumenkapazität erhöhen. Dieser automatisierte Prozess bringt den Bedarf an Wachstum mit kontrollierter, begrenzter Expansion in Einklang.
- Vor der Erweiterung eines Volumes führt die Automatisierung Säuberungsaufgaben (Windows: Disk Cleaner, Linux: Logrotate + Simple Service Manager Agent Log entfernen) auf der Instanz aus, um Speicherplatz freizugeben.

Note

Die Bereinigungsaufgaben werden nicht auf Instanzen der EC2 „T“-Familie ausgeführt, da sie für die kontinuierliche Funktionalität auf CPU-Guthaben angewiesen sind.

- Unter Linux unterstützt die Automatisierung nur die Erweiterung der Dateisysteme vom Typ EXT2, EXT3, EXT4 und XFS.
- Unter Windows unterstützt die Automatisierung nur das New Technology File System (NTFS) und das Resilient File System (ReFS).
- Die Automatisierung erweitert keine Volumes, die Teil von Logical Volume Manager (LVM) oder eines RAID-Arrays sind.
- Durch die Automatisierung werden die Instance-Speicher-Volumes nicht erweitert.
- Die Automatisierung ergreift keine Maßnahmen, wenn das betroffene Volumen bereits größer als 2 TiB ist.
- Die Erweiterung durch Automatisierung ist auf maximal dreimal pro Woche und insgesamt auf das Fünffache während der gesamten Lebensdauer des Systems begrenzt.
- Durch die Automatisierung wird das Volumen nicht erhöht, wenn die vorherige Erweiterung innerhalb der letzten sechs Stunden stattgefunden hat.

Wenn diese Regeln verhindern, dass die Automatisierung Maßnahmen ergreift, kontaktiert AMS Sie über eine ausgehende Serviceanfrage, um die nächsten zu ergreifenden Maßnahmen festzulegen.

Automatisierung der Behebung von Ereignissen bei geringem Speicherplatz in Amazon RDS

So funktioniert die automatische Behebung von AWS Managed Services (AMS) bei Problemen mit unzureichendem Speicherplatz in Amazon RDS:

- Bevor versucht wird, den Amazon RDS-Instance-Speicher zu erweitern, führt die Automatisierung mehrere Prüfungen durch, um sicherzustellen, dass sich die Amazon RDS-Instance in einem modifizierbaren und verfügbaren oder speichervollen Zustand befindet.
- Wenn CloudFormation Stack-Drift erkannt wird, erfolgt die Behebung über die Amazon RDS-API.
- Die Behebungsaktion wird in den folgenden Szenarien nicht ausgeführt:
 - Der Amazon RDS-Instance-Status ist nicht „verfügbar“ oder „Speicher voll“.
 - Der Amazon RDS-Instance-Speicher kann derzeit nicht geändert werden (z. B. wenn der Speicher in den letzten sechs Stunden geändert wurde).
 - Für die Amazon RDS-Instance ist die automatische Speicherskalierung aktiviert.
 - Die Amazon RDS-Instance ist keine Ressource innerhalb eines CloudFormation Stacks.
- Die Behebung ist auf eine Erweiterung alle sechs Stunden und nicht mehr als drei Erweiterungen innerhalb eines fortlaufenden Zeitraums von vierzehn Tagen begrenzt.
- Wenn diese Szenarien eintreten, meldet sich AMS mit einem ausgehenden Vorfall an Sie, um die nächsten Maßnahmen festzulegen.

Zusätzliche CloudWatch Alarme in AMS erstellen

Sie können neue CloudWatch Alarme mithilfe der AWS Managed Services (AMS) Deployment | Überwachung und Benachrichtigung | CloudWatch | Änderungsart von Alarmen erstellen erstellen.

Important

AMS überwacht keine von Ihnen erstellten CloudWatch Alarme.

Verwenden von benutzerdefinierten CloudWatch Metriken und Alarmen für EC2 Amazon-Instances (funktioniert nur für veränderbare Bereitstellungen, die nicht auf aktualisierten, für Auto Scaling Scaling-Gruppen AMIs bereitgestellten Updates basieren):

1. Erstellen Sie Ihr Anwendungsüberwachungsskript und Ihre benutzerdefinierte Metrik. Weitere Informationen und Zugriff auf Beispielskripts finden Sie unter [Monitoring Memory and Disk Metrics for Amazon EC2 Linux Instances](#). Die CloudWatch Amazon-Überwachungsskripte für EC2 Linux-Amazon-Instances zeigen, wie CloudWatch benutzerdefinierte Amazon-Metriken erstellt und verwendet werden. Diese Perl-Beispielskripts umfassen ein voll funktionsfähiges Beispiel, bei dem Speicher-, Auslagerungs- und Speicherplatz-Auslastungsmetriken für eine Linux-Instance gemeldet werden.
2. Laden Sie Ihr Überwachungsskript hoch. Um das Überwachungsskript in Ihre Auto Scaling Scaling-Gruppen- oder EC2 Amazon-Instance-Konfiguration hochzuladen, können Sie es UserData bei der Konfiguration Ihrer Auto Scaling Scaling-Gruppe oder EC2 Amazon-Instance verwenden, oder, falls Ihre Anwendung mit bereitgestellt wurde CodeDeploy, können Sie die Konfiguration mit Deployment | Applications | CodeDeploy Application | Deploy CT (ct-2edc3sd1sqmrb) ändern.
3. Veröffentlichen Sie Ihre benutzerdefinierte Metrik in CloudWatch (wenn Sie zum ersten Mal einen Datenpunkt für eine neue benutzerdefinierte Metrik veröffentlichen, wird er erstellt), siehe [Benutzerdefinierte Metriken veröffentlichen](#).
4. Erstellen Sie den CloudWatch Alarm, siehe [CloudWatch Alarm für eine Instanz erstellen](#).

 Important

Überwachungsdaten müssen an diesen Pfad gesendet werden [infra/INSTANCE_ID/YOUR_CUSTOM_METRIC]

Um einen CloudWatch Alarm zu ändern oder zu löschen, reichen Sie einen RFC mit Management | Other | Other | Create Change Type (ct-1e1xtak34nx76) mit den Parametern ein, die erforderlich sind, um die Aktion abzuschließen, wie in der Amazon-API-Referenz beschrieben. CloudWatch [PutMetricAlarm](#)

CloudWatch Sie können den Event-Stream verwenden. AMS ist integriert CloudWatch und Sie können anfordern, dass jeder AWS-API-Aufruf ein CloudWatch Ereignis auslöst.

Reichen Sie dazu ein Management | Other | Other | Update CT (ct-0xdawir96cy7k) mit den API-Aufrufen ein, an denen Sie interessiert sind. Ein AMS-Mitarbeiter wird mit Ihnen sprechen, um die Anforderungen zu ermitteln. Weitere Informationen finden Sie in der [CloudWatch Amazon-Dokumentation](#).

Um Zugriff auf den CloudWatch Event-Stream zu erhalten, reichen Sie ein CT (ct-0xdawir96cy7k) für Management | Other | Other | Update CT (ct-0xdawir96cy7k) ein, um eine Partei zum Thema SNS-Benachrichtigung hinzuzufügen. Ein AMS-Mitarbeiter wird mit Ihnen sprechen, um die Anforderungen zu ermitteln.

Benutzerdefinierte CloudWatch Metriken und Alarme in AMS erstellen

Sie können Ihre Geschäfts- und Anwendungskennzahlen in Amazon speichern CloudWatch. Sie können Diagramme anzeigen und Alarme auf der Grundlage dieser Metriken einrichten, genauso wie Sie es für die Metriken tun können, die CloudWatch bereits für Ihre AWS Managed Services (AMS) -Ressourcen gespeichert sind. Weitere Informationen finden Sie CloudWatch unter [Amazon CloudWatch Concepts](#).

Amazon SNS ermöglicht Anwendungen das Senden zeitkritischer Nachrichten an mehrere Abonnenten über einen „Push“-Mechanismus gegen das AMS Managed Monitoring System oder MMS, Amazon SNS (SNS) -Thema, unter dem die Alarme veröffentlicht werden; in diesem Fall MMS und Ihre SQS-Warteschlangen. Sie können damit benutzerdefinierte Messwerte erstellen und CloudWatch sich über ein SNS-Thema von AMS entsprechend benachrichtigen lassen. Gehen Sie dazu wie folgt vor.

Note

Dieser Prozess funktioniert nicht für unveränderliche Bereitstellungen, die auf aktualisierten, in Auto Scaling Scaling-Gruppen AMIs bereitgestellten Versionen basieren. Er eignet sich für Bereitstellungen veränderbarer Anwendungen (nicht ASG).

Das Einrichten einer benutzerdefinierten Metrik innerhalb der Einschränkungen von AMS Advanced ist eine komplexe Aufgabe. Ein Beispiel von finden Sie unter CloudWatch [Beispiel: Zählen der Vorkommen eines Begriffs](#).

1. Erstellen Sie Ihr Anwendungsüberwachungsskript und eine benutzerdefinierte Metrik (z. B. das Beispiel „Anzahl der Vorkommen“). Weitere Informationen und Zugriff auf Beispielskripts finden Sie unter [Monitoring Memory and Disk Metrics for Amazon EC2 Linux Instances](#).
2. Laden Sie Ihr Überwachungsskript hoch. Um das Überwachungsskript in Ihre Auto Scaling Scaling-Gruppen- oder EC2 Amazon-Instance-Konfiguration hochzuladen, können Sie es UserDatabei der Konfiguration Ihrer Auto Scaling Scaling-Gruppe oder EC2 Amazon-Instance verwenden, oder, falls Ihre Anwendung mit bereitgestellt wurde CodeDeploy, können Sie die Konfiguration mit Deployment | Applications | CodeDeploy Application | Deploy CT (ct-2edc3sd1sqmrb) ändern.
3. Veröffentlichen Sie Ihre benutzerdefinierte Metrik in CloudWatch (wenn Sie zum ersten Mal einen Datenpunkt für eine neue benutzerdefinierte Metrik veröffentlichen, wird er erstellt), siehe [Benutzerdefinierte Metriken veröffentlichen](#).
4. Um Ihre Kundenmetrik in Ihr Anwendungsüberwachungssystem zu integrieren, bitten Sie AMS, ein SNS-Thema für die Metrik zu erstellen, indem Sie einen RFC mit dem Typ Bereitstellung | Überwachung und Benachrichtigung | SNS | Änderungstyp erstellen (ct-3dfnglm4ombbs) einreichen.
5. Erstellen Sie den CloudWatch Alarm, siehe [CloudWatch Amazon-Alarme erstellen](#).

 Important

Überwachungsdaten müssen an diesen Pfad [infra/*INSTANCE_ID/YOUR_CUSTOM_METRIC*] gesendet werden.

Verwenden von CloudWatch Application Insights für .Net und SQL Server in AMS

Sie können Amazon CloudWatch Application Insights verwenden, um die Monitore für Ihre AWS Managed Services (AMS) -Anwendungsressourcen einzurichten, um Daten kontinuierlich auf Anzeichen von Problemen mit Ihren Anwendungen zu analysieren und Ihre mittlere Reparaturzeit (MTTR) bei der Behebung von Anwendungsproblemen zu reduzieren. Einzelheiten zu CloudWatch Application Insights finden Sie unter [CloudWatch Application Insights für .NET und SQL Server](#).

 Important

AMS überwacht keine Probleme in CloudWatch Application Insights, da es sich um Anwendungscode handelt, der von Ihnen gesteuert wird.

Um CloudWatch Application Insights zu verwenden, reichen Sie einen RFC mit dem Änderungstyp Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) (ct-3dpd8mdd9jn1r) mit der Anforderung ein, eine IAM-Rolle zu erstellen, die Ihnen die Berechtigung zur Konfiguration von Application Insights erteilt. CloudWatch Es gibt zwei Möglichkeiten, die identifizierten Probleme zu erhalten: über ein SNS-Thema oder mit einem Ziel in den Ereignisregeln. CloudWatch Geben Sie im RFC an, welche Sie möchten. Wenn Sie planen, CloudWatch Ereignisregeln zu verwenden, geben Sie auch die Regeldefinition im RFC an. Nachdem Sie CloudWatch Application Insights eingerichtet haben, erhalten Sie eine Benachrichtigung über potenzielle Probleme, einschließlich Informationen, die auf eine mögliche Ursache hinweisen.

Informationen dazu, wie Sie diese Rolle übernehmen können, finden Sie im AMS Onboarding Guide [Federate your Active Directory with the AMS IAM Roles](#).

Verwenden von Amazon EventBridge Managed Rules in AMS

AMS Advanced verwendet Amazon EventBridge Managed Rules. Eine verwaltete Regel ist ein einzigartiger Regeltyp, der direkt mit AMS verknüpft ist. Diese Regeln ordnen eingehende Ereignisse zu und senden sie zur Verarbeitung an Ziele. Verwaltete Regeln sind von AMS vordefiniert und enthalten Ereignismuster, die vom Service für die Verwaltung von Kundenkonten benötigt werden. Sofern nicht anders definiert, kann nur der Service, für den sie verantwortlich ist, diese verwalteten Regeln verwenden.

Von AMS verwaltete Regeln sind mit dem `events.managedservices.amazonaws.com` Service Principal verknüpft. Diese verwalteten Regeln werden über die [AWSServiceRoleForManagedServices_Eventsdienstbezogene Rolle](#) verwaltet. Um diese Regeln zu löschen, ist eine besondere Bestätigung durch den Kunden erforderlich. Weitere Informationen finden Sie unter [Löschen verwalteter Regeln für AMS](#).

Weitere Informationen zu Regeln finden Sie unter [Regeln](#) im EventBridge Amazon-Benutzerhandbuch.

Von AMS bereitgestellte Amazon EventBridge Managed Rules

Von Amazon EventBridge verwaltete Regeln

Regelname	Beschreibung	Definition
AMSAdvancedCoreRule	Diese Regel leitet Amazon CloudWatch Alarms an AMS Monitoring weiter. Die CloudWatch Alarms überwachen CloudWatch Alarme.	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"], } }</pre>

Verwaltete Regeln für AMS erstellen

Sie müssen Amazon EventBridge Managed Rules nicht manuell erstellen. Wenn Sie in der AWS Management Console, der oder der AWS CLI AWS API bei AMS einsteigen, erstellt AMS sie für Sie.

Verwaltete Regeln für AMS bearbeiten

AMS erlaubt Ihnen nicht, die verwalteten Regeln zu bearbeiten. Name und Ereignismuster für jede verwaltete Regel sind von AMS vordefiniert.

Verwaltete Regeln für AMS löschen

Sie müssen die verwalteten Regeln nicht manuell löschen. Wenn Sie in der AWS Management Console, der oder der AWS API aus AMS aussteigen AWS CLI, bereinigt AMS die Ressourcen und löscht alle verwalteten Regeln, die AMS gehören, für Sie.

Falls AMS die verwalteten Regeln beim Offboarding nicht entfernt, können Sie die verwalteten Regeln auch über die EventBridge Amazon-Konsole, die AWS CLI oder die AWS API manuell löschen.

Dazu müssen Sie zunächst Ihr Konto bei AMS verlassen und das Löschen der verwalteten Regeln erzwingen.

Vertrauenswürdiger Remediator in AMS

Trusted Remediator ist eine AWS Managed Services Services-Lösung, die die Problembehebung und Empfehlungen automatisiert. [AWS Trusted Advisor](#)[AWS Compute Optimizer](#) Trusted Remediator erstellt Empfehlungen, wann Trusted Advisor und Compute Optimizer zeigt Ihnen Möglichkeiten auf, Kosten zu senken, die Systemverfügbarkeit zu verbessern, die Leistung zu optimieren oder Sicherheitslücken für Sie zu schließen. AWS-Konten Mit Trusted Remediator können Sie diese Empfehlungen zu Sicherheit, Leistung, Kostenoptimierung, Fehlertoleranz und Servicebeschränkungen auf sichere, standardisierte Weise umsetzen und dabei etablierte Best Practices verwenden. Trusted Remediator ermöglicht Ihnen die Konfiguration einer Behebungslösung und wird automatisch nach einem von Ihnen erstellten Zeitplan ausgeführt, wodurch der Behebungsprozess vereinfacht wird. Mit diesem optimierten Ansatz werden Probleme konsistent, effizient und ohne manuelles Eingreifen behoben.

Die wichtigsten Vorteile von Trusted Remediator

Im Folgenden sind die wichtigsten Vorteile von Trusted Remediator aufgeführt:

- **Verbesserte Sicherheit, Leistung und Kostenoptimierung:** Trusted Remediator hilft Ihnen dabei, die allgemeine Sicherheitslage Ihrer Konten zu verbessern, die Ressourcennutzung zu optimieren und die Betriebskosten zu senken.
- **Self-Service-Einrichtung und Konfiguration:** Sie können Trusted Remediator so konfigurieren, dass es Ihren Anforderungen und Präferenzen entspricht.
- **Automatisierte Behebung von Trusted Advisor Prüfungen und AWS Compute Optimizer Empfehlungen:** Nach der Konfiguration führt Trusted Remediator automatisch die Behebungsmaßnahmen für ausgewählte Prüfungen aus. Durch diese Automatisierung entfällt die Notwendigkeit manueller Eingriffe.
- **Implementierung bewährter Verfahren:** Abhilfemaßnahmen basieren auf etablierten bewährten Verfahren, sodass Probleme auf standardisierte und effektive Weise angegangen werden.
- **Geplante Ausführung:** Sie können den Zeitplan für die Behebung wählen, der Ihren day-to-day betrieblichen Arbeitsabläufen entspricht.

Trusted Remediator ermöglicht es Ihnen, identifizierte Probleme in Ihren AWS Umgebungen proaktiv anzugehen und hilft Ihnen dabei, bewährte Verfahren einzuhalten und eine sichere, leistungsstarke und kostengünstige Cloud-Infrastruktur aufrechtzuerhalten.

So funktioniert Trusted Remediator

Im Folgenden wird der Trusted Remediator-Arbeitsablauf veranschaulicht:

Trusted Remediator bewertet Trusted Advisor und empfiehlt Compute Optimizer für Sie AWS-Konten und erstellt diese. AWS Systems Manager [OpsItems](#) OpsCenter Anschließend können Sie Trusted Remediator-Automatisierungsdokumente verwenden, um das Problem automatisch oder manuell zu beheben. OpsItems Im Folgenden finden Sie Einzelheiten zu den einzelnen Behebungstypen:

- **Automatisierte Behebung:** Trusted Remediator führt das Automatisierungsdokument aus und überwacht den Lauf. Nach Abschluss des Automatisierungsdokuments löst Trusted Remediator das Opsitem auf.
- **Manuelle Korrektur:** Trusted Remediator erstellt das OpsItem , damit Sie es überprüfen können. Nach der Überprüfung können Sie einen automatisierten RFC ([Trusted Remediator | Finding | Remediate](#)) erstellen und den Typ ändern, um die Ressource zu korrigieren. Informationen zu den manuellen Behebungsschritten finden Sie unter. [Führen Sie manuelle Korrekturen in Trusted Remediator aus](#)

Behebungsprotokolle werden in einem Amazon S3 S3-Bucket gespeichert. Sie können die Daten im S3-Bucket verwenden, um benutzerdefinierte QuickSight Dashboards für die Berichterstattung zu erstellen. AMS stellt auf Anfrage auch Berichte für Trusted Remediator bereit. Um diese Berichte zu erhalten, wenden Sie sich an Ihren CSDM.

Wichtige Begriffe für Trusted Remediator

Die folgenden Begriffe sollten Sie kennen, wenn Sie Trusted Remediator in AMS verwenden:

- **AWS Trusted Advisor und AWS Compute Optimizer:** Cloud-Optimierungsdienste bereitgestellt von AWS. Trusted Advisor und Compute Optimizer untersuchen Ihre AWS Umgebung und geben Empfehlungen auf der Grundlage von Best Practices in den folgenden sechs Kategorien:
 - Kostenoptimierung
 - Performance

- Sicherheit
- Fehlertoleranz
- Operative Exzellenz
- Service Limits

Weitere Informationen erhalten Sie unter [AWS Trusted Advisor](#) und [AWS Compute Optimizer](#).

- Trusted Remediator: Eine AMS-Problembhebungslösung für [Trusted Advisor](#) Prüfungen und Empfehlungen. [AWS Compute Optimizer](#) Trusted Remediator hilft Ihnen dabei, Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen mit bekannten Best Practices sicher zu beheben, um Sicherheit und Leistung zu verbessern und Kosten zu senken. Trusted Remediator ist einfach einzurichten und zu konfigurieren. Sie konfigurieren einmal und Trusted Remediator führt die Problembhebungen nach Ihrem bevorzugten Zeitplan (täglich oder wöchentlich) durch.
- AWS Systems Manager SSM-Dokument: Eine JSON- oder YAML-Datei, die die Aktionen definiert, die auf Ihren Ressourcen AWS Systems Manager ausgeführt werden. AWS Das SSM-Dokument dient als deklarative Spezifikation zur Automatisierung betrieblicher Aufgaben über mehrere AWS Ressourcen und Instanzen hinweg.
- AWS Systems Manager OpsCenter OpsItem: Eine Cloud-Ressource für das betriebliche Problemmanagement, mit der Sie betriebliche Probleme in Ihrer AWS Umgebung verfolgen und lösen können. OpsItems bietet eine zentrale Ansicht und ein Verwaltungssystem für betriebliche Daten und Probleme in allen AWS-Services Ressourcen. Jedes Problem OpsItem stellt ein betriebliches Problem dar, z. B. ein potenzielles Sicherheitsrisiko, ein Leistungsproblem oder einen betrieblichen Vorfall.
- Konfiguration: Eine Konfiguration besteht aus einer Reihe von Attributen, die in gespeichert sind [AWS AppConfig, eine Fähigkeit von AWS Systems Manager](#). Die Trusted Remediator-Anwendung AWS AppConfig hilft bei der Konfiguration von Behebungen auf Kontoebene.
- Ausführungsmodus: Der Ausführungsmodus ist ein Konfigurationsattribut, das festlegt, wie die Behebung für jedes Trusted Advisor Prüfergebnis ausgeführt wird. Es gibt vier unterstützte Ausführungsmodi: Automatisiert, Manuell, Bedingt, Inaktiv.
- Überschreiben von Ressourcen: Diese Funktion verwendet Ressourcen-Tags, um eine Konfiguration für bestimmte Ressourcen zu überschreiben.
- Protokoll der Behebungselemente: Eine Protokolldatei im S3-Protokoll-Bucket von Trusted Remediator Remediator. Das Behebungselementprotokoll wird erstellt, wenn die Behebung erstellt wird. OpsItems Diese Protokolldatei enthält manuelle Ausführungskorrekturen OpsItems und automatische Ausführungskorrekturen. OpsItems Verwenden Sie diese Protokolldatei, um alle Behebungselemente nachzuverfolgen.

- **Protokoll zur automatisierten Problembehebung:** Eine Protokolldatei im S3-Protokoll-Bucket der Trusted Remediator-Korrektur. Das Protokoll zur automatischen Problembehebung wird erstellt, wenn die automatisierte Ausführung eines SSM-Dokuments abgeschlossen ist. Dieses Protokoll enthält SSM-Ausführungsdetails für die automatische Behebung der Ausführung. OpsItems Verwenden Sie diese Protokolldatei, um automatisierte Problembehebungen nachzuverfolgen.

Erste Schritte mit Trusted Remediator in AMS

Trusted Remediator ist in AMS ohne zusätzliche Kosten erhältlich. Trusted Remediator unterstützt Konfigurationen mit einem Konto und mehreren Konten.

Integrieren Sie Trusted Remediator

Um Ihre AMS-Konten bei Trusted Remediator zu integrieren, senden Sie eine E-Mail an Ihre Cloud-Architekten oder Cloud Service Delivery Manager (CSDMs). Geben Sie in der E-Mail folgende Informationen an:

- **AWS-Konten:** Die zwölfstellige Konto-Identifikationsnummer. Alle Konten, die Sie bei Trusted Remediator registrieren möchten, müssen demselben AMS Advanced-Kunden gehören.
- **Delegiertes Administratorkonto:** Das Konto, das für Trusted Advisor die Compute Optimizer-Prüfkonfiguration für einzelne oder mehrere Konten verwendet wird.
- **Mitgliedskonten:** Dies sind die Konten, die mit dem delegierten Administratorkonto verknüpft sind. Diese Konten erben die Konfigurationen des delegierten Administratorkontos. Sie können ein Mitgliedskonto oder mehrere Mitgliedskonten haben.

Note

Mitgliedskonten erben die Konfigurationen des delegierten Administratorkontos. Wenn Sie unterschiedliche Konfigurationen für bestimmte Konten benötigen, integrieren Sie mehrere delegierte Administratorkonten mit Ihren bevorzugten Konfigurationen. Planen Sie die Kontostruktur und die Konfigurationen mit Ihren Cloud-Architekten, bevor Sie an Bord gehen.

- **AWS-Region:** Der AWS-Region Ort, an dem sich Ihre Ressourcen befinden. Eine Liste von finden Sie AWS-Regionen unter [AWS-Services Nach Regionen geordnet](#).
- **Behebungszeitplan und -zeit:** Ihr bevorzugter Behebungszeitplan (täglich oder wöchentlich). Trusted Remediator sammelt Trusted Advisor Prüfungen und leitet die Behebung zum geplanten

Zeitpunkt ein. Sie können beispielsweise den Zeitplan für die Problembehebung auf jeden Sonntag um 1:00 Uhr (australische Eastern Standard Time) festlegen.

- Benachrichtigungs-E-Mail: Trusted Remediator verwendet die Benachrichtigungs-E-Mail, um Sie täglich darüber zu informieren, ob es Abhilfemaßnahmen gibt. Der Betreff der Benachrichtigungs-E-Mail lautet „Trusted Remediator Remediation Summary“ und der Inhalt enthält Informationen zu Trusted Remediator-Korrekturen, die in den letzten 24 Stunden durchgeführt wurden.

Note

Überprüfen Sie Ihre Anwendungen und Ressourcen nach jeder geplanten Problembehebung. Wenn Sie zusätzlichen Support benötigen, wenden Sie sich an AMS.

Nachdem Sie Ihre Onboard-Anfrage mit den erforderlichen Angaben bei Ihrer CA oder CSDM eingereicht haben, überträgt AMS Ihre Konten auf Trusted Remediator. Trusted Remediator verwendet eine Fähigkeit von AWS AppConfig AWS Systems Manager, um die Konfiguration für die Prüfungen zu definieren. Trusted Advisor Bei diesen Konfigurationen handelt es sich um eine Reihe von Attributen, die in AWS AppConfig gespeichert sind. Um zu verhindern, dass Ihre Ressourcen unbefugt belastet werden, werden alle unterstützten Trusted Advisor Prüfungen auf Inaktiv gesetzt, wenn Konten in Trusted Remediator integriert werden. Diese Konfigurationen helfen Ihnen dabei, bestimmte Trusted Advisor Prüfungen automatisch zu korrigieren oder die verbleibenden Prüfungen zu bewerten und manuell zu korrigieren. Die Konfigurationen sind in hohem Maße anpassbar, sodass Sie Konfigurationen für jede Trusted Advisor Prüfung anwenden können. Weitere Informationen finden Sie unter [Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator](#).

Konfigurieren Sie Trusted Remediator in Ihrem AWS-Konten

Wenn das Onboarding abgeschlossen ist, werden Sie von Ihrer CA oder Ihrem CDSM benachrichtigt und die Standardkonfigurationen werden in Ihrem delegierten Administrator erstellt. AWS-Konto Die Konfiguration wird in der Trusted AWS AppConfig Remediator-Anwendung gespeichert. Sie können RFC [Management | Trusted Remediator | Remediation configuration | Update verwenden, um Konfigurationsupdates](#) anzufordern. Weitere Informationen finden Sie unter [Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator](#).

Gehen Sie wie folgt vor, um die Standardkonfigurationen von Trusted Remediator anzuzeigen:

1. Öffnen Sie die AWS Systems Manager Konsole unter. <https://console.aws.amazon.com/systems-manager/>

 Note

Stellen Sie sicher, dass Sie sich im delegierten Administratorkonto befinden.

2. Wählen Sie Anwendungsverwaltung, AppConfig.
3. Wählen Sie Trusted Remediator aus der Liste der Anwendungen aus.

Im Folgenden finden Sie ein Beispiel für die AWS AppConfig Konsole, in der Trusted Remediator-Konfigurationen angezeigt werden:

Wählen Sie die Prüfungen und Empfehlungen aus, die behoben werden sollen

Standardmäßig ist der Wiederherstellungsausführungsmodus für alle Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen in Ihrer Konfiguration inaktiv. Dies verhindert unbefugte Problembehebungen und schont Ressourcen. AMS stellt kuratierte Dokumente zur SSM-Automatisierung zur Behebung von Schecks zur Trusted Advisor Verfügung.

Gehen Sie wie folgt vor, um die Prüfungen auszuwählen, die Sie mit Trusted Remediator korrigieren möchten:

1. Sehen Sie sich die Liste der unterstützten [Trusted Advisor und Compute Optimizer Optimizer-Empfehlungen oder den Namen der zugehörigen SSM-Automatisierungsdokumente](#) an, um zu entscheiden, welche Prüfungen und Empfehlungen Sie mit Trusted Remediator korrigieren möchten.
2. Senden Sie eine Anfrage [für Management | Trusted Remediator | Behebungskonfiguration | Aktualisierung, um die Konfiguration](#) für Ihre ausgewählten Prüfungen zu aktualisieren. Trusted Advisor Anweisungen zur Auswahl von Prüfungen finden Sie unter [Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator](#)

Verfolgen Sie Ihre Abhilfemaßnahmen in Trusted Remediator

Nachdem Sie Ihre Konfiguration auf Kontoebene aktualisiert haben, erstellt Trusted Remediator für jede Problembehebung neue Änderungen. OpsItems Trusted Remediator führt das SSM-Dokument zur automatisierten Behebung gemäß Ihrem Behebungsplan aus. OpsItems Anweisungen, wie Sie alle Behebungsmaßnahmen OpsItems von der Systems Manager OpsCenter Manager-Konsole aus anzeigen können, finden Sie unter [Behebungen in Trusted Remediator nachverfolgen](#).

Führen Sie manuelle Korrekturen in Trusted Remediator aus

Sie können Trusted Advisor Prüfungen mithilfe eines automatisierten RFC manuell korrigieren. Wenn Sie sich für die manuelle Korrektur entscheiden, erstellt Trusted Remediator eine manuelle Ausführung. OpsItem Weitere Informationen finden Sie unter [Führen Sie manuelle Korrekturen in Trusted Remediator aus](#).

Compute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden

In der folgenden Tabelle sind die unterstützten Compute Optimizer Optimizer-Empfehlungen, SSM-Automatisierungsdokumente, vorkonfigurierte Parameter und das erwartete Ergebnis der Automatisierungsdokumente aufgeführt. Überprüfen Sie das erwartete Ergebnis, um mögliche Risiken auf der Grundlage Ihrer Geschäftsanforderungen besser zu verstehen, bevor Sie ein SSM-Automatisierungsdokument zur Behebung von Prüfungen aktivieren.

Stellen Sie sicher, dass die entsprechende Konfigurationsregel für jede Compute Optimizer Optimizer-Prüfung für die unterstützten Prüfungen vorhanden ist, für die Sie die Problembehebung aktivieren möchten. Weitere Informationen finden Sie unter [AWS Compute Optimizer Für Trusted Advisor Prüfungen anmelden](#).

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Passende Dimensionierung		
Empfehlungen Amazon EC2 Amazon-Instanzen	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Der EC2 Amazon-Instance-Typ wurde gemäß den Empfehlungen von Compute Optimizer aktualisiert. Es werden die optimalsten Optionen ausgewählt, wobei dieselben Plattformparameter (Architektur, Hypervisor, Netzwerkschnittstelle, Virtualisierungstyp usw.) beibehalten	• MinimumDaysSinceLastChange: Der Parameter zur Angabe der Mindestanzahl von Tagen seit der letzten Änderung des Instanztyps. Der Standardwert ist 7 Tage. Keine Einschränkungen • AMIBeforeResize erstellen: Um das Instance-AMI vor der Größenänderung als Backup zu erstellen, setzen Sie den Wert auf „True“. Um kein Backup zu

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
	werden, sofern die Option vorhanden ist.	erstellen, setzen Sie den Wert auf „False“. Die Standardeinstellung ist „True“. Keine Einschränkungen

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Amazon EBS-Volumenempfehlungen	AWSManagedServices-ModifyEBSVolume Das Amazon EBS-Volumen wird gemäß den Empfehlungen von Compute Optimizer geändert. Die Änderung kann Volumentyp, Größe, IOPS und Volume-Generierung (gp2, gp3 usw.) umfassen.	• CreateSnapshot: Um vor dem Ändern des Volumes einen Snapshot zu erstellen, setzen Sie den Wert auf „True“. Um keinen Snapshot zu erstellen, setzen Sie ihn auf „False“. Die Standardinstellung ist „True“. Keine Einschränkungen • VolumeType: Der gewünschte Datenträgertyp. Wenn kein Typ angegeben ist, wird der vorhandene Typ beibehalten. Keine Einschränkungen • VolumeSize: Die gewünschte Größe des Volumes in GiB. Die Größe des Zielvolumes muss größer oder gleich der vorhandenen Größe des Volumes sein. Wenn keine Größe angegeben ist, wird die vorhandene Größe beibehalten. Keine Einschränkungen • IOPS: Die angeforderte Anzahl von I/O Vorgängen pro Sekunde (IOPS). Dieser Parameter ist nur für io1-, io2- und gp3-Volumes gültig. Keine Einschränkungen • Durchsatz: Der Durchsatz, der für ein Volumen bereitgestellt werden

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		muss, mit einem Maximum von 1000 MiB/s. Dieser Parameter ist nur für GP3-Volumes gültig. Keine Einschränkungen • RemediateStackDrift: Wenn eine Abweichung durch eine Änderung der Lautstärke verursacht wird, wird die Einstellung auf „True“ gesetzt, um die Behebung von Abweichungen einzuleiten. Um nicht zu versuchen, Abweichungen zu beheben, setzen Sie den Wert auf „Falsch“. Die Standardinstellung ist „True“. Keine Einschränkungen
Empfehlungen für Lambda-Funktionen	AWSManagedServices-TrusteRemediatorOptimizeLambdaMemory AWS Lambda Funktionsspeicher optimiert gemäß den Empfehlungen von Compute Optimizer.	RecommendedMemorySize : Benutzerdefinierte Speichergröße, falls diese von den empfohlenen Optionen abweicht. Keine Einschränkungen

Ungenutzte Ressourcen

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Amazon EBS-Volume im Leerlauf	AWSManagedServices-DeleteUnusedEBSVolume Ein nicht angehängtes Amazon EBS-Volume wird gelöscht.	• CreateSnapshot: Um vor dem Löschen des Volumes einen Snapshot zu erstellen, legen Sie den Wert auf „True“ fest. Um keinen Snapshot zu erstellen, setzen Sie ihn auf „False“. Die Standardeinstellung ist „True“. Keine Einschränkungen • MinimumUnattachedDays: Mindestens unangehängte Tage des zu löschenden Amazon EBS-Volumes, bis zu 62 Tage. Die Standardeinstellung ist 7. Keine Einschränkungen
Inaktive EC2 Amazon-Instanz	AWSManagedServices-StopEC2Instanzen Die inaktive EC2 Amazon-Instanz wird gestoppt.	ForceStopWithInstanceStore: Um den Stopp für Instances zu erzwingen, die den Instance-Speicher verwenden, setzen Sie den Wert auf „True“. Um den Stopp nicht zu erzwingen, setzen Sie den Wert auf „False“. Der Standardwert 'False' verhindert, dass die Instanz beendet wird. Keine Einschränkungen

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Amazon RDS-Instance im Leerlauf	AWSManagedServices-StopIdleRDSInstance Stoppen Sie eine Amazon RDS-Instanz im Leerlauf. Unterstützte Engines sind: MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL. Dieses Dokument gilt nicht für Aurora MySQL und Aurora PostgreSQL. Die Instanz wird für bis zu 7 Tage gestoppt und automatisch neu gestartet.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor von Trusted Remediator unterstützte Prüfungen

In der folgenden Tabelle sind die unterstützten Trusted Advisor Prüfungen, SSM-Automatisierungsdokumente, vorkonfigurierte Parameter und das erwartete Ergebnis der Automatisierungsdokumente aufgeführt. Überprüfen Sie das erwartete Ergebnis, um mögliche Risiken auf der Grundlage Ihrer Geschäftsanforderungen besser zu verstehen, bevor Sie ein Dokument zur SSM-Automatisierung zur Behebung von Prüfungen aktivieren.

Stellen Sie sicher, dass die entsprechende Konfigurationsregel für jede Trusted Advisor Prüfung für die unterstützten Prüfungen vorhanden ist, für die Sie die Problembehebung aktivieren möchten. Weitere Informationen finden Sie unter [AWS Trusted Advisor Checks anzeigen, die von bereitgestellt werden AWS Config](#). Wenn eine Prüfung über entsprechende AWS Security Hub CSPM Steuerelemente verfügt, stellen Sie sicher, dass die Security Hub-Steuerung aktiviert ist. Weitere Informationen finden Sie unter [Steuerelemente in Security Hub aktivieren](#). Informationen zur Verwaltung vorkonfigurierter Parameter finden Sie unter [Sie unter Konfiguration der Trusted Advisor Advisor-Prüfbehebung in Trusted Remediator](#).

Trusted Advisor Prüfungen zur Kostenoptimierung werden von Trusted Remediator unterstützt

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Z4 AUBRNSmz Nicht zugeordnete elastische IP-Adressen	AWSManagedServices-TrustedRemediatorReleaseElasticIP Gibt eine elastische IP-Adresse frei, die keiner Ressource zugeordnet ist.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c18d2gz150 — Amazon-Instances wurden gestoppt EC2	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime — EC2 Amazon-Instances, die für eine bestimmte Anzahl von Tagen gestoppt wurden, werden beendet.	• AMIBeforeKündigung erstellen: Um das Instance-AMI als Backup zu erstellen, bevor Sie die EC2 Amazon-Instance beenden, wählen Sie <code>true</code>. Um vor dem Beenden kein Backup zu erstellen, wählen Sie <code>false</code>. Der Standardwert ist <code>true</code>. • AllowedDays: Die Anzahl der Tage, an denen sich die Instanz im gestoppten Zustand befindet, bevor sie beendet wird. Der Standardwert ist 30. Keine Einschränkungen
c18d2gz128 Amazon-ECR-Repository ohne konfigurierte Lebenszyklus-Richtlinie	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Erstellt eine Lebenszyklusrichtlinie für das angegebene Repository, falls noch keine Lebenszyklusrichtlinie vorhanden ist.	ImageAgeLimit: Die maximale Altersgrenze in Tagen (1—365) für „jedes“ Bild im Amazon ECR-Repository. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
DAvU99Dc4C Nicht ausgelastete Amazon EBS-Volumes	AWSManagedServices-DeleteUnusedEBSVolume Löscht nicht ausgelastete Amazon EBS-Volumes, wenn die Volumes in den letzten 7 Tagen nicht angehängt wurden. Ein Amazon EBS-Snapshot wird standardmäßig erstellt.	• CreateSnapshot: Wenn auf <code>gesetztttrue</code>, erstellt die Automatisierung einen Snapshot des Amazon EBS-Volumes, bevor es gelöscht wird. Die Standardinstellung lautet <code>true</code>. Gültige Werte sind <code>true</code> und <code>false</code> (Groß- und Kleinschreibung beachten). • MinimumUnattachedDays: Minstdauer des zu löschenden EBS-Volumes ohne Anhängen, bis zu 62 Tage. Wenn diese Einstellung auf <code>gesetzt ist0</code>, überprüft das SSM-Dokument nicht den Zeitraum, in dem das Volumen nicht angehängt wurde, und löscht das Volume, wenn das Volume derzeit nicht angehängt ist. Der Standardwert ist. 7 Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
hj M8 LMh88u Load Balancer im Leerlauf	AWSManagedServices-DeleteIdleClassicLoadBalancer Löscht einen Classic Load Balancer im Leerlauf, wenn er unbenutzt ist und keine Instances registriert sind.	IdleLoadBalancerDays: Die Anzahl der Tage, an denen der Classic Load Balancer 0 angeforderte Verbindungen hat, bevor er als inaktiv eingestuft wird. Die Standardeinstellung ist sieben Tage. Wenn die auto Ausführung aktiviert ist, löscht die Automatisierung inaktive Classic Load Balancer, wenn keine aktiven Back-End-Instances vorhanden sind. Für alle Classic Load Balancer im Leerlauf, die über aktive Back-End-Instances, aber keine fehlerfreien Back-End-Instances verfügen, wird keine auto Korrektur verwendet und OpsItems für die manuelle Korrektur wird eine automatische Korrektur erstellt.
TI 39 Half U8 Amazon RDS-DB-Instances im Leerlauf	AWSManagedServices-StopIdleRDSInstance Die Amazon RDS-DB-Instance, die sich in den letzten sieben Tagen im Leerlauf befand, wurde gestoppt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
COr6dfpM05 AWS Lambda aufgrund der Speichergröße überdimensionierte Funktionen	AWSManagedServices-ResizeLambdaMemory AWS Lambda Die Speichergröße der Funktion wird auf die empfohlene Speichergröße von angepasst. Trusted Advisor	RecommendedMemorySize: Die empfohlene Speicherzuweisung für die Lambda-Funktion. Der Wertebereich liegt zwischen 128 und 10240. Wenn die Größe der Lambda-Funktion vor der Ausführung der Automatisierung geändert wurde, werden die Einstellungen möglicherweise von dieser Automatisierung mit dem von empfohlenen Wert überschrieben. Trusted Advisor
QCH7dWOUx1 EC2 Amazon-Instances mit geringer Auslastung	AWSManagedServices-StopEC2Instance (Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus.) EC2 Amazon-Instances mit geringer Auslastung werden gestoppt.	ForceStopWithInstanceStore: Aufsetzen, <code>true</code> um das Stoppen von Instances mithilfe des Instance-Speichers zu erzwingen. Ansonsten auf <code>false</code> festlegen. Der Standardwert von <code>false</code> verhindert, dass die Instanz gestoppt wird. Gültige Werte sind wahr oder falsch (Groß- und Kleinschreibung beachten). Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
QCH7dWOUx1 EC2 Amazon-Instances mit geringer Auslastung	AWSManagedServices-Resizeln stanceByOneLevel Die Größe der EC2 Amazon-Instance wird innerhalb desselben Instance-Familientyps um einen Instance-Typ nach unten geändert. Die Instance wird während der Größenänderung gestoppt und gestartet und nach Abschluss der Ausführung des SSM-Dokuments wieder in den Ausgangszustand versetzt. Diese Automatisierung unterstützt keine Größenänderung von Instances, die sich in einer Auto Scaling Scaling-Gruppe befinden.	• MinimumDaysSinceLastChange: Mindestanzahl von Tagen seit der letzten Änderung des Instance-Typs. Wenn der Instanztyp innerhalb einer bestimmten Zeit geändert wurde, wird der Instanztyp nicht geändert. Verwenden Sie 0, um diese Überprüfung zu überspringen. Der Standardwert ist 7. • AMIBeforeGröße ändern: Um das Instanz-AMI vor der Größenänderung als Backup zu erstellen, wählen Sie <code>true</code>. Um kein Backup zu erstellen, wählen Sie <code>false</code>. Der Standardwert ist <code>false</code>. Gültige Werte sind <code>true</code> und <code>false</code> (Groß- und Kleinschreibung beachten). • ResizelfStopped: Um mit der Änderung der Instanzgröße fortzufahren, auch wenn sich die Instance im gestoppten Zustand befindet, wählen Sie <code>true</code>. Um die Größe der Instanz nicht automatisch zu ändern, wenn sie gestoppt ist, wählen Sie <code>false</code>. Gültige Werte sind <code>true</code> und <code>false</code> (Groß- und Kleinschreibung beachten). Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
QCH7dWOUx1 EC2 Amazon-Instances mit geringer Auslastung	AWSManagedServices-TerminateInstance EC2 Amazon-Instances mit geringer Auslastung werden beendet, wenn sie nicht Teil einer Auto Scaling Group sind und der Kündigungsschutz nicht aktiviert ist. Ein AMI wird standardmäßig erstellt.	AMIBeforeTermination erstellen: Setzen Sie diese Option auf <code>true</code> oder, <code>false</code> um ein Instance-AMI als Backup zu erstellen, bevor Sie die EC2 Instance beenden. Der Standardwert ist <code>true</code> . Gültige Werte sind <code>true</code> und <code>false</code> (Groß- und Kleinschreibung beachten). Keine Einschränkungen
G31sq1e9u Nicht ausgelastete Amazon Redshift-Cluster	AWSManagedServices-PauseRedshiftCluster Der Amazon Redshift Redshift-Cluster ist angehalten.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1cj39rr6v Konfiguration zum Abbruch unvollständiger mehrteiliger Uploads in Amazon S3	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Der Amazon S3 S3-Bucket ist mit einer Lebenszyklusregel konfiguriert, um mehrteilige Uploads abzubrechen, die nach bestimmten Tagen unvollständig bleiben.	DaysAfterInitiation: Die Anzahl der Tage, nach denen Amazon S3 einen unvollständigen mehrteiligen Upload stoppt. Die Standardeinstellung ist auf 7 Tage festgelegt. Keine Einschränkungen
c1z7kmr00n Amazon-Empfehlungen zur EC2 Kostenoptimierung für Instances	Verwenden Sie EC2 Amazon-Instance-Empfehlungen und Idle EC2 Amazon-Instance von Compute Optimizer Optimizer-Empfehlungen , die von Trusted Remediator unterstützt werden.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1z7kmr02n Amazon EBS-Empfehlungen zur Kostenoptimierung für Volumen	Verwenden Sie Amazon EBS-Volumenempfehlungen und Amazon EBS-Volumen im Leerlauf von. Compute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1z7kmr03n Empfehlungen zur Amazon RDS-Kostenoptimierung für DB-Instances	Verwenden Sie die Amazon RDS-Instance im Leerlauf von Compute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden .	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1z7kmr05n AWS Lambda Empfehlungen zur Kostenoptimierung für Funktionen	Verwenden Sie Lambda-Funktionsempfehlungen von Compute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden .	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor Sicherheitsüberprüfungen, die von Trusted Remediator unterstützt werden

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
12 Fnkpl8Y5	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey	Vorkonfigurierte Parameter sind nicht zulässig.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Exposed Access Keys	Der offengelegte IAM-Zugriffsschlüssel ist deaktiviert.	Anwendungen, die mit einem offengelegten IAM-Zugriffsschlüssel konfiguriert sind, können sich nicht authentifizieren.
Hs4Ma3G127 - API-Gateway-REST- und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein AWS Security Hub CSPM APIGatewayEntsprechender Check: 1.	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging Die Ausführungsprotokollierung ist auf der API-Phase aktiviert.	LogLevel: Protokollierungsebene zur Aktivierung der Ausführungsprotokollierung, ERROR — Die Protokollierung ist nur für Fehler aktiviert. INFO - Die Protokollierung ist für alle Ereignisse aktiviert. Sie müssen API Gateway die Berechtigung zum Lesen und Schreiben von Protokollen CloudWatch für Ihr Konto erteilen, um das Ausführungsprotokoll zu aktivieren. Weitere Informationen finden Sie unter CloudWatch Protokollierung für REST APIs in API Gateway einrichten.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G129 — API Gateway REST-API-Stufen sollten die Ablaufverfolgung aktiviert haben AWS X-Ray AWS Security Hub CSPM APIGatewayEntsprechender Check: 3.	AWSManagedServices-EnableApiGatewayXRayTracing X-Ray-Tracing ist auf der API-Phase aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G20 2 - API-Gateway-REST-API-Cache-Daten sollten im Ruhezustand verschlüsselt werden AWS Security Hub CSPM Entsprechender APIGatewayScheck: 5.	AWSManagedServices-EnableAPIGatewayCacheEncryption Aktivieren Sie die Verschlüsselung im Ruhezustand für API-Gateway-REST-API-Cachedaten, wenn in der API-Gateway-REST-API-Stufe der Cache aktiviert ist.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G177 - Entsprechende AWS Security Hub CSPM Prüfung — Auto Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Integritätsprüfungen verwenden 1. AutoScaling	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck Elastic Load Balancing Health Checks sind für die Auto Scaling Group aktiviert.	HealthCheckGracePeriod: Die Zeit in Sekunden, die Auto Scaling wartet, bevor der Integritätsstatus einer Amazon Elastic Compute Cloud-Instance überprüft wird, die in Betrieb genommen wurde. Die Aktivierung von Elastic Load Balancing Health Checks kann dazu führen, dass eine laufende Instance ersetzt wird, wenn einer der Elastic Load Balancing Load Balancer, die der Auto Scaling Scaling-Gruppe zugeordnet sind, sie als fehlerhaft meldet. Weitere Informationen finden Sie unter Einen Elastic Load Balancing Load Balancer zu Ihrer Auto Scaling Scaling-Gruppe hinzufügen
Hs4Ma3G245 — CloudFormation Stacks sollten in Amazon Simple Notification Service integriert werden AWS Security Hub CSPM Entsprechender CloudFormationCheck: 1.	AWSManagedServices-EnableCFNSTackNotification Ordnen Sie einen CloudFormation Stack einem Amazon SNS SNS-Thema für die Benachrichtigung zu.	BenachrichtigungARNs: Die ARNs Amazon SNS SNS-Themen, die mit ausgewählten CloudFormation Stacks verknüpft werden sollen. Um die auto Korrektur zu aktivieren, muss der NotificationARNs vorkonfigurierte Parameter angegeben werden.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G210 — Bei Distributionen sollte die Protokollierung aktiviert sein CloudFront Entsprechender AWS Security Hub CSPM Scheck CloudFront: 2.	AWSManagedServices-EnableCloudFrontDistributionLogging Die Protokollierung ist für CloudFront Amazon-Distributionen aktiviert.	• BucketName: Der Name des Amazon S3 S3-Buckets, in dem Sie Zugriffsprotokolle speichern möchten. • S3KeyPrefix: Das Präfix für den Standort im S3-Bucket für die CloudFront Amazon-Verteilungsprotokolle. • IncludeCookies: Gibt an, ob Cookies in die Zugriffsprotokolle aufgenommen werden sollen. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: • BucketName • S3KeyPrefix • IncludeCookies Informationen zu diesen Behebungsbeschränkungen finden Sie unter Wie aktiviere ich die Protokollierung für meine Distribution? CloudFront

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G109 — CloudTrail Die Überprüfung der Protokolldatei sollte aktiviert sein AWS Security Hub CSPM Entsprechender CloudTrailCheck: 4.	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation Aktiviert die Überprüfung des CloudTrail Trail-Logs.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G108 — CloudTrail Trails sollten in Amazon Logs integriert werden CloudWatch Entsprechender AWS Security Hub CSPM CloudTrail IScheck: 5.	AWSManagedServices-IntegrierteCloudTrailWithCloudWatch AWS CloudTrail ist in CloudWatch Logs integriert.	• CloudWatchLogsLogGroupName: Name der CloudWatch Logs-Protokollgruppe, an die CloudTrail Logs übermittelt werden. Sie müssen eine Protokollgruppe verwenden, die in Ihrem Konto vorhanden ist. • CloudWatchLogsRoleName: Name der IAM-Rolle, von der der CloudWatch Logs-Endpunkt annehmen soll, in die Protokollgruppe eines Benutzers zu schreiben. Sie müssen eine Rolle verwenden, die in Ihrem Konto vorhanden ist. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G217 — CodeBuild Projektumgebungen sollten über eine Protokollierungskonfiguration verfügen AWS Entsprechender AWS Security Hub CSPM CodeBuild Scheck: 4.	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig Aktiviert die Protokollierung für das CodeBuild Projekt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G306 - Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Check: DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Entfernt den öffentlichen Zugriff aus dem manuellen Cluster-Snapshot von Amazon DocumentDB.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G308 — Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Check: DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Aktiviert den Löschschutz für den Amazon DocumentDB-Cluster.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G323 - Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Check: DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection Aktiviert den Löschschutz für DynamoDB-Tabellen, die nicht von AMS stammen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
EPS02JT06W — Öffentliche Amazon EBS-Snapshots	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot Der öffentliche Zugriff für Amazon EBS Snapshot ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G118 - VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Verkehr zulassen AWS Security Hub CSPM Entsprechender EC2Scheck: 2.	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Alle Eingangs- und Ausgangsregeln in der Standardsicherheitsgruppe werden entfernt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G117 — Angehängte EBS-Volumes sollten im Ruhezustand verschlüsselt werden AWS Security Hub CSPM Entsprechender EC2Check: 3.	AWSManagedServices-EncryptInstanceVolume Das angehängte Amazon EBS-Volume auf der Instance ist verschlüsselt.	• KMSKeyID: AWS KMS Schlüssel-ID oder ARN zum Verschlüsseln des Volumes. • DeleteStaleNonEncryptedSnapshotBackups: Eine Markierung, die entscheidet, ob das Snapshot-Backup der alten unverschlüsselten Volumes gelöscht werden soll. Die Instanz wird im Rahmen der Problembehebung neu gestartet und ein Rollback ist möglich, wenn diese Einstellung auf „Hilft bei der Wiederherstellung“ gesetzt DeleteStaleNonEncryptedSnapshotBackups false ist.
Hs4Ma3G120 — Gestoppte EC2 Instanzen sollten nach einem bestimmten Zeitraum entfernt werden AWS Security Hub CSPM Entsprechender EC2Scheck: 4.	AWSManagedServices-TerminateInstance(Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus) EC2 Amazon-Instances, die für 30 Tage gestoppt wurden, werden beendet.	AMIBeforeKündigung erstellen: Um das Instance-AMI vor dem Beenden der EC2 Instance als Backup zu erstellen, wählen Sie true. Um vor dem Beenden kein Backup zu erstellen, wählen Sie false. Der Standardwert ist true. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G120 — Gestoppte EC2 Instanzen sollten nach einem bestimmten Zeitraum entfernt werden AWS Security Hub CSPM Entsprechender EC2Scheck: 4.	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime — EC2 Amazon-Instances, die für die im Security Hub definierte Anzahl von Tagen gestoppt wurden (Standardwert ist 30), werden beendet.	AMIBeforeKündigung erstellen: Um das Instance-AMI vor dem Beenden der EC2 Instance als Backup zu erstellen, wählen Sie <code>true</code>. Um vor dem Beenden kein Backup zu erstellen, wählen Sie <code>false</code>. Der Standardwert ist <code>true</code>. Keine Einschränkungen
Hs4Ma3G121 — Die EBS-Standardverschlüsselung sollte aktiviert sein Entsprechender AWS Security Hub CSPM EC2Scheck: 7.	AWSManagedServices-EncryptEBSDByDefault Die Amazon EBS-Verschlüsselung ist standardmäßig aktiviert für AWS-Region	Vorkonfigurierte Parameter sind nicht zulässig. Die standardmäßige Verschlüsselung ist eine regionsspezifische Einstellung. Wenn Sie es für eine Region aktivieren, können Sie es nicht für einzelne Volumes oder Snapshots in dieser Region deaktivieren.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G124 — EC2 Amazon-Instances sollten Instance Metadata Service Version 2 () verwenden IMDSv2 AWS Security Hub CSPM Entsprechender EC2Scheck: 8.	AWSManagedServices-TrustedRemediatorInstanz aktivieren EC2 IMDSv2 EC2 Amazon-Instances verwenden Instance Metadata Service Version 2 (IMDSv2).	• IMDSv1MetricCheckPeriod: Die Anzahl der Tage (42-455), in denen IMDSv1 Nutzungsmetriken analysiert CloudWatch werden sollen. Wenn die EC2 Amazon-Instance innerhalb des angegebenen Zeitraums erstellt wurde, beginnt die Analyse mit dem Erstellungsdatum der Instance. • HttpPutResponseHopLimit: Die maximale Anzahl von Netzwerk-Hops, die für das Instance-Metadaten-Token zulässig sind. Dieser Wert kann zwischen 2 Hops 1 und Hops konfiguriert werden. Ein Hop-Limit von 1 schränkt den Token-Zugriff auf Prozesse ein, die direkt auf der Instance ausgeführt werden, während ein Hop-Limit von von den auf der Instance ausgeführten Containern den Zugriff 2 ermöglicht. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G207 — EC2 Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen AWS Security Hub CSPM Entsprechender EC2Scheck: 1.5	AWSManagedServices-UpdateAutoAssignPublicIpv4 Adressen VPC-Subnetze sind so konfiguriert, dass öffentliche IP-Adressen nicht automatisch zugewiesen werden.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G209 — Nicht verwendete Network Access Control Lists wurden entfernt Entsprechender AWS Security Hub CSPM EC2Scheck: 1.6	AWSManagedServices-DeleteUnusedNACL Löschen Sie ungenutzte Netzwerk-ACL	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G215 - Unbenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden Entsprechender AWS Security Hub CSPM EC2Scheck: 2.2	AWSManagedServices-DeleteSecurityGroups Löschen Sie nicht verwendete Sicherheitsgruppen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G247 — Amazon EC2 Transit Gateway sollte VPC-Anhangsanfrage nicht automatisch akzeptieren AWS Security Hub CSPM Entsprechender EC2Scheck: 2.3	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Deaktiviert die automatische Annahme von VPC-Anhangsanforderungen für das angegebene Amazon EC2 Transit Gateway, das nicht von AMS stammt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G235 — Für private ECR-Repositoryn sollte die Tag-Unveränderlichkeit konfiguriert sein Entsprechender AWS Security Hub CSPM Check: ECR.2	AWSManagedServices-TrustedR emediatorSetImageTagImmutability Setzt die Mutabilitätseinstellungen für das Image-Tag für das angegebene Repository auf IMMUTABLE.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G216 — Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein Entsprechender AWS Security Hub CSPM Check: ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy Für das ECR-Repository ist eine Lebenszyklusrichtlinie konfiguriert.	LifecyclePolicyText: Der Richtlinientext für das JSON-Repository, der auf das Repository angewendet werden soll. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: LifecyclePolicyText

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G325 — Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog Das Auditprotokoll ist für den EKS-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G183 — Der Application Load Balancer sollte so konfiguriert sein, dass er HTTP-Header löscht AWS Security Hub CSPM Entsprechender Check: ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer ist für ungültige Header-Felder konfiguriert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G184 — Die Protokollierung von Application Load Balancers und Classic Load Balancers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: ELB.5	AWSManagedServices-EnableELBLogging (Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus) Die Protokollierung von Application Load Balancer und Classic Load Balancer ist aktiviert.	• BucketName: Der Bucket-Name (nicht der ARN). Stellen Sie sicher, dass die Bucket-Richtlinie für die Protokollierung korrekt konfiguriert ist. • S3KeyPrefix: Das Präfix für den Speicherort im Amazon S3 S3-Bucket für die Elastic Load Balancing Balancing-Protokolle. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: • BucketName • S3KeyPrefix Der Amazon S3 S3-Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Erlaubnis erteilt, die Zugriffsp rotokolle in den Bucket zu schreiben.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G184 — Die Protokollierung von Application Load Balancers und Classic Load Balancers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: ELB.5	AWSManagedServices-EnableELBLoggingV2 Die Protokollierung von Application Load Balancer und Classic Load Balancer ist aktiviert.	• TargetBucketTagKey: Der Tag-Name (Groß- und Kleinschreibung beachten), der zur Identifizierung des Amazon S3 S3-Ziel-Buckets verwendet wird. Verwenden Sie diesen Wert zusammen mit <code>TargetBucketTagValue</code> , um den Bucket zu taggen, der als Ziel-Bucket für die Zugriffsprotokollierung dienen soll. • TargetBucketTagValue: Der Tag-Wert (Groß- und Kleinschreibung beachten), der zur Identifizierung des Amazon S3 S3-Ziel-Buckets verwendet wird. Verwenden Sie diesen Wert zusammen mit <code>TargetBucketTagKey</code> , um den Bucket zu taggen, der als Ziel-Bucket für die Zugriffsprotokollierung dienen soll. • S3BucketPrefix: Das Präfix (logische Hierarchie) für den Amazon S3 S3-Bucket. Das von Ihnen angegebene Präfix darf die Zeichenfolge AWSLogs nicht enthalten. Weitere Informationen finden Sie unter Organisieren von Objekten mit Präfixen. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfig

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		urierten Parameter angegeben werden: • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix Der Amazon S3 S3-Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Erlaubnis erteilt, die Zugriffsprotokolle in den Bucket zu schreiben.
Hs4Ma3G326 — Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess Die Amazon EMR-Einstellungen für den öffentlichen Zugriff sperren sind für das Konto aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G135 - AWS KMS Schlüssel sollten nicht ungewollt gelöscht werden Entsprechender AWS Security Hub CSPM Scheck: KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS Das Löschen des Schlüssels wurde abgebrochen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G299 — Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein Entsprechender AWS Security Hub CSPM Scheck: Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection Aktiviert den Löschschutz für den Amazon Neptune Neptune-Cluster.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G319 — Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein AWS Security Hub CSPM Entsprechender NetworkFirewallScheck: 9.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection- Aktiviert den Löschschutz für die AWS-Netzwerk-Firewall.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G223 — OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden Entsprechender AWS Security Hub CSPM OpenSearchScheck: 3.	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption Die Node-zu-Knoten-Verschlüsselung ist für die Domain aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Nachdem die node-to-node Verschlüsselung aktiviert wurde, können Sie die Einstellung nicht deaktivieren. Erstellen Sie stattdessen einen manuellen Snapshot der verschlüsselten Domain, erstellen Sie eine weitere Domain, migrieren Sie Ihre Daten und löschen Sie dann die alte Domain.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G222 — OpenSearch Die Protokollierung von Domänenfehlern in Logs sollte aktiviert sein CloudWatch Entsprechender AWS Security Hub CSPM Check: Opensearch.4	AWSManagedServices-EnableOpenSearchLogging Die Fehlerprotokollierung ist für die Domain aktiviert. OpenSearch	CloudWatchLogGroupArn: Der ARN einer Amazon CloudWatch Logs-Protokollgruppe. Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden: CloudWatchLogGroupArn Die CloudWatch Amazon-Ressourcenrichtlinie muss mit Berechtigungen konfiguriert werden. Weitere Informationen finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service-Benutzerhandbuch
Hs4Ma3G221 — Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein Entsprechender Check AWS Security Hub CSPM : Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch Domains sind mit aktivierter Audit-Protokollierung konfiguriert.	CloudWatchLogGroupArn: Der ARN der CloudWatch Logs-Gruppe, in der Logs veröffentlicht werden sollen. Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden: CloudWatchLogGroupArn Die CloudWatch Amazon-Ressourcenrichtlinie muss mit Berechtigungen konfiguriert werden. Weitere Informationen finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service-Benutzerhandbuch

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G220 — Verbindungen zu OpenSearch Domains sollten mit TLS 1.2 verschlüsselt werden Entsprechender AWS Security Hub CSPM Check: <u>Opensearch.8</u>	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 Die TLS-Richtlinie ist auf `policy-min-TLS-1-2-2019-07` gesetzt und nur verschlüsselte Verbindungen über HTTPS (TLS) sind erlaubt.	Vorkonfigurierte Parameter sind nicht erlaubt. Für die Verwendung von TLS 1.2 sind Verbindungen zu OpenSearch Domänen erforderlich. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Testen Sie Ihre Anwendungen mit dieser Funktion, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.
Hs4Ma3G194 — Amazon RDS-Snapshot sollte privat sein Entsprechender AWS Security Hub CSPM Check: RDS.1	AWSManagedServices-DisablePublicAccessOnRDSnapshotV2 Der öffentliche Zugriff für Amazon RDS-Snapshot ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G192 — RDS-DB-Instances sollten den öffentlichen Zugriff verbieten, wie in der Konfiguration festgelegt PubliclyAccessible AWS AWS Security Hub CSPM Entsprechender Check: RDS.2	AWSManagedServices-TrustedReaderDisablePublicAccessOnRDSInstance Deaktivieren Sie den öffentlichen Zugriff auf die RDS-DB-Instance.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G189 — Die erweiterte Überwachung ist für Amazon RDS-DB-Instances konfiguriert Entsprechender AWS Security Hub CSPM Scheck: RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring Aktivieren Sie die erweiterte Überwachung für Amazon RDS-DB-Instances	• MonitoringInterval: Das Intervall in Sekunden zwischen den Punkten, an denen Enhanced Monitoring-Metriken für die DB-Instance erfasst werden. Gültige Intervalle sind 0, 1, 5, 10, 15, 30 und 60. Um die Erfassung von Metriken für erweiterte Überwachung zu deaktivieren, geben Sie 0 an. • MonitoringRoleName: Der Name der IAM-Rolle, die es Amazon RDS ermöglicht, erweiterte Überwachungsmetriken an Amazon CloudWatch Logs zu senden. Wenn keine Rolle angegeben ist, <code>rds-monitoring-role</code> wird die Standardrolle verwendet oder erstellt, falls sie nicht existiert. Wenn die erweiterte Überwachung vor der Ausführung der Automatisierung aktiviert ist, werden die Einstellungen möglicherweise durch diese Automatisierung mit den in den vorkonfigurierten Parametern konfigurierten <code>MonitoringRoleName</code> Werten <code>MonitoringInterval</code> und überschrieben.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G190 — Bei Amazon RDS-Clustern sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Der Löschschutz ist für Amazon RDS-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G198 — Für Amazon RDS-DB-Instances sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Der Löschschutz ist für Amazon RDS-Instances aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G199 — RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch Entsprechender AWS Security Hub CSPM Scheck: RDS.9	AWSManagedServices-TrustedR emediatorEnableRDSLogExports RDS-Protokollexporte sind für die RDS-DB-Instance oder den RDS-DB-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. AWSServiceRoleForRDS für die dienstverknüpfte Rolle ist erforderlich.
Hs4Ma3G160 — Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden Entsprechender AWS Security Hub CSPM Scheck: RDS.10	AWSManagedServices-UpdateRD SIAMDatabaseAuthentication AWS Identity and Access Management Die Authentifizierung ist für die RDS-Instanz aktiviert.	ApplyImmediately: Gibt an, ob die Änderungen in dieser Anfrage und alle ausstehenden Änderungen so schnell wie möglich asynchron angewendet werden. Um die Änderung sofort anzuwenden, wählen Sie <code>true</code>. Um die Änderung für das nächste Wartungsfenster zu planen, wählen Sie <code>false</code>. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G161 — Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden Entsprechender AWS Security Hub CSPM Scheck: RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication Die IAM-Authentifizierung ist für den RDS-Cluster aktiviert.	ApplyImmediately: Gibt an, ob die Änderungen in dieser Anfrage und alle ausstehenden Änderungen so schnell wie möglich asynchron angewendet werden. Um die Änderung sofort anzuwenden, wählen Sie <code>true</code>. Um die Änderung für das nächste Wartungsfenster zu planen, wählen Sie <code>false</code>. Keine Einschränkungen
Hs4Ma3G162 — Automatische RDS-Upgrades für kleinere Versionen sollten aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Die automatische Upgrade-Konfiguration für Nebenversionen für Amazon RDS ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Die Amazon RDS-Instance muss sich im <code>available</code> Status befinden, damit diese Korrektur durchgeführt werden kann.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G163 — RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren Entsprechender AWS Security Hub CSPM Scheck: RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagToSnapshot Die Einstellung für Amazon RDS-Cluster ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Amazon RDS-Instances müssen sich im Status „Verfügbar“ befinden, damit diese Korrektur durchgeführt werden kann.
Hs4Ma3G164 — RDS-DB-Instances sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren Entsprechender AWS Security Hub CSPM Scheck: RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot Die Einstellung für Amazon RDS ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Amazon RDS-Instances müssen sich im Status „Verfügbar“ befinden, damit diese Korrektur durchgeführt werden kann.
RSS93 HQwa1 Öffentliche Amazon RDS-Snapshots	AWSManagedServices-DisablePublicAccessOnRDSnapshotV2 Der öffentliche Zugriff für Amazon RDS-Snapshot ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G103 — Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten Entsprechender AWS Security Hub CSPM Scheck: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster Der öffentliche Zugriff auf den Amazon Redshift Redshift-Cluster ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Durch die Deaktivierung des öffentlichen Zugriffs werden alle Clients blockiert, die aus dem Internet kommen. Und der Amazon Redshift Redshift-Cluster befindet sich für einige Minuten im Änderungsstatus, während die Behebung den öffentlichen Zugriff auf den Cluster deaktiviert.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G106 — Bei Amazon Redshift-Clustern sollte die Auditprotokollierung aktiviert sein Entsprechender AWS Security Hub CSPM Check: Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging Die Audit-Protokollierung ist für Ihren Amazon Redshift Redshift-Cluster während des Wartungsfensters aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter bereitgestellt werden. BucketName: Der Bucket muss sich im selben Bucket befinden. AWS-Region Der Cluster muss über die Berechtigungen „Read Bucket“ und „Put Object“ verfügen. Wenn die Redshift-Clusterprotokollierung vor der Ausführung der Automatisierung aktiviert ist, werden die Protokollierungseinstellungen möglicherweise durch diese Automatisierung mit den in den vorkonfigurierten Parametern konfigurierten S3KeyPrefix Werten BucketName und überschrieben.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G105 — Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein Entsprechender AWS Security Hub CSPM Check: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade- Upgrades der Hauptversionen werden während des Wartungsfensters automatisch auf den Cluster angewendet. Es gibt keine unmittelbare Ausfallzeit für den Amazon Redshift Redshift-Cluster, aber Ihr Amazon Redshift Redshift-Cluster kann während seines Wartungsfensters Ausfallzeiten haben, wenn er auf eine Hauptversion aktualisiert wird.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G104 — Amazon Redshift Redshift-Cluster sollten erweitert es VPC-Routing verwenden Entsprechender AWS Security Hub CSPM Check: Redshift.7	AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting Verbessertes VPC-Routing ist für Amazon Redshift Redshift-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G173 — Die Einstellung S3 Block Public Access sollte auf Bucket-Ebene aktiviert sein AWS Security Hub CSPM Entsprechender Check: S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Öffentliche Zugriffssperren auf Bucket-Ebene werden für den Amazon S3 S3-Bucket angewendet.	Vorkonfigurierte Parameter sind nicht zulässig. Diese Korrektur kann sich auf die Verfügbarkeit von S3-Objekten auswirken. Informationen darüber, wie Amazon S3 den Zugriff bewertet, finden Sie unter Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G230 — Die Protokollierung des S3-Bucket-Servers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: S3.9	AWSManagedServices-EnableBucketAccessLogging(Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus) Die Protokollierung Amazon S3 S3-Serverzugriffs ist aktiviert.	• TargetBucket: Der Name des S3-Buckets zum Speichern von Serverzugriffsprotokollen. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte (bei Werten wird Groß- und Kleinschreibung beachtet). Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden , wählen Sie SimplePrefix . Um den partitionierten S3-Schlüssel für Protokollobjekte und EventTime für das partitionierte Präfix zu verwenden, wählen Sie. PartitionedPrefixEventTime Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte Präfix zu verwenden , wählen Sie. PartitionedPrefixDeliveryTime Gültige Werte sind SimplePrefix , PartitionedPrefixEventTime und PartitionedPrefixDeliveryTime . Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden: TargetBucket

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung .

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G230 — Die Protokollierung des S3-Bucket-Servers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 — Die Amazon S3 S3-Bucket-Protokollierung ist aktiviert.	• TargetBucketTagKey: Der Tag-Name (Groß- und Kleinschreibung beachten) zur Identifizierung des Ziel-Buckets. Verwenden Sie dieses und TargetBucketTagValue, um den Bucket zu taggen, der als Ziel-Bucket für die Zugriffsprotokollierung verwendet werden soll. • TargetBucketTagValue: Der Tag-Wert (Groß- und Kleinschreibung beachten) zur Identifizierung des Ziel-Buckets. Verwenden Sie diesen Wert und TargetBucketTagKeymarkieren Sie den Bucket, der als Ziel-Bucket für die Zugriffsprotokollierung verwendet werden soll. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte (Werte unterscheiden Groß- und Kleinschreibung): Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden, wählen Sie SimplePrefix. Um den partitionierten S3-Schlüssel für Protokollobjekte und das partitionierte Präfix zu verwenden EventTime , wählen Sie. PartitionedPrefixEventTime Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Präfix zu verwenden, wählen Sie. PartitionedPrefixDeliveryTime Der Standardwert ist PartitionedPrefixEventTime. Um die auto Korrektur zu aktivieren, müssen die folgenden Parameter angegeben werden: TargetBucketTagKeyund TargetBucketTagValue. Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Pfx0 RwgBli Amazon S3 Bucket-Berechtigungen	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Blockieren des öffentlichen Zugriffs	Es sind keine vorkonfigurierten Parameter zulässig. Diese Prüfung besteht aus mehreren Warnkriterien. Diese Automatisierung behebt Probleme mit dem öffentlichen Zugriff. Die Behebung anderer Konfigurationsprobleme, die mit gekennzeichnet sind, wird Trusted Advisor nicht unterstützt. Diese Korrektur unterstützt die Wiederherstellung von AWS-Service erstellten S3-Buckets (z. B. cf-templates-000000000000).
Hs4Ma3G272 — Benutzer sollten keinen Root-Zugriff auf Notebook-Instanzen haben SageMaker AWS Security Hub CSPM Entsprechender SageMaker Scheck : 3.	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess Der Root-Zugriff für Benutzer ist für die SageMaker Notebook-Instanz deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Diese Korrektur führt zu einem Ausfall, wenn sich die SageMaker Notebook-Instanz im Status befindet. InService

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G179 — SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS Entsprechender AWS Security Hub CSPM Scheck: SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest Das SNS-Thema ist mit serverseitiger Verschlüsselung konfiguriert.	KmsKeyId: Die ID eines AWS verwalteten Kundenhauptschlüssels (CMK) für Amazon SNS oder eines benutzerdefinierten CMK, der für die serverseitige Verschlüsselung (SSE) verwendet werden soll. Die Standardeinstellung ist auf eingestellt. <code>alias/aws/sns</code> Wenn ein benutzerdefinierter AWS KMS Schlüssel verwendet wird, muss er mit den richtigen Berechtigungen konfiguriert werden. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung (SSE) für ein Amazon SNS SNS-Thema aktivieren
Hs4Ma3G158 — SSM-Dokumente sollten nicht öffentlich sein Entsprechender AWS Security Hub CSPM Scheck: SSM.4	AWSManagedServices-TrustedResourceMediatorDisableSSMDocPublicSharing- Deaktiviert das öffentliche Teilen von SSM-Dokumenten.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G136 — Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden Entsprechender AWS Security Hub CSPM Scheck: SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Nachrichten in Amazon SQS sind verschlüsselt.	• SqsManagedSseEnabled: Auf aktiviert, <code>true</code> um serverseitige Warteschlangenverschlüsselung mit Amazon SQS SQS-eigenen Verschlüsselungsschlüsseln zu aktivieren, eingestellt auf, <code>false</code> um serverseitige Warteschlangenverschlüsselung mit einem Schlüssel zu aktivieren. AWS KMS • KMSKeyID: Die ID oder der Alias eines AWS verwalteten Kundenhauptschlüssels (CMK) für Amazon SQS oder eines benutzerdefinierten CMK, der für die serverseitige Verschlüsselung der Warteschlange verwendet werden soll. Wird verwendet, falls nicht angegeben. <code>alias/aws/sqs</code> • KmsDataKeyReusePeriodSeconds: Die Zeitspanne in Sekunden, für die Amazon SQS einen Datenschlüssel wiederverwenden kann, um Nachrichten zu verschlüsseln oder zu entschlüsseln, bevor er erneut anruft. AWS KMS Eine Ganzzahl stellt Sekunden dar, und zwar zwischen 60 Sekunden (1 Minute) und 86 400 Sekunden (24 Stunden). Diese Einstellung wird ignoriert, wenn sie auf <code>gesetzt</code> ist. <code>SqsManagedSseEnabled</code> ist <code>true</code>

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Anonym SendMessage und ReceiveMessage Anfragen an die verschlüsselte Warteschlange werden abgelehnt. Alle Anfragen zu Warteschlangen mit aktiviertem SSE müssen HTTPS und Signature Version 4 verwenden.

Trusted Advisor von Trusted Remediator unterstützte Fehlertoleranzprüfungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz138 Amazon DynamoDB DynamoDB- Wiederher- stellung Point-in- time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Aktiviert die point-in-time Wiederherstellung für DynamoDB-Tabellen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
R365s2qddf Amazon S3 Bucket-Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Die Amazon S3 S3-Bucket-Versionierung ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Diese Korrektur unterstützt nicht die Standardisierung AWS-Service erstellter S3-Buckets (zum Beispiel cf-templates-000000000000).

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
BueAdJ7nRP Amazon S3 Bucket-Protokollierung	AWSManagedServices-EnableBucketAccessLogging Die Amazon S3 S3-Bucket-Protokollierung ist aktiviert.	• TargetBucket: Der Name des S3-Buckets zum Speichern von Serverzugriffsprotokollen. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte. Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden , wählen SieSimplePrefix . Um den partitionierten S3-Schlüssel für Protokollobjekte und das partitionierte Präfix zu verwenden EventTime , wählen Sie. PartitionedPrefixEventTime Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte Präfix zu verwenden, wählen Sie. PartitionedPrefixDeliveryTime Der Standardwert ist PartitionedPrefixEventTime . Gültige Werte sind und (Groß SimplePrefix - PartitionedPrefixEventTime und Kleinschreibung beachtenPartitionedPrefixDeliveryTime). Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden:

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		• TargetBucket Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung.
F2ik5R6DEP Amazon RDS Multi-AZ	AWSManagedServices-TrustedR emediatorEnableRDSMultiAZ Die Bereitstellung in mehreren Verfügbarkeitszonen ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Während dieser Änderung kann es zu Leistungseinbußen kommen.
H7 IgTzj TYb Amazon-EBS-Snapshots	AWSManagedServices-TrustedR emediatorCreateEBSSnapshot Amazon EBSsnapshots wurden gegründet.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
op QPADk ZvH RDS-Backups	AWSManagedServices-EnableRDSBackupRetention Die Aufbewahrung von Amazon RDS-Backups ist für die Datenbank aktiviert.	• BackupRetentionPeriod: Die Anzahl der Tage (1—35) für die Aufbewahrung automatisierter Backups. • ApplyImmediately: Gibt an, ob die Änderung der Aufbewahrung von RDS-Backups und alle ausstehenden Änderungen so schnell wie möglich asynchron angewendet werden. Wählen Sie <code>true</code>, ob die Änderung sofort angewendet werden <code>false</code> soll, oder ob Sie die Änderung für das nächste Wartungsfenster planen möchten. Wenn der <code>ApplyImmediately</code> Parameter auf <code>true</code> gesetzt ist, werden die ausstehenden Änderungen in der Datenbank zusammen mit der RDS Backup Aufbewahrungseinstellung übernommen.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1qf5bt013 Bei Amazon RDS-DB-Instances ist die automatische Speicherskalierung deaktiviert	AWSManagedServices-TrustedReaderEnableRDSInstanceStorageAutoScaling- Die automatische Speicherskalierung ist für die Amazon RDS-DB-Instance aktiviert.	MaxAllocatedStorageIncrease Percentage: Der prozentuale Anstieg des Stroms Allocated Storage, der MaxAllocatedStorage eingestellt werden soll. Die Standardeinstellung ist auf eingestellt26. Sie müssen den maximalen Speicherschwellenwert auf mindestens 10% über dem aktuell zugewiesenen Speicherplatz festlegen. Es hat sich bewährt, den maximalen Speicherschwellenwert auf mindestens 26% zu erhöhen. Einzelheiten finden Sie unter Automatisches Kapazitätmanagement mit Amazon Relational Database Service Storage Autoscaling. Keine Einschränkungen
7q GXs KIUw Classic Load Balancer Balancer-Verbindungsabbau	AWSManagedServices-TrustedReaderEnableCLBConnectionDraining Das Entleeren von Verbindungen ist für Classic Load Balancer aktiviert.	ConnectionDrainingTimeout: Die maximale Zeit in Sekunden, um die bestehenden Verbindungen offen zu halten, bevor die Instances deregistriert werden. Die Standardeinstellung ist auf Sekunden festgelegt. 300 Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz106 Amazon EBS nicht im AWS Backup Plan enthalten	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS ist im AWS Backup Plan enthalten.	Bei der Problembehebung wird das Amazon EBS-Volume mit dem folgenden Tag-Paar versehen. Das Tag-Paar muss den tagbasierten Ressourcenauswahlkriterien für entsprechen. AWS Backup • TagKey • TagValue Keine Einschränkungen
c18d2gz107 Amazon DynamoDB-Tabelle nicht im Plan enthalten AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan Amazon DynamoDB Table ist im AWS Backup Plan enthalten.	Remediation kennzeichnet Amazon DynamoDB mit dem folgenden Tag-Paar. Das Tag-Paar muss den tagbasierten Ressourcenauswahlkriterien für entsprechen. AWS Backup • TagKey • TagValue Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz117 Amazon EFS nicht im AWS Backup Plan enthalten	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS ist im AWS Backup Plan enthalten.	Bei der Problembehebung wird Amazon EFS mit dem folgenden Tag-Paar versehen. Das Tag-Paar muss den tagbasierten Ressourcenwahlkriterien für entsprechen. AWS Backup • TagKey • TagValue Keine Einschränkungen
c18d2gz105 Network Load Balancer – Zonenübergreifender Lastausgleich	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Zonenübergreifendes Load Balancing ist auf dem Network Load Balancer aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt026 Der Amazon synchronously_commit RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter synchronously_commit ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1qf5bt030 Der Amazon innodb_flush_log_at_trx_commit RDS-Parameter ist nicht 1	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Der Parameter innodb_flush_log_at_trx_commit ist 1 für Amazon RDS auf eingestellt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt031 Der Amazon sync_binlog RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Der Parameter sync_binlog ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt036 Die Amazon innodb_default_row_format RDS-Parametereinstellung ist unsicher	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Der Parameter innodb_default_row_format ist DYNAMIC für Amazon RDS auf eingestellt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c18d2gz144 EC2 Detaillierte Amazon-Überwachung nicht aktiviert	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Die detaillierte Überwachung ist für Amazon aktiviert EC2.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor Leistungsprüfungen werden von Trusted Remediator unterstützt

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
COr6dfpM06 AWS Lambda Funktionen sind im Hinblick auf die Speichergröße nicht ausreichend bereitgestellt	AWSManagedServices-ResizeLambdaMemory Die Speichergröße der Lambda-Funktionen wird auf die empfohlene Speichergröße von angepasst. Trusted Advisor	RecommendedMemorySize: Die empfohlene Speicherzuweisung für die Lambda-Funktion. Der Wertebereich liegt zwischen 128 und 10240. Wenn die Größe der Lambda-Funktion vor der Ausführung der Automatisierung geändert wird, überschreibt diese Automatisierung möglicherweise die Einstellungen mit dem von empfohlenen Wert. Trusted Advisor
ZRxQIPsb6c EC2 Amazon-Instances mit hoher Auslastung	AWSManagedServices-ResizelnstanceByOneLevel Die Größe von EC2 Amazon-Instances wird um einen Instance-Typ höher im selben Instance-Familientyp geändert. Die Instances werden während der Größenänderung gestoppt und gestartet und nach Abschluss der Ausführung wieder in den Ausgangszustand versetzt. Diese Automatisierung unterstützt keine Größenänderung von Instances, die sich in einer Auto Scaling Group befinden.	• MinimumDaysSinceLastChange: Die Mindestanzahl von Tagen seit der letzten Änderung des Instance-Typs. Wenn der Instanztyp innerhalb der angegebenen Zeit geändert wurde, wird der Instanztyp nicht geändert. Verwenden Sie 0, um diese Überprüfung zu überspringen. Der Standardwert ist 7. • AMIBeforeGröße ändern: Um das Instanz-AMI vor der Größenänderung als Backup zu erstellen, wählen Sie true. Um kein Backup zu erstellen, wählen Sie false. Der Standardwert ist false. Gültige Werte sind true und false (Groß- und Kleinschreibung beachten).

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		• <code>ResizeStopped</code>: Um mit der Änderung der Instanzgröße fortzufahren, auch wenn sich die Instance im gestoppten Zustand befindet, wählen Sie <code>true</code>. Um die Größe der Instanz nicht automatisch zu ändern, wenn sie gestoppt ist, wählen Sie <code>false</code>. Gültige Werte sind <code>true</code> und <code>false</code> (Groß- und Kleinschreibung beachten). Keine Einschränkungen
c1qf5bt021 Amazon <code>innodb_change_buffering</code> RDS-Parameter, der weniger als den optimalen Wert verwendet	<code>AWSManagedServices-TrustsRemediatorRemediateRDSParameterGroupParameter</code> Der Wert des <code>innodb_change_buffering</code> Parameters ist <code>NONE</code> für Amazon RDS auf festgelegt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt025 Der Amazon <code>autovacuum</code> RDS-Parameter ist ausgeschaltet	<code>AWSManagedServices-TrustsRemediatorRemediateRDSParameterGroupParameter</code> Der Parameter <code>autovacuum</code> ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1qf5bt028 Der Amazon <code>enable_indeonlyscan</code> RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Der Parameter <code>enable_indeonlyscan</code> ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt029 Der Amazon <code>enable_indeonlyscan</code> RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Der Parameter <code>enable_indeonlyscan</code> ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt032 Der Amazon <code>innodb_stats_persistent</code> RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Der Parameter <code>innodb_stats_persistent</code> ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt037 Der Amazon <code>general_log</code> RDS-Parameter ist aktiviert	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Der Parameter <code>general_log</code> ist für Amazon RDS ausgeschaltet.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor Von Trusted Remediator unterstützte Prüfungen von Service-Limits

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Ln7RR0L7J9 EC2VPC Elastic IP-Adresse	AWSManagedServices-UpdateVpcElasticIPQuota Ein neues Limit für EC2 elastische IP-Adressen von VPC wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
kM7QQ0L7J9 VPC-Internet-Gateways	AWSManagedServices-IncreaseServiceQuota- Ein neues Limit für VPC-Internet-Gateways wird angefordert. Standardmäßig wird das Limit um drei erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
JL7PP0L7J9 VPC	AWSManagedServices-IncreaseServiceQuota Ein neues Limit für VPC wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
FW7HH0L7J9 Auto Scaling-Gruppen	AWSManagedServices-Increase ServiceQuota Ein neues Limit für Auto Scaling Scaling-Gruppen wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
3Njm0 DJQO9 RDS-Optionsgruppen	AWSManagedServices-Increase ServiceQuota Ein neues Limit für Amazon RDS-Optionsgruppen wird beantragt. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
EM8b3yLRTr ELB Application Load Balancers	AWSManagedServices-Increase ServiceQuota Ein neues Limit für ELB Application Load Balancers wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
8 WiQ K YSt25 ELB Network Load Balancers	AWSManagedServices-Increase ServiceQuota Ein neues Limit für ELB Network Load Balancers wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.

Trusted Advisor Prüfungen der betrieblichen Exzellenz werden von Trusted Remediator unterstützt

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz125 Amazon API Gateway protokolliert keine Ausführungsprotokolle	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging Die Ausführungsprotokollierung ist auf der API-Phase aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Sie müssen API Gateway die Berechtigung zum Lesen und Schreiben von Protokollen CloudWatch für Ihr Konto erteilen, um das Ausführungsprotokoll zu aktivieren. Weitere Informationen finden Sie unter CloudWatch Protokollierung für REST APIs in API Gateway einrichten .
c18d2gz168	AWSManagedServices-TrustedRemediatorEnableELBDeletionP	Vorkonfigurierte Parameter sind nicht zulässig.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Elastic-Load-Balancing-Löschschutz ist für Load Balancer nicht aktiviert	rotection- Der Löschschutz ist für den Elastic Load Balancer aktiviert.	Keine Einschränkungen
c1qf5bt012 Amazon RDS Performance Insights ist ausgeschaltet	AWSManagedServices-TrustedR emediatorEnableRDSPerformanceInsights Performance Insights ist für Amazon RDS aktiviert.	- PerformanceInsightsRetentionPeriod: Die Anzahl der Tage, für die Performance Insights Insights-Daten aufbewahrt werden sollen. Gültige Werte: 7 oder Monat * 31, wobei Monat eine Anzahl von Monaten zwischen 1 und 23 ist. Beispiele: 93 (3 Monate* 31), 341 (11 Monate* 31), 589 (19 Monate* 31) oder 731. - PerformanceInsightsKMSKeyId: Die AWS KMS Schlüssel-ID für die Verschlüsselung von Performance Insights Insights-Daten. Wenn Sie keinen Wert für PerformanceInsights KMSKey Id angeben, verwendet Amazon RDS Ihren AWS KMS Standardschlüssel. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1fd6b96l4 Amazon S3 S3-Zugriffsprotokolle aktiviert	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 Die Protokollierung des Amazon S3 S3-Bucket-Zugriffs ist aktiviert.	• TargetBucketTagValue: Der Tag-Wert (Groß- und Kleinschreibung beachten) zur Identifizierung des Ziel-Buckets. Verwenden Sie ihn und TargetBucketTagKey markieren Sie den Bucket, der als Ziel-Bucket für die Zugriffsprotokollierung verwendet werden soll. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte (bei Werten wird Groß- und Kleinschreibung beachtet). Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden , wählen Sie SimplePrefix . Um den partitionierten S3-Schlüssel für Protokollobjekte und EventTime für das partitionierte Präfix zu verwenden, wählen Sie. PartitionedPrefixEventTime Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte Präfix zu verwenden , wählen Sie. PartitionedPrefixDeliveryTime Gültige Werte sind SimplePrefix , PartitionedPrefixEventTime und PartitionedPrefixDeliveryTime .

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden: TargetBucketTagKey und TargetBucketTagValue Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung.

Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator

Konfigurationen werden AWS AppConfig als Teil der Trusted Remediator-Anwendung gespeichert. Jede Trusted Advisor Prüfkategorie hat ein eigenes Konfigurationsprofil. Weitere Informationen zu Trusted Advisor Kategorien finden Sie unter [Prüfkategorien anzeigen](#).

Sie können beantragen, dass Behebungen pro Ressource oder pro Trusted Advisor Prüfung konfiguriert werden. Sie können Ausnahmen mithilfe von Ressourcen-Tags anwenden.

Note

Die Behebung von Trusted Advisor Ergebnissen ist derzeit mit konfiguriert AWS AppConfig, und diese Funktion wird heute vollständig unterstützt. AMS geht davon aus, dass sich dies in future ändern wird. Es ist eine bewährte Methode, Gebäudeautomationen zu vermeiden, die darauf angewiesen sind AWS AppConfig, da sich diese Methode ändern kann. Beachten Sie, dass Sie aus Kompatibilitätsgründen möglicherweise in future Automatisierungen

aktualisieren oder ändern müssen, die auf der aktuellen AWS AppConfig Implementierung basieren.

Das Feature-Flag Compute Optimizer -> EC2 Instances hat zusätzliche Parameter:

- allow-upscale Um das Hochskalieren von nicht optimierten Instances mit unzureichender Bereitstellung zu ermöglichen. EC2 Der Standardwert ist „false“.
- min-savings-opportunity-percentage Die Möglichkeit der automatischen Problembehebung in Prozent mit minimalen Einsparungen. Der Standardwert ist 10%

Standardkonfigurationen für die Problembehebung

Die Konfigurationen für einzelne Trusted Advisor Prüfungen werden als AWS AppConfig Flags gespeichert. Der Flag-Name stimmt mit dem Schecknamen überein. Jede Prüfkongfiguration enthält die folgenden Attribute:

- Ausführungsmodus: Legt fest, wie Trusted Remediator die Standardbehebung durchführt:
 - Automatisiert: Trusted Remediator korrigiert Ressourcen automatisch, indem es ein Dokument erstellt OpsItem, das SSM-Dokument ausführt und es nach erfolgreicher Ausführung wieder auflöst. OpsItem
 - Manuell: Ein OpsItem wird erstellt, aber das SSM-Dokument wird nicht automatisch ausgeführt. Sie überprüfen das OpsItem und führen die Behebung mithilfe des automatisierten RFC durch. Weitere Informationen finden Sie unter [Arbeiten Sie mit Behebungen in Trusted Remediator](#).
 - Bedingt: Die Wiederherstellung ist standardmäßig deaktiviert. Sie können es mithilfe von Tags für bestimmte Ressourcen aktivieren. Weitere Informationen finden Sie in den folgenden Abschnitten [Passen Sie die Problembehebung mit Ressourcen-Tags individuell an](#) und [Passen Sie die Problembehebung mit Tags zum Überschreiben von Ressourcen individuell an](#).
- Inaktiv: Es findet keine Korrektur statt und es OpsItem werden keine erstellt. Sie können den Ausführungsmodus für die Trusted Advisor Prüfung, die auf inaktiv gesetzt ist, nicht überschreiben.
- vorkonfigurierte Parameter: Geben Sie Werte für SSM-Dokumentparameter ein, die für die automatische Korrektur erforderlich sind, im Format von, getrennt durch ein Komma (Parameter=Value,). Informationen zu [Trusted Advisor von Trusted Remediator unterstützte Prüfungen](#) den unterstützten vorkonfigurierten Parametern für das zugehörige SSM-Dokument finden Sie für jede Prüfung.

- **alternative-automation-document:** Dieses Attribut hilft dabei, das vorhandene Automatisierungsdokument durch ein anderes unterstütztes Dokument zu überschreiben (falls für die jeweilige Prüfung verfügbar). Dieses Attribut ist standardmäßig nicht ausgewählt.

Note

Das **alternative-automation-document** Attribut unterstützt keine benutzerdefinierten Automatisierungsdokumente. Sie können die vorhandenen unterstützten Trusted Remediator-Automatisierungsdokumente verwenden, die unter aufgeführt sind. [Trusted Advisor von Trusted Remediator unterstützte Prüfungen](#)

Zur Überprüfung gibt es Qch7DwouX1 beispielsweise drei zugehörige SSM-Dokumente: AWSManagedServices-StopEC2Instance, und AWSManagedServices-ResizeInstanceByOneLevel. AWSManagedServices-TerminateInstance Der Wert für **alternative-automation-document** kann entweder AWSManagedServices-ResizeInstanceByOneLevel oder sein AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance ist das SSM-Standarddokument, das behoben werden muss). Qch7DwouX1

Der Wert für jedes Attribut muss den Einschränkungen dieses Attributs entsprechen.

Tip

Bevor Sie die Standardkonfigurationen für Ihre Trusted Advisor Prüfungen anwenden, empfiehlt es sich, die in den folgenden Abschnitten beschriebenen Funktionen zur Kennzeichnung von Ressourcen und zur Außerkraftsetzung von Ressourcen in Betracht zu ziehen. Die Standardkonfigurationen gelten für alle Ressourcen innerhalb des Kontos, was möglicherweise nicht in allen Fällen wünschenswert ist.

Im Folgenden finden Sie ein Beispiel für einen Konsolen-Screenshot, bei dem der Ausführungsmodus auf Manuell gesetzt ist und die Attribute den jeweiligen Einschränkungen entsprechen.

Passen Sie die Problembehebung mit Ressourcen-Tags individuell an

Mit den `manual-for-tagged-only` Attributen `automated-for-tagged-only` und in der Prüfkonfiguration können Sie Ressourcen-Tags angeben, mit denen Sie festlegen können, wie Sie einzelne Prüfungen korrigieren möchten. Es hat sich bewährt, diese Methode zu verwenden, wenn Sie ein einheitliches Behebungsverhalten auf eine Gruppe von Ressourcen anwenden müssen, die dasselbe Tag oder dieselben Tags verwenden. Im Folgenden finden Sie Beschreibungen für diese Tags:

- `automated-for-tagged-only`: Geben Sie Ressourcen-Tags (ein oder mehrere Tag-Paare, durch Kommas getrennt) für Prüfungen an, die unabhängig vom Standardausführungsmodus automatisch behoben werden sollen.
- `manual-for-tagged-only`: Geben Sie Ressourcen-Tags (ein oder mehrere Tag-Paare, durch Kommas getrennt) für Problembehebungen an, die unabhängig vom Standardausführungsmodus manuell ausgeführt werden sollen.

Wenn Sie beispielsweise die automatische Behebung für alle Ressourcen aktivieren möchten, die nicht zur Produktion gehören, und die manuelle Korrektur für Produktionsressourcen erzwingen möchten, können Sie Ihre Konfiguration wie folgt festlegen:

```
"execution-mode": "Conditional",  
"automated-for-tagged-only": "Environment=Non-Production",  
"manual-for-tagged-only": "Environment=Production",
```

Nachdem Sie die vorherigen Konfigurationen für Ihre Ressourcen eingerichtet haben, überprüfen Sie, ob das Behebungsverhalten wie folgt aussieht:

- Ressourcen, die mit 'Environment=Non-Production' gekennzeichnet sind, werden automatisch behoben.
- Ressourcen, die mit 'Environment=Production' gekennzeichnet sind, erfordern zur Behebung manuelles Eingreifen.
- Ressourcen ohne das Tag 'Environment' folgen dem Standard-Ausführungsmodus (in diesem Fall 'Bedingt'). Es werden also keine Maßnahmen für die verbleibenden Ressourcen ergriffen).

Wenn Sie weitere Unterstützung bei Ihren Konfigurationen benötigen, wenden Sie sich an Ihren Cloud-Architekten.

Passen Sie die Problembehebung mit Tags zum Überschreiben von Ressourcen individuell an

Mithilfe von Tags zum Überschreiben von Ressourcen können Sie das Behebungsverhalten für einzelne Ressourcen unabhängig von ihren Tags anpassen. Indem Sie einer Ressource ein bestimmtes Tag hinzufügen, überschreiben Sie den Standardausführungsmodus für diese Ressource und die Trusted Advisor Prüfung. Das Resource-Override-Tag hat Vorrang vor der Standardkonfiguration und den Einstellungen für das Ressourcen-Tagging. Wenn Sie also für eine Ressource, die das Resource Override-Tag verwendet, den Standardausführungsmodus auf Automatisiert, Manuell oder Bedingt festlegen, überschreibt dies den Standardausführungsmodus und alle Konfigurationen für das Ressourcen-Tagging.

Gehen Sie wie folgt vor, um den Ausführungsmodus für eine Ressource zu überschreiben:

1. Identifizieren Sie die Ressourcen, für die Sie die Behebungskonfiguration überschreiben möchten.
2. Ermitteln Trusted Advisor Sie die Scheck-ID für den Scheck, den Sie überschreiben möchten. Den Scheck IDs für unterstützte Trusted Advisor Check-ins finden Sie unter [Trusted Advisor von Trusted Remediator unterstützte Prüfungen](#).
3. Fügen Sie den Ressourcen mithilfe des Änderungstyps Tag [| Update oder Tag | Bulk-Update ein Tag](#) mit dem folgenden Schlüssel und Wert hinzu:
 - Tag-Schlüssel: TR-*Trusted Advisor check ID*-Execution-Mode (Groß- und Kleinschreibung beachten)

Ersetzen Sie es im vorherigen Beispiel Trusted Advisor check ID mit einem Tag-Schlüssel durch den eindeutigen Bezeichner des Trusted Advisor Schecks, den Sie überschreiben möchten.

- Tag-Wert: Verwenden Sie einen der folgenden Werte für den Tag-Wert:
 - Automatisiert: Trusted Remediator korrigiert automatisch die Ressource für diese Trusted Advisor Prüfung.
 - Manuell: Für die Ressource OpsItem wird eine erstellt, aber die Behebung wird nicht automatisch durchgeführt. Sie überprüfen die Problembehebung und führen sie mithilfe der automatisierten Methode durch. Weitere Informationen finden Sie unter [Arbeiten Sie mit Behebungen in Trusted Remediator](#).
 - Inaktiv: Für diese Ressource und die angegebene Trusted Advisor Prüfung wurden keine Korrektur und OpsItem Erstellung durchgeführt.

Um beispielsweise ein Amazon EBS-Volume mit der Trusted Advisor Scheck-ID automatisch zu korrigieren, DAvU99Dc4C fügen Sie dem EBS-Volume ein Tag hinzu. Der Tag-Schlüssel ist TR-DAvU99Dc4C-Execution-Mode und der Tag-Wert ist. Automated

Im Folgenden finden Sie ein Beispiel für die Konsole, in der der Abschnitt „Tags“ angezeigt wird:

Entscheidungsworkflow für den Ausführungsmodus

Es gibt mehrere Ebenen, um den Ausführungsmodus für Ihre Ressourcen und jede Trusted Advisor Prüfung zu konfigurieren. Das folgende Diagramm zeigt, wie Trusted Remediator anhand Ihrer Konfigurationen entscheidet, welcher Ausführungsmodus verwendet werden soll:

Tutorials zur Konfiguration von Problembehebungen

Die folgenden Tutorials enthalten Beispiele für die Erstellung gängiger Problembehebungen in Trusted Remediator

Korrigieren Sie alle Ressourcen manuell

In diesem Beispiel wird die manuelle Korrektur für alle Amazon EBS-Volumes mit der Trusted Advisor Scheck-ID DAv U99Dc4C (Underused Amazon EBS Volumes) konfiguriert.

Konfigurieren Sie die manuelle Korrektur für Amazon EBS-Volumes mit der Prüf-ID U99Dc4C DAv

1. Verwenden Sie die Option Remediation Configuration|Update, change type, um das Konfigurationsupdate anzufordern.
2. Legen Sie die folgenden Parameter fest:
 - CheckIds: U99Dc4C DAv
 - ExecutionMode: Manuell

Note

In einer einzigen Anfrage können mehrere Prüfungen konfiguriert werden. Fügen Sie für Prüfungen, die dieselbe Konfiguration erfordern, mehrere Prüfungen IDs in

den `CheckIdsParameter` ein. Für Prüfungen, die eine andere Konfiguration erfordern, erstellen Sie ein neues `RemediationConfigurationObjekt`.

3. Reichen Sie den RFC ein.

Korrigieren Sie alle Ressourcen automatisch, mit Ausnahme der ausgewählten Ressourcen

In diesem Beispiel wird die automatische Problembehebung für alle Amazon EBS-Volumes mit der Trusted Advisor Scheck-ID DAV U99Dc4C (Nicht ausgelastete Amazon EBS-Volumes) konfiguriert, mit Ausnahme der angegebenen Volumes, die nicht behoben werden (als Inaktiv gekennzeichnet).

Automatische Problembehebung für Amazon EBS-Volumes mit der Prüf-ID DAV U99Dc4C konfigurieren, mit Ausnahme ausgewählter inaktiver Ressourcen

1. Automatische Problembehebung für ausgewählte Amazon EBS-Volumes außer Kraft setzen:

Verwenden Sie den Änderungstyp [Tag | Update](#) oder [Tag | Bulk-Update](#), um Volumes, die von der automatischen Problembehebung ausgeschlossen werden sollen, das folgende Tag zuzuweisen:

- Schlüssel: TR- DAV U99Dc4C-Ausführungsmodus
- Wert: Inaktiv

2. Verwenden Sie den Änderungstyp `Standardisierungskonfiguration|Update`, um das Konfigurationsupdate anzufordern.

3. Legen Sie die folgenden Parameter fest:

- `CheckIds`: U99Dc4C DAV
- `ExecutionMode`: Automatisiert

4. Reichen Sie den RFC ein.

Korrigieren Sie markierte Ressourcen automatisch

In diesem Beispiel wird die automatische Problembehebung für alle Amazon EBS-Volumes mit dem Tag `Stage=NonProd` mit der Trusted Advisor Prüf-ID DAV U99Dc4C (Underused Amazon EBS Volumes) konfiguriert. Alle anderen Ressourcen ohne dieses Tag werden nicht behoben.

Automatische Problembehebung für Amazon EBS-Volumes mit dem Tag **Stage=NonProd** für die Scheck-ID U99Dc4C konfigurieren DAV

1. Verwenden Sie die Option [Remediation Configuration | Update, change type, um das Konfigurationsupdate](#) anzufordern.
2. Legen Sie die folgenden Parameter fest:
 - CheckIds: U99Dc4C DAV
 - ExecutionMode: Bedingt
 - AutomatedForTaggedOnly: {"Phase": " NonProd „}

 Note

Der für den AutomatedForTaggedOnlyParameter angegebene Wert überschreibt den zuvor konfigurierten Wert. Um vorhandene Tags beizubehalten, nehmen Sie sie in den neuen Wert auf.

3. Reichen Sie den RFC ein.

Konfiguration auf Standard zurücksetzen

In diesem Beispiel wird die bestehende automated-for-tagged-onlyKonfiguration für den Check Hs4Ma3G104 entfernt. Um die zuvor angewendete Tag-Konfiguration zu entfernen, setzen Sie den AutomatedForTaggedOnlyParameterwert auf {}.

Setzen Sie die Konfiguration für die Prüfung Hs4Ma3G104 auf die Standardkonfiguration zurück

1. Verwenden Sie den Änderungstyp [Remediation Configuration | Update](#), um das Konfigurationsupdate anzufordern.
2. Legen Sie die folgenden Parameter fest:
 - CheckIds: Hs4Ma3G104
 - ExecutionMode: Geben Sie den aktuell verwendeten Wert ein
 - AutomatedForTaggedOnly: {}
3. Reichen Sie den RFC ein.

Arbeiten Sie mit Behebungen in Trusted Remediator

Behebungen in Trusted Remediator nachverfolgen

Gehen Sie wie folgt vor, um OpsItems Behebungen nachzuverfolgen:

1. Öffnen Sie die AWS Systems Manager Konsole unter. <https://console.aws.amazon.com/systems-manager/>
2. Wählen Sie Operations Management, OpsCenter.
3. (Optional) Filtern Sie die Liste nach Quelle=Trusted Remediator, um nur Trusted Remediator OpsItems in die Liste aufzunehmen.

Im Folgenden finden Sie ein Beispiel für den OpsCenter Bildschirm, der nach Source=Trusted Remediator gefiltert wurde:

Note

Zusätzlich zur Anzeige OpsItems von können Sie die OpsCenter Behebungsprotokolle im AMS S3-Bucket einsehen. Weitere Informationen finden Sie unter [Behebungsprotokolle in Trusted Remediator](#).

Führen Sie manuelle Korrekturen in Trusted Remediator aus

Trusted Remediator erstellt vier Prüfungen, OpsItems die für die manuelle Behebung konfiguriert sind. Sie müssen diese Prüfungen überprüfen und den Behebungsprozess manuell starten.

Gehen Sie wie folgt vor OpsItem, um das manuell zu korrigieren:

1. Öffnen Sie die AWS Systems Manager Konsole unter. <https://console.aws.amazon.com/systems-manager/>
2. Wählen Sie Operations Management, OpsCenter.
3. (Optional) Filtern Sie die Liste nach Quelle=Trusted Remediator, um nur Trusted Remediator OpsItems in die Liste aufzunehmen.
4. Wählen Sie die aus OpsItem , die Sie überprüfen möchten.

5. Überprüfen Sie die Betriebsdaten von OpsItem. Die Betriebsdaten umfassen die folgenden Elemente:
- `trustedAdvisorCheckKategorie`: Die Kategorie der Trusted Advisor Scheck-ID. Zum Beispiel Fehlertoleranz
 - `trustedAdvisorCheckID`: Die eindeutige Trusted Advisor Scheck-ID.
 - `trustedAdvisorCheckMetadaten`: Die Metadaten der Ressource, einschließlich der Ressourcen-ID.
 - `trustedAdvisorCheckName`: Der Name des Trusted Advisor Schecks.
 - `trustedAdvisorCheckStatus`: Der Status der Trusted Advisor Prüfung, die für die Ressource erkannt wurde.
 - `trustedAdvisorCheckManualRemediation`: Die benutzerdefinierten Daten, die Referenzdetails für die manuelle Korrektur enthalten.
 - `ManualExecutionInput`: Ein Objekt, das Parameter definiert, für die Sie Werte ändern können, wenn Sie die manuelle Korrektur ausführen.
 - `DocumentName`: Der Name des Runbooks (SSM-Dokument).
 - `CustomizableParameters`: Parameternamen, die Sie ändern können.
 - `DefaultInput`: Ein Objekt, das Parameternamen und -werte definiert, die für die manuelle Korrektur verwendet werden sollen. Die Werte werden auf der Grundlage vorkonfigurierter Parameter aufgefüllt.
6. Gehen Sie wie folgt vor, um das OpsItem manuell zu korrigieren:
- a. Verwenden Sie [Trusted Remediator | Finding | Remediate](#) ct-1c7ch8z5phrjp (Änderungstyp)
 - b. Geben Sie Werte für die folgenden Parameter ein:
 - `DocumentName`: Muss sein `AWSManagedServices-RemediateTrustedRemediatorFinding`.
 - `Region`: Die AWS-Region, in der Form `us-east-1`.
 - `Parameter`: Geben Sie die Parameter für die manuelle Korrektur ein:
 - `OpsItemId`: Die ID des Ops-Elements.
 - `RemediationDocumentName`: Der Name des zu verwendenden SSM-Automatisierungsdokuments. Das Dokument muss dem Ops-Objekt zugeordnet sein. Wenn dem Ops-Objekt mehrere Dokumente zugeordnet sind, `DocumentName` muss das angegeben werden.

- RemediationParameters: Eine key/value Zuordnung von Parametern für die Ausführung der Automatisierung in der Form: `{\"ParameterName1\": [\"ParameterValue1\"], \"ParameterName2\": [\"ParameterValue2\"]}`. Sie können nur Parameter verwenden, die im Ops-Objekt vorhanden sind `trustedAdvisorCheckManualRemediation CustomizableParameters`. Wenn nicht angegeben, werden Parameter und Werte aus dem Ops-Element abgerufen.
- c. Wählen Sie Ausführen aus. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
- d. Überwachen Sie den Fortschritt der RFC-Ausführung.
- e. Nach Abschluss der Ausführung OpsItem ist das behoben. Wenn der RFC fehlgeschlagen ist, folgen Sie den Schritten unter [Beheben Sie Fehler bei Behebungen in Trusted Remediator](#). Wenn Sie weitere Unterstützung bei der Fehlerbehebung benötigen, wenden Sie sich an AMS.

Beheben Sie Fehler bei Behebungen in Trusted Remediator

Wenden Sie sich an AMS, wenn Sie Unterstützung bei manuellen Problembehebungen und Mängelbehebungsfehlern benötigen.

Gehen Sie wie folgt vor, um den Status und die Ergebnisse der Problembehebung einzusehen:

1. Öffnen Sie die AWS Systems Manager Konsole unter <https://console.aws.amazon.com/systems-manager/>
2. Wählen Sie Operations Management, OpsCenter.
3. (Optional) Filtern Sie die Liste nach Quelle=Trusted Remediator, um nur Trusted Remediator OpsItems in die Liste aufzunehmen.
4. Wählen Sie die aus OpsItem, die Sie überprüfen möchten.
5. Überprüfen Sie im Abschnitt Automatisierungsausführungen den Namen und den Status des Dokuments sowie die Ergebnisse.
6. Sehen Sie sich die folgenden häufigen Automatisierungsfehler an. Wenn Ihre Probleme hier nicht aufgeführt sind, wenden Sie sich an Ihren CSDM, um Unterstützung zu erhalten.

Häufige Fehler bei der Problembehebung

Unter Automatisierungsausführungen sind keine Ausführungen aufgeführt

Keine Ausführungen im Zusammenhang mit dem deuten OpsItem möglicherweise darauf hin, dass die Ausführung aufgrund falscher Parameterwerte nicht gestartet werden konnte.

Fehlerbehebungsschritte

1. Überprüfen Sie in den Betriebsdaten den `trustedAdvisorCheckAutoRemediation` Eigenschaftswert.
2. Stellen Sie sicher, dass die Werte für `DocumentName` und `Parameter` korrekt sind. Die richtigen Werte finden Sie in [Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator](#) den Einzelheiten zur Konfiguration der SSM-Parameter. Informationen zu den unterstützten Prüfungsparametern finden Sie unter [Trusted Advisor von Trusted Remediator unterstützte Prüfungen](#)
3. Stellen Sie sicher, dass die Werte im SSM-Dokument den zulässigen Mustern entsprechen. Um die Parameterdetails im Dokumentinhalt anzuzeigen, wählen Sie den Dokumentnamen im Abschnitt `Runbooks` aus.
4. Nachdem Sie die Parameter überprüft und korrigiert haben, korrigieren Sie die manuell. OpsItem Die Schritte zur Behebung finden Sie unter. [Führen Sie manuelle Korrekturen in Trusted Remediator aus](#)
5. Um zu verhindern, dass dieser Fehler erneut auftritt, stellen Sie sicher, dass Sie die Behebung mit den richtigen Parameterwerten in Ihrer Konfiguration konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator](#).

Fehlgeschlagene Ausführungen bei Automatisierungsausführungen

Behebungsdokumente enthalten mehrere Schritte, die mit der AWS-Services Ausführung verschiedener Aktionen zusammenhängen. APIs Gehen Sie wie folgt vor, um eine bestimmte Ursache für den Fehler zu ermitteln:

Fehlerbehebungsschritte

1. Um die einzelnen Ausführungsschritte anzuzeigen, wählen Sie im Abschnitt `Automatisierungsausführungen` den Link `Ausführungs-ID` aus. Im Folgenden finden Sie ein Beispiel für die Systems Manager Manager-Konsole, in der die Ausführungsschritte für eine ausgewählte Automatisierung angezeigt werden:

2. Wählen Sie den Schritt mit dem Status Fehlgeschlagen aus. Im Folgenden finden Sie Beispiele für Fehlermeldungen:

- NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist

Dieser Fehler weist darauf hin, dass in den vorkonfigurierten Parametern der Wartungskonfiguration der falsche Bucket-Name angegeben wurde.

Um diesen Fehler zu beheben, [führen Sie die Automatisierung manuell mit dem richtigen Bucket-Namen](#) aus. Um zu verhindern, dass dieses Problem erneut auftritt, [aktualisieren Sie die Wartungskonfiguration](#) mit dem richtigen Bucket-Namen.

- DB instance my-db-instance-1 is not in available status for modification.

Dieser Fehler weist darauf hin, dass die Automatisierung die erwarteten Änderungen nicht vornehmen konnte, da sich die DB-Instance in einem ungültigen Zustand befand.

Um diesen Fehler zu beheben, [führen Sie die Automatisierung manuell aus](#).

Behebungsprotokolle in Trusted Remediator

Trusted Remediator erstellt Protokolle im JSON-Format und lädt sie auf Amazon Simple Storage Service hoch. Die Protokolldateien werden in einen von AMS erstellten und benannten S3-Bucket hochgeladen. `ams-trusted-remediator-{your-account-id}-logs` AMS erstellt den S3-Bucket im Delegated Administrator-Konto. Sie können die Protokolldateien importieren, QuickSight um benutzerdefinierte Behebungsberichte zu erstellen.

Protokoll der Behebungselemente

Trusted Remediator erstellt das `Remediation item log`, wenn eine Behebung OpsItem erstellt wird. Dieses Protokoll enthält manuelle und automatisierte OpsItem Problembehebungen. OpsItem Sie können den `verwendenRemediation item log`, um den Überblick über alle Behebungen nachzuverfolgen.

Speicherort des Korrekturprotokolls für Compute Optimizer Optimizer-Empfehlungen

`s3://ams-trusted-remediator-delegated-administrator-account-id-logs/
compute_optimizer_remediation_items/remediation creation time in yyyy-mm-`

dd format/10 digits epoch time or unix timestamp-Trusted Advisor check ID-Resource ID.json

Speicherort für das Protokoll des Behebungselements für Prüfungen Trusted Advisor

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/remediation_items/*remediation creation time in yyyy-mm-dd format/10 digits epoch time or unix timestamp-Trusted Advisor check ID- Resource ID.json*

URL der Beispieldatei für das Behebungselement

s3:///ams-trusted-remediator-*111122223333*-logs/remediation_items/*2023-02-06/1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json*

Protokollformat für Compute Optimizer Remediation-Elemente

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Protokollformat für das Behebungselement

```
{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}
```

Compute Optimizer Remediation-Artikelprotokollformat, Beispielinhalt

```
{
```

```

"AccountID": "123456789012",
"ComputeOptimizerCheckID": "compute-optimizer-ebs",
"ComputeOptimizerCheckName": "EBS volumes",
"ResourceID": "vol-1235589366f77aca7",
"RemediationTime": 1755044783,
"ExecutionMode": "Manual",
"OpsItemID": "oi-b8888b38fe78"
}

```

Trusted Advisor Protokollformat des Behebungselements, Beispielinhalt

```

{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}

```

Protokoll zur Ausführung automatisierter Problembehebungen, Compute Optimizer und Trusted Advisor

Trusted Remediator erstellt das `Automated remediation execution log`, wenn ein automatisierter SSM-Dokumentenlauf abgeschlossen ist. Dieses Protokoll enthält SSM-Ausführungsdetails nur für die automatisierte Problembehebung. OpsItem Sie können diese Protokolldatei verwenden, um automatisierte Problembehebungen nachzuverfolgen.

Compute Optimizer — Speicherort des automatisierten Behebungsprotokolls

```

s3://ams-trusted-remediator-delegated-administrator-account-id-logs//
remediation_executions/remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Compute Optimizer recommendation
ID.json

```

Trusted Advisor Speicherort des automatisierten Behebungsprotokolls

```

s3://ams-trusted-remediator-delegated-administrator-account-id-logs//
remediation_executions/remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource
ID.json

```


Compute Optimizer — Beispiel für den Speicherort eines automatisierten Behebungsprotokolls

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2025-06-26/1750908858-123456789012-compute-  
optimizer-ec2-i-1235173471d2cd789.json
```

Trusted Advisor Beispiel für den Speicherort des automatisierten Behebungsprotokolls

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-  
vol-00bd8965660b4c16d.json
```

Format eines Beispielinhalts im Format eines automatisierten Behebungsprotokolls

```
{  
  "OpsItemID": "oi-767c77e05301",  
  "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",  
  "SSMExecutionStatus": "Success"}
```

Bewährte Methoden in Trusted Remediator

Im Folgenden finden Sie bewährte Methoden, die Ihnen bei der Verwendung von Trusted Remediator helfen sollen:

- Wenn Sie sich über die Ergebnisse der Korrektur nicht sicher sind, beginnen Sie mit dem manuellen Ausführungsmodus. Manchmal kann die automatische Ausführung von Korrekturen von Anfang an zu unerwarteten Ergebnissen führen.
- Führen Sie eine wöchentliche Überprüfung der Abhilfemaßnahmen durch OpsItems , um Einblicke in die Trusted Remediator-Ergebnisse zu erhalten.
- Mitgliedskonten erben die Konfigurationen des delegierten Administratorkontos. Daher ist es wichtig, die Konten so zu strukturieren, dass Sie mehrere Konten mit denselben Konfigurationen verwalten können. Mithilfe von Tags können Sie Ressourcen von der Standardkonfiguration ausnehmen.

Vertrauenswürdiger Remediator FAQs

Im Folgenden finden Sie häufig gestellte Fragen zu Trusted Remediator:

Was ist Trusted Remediator und welche Vorteile habe ich davon?

Wenn Compute Optimizer eine Nichteinhaltung feststellt, Trusted Advisor oder eine Empfehlung von Compute Optimizer ausgibt, reagiert Trusted Remediator gemäß Ihren angegebenen Einstellungen, indem es entweder Abhilfemaßnahmen durchführt, die Genehmigung durch manuelle Korrekturen einholt oder die Abhilfemaßnahmen in Ihrem bevorstehenden Monthly Business Review (MBR) meldet. Die Behebung erfolgt zu Ihrem bevorzugten Zeitpunkt oder Zeitplan. Trusted Remediator bietet Ihnen die Möglichkeit, Prüfungen selbst zu verwalten und entsprechend zu reagieren. Sie haben die Flexibilität, Trusted Advisor Prüfungen einzeln oder in großen Mengen zu konfigurieren und zu korrigieren. Mit einer Bibliothek getesteter Dokumente zur Problembehebung erhöht AMS Ihre Konten ständig, indem es Sicherheitsüberprüfungen durchführt und bewährte Verfahren befolgt. AWS Sie werden nur benachrichtigt, wenn Sie dies in Ihrer Konfiguration angeben. AMS-Benutzer können sich ohne zusätzliche Kosten für Trusted Remediator anmelden.

In welcher Beziehung steht Trusted Remediator zu anderen und wie funktioniert Trusted Remediator mit anderen zusammen? AWS-Services

Im Rahmen Ihres bestehenden Enterprise Support-Plans haben Sie Zugriff auf Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen. Trusted Remediator lässt sich in Trusted Advisor Compute Optimizer integrieren, um bestehende AMS-Automatisierungsfunktionen zu nutzen. Insbesondere verwendet AMS AWS Systems Manager Automatisierungsdokumente (Runbooks) für automatisierte Problembehebungen. AWS AppConfig wird verwendet, um die Behebungsworkflows zu konfigurieren. Sie können alle aktuellen und vergangenen Behebungen über den Systems Manager OpsCenter einsehen. Die Behebungsprotokolle werden in einem Amazon S3 S3-Bucket gespeichert. Sie können die Protokolle verwenden, um benutzerdefinierte Berichts-Dashboards zu importieren und darin zu erstellen. QuickSight

Wer konfiguriert die Abhilfemaßnahmen?

Sie sind der Eigentümer der Konfigurationen in Ihrem Konto. Die Verwaltung Ihrer Konfigurationen liegt in Ihrer Verantwortung. Sie können sich auch an AMS wenden, wenn es um Konfigurationsänderungen, Support und manuelle Problembehebungen sowie um Problembehebungsfehler geht.

Wie installiere ich Dokumente zur SSM-Automatisierung?

Dokumente zur SSM-Automatisierung werden automatisch an integrierte AMS-Konten weitergegeben.

Werden AMS-eigene Ressourcen ebenfalls berichtigt?

AMS-eigene Ressourcen werden von Trusted Remediator nicht gekennzeichnet. Trusted Remediator konzentriert sich nur auf Ihre Ressourcen.

In welcher AWS-Regionen Version ist Trusted Remediator verfügbar und wer kann ihn verwenden?

Trusted Remediator ist für AMS Advanced-Kunden verfügbar. Eine aktuelle Liste der Support-Regionen finden Sie unter [AWS-Services Nach Regionen geordnet](#).

Wird Trusted Remediator zu einer Verlagerung von Ressourcen führen?

Da SSM-Automatisierungsdokumente Ressourcen direkt über die AWS API aktualisieren, kann es zu einer Verlagerung von Ressourcen kommen. Sie können Tags verwenden, um Ressourcen zu trennen, die mit Ihren vorhandenen Paketen erstellt wurden. CI/CD Sie können Trusted Remediator so konfigurieren, dass die markierten Ressourcen ignoriert werden, während Ihre anderen Ressourcen trotzdem repariert werden.

Wie pausiere oder beende ich Trusted Remediator?

Verwenden Sie den Änderungstyp [Verwaltung | Trusted Remediator | Status | Aktivieren oder Deaktivieren](#), um den Trusted Remediator-Dienst zu beenden. Verwenden Sie denselben Änderungstyp, um Trusted Remediator erneut zu aktivieren.

Wie kann ich Prüfungen korrigieren, die von Trusted Remediator nicht unterstützt werden?

Sie können AMS weiterhin über Operations On Demand (OOD) kontaktieren, wenn Prüfungen nicht unterstützt werden. AMS unterstützt Sie bei der Behebung dieser Prüfungen. Weitere Informationen finden Sie unter [Operations On Demand](#).

Welche Ressourcen stellt Trusted Remediator für Ihre Konten bereit?

Trusted Remediator stellt die folgenden Ressourcen im delegierten Administratorkonto von Trusted Remediator bereit:

- Ein Amazon S3 S3-Bucket mit dem Namen `ams-trusted-remediator-{your-account-id}-logs`. Trusted Remediator erstellt den `Remediation item log` im JSON-Format, wenn eine Problembehebung erstellt OpsItem wird, und lädt die Protokolldateien in diesen Bucket hoch.
- Eine AWS AppConfig Anwendung zur Speicherung der Behebungsconfigurationen für unterstützte Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen.

Trusted Remediator stellt keine Ressourcen im Trusted Remediator-Mitgliedskonto bereit.

Verwaltung von Protokollen

Themen

- [Was ist Protokollverwaltung?](#)
- [So funktioniert die AMS-Protokollierung](#)
- [Zugriff auf Ihre Logs](#)
- [Anpassung Ihrer Log-Konfiguration](#)

Das AMS-Protokollmanagement sammelt, aggregiert und kontrolliert die Aufbewahrung der Protokolle aus dem verwalteten Konto. AWS Die Protokollverwaltung fasst Protokolle von EC2 Amazon-Instances und AWS Ressourcen, die in Ihrem Konto bereitgestellt werden, in CloudWatch Logs zusammen. Die vollständige Liste der Dienste, von denen derzeit Protokolle aggregiert werden, finden Sie unter. [Aggregierte AMS-Serviceprotokolle](#)

Was ist Protokollverwaltung?

Protokollmanagement ist der Prozess des Umgangs mit Protokollereignissen, die von Instances, Anwendungen und AWS-Services generiert werden. Diese Funktion definiert, wie AMS die in Ihrem verwalteten AWS-Konto generierten Protokollereignisse verarbeitet, speichert und rotiert. Infrastrukturprotokolle werden bei der Behebung von Vorfällen und zur Unterstützung von Systemprüfungen verwendet.

So funktioniert die AMS-Protokollierung

Die Protokollverwaltung von AMS Single Account landing zone (SALZ) verwendet eine Vielzahl vorinstallierter Agenten und Tools, die beim Onboarding oder der Bereitstellung von Instanzen und Anwendungen implementiert werden.

Die Protokollierung wird während des Kontoeinführungsprozesses und beim Start eines Stacks konfiguriert.

AMS-Logs landing zone mehrere Konten (MALZ), die von Instances und AWS-Services erstellt wurden, sind in CloudWatch Logs oder Amazon Simple Storage Service (Amazon S3) für jedes von AMS verwaltete Konto verfügbar. Die AMS-Landezone mit mehreren Konten bietet ein zentrales Logging-Konto, das als zentrale Aggregationsstelle für einige Logs dient, die von einzelnen Anwendungskonten erstellt wurden.

In den Tabellen in den [Zugriff auf Ihre Logs](#) Unterabschnitten wird beschrieben, welche Protokolle in den einzelnen Konten und welche im zentralen Logging-Konto verfügbar sind.

Zugriff auf Ihre Logs

Um auf Ihre Protokolle zugreifen zu können, stellen Sie sicher, dass Sie über eine der erforderlichen IAM-Rollen verfügen und sich in Ihrem AMS-Konto befinden. Navigieren Sie dann zu dem angezeigten Verzeichnis.

Multi-Account Landing Zone (MALZ)

Stellt fünf Standard-IAM-Rollen bereit, von denen jede den Zugriff auf alle Logs in Ihrem Konto ermöglicht (allen ist das Präfix vorangestellt): `AWSManagedServices`

- `AdminRole`
- `CaseRole`
- `ChangeManagementRole`
- `ReadOnlyRole`
- `SecurityOpsRole`

Der Zugriff auf diese Rollen wird über einen Verbund konfiguriert, wobei jede Rolle einer Gruppe innerhalb Ihrer Active Directory-Domäne zugeordnet wird.

Weitere Informationen zu diesen Rollen finden Sie unter [IAM-Benutzerrolle in AMS](#).

Single-Account Landing Zone (SALZ)

Die Standardeinstellung `Customer_ReadOnly_Role` für die landing zone für Einzelkonten von AMS ermöglicht Ihnen den Zugriff auf alle Logs in Ihrem Konto. Der Zugriff auf die Protokolle wird mithilfe von AWS Identity and Access Management (IAM) -Rollen gesteuert, die Active Directory-Gruppen zugeordnet sind.

Aggregierte AMS-Serviceprotokolle

Jeder AWS Service protokolliert sich entweder in CloudWatch Logs oder an einem bestimmten Ort in einem Amazon S3 S3-Bucket.

 Note

Sofern nicht ausdrücklich angegeben, sind alle Protokollspeicherorte lokal für das Konto, das die Protokolle generiert hat, und werden nicht im zentralen Logging-Konto zusammengefasst. Um die CloudTrail Standard-AMS-Trailnamen in den Konten SALZ und MALZ zu finden, gehen Sie zur AWS-Konsole für CloudTrail und dann zur Seite Trails und suchen Sie nach AMS. Da AMS-Ressourcen Tags haben, können Sie die Trails auf diese Weise finden. Beispiel für ein CloudTrail AMS-Tag:

```
Environment    AMSInfrastructure
```

Um auf Ihre Protokolle zugreifen zu können, stellen Sie sicher, dass Sie über eine der erforderlichen IAM-Rollen verfügen und sich in Ihrem AMS-Konto befinden. Navigieren Sie dann zu dem angezeigten Verzeichnis.

Multi-Account Landing Zone

Aggregierte Serviceprotokolle für die AMS-Landezone mit mehreren Konten

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
1	Amazon Aurora	Allgemeine, langsame Abfragen und Fehlerprotokolle.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	AWS CloudFormation (CFN)	Nur Protokollierung von API-Aufrufen.	AWS CloudFormation API-Aufrufe werden über dokumentiert CloudTrail, das seine Protokolle an den sendet CloudWatch LogGroup und die Protokolle dann mit einem S3-Bucket synchronisiert. Protokolle werden standardmäßig für 14 Tage im CloudWatch LogGroup und auf unbestimmte Zeit im S3-Bucket aufbewahrt.

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
			CloudWatch LogGroup://Landing-Zone-Logs CloudTrail S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs-ams-a {} -log-management- {} <i>account_ID region</i> Pfad://{}//AWSLogs<i>account_ID</i> CloudTrail
3	Amazon CloudFront (CloudFront)	Protokollierung von Benutzeranfragen. CloudFront Die Protokollierung muss explizit aktiviert werden. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren .	S3-Bucket: aws-a {<i>account_ID</i> } -log-management- {} <i>region</i> Pfad: AWS/RedShift/{} <i>CloudFront distribution ID</i>
4	Amazon CloudWatch (CloudWatch)	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Pfad:/AWSLogs/{<i>account_ID</i> }/CloudTrail/
5	Amazon Elastic Block Store (Amazon EBS)	Der EBS-Dienst erstellt keine Protokolle.	Nicht zutreffend

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
6	Amazon Elastic Compute Cloud (Amazon EC2)	System- und Anwendungsprotokolle. Weitere Informationen finden Sie unter Amazon Elastic Compute Cloud (Amazon EC2) — Protokolle auf Systemebene.	CloudWatch Protokolle:/{ <i>instance ID</i> }
7	Amazon Elastic File System (Amazon EFS)	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Pfad:/AWSLogs/{<i>account_ID</i> }/CloudTrail/

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
8	Elastic Load Balancing (ELB)	Zugriffs- und Fehlerprotokolleinträge. Elastic Load Balancer protokollieren alle an sie gesendeten Anfragen, einschließlich Anfragen, die nicht an Back-End-Instances weitergeleitet werden. Wenn ein Client beispielsweise eine falsch formatierte Anfrage sendet oder es keine fehlerfreien Instances gibt, die darauf antworten könnten, wird die Anfrage trotzdem protokolliert. Weitere Informationen zu Elastic Load Balancing Logeinträgen finden Sie unter • Classic Load Balancers: Zugriff auf Protokolleinträge. • Application Load Balancers: Zugriff auf Protokolleinträge. • Network Load Balancers: Zugriffsprotokolleinträge.	API-Aufrufprotokolle: CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Pfad:/AWSLogs/{<i>account_ID</i> }/CloudTrail/ Zugriffsprotokolle: S3-Bucket: mc-a {<i>account_ID</i> } -logs {} <i>region</i> Pfad: aws/elbaccess
9	Amazon OpenSearch Service (OpenSearch Dienst)	Service-Fehlerprotokolle. Sie müssen die OpenSearch Protokollierung explizit aktivieren. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren	CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Pfad:/AWSLogs/{<i>account_ID</i> }/CloudTrail/

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
10	Amazon ElastiCache	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup://CloudTrail/Landing-Zone-Logs
11	Amazon GuardDuty		S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} - {} <i>account_ID region</i>
12	Amazon Inspector		Pfad:/AWSLogs/{ <i>account_ID</i> }/ CloudTrail/
13	Amazon Macie		
14	Amazon Redshift	Verbindungs-, Benutzer- und Aktivitätsprotokolle. Die Protokollierung ist standardmäßig aktiviert, wenn Sie Ihren Redshift-Cluster erstellen, indem Sie den Create Redshift Cluster CT (ct-1malj7snzxrkr) aufrufen. Weitere Informationen finden Sie unter Datenbank-Auditprotokollierung.	S3-Bucket: ams-a {<i>account_ID</i> } -log-management- {} <i>region</i> Pfad: /AWS//{} RedShift <i>CloudFront Distribution ID</i>

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
15	Amazon Relational Database Service (RDS)	Für den Datenbanktyp spezifische Protokolle. Sie müssen die RDS-Protokollierung explizit aktivieren. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren Sie können nur über eine gespeicherte Prozedur auf MSSQL-Protokolle zugreifen. Weitere Informationen finden Sie unter Archivieren von Protokolldateien.	CloudWatch LogGroup: /aws/rds/ (<i>instanceid</i>)/{/ <i>cluster database_name</i> <i>log_name</i>

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
16	Amazon S3 (S3)	Bucket-Zugriffsprotokolle. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage, z. B. den Anforderer, den Bucket-Namen, die Anforderungszeit, die Anforderungsaktion, den Antwortstatus und den Fehlercode (falls vorhanden). Die Zugriffsprotokollierinformationen können für Sicherheits- und Zugriffsüberprüfungen nützlich sein. Außerdem erfahren Sie damit mehr über Ihren Kundenstamm und erhalten einen Überblick über Ihre Amazon-S3-Rechnung. Weitere Informationen zu S3-Zugriffsprotokolleinträgen finden Sie unter Format des S3-Serverzugriffsprotokolls.	S3-Bucket: mc-a {<i>account_ID</i>} -log-management- {<i>region</i>} Pfad: /aws/s3access/ {<i>bucket_name</i>} S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-s3-access-logs- {<i>region</i>} - {<i>account_ID</i>} {<i>region</i>} Pfad: /
17	Amazon Simple Email Service (SES)	SES-API-Dienstanrufe.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {<i>region</i>} - {<i>account_ID</i>} {<i>region</i>} Pfad: /AWSLogs/{<i>account_ID</i>} /CloudTrail/
18	Amazon Virtual Private Cloud (VPC)	VPC-Flussdaten (Informationen über den IP-Verkehr zu und von den Netzwerkschnittstellen Ihrer VPC).	CloudWatch LogGroup: /aws/vpcflow/ {<i>VPC_ID</i>}

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
19	Auto Scaling	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs
20	AWS Certificate Manager		S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Pfad:/AWSLogs/{<i>account_ID</i> }/CloudTrail/
21	AWS CodeDeploy	Instanzspezifische Bereitstellungsprotokolle.	Auf Instanz
22	AWS Config	AWS Config API-Serviceaufrufen.	CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Pfad:/AWSLogs/{<i>account_ID</i> }/CloudTrail/
		Änderungen der Ressourcenkonfiguration, wie sie von AWS Config verfolgt werden.	S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {} <i>account_ID</i> } - {} <i>region</i> Pfad:/AWSLogs/{<i>account_ID</i> }/Config/
23	AWS Database Migration Service	Protokolle zur Datenbankmigration . Weitere Informationen finden Sie unter Einführung in die Protokollierung in AWS Database Migration Service.	Konsole für die Datenbankmigration

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
24	AWS Direct Connect (DX)	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs
25	AWS-Gletscher		S3-Bucket [im zentralen Logging-Konto]: aws-landing-zone-logs - {}
26	AWS IAM (IAM)		- {} <i>account_ID region</i>
27	AWS Key Management Service		Pfad:/AWSLogs/{ <i>account_ID</i> }/CloudTrail/
28	AWS-Managementkonsole (Konsole oder AWS-Konsole)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Single-Account Landing Zone

Aggregierte Serviceprotokolle für die AMS-Landezone mit einem Konto

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
1	Amazon Aurora	Allgemeine, langsame Abfragen und Fehlerprotokolle.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	Amazon CloudFormation (CloudFor	Nur Protokollierung von API-Aufrufen.	CloudFormation API-Aufrufe werden über dokumentiert CloudTrail, das seine Protokoll

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
	mation oder CFN)		e an den sendet CloudWatch LogGroup und die Protokolle dann mit einem S3-Bucket synchronisiert. CloudWatch LogGroup: /aws/ams/cloudtrail S3-Bucket: <code>ams-a {<i>account_ID</i>} -log-management- {<i>region</i>}</code>
3	Amazon CloudFront (CloudFront)	Protokollierung von Benutzeranfragen. Sie müssen die CloudFront Protokollierung explizit aktivieren. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren	S3-Bucket: <code>ams-a {<i>account_ID</i>} -log-management- {<i>region</i>}</code> Pfad: <code>AWS/RedShift/{<i>CloudFront_distribution_ID</i>}</code>
4	Amazon CloudWatch (CloudWatch)	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	Der EBS-Dienst erstellt keine Protokolle.	Nicht zutreffend
6	Amazon Elastic Compute Cloud (EC2)	System- und Anwendungsprotokolle. Weitere Informationen finden Sie unter Amazon Elastic Compute Cloud (Amazon EC2) — Protokolle auf Systemebene.	CloudWatch Protokolle: / <code>{<i>instance_ID</i>}</code>

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
7	Amazon Elastic File System (Amazon EFS)	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup: /aws/ams/cloudtrail
8	Elastic Load Balancing (ELB)	Zugriffs- und Fehlerprotokolleinträge. Elastic Load Balancer protokollieren alle an sie gesendeten Anfragen, einschließlich Anfragen, die nicht an Back-End-Instances weitergeleitet werden. Wenn ein Client beispielsweise eine falsch formatierte Anfrage sendet oder es keine fehlerfreien Instances gibt, die darauf antworten könnten, wird die Anfrage trotzdem protokolliert. Weitere Informationen zu Elastic Load Balancer-Logeinträgen finden Sie unter • Classic Load Balancers: Logeinträge für den Zugriff. • Application Load Balancers: Zugriff auf Protokolleinträge. • Network Load Balancers: Zugriffsprotokolleinträge.	CloudWatch LogGroup: /aws/ams/cloudtrail S3-Bucket: mc-a {<i>account_ID</i>} -logs- {} <i>region</i> Pfad: aws/elbaccess

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
9	Amazon OpenSearch Service (OpenSearch Dienst)	Service-Fehlerprotokolle. Sie müssen die OpenSearch Protokollierung explizit aktivieren. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren	CloudWatch LogGroup: /aws/ams/ cloudtrail
10	Amazon ElastiCache	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup: /aws/ams/ cloudtrail
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Verbindungs-, Benutzer- und Aktivitätsprotokolle. Die Protokollierung ist standardmäßig aktiviert, wenn Sie Ihren Redshift-Cluster erstellen, indem Sie den Create Redshift Cluster CT (ct-1malj7snzxrkr) aufrufen. Weitere Informationen finden Sie unter Datenbank-Auditprotokollierung.	S3-Bucket: <code>ams-a {account_ID } -log-management- {region}</code> Pfad: <code>/AWS/{ } RedShift CloudFront_Distribution_ID</code>

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
15	Amazon Relational Database Service (RDS)	Für den Datenbanktyp spezifische Protokolle. Die RDS-Protokollierung muss explizit aktiviert werden. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren Sie können nur über eine gespeicherte Prozedur auf MSSQL-Protokolle zugreifen. Weitere Informationen finden Sie unter Archivieren von Protokolldateien.	CloudWatch LogGroup: /aws/rds/ (Instanz Cluster)/{Datenbankname}/{Protokollname}

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
16	Amazon S3 (S3)	Bucket-Zugriffsprotokolle. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanforderung, z. B.: Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode (falls vorhanden). Informationen zum Zugriffsprotokoll können bei Sicherheits- und Zugriffsprüfungen nützlich sein. Sie können Ihnen auch dabei helfen, mehr über Ihren Kundenstamm zu erfahren und Ihre Amazon S3 S3-Rechnung zu verstehen. Weitere Informationen zu S3-Zugriffsprotokolleinträgen finden Sie unter Format des S3-Serverzugriffsprotokolls.	S3-Bucket: mc-a {<i>account_ID</i> } -log-management- { <i>region</i> Pfad: /aws/s3access/ { <i>bucket_name</i>
17	Amazon Simple Email Service (SES)	SES-API-Dienstanrufe.	CloudWatch LogGroup: /aws/ams/cloudtrail S3-Bucket: ams-a {<i>account_ID</i> } -log-management- { <i>region</i> Pfad: AWS/CloudTrail/AWSLogs /{}/{ <i>account_ID</i> } CloudTrail <i>region</i>
18	Amazon Virtual Private Cloud (VPC)	VPC-Flussdaten (Informationen über den IP-Verkehr zu und von den Netzwerkschnittstellen Ihrer VPC).	CloudWatch LogGroup: /aws/vpcflow/ {vpc_id}

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
19	Auto Scaling	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	Instanzspezifische Bereitstellungsprotokolle.	Auf einer Instanz
22	AWS Config	AWS Config API-Serviceaufrufen.	CloudWatch LogGroup: /aws/ams/cloudtrail S3-Bucket: <code>ams-a {account_ID} -log-management- {region}</code> Pfad: <code>AWS/CloudTrail/AWSLogs/{}/{account_ID} CloudTrail region</code>
23	AWS Database Migration Service	Datenbankmigrationsprotokolle. Weitere Informationen finden Sie unter Einführung in die Protokollverwaltung in AWS Database Migration Service .	Konsole für die Datenbankmigration
24	AWS Direct Connect (DX)	Nur Protokollierung von API-Aufrufen.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS-Gletscher		
26	AWS IAM (IAM)		
27	AWS Key Management Service		

	Service-Name	Einzelheiten protokollieren	Speicherort protokollieren
28	AWS-Managementkonsole (Konsole oder AWS-Konsole)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Protokolle für gemeinsame Dienste von AMS

In der folgenden Tabelle werden die Protokolle und der Speicherort der Protokolle für die AMS Shared Services in Ihrem Konto beschrieben.

Um auf Ihre Protokolle zugreifen zu können, stellen Sie sicher, dass Sie über eine der erforderlichen IAM-Rollen verfügen und sich in Ihrem AMS-Konto befinden. Navigieren Sie dann zu dem angezeigten Verzeichnis.

AMS-Landingzone für ein einzelnes Konto Shared Services Logging

	Name des gemeinsamen Dienstes	Einzelheiten protokollieren	Speicherort protokollieren
1	Bastion-Hosts	Informationen zu Benutzern , die auf den Bastion-Host zugreifen.	Linux-Bastionen: CloudWatch Protokolle:/{Instanz-ID}/var/log/secure CloudWatch Protokolle:/{Instanz-ID}/var/log/audit/audit.log Windows-Bastionen:

	Name des gemeinsamen Dienstes	Einzelheiten protokollieren	Speicherort protokollieren
			CloudWatch Protokolle:/{Instanz-ID}/SecurityEventLog
2	Hosts für die Verwaltung	Ausgabe von Skripten, die bei automatisierten Zugriffsverwaltungsaktionen innerhalb des Kontos helfen.	CloudWatch Protokolle:/{Instanz-ID}/ApplicationEventLog
4	EPS-Hosts (DSM)	Informationen zur Registrierung von Instances auf der Deep Security Management-Plattform.	CloudWatch Protokolle:/{Instanz-ID}/.log var/log/DSM
5	Verzeichnisdienste	Informationen zur Kontoanmeldung, zur Kontoverwaltung, zur detaillierten Nachverfolgung, zum Objektzugriff, zur Änderung der Richtlinien und zur Nutzung von Rechten innerhalb des Kontoverzeichnisses. Sie müssen die Verzeichnisdienste-Protokollierung explizit aktivieren. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren.	CloudWatch Protokolle: /aws/directoryservice/ {Verzeichnis-ID} — {Verzeichnis-DNS-Name}

	Name des gemeinsamen Dienstes	Einzelheiten protokollieren	Speicherort protokollieren
6	Lambdas	Ausgabe verschiedener Lambdas, die bei automatisierten Betriebsaktionen innerhalb des Kontos helfen.	CloudWatch Protokolle: /aws/lambda/ {Lambda-Name}

AMS-Landingzone für mehrere Konten Shared Services Logging

	Name des gemeinsamen Dienstes	Einzelheiten protokollieren	Speicherort protokollieren
1	Bastionen	Ausgabe von Instanzanmeldungen und Authentifizierungsfehlern.	Linux CloudWatch Bastions-Protokolle:/{ <i>instance_ID</i> }/log var/log/secure CloudWatch Windows-Bastions-Protokolle:/{ <i>instance_ID</i> }/SecurityEventLog
2	Hosts für die Verwaltung	Ausgabe von Skripten, die bei automatisierten Zugriffsverwaltungsaktionen innerhalb des Kontos helfen.	CloudWatch Protokolle:/ { <i>instance_ID</i> }/ApplicationEventLog
3	EPS-Hosts (DSM)	Informationen zur Registrierung von Instances auf der Deep Security Management-Plattform.	CloudWatch Protokolle:/{ <i>instance_ID</i> }/log var/log/DSM
4	Verzeichnisdienste	Informationen zur Kontoanmeldung, zur Kontoverwaltung, zur detaillierten Nachverfolgung, zum Objektzugriff, zur	CloudWatch Protokolle: /aws/directoryservice/ { } - { } <i>directory_ID</i> <i>directory_DNS_name</i>

	Name des gemeinsamen Dienstes	Einzelheiten protokollieren	Speicherort protokollieren
		Änderung der Richtlinien und zur Nutzung von Rechten innerhalb des Kontoverzeichnisses. Sie müssen die Verzeichnisdienste-Protokollierung explizit aktivieren. Weitere Informationen finden Sie unter Protokollierung für unterstützte Dienste aktivieren.	
5	Lambdas	Ausgabe verschiedener Lambdas, die bei automatisierten Betriebsaktionen innerhalb des Kontos helfen.	CloudWatch Protokolle: /aws/lambda/ { } <i>Lambda_name</i>

Amazon Elastic Compute Cloud (Amazon EC2) — Protokolle auf Systemebene

Instance-Logs werden von einem CloudWatch Logs-Agenten erfasst, der auf der Instance ausgeführt wird. Auf sie kann über eine CloudWatch Log-Gruppe mit dem gleichen Namen wie die Instance zugegriffen werden. Wenn die Instanz-ID beispielsweise i-0123456789abcdef0 lautet und der Name der Protokolldatei lautet `/var/log/messages`, the Log Group would be i-0123456789abcdef0 and the Log Stream `/var/log/messages`

Siehe auch [Aggregierte AMS-Serviceprotokolle](#).

Um auf Ihre Logs zugreifen zu können, stellen Sie sicher, dass Sie über eine der erforderlichen IAM-Rollen verfügen und sich in Ihrem AMS-Konto befinden. Navigieren Sie dann zu dem angezeigten Verzeichnis.

 Note

Die folgenden Protokolle werden standardmäßig gesammelt.

Amazon Linux//Red Hat Linux//Centos Linux//Ubuntu//SUSE Linux

Protokolldatei//Protokollstream

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

 Note

Informationen zum Zugriff auf Protokolle für Amazon Linux 2023 finden Sie unter [Warum fehlen im Verzeichnis /var/log Protokolle in meiner EC2 Amazon Linux 2023-Instance?](#)

Windows

Protokolldatei//Protokollstream

SecurityEventLog

```
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

Integration mit Splunk

AMS unterstützt AWS Lambda Lambda-basierte Push-to-Customer-Log-Analyseservices wie Splunk.

AMS nutzt das Splunk-Add-on für Amazon Web Services, mit dem AWS-Daten zu Splunk gestreamt werden können. [Weitere Informationen finden Sie unter Hardware- und Softwareanforderungen.](#)

Weitere Informationen finden Sie in diesem Splunk-Blogbeitrag [So streamen Sie CloudWatch AWS-Logs nach Splunk \(Hinweis: Es ist einfacher als Sie denken\)](#). Da das CloudWatch Log-Streaming für AMS-Kunden standardmäßig aktiviert ist und AMS die AWS-Lambda-Funktion für Sie konfiguriert, müssen Sie jedoch die Splunk HTTP Event Collector (HEC) -Eingabe konfigurieren und eine Anfrage für die zusätzliche Funktionalität an AMS senden.

So könnten die Dateneingabeeinstellungen aussehen:

Anpassung Ihrer Log-Konfiguration

Sie können die Aufbewahrung von Protokolldaten für CloudWatch Protokolle ändern und die Protokollierung für zusätzliche AWS-Services aktivieren.

Änderung der CloudWatch Protokollspeicherung

Sie können die Einstellung für die Aufbewahrung von Protokolldaten für CloudWatch Protokolle ändern. Standardmäßig werden Protokolle unbegrenzt aufbewahrt und laufen nicht ab. Sie können die Aufbewahrungsrichtlinie für jede Protokollgruppe anpassen und Protokolle entweder unbegrenzt speichern oder einen Aufbewahrungszeitraum zwischen 10 Jahren und einem Tag auswählen. Die zulässige Mindestaufbewahrungsdauer in AMS finden Sie im Dokument AMS Technical Standards,

das über AWS Artifact verfügbar ist. Um auf AWS Artifact zuzugreifen, wenden Sie sich an Ihren CSDM, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

Die Funktion zur Aufbewahrung von CloudWatch Protokollen löscht die Protokollereignisse in einem Stream auf der Grundlage der Aufbewahrungsrichtlinie. Protokollstreams oder Protokollgruppen werden nicht gelöscht. Allgemeine Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch [Was ist Amazon CloudWatch Logs?](#) .

Informationen zum Anpassen des Aufbewahrungszeitraums für Protokolle und weitere Informationen finden Sie unter [Ändern der Aufbewahrung von Protokolldaten in CloudWatch Protokollen](#).

Protokollierung für unterstützte Dienste aktivieren

Bei einigen Diensten ist die Protokollierung standardmäßig nicht aktiviert und eine ausdrückliche Aktivierung ist erforderlich.

Um die Protokollierung für CloudFront, OpenSearch, Amazon RDS und Route53 zu aktivieren, reichen Sie einen RFC an Management | Other | Other | Create change type (ct-1e1xtak34nx76) mit den folgenden Werten ein und ersetzen Sie sie gegebenenfalls: *variables*

Subject: Enable logging for *SERVICE_NAME*
Description: Service ARN: *SERVICE_ARN*

Sicherheitsmanagement

Das Sicherheitsmanagement von AWS Managed Services (AMS) ist der Prozess, mit dem AMS die Vermögenswerte einer Organisation identifiziert und Richtlinien und Verfahren zum Schutz dieser Vermögenswerte implementiert.

Note

AMS verfügt jetzt über einen Änderungstyp (CT), Deployment | Advanced Stack Components | ACM-Zertifikat mit zusätzlichem SANs | Create (ct-3l14e139i5p50), mit dem Sie eine Zertifikatsanfrage einreichen können. AWS Certificate Manager Weitere Informationen finden Sie unter [AWS::CertificateManager::Certificate](#). Dieses CT ermöglicht die Erstellung eines zusätzlichen alternativen Antragstellers (SAN).

Ein besseres Verständnis der allgemeinen AWS Sicherheit finden Sie unter [Bewährte Methoden für Sicherheit, Identität und Compliance](#).

AMS kategorisiert Sicherheitsrisiken wie folgt:

- Bekannte Risiken, die durch Anti-Malware erkannt wurden und im Rahmen des Malware-Abwehrprozesses behandelt werden.
- Sicherheitsereignisse, einschließlich Zugriffsverletzungen, die im Rahmen der Verwaltung von Sicherheitsereignissen behandelt werden.

Themen

- [Datenschutz in AMS](#)
- [Identitäts- und Zugriffsverwaltung](#)
- [Reaktion auf Sicherheitsvorfälle in AMS](#)
- [Sicherheitsüberprüfungen für Änderungsanfragen in AMS Advanced](#)

Datenschutz in AMS

AMS überwacht Ihre verwalteten Konten kontinuierlich, indem es native AWS Dienste wie Amazon GuardDuty, Amazon Macie (optional) und andere interne firmeneigene Tools und Prozesse nutzt. Nachdem ein Alarm ausgelöst wurde, übernimmt AMS die Verantwortung für die erste Auswahl

und Reaktion auf den Alarm. Unsere Reaktionsprozesse basieren auf NIST-Standards. AMS testet gemeinsam mit Ihnen regelmäßig seine Reaktionsprozesse mithilfe von Security Incident Response Simulation, um Ihren Arbeitsablauf an die bestehenden Sicherheitsreaktionsprogramme unserer Kunden anzupassen.

Wenn AMS einen Verstoß oder die unmittelbare Gefahr eines Verstoßes gegen Ihre Sicherheitsrichtlinien feststellt, erfassen wir Informationen, einschließlich der betroffenen Ressourcen und aller konfigurationsbezogenen Änderungen. AWS AMS bietet rund um die Uhr follow-the-sun Support mit engagierten Mitarbeitern, die die Überwachungs-Dashboards, die Warteschleifen für Vorfälle und Serviceanfragen für all Ihre verwalteten Konten aktiv überprüfen und untersuchen. AMS untersucht die Ergebnisse zusammen mit unseren Sicherheitsexperten, um die Aktivitäten zu analysieren und Sie über die in Ihrem Konto aufgeführten Ansprechpartner für die Sicherheits Eskalation zu benachrichtigen.

Auf der Grundlage unserer Ergebnisse setzt sich AMS proaktiv mit Ihnen in Verbindung. Wenn Sie der Meinung sind, dass die Aktivität nicht autorisiert oder verdächtig ist, arbeitet AMS mit Ihnen zusammen, um das Problem zu untersuchen und zu beheben oder einzudämmen. Es gibt bestimmte Arten von Ergebnissen, bei GuardDuty denen Sie die Auswirkungen bestätigen müssen, bevor AMS Maßnahmen ergreifen kann. Beispielsweise weist der GuardDuty Befundtyp UnauthorizedAccess:IAMUser/darauf hin ConsoleLogin, dass sich einer Ihrer Benutzer von einem ungewöhnlichen Ort aus angemeldet hat. AMS benachrichtigt Sie und bittet Sie, das Ergebnis zu überprüfen, um zu bestätigen, ob dieses Verhalten legitim ist.

Amazon Macie

AWS Managed Services empfiehlt, dass Sie Macie verwenden, um eine große und umfassende Liste vertraulicher Daten wie persönliche Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII) und Finanzdaten zu ermitteln.

Macie kann so konfiguriert werden, dass es regelmäßig auf jedem Amazon S3 S3-Bucket ausgeführt wird, wodurch die Bewertung aller neuen oder geänderten Objekte innerhalb eines Buckets im Laufe der Zeit automatisiert wird. Sobald Sicherheitsfeststellungen vorliegen, benachrichtigt AMS Sie und arbeitet mit Ihnen zusammen, um gegebenenfalls Abhilfemaßnahmen zu treffen.

Weitere Informationen finden Sie unter [Analysieren der Ergebnisse von Amazon Macie](#).

Amazon Macie-Sicherheit

Macie ist ein künstlich intelligence/AI betriebener Sicherheitsservice, der Ihnen hilft, Datenverlust zu verhindern, indem er sensible Daten, die in AWS gespeichert sind, automatisch erkennt, klassifiziert

und schützt. Macie verwendet maschinelles Lernen, um sensible Daten wie personenbezogene Daten (PII) oder geistiges Eigentum zu erkennen, weist ihnen einen Geschäftswert zu und bietet Transparenz darüber, wo diese Daten gespeichert sind und wie sie in Ihrem Unternehmen verwendet werden. Macie überwacht kontinuierlich die Datenzugriffsaktivitäten auf Anomalien und gibt Warnmeldungen aus, wenn das Risiko eines unbefugten Zugriffs oder unbeabsichtigter Datenlecks erkannt wird. Der Macie-Service unterstützt Amazon S3 und AWS CloudTrail Datenquellen.

AMS sucht kontinuierlich nach Warnmeldungen von Macie und ergreift im Falle einer Warnung schnell Maßnahmen, um Ihre Ressourcen und Ihr Konto zu schützen. Mit der Aufnahme von Macie in die Liste der Dienste, die AMS unterstützt, sind wir nun auch dafür verantwortlich, Macie gemäß Ihren Anweisungen in all Ihren Konten zu aktivieren und zu konfigurieren. Sie können Macie-Benachrichtigungen und unsere aktuellen Aktionen in der AWS-Konsole oder in unterstützten Integrationen einsehen. Während der Kontoeröffnung können Sie Konten angeben, die Sie zum Speichern personenbezogener Daten verwenden. Für alle neuen Konten mit PII empfehlen wir die Verwendung von Macie. Für bestehende Konten mit PII kontaktieren Sie uns und wir werden es in Ihrem Konto aktivieren. Dadurch steht Ihnen eine zusätzliche Schutzebene zur Verfügung und Sie können alle Vorteile von Macie in Ihrer von AMS verwalteten AWS-Umgebung nutzen.

AMS Macie FAQs

- Warum brauche ich Macie, wenn Trend Micro auf allen AMS-Konten aktiviert ist? GuardDuty

Macie hilft Ihnen beim Schutz Ihrer Daten in Amazon S3, indem es Ihnen hilft, zu klassifizieren, welche Daten Sie haben, welchen Wert diese Daten für das Unternehmen haben und welches Verhalten mit dem Zugriff auf diese Daten verbunden ist. Amazon GuardDuty bietet umfassenden Schutz Ihrer AWS-Konten, -Workloads und -Daten, indem es Ihnen hilft, Bedrohungen wie die Erkennung von Bedrohungsakteuren, Instance-Probleme und problematische Kontoaktivitäten zu identifizieren. Beide Services beinhalten Benutzerverhaltensanalysen, maschinelles Lernen und Anomalieerkennung, um Bedrohungen in ihren jeweiligen Kategorien zu erkennen. Trend Micro konzentriert sich nicht auf die Identifizierung personenbezogener Daten und der damit verbundenen Bedrohungen.

- Wie aktiviere ich Macie in meinem AMS-Konto?

Wenn Sie PII/PHI Daten in Ihren Konten gespeichert haben oder beabsichtigen, diese zu speichern, wenden Sie sich an Ihren CSDM oder stellen Sie eine Serviceanfrage, um Macie für Ihre neuen oder bestehenden, von AMS verwalteten Konten zu aktivieren.

- Was sind die Kosten, wenn ich Macie in meinem AMS-Konto aktiviere?

Die Preisgestaltung von Macie funktioniert für AMS ähnlich wie für andere Dienste wie Amazon Elastic Compute Cloud (Amazon EC2). Sie zahlen für Amazon Macie auf der Grundlage der Nutzung und eine AMS-Erhöhung auf der Grundlage Ihrer SLAs. Die Macie-Gebühren basieren auf der Nutzung (siehe [Amazon Macie Macie-Preise](#)) und werden auf der Grundlage von AWS CloudTrail Ereignissen und Amazon S3 S3-Speicherplatz berechnet. Bitte beachten Sie, dass Macie-Gebühren ab dem zweiten Monat nach der Aktivierung tendenziell flacher werden, da die Gebühren auf der Grundlage inkrementeller Daten berechnet werden, die Amazon S3 S3-Buckets hinzugefügt werden.

Weitere Informationen zu Macie finden Sie unter [Amazon Macie](#).

GuardDuty

GuardDuty ist ein Service zur kontinuierlichen Sicherheitsüberwachung, der Feeds mit Bedrohungsinformationen wie Listen bössartiger IP-Adressen und Domains sowie maschinelles Lernen verwendet, um unerwartete und potenziell unautorisierte und böswillige Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. Dazu können Probleme wie die Eskalation von Rechten, die Verwendung offengelegter Anmeldeinformationen oder die Kommunikation mit bössartigen IP-Adressen oder Domains gehören. GuardDuty überwacht auch das Verhalten beim Zugriff auf Amazon Web Services Services-Konten auf Anzeichen einer Beeinträchtigung, wie z. B. unautorisierte Infrastrukturbereitstellungen, wie z. B. Instances, die in einer Region bereitgestellt wurden, die noch nie verwendet wurde, oder ungewöhnliche API-Aufrufe, wie z. B. eine Änderung der Passwortrichtlinie zur Verringerung der Passwortstärke. Weitere Informationen finden Sie im [GuardDuty Benutzerhandbuch](#).

Gehen Sie wie folgt vor, um Ihre GuardDuty Ergebnisse einzusehen und zu analysieren.

1. Öffnen Sie die [GuardDuty -Konsole](#).
2. Wählen Sie Ergebnisse und dann ein bestimmtes Ergebnis aus, um Details anzuzeigen. Die Details für jedes Ergebnis unterscheiden sich je nach Art des Ergebnisses, den beteiligten Ressourcen und der Art der Aktivität.

Weitere Informationen zu verfügbaren Suchfeldern finden Sie unter [GuardDuty Findungsdetails](#).

GuardDuty Sicherheit

Amazon GuardDuty bietet Bedrohungserkennung, mit der Sie Ihre AWS-Konten und Workloads kontinuierlich überwachen und schützen können. Amazon GuardDuty analysiert kontinuierliche Streams von Metadaten, die aus Ihren Konto- und Netzwerkaktivitäten generiert wurden und in AWS CloudTrail Ereignissen, Amazon VPC-Flussprotokollen und DNS-Protokollen (Domain Name System) zu finden sind. Es nutzt auch integrierte Bedrohungsinformationen wie bekannte bösartige IP-Adressen, Anomalieerkennung und maschinelles Lernen, um Bedrohungen genauer zu identifizieren. GuardDuty ist ein überwachter AMS-Dienst. Weitere Informationen zur GuardDuty Amazon-Überwachung finden Sie unter [GuardDuty Überwachung](#). Weitere Informationen finden Sie GuardDuty unter [Amazon GuardDuty](#).

Alle neuen AMS-Konten sind standardmäßig GuardDuty aktiviert. AMS wird GuardDuty bei der Kontoeröffnung konfiguriert. Sie können jederzeit Änderungsanträge einreichen, um die Einstellungen zu ändern. GuardDuty Die Preisgestaltung funktioniert für AMS ähnlich wie für andere Dienste wie Amazon Elastic Compute Cloud (Amazon EC2). Sie zahlen auf der GuardDuty Grundlage der Nutzung und eine AMS-Erhöhung auf der Grundlage Ihrer SLAs. GuardDuty Die Gebühren basieren auf der Nutzung ([GuardDuty Amazon-Preise](#)) und werden auf der Grundlage von AWS CloudTrail Ereignissen und dem Volumen Ihres Amazon VPC Flow-Protokolls berechnet.

Für GuardDuty AMS sind die folgenden primären Erkennungskategorien aktiviert:

- Erkennung — Aktivität, die auf die Entdeckung durch einen Bedrohungsakteur hindeutet, wie z. B. ungewöhnliche API-Aktivitäten, VPC-Port-Scans, ungewöhnliche Muster fehlgeschlagener Anmeldeanfragen oder unblockierte Port-Sondierung von einer bekannten schlechten IP aus.
- Instance-Problem — Problematische Instance-Aktivitäten, z. B. Kryptowährungs-Mining, Malware, die Algorithmen zur Domaingenerierung (DGA) verwendet, ausgehende Denial-of-Service-Aktivitäten, ungewöhnlich hohes Volumen an Netzwerkverkehr, ungewöhnliche Netzwerkprotokolle, ausgehende Instance-Kommunikation mit einer bekannten bösartigen IP, temporäre EC2 Amazon-Anmeldeinformationen, die von einer externen IP-Adresse verwendet werden, und Datenexfiltration mithilfe von DNS.
- Kontoaktivität — Zu den häufigsten Mustern, die auf Kontoaktivitäten hinweisen, gehören API-Aufrufe von einem ungewöhnlichen Geolokalisierungs- oder Anonymisierungs-Proxy, Versuche, die AWS CloudTrail Protokollierung zu deaktivieren, ungewöhnliche Instance- oder Infrastrukturstarts, Infrastrukturbereitstellungen in einer ungewöhnlichen AWS-Region und API-Aufrufe von bekannten bösartigen IP-Adressen.

AMS verwendet GuardDuty in Ihren verwalteten Konten, um kontinuierlich nach Ergebnissen und Warnmeldungen zu suchen. Falls Sie benachrichtigt werden, ergreift AMS Operations proaktive Maßnahmen, um Ihre Ressourcen GuardDuty und Ihr Konto zu schützen. Sie können sich die GuardDuty Ergebnisse und unsere Aktionen in der AWS-Konsole oder in unterstützten Integrationen ansehen.

GuardDuty funktioniert mit Trend Micro Deep Security Manager in Ihrem Konto. Trend Micro Deep Security Manager bietet hostbasierte Intrusion Detection- und Intrusion Prevention-Services. Die Trend Micro Web Reputation Services überschneiden sich teilweise mit GuardDuty der Fähigkeit, zu erkennen, wenn ein Host versucht, mit einem Host oder Web-Service zu kommunizieren, der bekanntermaßen eine Bedrohung darstellt. Es GuardDuty bietet jedoch zusätzliche Kategorien für die Erkennung von Bedrohungen und erreicht dies durch die Überwachung des Netzwerkverkehrs — eine Methode, die die hostbasierte Erkennung von Trend Micro ergänzt. Die netzwerkbasierende Bedrohungserkennung erhöht die Sicherheit, indem sie verhindert, dass Kontrollen fehlschlagen, wenn der Host ein problematisches Verhalten zeigt. AMS empfiehlt die Verwendung GuardDuty in all Ihren AMS-Konten.

Weitere Informationen über Trend Micro finden Sie im [Trend Micro Deep Security Help Center](#). Beachten Sie, dass Links, die nicht von Amazon stammen, sich ändern können, ohne uns darüber in Kenntnis zu setzen.

GuardDuty Überwachung

GuardDuty informiert Sie über den Status Ihrer AWS-Umgebung, indem es [Sicherheitserkenntnisse generiert](#), die AMS erfasst und bei denen Warnmeldungen angezeigt werden.

Amazon GuardDuty überwacht die Sicherheit Ihrer AWS-Umgebung, indem es VPC-Flow-Logs, AWS CloudTrail Event-Logs und Domain Name System-Logs analysiert und verarbeitet. Sie können diesen Überwachungsumfang erweitern, indem Sie ihn so konfigurieren, GuardDuty dass auch Ihre eigenen benutzerdefinierten, vertrauenswürdigen IP-Listen und Bedrohungslisten verwendet werden.

- Vertrauenswürdige IP-Listen bestehen aus IP-Adressen, die Sie für die sichere Kommunikation mit Ihrer AWS-Infrastruktur und Ihren AWS-Anwendungen zugelassen haben. GuardDuty generiert keine Ergebnisse für IP-Adressen auf vertrauenswürdigen IP-Listen. Es kann immer nur eine Liste vertrauenswürdiger IPs pro AWS-Konto pro Region hochgeladen werden.
- Bedrohungslisten bestehen aus bekannten böartigen IP-Adressen. GuardDuty generiert Ergebnisse auf der Grundlage von Bedrohungslisten. Es kann immer nur bis zu sechs Bedrohungslisten pro AWS-Konto pro Region hochgeladen werden.

Verwenden Sie zur Implementierung GuardDuty AMS CT Deployment | Monitoring and Notification | GuardDuty IP Set | Create (ct-08avsj2e9mc7g), um einen Satz zugelassener IP-Adressen zu erstellen. Sie können auch das AMS CT Deployment | Monitoring and Notification | GuardDuty Threat Intel Set | Create (ct-25v6r7t8gvkq5) verwenden, um einen Satz verweigerter IP-Adressen zu erstellen.

Eine Liste der Dienste, die AMS überwacht, finden Sie unter. [Was überwacht das AMS-Überwachungssystem?](#)

DNS-Firewall mit Amazon Route 53-Resolver

Amazon Route 53 Resolver reagiert rekursiv auf DNS-Abfragen von AWS Ressourcen für öffentliche Aufzeichnungen, Amazon VPC-spezifische DNS-Namen und private gehostete Zonen von Amazon Route 53 und ist standardmäßig in allen verfügbar. VPCs Mit der Route-53-Resolver-DNS-Firewall können Sie ausgehenden DNS-Datenverkehr für Ihre virtuelle private Cloud (VPCs, Virtual Private Clouds) filtern und regulieren. Dazu erstellen Sie wiederverwendbare Sammlungen von Filterregeln in Regelgruppen der DNS-Firewall, ordnen die Regelgruppen Ihrer VPC zu und überwachen dann Aktivitäten in DNS-Firewall-Protokollen und -Metriken. Je nach Aktivität können Sie das Verhalten der DNS-Firewall entsprechend anpassen. Weitere Informationen finden Sie unter [Verwenden der DNS-Firewall zum Filtern von ausgehendem DNS-Verkehr](#).

Gehen Sie wie folgt vor, um Ihre Route 53 Resolver DNS-Firewall-Konfiguration anzuzeigen und zu verwalten:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie unter DNS-Firewall die Option Regelgruppen aus.
3. Überprüfen, bearbeiten oder löschen Sie Ihre bestehende Konfiguration oder erstellen Sie eine neue Regelgruppe. Weitere Informationen finden Sie unter [So funktioniert die Route 53 Resolver DNS Firewall](#).

Amazon Route 53 Resolver DNS-Firewall-Überwachung und Sicherheit

Die Amazon Route 53 DNS-Firewall verwendet die Konzepte Regelzuordnungen, Regelaktion und Regelauswertungspriorität. Eine Domainliste ist ein wiederverwendbarer Satz von Domainspezifikationen, die Sie in einer DNS-Firewall-Regel innerhalb einer Regelgruppe verwenden. Wenn Sie eine Regelgruppe mit einer VPC verknüpfen, vergleicht die DNS-Firewall Ihre DNS-

Abfragen mit den Domainlisten, die in den Regeln verwendet werden. Wenn die DNS-Firewall eine Übereinstimmung findet, verarbeitet sie die DNS-Abfrage entsprechend der Aktion der Abgleichsregel. Weitere Informationen zu Regelgruppen und Regeln finden Sie unter [Regelgruppen und Regeln für die DNS-Firewall](#).

Domainlisten lassen sich in zwei Hauptkategorien einteilen:

- Verwaltete Domainlisten, die für Sie AWS erstellt und verwaltet werden.
- Ihre eigenen Domainlisten, die Sie erstellen und verwalten.

Regelgruppen werden anhand ihres Zuordnungsprioritätsindex bewertet.

Standardmäßig stellt AMS eine Basiskonfiguration bereit, die aus der folgenden Regel und Regelgruppe besteht:

- Eine Regelgruppe mit dem Namen `DefaultSecurityMonitoringRule`. Die Regelgruppe hat die höchste Zuordnungspriorität, die zum Zeitpunkt der Erstellung für jede vorhandene VPC in jeder aktivierten AWS-Region Version verfügbar ist.
- Eine Regel `DefaultSecurityMonitoringRule` mit Priorität 1 innerhalb der `DefaultSecurityMonitoringRule` Regelgruppe, die die Liste der `AWSManagedDomainsAggregateThreatList` verwalteten Domänen mit der Aktion `ALERT` verwendet.

Wenn Sie über eine bestehende Konfiguration verfügen, wird die Basiskonfiguration mit einer niedrigeren Priorität als Ihre bestehende Konfiguration bereitgestellt. Ihre bestehende Konfiguration ist die Standardkonfiguration. Sie verwenden die AMS-Basiskonfiguration als Sammellösung, wenn Ihre bestehende Konfiguration keine Anweisung mit höherer Priorität zum Umgang mit der Abfrageauflösung enthält. Gehen Sie wie folgt vor, um die Basiskonfiguration zu ändern oder zu entfernen:

- Wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM) oder Cloud Architect (CA).
- Erstellen Sie mithilfe von [Management | Other | Other | Create CT \(ct-1e1xtak34nx76\) einen Änderungsantrag](#) (RFC).
- Erstellen Sie eine Serviceanfrage.

Wenn Ihr Konto im Entwicklermodus oder im Direktänderungsmodus betrieben wird, können Sie die Änderungen selbst vornehmen.

AWS Certificate Manager (ACM) -Zertifikat

AMS verfügt über ein CT, Deployment | Advanced Stack Components | ACM-Zertifikat mit zusätzlichem SANs | Create (ct-3l14e139i5p50), mit dem Sie eine Anfrage für ein AWS Certificate Manager Manager-Zertifikat mit bis zu fünf zusätzlichen Subject Alternative Names (SAN) (wie example.com, example.net und example.org) einreichen können. [Einzelheiten finden Sie unter Was ist? AWS Certificate Manager](#) und [Merkmal des ACM-Zertifikats](#).

Note

Bei dieser Timeout-Einstellung geht es nicht nur um den Lauf, sondern auch um Ihre Validierung des ACM-Zertifikats durch E-Mail-Validierung. Ohne Ihre Validierung schlägt der RFC fehl.

Datenverschlüsselung in AMS

AMS verwendet mehrere AWS Dienste für die Datenverschlüsselung, insbesondere Amazon Simple Storage Service, AWS Key Management Service (AWS KMS), Amazon Elastic Block Store, Amazon Relational Database Service Amazon Redshift, Amazon ElastiCache, AWS Lambda, und Amazon OpenSearch Service.

Amazon S3

Amazon S3 bietet verschiedene Optionen für die Objektverschlüsselung, um Daten während der Übertragung und im Ruhezustand zu schützen. Bei der serverseitigen Verschlüsselung wird das Objekt verschlüsselt, bevor es auf Datenträgern im Rechenzentrum gespeichert wird. Wenn die Objekte heruntergeladen werden, werden sie wieder entschlüsselt. Wenn Sie Ihre Anforderung authentifizieren und Zugriffsberechtigungen besitzen, gibt es in Bezug auf die Art und Weise, wie Sie auf verschlüsselte oder nicht verschlüsselte Objekte zugreifen, keinen Unterschied. Weitere Informationen finden Sie unter [Datenschutz in Amazon S3](#).

Amazon EBS

Mit der Amazon EBS-Verschlüsselung müssen Sie keine eigene Schlüsselverwaltungsinfrastruktur aufbauen, warten und sichern. Die Amazon EBS-Verschlüsselung verwendet AWS KMS Schlüssel bei der Erstellung verschlüsselter Volumes und Snapshots. Verschlüsselungsvorgänge finden auf den Servern statt, die EC2 Amazon-Instances hosten. Dadurch wird sichergestellt, dass sowohl

data-at-rest eine Instance als auch data-in-transit zwischen einer Instance und dem zugehörigen Amazon EBS-Speicher sicher ist. Sie können diesen Instances sowohl verschlüsselte als auch unverschlüsselte Volumes gleichzeitig zuordnen. Weitere Informationen finden Sie unter [Amazon EBS-Verschlüsselung](#).

Amazon RDS

Amazon RDS kann Ihre Amazon-RDS-DB-Instances verschlüsseln. Zu den Daten, die im Ruhezustand verschlüsselt werden, gehören der zugrunde liegende Speicher für DB-Instances, deren automatische Backups, Read Replicas und Snapshots. Amazon RDS-verschlüsselte DB-Instances verwenden den Industriestandard-Verschlüsselungsalgorithmus AES-256, um Ihre Daten auf dem Server zu verschlüsseln, der Ihre Amazon RDS-DB-Instances hostet. Nachdem Ihre Daten verschlüsselt wurden, verarbeitet Amazon RDS die Authentifizierung des Zugriffs und die Entschlüsselung Ihrer Daten transparent und mit minimalen Auswirkungen auf die Leistung. Sie müssen Ihre Datenbank-Client-Anwendungen nicht ändern, um Verschlüsselung anzuwenden. Weitere Informationen finden Sie unter [Verschlüsseln von Amazon RDS-Ressourcen](#).

Amazon Simple Queue Service

Zusätzlich zur Standardoption für verwaltete serverseitige Verschlüsselung (SSE) von Amazon SQS können Sie mit Amazon SQS-Managed SSE (SSE-SQS) eine benutzerdefinierte verwaltete serverseitige Verschlüsselung erstellen, die von Amazon SQS verwaltete Verschlüsselungsschlüssel verwendet, um sensible Daten zu schützen, die über Nachrichtenwarteschlangen gesendet werden. Mit serverseitiger Verschlüsselung (SSE) können Sie vertrauliche Daten in verschlüsselten Warteschlangen übertragen. SSE schützt den Inhalt von Nachrichten in Warteschlangen mit von Amazon SQS verwalteten Verschlüsselungsschlüsseln (SSE-SQS) oder Schlüsseln, die in (SSE-KMS) verwaltet werden. AWS KMS [Informationen zur Verwaltung von SSE mithilfe von finden Sie unter Verschlüsselung im Ruhezustand. AWS-Managementkonsole](#)

Datenverschlüsselung im Ruhezustand

OpenSearch Servicedomänen bieten die Verschlüsselung von Daten im Ruhezustand, eine Sicherheitsfunktion, die dazu beiträgt, unbefugten Zugriff auf Ihre Daten zu verhindern. Die Funktion verwendet AWS Key Management Service (AWS KMS) zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel und den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) zur Durchführung der Verschlüsselung. Weitere Informationen finden Sie unter [Verschlüsselung ruhender Daten für Amazon OpenSearch Service](#).

Schlüsselverwaltung

AWS KMS ist ein verwalteter Service, der es Ihnen leicht macht, Kunden-Masterschlüssel (CMKs) zu erstellen und zu kontrollieren, also die Verschlüsselungsschlüssel, die zur Verschlüsselung Ihrer Daten verwendet werden. AWS KMS CMKs sind durch Hardware-Sicherheitsmodule (HSMs) geschützt, die vom FIPS 140-2 Cryptographic Module Validation Program validiert wurden, außer in den Regionen China (Peking) und China (Ningxia). Weitere Informationen finden Sie unter [Was ist der AWS Key Management Service?](#)

Identitäts- und Zugriffsverwaltung

AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen. Während des AMS-Onboardings sind Sie dafür verantwortlich, kontoübergreifende IAM-Administratorrollen in jedem Ihrer verwalteten Konten zu erstellen.

IAM-Sicherheitsvorkehrungen für die Multi-Account Landing Zone (MALZ)

Die AMS Multi-Account landing zone (MALZ) erfordert eine Active Directory-Vertrauensstellung (AD) als primäres Entwurfsziel des AMS Access Management, damit jede Organisation (sowohl AMS als auch Kunde) die Lebenszyklen ihrer eigenen Identitäten verwalten kann. Dadurch entfällt die Notwendigkeit, Anmeldeinformationen im Verzeichnis des jeweils anderen zu speichern. Die unidirektionale Vertrauensstellung ist so konfiguriert, dass das verwaltete Active Directory innerhalb des Netzwerks dem kundeneigenen oder verwalteten AD AWS-Konto vertraut, um Benutzer zu authentifizieren. Da es sich bei der Vertrauensstellung nur um eine Richtung handelt, bedeutet dies nicht, dass das Active Directory des Kunden dem Managed AD vertraut.

In dieser Konfiguration wird das Kundenverzeichnis, das Benutzeridentitäten verwaltet, als Benutzergesamtstruktur bezeichnet, und das verwaltete AD, an das EC2 Amazon-Instances angehängt sind, wird als Resource Forest bezeichnet. Dies ist ein häufig verwendetes Microsoft-Entwurfsmuster für die Windows-Authentifizierung. Weitere Informationen finden Sie unter [Forest Design Models](#).

Dieses Modell ermöglicht es beiden Organisationen, ihre jeweiligen Lebenszyklen zu automatisieren, und ermöglicht sowohl AMS als auch Ihnen, den Zugriff schnell zu widerrufen, wenn ein Mitarbeiter das Unternehmen verlässt. Wenn beide Organisationen ohne dieses Modell ein gemeinsames Verzeichnis verwenden (oder users/groups in den Verzeichnissen des jeweils anderen Unternehmens erstellt), müssten beide Organisationen zusätzliche Workflows und

Benutzersynchronisierungen einrichten, um zu berücksichtigen, ob Mitarbeiter beginnen und gehen. Dies birgt Risiken, da dieser Prozess Latenz aufweist und fehleranfällig sein kann.

Voraussetzungen für den MALZ-Zugriff

MALZ Identity Provider-Integration für den Zugriff auf die AWS/AMS-Konsole, CLI, SDK.

Einseitige Vertrauensstellung für EC2 Amazon-Instances in Ihrem AMS-Konto.

Authentifizierung mit Identitäten

AMS verwendet IAM-Rollen, was eine Art von IAM-Identität ist. Eine IAM-Rolle ist einem Benutzer insofern sehr ähnlich, als es sich um eine Identität mit Berechtigungsrichtlinien handelt, die festlegen, was die Identität tun kann und was nicht. AWS einer Rolle sind jedoch keine Anmeldeinformationen zugeordnet, und anstatt eindeutig einer Person zugeordnet zu sein, soll eine Rolle von jedem übernommen werden können, der sie benötigt. Ein IAM-Benutzer kann eine Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu erlangen.

Zugriffsrollen werden durch die interne Gruppenmitgliedschaft gesteuert, die vom Operations Management verwaltet und regelmäßig überprüft wird.

IAM-Benutzerrolle in AMS

Eine IAM-Rolle ähnelt einem IAM-Benutzer insofern, als es sich um eine AWS Identität mit Berechtigungsrichtlinien handelt, die festlegen, was die Identität tun darf und was nicht. AWS Eine Rolle ist jedoch nicht einer einzigen Person zugeordnet, sondern kann von allen Personen angenommen werden, die diese Rolle benötigen.

Derzeit gibt es eine AMS-Standardbenutzerrolle für AMS-Standardkonten und eine zusätzliche Rolle `customer_managed_ad_user_role` für AMS-Konten mit Managed Active Directory. `Customer_ReadOnly_Role`

Die Rollenrichtlinien legen Berechtigungen für CloudWatch Amazon S3 S3-Protokollaktionen, AMS-Konsolenzugriff, Leseinschränkungen für die meisten AWS-Services, eingeschränkten Zugriff auf die S3-Konsole des Kontos und AMS-Change-Typ-Zugriff fest.

Darüber hinaus `Customer_ReadOnly_Role` verfügt über mutative Reserved-Instance-Berechtigungen, mit denen Sie Instances reservieren können. Es hat einige

Kosteneinsparungsmöglichkeiten. Wenn Sie also wissen, dass Sie über einen längeren Zeitraum eine bestimmte Anzahl von EC2 Amazon-Instances benötigen, können Sie diese APIs aufrufen. Weitere Informationen finden Sie unter [Amazon EC2 Reserved Instances](#).

 Note

Das AMS Service Level Objective (SLO) für die Erstellung benutzerdefinierter IAM-Richtlinien für IAM-Benutzer beträgt vier Arbeitstage, es sei denn, eine bestehende Richtlinie wird wiederverwendet. Wenn Sie die bestehende IAM-Benutzerrolle ändern oder eine neue hinzufügen möchten, reichen Sie jeweils einen [IAM: Update Entity oder IAM: Create Entity](#) RFC ein.

Wenn Sie mit Amazon IAM-Rollen nicht vertraut sind, finden Sie wichtige Informationen unter [IAM-Rollen](#).

Multi-Account-Landingzone (MALZ): Die standardmäßigen, nicht angepassten Richtlinien für Benutzerrollen für mehrere Konten von AMS finden Sie unter Weiter. [MALZ: Standard-IAM-Benutzerrollen](#)

MALZ: Standard-IAM-Benutzerrollen

JSON-Richtlinienerklärungen für die standardmäßigen AMS-Landingzone-Benutzerrollen mit mehreren Konten.

 Note

Die Benutzerrollen sind anpassbar und können je nach Konto unterschiedlich sein. Anweisungen zur Suche nach Ihrer Rolle finden Sie hier.

Dies sind Beispiele für die standardmäßigen MALZ-Benutzerrollen. Um sicherzustellen, dass Sie die benötigten Richtlinien festgelegt haben, führen Sie den AWS-Befehl aus [get-role](#) oder melden Sie sich bei der AWS-Management -> [IAM-Konsole](#) an und wählen Sie im Navigationsbereich Rollen aus.

Rollen der wichtigsten OU-Konten

Ein Kernkonto ist ein von Malz verwaltetes Infrastrukturkonto. AMS-Landingzone mit mehreren Konten Zu den Kernkonten gehören ein Verwaltungskonto und ein Netzwerkkonto.

Core-OU-Konto: Allgemeine Rollen und Richtlinien

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Öffentliche verwaltete AWS-Richtlinie).
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie).
AWSManagedServicesChangeManagementRole (Version des Hauptkontos)	ReadOnlyAccess AWSSupportAccess AMSChangeManagementReadOnlyPolicy AMSChangeManagementInfrastructurePolicy

OU-Hauptkonto: Rollen und Richtlinien für Verwaltungskonten

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesBillingRole	AMSBillingRichtlinie (AMSBillingRichtlinie).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Öffentliche verwaltete AWS-Richtlinie).
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie).
AWSManagedServicesChangeManagementRole (Version des Verwaltungskontos)	ReadOnlyAccess AWSSupportAccess AMSChangeManagementReadOnlyPolicy AMSChangeManagementInfrastructurePolicy

Rolle	Richtlinie oder Richtlinien
	<u>AMSMasterAccountSpecificChangeManagementInfrastructurePolicy</u>

OU-Hauptkonto: Rollen und Richtlinien für Netzwerkkonten

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesReadOnlyRole	<u>ReadOnlyAccess</u> (Öffentliche verwaltete AWS-Richtlinie).
AWSManagedServicesCaseRole	<u>ReadOnlyAccess</u> <u>AWSSupportZugriff</u> (Öffentliche AWS-verwaltete Richtlinie).
AWSManagedServicesChangeManagementRole (Version des Netzwerkkontos)	<u>ReadOnlyAccess</u> <u>AWSSupportAccess</u> <u>AMSChangeManagementReadOnlyPolicy</u> <u>AMSChangeManagementInfrastructurePolicy</u> <u>AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy</u>

Rollen von Anwendungskonten

Anwendungskontrollen werden auf Ihre anwendungsspezifischen Konten angewendet.

Anwendungskonto: Rollen und Richtlinien

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesReadOnlyRole	<u>ReadOnlyAccess</u> (Öffentliche verwaltete AWS-Richtlinie).

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie). Diese Richtlinie bietet Zugriff auf alle Support-Aktivitäten und Ressourcen. Weitere Informationen finden Sie unter Erste Schritte mit AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess AWSsupportBeispiel für Access Diese Richtlinie bietet Zugriff auf alle Support-Aktivitäten und Ressourcen. AWSCertificateManagerFullAccess Informationen, (Öffentliche verwaltete AWS-Richtlinie) AWSWAFFullAccess Informationen, (Öffentliche AWS-verwaltete Richtlinie). Diese Richtlinie gewährt vollen Zugriff auf AWS-WAF-Ressourcen. AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (Version des Anwendungskontos)	ReadOnlyAccess AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie). Diese Richtlinie bietet Zugriff auf alle Support-Aktivitäten und Ressourcen. Weitere Informationen finden Sie unter Erste Schritte mit AWS Support.

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesAdminRole	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Richtlinie
	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccess
	AMSS3Richtlinie
	AMSReservedInstancesPolicy

Beispiele für Richtlinien

Für die meisten verwendeten Richtlinien werden Beispiele bereitgestellt. Um die `ReadOnlyAccess` Richtlinie einzusehen (die Seiten lang ist, da sie nur Lesezugriff auf alle AWS Services bietet), können Sie diesen Link verwenden, wenn Sie ein aktives AWS-Konto haben: [ReadOnlyAccess](#). Außerdem ist hier eine komprimierte Version enthalten.

AMSBillingRichtlinie

AMSBillingPolicy

Die neue Rolle „Abrechnung“ kann von Ihrer Buchhaltungsabteilung verwendet werden, um Rechnungsinformationen oder Kontoeinstellungen im Verwaltungskonto einzusehen und zu ändern. Sie verwenden diese Rolle, um auf Informationen wie alternative Kontakte zuzugreifen, die Nutzung der Kontoressourcen einzusehen, Ihre Abrechnung im Auge zu behalten oder sogar Ihre Zahlungsmethoden zu ändern. Diese neue Rolle umfasst alle Berechtigungen, die auf der [Webseite AWS Billing IAM-Aktionen](#) aufgeführt sind.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aws-portal:ViewBilling",
        "aws-portal:ModifyBilling"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToBilling"
    },
    {
      "Action": [
        "aws-portal:ViewAccount",
        "aws-portal:ModifyAccount"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountSettings"
    },
    {
      "Action": [
        "budgets:ViewBudget",
        "budgets:ModifyBudget"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountBudget"
    },
    {
      "Action": [
        "aws-portal:ViewPaymentMethods",
```

```
        "aws-portal:ModifyPaymentMethods"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPaymentMethods"
},
{
    "Action": [
        "aws-portal:ViewUsage"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToUsage"
},
{
    "Action": [
        "cur:DescribeReportDefinitions",
        "cur:PutReportDefinition",
        "cur>DeleteReportDefinition",
        "cur:ModifyReportDefinition"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostAndUsageReport"
},
{
    "Action": [
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPricing"
},
{
    "Action": [
        "ce:*",
        "compute-optimizer:*"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostExplorerComputeOptimizer"
},
}
```

```
{
  "Action": [
    "purchase-orders:ViewPurchaseOrders",
    "purchase-orders:ModifyPurchaseOrders"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToPurchaseOrders"
},
{
  "Action": [
    "redshift:AcceptReservedNodeExchange",
    "redshift:PurchaseReservedNodeOffering"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToRedshiftAction"
},
{
  "Action": "savingsplans:*",
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AWSSavingsPlansFullAccess"
}
]
```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

Berechtigungen zum Einsehen aller AMS-Änderungstypen und des Verlaufs der angeforderten Änderungstypen.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Berechtigungen zum Anfordern des Änderungstyps Deployment | Verwaltete landing zone | Verwaltungskonto | Anwendungskonto erstellen (mit VPC).

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Berechtigungen zum Anfordern der Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Änderungstyp der Anwendungsroutentabelle erstellen.

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy(für die Verwaltung | Andere | Andere CTs)

Berechtigungen zum Anfordern der Verwaltung | Andere | Andere | Erstellung und Verwaltung | Andere | Andere | Änderungstypen aktualisieren.

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

Berechtigungen zum Einsehen von passwords/hasches Geheimnissen, die von AMS geteilt wurden AWS Secrets Manager (z. B. Passwörter für die Infrastruktur zu Prüfungszwecken).

Berechtigungen zum Erstellen von password/hasches Geheimnissen zur Weitergabe an AMS. (zum Beispiel Lizenzschlüssel für Produkte, die bereitgestellt werden müssen).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
      "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    ]
  },
  {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  }
]
```

```
},
{
  "Sid": "AllowReadAccessToAMSNameSpace",
  "Effect": "Deny",
  "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
  ],
  "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
}
]
```

AMSChangeManagementPolicy

AMSChangeManagementPolicy

Berechtigungen zum Anfordern und Anzeigen aller AMS-Änderungstypen sowie des Verlaufs der angeforderten Änderungstypen.

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

Berechtigungen zur Verwaltung von Amazon EC2 Reserved Instances; Preisinformationen finden Sie unter [Amazon EC2 Reserved Instances](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowReservedInstancesManagement",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyReservedInstances",
      "ec2:PurchaseReservedInstancesOffering"
    ],
    "Resource": [
      "*"
    ]
  }
]
```

```
}]  
}
```

AMSS3Richtlinie

AMSS3Policy

Berechtigungen zum Erstellen und Löschen von Dateien aus vorhandenen Amazon S3 S3-Buckets.

 Note

Diese Berechtigungen gewähren nicht die Möglichkeit, S3-Buckets zu erstellen. Dies muss mit dem Änderungstyp Deployment | Erweiterte Stack-Komponenten | S3-Speicher | Create erfolgen.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:AbortMultipartUpload",  
        "s3:DeleteObject",  
        "s3:PutObject"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```

AWSSupportZugriff

AWSSupportAccess

Voller Zugriff auf Support. Weitere Informationen finden Sie unter [Erste Schritte mit Support](#).
Informationen zum Premium-Support finden Sie unter [Support](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "support:*"
    ],
    "Resource": "*"
  }]
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions(Öffentlich AWS verwaltete Richtlinie)

Berechtigungen zum Abonnieren, Abbestellen und Ansehen von AWS Marketplace Abonnements.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess

Voller Zugriff auf AWS Certificate Manager. Weitere Informationen finden Sie unter [AWS Certificate Manager](#).

[AWSCertificateManagerFullAccess](#) Informationen, (Öffentliche AWS-verwaltete Richtlinie).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm:*"
    ],
    "Resource": "*"
  }]
}
```

AWSWAFFullZugriff

AWSWAFFullAccess

Voller Zugriff auf AWS WAF. Weitere Informationen finden Sie unter [AWS WAF - Web Application Firewall](#).

[AWSWAFFullAccess](#) Informationen, (Öffentlich AWS verwaltete Richtlinie). Diese Richtlinie gewährt vollen Zugriff auf AWS WAF Ressourcen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "waf:*",
      "waf-regional:*",
      "elasticloadbalancing:SetWebACL"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

ReadOnlyAccess

ReadOnlyAccess

Schreibgeschützter Zugriff auf alle AWS Dienste und Ressourcen auf der AWS Konsole. Wenn ein neuer Dienst AWS gestartet wird, aktualisiert AMS die ReadOnlyAccess Richtlinie, um Nur-Lese-Berechtigungen für den neuen Dienst hinzuzufügen. Die aktualisierten Berechtigungen werden auf alle Auftraggeber-Entitäten angewendet, an die die Richtlinie angefügt ist.

Dies gewährt nicht die Möglichkeit, sich bei EC2 Hosts oder Datenbank-Hosts anzumelden.

Wenn Sie eine aktive Richtlinie haben AWS-Konto, können Sie diesen Link verwenden [ReadOnlyAccess](#), um die gesamte ReadOnlyAccess Richtlinie einzusehen. Die gesamte ReadOnlyAccess Richtlinie ist sehr lang, da sie nur Lesezugriff für alle bietet. AWS-Services Das Folgende ist ein teilweiser Auszug der Richtlinie. ReadOnlyAccess

Single-Account-Landingzone (SALZ): Die standardmäßigen, unangepassten Benutzerrollenrichtlinien für Single-Account-Landingzonen von AMS finden Sie unter [SALZ: Standard-IAM-Benutzerrolle](#) Weiter.

SALZ: Standard-IAM-Benutzerrolle

JSON-Richtlinienerklärungen für die standardmäßige AMS-Landingzone-Benutzerrolle mit einem Konto.

Note

Die SALZ-Standardbenutzerrolle ist anpassbar und kann je nach Konto unterschiedlich sein. Anweisungen zur Suche nach Ihrer Rolle finden Sie hier.

Im Folgenden finden Sie ein Beispiel für die standardmäßige SALZ-Benutzerrolle. Führen Sie den [get-role](#)Befehl aus, um sicherzustellen, dass Sie die Richtlinien für Sie festgelegt haben. Oder melden Sie sich bei der AWS Identity and Access Management Konsole unter an <https://console.aws.amazon.com/iam/>und wählen Sie dann Rollen aus.

Die Rolle „Nur Lesen“ für den Kunden ist eine Kombination aus mehreren Richtlinien. Es folgt eine Aufschlüsselung der Rolle (JSON).

Audit-Richtlinie für Managed Services:

ReadOnly IAM-Richtlinie für Managed Services

Benutzerrichtlinie für Managed Services

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerToListTheLogBucketLogs",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "aws/*",
            "app/*",
            "encrypted",
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
```

```
"Resource": [
  "arn:aws:s3:::mc-a*-logs-*/aws/*",
  "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
],
{
  "Sid": "AllowAccessToOtherObjects",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteObject*",
    "s3:Get*",
    "s3:List*",
    "s3:PutObject*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "AllowCustomerToListTheLogBucketRoot",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*"
  ],
  "Condition": {
    "StringEquals": {
      "s3:prefix": [
        "",
        "/"
      ]
    }
  }
},
{
  "Sid": "AllowCustomerCWLConsole",
  "Effect": "Allow",
  "Action": [
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups"
  ],
  "Resource": [
```



```

    "arn:aws:logs:*:*:log-group:*"
  ],
},
{
  "Sid": "AllowCustomerCWLAccessLogs",
  "Effect": "Allow",
  "Action": [
    "logs:FilterLogEvents",
    "logs:GetLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/*",
    "arn:aws:logs:*:*:log-group:/infra/*",
    "arn:aws:logs:*:*:log-group:/app/*",
    "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
  ]
},
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "ModifyAWSBillingPortal",
  "Effect": "Allow",
  "Action": [
    "aws-portal:Modify*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "DenyDeleteCWL",
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ]
}

```

```

    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:*"
    ]
},
{
    "Sid": "DenyMCCWL",
    "Effect": "Deny",
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
    ]
},
{
    "Sid": "DenyS3MCNamespace",
    "Effect": "Deny",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*audit/*",
        "arn:aws:s3:::mc-a*-internal-*/",
        "arn:aws:s3:::mc-a*-internal-*"
    ]
},
{
    "Sid": "ExplicitDenyS3CfnBucket",
    "Effect": "Deny",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::cf-templates-*"
    ]
},

```

```
{
  "Sid": "DenyListBucketS3LogsMC",
  "Action": [
    "s3:ListBucket"
  ],
  "Effect": "Deny",
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*"
  ],
  "Condition": {
    "StringLike": {
      "s3:prefix": [
        "auditlog/*",
        "encrypted/mc/*",
        "mc/*"
      ]
    }
  }
},
{
  "Sid": "DenyS3LogsDelete",
  "Effect": "Deny",
  "Action": [
    "s3:Delete*",
    "s3:Put*"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*/*"
  ]
},
{
  "Sid": "DenyAccessToKmsKeysStartingWithMC",
  "Effect": "Deny",
  "Action": [
    "kms:*"
  ],
  "Resource": [
    "arn:aws:kms::*:key/mc-*",
    "arn:aws:kms::*:alias/mc-*"
  ]
},
{
  "Sid": "DenyListingOfStacksStartingWithMC",
  "Effect": "Deny",
```

```

    "Action": [
      "cloudformation:*"
    ],
    "Resource": [
      "arn:aws:cloudformation:*:*:stack/mc-*"
    ]
  },
  {
    "Sid": "AllowCreateCWMetricsAndManageDashboards",
    "Effect": "Allow",
    "Action": [
      "cloudwatch:PutMetricData"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AllowCreateandDeleteCWDashboards",
    "Effect": "Allow",
    "Action": [
      "cloudwatch:DeleteDashboards",
      "cloudwatch:PutDashboard"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

Gemeinsame Richtlinie für Customer Secrets Manager

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    }
  ]
}

```

```

    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
    {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}

```

Abonnementrichtlinie für Customer Marketplace

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ]
    }
  ]
}

```

```
    ],  
    "Resource": [  
        "*"   
    ]  
}  
]  
}
```

Protokollierung und Überwachung von Sicherheitsereignissen

AMS überwacht die verwaltete Umgebung kontinuierlich auf Sicherheitsbedrohungen. Sicherheitsereignisse können von AMS oder von Ihnen entdeckt werden. AMS aktualisiert seinen Automatisierungsprozess regelmäßig auf der Grundlage des Computer Security Incident Handling Guide des National Institute of Standards and Technology (NIST), um Sicherheitsbedrohungen besser erkennen zu können.

Endpunktsicherheit (EPS)

Zu den Ressourcen, die Sie in Ihrer AMS Advanced-Umgebung bereitstellen, gehört automatisch die Installation eines Endpoint Security (EPS) -Überwachungsclients. Dieser Prozess stellt sicher, dass die von AMS Advanced verwalteten Ressourcen rund um die Uhr überwacht und unterstützt werden. Darüber hinaus überwacht AMS Advanced alle Agentenaktivitäten, und es wird ein Vorfall ausgelöst, wenn ein Sicherheitsereignis erkannt wird.

Note

Sicherheitsvorfälle werden als Vorfälle behandelt. Weitere Informationen finden Sie unter [Reaktion auf Vorfälle](#).

Endpoint Security bietet Anti-Malware-Schutz, insbesondere werden die folgenden Aktionen unterstützt:

- EC2 Instanzen werden bei EPS registriert
- EC2 Instanzen werden von EPS abgemeldet
- EC2 Instanzen Anti-Malware-Schutz in Echtzeit
- Vom EPS-Agenten initiiertes Heartbeat
- EPS stellt die Datei unter Quarantäne wieder her

- EPS-Ereignisbenachrichtigung
- EPS-Berichterstattung

AMS Advanced verwendet Trend Micro für Endpoint Security (EPS). Dies sind die EPS-StandardEinstellungen. Weitere Informationen über Trend Micro finden Sie im [Trend Micro Deep Security Help Center](#). Beachten Sie, dass Links, die nicht von Amazon stammen, sich ändern können, ohne uns darüber in Kenntnis zu setzen.

Die Standardeinstellungen für AMS Advanced Multi-Account landing zone (MALZ) werden in den folgenden Abschnitten beschrieben. Informationen zu den nicht standardmäßigen EPS-Einstellungen für AMS Multi-Accounts Landing Zone finden Sie unter [AMS Advanced Multi-Account Landing Zone EPS-StandardEinstellungen](#).

 Note

[Sie können Ihr eigenes EPS mitbringen. Weitere Informationen finden Sie unter AMS Bring your own EPS.](#)

Allgemeine EPS-Einstellungen

Allgemeine Netzwerkeinstellungen für Endpoint Security.

EPS-StandardEinstellungen

Einstellung	Standard
Firewall-Ports (Sicherheitsgruppe der Instanzen)	Bei EPS Deep Security Manager-Agenten (DSMs) muss Port 4120 für die Agent/Relay Kommunikation mit Manager und Port 4119 für die Manager-Konsole geöffnet sein. Bei EPS-Relays muss Port 4122 für die Kommunika tion zu Relay geöffnet sein. Manager/Agent Für die eingehende Kommunikation zwischen Kundeninstanzen sollten keine spezifisc hen Ports geöffnet sein, da die Agenten alle Anfragen initiieren.

Einstellung	Standard
Richtung der Kommunikation	Agent/Appliance wurde initiiert
Taktintervall	Zehn Minuten
Anzahl der verpassten Herzschläge vor einer Warnung	Zwei
Maximal zulässige Abweichung (Differenz) zwischen Serverzeiten	Unbegrenzt
Löst Offlinefehler für inaktive (registrierte, aber nicht online) virtuelle Maschinen aus	Nein
Standardrichtlinie	Basisrichtlinie (im Folgenden beschrieben)
Aktivierung mehrerer Computer mit demselben Hostnamen	Ist erlaubt
Es werden Warnmeldungen für ausstehende Updates ausgelöst	Nach sieben Tagen
Zeitplan aktualisieren	AMS strebt einen monatlichen Veröffentlichungszyklus für die Software-Updates für Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA) an. AMS hält jedoch kein SLA für Updates ein. Updates werden während einer Bereitstellung flottenweit von AMS-Entwicklerteams durchgeführt. DSA/DSA-Updates werden in Trend Micro DSM Systemereignissen protokolliert, die AMS standardmäßig 13 Wochen lang lokal speichert. Die Herstellerdokumentation finden Sie im Trend Micro Deep Security Help Center unter Systemereignisse. Protokolle werden auch in die Protokollgruppe/aws/ams/eps/var/log/DSM.log in Amazon CloudWatch exportiert.

Einstellung	Standard
Quelle aktualisieren	Trend Micro Update Server (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
Löschen von Ereignis- oder Protokolldaten	Ereignisse und Protokolle werden nach sieben Tagen aus der DSM-Datenbank gelöscht.
Die Versionen der Agentensoftware werden gespeichert	Bis zu fünf
Die neuesten Regelaktualisierungen finden statt	Bis zu zehn
Speicherung von Protokollen	Standardmäßig werden Protokolldateien sicher in Amazon S3 gespeichert. Sie können sie jedoch auch in Amazon Glacier archivieren, um Audit- und Compliance-Anforderungen zu erfüllen.

Grundlegende Richtlinie

Standardeinstellungen der Basisrichtlinie für Endpoint Security.

EPS-Basisrichtlinie

Einstellung	Standard
Aktivierte Module	Anti-Malware
Deaktivierte Module	Web Reputation
	Firewall
	Schutz vor Eindringlingen
	Überwachung der Integrität
	Inspektion von Protokollen

Einstellung	Standard
	Kontrolle von Anwendungen

Anti-Malware

Anti-Malware-Einstellungen für Endpoint Security.

Standardeinstellungen für EPS-Anti-Malware

Einstellung	Standard	Hinweise
Echtzeit-Scan	Alles scannen Jeden Day/All Tag (24 Stunden)	Alle verdächtigen Viren unter Quarantäne stellen. Aktivierung IntelliTrap und spyware/grayware Schutz. Spyware und Grayware lösen Anti-Malware aus und führen dazu, dass das Objekt unter Quarantäne gestellt wird.
Manueller Scan	Alles scannen	Muss angefordert werden, dann folgt die Standardkonfiguration für den Echtzeitscan.
Geplanter Scan	Alles scannen	Jeweils am letzten Sonntag im Monat, 6 Uhr morgens, festgelegt.
Intelligenter Schutz	Disabled	N/A

Einstellung	Standard	Hinweise
Dateien in Quarantäne	Trend Micro Deep Security Manager (DSM)	Etwa 1 GB Festplatte ist für die Quarantäne reserviert.
Scan-Beschränkung	Trend Micro DSM	Dateien aller Größen scannen.
Erlaubte Spyware oder Grayware	Keine	N/A
Benachrichtigung über ein lokales Ereignis	Ja	N/A

Prozess zur Abwehr von Schadsoftware

AMS verwendet die Deep Security Platform (Anti-Malware-System) von Trend Micro, um Malware auf Ihren von AMS verwalteten Instances zu erkennen und darauf zu reagieren. Standardmäßig läuft der Trend Micro Detection Agent auf allen EC2 Amazon-Instances, einschließlich denen in den Shared Services und privaten Subnetzen, sowohl für Windows- als auch für Linux-Betriebssysteme. Das Anti-Malware-System ist mit der AMS-Überwachung verbunden, sodass bei jedem Malware-Fund ein Ereignis ausgelöst wird. Wenn es Auswirkungen auf den Kunden gibt, wird das Ereignis an den Incident-Management-Prozess weitergeleitet (weitere Informationen finden Sie unter [Reaktion auf AMS-Vorfälle](#)). Während AMS die Auswirkungen bewertet, werden Sie benachrichtigt und es wird versucht, die Auswirkungen zu mindern.

Die Definitionen von Trend Micro Anti-Malware werden automatisch aktualisiert, wenn Trend Micro Updates veröffentlicht.

Beim Onboarding der Anwendung geben Sie an, welche Aktion AMS ergreifen soll, wenn auf einer Instanz Malware gefunden wird:

- Stellen Sie sicher, dass die Datei in Quarantäne auf der Zulassungsliste steht, entfernen Sie sie aus der Quarantäne und geben Sie sie wieder im Dateisystem frei.
- Löschen Sie die Datei in Quarantäne und entfernen Sie sie aus der Instanz.
- Unterbrechen Sie die Instanz und ersetzen Sie sie. Die gesperrte Instanz steht Ihnen dann zur Verfügung, um sie für forensische Untersuchungen bereitzustellen.

Nach dem Onboarding der Anwendung:

- Wenn das Anti-Malware-System Malware auf einer Instance entdeckt, stellt AMS die Malware automatisch unter Quarantäne. Dies löst ein Ereignis und eine Folgeuntersuchung aus.
- AMS benachrichtigt Sie mit einer Servicebenachrichtigung über das Ereignis und beginnt mit der Ausführung der von Ihnen ausgewählten Standardmaßnahme zur Risikominderung.
- Wenn Sie keine Standardaktion ausgewählt haben, fragt AMS Sie, welche Maßnahme zu ergreifen ist. Nach Erhalt Ihrer Anweisungen führt AMS die ausgewählte Aktion aus und benachrichtigt Sie. AMS benachrichtigt Sie erneut, nachdem die Aktion abgeschlossen ist, einschließlich der Einzelheiten, die für die forensische Analyse erforderlich sind, falls zutreffend.

IDS und IPS in Trend Micro Deep Security aktivieren

Sie können verlangen, dass AMS die nicht standardmäßigen Funktionen Trend Micro Intrusion Detection System (IDS) und Intrusion Protection Systems (IPS) für Ihr Konto aktiviert.

Senden Sie dazu eine Aktualisierungsanfrage (Verwaltung | Andere | Andere | Update) und fügen Sie eine Liste mit E-Mail-Adressen für den Empfang von IDS- und IPS-Benachrichtigungen bei. Diese Adressen werden zu einem SNS-Thema in Ihrem Konto hinzugefügt, das AMS für Sie erstellt.

Note

AMS kann keinen Trend Micro Service hinzufügen, der unsere Fähigkeit, andere AMS-Dienste anzubieten, beeinträchtigen könnte.

Vollständige System-Malware-Scans

Der Payment Card Industry Data Security Standard (PCI DSS) erfordert vollständige System-Malware-Scans, die standardmäßig auf Ihrer von AMS verwalteten VPC aktiviert sind. Vollständige Systemscans sind so eingestellt, dass sie um 2 Uhr morgens (in der auf dem Server festgelegten Zeitzone) durchgeführt werden, da sie viel CPU verbrauchen. Vollständige Systemscans werden zusätzlich zu regulären Malware-Scans durchgeführt, die nicht viel CPU beanspruchen.

Es gibt einen neuen Management-Change-Typ (CT), Malware-Scans deaktivieren, mit dem Sie vollständige System-Malware-Scans deaktivieren können. Sie finden den CT unter Verwaltung | Host-Sicherheit | Vollständiger Systemscan | Klassifizierung deaktivieren, ID ändern ct-1pybwg08h8qsz.

Um Scans wieder zu aktivieren, verwenden Sie das CT Management | Other | Other | Update. Durch die Deaktivierung vollständiger Systemscans werden Ihre regulären Malware-Scans nicht deaktiviert.

Amazon Inspector-Sicherheit

Der Amazon Inspector-Service überwacht die Sicherheit Ihrer AMS-verwalteten Stacks. Amazon Inspector ist ein automatisierter Sicherheitsbewertungsservice, der dabei hilft, Sicherheits- und Compliance-Lücken in der bereitgestellten Infrastruktur zu identifizieren AWS. Mit den Sicherheitsbeurteilungen von Amazon Inspector können Sie Stacks automatisch auf Sicherheitslücken, Sicherheitslücken und Abweichungen von bewährten Methoden untersuchen, indem Sie Ihre EC2 Amazon-Instances auf unbeabsichtigten Netzwerkzugriff und Sicherheitslücken überprüfen. Nach der Durchführung einer Bewertung erstellt Amazon Inspector eine detaillierte Liste der Sicherheitsfeststellungen, die nach Schweregrad priorisiert sind. Amazon Inspector-Assessments werden als vordefinierte Regelpakete angeboten, die den gängigen bewährten Sicherheitsmethoden und Definitionen zugeordnet sind. Diese Regeln werden regelmäßig von AWS Sicherheitsforschern aktualisiert. Weitere Informationen zu Amazon Inspector finden Sie unter [Amazon Inspector](#).

AMS Amazon Inspector FAQs

- Ist Amazon Inspector standardmäßig auf meinen AMS-Konten installiert?

Nein. Amazon Inspector ist nicht Teil des standardmäßigen AMI-Builds oder der Workload-Erfassung.

- Wie greife ich auf Amazon Inspector zu und installiere es?

Reichen Sie einen RFC (Management | Other | Other | Create) ein, um den Kontozugriff und die Installation bei Inspector anzufordern. Das AMS-Betriebsteam ändert die ReadOnly Rolle Customer_ _Role, um Zugriff auf die Amazon Inspector Inspector-Konsole (ohne SSM-Zugriff) zu gewähren.

- Muss der Amazon Inspector Agent auf allen EC2 Amazon-Instances installiert sein, die ich bewerten möchte?

Nein, Amazon Inspector-Assessments mit dem Regelpaket zur Netzwerkerreichbarkeit können ohne einen Agenten für alle EC2 Amazon-Instances ausgeführt werden. Der Agent ist für Regelpakete zur Hostbewertung erforderlich. Weitere Informationen zur Agenteninstallation finden Sie unter [Amazon Inspector Agents installieren](#).

- Fallen für diesen Service zusätzliche Kosten an?

Ja. Die Preise von Amazon Inspector finden Sie auf der [Preisseite von Amazon Inspector](#).

- Was sind die Ergebnisse von Amazon Inspector?

Bei den Ergebnissen handelt es sich um potenzielle Sicherheitsprobleme, die bei der Bewertung des ausgewählten Bewertungsziels durch Amazon Inspector entdeckt wurden. Die Ergebnisse werden in der Amazon Inspector Inspector-Konsole oder in der API angezeigt und enthalten sowohl eine detaillierte Beschreibung der Sicherheitsprobleme als auch Empfehlungen zu deren Lösung.

- Sind Berichte über die Bewertung durch Amazon Inspector verfügbar?

Ja. Ein Bewertungsbericht ist ein Dokument mit Details zu den Testobjekten des Bewertungslaufs und den entsprechenden Ergebnissen. Die Ergebnisse Ihrer Bewertung werden als Standardberichte ausgegeben, die Sie erstellen und an Ihr Team weiterleiten können, um Abhilfemaßnahmen zu initiieren, mehr Auditdaten zur Compliance abzurufen oder zu Referenzzwecken zu speichern. Ein Amazon Inspector-Assessmentbericht kann für einen Bewertungslauf generiert werden, sobald dieser erfolgreich abgeschlossen wurde.

- Kann ich Tags verwenden, um die Stacks zu identifizieren, für die ich Amazon Inspector Inspector-Berichte ausführen möchte?

Ja.

- Haben AMS Operations-Teams Zugriff auf die Bewertungsergebnisse von Amazon Inspector?

Ja. Jeder, der Zugriff auf die Amazon Inspector Inspector-Konsole in AWS hat, kann Ergebnisse und Bewertungsberichte einsehen.

- Werden die AMS Operations-Teams auf der Grundlage der Ergebnisse der Amazon Inspector Inspector-Berichte Maßnahmen empfehlen oder Maßnahmen ergreifen?

Nein. Wenn Sie möchten, dass Änderungen auf der Grundlage der Ergebnisse des Amazon Inspector Inspector-Berichts vorgenommen werden, müssen Sie Änderungen über einen RFC (Management | Other | Other | Update) beantragen.

- Wird AMS benachrichtigt, wenn ich einen Amazon Inspector Inspector-Bericht erstelle?

Wenn Sie Zugriff auf Amazon Inspector anfordern, benachrichtigt der AMS-Operator, der den RFC ausführt, Ihren CSDM über die Anfrage.

Weitere Informationen finden Sie unter [Amazon Inspector FAQs](#).

Reaktion auf AMS-Vorfälle

AMS verwendet traditionelle bewährte Verfahren für das IT-Servicemanagement (ITSM), um den Service bei Bedarf so schnell wie möglich wiederherzustellen.

Wir bieten rund um die Uhr follow-the-sun Support über mehrere Betriebszentren auf der ganzen Welt, wobei engagierte Mitarbeiter die Dashboards und Warteschlangen für Zwischenfälle aktiv überwachen.

Unsere Betriebstechniker verwenden interne Tools zur Vorfallverfolgung, um Vorfälle zu identifizieren, zu protokollieren, zu kategorisieren, zu priorisieren, zu diagnostizieren, zu lösen und zu schließen und Ihnen über die AMS-Konsole oder über die API Updates zu all diesen Aktivitäten zur Verfügung zu stellen. Support Unsere Mitarbeiter, von denen viele Zeit in verschiedenen Technologieprofilen und Rollen im AWS Premium Support verbracht haben, nutzen eine Vielzahl interner Support Tools, um sie bei all diesen Aktivitäten zu unterstützen. Diese Mitarbeiter sind mit den von AMS unterstützten Infrastrukturen bestens vertraut und verfügen über technische Fähigkeiten auf Expertenniveau, um alle identifizierten Support-Probleme zu lösen. In den seltenen Fällen, in denen unsere Mitarbeiter Unterstützung benötigen, stehen die Premium Support- und AWS Serviceteams bei Bedarf zur Verfügung.

In Fällen, in denen sich Vorfälle mit hoher Priorität auf Ihre kritischen Workloads auswirken, empfiehlt AMS eine Wiederherstellung der Infrastruktur. Oft besteht ein Kompromiss zwischen der Behebung eines Problems oder der Wiederherstellung anhand eines zweifelsfrei funktionierenden Backups. Dabei sind Kundenrisiken und Auswirkungen von Serviceausfällen ausschlaggebend. Wenn Sie Zeit haben, sich der Problembehebung zu widmen, hilft Ihnen AMS, aber wenn die Wiederherstellung dringend ist, können wir sofort eine Wiederherstellung einleiten.

Note

Kurzlebige Daten, die nicht Teil der Stack-Vorlage oder der Datenwiederherstellung sind, gehen verloren. AMS unternimmt angemessene Anstrengungen, um die Infrastruktur wiederherzustellen, solange keine AWS Serviceangebote verfügbar sind. Die Wiederherstellung der Infrastruktur ist abgeschlossen, sobald die AWS Serviceangebote verfügbar sind.

Wenn Sie eine Wiederherstellung der Infrastruktur nicht wie von AMS empfohlen autorisieren, haben Sie keinen Anspruch auf eine Servicegutschrift für die AMS-Serviceverpflichtung für die Zeit zur Behebung von Störungen.

Compliance-Validierung

AMS implementiert und verwaltet eine Bibliothek mit AWS Config Regeln und Abhilfemaßnahmen zum Schutz vor Fehlkonfigurationen, die die Sicherheit und Betriebsintegrität Ihrer Konten beeinträchtigen könnten.

Wenn beispielsweise ein Amazon S3 S3-Bucket erstellt wird, AWS Config kann der Amazon S3 S3-Bucket anhand einer Regel bewertet werden, nach der Amazon S3 S3-Buckets den öffentlichen Lesezugriff verweigern müssen. Wenn die Amazon S3 S3-Bucket-Richtlinie oder die Bucket Access Control List (ACL) öffentlichen Lesezugriff zulässt, werden sowohl AWS Config der Bucket als auch die Regel als nicht konform gekennzeichnet. Diese AWS-Config-Regeln kennzeichnen Ressourcen auf der Grundlage des Ergebnisses ihrer Bewertung entweder als konform, nicht konform oder nicht zutreffend. Weitere Informationen zum AWS Config Service finden Sie im [AWS Config Entwicklerhandbuch](#).

Sie können die AWS Config Konsole, AWS CLI oder AWS Config API verwenden, um die in Ihrem Konto bereitgestellten Regeln und den Konformitätsstatus Ihrer Regeln und Ressourcen einzusehen. Weitere Informationen finden Sie in der AWS Config Dokumentation: [Konfigurationskonformität anzeigen](#).

Note

Zusätzliche Informationen zu diesem Thema finden Sie in den AWS Artifact-Berichten. Weitere Informationen finden Sie unter [Herunterladen von Berichten in AWS Artifact](#). Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact. Diese Informationen sind nicht in diesem Benutzerhandbuch enthalten, da sie sensible Sicherheitsinhalte enthalten.

Die Landing Zone für mehrere Konten zeigt den Compliance-Status Ihres AWS-Config-Regeln

Die AMS-Landingzone für mehrere Konten nutzt den AWS Config Aggregator-Service, um eine zentrale Übersicht über die Einhaltung der Vorschriften für all Ihre Konten zu erstellen. Das bedeutet, dass Sie den Compliance-Status Ihrer AWS-Config-Regeln gesamten AMS-Landingzone-Umgebung mit mehreren Konten unter dem AWS Config Aggregator in Ihrem Sicherheitskonto einsehen können.

Im Folgenden finden Sie ein Beispiel für den AWS Config Aggregator, der den zentralen Compliance-Status aller Konten zeigt. AWS-Config-Regeln

Weitere Informationen finden Sie in der AWS-Dokumentation für [Config Aggregator](#).

- Wie verwendet AMS die AWS Config-Regeln?

AMS erstellt AWS-Config-Regeln, um Einblick in die Konfiguration Ihrer AWS Ressourcen unter Berücksichtigung der in den Regeln festgelegten Bedingungen zu geben. Wenn eine Regel nicht konform ist, können Sie eine Änderung beantragen, und das AMS Ops-Team wird mit Ihnen zusammenarbeiten, um Abhilfemaßnahmen zu ergreifen.

- In diesem Fall werden die folgenden Änderungen in Ihren AMS-Konten angezeigt:
 - AWS-Config-Regeln unter AWS Config > Regeln
 - Benutzerdefinierte Konfigurationsregeln mit ihren Lambda-Funktionen sind in Ihrem Konto vorhanden
 - Aggregator im Sicherheitskonto konfigurieren und Autorisierung konfigurieren in allen Konten (nur Landing Zone für mehrere Konten)

Im Folgenden finden Sie ein Beispiel AWS-Config-Regeln und die Ergebnisse der Konformitätsbewertung sind unten aufgeführt:

Weitere Informationen zu AWS Config finden Sie unter:

- AWS Config: [Was ist Config?](#)
- AWS Config Rules: [Ressourcen anhand von Regeln auswerten](#)
- AWS-Konfigurationsregeln: [Dynamische Konformitätsprüfung: AWS-Konfigurationsregeln — Dynamische Konformitätsprüfung für Cloud-Ressourcen](#)
- AWS Config Aggregator: Datenaggregation [mit mehreren Konten und mehreren Regionen](#)

Einschränkungen der Richtlinien für die Kontrolle des AMS-Landezonendienstes für mehrere Konten

Dieser Abschnitt wurde redigiert, da er sensible AMS-Sicherheitsinformationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen,

können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

Ausfallsicherheit

Die AWS globale Infrastruktur basiert auf AWS-Regionen Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Sicherheit der Infrastruktur

Note

Zusätzliche Informationen zu diesem Thema finden Sie in den AWS Artifact-Berichten. Weitere Informationen finden Sie unter [Herunterladen von Berichten in AWS Artifact](#). Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact. Diese Informationen sind nicht in diesem Benutzerhandbuch enthalten, da sie sensible Sicherheitsinhalte enthalten.

Sicherheitskontrolle für end-of-support Betriebssysteme

Betriebssysteme, die außerhalb des allgemeinen Supportzeitraums von "end-of-support" oder EOS des Betriebssystemherstellers liegen und keine Sicherheitsupdates erhalten, bergen ein erhöhtes Sicherheitsrisiko.

AWS bietet einige Dienste an, die bei der Handhabung des Betriebssystems helfen end-of-support. Informationen zu Windows end-of-support finden Sie unter [End-of-SupportMigrationsprogramm für Windows Server](#).

 Note

Zusätzliche Informationen zu diesem Thema finden Sie in den AWS Artifact-Berichten. Weitere Informationen finden Sie unter [Herunterladen von Berichten in AWS Artifact](#). Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact. Diese Informationen sind nicht in diesem Benutzerhandbuch enthalten, da sie sensible Sicherheitsinhalte enthalten.

Verwenden von Sicherheitsgruppen

Eine Sicherheitsgruppe agiert als virtuelle Firewall, die den Datenverkehr für eine oder mehrere Instances steuert. AMS-Sicherheitsgruppen ermöglichen es Ihnen, Regeln für eingehenden und ausgehenden Datenverkehr auf Instanzebene festzulegen. Sie können eine Sicherheitsgruppe erstellen und Ressourcen in Ihrem AMS-Konto, EC2 Amazon-Instances, Amazon RDS-DB-Instances, Load Balancers, Deep Security Manager (DSM) -Replikationsinstanzen, EFS-Mount-Zielen und ElastiCache Clustern angeben, die der Sicherheitsgruppe zugeordnet werden sollen. Nach der Zuordnung wird der Datenverkehr zu oder von diesen Instances durch die in der Sicherheitsgruppe festgelegten Regeln eingeschränkt.

Weitere Informationen zur allgemeinen AWS-Sicherheit finden Sie unter [Bewährte Methoden für Sicherheit, Identität und Compliance](#) und [Amazon EC2 Security Groups für Linux-Instances](#).

AMS verfügt jetzt über eine Reihe von Änderungstypen für die Erstellung und Verwaltung von Sicherheitsgruppen:

- Bereitstellung | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Erstellen (ct-10xx2g2d7hc90)
- Verwaltung | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Löschen (ct-3cp96z7r065e4)
- Verwaltung | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Update (ct-3memthlcmvc1b)

Beispiele [finden](#) Sie unter Sicherheitsgruppen.

Sicherheitsgruppen

In AWS VPCs agieren AWS-Sicherheitsgruppen als virtuelle Firewalls und kontrollieren den Datenverkehr für einen oder mehrere Stacks (eine Instanz oder eine Reihe von Instances). Wenn ein Stack gestartet wird, wird er einer oder mehreren Sicherheitsgruppen zugeordnet, die festlegen, welcher Datenverkehr ihn erreichen darf:

- Für Stacks in Ihren öffentlichen Subnetzen akzeptieren die Standardsicherheitsgruppen Traffic von HTTP (80) und HTTPS (443) von allen Standorten (dem Internet). Die Stacks akzeptieren auch internen SSH- und RDP-Verkehr aus Ihrem Unternehmensnetzwerk und AWS-Bastionen. Diese Stacks können dann über jeden beliebigen Port ins Internet gelangen. Sie können auch in Ihre privaten Subnetze und andere Stacks in Ihrem öffentlichen Subnetz gelangen.
- Stacks in Ihren privaten Subnetzen können zu jedem anderen Stack in Ihrem privaten Subnetz austreten, und Instances innerhalb eines Stacks können vollständig über jedes Protokoll miteinander kommunizieren.

Important

Die Standardsicherheitsgruppe für Stacks in privaten Subnetzen ermöglicht es allen Stacks in Ihrem privaten Subnetz, mit anderen Stacks in diesem privaten Subnetz zu kommunizieren. Wenn Sie die Kommunikation zwischen Stacks innerhalb eines privaten Subnetzes einschränken möchten, müssen Sie neue Sicherheitsgruppen erstellen, die die Einschränkung beschreiben. Wenn Sie beispielsweise die Kommunikation mit einem Datenbankserver einschränken möchten, sodass die Stacks in diesem privaten Subnetz nur von einem bestimmten Anwendungsserver über einen bestimmten Port kommunizieren können, fordern Sie eine spezielle Sicherheitsgruppe an. Wie das geht, wird in diesem Abschnitt beschrieben.

Standardsicherheitsgruppen

MALZ

In der folgenden Tabelle werden die Standardeinstellungen für eingehende Sicherheitsgruppen (SG) für Ihre Stacks beschrieben. Die SG trägt den Namen „SentinelDefaultSecurityGroupPrivateOnly-VPC-ID“, wobei **ID** es sich um eine VPC-ID in Ihrem AMS-Landingzone-Konto mit mehreren Konten handelt. Der gesamte Datenverkehr darf über diese Sicherheitsgruppe nach "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" ausgehen (der gesamte lokale Verkehr innerhalb von Stack-Subnetzen ist zulässig).

Jeglicher Datenverkehr darf von einer zweiten Sicherheitsgruppe "" nach 0.0.0.0/0 ausgehen. SentinelDefaultSecurityGroupPrivateOnly

Tip

Wenn Sie eine Sicherheitsgruppe für einen AMS-Änderungstyp wie EC2 Create oder OpenSearch Create Domain auswählen, würden Sie eine der hier beschriebenen Standardsicherheitsgruppen oder eine von Ihnen erstellte Sicherheitsgruppe verwenden. Sie finden die Liste der Sicherheitsgruppen pro VPC entweder in der EC2 AWS-Konsole oder in der VPC-Konsole.

Es gibt zusätzliche Standardsicherheitsgruppen, die für interne AMS-Zwecke verwendet werden.

AMS-Standardsicherheitsgruppen (eingehender Verkehr)

Typ	Protocol (Protokoll)	Port-Bereich	Quelle
Gesamter Datenverkehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnly (schränkt ausgehenden Datenverkehr auf Mitglieder derselben Sicherheitsgruppe ein)
Gesamter Datenverkehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (schränkt ausgehenden Verkehr nicht ein)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Quelle 0.0.0.0/0) SSH- und RDP-Zugriff ist von Bastionen aus erlaubt	SentinelDefaultSecurityGroupPublic (schränkt den ausgehenden Verkehr nicht ein)
MALZ-Bastionen:			
SSH	TCP	22	SharedServices VPC CIDR und DMZ VPC CIDR sowie vom Kunden bereitgestelltes On-Premise-System CIDRs
SSH	TCP	22	
RDP	TCP	3389	

Typ	Protocol (Protokol I)	Port-Bereich	Quelle
RDP	TCP	3389	

SALZ-Bastionen:

SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- SG WindowsBastion
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

SALZ

In der folgenden Tabelle werden die Standardeinstellungen für eingehende Sicherheitsgruppen (Inbound Security Group, SG) für Ihre Stacks beschrieben. Die SG trägt den Namen "mc-initial-garden- SentinelDefaultSecurityGroupPrivateOnly -*ID*", wobei *ID* es sich um einen eindeutigen Bezeichner handelt. Der gesamte Datenverkehr darf über diese Sicherheitsgruppe nach "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" ausgehen (der gesamte lokale Verkehr innerhalb von Stack-Subnetzen ist zulässig).

Der gesamte Datenverkehr darf von einer zweiten Sicherheitsgruppe "- -" nach 0.0.0.0/0 ausgesendet werden. mc-initial-garden SentinelDefaultSecurityGroupPrivateOnlyEgressAll *ID*

Tip

Wenn Sie eine Sicherheitsgruppe für einen AMS-Änderungstyp wie EC2 Create oder OpenSearch Create Domain auswählen, würden Sie eine der hier beschriebenen Standardsicherheitsgruppen oder eine von Ihnen erstellte Sicherheitsgruppe verwenden. Sie finden die Liste der Sicherheitsgruppen pro VPC entweder in der EC2 AWS-Konsole oder in der VPC-Konsole.

Es gibt zusätzliche Standardsicherheitsgruppen, die für interne AMS-Zwecke verwendet werden.

AMS-Standardsicherheitsgruppen (eingehender Verkehr)

Typ	Protocol (Protokol l)	Port-Bereich	Quelle
Gesamter Datenverl ehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnly (schränkt ausgehenden Datenverkehr auf Mitglieder derselben Sicherheitsgruppe ein)
Gesamter Datenverl ehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (schränkt ausgehenden Verkehr nicht ein)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Quelle 0.0.0.0/0) SSH- und RDP- Zugriff ist von Bastionen aus erlaubt	SentinelDefaultSecurityGroupPublic (schränkt den ausgehenden Verkehr nicht ein)
MALZ-Bastionen:			
SSH	TCP	22	SharedServices VPC CIDR und DMZ VPC CIDR sowie vom Kunden bereitgestelltes On-Premise- System CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ-Bastionen:			
SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- SG WindowsBastion
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

Sicherheitsgruppen erstellen, ändern oder löschen

Sie können benutzerdefinierte Sicherheitsgruppen anfordern. In Fällen, in denen die Standardsicherheitsgruppen nicht den Anforderungen Ihrer Anwendungen oder Ihrer Organisation entsprechen, können Sie neue Sicherheitsgruppen ändern oder erstellen. Eine solche Anfrage würde als genehmigungspflichtig erachtet und vom AMS-Betriebsteam geprüft.

Um eine Sicherheitsgruppe außerhalb von Stacks zu erstellen und einen RFC mit dem Deployment | Advanced stack components | Security group | Create (review required) Änderungstyp (VPCsct-1oxx2g2d7hc90) einzureichen.

Verwenden Sie für Änderungen an Active Directory (AD) -Sicherheitsgruppen die folgenden Änderungstypen:

- Um einen Benutzer hinzuzufügen: Senden Sie einen RFC mit Management | Directory Service | Benutzer und Gruppen | Benutzer zur Gruppe hinzufügen [ct-24pi85mjtza8k]
- Um einen Benutzer zu entfernen: Senden Sie einen RFC mit Management | Directory Service | Benutzer und Gruppen | Benutzer aus Gruppe entfernen [ct-2019s9y3nfml4]

Note

Wenn Sie „Überprüfung erforderlich“ verwenden CTs, empfiehlt AMS, die ASAP-Scheduling-Option zu verwenden (wählen Sie ASAP in der Konsole, lassen Sie Start- und Endzeit leer in der API/CLI), da diese einen AMS-Operator CTs erfordern, der den RFC überprüft und möglicherweise mit Ihnen kommuniziert, bevor er genehmigt und ausgeführt werden kann. Wenn Sie diese einplanen, achten Sie darauf RFCs, dass Sie mindestens 24 Stunden einplanen. Wenn die Genehmigung nicht vor der geplanten Startzeit erfolgt, wird der RFC automatisch abgelehnt.

Suchen Sie nach Sicherheitsgruppen

Verwenden Sie die EC2 Konsole, um die Sicherheitsgruppen zu finden, die einem Stack oder einer Instance zugeordnet sind. Nachdem Sie den Stack oder die Instance gefunden haben, können Sie alle damit verbundenen Sicherheitsgruppen sehen.

Möglichkeiten, Sicherheitsgruppen in der Befehlszeile zu finden und die Ausgabe zu filtern, finden Sie unter [describe-security-groups](#).

AMS-Bibliothek für präventive und detektive Kontrollen

AWS Managed Services (AMS) bietet Ihnen eine Auswahl an bewährten Service-Kontrollrichtlinien (SCPs), die Sie nutzen können ConfigRules , um Ihre Sicherheitslage zu verbessern und Compliance-Lücken in Ihren AMS-Konten zu verringern. [library/catalog](#)

Themen

- [Kuratierte Regeln SCPs und Konfigurationsregeln](#)
- [Benutzerdefinierte Benachrichtigung für Config-Regeln](#)

Kuratierte Regeln SCPs und Konfigurationsregeln

Kuratierte Regeln SCPs und Konfigurationsregeln für AMS Advanced.

- Richtlinien zur Dienststeuerung (SCPs): Die bereitgestellten Richtlinien SCPs gelten zusätzlich zu den AMS-Standardrichtlinien.

Sie können diese Bibliothekssteuerungen zusammen mit den Standardsteuerungen verwenden, um bestimmte Sicherheitsanforderungen zu erfüllen.

- Konfigurationsregeln: Als Basismaßnahme empfiehlt AMS, zusätzlich zu den standardmäßigen AMS-Konfigurationsregeln (Standardregeln unter AMS-Artefakte) [Conformance Packs](#) (siehe Conformance Packs im AWS Config Handbuch) anzuwenden. Die Conformance Packs decken einen Großteil der Compliance-Anforderungen ab und werden von AWS regelmäßig aktualisiert.

Die hier aufgeführten Regeln können verwendet werden, um anwendungsfallspezifische Lücken zu schließen, die nicht durch Conformance Packs abgedeckt werden

Note

Da die AMS-Standardregeln und Konformitätspakete im Laufe der Zeit aktualisiert werden, werden Sie möglicherweise Duplikate dieser Regeln sehen.

AMS empfiehlt generell, doppelte Konfigurationsregeln regelmäßig zu bereinigen.

Für AMS Advanced sollten Config Rules keine automatischen Korrekturen verwenden

(siehe [Behebung nicht konformer AWS-Ressourcen durch AWS-Konfigurationsregeln](#)), um Änderungen zu vermeiden. out-of-band

SCP-AMS-001: Beschränken Sie die EBS-Erstellung

Verhindern Sie die Erstellung von EBS-Volumes, wenn Sie die Verschlüsselung nicht aktiviert haben.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002: Schränkt den Start ein EC2

Verhindern Sie den Start einer EC2 Instance, wenn das EBS-Volume unverschlüsselt ist. Dazu gehört auch, dass ein unverschlüsselter EC2 Start verweigert wird, AMIs da dieser SCP auch für Root-Volumes gilt.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Effect": "Deny"
}
```

SCP-ADV-001: RFC-Einreichungen einschränken

Schränken Sie die Übermittlung bestimmter automatisierter Funktionen RFCs wie Create VPC oder Delete VPC ein. Dies ist hilfreich, wenn Sie detailliertere Berechtigungen auf Ihre Verbundrollen anwenden möchten.

Sie möchten beispielsweise, dass standardmäßig `AWSTransferManagement` Rolle die meisten verfügbaren Daten übermittelt werden können, RFCs mit Ausnahme derjenigen, die das Erstellen und Löschen einer VPC, das Erstellen zusätzlicher Subnetze, das Offboarding eines Anwendungskontos, das Aktualisieren oder Löschen von SAML-Identitätsanbietern ermöglichen:

SCP-AMS-003: Schränkt die Erstellung von RDS in AMS ein EC2

Verhindern Sie die Erstellung von Amazon EC2 - und RDS-Instances, die keine spezifischen Tags haben, und lassen Sie dies gleichzeitig der AMS Backup IAM AMS-Standardrolle zu. Dies ist für Disaster Recovery oder DR erforderlich.

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam:*:<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

SCP-AMS-004: S3-Uploads einschränken

Verhindert das Hochladen unverschlüsselter S3-Objekte.

```
{
  "Sid": "DenyUnencryptedS3Uploads",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
    }
  },
}
```

```
        "Null": {
            "s3:x-amz-server-side-encryption": "false"
        }
    }
}
```

SCP-AMS-005: Beschränken Sie den API- und Konsolenzugriff

Verhindern Sie als Kunde den Zugriff auf AWS-Konsole und API für Anfragen, die von bekannten schlechten IP-Adressen kommen InfoSec.

SCP-AMS-006: Verhindert, dass die IAM-Entität das Mitgliedskonto aus der Organisation entfernt

Verhindern Sie, dass eine AWS Identity and Access Management Entität Mitgliedskonten aus der Organisation entfernt.

```
{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}
```

SCP-AMS-007: Verhindern Sie die gemeinsame Nutzung von Ressourcen mit Konten außerhalb Ihrer Organisation

Verhindern Sie die gemeinsame Nutzung von Ressourcen mit externen Konten außerhalb Ihrer AWS Organisation

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "Bool": {
```

```

        "ram:AllowsExternalPrincipals": "true"
    }
}
},
{
    "Effect": "Deny",
    "Action": [
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
        "Bool": {
            "ram:RequestedAllowsExternalPrincipals": "true"
        }
    }
}
}

```

SCP-AMS-008: Verhindern Sie die gemeinsame Nutzung mit Organisationen oder Organisationseinheiten () OUs

Verhindern Sie die gemeinsame Nutzung von Ressourcen mit einer and/or Account-Organisationseinheit, die sich in einer Organisation befindet.

```

{
    "Effect": "Deny",
    "Action": [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringLike": {
            "ram:Principal": [
                "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
                "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
            ]
        }
    }
}
}

```

SCP-AMS-009: Hindert Benutzer daran, Einladungen zur gemeinsamen Nutzung von Ressourcen anzunehmen

Verhindern Sie, dass Mitgliedskonten Einladungen AWS RAM zum Beitritt zu Resource Shares annehmen. Diese API unterstützt keine Bedingungen und verhindert, dass Inhalte nur von externen Konten geteilt werden.

```
{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}
```

SCP-AMS-010: Aktionen zur Aktivierung und Deaktivierung der Kontoregion verhindern

Verhindern Sie die Aktivierung oder Deaktivierung neuer AWS Regionen für Ihre AWS Konten.

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011: Aktionen zur Änderung der Abrechnung verhindern

Vermeiden Sie Änderungen an der Abrechnungs- und Zahlungskonfiguration.

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

SCP-AMS-012: Verhindert das Löschen oder Ändern bestimmter CloudTrails

Verhindern Sie Änderungen an bestimmten AWS CloudTrail Pfaden.

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:PutInsightSelectors",
    "cloudtrail:UpdateEventDataStore",
    "cloudtrail:UpdateTrail",
    "cloudtrail:StopLogging"
  ],
  "Resource": [
    "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
  ]
}
```

SCP-AMS-013: Verhindert die Deaktivierung der Standard-EBS-Verschlüsselung

Verhindern Sie die Deaktivierung der standardmäßigen Amazon EBS-Verschlüsselung.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP-AMS-014: Das Erstellen einer Standard-VPC und eines Subnetzes verhindern

Verhindern Sie die Erstellung einer standardmäßigen Amazon-VPC und von Subnetzen.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc"
  ],
}
```

```
"Resource": "*"
}
```

SCP-AMS-015: Verhindert das Deaktivieren und Ändern GuardDuty

Verhindern Sie, dass Amazon GuardDuty geändert oder deaktiviert wird.

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
  ]
}
```



```
"guardduty:UpdateThreatIntelSet"
],
"Resource": "*"
}
```

SCP-AMS-016: Root-Benutzeraktivitäten verhindern

Verhindern Sie, dass der Root-Benutzer eine Aktion ausführt.

```
{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:root"
      ]
    }
  }
}
```

SCP-AMS-017: Verhindert die Erstellung von Zugriffsschlüsseln für den Root-Benutzer

Verhindern Sie die Erstellung von Zugriffsschlüsseln für den Root-Benutzer.

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018: Verhindert die Deaktivierung der Sperrung des öffentlichen Zugriffs auf das S3-Konto

Verhindern Sie, dass der öffentliche Zugriff auf ein Amazon S3 S3-Konto gesperrt wird. Dadurch wird verhindert, dass ein Bucket im Konto veröffentlicht wird.

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```

```
}
```

SCP-AMS-019: Verhindern, dass AWS Config deaktiviert oder Config-Regeln geändert werden

Verhindern Sie das Deaktivieren oder Ändern von AWS Config Regeln.

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",
    "config:StopConfigurationRecorder"
  ],
  "Resource": "*"
}
```

SCP-AMS-020: Alle IAM-Aktionen verhindern

Alle IAM-Aktionen verhindern.

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021: Verhindert das Löschen von Log-Gruppen und Streams CloudWatch

Verhindern Sie das Löschen von Amazon CloudWatch Logs-Gruppen und -Streams.

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": "*"
}
```

```
}
```

SCP-AMS-022: Das Löschen von Glacier verhindern

Verhindern Sie das Löschen von Amazon Glacier.

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

SCP-AMS-023: Das Löschen von IAM Access Analyzer verhindern

Verhindern Sie das Löschen von IAM Access Analyzer.

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024: Änderungen am Security Hub verhindern

Verhindern Sie das Löschen von AWS Security Hub CSPM.

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-025: Löschen unter Directory Service verhindern

Verhindern Sie das Löschen von Ressourcen unter Directory Service.

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",
    "ds:DisableSso",
    "ds:UnshareDirectory"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-026: Die Nutzung eines Dienstes auf der Denylist verhindern

Verhindern Sie die Nutzung von Diensten, die auf der Liste stehen.

Note

Ersetzen Sie *service1* und *service2* durch Ihre Dienstnamen. Beispiel *access-analyzer* oder *IAM*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:*"]
}
```

SCP-AMS-027: Verhindert die Nutzung von Diensten, die auf der Liste stehen, in bestimmten Regionen

Verhindern Sie die Nutzung von Diensten, die auf der Liste stehen, in bestimmten Regionen. AWS

 Note

Ersetzen Sie *service1* und *service2* durch Ihre Dienstnamen. Beispiel *access-analyzer* oder *IAM*.

Ersetzen Sie *region1* und *region2* durch Ihre Dienstnamen. Beispiel *us-west-2* oder *use-east-1*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"],
  "Condition": {
    "StringEquals": {
      "aws:RequestedRegion": [
        "region1",
        "region2"
      ]
    }
  }
}
```

SCP-AMS-028: Verhindert, dass Tags geändert werden, außer durch autorisierte Principals

Verhindern Sie, dass Tag-Änderungen durch alle Benutzer außer den autorisierten Hauptbenutzern vorgenommen werden. Verwenden Sie Autorisierungs-Tags, um Principals zu autorisieren.

Autorisierungs-Tags müssen Ressourcen und Prinzipalen zugeordnet sein. A user/role gilt nur dann als autorisiert, wenn das Tag sowohl auf der Ressource als auch auf dem Prinzipal übereinstimmt.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- [Sicherung von Ressourcen-Tags, die für die Autorisierung verwendet werden, mithilfe einer Dienststeuerungsrichtlinie in AWS Organizations](#)
- [Verhindern Sie, dass Tags nur von autorisierten Prinzipalen geändert werden](#)

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ]
}
```

```
],
"Resource": [
  "*"
],
"Condition": {
  "StringNotEquals": {
    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
    "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
  },
  "Null": {
    "ec2:ResourceTag/access-project": false
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
        "access-project"
      ]
    }
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
    "*"
  ],
}
```

```
"Condition": {
  "StringNotEquals": {
    "aws:PrincipalArn": "arn:aws:iam::{{ACCOUNT_ID}}:{{RESOURCE_TYPE}}/{{RESOURCE_NAME}}"
  },
  "Null": {
    "aws:PrincipalTag/access-project": true
  }
}
```

SCP-AMS-029: Benutzer daran hindern, Amazon VPC Flow Logs zu löschen

Verhindern Sie das Löschen von Amazon VPC Flow Logs.

```
{
  "Action": [
    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-030: Die gemeinsame Nutzung des VPC-Subnetzes mit einem anderen Konto als dem Netzwerkkonto verhindern

Vermeiden Sie die gemeinsame Nutzung von Amazon VPC-Subnetzen mit anderen Konten als dem Netzwerkkonto.

Note

Ersetzen Sie es *NETWORK_ACCOUNT_ID* durch Ihre Netzwerkkonto-ID.

```
{
```

```

"Effect": "Deny",
"Action": [
  "ram:AssociateResourceShare",
  "ram:CreateResourceShare"
],
"Resource": "*",
"Condition": {
  "StringNotEquals": {
    "ram:Principal": "NETWORK_ACCOUNT_ID"
  },
  "StringEquals": {
    "ram:RequestedResourceType": "ec2:Subnet"
  }
}
}

```

SCP-AMS-031: Verhindert das Starten von Instances mit verbotenen Instanztypen

Verhindern Sie das Starten verbotener EC2 Amazon-Instance-Typen.

Note

Ersetzen Sie *instance_type1* und *instance_type2* durch die Instance-Typen, die Sie einschränken möchten, z. B. *t2.micro* oder durch eine Platzhalterzeichenfolge wie. **.nano*

```

{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}

```


SCP-AMS-032: Verhindert das Starten von Instanzen ohne IMDSv2

Vermeiden Sie EC2 Amazon-Instances ohne IMDSv2.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]
```

SCP-AMS-033: Verhindert Änderungen an einer bestimmten IAM-Rolle

Verhindern Sie Änderungen an bestimmten IAM-Rollen.

```
{
  "Action": [
    "iam:AttachRolePolicy",
    "iam:DeleteRole",
    "iam:DeleteRolePermissionsBoundary",
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}
```

SCP-AMS-034: Verhindert Änderungen an bestimmten IAM-Rollen AssumeRolePolicy

Verhindert Änderungen an den vier AssumeRolePolicy angegebenen IAM-Rollen.

```
{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}
```

ConfigRule: Erforderliche Tags

Prüfen Sie, ob EC2 Instanzen über benutzerdefinierte Tags verfügen, die Sie benötigt haben. Darüber hinaus ist dies auch nützlich für Ihr Kostenmanagement InfoSec

```
ConfigRuleName: required-tags
  Description: >-
    A Config rule that checks whether EC2 instances have the required tags.
  Scope:
    ComplianceResourceTypes:
      - 'AWS::EC2::Instance'
  InputParameters:
    tag1Key: COST_CENTER
    tag2Key: APP_ID
  Source:
    Owner: AWS
    SourceIdentifier: REQUIRED_TAGS
```

ConfigRule: Zugriffstaste gedreht

Vergewissern Sie sich, dass die Zugriffsschlüssel innerhalb des angegebenen Zeitraums rotiert werden. In der Regel sind dies 90 Tage gemäß den typischen Compliance-Anforderungen.

```
ConfigRuleName: access-keys-rotated
  Description: >-
    A config rule that checks whether the active access keys are rotated
    within the number of days specified in maxAccessKeyAge. The rule is
    NON_COMPLIANT if the access keys have not been rotated for more than
    maxAccessKeyAge number of days.
  InputParameters:
    maxAccessKeyAge: '90'
  Source:
    Owner: AWS
    SourceIdentifier: ACCESS_KEYS_ROTATED
    MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: IAM-Root-Zugriffsschlüssel in AMS

Stellen Sie sicher, dass in einem Konto kein Root-Zugriffsschlüssel vorhanden ist. Bei AMS Advanced-Konten wird davon ausgegangen, dass dies konform ist out-of-the-box.

```
ConfigRuleName: iam-root-access-key-check
  Description: >-
    A config rule that checks whether the root user access key is available. The
    rule is COMPLIANT if the user access key does not exist.
  Source:
    Owner: AWS
```

```
SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: SSM verwaltet EC2

Vergewissern Sie EC2s sich, dass Sie von SSM Systems Manager verwaltet werden.

```
ConfigRuleName: ec2-instance-managed-by-systems-manager
Description: >-
  A Config rule that checks whether the EC2 instances in the
  account are managed by AWS Systems Manager.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
    - 'AWS::SSM::ManagedInstanceInventory'
Source:
  Owner: AWS
  SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule: Ungenutzter IAM-Benutzer in AMS

Sucht nach IAM-Benutzeranmeldedaten, die für einen bestimmten Zeitraum nicht verwendet wurden. Wie bei der Schlüsselrotationsprüfung werden auch hier in der Regel 90 Tage für typische Compliance-Anforderungen vorgegeben.

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: S3-Bucket-Protokollierung

Vergewissern Sie sich, dass die Protokollierung für S3-Buckets im Konto aktiviert wurde.

```
ConfigRuleName: s3-bucket-logging-enabled
```

Description: >-

A Config rule that checks whether logging is enabled for S3 buckets.

Scope:

ComplianceResourceTypes:

- 'AWS::S3::Bucket'

Source:

Owner: AWS

SourceIdentifier: S3_BUCKET_LOGGING_ENABLED

ConfigRule: Versionierung von S3-Buckets

Vergewissern Sie sich, dass Versionierung und MFA-Delete (optional) für alle S3-Buckets aktiviert sind

ConfigRuleName: s3-bucket-versioning-enabled

Description: >-

A Config rule that checks whether versioning is enabled for S3 buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.

Scope:

ComplianceResourceTypes:

- 'AWS::S3::Bucket'

Source:

Owner: AWS

SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED

ConfigRule: Öffentlicher S3-Zugriff

Vergewissern Sie sich, dass die Einstellungen für den öffentlichen Zugriff (Public ACL, Public Policy, Public Buckets) für das gesamte Konto eingeschränkt sind

ConfigRuleName: s3-account-level-public-access-blocks

Description: >-

A Config rule that checks whether the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item.

Scope:

ComplianceResourceTypes:

- 'AWS::S3::AccountPublicAccessBlock'

InputParameters:

IgnorePublicAcls: 'True'

BlockPublicPolicy: 'True'

BlockPublicAcls: 'True'

```
RestrictPublicBuckets: 'True'
Source:
  Owner: AWS
SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
```

ConfigRule: Nicht archivierte Ergebnisse GuardDuty

Suchen Sie nach nicht archivierten GuardDuty Ergebnissen, die älter als die angegebene Dauer sind. Die Standarddauer beträgt 30 Tage für Befunde mit niedriger Geschwindigkeit, 7 Tage für Ergebnisse mit mittlerer Geschwindigkeit und 1 Tag für Ergebnisse mit hoher Geschwindigkeit.

```
ConfigRuleName: guardduty-non-archived-findings
Description: >-
  A Config rule that checks whether the Amazon GuardDuty has findings that
  are non archived. The rule is NON_COMPLIANT if GuardDuty has non
  archived low/medium/high severity findings older than the specified number.
InputParameters:
  daysLowSev: '30'
  daysMediumSev: '7'
  daysHighSev: '1'
Source:
  Owner: AWS
  SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: CMK-Löschung

Suchen Sie nach AWS Key Management Service benutzerdefinierten Hauptschlüsseln (CMKs), deren Löschung geplant ist (auch bekannt als ausstehend). Dies ist von entscheidender Bedeutung, da Unwissenheit über das Löschen von CMK dazu führen kann, dass Daten nicht wiederhergestellt werden können

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
Description: >-
  A config rule that checks whether customer master keys (CMKs) are not
  scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
  NON_COMPLIANT if CMKs are scheduled for deletion.
Source:
  Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: CMK-Rotation

Vergewissern Sie sich, dass die automatische Rotation für jeden CMK im Konto aktiviert ist

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Benutzerdefinierte Benachrichtigung für Config-Regeln

Es kann vorkommen, dass kritische Konfigurationsregeln nicht eingehalten werden, sodass Sie Ihr Team InfoSec und das Führungsteam entsprechend sensibilisieren müssen. Für solche Szenarien empfiehlt AMS, eine benutzerdefinierte Benachrichtigung über Verstöße zu konfigurieren, die ereignisgesteuert werden.

Beispiel:

```
ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the mandated tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
Properties:
  Name: CWEventForrequired-tags
  Description: >-
    SNS Notification for Non-Compliant Events of Config Rule:
    required-tags
```

```
State: ENABLED
EventPattern:
  detail-type:
    - Config Rules Compliance Change
  source:
    - aws.config
  detail:
    newEvaluationResult:
      complianceType:
        - NON_COMPLIANT
    configRuleARN:
      - 'Fn::GetAtt':
          - RequiredEC2Tags
          - Arn
Targets:
  - Id: RemediationNotification
    Arn:
      Ref: SnsTopic
    InputTransformer:
      InputTemplate: >-
        "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
        COST_CENTER, APP_ID, Name, and Backup."
      InputPathsMap:
        instance_id: $.detail.resourceId
SnsTopic:
  Type: 'AWS::SNS::Topic'
  Properties:
    Subscription:
      - Endpoint: Cloud_Ops_Leaders@customer.com
        Protocol: email
    TopicName: noncompliant-instance-notification
SnsTopicPolicy:
  Type: 'AWS::SNS::TopicPolicy'
  Properties:
    PolicyDocument:
      Statement:
        - Sid: __default_statement_ID
          Effect: Allow
          Principal:
            AWS: '*'
          Action:
            - 'SNS:GetTopicAttributes'
            - 'SNS:SetTopicAttributes'
            - 'SNS:AddPermission'
```



```
- 'SNS:RemovePermission'
- 'SNS:DeleteTopic'
- 'SNS:Subscribe'
- 'SNS:ListSubscriptionsByTopic'
- 'SNS:Publish'
- 'SNS:Receive'
Resource:
  Ref: SnsTopic
Condition:
  StringEquals:
    'AWS:SourceOwner':
      Ref: 'AWS::AccountId'
- Sid: TrustCWEToPublishEventsToMyTopic
  Effect: Allow
  Principal:
    Service: events.amazonaws.com
  Action: 'sns:Publish'
  Resource:
    Ref: SnsTopic
Topics:
  - Ref: SnsTopic
```

Mit dem Amazon EventBridge Rule Service verknüpfte Rolle für AMS Advanced

AMS Advanced verwendet die serviceverknüpfte Rolle (SLR) mit dem Namen `AWSServiceRoleForManagedServices_Events`— Diese Rolle vertraut darauf, dass einer der AWS Managed Services Service Principals (`events.managedservices.amazonaws.com`) die Rolle für Sie übernimmt. Der Service EventBridge verwendet die Rolle, um eine verwaltete Regel zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem AWS Konto erforderlich ist, um Informationen zur Änderung des Alarmstatus von Ihrem Konto an AWS Managed Services zu übermitteln.

Berechtigungen für EventBridge SLR für AMS Advanced

Die serviceverknüpfte Rolle `AWSServiceRoleForManagedServices_Events` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `events.managedservices.amazonaws.com`

Dieser Rolle ist die `AWSManagedServices_EventsServiceRolePolicy` AWS verwaltete Richtlinie beigelegt (siehe [verwaltete AWS-Richtlinie: AWSManagedServices_EventsServiceRolePolicy](#)). Der Dienst verwendet die Rolle, um Informationen zur Änderung des Alarmstatus von Ihrem Konto

an AWS Managed Services zu übermitteln. Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Service-Linked Role Permissions](#) im AWS Identity and Access Management-Benutzerhandbuch.

Sie können die JSON-Datei `AWSServiceRoleForManagedServices_EventsServiceRolePolicy` in dieser ZIP-Datei herunterladen: [EventsServiceRolePolicy.zip](#).

Eine EventBridge Spiegelreflexkamera für AMS Advanced erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie in der AWS Management Console, der oder der AWS CLI AWS API bei AMS einsteigen, erstellt AMS Advanced die serviceverknüpfte Rolle für Sie.

 Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie den AMS Advanced-Service vor dem 7. Februar 2023 genutzt haben. Als er begann, serviceverknüpfte Rollen zu unterstützen, hat AMS Accelerate die `AWSServiceRoleForManagedServices_Events` Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter [In meinem IAM-Konto wird eine neue Rolle angezeigt](#).

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie bei AMS einsteigen, erstellt AMS Advanced die dienstbezogene Rolle erneut für Sie.

Eine EventBridge Spiegelreflexkamera für AMS Advanced bearbeiten

AMS Advanced erlaubt es Ihnen nicht, die `AWSServiceRoleForManagedServices_Events` serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer EventBridge Spiegelreflexkamera für AMS Advanced

Sie müssen die Rolle `AWSServiceRoleForManagedServices_Events` nicht manuell löschen. Wenn Sie in der AWS Management Console, der AWS CLI oder der AWS API ein Offboard von AMS

ausführen, bereinigt AMS Advanced die Ressourcen und löscht die mit dem Service verknüpfte Rolle für Sie.

Sie können die IAM-Konsole, die AWS CLI oder die AWS API auch verwenden, um die serviceverknüpfte Rolle manuell zu löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

Note

Wenn der AMS Advanced-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AMS Advanced-Ressourcen zu löschen, die von der `AWSServiceRoleForManagedServices_Events` serviceverknüpften Rolle verwendet werden

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die `AWSServiceRoleForManagedServices_Events` serviceverknüpfte Rolle zu löschen.

Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Bewährte Methoden für die Gewährleistung der Sicherheit

Dieser Abschnitt wurde redigiert, da er sensible AMS-Sicherheitsinformationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

Nicht standardmäßige EPS-Einstellungen für die AMS-Landingzone mit mehreren Konten

Dieser Abschnitt wurde redigiert, da er vertrauliche AMS-Sicherheitsinformationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

AMS-Leitplanken

Bei einer Guardrail handelt es sich um eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten AMS-Umgebung gewährleistet.

Dieser Abschnitt wurde redigiert, da er sensible AMS-Sicherheitsinformationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

Richtlinien zur Steuerung des MALZ-Service

Dieser Abschnitt wurde redigiert, da er sensible sicherheitsrelevante AMS-Informationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu [Erste Schritte mit AWS](#) Artifact.

Reaktion auf Sicherheitsvorfälle in AMS

Sicherheit hat bei AWS Managed Services (AMS) oberste Priorität. AMS stellt Ressourcen und Kontrollen in Ihren Konten bereit, um diese zu verwalten. AWS hat ein Modell der geteilten Verantwortung: AWS verwaltet die Sicherheit der Cloud, und Sie sind für die Sicherheit in der Cloud verantwortlich. AMS schützt Ihre Daten und Vermögenswerte und trägt dazu bei, Ihre AWS Infrastruktur zu schützen, indem es Sicherheitskontrollen einsetzt und Sicherheitsprobleme aktiv überwacht. Diese Funktionen helfen Ihnen dabei, eine Sicherheitsgrundlage für Anwendungen zu schaffen, die in der AWS Cloud ausgeführt werden. AMS arbeitet im Rahmen von Security Incident Response mit Ihnen zusammen, um die Auswirkungen zu bewerten und dann auf der Grundlage von Best-Practice-Empfehlungen Eindämmungs- und Abhilfemaßnahmen durchzuführen.

Wenn eine Abweichung vom Ausgangswert auftritt, z. B. durch eine Fehlkonfiguration oder eine Änderung externer Faktoren, müssen Sie reagieren und Nachforschungen anstellen. Um dies erfolgreich zu tun, müssen Sie die grundlegenden Konzepte der Reaktion auf Sicherheitsvorfälle in Ihrer AMS-Umgebung verstehen. Sie müssen auch die Anforderungen für die Vorbereitung, Schulung und Schulung von Cloud-Teams verstehen, bevor Sicherheitsprobleme auftreten. Es ist wichtig, die Kontrollen und Funktionen zu kennen, die Sie verwenden können, Reaktionspläne für häufig auftretende Sicherheitsprobleme wie die Kompromittierung von Benutzerkonten oder den Missbrauch privilegierter Konten zu erstellen und Abhilfemaßnahmen zu identifizieren, die mithilfe von

Automatisierung die Reaktionsgeschwindigkeit und Konsistenz verbessern. Darüber hinaus müssen Sie Ihre Compliance- und regulatorischen Anforderungen im Zusammenhang mit dem Aufbau eines Programms zur Reaktion auf Sicherheitsvorfälle zur Erfüllung dieser Anforderungen verstehen.

Die Reaktion auf Sicherheitsvorfälle kann komplex sein, aber durch die Implementierung eines iterativen Ansatzes können Sie den Prozess vereinfachen und es dem Incident-Response-Team ermöglichen, durch frühzeitige und kontinuierliche Erkennung und Reaktion alle Beteiligten zufrieden zu stellen. In diesem Leitfaden stellen wir Ihnen die Methodik vor, die AMS für die Reaktion auf Vorfälle verwendet, die AMS Responsibility Matrix (RACI), wie Sie sich auf ein Sicherheitsereignis vorbereiten können, wie Sie AMS bei Sicherheitsvorfällen einbeziehen können, und einige der von AMS verwendeten Runbooks zur Reaktion auf Vorfälle.

So funktioniert AMS Security Incident Response

AWS Managed Services entspricht dem NIST 800-61 [Leitfaden zur Behandlung von Sicherheitsvorfällen für die Reaktion auf](#) Sicherheitsvorfälle. Durch die Ausrichtung an diesem Industriestandard bieten wir einen konsistenten Ansatz für das Management von Sicherheitsereignissen und halten uns an bewährte Verfahren bei der Sicherung und Reaktion auf Sicherheitsvorfälle in Ihrer Cloud.

Lebenszyklus der Reaktion auf Vorfälle

Wenn die Erkennung eine Sicherheitswarnung identifiziert und generiert oder Sie Sicherheitsunterstützung anfordern, stellt das AWS Managed Services Operations Team sicher, dass eine zeitnahe Untersuchung stattfindet, führt Automatisierungen zur Datenerfassung, Triage und Analyse durch, informiert Sie über die Analyse, führt Untersuchungen und alle Eindämmungsaktivitäten durch und veröffentlicht dann die Ereignisanalyse.

Die während der Reaktion auf den Vorfall durchgeführten Aktivitäten zur Erfassung, Auswertung, Analyse und Eindämmung von Daten variieren je nach Art des untersuchten Sicherheitsereignisses. Beispiele für Workflows zur Reaktion auf Sicherheitsvorfälle für ausgewählte Szenarien finden Sie am Ende dieses Dokuments.

Bei Vorfällen bestimmt AMS dynamisch die richtige Vorgehensweise, was dazu führen kann, dass dokumentierte Schritte gegebenenfalls neu angeordnet oder umgangen werden, um sicherzustellen, dass das richtige Ergebnis eintritt.

Vorbereitung

Im Zuge der Weiterentwicklung der Bedrohungslandschaft erweitert AMS kontinuierlich die Erkennungs- und Reaktionsmöglichkeiten. Wenn neue Erkennungen hinzukommen, integriert AMS die Warnmeldungen dieser neuen Erkennungen in die Erkennungs- und Reaktionsplattform. Die Sicherheitsmitarbeiter von AMS sind darauf geschult, Ihnen während des gesamten Sicherheitsvorfall-Reaktionszyklus Nachforschungen anzustellen und mit Ihnen zusammenzuarbeiten.

Aufgrund dieses partnerschaftlichen Ansatzes ist es wichtig, dass Ihre Sicherheits- und Anwendungsteams bereit sind, mit AMS zusammenzuarbeiten, um Sicherheitsvorfälle zu behandeln, sobald diese Ereignisse eintreten. Diese Dokumentation erklärt, was Sie bei einem Sicherheitsereignis erwartet, und hilft Ihnen, sich auf eine schnelle Reaktion vorzubereiten, wenn ein Sicherheitsvorfall eintritt.

Diese Dokumentation verwendet die NIST 800-61-Definition eines Ereignisses als jedes beobachtbare Ereignis in einem System oder Netzwerk und als Vorfall als Verstoß oder unmittelbar drohende Verletzung von Richtlinien, Richtlinien zur akzeptablen Nutzung oder Standardsicherheitspraktiken.

Checkliste für die Vorbereitung

Arbeiten Sie die folgende Checkliste mit Ihrem AMS Cloud Solution Delivery Manager (CSDM) und AMS Cloud Architect (CA) durch:

- Verstehen Sie, welche Workloads in welchen Konten ausgeführt werden.
- Verstehen Sie, welche internen Teams für die verschiedenen Workloads verantwortlich sind, und kennzeichnen Sie sie entsprechend in den Workloads.
- Pflegen Sie intern die Kontaktdaten anderer Teams, die möglicherweise bei der Untersuchung eines Sicherheitsvorfalls und bei Entscheidungen zur Eindämmung benötigt werden.
- Vergewissern Sie sich, dass die Sicherheitskontakte auf dem neuesten Stand sind und allen verwalteten AWS Konten hinzugefügt wurden. Die Kontakte werden pro Konto verwaltet.
- Informieren Sie sich darüber, wie Sie AMS über einen Sicherheitsvorfall informieren können, und machen Sie sich mit dem Schweregrad und den zu erwartenden Reaktionszeiten vertraut.
- Stellen Sie sicher, dass eingehende Sicherheitsbenachrichtigungen an die entsprechenden Personen und Systeme wie Pager oder Ihr Security Operations Center weitergeleitet werden.

- Erfahren Sie, welche Protokollquellen Ihnen zur Verfügung stehen, wo diese in Ihren Konten gespeichert sind und wer Zugriff darauf hat.
- Erfahren Sie, wie Sie CloudWatch Insights verwenden können, um Logs bei Untersuchungen abzufragen.
- Machen Sie sich mit den Containment-Optionen vertraut, die Ihnen je nach Ressource (EC2, IAM, S3 usw.) zur Verfügung stehen, und welche Auswirkungen dies auf Ihre Workload-Verfügbarkeit hat, wenn Sie sich im Containment befinden.

Detect

Während der Verwaltung Ihrer AWS Konten überwacht AMS anhand von Daten, die aus Erkennungsquellen und Kontrollen gesammelt wurden, einschließlich, aber nicht beschränkt auf Amazon, Amazon, VPC Flow Logs, Amazon Macie und interne Threat Intelligence-Feeds von Amazon CloudWatch, Amazon, Amazon, Amazon, Amazon, Amazon, Amazon, Amazon GuardDuty, Amazon, auf Anomalien im Hinblick auf Benutzerverhalten, Kontoaktivitäten AWS Config und potenzielle Sicherheitsereignisse.

AMS verwendet sowohl native AWS Dienste als auch andere Erkennungstechnologien, um auf Sicherheitsereignisse zu reagieren, die verursacht werden durch:

- Typen zur Suche nach Konformität bei der Config
- GuardDuty Typen finden
- Macie Findet Typen
- DNS-Firewall-Ereignisse für Amazon Route 53 Resolver
- AMS-Sicherheitsereignisse (Cloud-Watch-Alarme)

Im Zuge der Weiterentwicklung von Diensten, Produkten und Bedrohungsökosystemen kommen weitere Erkenntnisse hinzu.

Melden Sie Sicherheitsereignisse an AMS

Melden Sie einen Vorfall über das AMS Support Portal oder Support Center, um AMS über einen Sicherheitsvorfall zu informieren oder um Untersuchungen anzufordern.

Analysieren

Nachdem ein Sicherheitsereignis identifiziert und gemeldet wurde, besteht der nächste Schritt darin, zu analysieren, ob es sich bei dem gemeldeten Ereignis um einen falsch positiven oder einen echten Vorfall handelt. AMS verwendet Automatisierungs- und manuelle Ermittlungstechniken, um mit Sicherheitsereignissen umzugehen. Die Analyse umfasst die Untersuchung von Protokollen aus verschiedenen Erkennungsquellen wie Netzwerkdatenverkehrsprotokollen, Hostprotokollen, CloudTrail Ereignissen, AWS Serviceprotokollen usw. Bei der Analyse wird auch nach Mustern gesucht, die durch Korrelation ein anomales Verhalten zeigen.

Ihre Partnerschaft ist erforderlich, um den spezifischen Kontext der Kontoumgebung zu verstehen und herauszufinden, was für Ihr Konto und Ihre Workloads normal ist. Auf diese Weise kann AMS eine Anomalie schneller erkennen und schneller auf Vorfälle reagieren.

Bearbeitung von Mitteilungen von AMS über Sicherheitsereignisse

AMS hält Sie während der Untersuchung auf dem Laufenden, indem es Ihre Sicherheitskontakte über ein Incident-Ticket kontaktiert. Ihr AMS Cloud Service Delivery Manager (CSDM) und Ihr AMS Cloud Architect (CA) sind die Ansprechpartner, an die Sie sich während einer aktiven Sicherheitsuntersuchung für jegliche Kommunikation wenden können.

Die Kommunikation umfasst die automatische Benachrichtigung, wenn eine Sicherheitswarnung generiert wird, die Kommunikation nach der Ereignisanalyse, die Einrichtung von Call Bridges und die fortlaufende Übermittlung von Artefakten wie Protokolldateien, Snapshots infizierter Ressourcen sowie die Übermittlung der Untersuchungsergebnisse an Sie während des Sicherheitsereignisses.

Die Standardfelder, die in AMS-Sicherheitswarnmeldungen enthalten sind, sind unten aufgeführt. Diese Felder bieten Ihnen Informationen, sodass Sie Ereignisse zur Behebung an die entsprechenden Teams in Ihrer Organisation weiterleiten können.

- Typ wird gesucht
- Identifier finden (sofern relevant)
- Schweregrad ermitteln
- Beschreibung finden
- Datum und Uhrzeit der Suche wurden erstellt
- AWS Konto-ID
- Region (wo relevant)
- AWS Ressourcen (IAMuser/role/policy, S3 EC2, EKS)

Je nach Finding-Typ werden zusätzliche Felder bereitgestellt. EKS-Ergebnisse enthalten beispielsweise Pod-, Container- und Cluster-Details.

Enthalten

Der Eindämmungsansatz von AMS basiert auf einer Partnerschaft mit Ihnen. Sie kennen Ihr Unternehmen und wissen, welche Auswirkungen Containment-Aktivitäten wie Netzwerkisolierung, Deprovisionierung von IAM-Benutzern oder -Rollen, Neuaufbau von Instanzen usw. haben können.

Ein wesentlicher Bestandteil der Eindämmung ist die Entscheidungsfindung. Fahren Sie beispielsweise ein System herunter, isolieren Sie eine Ressource vom Netzwerk, schalten Sie den Zugriff aus oder beenden Sie Sitzungen. Diese Entscheidungen sind leichter zu treffen, wenn es vorher festgelegte Strategien und Verfahren gibt, um den Vorfall einzudämmen. AMS stellt die Eindämmungsstrategie bereit und implementiert dann die Lösung, nachdem Sie das mit der Implementierung der Eindämmungsmaßnahmen verbundene Risiko berücksichtigt haben.

Je nach den zu analysierenden Ressourcen gibt es unterschiedliche Eindämmungsoptionen. AMS geht davon aus, dass bei der Untersuchung eines Vorfalls mehrere Eindämmungsarten gleichzeitig eingesetzt werden. Zu diesen Beispielen gehören unter anderem:

- Wenden Sie Schutzregeln an, um unbefugten Datenverkehr zu blockieren (Sicherheitsgruppe, NACL, WAF-Regeln, SCP-Regeln, Liste verweigern, Signaturaktion auf Quarantäne oder Sperren festlegen)
- Isolierung von Ressourcen
- Netzwerkisolierung
- Deaktivierung von IAM-Benutzern, -Rollen und -Richtlinien
- Ändern/Reduzieren der IAM-Benutzer- und Rollenrechte
- Rechenressourcen beenden, aussetzen oder löschen
- Einschränkung des öffentlichen Zugriffs auf die betroffene Ressource
- Rotierende Zugriffsschlüssel, API-Schlüssel und Passwörter
- Löschen offengelegter Anmeldeinformationen und vertraulicher Informationen

AMS empfiehlt Ihnen, die Art der Eindämmungsstrategien für jede Art von schwerwiegenden Vorfällen, die ihrem Risikoappetit entsprechen, zu prüfen. Die Kriterien sind klar dokumentiert, um im Falle eines Vorfalls die Entscheidungsfindung zu erleichtern. Zu den Kriterien für die Festlegung der geeigneten Strategie gehören:

- Mögliche Schäden an Ressourcen
- Bewahrung von Beweismitteln
- Nichtverfügbarkeit von Diensten (z. B. Netzwerkkonnektivität, Dienste, die für externe Parteien bereitgestellt werden)
- Zeit und Ressourcen, die für die Umsetzung der Strategie benötigt wurden
- Wirksamkeit der Strategie (z. B. teilweise Eindämmung, vollständige Eindämmung)
- Dauerhaftigkeit der Lösung (z. B. Entscheidungen zwischen Einwegtüren und Einwegtüren)
- Dauer der Lösung (z. B. Notfalllösung, die innerhalb von vier Stunden entfernt wird, vorübergehende Behelfslösung, die innerhalb von zwei Wochen entfernt wird, dauerhafte Lösung).
- Wenden Sie Sicherheitskontrollen an, die Sie aktivieren können, um das Risiko zu verringern und Zeit für die Definition und Implementierung einer effektiveren Eindämmung zu gewinnen.

Die Geschwindigkeit der Eindämmung ist entscheidend. AMS empfiehlt einen schrittweisen Ansatz, um eine effiziente und effektive Eindämmung durch strategische Strategien für kurz- und langfristige Konzepte zu erreichen.

Verwenden Sie diesen Leitfaden, um Ihre Eindämmungsstrategie zu überdenken, die je nach Ressourcentyp unterschiedliche Techniken beinhaltet.

- Eindämmungsstrategie
 - Kann AMS den Umfang des Sicherheitsvorfalls ermitteln?
 - Falls ja, identifizieren Sie alle Ressourcen (Benutzer, Systeme, Ressourcen).
 - Falls nein, untersuchen Sie dies parallel zur Ausführung des nächsten Schritts für identifizierte Ressourcen.
 - Kann die Ressource isoliert werden?
 - Falls ja, fahren Sie mit der Isolierung der betroffenen Ressourcen fort.
 - Falls nein, arbeiten Sie mit den Systembesitzern und Managern zusammen, um weitere Maßnahmen zur Eindämmung des Problems zu ergreifen.
 - Sind alle betroffenen Ressourcen von den nicht betroffenen Ressourcen isoliert?
 - Falls ja, fahren Sie mit dem nächsten Schritt fort.
 - Falls nein, isolieren Sie die betroffenen Ressourcen weiter, bis eine kurzfristige Eindämmung erreicht ist, um zu verhindern, dass der Vorfall weiter eskaliert.
- Systemsicherung

- Wurden für weitere Analysen Sicherungskopien der betroffenen Systeme erstellt?
- Werden die forensischen Kopien verschlüsselt und an einem sicheren Ort gespeichert?
- Falls ja, fahren Sie mit dem nächsten Schritt fort.
- Falls nein, verschlüsseln Sie die forensischen Bilder und speichern Sie sie an einem sicheren Ort, um eine versehentliche Verwendung, Beschädigung und Manipulation zu verhindern.

Ausrotten

Nach der Eindämmung eines Vorfalls kann eine Beseitigung erforderlich sein, um die Bedrohungsquellen vollständig zu eliminieren und das System zu schützen, bevor Sie mit der nächsten Wiederherstellungsphase fortfahren. Zu den Maßnahmen zur Beseitigung können das Löschen von Malware und das Entfernen gefährdeter Benutzerkonten sowie die Identifizierung und Behebung aller ausgenutzten Sicherheitslücken gehören. Bei der Beseitigung ist es wichtig, alle betroffenen Konten, Ressourcen und Instanzen in der Umgebung zu identifizieren, damit sie behoben werden können.

Es hat sich bewährt, dass die Beseitigung und Wiederherstellung schrittweise erfolgt, sodass die Maßnahmen zur Behebung priorisiert werden. Bei größeren Vorfällen kann die Wiederherstellung Monate dauern. In den ersten Phasen muss die Absicht bestehen, die allgemeine Sicherheit durch relativ schnelle (Tage bis Wochen) wichtige Änderungen zu erhöhen, um future Vorfälle zu verhindern. Die späteren Phasen müssen sich auf längerfristige Änderungen (z. B. Änderungen der Infrastruktur) und laufende Arbeiten konzentrieren, um das Unternehmen so sicher wie möglich zu halten.

Bei einigen Vorfällen ist die Beseitigung entweder nicht erforderlich oder sie erfolgt während der Wiederherstellung.

Berücksichtigen Sie dabei Folgendes:

- Kann das System erneut erstellt und anschließend mit Patches oder anderen Gegenmaßnahmen abgesichert werden, um das Risiko von Angriffen zu verhindern oder zu verringern?
- Werden alle von den Angreifern hinterlassenen Schadsoftware und anderen Artefakte entfernt und die betroffenen Systeme gegen weitere Angriffe abgesichert?

Wiederherstellung

AMS arbeitet mit Ihnen zusammen, um den normalen Betrieb der Systeme wiederherzustellen, sicherzustellen, dass die Systeme normal funktionieren, und (falls zutreffend) Sicherheitslücken zu beheben, um ähnliche Vorfälle zu verhindern.

Berücksichtigen Sie dabei Folgendes:

- Wurden die betroffenen Systeme gepatcht und sind sie gegen den jüngsten Angriff und mögliche zukünftige Angriffe abgesichert?
- An welchem Tag und zu welcher Uhrzeit können die betroffenen Systeme wieder in Betrieb genommen werden?
- Welche Tools werden Sie verwenden, um zu testen, zu überwachen und sicherzustellen, dass die Systeme, die Sie in Betrieb nehmen, nicht anfällig für die ersten Angriffstechniken sind?

Bericht nach dem Vorfall

Nach dem Ereignis führt AMS einen Ermittlungsprozess zur Überprüfung aller Sicherheitsvorfälle durch. Und AMS leitet einen Prozess zur Fehlerkorrektur (COE) ein, um Sicherheitsvorfälle zu beheben, die durch ein System oder einen verfahrenstechnischen Fehler verursacht wurden, der plausibel verbesserungswürdig ist. AMS arbeitet mit Ihnen zusammen, um die Erfahrung mit Sicherheitsuntersuchungen kontinuierlich zu verbessern. Der COE-Prozess hilft AMS dabei, die Faktoren zu identifizieren, die sich auf die Kunden auswirken, und verknüpft diese Ursachen mit den nächsten Maßnahmen, die verhindern können, dass sich ähnliche Ereignisse wiederholen, oder trägt dazu bei, die Dauer oder das Ausmaß der Auswirkungen zu verringern.

Das Verfahren zur Überprüfung von Sicherheitsvorfällen befasst sich mit den folgenden Punkten, um Verbesserungsmöglichkeiten zu ermitteln:

- Wie lange verging zwischen dem Beginn des Vorfalls, der Entdeckung des Vorfalls, der ersten Folgenabschätzung und den einzelnen Phasen der Bearbeitung des Vorfalls (z. B. Eindämmung, Behebung)?
- Wie lange hat es gedauert, bis das Incident-Response-Team auf den ersten Bericht über den Vorfall reagiert hat?
- Wie lange hat es gedauert, eine erste Folgenabschätzung durchzuführen?
- War das vermeidbar und wie? Gibt es ein Tool oder einen Prozess, der dies hätte verhindern können?

- Hätten wir das früher erkennen können und wie?
- Was hätte die Untersuchung beschleunigen können?
- Wurden die dokumentierten Verfahren zur Reaktion auf Vorfälle eingehalten? Waren sie ausreichend?
- Wurde der Informationsaustausch mit anderen Interessenträgern rechtzeitig durchgeführt? Wie könnte er verbessert werden?
- War die Zusammenarbeit mit anderen Teams (AWS Sicherheit, Kundenteams, AWS Entwicklungsteam und Kundensicherheitsteam) effektiv? Wenn nicht, was könnte verbessert werden?
- Welche Vorbereitungsschritte fehlten, die hätten helfen können: Eskalationsmatrizen, RACIs, Modelle der geteilten Verantwortung und so weiter? Müssen Runbooks aktualisiert werden?
- Was war der Unterschied zwischen der ursprünglichen Folgenabschätzung und der endgültigen Folgenabschätzung? Was können wir tun, um die Genauigkeit der Bewertungen zu einem früheren Zeitpunkt der Reaktion auf Vorfälle zu verbessern?
- Welche Maßnahmen ergeben sich aus den gewonnenen Erkenntnissen?

Runbooks zur Reaktion auf Sicherheitsvorfälle in AMS

Dieser Abschnitt enthält zwei Runbooks:

- [Reaktion auf Root-Benutzeraktivitäten](#)
- [Reaktion auf Malware-Ereignisse](#)

Reaktion auf Root-Benutzeraktivitäten

Der [Root-Benutzer](#) ist der Superuser in Ihrem AWS Konto. Beachten Sie, dass AMS die Root-Nutzung überwacht. Es hat sich bewährt, den Root-Benutzer nur für die wenigen Aufgaben zu verwenden, für die er erforderlich ist, z. B. um Ihre Kontoeinstellungen zu ändern, den AWS Identity and Access Management (IAM-) Zugriff auf die Abrechnung und das Kostenmanagement zu aktivieren, Ihr Root-Passwort zu ändern und die Multi-Faktor-Authentifizierung (MFA) zu aktivieren. Weitere Informationen finden Sie unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind](#).

Weitere Informationen darüber, wie AMS über die geplante Root-Nutzung informiert werden kann, finden Sie unter [Wann und wie wird das Root-Konto in AMS verwendet?](#)

Wenn Root-Benutzeraktivitäten erkannt werden, entweder fehlgeschlagene Anmeldeversuche, die auf einen Brute-Force-Angriff hinweisen könnten, oder Aktivitäten im Konto nach einer erfolgreichen Anmeldung, wird ein Ereignis generiert und ein Vorfall an Ihre definierten Sicherheitskontakte gesendet.

AWS Managed Services Operations untersucht ungeplante Root-Benutzeraktivitäten, führt Datenerfassung, Triage und Analyse durch und führt Eindämmungsaktivitäten auf Ihre Anweisung hin durch, gefolgt von einer Analyse nach dem Ereignis.

Wenn Sie das AMS Advanced-Betriebsmodell nutzen, erhalten Sie zusätzliche Mitteilungen von den Technikern von AMS CSDM und AMS Ops, die ungeplante Root-Benutzeraktivitäten bestätigen, da AMS für die Sicherung der Root-Benutzeranmeldedaten verantwortlich ist. AMS untersucht die Root-Benutzeraktivitäten, bis Sie einen weiteren Weg bestätigt haben.

Vorbereitung

Informieren Sie AMS über jede geplante Nutzung des Root-Benutzers, indem Sie eine AMS-Serviceanfrage mit den Daten und Zeiten des geplanten Ereignisses einreichen, um unnötige Maßnahmen zur Reaktion auf Vorfälle zu vermeiden.

Nehmen Sie regelmäßig Kontakt GameDays mit AMS auf, um die Prozesse von AMS zur Reaktion auf Kundenvorfälle zu überprüfen, Mitarbeiter und Systeme auf dem neuesten Stand zu halten, und bauen Sie gemeinsam mit verantwortlichen Personen ein gutes Gedächtnis auf, um eine schnellere Reaktion auf Vorfälle zu erreichen.

Phase A: Erkennen

AMS überwacht die Konten anhand von Erkennungsquellen, einschließlich GuardDuty AMS-Überwachung, auf Root-Aktivitäten.

Wenn Sie AMS Accelerate verwenden, reagiert das Betriebsmodell auf den Vorfall und fordert eine Untersuchung auf unerwartete Root-Benutzeraktivitäten an. In diesem Fall initiiert AMS Operations das Runbook für kompromittierte Konten.

Wenn Sie AMS Advanced verwenden, reagiert das Betriebsmodell auf den Vorfall oder informiert das CSDM über geplante Root-Benutzeraktivitäten, um eine aktive Untersuchung zur Kontengefährdung zu beenden.

Phase B: Analysieren

AMS führt eine gründliche Untersuchung der Root-Benutzerereignisse durch, wenn festgestellt wird, dass die Aktivität nicht autorisiert ist. Sowohl mithilfe von Automatisierungen als auch mithilfe des

AMS Security Response Teams werden Protokolle und Ereignisse auf Anomalien und unerwartetes Verhalten von Root-Benutzern analysiert. Mithilfe von Protokollen können Sie feststellen, ob die Aktivität unbekannt ist, ob es sich um ein autorisiertes Root-Benutzer-Ereignis handelt oder ob weitere Untersuchungen erforderlich sind.

Zu den Informationen, die während der Untersuchung zur Unterstützung interner Kontrollen zur Verfügung gestellt wurden, gehören unter anderem:

- Kontoinformationen: Für welches Konto wurde das Root-Konto verwendet?
- E-Mail-Adresse für den Root-Benutzer: Jeder Root-Benutzer ist mit einer E-Mail-Adresse aus Ihrer Organisation verknüpft
- Authentifizierungsdetails: Wo und wann hat der Root-Benutzer auf Ihre Umgebung zugegriffen?
- Aktivitätsaufzeichnungen: Was hat der Benutzer getan, als er als Root angemeldet war? Diese Aufzeichnungen liegen in Form von CloudWatch Ereignissen vor. Zu verstehen, wie man diese Protokolle liest, hilft bei der Untersuchung.

Es hat sich bewährt, dass Sie bereit sind, die Analyseinformationen zu erhalten, und einen Plan haben, wie Sie autorisierte Ansprechpartner für Konten in Ihrem Unternehmen erreichen können. Da Stammbenutzer nicht als Einzelpersonen benannt werden, können Fragen schnell intern weitergeleitet werden, wenn Sie feststellen, wer Zugriff auf die für das Konto verwendete Stamm-E-Mail-Adresse innerhalb Ihrer Organisation hat.

Phase C: Eindämmen und Ausrotten

AMS arbeitet mit Ihren Sicherheitsteams zusammen, um die Eindämmung auf Anweisung Ihrer autorisierten Ansprechpartner für Kundensicherheit durchzuführen. Zu den Eindämmungsoptionen gehören:

- Rotation der entsprechenden Anmeldeinformationen und Schlüssel.
- Beenden aktiver Sitzungen mit Konten und Ressourcen.
- Beseitigung der erstellten Ressourcen.

Während der Eindämmungsmaßnahmen arbeitet AMS eng mit Ihrem Sicherheitsteam zusammen, um sicherzustellen, dass Störungen Ihrer Workloads so gering wie möglich gehalten werden und die Root-Zugangsdaten angemessen gesichert sind.

Nach Abschluss des Eindämmungsplans arbeiten Sie mit dem AMS Operations Team zusammen, um alle erforderlichen Wiederherstellungsmaßnahmen durchzuführen.

Bericht nach dem Vorfall

Bei Bedarf leitet AMS den Überprüfungsprozess der Untersuchung ein, um alle gewonnenen Erkenntnisse zu ermitteln. Im Rahmen der Durchführung eines COE teilt AMS den betroffenen Kunden alle relevanten Ergebnisse mit, um ihnen zu helfen, ihren Prozess zur Reaktion auf Vorfälle zu verbessern.

AMS dokumentiert alle endgültigen Einzelheiten der Untersuchung, erfasst die entsprechenden Kennzahlen und meldet den Vorfall dann allen internen Teams von AMS, die Informationen benötigen, einschließlich der von Ihnen zugewiesenen CSDM und CA.

Reaktion auf Malware-Ereignisse

EC2 Amazon-Instances werden verwendet, um eine Vielzahl von Workloads zu hosten, darunter Software von Drittanbietern und individuell entwickelte Software, die von Anwendungsteams innerhalb von Organisationen bereitgestellt wird. AMS stellt Images bereit und ermutigt Sie dazu, Ihre Workloads auf Images bereitzustellen, die von AMS fortlaufend gepatcht und gewartet werden.

Während des Betriebs von Instances überwacht AMS mithilfe einer Vielzahl von Sicherheitserkennungskontrollen, darunter Amazon GuardDuty, Endpoint Protection, Network Traffic und interne Threat Intelligence-Feeds von Amazon, auf Verhaltens- oder Aktivitätsanomalien.

AMS-Kunden mit dem AMS Advanced-Betriebsmodell haben den Endpoint Security (EPS) - Monitoring-Client automatisch auf den bereitgestellten Ressourcen installiert. Dadurch wird sichergestellt, dass die Ressourcen rund um die Uhr überwacht und unterstützt werden, einschließlich der Entstehung eines Sicherheitsvorfalls, wenn ein Ereignis erkannt wird.

AMS überwacht auch GuardDuty Malware-Ergebnisse. Diese sind sowohl für AMS Advanced als auch für AMS Accelerate verfügbar, sofern sie aktiviert sind. Weitere Informationen finden Sie unter [Malware-Schutz bei Amazon GuardDuty](#).

Note

Wenn Sie sich für [Bring Your Own EPS](#) entschieden haben, unterscheidet sich das Verfahren zur Reaktion auf Vorfälle von dem, was auf dieser Seite beschrieben wird. Weitere Informationen finden Sie in der Dokumentation, auf die verwiesen wird.

Wenn Malware erkannt wird, wird ein Vorfall erstellt und Sie werden darüber informiert. Auf diese Benachrichtigung folgen alle aufgetretenen Behebungsmaßnahmen. AMS Operations untersucht, führt Datenerfassung, Sortierung und Analyse durch und führt dann auf Ihre Anweisung hin Eindämmungsmaßnahmen durch, gefolgt von Analysen nach dem Ereignis.

Phase A: Erkennen

AMS überwacht Instances auf Ereignissen mit einer GuardDuty Sicherheitslösung für Endpunkte. AMS bestimmt die geeigneten Anreicherungs- und Triage-Aktivitäten, damit Sie je nach Befund- oder Warnungstyp Entscheidungen zur Eindämmung oder Risikoakzeptanz treffen können.

Die Datenerfassung erfolgt auf der Grundlage des Ergebnistyps. Bei der Datenerhebung werden mehrere Datenquellen innerhalb und außerhalb des betroffenen Kontos abgefragt, um sich ein Bild von der beobachteten Aktivität oder den besorgniserregenden Konfigurationen zu machen.

AMS korreliert die Ergebnisse mit allen anderen Alarmen und Warnmeldungen oder Telemetriedaten von allen betroffenen Konten oder AMS-Bedrohungsinformationsplattformen.

Phase B: Analysieren

Nachdem die Daten gesammelt wurden, werden sie analysiert, um mögliche Aktivitäten oder besorgniserregende Indikatoren zu identifizieren. In dieser Phase der Untersuchung arbeitet AMS mit Ihnen zusammen, um Geschäfts- und Domänenwissen über die Instanzen und Workloads zu integrieren, damit Sie besser verstehen, was erwartet wird und was ungewöhnlich ist.

Zu den Informationen, die während der Untersuchung zur Unterstützung interner Kontrollen zur Verfügung gestellt wurden, gehören unter anderem:

- Kontoinformationen: Auf welchem Konto wurde die Malware-Aktivität beobachtet?
- Instanzdetails: Welche Instanz (en) sind von den Malware-Ereignissen betroffen?
- Zeitstempel des Ereignisses: Wann wurde die Warnung ausgelöst?
- Informationen zur Arbeitslast: Was läuft auf der Instance?
- Malware-Details, falls relevant: Malware-Familien und Open-Source-Informationen zu der Malware.
- Benutzer- oder Rollendetails: Welche Benutzer oder Rollen sind von der Aktivität betroffen und an der Aktivität beteiligt?
- Aktivitätsaufzeichnungen: Welche Aktivitäten werden auf der Instance aufgezeichnet? Diese liegen in Form von CloudWatch Ereignissen und Systemereignissen aus der Instanz vor. Wenn Sie wissen, wie diese Protokolle gelesen werden, können Sie sie leichter untersuchen

- **Netzwerkaktivität:** Welche Endpunkte stellen eine Verbindung zu der Instance her, mit wem stellt die Instance eine Verbindung her und was ist die Traffic-Analyse?

Es hat sich bewährt, darauf vorbereitet zu sein, Ermittlungsinformationen zu erhalten, und einen Plan zu haben, wie Sie die entsprechenden Kontaktstellen für Accounts, Instances und Workloads innerhalb Ihres Unternehmens kontaktieren können. Wenn Sie Ihre Netzwerktopologie und die erwartete Verbindung kennen, können Sie die Folgenabschätzung beschleunigen. Kenntnisse über geplante Penetrationstests in der Umgebung und aktuelle Implementierungen, die von Anwendungsbesitzern durchgeführt wurden, können die Untersuchung ebenfalls beschleunigen.

Wenn Sie feststellen, dass die Aktivität geplant und autorisiert ist, wird der Vorfall aktualisiert und die Untersuchung abgeschlossen. Wenn der Kompromiss bestätigt wird, legen Sie und AMS den geeigneten Eindämmungsplan fest.

Phase C: Eindämmen und Ausrotten

AMS arbeitet mit Ihnen zusammen, um auf der Grundlage der gesammelten Daten und der bekannten Informationen geeignete Maßnahmen zur Eindämmung zu ermitteln. Zu den Eindämmungsoptionen gehören unter anderem:

- Aufbewahrung von Daten durch Schnappschüsse
- Änderung der Netzwerkregeln zur Begrenzung des Datenverkehrs innerhalb oder außerhalb von Instanzen
- Änderung der SCP-, IAM-Benutzer- und Rollenrichtlinien zur Beschränkung des Zugriffs
- Instanzen beenden, aussetzen oder ausschalten
- Beenden aller dauerhaften Verbindungen
- Rotieren der entsprechenden Anmeldeinformationen/Schlüssel

Wenn Sie sich dafür entscheiden, eine Eradikationsaktivität gegen die Instance durchzuführen, unterstützt Sie AMS dabei, dies zu erreichen. Zu den Optionen gehören, sind aber nicht beschränkt auf:

- Unerwünschte Software entfernen
- Neuaufbau der Instanz aus einem sauberen, vollständig gepatchten Image und erneutes Bereitstellen von Anwendungen und Konfiguration
- Wiederherstellung der Instanz aus einem früheren Backup

- Bereitstellen von Anwendungen und Diensten auf einer anderen Instanz innerhalb Ihres Kontos, die möglicherweise zum Hosten der Workloads geeignet ist.

Es ist wichtig, vor der Wiederherstellung des Dienstes festzustellen, wie die Malware übertragen und auf der Instanz ausgeführt wurde, um sicherzustellen, dass alle zusätzlichen Kontrollen angewendet werden, um ein erneutes Auftreten der Malware auf der Instanz zu verhindern. AMS stellt Ihren forensischen Partnern oder Teams bei Bedarf zusätzliche Erkenntnisse oder Informationen zur Verfügung, um die Forensik zu unterstützen.

Derzeit arbeiten Sie für die Wiederherstellungsaktivitäten mit AMS Operations zusammen. AMS arbeitet eng mit Ihnen zusammen, um Unterbrechungen der Workloads zu minimieren und die Instanzen zu sichern.

Bericht nach dem Vorfall

Bei Bedarf leitet AMS die Überprüfung der Untersuchung ein, um die gewonnenen Erkenntnisse zu ermitteln. Im Rahmen der Durchführung eines COE teilt AMS Ihnen die relevanten Ergebnisse mit, damit Sie Ihren Prozess zur Reaktion auf Vorfälle verbessern können.

AMS dokumentiert die letzten Einzelheiten der Untersuchung, sammelt geeignete Kennzahlen und meldet den Vorfall den internen Teams von AMS, die Informationen benötigen, einschließlich der von Ihnen zugewiesenen CSDM und CA.

Sicherheitsüberprüfungen für Änderungsanfragen in AMS Advanced

Das Verfahren zur Überprüfung von Änderungsanträgen in AWS Managed Services stellt sicher, dass AMS eine Sicherheitsüberprüfung der angeforderten Änderungen durchführt, da diese in Ihrem Namen in Ihrem Konto implementiert werden.

[AMS Fortgeschrittene technische Standards](#) definieren Sie die Mindestsicherheitskriterien, Konfigurationen und Prozesse, um die grundlegende Sicherheit Ihrer Konten zu gewährleisten. Wenn AMS die angeforderten Änderungen umsetzt, halten wir uns an diese Standards.

AMS bewertet alle Änderungsanfragen anhand der technischen Standards von AMS. Jede Änderung, die die Sicherheitslage Ihres Kontos durch Abweichung von den technischen Standards beeinträchtigen könnte, wird einer Sicherheitsüberprüfung unterzogen. Während

dieses Prozesses werden relevante Risiken von AMS hervorgehoben und von Ihrem autorisierten Risikobeauftragten geprüft und genehmigt, um ein ausgewogenes Verhältnis zwischen Sicherheits- und Geschäftsanforderungen zu gewährleisten.

Prozess des Kundensicherheitsrisikomanagements

Der AMS Advanced Customer Security Risk Management (CSRM) -Prozess hilft dabei, Risiken klar zu identifizieren und den richtigen Eigentümern mitzuteilen. Dieser Prozess minimiert die Sicherheitsrisiken in Ihrer Umgebung und reduziert den laufenden Betriebsaufwand für identifizierte Risiken.

Wenn jemand aus Ihrem Unternehmen AMS auffordert, eine Änderung an Ihrer verwalteten Umgebung vorzunehmen, überprüft AMS die Änderung standardmäßig, um festzustellen, ob die Anfrage nicht den technischen Standards entspricht, was sich auf die Sicherheitslage Ihres Kontos auswirken kann. Wenn ein hohes oder sehr hohes Sicherheitsrisiko besteht, wird die Änderungsprüfung von Ihrem autorisierten Sicherheitspersonal akzeptiert oder abgelehnt. Angeforderte Änderungen werden auch im Hinblick auf nachteilige Auswirkungen auf die Fähigkeit von AMS, das Konto zu führen, geprüft. Wenn bei der Überprüfung mögliche nachteilige Auswirkungen festgestellt werden, sind zusätzliche Prüfungen und Genehmigungen innerhalb von AMS erforderlich.

Sie können sich bei hohen oder sehr hohen Risiken vom genehmigungsbasierten Workflow im CSRM-Prozess abmelden. Um die CSRM-Option für bestimmte Konten von Standard-CSRM auf Nur Benachrichtigung zu ändern, arbeiten Sie mit Ihren Cloud Service Delivery Managern zusammen, um eine einmalige Risikoakzeptanz einzurichten. Wenn Sie sich für die Option Nur Benachrichtigung entscheiden, implementiert AMS die angeforderten Änderungen unabhängig von der Risikokategorie. Außerdem sendet AMS eine Risikobenachrichtigung an Ihre autorisierten Risikogenehmiger, anstatt vor der Implementierung der Änderung eine Genehmigung einzuholen. Sprechen Sie mit Ihren Cloud-Architekten oder Cloud Service Delivery Managern, um weitere Informationen zum AMS CSRM-Prozess zu erhalten, wie Sie die standardmäßige CSRM-Option beim Onboarding neuer AMS-Konten ändern oder bestehende Konten aktualisieren können.

Note

AMS empfiehlt dringend, dass Sie in all Ihren Konten die Standardoption Standard CSRM verwenden.

AMS Fortgeschrittene technische Standards

Im Folgenden sind die Kategorien der technischen Standards von AMS Advanced aufgeführt:

ID	Kategorie
AMS-STD-001	Konfiguration des Kennzeichnens
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	Netzwerksicherheit
AMS-STD-004	Penetrationstests
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	Host-Sicherheit
AMS-STD-007	Protokollierung
AMS-STD-008	AMS-VERRÜCKT
AMS-STD-009	Sonstiges

Standardsteuerungen in AMS Advanced

Im Folgenden sind die Standardsteuerungen in AMS aufgeführt:

AMS-STD-001 — Tagging-Konfiguration

Im Folgenden finden Sie die Standardsteuerung für 001 — Tagging-Konfiguration.

1. Alle AWS Ressourcen, die das AMS-Team für Betriebs- und Managementzwecke benötigt, müssen das folgende Schlüssel-Wert-Paar aufweisen.

- Appld= AMSInfrastructure
- Umgebung= AMSInfrastructure
- AppName = AMSInfrastructure
- AMSResource=Wahr

2. Alle Tags, die vom AMS-Team benötigt werden, mit Ausnahme der zuvor aufgeführten, müssen Präfixe haben, die in der Liste der AMS-Präfixe aufgeführt sind (siehe Hinweis).
3. Die vom AMS-Team benötigten Tagwerte (AppId, Umgebung und AppName) können für alle Ressourcen geändert werden, die Sie auf der Grundlage Ihrer Änderungsanforderungen erstellt haben.
4. Alle von AMS benötigten Tags auf Stacks dürfen aufgrund Ihrer Änderungsanfragen nicht gelöscht werden.
5. Sie können die AMS-Tag-Benennungskonvention nicht für Ihre Infrastruktur verwenden, wie in Punkt 2 erwähnt.
6. Sie können benutzerdefinierte Tags in den von AMS benötigten Ressourcen erstellen lassen (in der Regel für Anwendungsfälle in den Bereichen Abrechnung und Kostenberichterstattung). Benutzerdefinierte Tags werden beibehalten, wenn Ressourcen durch ein Stack-Update und nicht durch das Aktualisieren der Vorlage aktualisiert werden.

 Note

Liste der AMS-Präfixe

1. ams-*
2. AWSManagedLeistungen*
3. /ams/ *
4. ams*
5. AMS*
6. Ams*
7. mc*
8. MC*
9. Mc*
- 10.Wächter*
- 11.Wächter*
- 12.Verwaltete_Dienste*
- 13Neues AMS*
- 14AWS_*
- 15aws*

16.VPC_*
17.CloudTrail*
18.Wolkenspur*
19/aws_reserviert/
20AUFNEHMEN*
21EPSDB*
22MMS*
23.TemplateId*
24.StackSet-bin*
25.StackSet-AWS-Landezone
26IAMPolicy*
27Kunde-mc-*
28.Wurzel*
29LandingZone*
30.StateMachine*
31.codedeploy_service_role
32.Verwaltungshost
33.sentinel.int.
34.eps
35.UnhealthyInServiceBastion
36.Frau-

AMS-STD-002 - (IAM) AWS Identity and Access Management

ID	Technischer Standard
1,0	Dauer des Timeouts
1.1	Das standardmäßige Timeout einer Sitzung für Verbundbenutzer beträgt eine Stunde und kann auf bis zu vier Stunden erhöht werden

ID	Technischer Standard
1.2	Die Standard-Stack-Zugriffszeit beträgt 12 Stunden.
2.0	AWS Nutzung des Root-Kontos
2.1	Wenn aus irgendeinem Grund ein Root-Konto genutzt wird, GuardDuty muss Amazon so konfiguriert werden, dass relevante Ergebnisse generiert werden.
2.2	Für Single-Account-Landingzone-Konten (SALZ) und Multi-Account-Landingzone-Verwaltungskonten (früher bekannt als Master/Billing Konto) muss für das Root-Benutzerkonto virtuelles MFA aktiviert sein und der MFA-Soft-Token wird bei der Kontoeröffnung verworfen, sodass sich weder AMS noch Kunden als Root anmelden können. Das Standardverfahren für den Verlust von AWS Root-Passwörtern muss in Verbindung mit Ihrem AMS Cloud Service Delivery Manager (CSDM) befolgt werden. Diese Konfiguration muss während des Lebenszyklus der von AMS verwalteten Konten beibehalten werden.
2.3	Sie dürfen keine Zugriffsschlüssel für das Root-Konto erstellen.
3.0	Erstellung und Änderung von Benutzern

ID	Technischer Standard
3.1	IAM users/roles mit programmatischem Zugriff und nur Leseberechtigungen können ohne zeitlich begrenzte Richtlinien erstellt werden. Die Erlaubnis, das Lesen von Objekten (z. B. S3:GetObject) in allen Amazon Simple Storage Service-Buckets des Kontos zuzulassen, ist jedoch nicht zulässig.
3.1.1	Menschliche IAM-Benutzer für Konsolenzugriff und mit Leseberechtigungen können mit der zeitgebundenen Richtlinie (bis zu 180 Tage) erstellt werden, während die removal/renewal/extension zeitgebundene Richtlinie zur Risikobenachrichtigung führt. Die Erlaubnis, das Lesen von Objekten (z. B. S3:GetObject) in allen S3-Buckets des Kontos zuzulassen, ist jedoch nicht zulässig.
3.2	IAM-Benutzer und -Rollen für den Konsolen- und programmatischen Zugriff mit allen infrastrukturverändernden Berechtigungen (Schreib- und Rechteverwaltung) im Kundenkonto dürfen nicht ohne Risikoübermittlung erstellt werden. Ausnahmen bestehen für S3-Schreibberechtigungen auf Objektebene, die ohne Risikoübernahme zulässig sind, sofern sich die spezifischen Buckets im Gültigkeitsbereich und bei Tagging-Vorgängen für Tags befinden, die nichts mit AMS zu tun haben.

ID	Technischer Standard
3.3	IAM-Benutzer mit programmatischem Zugriff, die benannt <code>customer_servicenow_logging_user</code> sind <code>customer_servicenow_user</code> und für die ServiceNow Integration in das SALZ- oder MALZ-Anwendungskonto und *Kernkonten* erforderlich sind, können ohne zeitlich begrenzte Richtlinien erstellt werden.
3.4	IAM-Benutzer mit programmatischem Zugriff, die die CloudEndure Integration in SALZ <code>customer_cloud_endure_policy</code> - und MALZ-Konten verwenden und <code>customer_cloud_endure_deny_policy</code> (mit schreibgeschütztem Zugriff) benötigen, können zwar erstellt werden, benötigen jedoch eine zeitlich begrenzte Richtlinie für den Zeitraum der geplanten Migration. Die Frist kann für einen Zeitraum von maximal 180 Tagen ohne RA gelten. Der SCP ist auch berechtigt, Änderungen für MALZ-Konten vorzunehmen, damit diese Richtlinien für den erforderlichen Zeitraum gültig sind. Sie definieren geeignete Migrationsfenster für Ihre Bedürfnisse und passen sie nach Bedarf an.
4.0	Richtlinien, Maßnahmen und APIs
4.1	Für alle Ihre IAM-Benutzer und Rollen in SALZ-Konten muss die standardmäßige Customer Deny Policy (CDP) gelten, um die AMS-Infrastruktur vor versehentlicher oder vorsätzlicher Beschädigung zu schützen.

ID	Technischer Standard
4.2	AMS SCPs muss in allen von AMS verwalteten Konten in MALZ aktiviert sein.
4.3	Identitäten, die administrative Aktionen mit KMS-Schlüsseln ausführen können, wie z. B. und PutKeyPolicy ScheduleKeyDeletion , dürfen nur AMS-Operatoren und Automatisierungsprinzipalen zur Verfügung stehen.
4.4	Eine Richtlinie darf den Administratorzugriff nicht mit einer Aussage wie „Wirkung“: „Zulassen“ mit „Aktion“: „*“ statt „Ressource“: „*“ ohne Risikobereitschaft gewähren.
4.5	Die IAM-Richtlinie darf keine Aktion beinhalten, die die Aktion S3: *** für einen beliebigen Bucket ohne Risikoübernahme zulassen beinhaltet.
4.6	API-Aufrufe gegen KMS-Schlüsselrichtlinien für AMS-Infrastrukturschlüssel in den IAM-Richtlinien des Kunden dürfen nicht zulässig sein.
4.7	Aktionen, die den Change-Management-Prozess (RFC) umgehen, dürfen nicht zugelassen werden, wie z. B. das Starten oder Stoppen der Instance, das Erstellen eines S3-Buckets oder einer RDS-Instanz usw.
4.8	Aktionen, die Änderungen an den DNS-Einträgen der AMS-Infrastruktur in Amazon Route 53 vornehmen, dürfen nicht zugelassen werden.

ID	Technischer Standard
4,9 bis 4,9	Menschliche IAM-Benutzer mit Konsolenzugriff, die nach Ablauf des ordnungsgemäßen Verfahrens erstellt wurden, dürfen keine Richtlinien direkt angehängt haben, mit Ausnahme der Richtlinien „Vertrauen“, „Rolle übernehmen“ und „Zeitbegrenzung“.
4.10	EC2 Amazon-Instanzprofile mit Lesezugriff auf ein bestimmtes Geheimnis oder einen Namespace AWS Secrets Manager innerhalb desselben Kontos können erstellt werden.
4.11	Berechtigungen für AWS Managed Services Change Management (AMSCM) oder AWS Managed Services Service Knowledge Management System (AMSSKMS) können jeder Rolle hinzugefügt werden (Fähigkeit, sie zu öffnen). SR/Incident/RFC
4.12	Die IAM-Richtlinie darf keine Aktion beinhalten, zu der auch die Aktionen Logs zulassen: DeleteLogGroup und Logs: DeleteLogStream für eine CloudWatch AMS-Amazon-Protokollgruppe gehören.
4.13	Berechtigungen zur Erstellung von Schlüsseln für mehrere Regionen dürfen nicht zulässig sein.
4.14	Um Zugriff auf S3-Buckets zu gewähren ARNs, die noch nicht in Ihren Konten erstellt wurden, verwenden Sie den dienstspezifischen S3-Bedingungsschlüssel, <code>s3:ResourceAccount</code> um die Kontonummer anzugeben.

ID	Technischer Standard
4.15	Sie können Ihr benutzerdefiniertes Dashboard anzeigen, erstellen, auflisten und löschen, aber nur auf CloudWatch Amazon-Dashboards anzeigen und auflisten.
4.15.1	Sie können Zugriff auf Ihr benutzerdefiniertes S3 Storage Lens-Dashboard haben, es anzeigen, erstellen, auflisten und löschen.
4.16	Für die Arbeit mit Amazon Redshift Redshift-Datenbanken können vollständige Berechtigungen im Zusammenhang mit SQL Workbench erteilt werden. roles/users
4.17	Als Alternative zur CLI können Kundenrollen beliebige AWS CloudShell Berechtigungen erteilt werden.
4.18	Eine IAM-Rolle mit einem AWS-Service vertrauenswürdigen Principal muss außerdem den technischen Standards von IAM entsprechen.
4.19	Service Linked Roles (SLRs) unterliegen nicht den technischen Standards von AMS IAM, da sie vom IAM Service Team erstellt und verwaltet werden.

ID	Technischer Standard
4.20	IAM-Richtlinien dürfen keinen uneingeschränkten Lesezugriff auf Amazon S3-Bucket-Objekte (z. B. Amazon S3:GetObject) für alle Buckets in einem Konto zulassen: • Konten im Entwicklermodus: Verstöße führen zu einer Risikobenachrichtigung • In Konten außerhalb des Entwicklermodus: Verstöße erfordern Risikobereitschaft
4.21	Alle IAM-Berechtigungen für den Ressourcentyp „Savingsplan“ können Kunden gewährt werden.
4.22	AMS-Techniker dürfen Kundendaten (Dateien, S3-Objekte, Datenbanken) nicht manuell in einen der Datenspeicherdienste wie Amazon S3, Amazon Relational Database Service, Amazon DynamoDB usw. oder in das Betriebssystem-Dateisystem kopieren oder verschieben.
4.23	Die SCP-Richtlinie darf nicht geändert werden, um zusätzlichen Zugriff auf eines der von AMS verwalteten Konten zu ermöglichen.
4.24	Jegliche Änderungen der SCP-Richtlinie, die die AMS-Infrastruktur oder die Verwaltungsfunktionen beeinträchtigen könnten, dürfen nicht zugelassen werden. (Hinweis: AMS-Ressourcen haben das Tag AppId=AMSIInfrastructure und folgen dem AMS Protected Namespace).
4.25	Die Funktion AMS Automated IAM Provisioning muss in Ihren Konten als Opt-in-Funktion aktiviert sein.

ID	Technischer Standard
4.26	Von Menschen übernommene Rollen oder Benutzer von AMS dürfen keinen Zugriff auf Kundeninhalte in S3, RDS, DynamoDB, Redshift, ElastiCache, EFS und haben. FSx Außerdem muss jeder Zugriff auf bekannte, neue APIs Veröffentlichungen von anderen, die Zugriff auf Kundeninhalte gewähren AWS-Services, in den Rollen des Operators ausdrücklich verweigert werden.
5.0	Verbund
5.1	Die Authentifizierung muss mithilfe des Verbunds im AMS-verwalteten Konto konfiguriert werden.
5.2	Es darf nur eine einseitige ausgehende Vertrauensstellung von AMS AD zu Ihrem Active Directory bestehen (AMS AD vertraut On-Prem AD).
5.3	Ihre Identitätsspeicher, die für die Authentifizierung bei AMS verwendet wurden, dürfen in AMS-verwalteten Anwendungskonten nicht vorhanden sein.
6.0	Kontenübergreifende Richtlinien
6.1	IAM-Rollen und Vertrauensrichtlinien zwischen AMS-Konten, die laut Kundendatensätzen demselben Kunden gehören, können konfiguriert werden.

ID	Technischer Standard
6.2	Vertrauensrichtlinien für IAM-Rollen zwischen AMS- und Nicht-AMS-Konten müssen nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird).
6.3	Vertrauensrichtlinien für IAM-Rollen zwischen AMS-Konten und Konten von Drittanbietern dürfen nicht ohne Risikobereitschaft konfiguriert werden.
6.4	Kontoübergreifende Richtlinien für den Zugriff auf alle Kunden, die CMKs zwischen AMS-Konten desselben Kunden verwaltet werden, können konfiguriert werden.
6.5	Kontoübergreifende Richtlinien für den Zugriff auf jeden KMS-Schlüssel innerhalb eines Nicht-AMS-Kontos über ein AMS-Konto können konfiguriert werden.
6.6	Kontoübergreifende Richtlinien für den Zugriff auf alle KMS-Schlüssel innerhalb eines AMS-Kontos durch ein Drittanbieterkonto dürfen nur zulässig sein, wenn das Risiko eingegangen wird.
6.6.1	Kontoübergreifende Richtlinien für den Zugriff auf jeden KMS-Schlüssel innerhalb eines AMS-Kontos über ein Nicht-AMS-Konto können nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört.

ID	Technischer Standard
6.7	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), zwischen AMS-Konten desselben Kunden können konfiguriert werden.
6.8	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), können von einem AMS-Konto mit schreibgeschütztem Zugriff in einem Nicht-AMS-Konto aus konfiguriert werden.
6.9	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift) mit Schreibberechtigungen von AMS für ein Nicht-AMS-Konto (oder ein Nicht-AMS-zu-AMS-Konto), müssen nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird).

ID	Technischer Standard
6.10	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), können von einem AMS-Konto mit schreibgeschütztem Zugriff aus einem Drittanbieter-Konto konfiguriert werden.
6.11	Kontoübergreifende Richtlinien für den Zugriff auf S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), von einem AMS-Konto mit Schreibzugriff in einem Drittanbieter-Konto aus dürfen nicht konfiguriert werden.
6.12	Kontoübergreifende Richtlinien von Drittanbieterkonten für den Zugriff auf einen S3-Bucket eines AMS-Kunden oder auf Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), dürfen nicht ohne Risikobewertung konfiguriert werden.
7.0	User Groups (Benutzergruppen)
7.1	IAM-Gruppen mit schreibgeschützten und nicht mutativen Berechtigungen sind zulässig.
8.0	Ressourcenbasierte Richtlinien
8.1	Die AMS-Infrastrukturressourcen müssen durch das Hinzufügen von ressourcenbasierten Richtlinien vor der Verwaltung durch unbefugte Identitäten geschützt werden.

ID	Technischer Standard
8.2	Ihre Ressourcen müssen mit ressourcenbasierten Richtlinien mit den geringsten Rechten konfiguriert werden, sofern Sie nicht ausdrücklich eine andere Richtlinie angeben.
9.0	Bereitgestellte Self-Service-Dienste (SSPS)
9.1	Die standardmäßige IAM-Rolle oder -Richtlinie von AMS (einschließlich Instanzprofil, SSPS, Muster) darf weder mit noch ohne Risikoberücksichtigung geändert werden. Ausnahmen sind (ohne Risikoakzeptanz) für Vertrauensrichtlinien zulässig. Das Markieren von Rollen-, Richtlinien- oder Benutzeränderungen ist auch in den SSP-Standardrollen zulässig.
9.3	Die SSPS-Richtlinie für die Systems Manager Automation-Konsolenrolle kann mit Ausnahme der Standardrolle keinen benutzerdefinierten Rollen zugewiesen werden. Andere SSPS-Richtlinien dürfen nur dann an benutzerdefinierte IAM-Rollen angehängt werden, wenn sichergestellt ist, dass durch das Anhängen der Richtlinie an eine benutzerdefinierte Rolle keine zusätzlichen Berechtigungen gewährt werden, die über das für den SSPS-Standarddienst vorgesehene Design hinausgehen.

AMS-STD-003 — Netzwerksicherheit

Im Folgenden finden Sie die Standardsteuerung für 003 — Netzwerksicherheit:

ID	Technischer Standard
	Netzwerkfunktionen

ID	Technischer Standard
1,0	Auf alle EC2 Instances darf nur über SSH oder RDP über Bastion-Hosts, Bastion-Host-VPC-CIDR-Bereich oder über denselben VPC-CIDR-Bereich der Instanz zugegriffen werden.
2.0	EC2 Elastic IP auf Instances ist zulässig
3.0	Die AMS-Steuerebene und damit auch TLS 1.2+ in der Datenebene müssen verwendet werden.
4,0	Der gesamte ausgehende Datenverkehr muss über das Konto IGW oder TGW weitergeleitet werden.
5.0	Eine Sicherheitsgruppe darf in der Regel für eingehenden Datenverkehr nicht die Quelle 0.0.0.0/0 haben, wenn sie nicht gemäß 9.0 an einen Load Balancer angehängt ist
6.0	S3-Buckets oder Objekte dürfen nicht ohne Risikobereitschaft veröffentlicht werden.
7.0	Der Serververwaltungszugriff auf die Ports SSH/22 oder SSH/2222 (nicht SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 oder 1604, LDAP/389 oder 636 und RPC/135, NETBIOS/137-139 darf nicht von außerhalb der VPC über Sicherheitsgruppen zugelassen werden.

ID	Technischer Standard
8.0	Der Zugriff auf die Datenbankverwaltung auf Ports (MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) oder auf einem benutzerdefinierten Port darf nicht von öffentlich zugelassen werden und nicht über eine Sicherheitsgruppe an VPC über DX, VPC-Peer oder VPN weitergeleitet werden. IPs
8.1	Jede Ressource, in der Kundendaten gespeichert werden können, sollte nicht direkt dem öffentlichen Internet zugänglich gemacht werden.
9.0	Direkter Anwendungszugriff über die Ports HTTP/80, HTTPS/8443 und HTTPS/443 aus dem Internet ist nur für Load Balancer zulässig, nicht jedoch für direkte Rechenressourcen wie Instances, Container usw. EC2 ECS/EKS/Fargate
10.0	Der Zugriff auf Anwendungen über die Ports HTTP/80 und HTTPS/443 aus dem privaten IP-Bereich des Kunden kann zugelassen werden.
11.0	Änderungen an den Sicherheitsgruppen, die den Zugriff auf die AMS-Infrastruktur kontrollieren, dürfen nicht ohne Risikobereitschaft zugelassen werden.
12.0	AMS Security bezieht sich jedes Mal auf die Standards, wenn eine Sicherheitsgruppe aufgefordert wird, einer Instance zugeordnet zu werden.

ID	Technischer Standard
13.0	Der Zugriff auf Kundenbastion an den Ports 3389 und 22 darf nur von privaten IP-Bereichen aus zugelassen werden, die über DX, VPC-Peer oder VPN in die VPC geroutet werden.
14.0	Die kontenübergreifende Zuordnung von privaten gehosteten Zonen mit einem VPCs AMS-Konto zu einem Nicht-AMS-Konto (oder einem Nicht-AMS-Konto zu AMS-Konto) muss nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS-Organisationskonto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird). Verwenden Sie dazu interne Tools.
15.0	VPC-Peering-Verbindungen zwischen Konten, die demselben Kunden gehören, können zugelassen werden.
16.0	Die AMIs AMS-Basis kann mithilfe interner Tools mit einem anderen Konto gemeinsam genutzt werden, sofern beide Konten demselben Kunden gehören (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird).
17.0	FTP-Port 21 darf in keiner der Sicherheitsgruppen konfiguriert werden, ohne dass ein Risiko eingegangen ist.

ID	Technischer Standard
18.0	Kontoübergreifende Netzwerkkonnektivität über das Transit-Gateway ist zulässig, solange sich alle Konten im Besitz des Kunden befinden.
19.0	Es ist nicht zulässig, ein privates Subnetz öffentlich zugänglich zu machen
20.0	VPC-Peering-Verbindungen mit Konten von Drittanbietern (die nicht dem Kunden gehören) dürfen nicht zugelassen werden.
21.0	Eine Verbindung mit einem Drittanbieterkonto (das nicht dem Kunden gehört) durch Transit Gateway darf nicht zugelassen werden.
22.0	Jeglicher Netzwerkverkehr, der für AMS zur Bereitstellung der Dienste für Kunden erforderlich ist, darf am Netzwerkausgangspunkt des Kunden nicht blockiert werden.
23,0	Die gemeinsame Nutzung von Resolver-Regeln mit Personen, die demselben Kunden AWS-Konto gehören, ist mit einer Risikobenachrichtigung zulässig
19.0	ICMP
19,1	Für eingehende ICMP-Anfragen EC2 von der Kundeninfrastruktur an Amazon ist eine Risikobenachrichtigung erforderlich.
19.2	Eingehende Anfragen von der Öffentlichkeit, die über DX, VPC-Peer oder VPN über eine Sicherheitsgruppe an Amazon VPC IPs weitergeleitet werden, sind zulässig.

ID	Technischer Standard
19.3	Eingehende Anfragen von der Öffentlichkeit, die IPs nicht über DX, VPC-Peer oder VPN über eine Sicherheitsgruppe an Amazon VPC weitergeleitet werden, erfordern eine Risikoakzeptanz.
19.4	Ausgehende ICMP-Anfragen von Amazon EC2 an ein beliebiges Ziel sind zulässig.
20.0	Gemeinsame Nutzung von Sicherheitsgruppen
20.1	Wenn eine Sicherheitsgruppe diesen Sicherheitsstandard erfüllt, kann sie von mehreren Mitgliedern VPCs desselben Kontos und von Konten derselben Organisation gemeinsam genutzt werden.
20.2	Wenn eine Sicherheitsgruppe diesen Standard nicht erfüllt und zuvor eine Risikoakzeptanz für diese Sicherheitsgruppe erforderlich war, ist die Verwendung der Funktion zur gemeinsamen Nutzung von Sicherheitsgruppen zwischen VPCs Konten innerhalb desselben Kontos oder zwischen Konten in derselben Organisation ohne Risikoakzeptanz für diese neue VPC oder dieses neue Konto nicht zulässig.

AMS-STD-004 — Penetrationstests

Im Folgenden finden Sie die Standardsteuerung für 004 - Penetrationstests

1. AMS unterstützt keine Pentest-Infrastruktur. Es liegt in der Verantwortung des Kunden. Kali ist beispielsweise keine AMS-unterstützte Linux-Distribution.
2. Kunden müssen sich an [Penetrationstests](#) halten.

3. AMS muss 24 Stunden im Voraus benachrichtigt werden, falls der Kunde Infrastruktur-Penetrationstests für Konten durchführen möchte.
4. AMS stellt dem Kunden eine Pentesting-Infrastruktur gemäß den Kundenanforderungen bereit, die ausdrücklich in der Änderungsanfrage oder Serviceanfrage des Kunden angegeben sind.
5. Das Identitätsmanagement für die Pentesting-Infrastruktur des Kunden liegt in der Verantwortung des Kunden.

AMS-STD-005 - GuardDuty

Das Folgende ist die Standardsteuerung für 005 - GuardDuty

1. GuardDuty muss in allen Kundenkonten jederzeit aktiviert sein.
2. GuardDuty Ergebnisse aus dem Customer Managed Application Account (CMA) in MALZ führen nicht zu Alarmen für das Betriebsteam.
3. GuardDuty Benachrichtigungen müssen im selben Konto oder in einem anderen verwalteten Konto derselben Organisation gespeichert werden.
4. Die Funktion „Liste vertrauenswürdiger IP-Adressen“ von GuardDuty darf nicht verwendet werden. Stattdessen kann die automatische Archivierung als Alternative verwendet werden, was für Auditzwecke nützlich ist.
5. GuardDuty Die Administrator-Delegierung darf in MALZ nicht aktiviert werden, da ein delegierter Administrator in der Lage wäre, Aktionen mit hohen Rechten wie die Deaktivierung der GuardDuty in den anderen Konten durchzuführen, ohne ein Risiko einzugehen.
6. GuardDuty Automatische Archivierungsfilter sollten den minimalen Bereich für die maximale Rendite verwenden. Wenn AMS beispielsweise mehrere unvorhersehbare Werte IPs in verschiedenen CIDR-Blöcken erkennt und es eine Unternehmens-ASN gibt, die für die Verwendung geeignet ist, verwenden Sie die ASN. Wenn Sie sich jedoch auf bestimmte Bereiche oder /32-Adressen beschränken können, dann sollten Sie sich auf diese Bereiche beschränken.

AMS-STD-006 — Host-Sicherheit

Im Folgenden finden Sie die Standardsteuerung für 006 - Host Security

- Ein Antiviren-Agent muss jederzeit auf allen EC2 Instanzen ausgeführt werden. (zum Beispiel Trend Micro DSM).
- Das Anti-Malware-Modul muss aktiviert sein.
- Der EPS-Agent muss alle Verzeichnisse und Dateien zum Scannen enthalten.

- Dateien, die von der Antiviren-Lösung unter Quarantäne gestellt wurden, können bei Bedarf mit Ihnen geteilt werden.
- Eine Sicherheitslösung für Endgeräte eines Drittanbieters sollte nicht installiert werden.
- Die Aktualisierungshäufigkeit der Antivirensignaturen muss auf mindestens einmal täglich festgelegt werden.
- Die geplante Scan-Frequenz muss auf mindestens einmal pro Monat festgelegt werden.
- Der Echtzeit-Scan (bei Zugriff) muss aktiviert sein und jederzeit ausgeführt werden.
- AMS darf auf Ihren Instances keine benutzerdefinierten Skripts ausführen, die nicht im Eigentum von AMS stehen oder von AMS erstellt wurden. (Hinweis: Sie können dies tun, indem Sie den Stack-Admin-Zugriff über den Stack-Admin-Zugriff CT oder mithilfe von [AWS Systems Manager Automation \(AMS SSPS\)](#) verwenden.
- Network Level Authentication (NLA) darf auf dem Windows-Host nicht deaktiviert werden.
- Das Host-Betriebssystem muss gemäß dem konfigurierten Patch-Zyklus mit den neuesten Sicherheitspatches auf dem neuesten Stand sein.
- Ein von AMS verwaltetes Konto darf keine nicht verwaltete Instanz im Konto haben.
- Die Erstellung von lokalen Administratorkonten auf Ihrer Instance durch AMS darf nicht zulässig sein.
- Das Schlüsselpaar on EC2 darf nicht erstellt werden.
- Sie dürfen keine Betriebssysteme verwenden, die als „End of Life“ (EOL) deklariert wurden und für die es keinen weiteren Sicherheitssupport durch den Anbieter oder Dritte gibt.

AMS-STD-007 — Protokollierung

Im Folgenden finden Sie die Standardsteuerung für 007 — Logging

ID	Technischer Standard
1,0	Typen von Protokollen
1.1	Betriebssystemprotokolle: Alle Hosts müssen mindestens Host-Authentifizierungsereignisse, Zugriffseignisse für alle Nutzungen erhöhter Rechte und Zugriffseignisse für alle Änderungen an der Zugriffs- und Rechtekon

ID	Technischer Standard
	figuration protokollieren, einschließlich Erfolg und Misserfolg.
1.2	AWS CloudTrail: Die Protokollierung von CloudTrail Verwaltungsereignissen muss aktiviert und konfiguriert sein, um Protokolle an einen S3-Bucket zu übermitteln.
1.3	VPC Flow Logs: Alle Netzwerkverkehrsprotokolle müssen über VPC Flow Logs protokolliert werden.
1.4	Amazon S3 S3-Serverzugriffsprotokollierung: Für von AMS vorgeschriebene S3-Buckets, in denen Protokolle gespeichert werden, muss die Serverzugriffsprotokollierung aktiviert sein.
1.5	AWS Config Snapshots: AWS Config müssen Konfigurationsänderungen für alle unterstützten Ressourcen in allen Regionen aufzeichnen und die Konfigurations-Snapshot-Dateien mindestens einmal täglich an S3-Buckets liefern.
1,6	EPS-Protokolle (Endpoint Protection System): Die Protokollierung der EPS-Lösung muss aktiviert und so konfiguriert sein, dass die Protokolle an eine Logs-Protokollgruppe CloudWatch gesendet werden.
1,7	Anwendungsprotokolle: Kunden können die Protokollierung in ihren Anwendungen aktivieren und sie in einer CloudWatch Protokollgruppe oder einem S3-Bucket speichern.

ID	Technischer Standard
1.8	S3-Protokollierung auf Objektebene: Kunden können die Protokollierung auf Objektebene in ihren S3-Buckets aktivieren.
1.9	Serviceprotokollierung: Kunden sind berechtigt, Protokolle für SSPS-Dienste wie für alle Kerndienste zu aktivieren und weiterzuleiten.
1.10	Elastic Load Classic/Application Load Balancer/ Network Balancing (Load Balancer) -Protokolle: Zugriffs- und Fehlerprotokolleinträge müssen in den von AMS 2.0 verwalteten S3-Buckets gespeichert werden.
2.0	Zugriffskontrolle
2.1	Sie dürfen keinen Schreib- oder Löschzugriff auf S3-Buckets haben, die von AMS zum Speichern von Protokollen und Logs (Protokollgruppen) benötigt CloudWatch werden.
2.2	Sie müssen nur Lesezugriff auf alle Protokolle in Ihren Konten haben.
2.3	Von AMS vorgeschriebene S3-Buckets, in denen Logs gespeichert werden, dürfen nach den Grundsätzen der Bucket-Richtlinien keine Benutzer von Drittanbieterkonten zulassen.
2.4	CloudWatch Protokolle aus Logs-Protokollgruppen dürfen ohne ausdrückliche Genehmigung Ihres autorisierten Sicherheitskontakts nicht gelöscht werden.
3.0	Aufbewahrung von Protokollen

ID	Technischer Standard
3.1	Für CloudWatch Protokollgruppen, die von AMS vorgeschrieben sind, muss eine Mindestaufbewahrungsdauer von 90 Tagen für die Protokolle gelten.
3.2	Von AMS vorgeschriebene S3-Buckets, in denen die Protokolle gespeichert werden, müssen eine Mindestaufbewahrungsdauer von 18 Monaten für die Protokolle haben.
3.3	AWS Backup Snapshots sollten mit einer Mindestdauer von 31 Tagen auf den unterstützten Ressourcen verfügbar sein.
4.0	Verschlüsselung
4.1	Die Verschlüsselung muss in allen S3-Buckets aktiviert sein, die von AMS Teams, das Protokolle speichert, benötigt werden.
4.2	Jegliche Protokollweiterleitung von Kundenkonten zu anderen Konten muss verschlüsselt sein.
5.0	Integrität
5.1	Der Integritätsmechanismus für Protokolldateien muss aktiviert sein. Die „Überprüfung der Protokolldatei“ muss in den von den AMS-Teams geforderten AWS CloudTrail Trails konfiguriert werden.
6.0	Weiterleitung von Protokollen
6.1	Jedes Protokoll kann von einem AMS-Konto an ein anderes AMS-Konto desselben Kunden weitergeleitet werden.

ID	Technischer Standard
6.2	Jedes Protokoll kann nur dann von AMS an ein Nicht-AMS-Konto weitergeleitet werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört.
6.3	Logs von einem Kundenkonto dürfen nicht an ein Drittanbieterkonto weitergeleitet werden (das nicht dem Kunden gehört).

AMS-STD-008 - AMS-MAD

Im Folgenden finden Sie die Standardsteuerung für 008 - AMS-MAD

ID	Technischer Standard
1,0	Zugriffsverwaltung
1.1	Nur AMS-privilegierte Benutzer mit interaktiven Anmeldungen und Automatisierungsaufgaben dürfen sich für die Verwaltung von verwaltetem AD in Kundenkonten am Management-Host anmelden.
1.2	AD-Administratoren dürfen nur delegierte Administratorrechte haben (AMS Delegated Administrator Group).
1.3	Techniker, die sich in die AD-Umgebungen des Kunden einloggen (Management-Host oder Instanzen), müssen über einen zeitlich begrenzten Zugriff verfügen.
1.4	Kunden haben mit den Remoteserver-Administratortools in einer EC2 Instanz nur Lesezugriff auf die AD-Objekte.

ID	Technischer Standard
1.5	Administratorrechte für den Active Directory-Benutzer oder die Active Directory-Gruppe dürfen nicht gewährt werden.
1,6	AWS Die gemeinsame Nutzung von Verzeichnissen mit Personen, die demselben Kunden AWS-Konto gehören, ist mit einer Risikobeachrichtigung zulässig.
2.0	Dienstkonten
2.1	Group Managed Service Accounts (gMSA) müssen überall dort verwendet werden, wo sie von Anwendungen unterstützt werden, und nicht das Standarddienstkonto.
2.2	Alle anderen Servicekonten müssen nach Abschluss des Risikoakzeptanzprozesses erstellt werden.
2.3	AD-Sicherheitsgruppen dürfen nicht wiederverwendet werden, sofern dies nicht ausdrücklich vom Kunden gewünscht wird. Neue AD-Gruppen sollten erstellt werden. Computerobjekte, die Zugriff auf das Dienstkonto anfordern, müssen der neuen Sicherheitsgruppe hinzugefügt werden.
2.4	Alle gMSA-Servicekonten müssen der Organisationseinheit (OU) „Managed Service Account“ hinzugefügt werden.
2.5	Alle Nicht-GMSA-Servicekonten müssen unter der Organisationseinheit „Benutzer→Dienstkonten“ hinzugefügt werden.
3.0	Gruppenrichtlinienobjekte (GPO)

ID	Technischer Standard
3.1	Alle Einstellungen unter dem Gruppenrichtlinien objekt „Windows-Einstellungen > Sicherheitseinstellungen“ dürfen nicht geändert werden, wenn dadurch die Sicherheitslage des Kontos gegenüber dem aktuellen Status in irgendeiner Weise beeinträchtigt wird.
3.2	In MALZ muss das GPO, das von einem Anwendungskonto aus RFCs eingereicht wird, das die Erstellung eines Gruppenrichtlinien objekts anfordert, mit der Organisationseinheit verknüpft sein, die dem App-Konto entspricht. Alle Daten GPOs , die sich auf alle Konten auswirken, müssen aus dem Shared Service-Konto stammen.
3.3	Das standardmäßige Zeitlimit für RDP-Leersitzungen muss für alle Server unter der Active Directory-Domäne auf 15 Minuten festgelegt werden.
4.0	Active Directory-Vertrauen
4.1	Eine unidirektionale ausgehende Vertrauensstellung (vom AMS gehostetes Verzeichnis zum Kundenverzeichnis) ist zulässig, wenn die IPs bedingten Weiterleitungen über DX, VPC-Peer oder VPN an VPC weitergeleitet werden.
5.0	Andere
5.1	Der Integritätsmechanismus für Protokolldateien muss aktiviert sein. Die „Überprüfung der Protokolldatei“ muss in den von den AMS-Teams geforderten AWS CloudTrail Trails konfiguriert werden.

ID	Technischer Standard
6.0	Weiterleitung von Protokollen
6.1	Kundenbenutzer, Gruppen, Computerobjekte, OU oder andere Entitäten dürfen die AMS-Namenskonvention nicht gemäß der AMS-Namenskonvention verwenden.
6.2	All dies OUs muss von AMS verwaltet werden.

AMS-STD-009 - Verschiedenes

Im Folgenden finden Sie die Standardsteuerung für 009 - Verschiedenes

- Wenn die Verschlüsselung in einer Ressource, einem Objekt, einer Datenbank oder einem Dateisystem aktiviert ist, darf sie nicht deaktiviert werden.

Änderungen, die hohe oder sehr hohe Sicherheitsrisiken in Ihrer Umgebung mit sich bringen

Die folgenden Änderungen stellen ein hohes oder sehr hohes Sicherheitsrisiko in Ihrer Umgebung dar:

AWS Identity and Access Management

- High_Risk-IAM-001: Erstellen Sie Zugriffsschlüssel für das Root-Konto
- High_Risk-IAM-002: Änderung der SCP-Richtlinie, um zusätzlichen Zugriff zu ermöglichen
- High_Risk-IAM-003: Änderung der SCP-Richtlinie, die die AMS-Infrastruktur beschädigen könnte
- High_Risk-IAM-004: Erstellung eines role/user mit der Infrastruktur verändernden Berechtigungen (Schreiben, Rechteverwaltung oder Tagging) im Kundenkonto
- High_Risk-IAM-005: IAM-Rollen vertrauen auf Vertrauensrichtlinien zwischen AMS-Konten und Konten von Drittanbietern (die nicht dem Kunden gehören)
- High_Risk-IAM-006: Kontoübergreifende Richtlinien für den Zugriff auf beliebige KMS-Schlüssel von einem AMS-Konto aus (durch ein Drittanbieterkonto)

- High_Risk-IAM-007: Kontoübergreifende Richtlinien von Drittanbieterkonten für den Zugriff auf einen S3-Bucket eines AMS-Kunden oder auf Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift)
- high_risk-IAM-008: Weisen Sie die IAM-Berechtigungen einer beliebigen Infrastruktur-Mutationsberechtigung im Kundenkonto zu
- High_Risk-IAM-009: Erlaubt das Auflisten und Lesen aller S3-Buckets im Konto
- high_risk-IAM-010: Automatisierte IAM-Bereitstellung mit Berechtigungen read/write

Netzwerksicherheit

- High_Risk-NET-001: Öffnen Sie die Betriebssystemmanagement-Ports SSH/22 oder SSH/2222 (nicht SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 oder 1604, LDAP/389 oder 636 und NETBIOS/137-139 aus dem Internet
- High_Risk-NET-002: Öffnen Sie die Datenbankmanagement-Ports MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 oder einen beliebigen Management-Kundenport aus dem Internet
- High_Risk-NET-003: Öffnen Sie die Anwendungsports HTTP/80, HTTPS/8443 und HTTPS/443 direkt auf beliebigen Rechenressourcen. Zum Beispiel Instanzen, Container usw. aus dem Internet EC2 ECS/EKS/Fargate
- High_Risk-NET-004: Alle Änderungen an den Sicherheitsgruppen, die den Zugriff auf die AMS-Infrastruktur kontrollieren
- High_Risk-NET-006: VPC-Peering mit dem Drittanbieter-Konto (nicht im Besitz des Kunden)
- High_Risk-NET-007: Kunden-Firewall als Ausgangspunkt für den gesamten AMS-Verkehr hinzufügen
- High_Risk-NET-008: Ein Transit Gateway Gateway-Anhang mit dem Drittanbieterkonto ist nicht zulässig
- High_Risk-S3-001: Bereitstellung oder Aktivierung des öffentlichen Zugriffs im S3-Bucket

Protokollierung

- CloudTrailHigh_Risk-Log-001: Deaktivieren. (Genehmigung durch Ops Site Manager erforderlich)
- High_Risk-Log-002: Deaktivieren Sie VPC-Flow-Logs. (Genehmigung durch Ops Site Manager erforderlich)

- High_Risk-Log-003: Protokollweiterleitung über eine beliebige Methode (S3-Ereignisbenachrichtigung, SIEM-Agent-Pull, SIEM-Agent-Push usw.) von einem AMS-verwalteten Konto an ein Drittanbieter-Konto (nicht im Besitz des Kunden)
- High_Risk-Log-004: Verwenden Sie den Nicht-AMS-Trail für CloudTrail

Host-Sicherheit

- High_Risk-Host-001: Deaktivieren Sie End Point Security im Konto aus beliebigem Grund. (Genehmigung durch Ops Site Manager erforderlich)
- High_Risk-Host-002: Deaktiviert das Patchen auf Ressourcen- oder Kontoebene.
- High_Risk-Host-003: Bereitstellen einer nicht verwalteten Instanz im Konto. EC2
- High_Risk-Host-004: Ausführen eines vom Kunden bereitgestellten benutzerdefinierten Skripts.
- High_Risk-Host-005: Erstellung von lokalen Administratorkonten auf Instanzen.
- High_Risk-Host-006: Suchausschlüsse für Trend Micro EPS-Dateitypen und -erweiterungen oder Deaktivierung des Malware-Schutzes auf Endpunkten.

Note

Für EPS-Anti-Malware-Ausschlüsse oder GuardDuty Unterdrückungsregeln im Zusammenhang mit Penetrationstests oder Schwachstellenscans oder Serviceproblemen, die sich auf die Leistung auswirken, ist keine Risikobereitschaft erforderlich, sodass proaktive Maßnahmen gerechtfertigt sind. events/known In diesen Situationen ist eine Risikobenachrichtigung ausreichend.

- High_Risk-Host-007: Erstellen für KeyPair EC2
- High_Risk-Host-008: Deaktivieren Sie die Endpunktsicherheit im EC2
- High_Risk-Host-009: Konten, die das Betriebssystem End of Life (EOL) verwenden

Sonstiges

- High_Risk-ENC-001: Deaktiviert die Verschlüsselung in jeder Ressource, falls sie aktiviert ist

Verwaltetes Active Directory

- High_Risk-AD-001: Stellen Sie Administratorrechte für Active Director-Benutzer oder Gruppen bereit
- high_risk-AD-002: GPO-Richtlinien, die den Sicherheitsstatus des Kontos verringern können

Kontinuitätsmanagement in AMS Advanced

Als Teil des Kontinuitätsmanagements bietet AWS Managed Services (AMS) automatisierten Zugriff auf AWS Backup, einen nativen Service mit AWS. Dies erleichtert den Zugriff auf einen Service, der Amazon EBS, Amazon EC2, Amazon RDS, Amazon EFS und mehr unterstützt.

Weitere Informationen finden Sie unter [AWS Backup: So funktioniert es](#).

Themen

- [Was ist Kontinuitätsmanagement?](#)
- [So funktioniert Kontinuitätsmanagement](#)
- [Reaktion auf die Notfallwiederherstellung](#)
- [Planung der Notfallwiederherstellung](#)

Was ist Kontinuitätsmanagement?

Continuity Management ist der Prozess, den AMS verwendet, um Backups und Snapshots für Ihr Konto bereitzustellen.

AMS ermöglicht den Zugriff AWS Backup über Änderungstypen, die Sie zur Erstellung und Verwaltung von Backup-Jobs und -Plänen verwenden.

So funktioniert Kontinuitätsmanagement

AMS verwendet [AWS Backup](#) für das Kontinuitätsmanagement.

Wenn Sie mit AMS beginnen, mit AWS Backup zu arbeiten:

1. Führen Sie ein Backup auf Abruf durch
2. Erstellen Sie einen Backup-Plan (optional, AMS bietet Standard-Backup-Pläne)
3. Verwenden Sie das Standard-AMS als Backup-Tresor (optional)
4. Verwalten Sie Ihre Backup-Pläne und Wiederherstellungspunkte (ausführen, verfeinern, löschen usw.)

AMS-Backup-Pläne

Ein Sicherungsplan ist ein Richtlinienausdruck, der definiert, wann und wie Sie unterstützte AWS-Ressourcen wie RDS-Datenbanken, EBS-Volumes, DynamoDB-Tabellen und EFS-Dateisysteme sichern möchten. Planungs- und Aufbewahrungsrichtlinien werden über benutzerdefinierte Backup-Pläne verwaltet, die Sie mithilfe eines Change Type (CT) mit AMS Advanced oder mithilfe AWS Backup von AMS Accelerate erstellen können. Weisen Sie Ihren Backup-Plänen mithilfe von Tags Ressourcen zu und sichern und speichern Sie AWS Backup automatisch Backups für zugewiesene Ressourcen gemäß dem definierten Backup-Plan. Sie können mehrere Backup-Pläne erstellen, wenn Sie Workloads mit unterschiedlichen Backup-Anforderungen haben.

Ein Backup-Plan kann bis zu sechs Backup-Regeln enthalten, die unter anderem einen Zeitplan und eine Aufbewahrungsfrist definieren. Der Backup-Zeitplan bestimmt, wann ein Backup-Job AWS Backup initiiert wird und wie oft ein Backup erstellt wird. Sie können eine Frequenz von stündlich, täglich, wöchentlich oder monatlich wählen. Die Einstellung für Löschtage bestimmt, wie viele Tage der Snapshot gespeichert wird, bevor er automatisch gelöscht wird.

Note

AMS Advanced: Wenn Sie vom alten AMS-Backup-System migriert werden, erstellt AMS aus Gründen der Abwärtskompatibilität einen Standard-Backup-Plan. Das Schlüssel/Wert-Paar in diesem Szenario ist Backup:True. Um die Abwärtskompatibilität zu unterstützen, wird bei diesem Wert nicht zwischen Groß- und Kleinschreibung unterschieden, sodass Backup:True oder Backup:True allesamt gültige Tags sind. Bei allen anderen Schlüssel/Wert-Paaren wird zwischen Groß- und Kleinschreibung unterschieden.

AWS Backup kann auf EBS-Volume-Ebene oder EC2 Amazon-Instance-Ebene betrieben werden, aber nicht beide gleichzeitig ausführen, da dies zu einem Race Condition führen kann, bei dem die Backups kollidieren können.

Standard-Backup-Pläne, landing zone für mehrere Konten

Beim neuen RFC zur Kontoerstellung stellt AMS sicher, dass es auf Kontoebene einen übergreifenden Standard-Backup-Plan gibt, um Ihre Workloads zu schützen. Die Werte für Pflichtfelder sind standardmäßig festgelegt, wie im folgenden Abschnitt dargestellt:

Standard-AMS-Backup-Plan

default-backup-plan

TAG-Schlüssel: Backup

TAG-Wert: True

```

RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years

```

Standard-AMS-Backup-Plan	Start Time	Aufbewahrung
stündliches Backup	N/A	N/A
tägliches Backup	täglich 23:30 Uhr UTC	7 Tage
wöchentliches Backup	wöchentlich um 23:30 Uhr UTC, nur am Samstag	4 Wochen
monatliches Backup	monatlich um 23:30 Uhr UTC, am ersten Tag des Monats	26 Wochen
jährliches Backup	23:30 Uhr UTC, am ersten Tag des Monats	2 Jahre

Verbesserter Standard-AMS-Backup-Plan

Dieser Plan ist eine Blaupause für AWS Backup bewährte Verfahren zum Schutz vor Ransomware-Angriffen. Er implementiert eine tägliche, wöchentliche, monatliche und jährliche Backup-Strategie. AWS Backup [Kontinuierliches Backup](#) ist mit maximaler Aufbewahrung (31 Tage) für die [unterstützten Ressourcen](#) aktiviert.

ams-enhanced-default-backup-Plan

TAG-Schlüssel: backup-orchestrator-enhanced

TAG-Wert: true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
  UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
  UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
  02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
  UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Verbesserter AMS-Backup-Plan	Start Time	Aufbewahrung
stündliches Backup	N/A	N/A
tägliches Backup	täglich 4:00 UTC	31 Tage
wöchentliches Backup	Samstag, 2:00 Uhr UTC	6 Wochen
monatliches Backup	1. des Monats, 2:00 UTC	26 Wochen
jährliches Backup	1. Januar, 2:00 Uhr UTC	2 Jahre

Datensensibler AMS-Backup-Plan

Dieser Plan ist eine Blaupause für bewährte Methoden von AWS Backup zum Schutz vor Ransomware-Angriffen für datensensible Anwendungen. Es implementiert eine stündliche, tägliche, wöchentliche, monatliche und jährliche Backup-Strategie. Die [kontinuierliche Sicherung von AWS Backup](#) ist mit maximaler Aufbewahrung (31 Tage) für [unterstützte Ressourcen](#) aktiviert.

ams-data-sensitive-backup-Plan

TAG-Schlüssel: backup-orchestrator-data-sensitive

TAG-Wert: true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Datensensibler AMS-Backup-Plan	Start Time	Aufbewahrung
stündliches Backup	zur vollen Stunde	7 Tage
tägliches Backup	täglich 4:00 UTC	31 Tage
wöchentliches Backup	Samstag, 2:00 Uhr UTC	6 Wochen
monatliches Backup	1. des Monats, 2:00 UTC	26 Wochen
jährliches Backup	1. Januar, 2:00 Uhr UTC	2 Jahre

AMS-Backup-Tresore

AWS Backup organisiert Snapshots in logischen Speichereinheiten, den sogenannten Tresoren.

Mithilfe von Tags können Sie Backup-Tresor-Benachrichtigungen auf individueller Tresorebene steuern. Sie können Benachrichtigungen für einen bestimmten Tresor deaktivieren, indem Sie das Tag hinzufügen `AMSNotificationOptOut` und den Wert für einen bestimmten Tresor `True` aufsetzen. Um weiterhin Benachrichtigungen aus dem Tresor zu erhalten, entfernen Sie das Tag.

Um eine Liste Ihrer AMS-Backups anzuzeigen, öffnen Sie die [AWS Backup Konsole](#). Wählen Sie im Navigationsbereich Backup-Tresore und wählen Sie einen der AMS-Backup-Tresore aus den folgenden Tabellen aus. Sehen Sie sich im Abschnitt Backups die Liste aller Backups im Backup-Tresor an. Wählen Sie ein Backup aus, das bearbeitet, gelöscht oder wiederhergestellt werden soll.

Tresore für AMS-Backup-Pläne

Name des AMS-Tresors	Beschreibung
ams-automated-backups	Dieser Tresor empfängt alle Wiederherstellungspunkte, die vom AMS AWS Backup Advanced-Standardplan verwendet wurden default-backup-plan.
ams-automated-enhanced-backups	Dieser Tresor empfängt alle Wiederherstellungspunkte, die vom erweiterten AWS Backup ams-enhanced-default-backupAMS-Advanced-Standardplan verwendet wurden.
ams-automated-data-sensitive-Backups	Dieser Tresor empfängt alle Wiederherstellungspunkte, die vom AMS AWS Backup ams-data-sensitive-backupAdvanced-Plan verwendet wurden.
ams-manual-backups	Dies ist der Standardspeicherort für alle Backups aus Start Backup Job RFC-Backupplänen (ct-2hhud2lx01tq7), wenn kein Tresorname definiert ist.
ams-custom-backups	Dies ist der Standardspeicherort für die Snapshots, die AMS vor dem Patchen einer Instanz mithilfe von Patch Orchestrator oder vor den monatlichen Patch-Aktivitäten erstellt. Diese werden gemäß der Standardrichtlinie für den AMS-Patch-Lebenszyklus von 60 Tagen automatisch entfernt.

AMS-Backup-Änderungstypen

AMS bietet mehrere, mit CTs denen Sie Backup-Pläne erstellen und verwenden können.

Important

Bearbeiten Sie Ihre AMS-Standard-Backup-Pläne nicht, da Ihre Änderungen verloren gehen könnten. Erstellen Sie stattdessen neue Pläne für Ihre benutzerdefinierten Konfigurationen.

- [Backup-Plan: Erstellen](#)
- [Backup-Job: Start](#)
- [Backup-Job: Stopp](#)
- [Erholungspunkt: Löschen](#)
- [DynamoDB | Aus Backup erstellen](#)
- [EBS-Volume: Aus Backup erstellen](#)
- [Amazon Elastic File System \(EFS\): Aus Backup erstellen](#)

Überwachung und Berichterstattung von AMS-Backups

Important

Die Überwachung und Berichterstattung von AMS-Backups sind nur in Regionen verfügbar, die von AMS unterstützt werden. Dies sind USA Ost (Virginia), USA West (Nordkalifornien), USA West (Oregon), USA Ost (Ohio), Kanada (Zentral), Südamerika (São Paulo), EU (Irland), EU (Frankfurt), EU (London), EU (Paris), Asien-Pazifik (Mumbai), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio).

AMS generiert tägliche Self-Service-Berichte sowie monatliche Berichte zur Ressourcenabdeckung und zum Status der Backup-Jobs. Die monatlichen Berichte werden in Monthly Business Reviews (MBRs) veröffentlicht. Weitere Informationen zu täglichen Backup-Berichten finden Sie unter [Täglicher Backup-Bericht](#).

AMS-Experten überwachen alle Ihre Backup-Aufgaben, die mit konfiguriert sind AWS Backup. Im Falle von Backup-Ausfällen untersucht AMS den Fehler und informiert Sie über die Ursache

und die Behebungsoptionen, sofern verfügbar. Um Warnmeldungen zu vermeiden, gibt AMS bei Ereignissen, die zu einer hohen Anzahl von Backup-Ausfällen in Ihren Konten führen, über Ihr CSDM eine kollektive Empfehlung ab, anstatt Sie bei jedem einzelnen Fehler zu benachrichtigen.

Beachten Sie, dass AMS keine Backups überwacht, die mithilfe der eigenständigen AWS Backup-Funktion eines Dienstes konfiguriert wurden.

Reaktion auf die Notfallwiederherstellung

Zusätzlich zu den in den folgenden Abschnitten beschriebenen Optionen sollten Sie wissen, welche Schritte Sie unternehmen müssen, um eine Notfallwiederherstellung (DR) mit AMS einzuleiten.

Wenn es zu einem Notfall kommt und Sie eine Wiederherstellung einleiten müssen, befolgen Sie diese allgemeinen Richtlinien:

1. Öffnen Sie einen Vorfall mit hoher Priorität mit der Kategorie Verfügbarkeit. AMS öffnet eine Konferenzbrücke und lädt Ihr Team ein, daran teilzunehmen.
2. Machen Sie sich mit der Liste der Ressourcen vertraut, die Sie wiederherstellen müssen.
3. Informieren Sie sich über die Ziellandzone (LZ), zu der Sie eine Wiederherstellung durchführen müssen (z. B. dasselbe Konto, eine andere AZ oder ein anderes Konto und eine andere Region).
4. Reichen Sie Wiederherstellungsanfragen für jede Ressource in der Ziellandzone ein. Folgen Sie Ihrem bestehenden DR-Plan oder sehen Sie sich die Optionen im folgenden Abschnitt an (z. B. [Katastrophenschutz für EC2 mit EBS-Snapshots auf AMS](#), oder [Notfallschutz für EC2 mit Elastic Disaster Recovery auf AMS](#)).
5. Stellen Sie die Anwendungsfunktionalität wieder her und nutzen Sie die AMS-Unterstützung zur Behebung von Infrastrukturproblemen.

AMS kann Ihnen bei der Vorbereitung dieser Veranstaltung und bei der Erstellung eines Notfallplans für Ihr Unternehmen helfen, der diese Fragen beantwortet. Weitere Informationen erhalten Sie von Ihrem Cloud Service Delivery Manager (CSDM) oder Cloud Architect (CA).

Planung der Notfallwiederherstellung

Disaster Recovery (DR) ist ein wichtiger Service für die Geschäftskontinuität und Einhaltung von Vorschriften in Unternehmen. AMS arbeitet mit Ihnen zusammen, um Sie bei der Planung, Implementierung und Wartung Ihrer DR-Strategie auf AMS zu unterstützen.

Die AMS-Landezone (LZ) mit mehreren Konten und Einzelkonten bietet native Multi-AZ-Hochverfügbarkeit für AMS-Infrastrukturkomponenten, die den meisten Katastrophenschutzszenarien gerecht werden. Je nach geografischer Abdeckung Ihres Unternehmens benötigen Sie jedoch möglicherweise regionalen Schutz. Für regionsübergreifende Verfügbarkeit und DR ist ein weiteres AMS-Konto in einer anderen Region erforderlich (dies gilt sowohl für die landing zone mit mehreren Konten als auch für die landing zone mit einem Konto).

AMS orientiert sich an den DR-Richtlinien von AWS, wie in diesem Blog Rapidly [Recovery mission-Critical Systems in a Disaster](#) beschrieben, und unterstützt die folgenden vier Optionen:

- Mehrere Standorte (oder hochverfügbar)
- Warmer Bereitschaftsmodus
- Pilotlicht
- Backup und Backup

Diese Optionen und deren AMS-Unterstützung werden in den folgenden Abschnitten beschrieben.

An mehreren Standorten oder hochverfügbar (HA)

Die HA-Lösung wird normalerweise durch die integrierten Funktionen der Anwendung bereitgestellt, z. B. Clustering oder synchrone Replikation. Benutzer werden sowohl zu Prod als auch zu Nodes weitergeleitet. HA/DR DNS verweist entweder direkt oder über einen Elastic Load Balancer (ELB) auf die Knoten.

Ihr AMS Cloud Architect (CA) wird im Rahmen Ihrer Well-Architected-Review und der DR-Planung mit Ihnen zusammenarbeiten.

HA DR nutzt anwendungs- und AWS systemeigene Dienste und Funktionen, wie in der folgenden Grafik dargestellt:

Die DR-Site kann dieselbe oder eine andere sein. AWS-Region

Note

In einer anderen Region (regionsübergreifend) wird es eine andere Active Directory-Umgebung geben.

DR-Schritte (Failover): Automatischer Failover, es sind keine manuellen Schritte erforderlich. Im Falle eines Fehlers in der primären LZ werden die Benutzer automatisch zum Knoten umgeleitet. DR/HA Dies wird sowohl durch die DNS- als auch durch die Anwendungskonfiguration erreicht.

HA DR-Metriken:

- Recovery Point Objective (RPO): <5 Minuten
- Wiederherstellungszeitziel und (RTO): <5 Minuten
- Wartungsaufwand: Hoch (In beiden Umgebungen sind synchrone Änderungen erforderlich, z. B. Anwendungskonfiguration, Patching, SG oder ALB, Zertifikate usw.).
- Kosten: Hoch

Warmer Bereitschaftsmodus

Der Begriff „Warm-Standby“ wird verwendet, um ein Disaster-Recovery-Szenario (DR) zu beschreiben, bei dem eine verkleinerte Version der Umgebung in der Cloud ausgeführt wird.

Die Datenreplikation erfolgt über die Anwendungsebene, in der Regel asynchron, auf eine Online-Instanz, während die übrigen Instanzen (z. B. Anwendungs- und Webebene) möglicherweise ausgeschaltet werden, um Kosten zu sparen. Benutzer werden nur zur Produktionsseite weitergeleitet. Andere AWS Ressourcen wie Elastic Load Balancer (ELB) können ebenfalls vorab am DR-Standort bereitgestellt werden.

Ihr AMS Cloud Architect (CA) wird im Rahmen Ihrer Well-Architected-Review und der DR-Planung mit Ihnen zusammenarbeiten.

Warm Standby DR nutzt anwendungs- und AWS systemeigene Dienste und Funktionen, wie in der folgenden Grafik dargestellt:

Der DR-Standort kann sich auf demselben oder einem anderen Standort befinden. AWS-Region

Note

In einer anderen Region (regionsübergreifend) wird es eine andere Active Directory-Umgebung geben.

DR (Failover) -Schritte:

1. Unterbrechen Sie die Datenreplikation und machen Sie die Dateninstanz am DR-Standort zum Master
2. Aktualisieren Sie die Anwendungskonfiguration nach Bedarf (neue IP, Servername usw.)
3. Leiten Sie DNS zur DR-Site (ELB) um
4. AD-Abhängigkeiten, falls erforderlich (Dienstkonten SPNs GPOs,, usw.)

HA DR-Metriken:

- Recovery Point Objective (RPO): <1 Stunde
- Recovery Time Objective und (RTO): <1 Stunde (abhängig von der Anzahl der Instanzen und der Orchestrierung)
- Wartungsaufwand: Hoch (In beiden Umgebungen sind synchrone Änderungen erforderlich, z. B. Anwendungskonfiguration, Patching, Sicherheitsgruppen (SG) oder Application Load Balancer (ALB), Zertifikate usw.).
- Kosten: Mittel

Pilot light

Bei diesem Disaster Recovery-Ansatz (DR) replizieren Sie einen Teil Ihrer Prod-Umgebung für eine begrenzte Anzahl von Kerndiensten. Ein kleiner Teil Ihrer Infrastruktur läuft ständig und synchronisiert gleichzeitig veränderbare Daten (wie Datenbanken oder Dokumente), während andere Teile Ihrer Infrastruktur ausgeschaltet sind und nur während Tests verwendet werden. Im Gegensatz zu einem Backup- und Recovery-Ansatz müssen Sie sicherstellen, dass Ihre wichtigsten Kernelemente bereits konfiguriert sind und in der DR-Landezone (der Kontrolllampe) ausgeführt werden.

Ihr AMS Cloud Architect wird im Rahmen Ihrer Well-Architected-Review und der DR-Planung mit Ihnen zusammenarbeiten.

Pilot Light DR nutzt anwendungs- und AWS systemeigene Dienste und Funktionen, wie in der folgenden Grafik dargestellt:

Der DR-Standort kann sich auf demselben oder einem anderen Standort befinden. AWS-Region

 Note

In einer anderen Region (regionsübergreifend) wird es eine andere Active Directory-Umgebung geben.

DR (Failover) -Schritte:

1. Unterbrechen Sie die Datenreplikation und machen Sie die Dateninstanz am DR-Standort zum Master
2. Starten Sie die ausgeschalteten Instanzen und die Infrastruktur
3. Aktualisieren Sie die Anwendungskonfiguration nach Bedarf (neue IP, Servername usw.)
4. Fügen Sie die Instanzen nach Bedarf zum ELB hinzu
5. Leiten Sie DNS zur DR-Site (ELB) um
6. AD-Abhängigkeiten, falls erforderlich (Dienstkonten SPNs GPOs,, usw.)

DR-Metriken von Pilot Light:

- Recovery Point Objective (RPO): <1 Stunde
- Recovery Time Objective und (RTO): ~1 Stunde (abhängig von der Anzahl der Instanzen und der Orchestrierung)
- Wartung: Mittel
- Kosten: Mittel

Sicherung und Wiederherstellung

Dieser einfache und kostengünstige Disaster Recovery (DR) -Ansatz sichert Ihre Daten und Anwendungen von überall in der DR-Landing landing zone, um sie bei der Wiederherstellung nach einem Notfall zu verwenden.

Ihr AMS Cloud Architect arbeitet im Rahmen Ihrer Backup- und DR-Planung mit Ihnen zusammen.

Backup and Restore DR verwendet automatisierte Tools und Prozesse von AMS, wie in der folgenden Grafik dargestellt:

Zwei Sicherungs- und Replikationsmethoden können verwendet werden:

- EBS-Snapshot (Recovery Point Objective (RPO) > 1 Stunde), auch bekannt als „EBS“
- AWS Elastic Disaster Recovery (Recovery Point Objective (RPO) ~ 0,25 Stunden), auch bekannt als „DRS“

Die DR-Site kann sich in derselben oder in einer anderen befinden. AWS-Region

 Note

Eine andere Region (regionsübergreifend) hat eine andere Active Directory-Umgebung.

DR (Failover) -Schritte:

1. Stellen Sie die Instanzen aus Snapshots wieder her (zweistufiger Vorgang, wobei zuerst die Platzhalterinstanz verwendet wird)
2. Aktualisieren Sie die Anwendungskonfiguration (neue IP, Servername usw.)
3. Richten Sie nach Bedarf eine andere Infrastruktur ein (SG, ELB usw.)
4. Leiten Sie DNS zur DR-Site (ELB) um
5. Aktualisieren oder stellen Sie bei Bedarf AD-Abhängigkeiten wieder her (Dienstkonten, Dienstprinzipalnamen (SPNs), Gruppenrichtlinienobjekte (GPOs) usw.)

DR-Metriken für Backup und Wiederherstellung:

- Recovery Point Objective (RPO): > 1 Stunde oder ~0,25 Stunden (abhängig von der ausgewählten Lösung — EBS oder DRE)
- Recovery Time Objective und (RTO): ~1 Stunde (abhängig von der Anzahl der Instanzen und der Orchestrierung)
- Wartungsaufwand: Hoch (In beiden Umgebungen sind synchrone Änderungen erforderlich, z. B. Anwendungskonfiguration, Patching, Sicherheitsgruppen oder Anwendungs-Loadbalancer, Zertifikate usw.).
- Kosten: Mittel

Katastrophenschutz für EC2 mit EBS-Snapshots auf AMS

Voraussetzungen:

- AMS Prod Landezone (Quelle)
- AMS DR-Landezone (DR-Ziel)
- EBS-Snapshots sind für EC2 Instanzen aktiviert ()AWS Backup

Lösung für die Snapshot-Replikation:

- Cross AZ: Nicht zutreffend — EBS-Snapshots sind standardmäßig innerhalb der Region hochverfügbar
- Regionsübergreifend: AWS Backup

Das folgende Diagramm stellt den EC2 Wiederherstellungsprozess von EBS-Snapshots auf AMS dar:

EC2 DR-Schritte auf AMS:

1. Rufen Sie einen RFC auf, um die EBS-Snapshots mit dem Zielkonto zu teilen (erforderlich für regionsübergreifende DR).

: Verwaltung, Erweiterte Stack-Komponenten, EBS-Snapshot, Teilen
2. Erstellen Sie einen EC2 Platzhalter-AMS-Stack im Zielsubnetz (DR-Site-Subnetz). Es wird empfohlen, den Stack mithilfe von CFN-Ingestion zu erstellen, da der Kunde die Schritte der Zuweisung von Sicherheitsgruppen und anderen (wie dem Hinzufügen der Instance zu einem ELB) im selben Stack kombinieren kann.

Typ ändern: Bereitstellung, Aufnahme, Stapel aus Vorlage, Erstellen CloudFormation

3. Rufen Sie einen RFC auf, um eine Wiederherstellung des EC2 Stack-Volumes durchzuführen.

Typ ändern: Management, Advanced Stack Components, EC2 Instance-Stack, Restore Volumes.

Das CT stellt die Volumes aus den in Schritt 1 geteilten Snapshots wieder her und fügt sie der in Schritt 2 erstellten Platzhalterinstanz hinzu.

CT-Funktionalität zur Volumenwiederherstellung:

- Fahren Sie die Platzhalterinstanz herunter
- Stellen Sie Volumes aus den Snapshots wieder her
- Tauschen Sie die Volumes aus

- Starten Sie die Instanz
- Verlasse die alte Domain
- Ändern des Hostnamens
- Starten Sie neu. AMS-Bootstrap-Skripte verbinden die Instance beim Start mit der Zieldomäne (DR)

CT-Eingabe für die Wiederherstellung des Volumens:

- InstanceId (Platzhalter-Instanz-ID)
- RootDeviceSnapshotId, der EBS-Snapshot für das wiederhergestellte Root-Volume
- KMSKeyId, die KMS-Schlüssel-ID oder ARN, um alle wiederhergestellten Volumes auf der EC2 Instanz zu verschlüsseln
- DeviceNames, bis zu 25 (optional)
- SnapshotIds, bis zu 25 (optional). Liste der Snapshots der wiederherzustellenden Volumes

Notfallschutz für EC2 mit Elastic Disaster Recovery auf AMS

Voraussetzungen:

- AMS Prod Landing Zone (Quelle)
- AMS DR-Landezone (DR-Ziel)
- Sie müssen zuerst den Elastic Disaster Recovery Service für alle Anwendungen initialisieren AWS-Regionen , in denen Sie ihn verwenden möchten.

Erstellen Sie eine IAM-Rolle in Ihrer DR landing zone (LZ) für den Zugriff auf die Elastic Disaster Recovery-Konsole.

- Wichtig: Ein SSM-Dokument wird als Aktion nach dem Start innerhalb von DRS erstellt. Diese Aktion muss auf all Ihren Servern in den PostLaunch Einstellungen aktiviert sein.
- Die Zielinstanz (Platzhalter) muss einen Tag-Schlüssel haben: "AWSDRS,, Wert:"AllowLaunchingIntoThisInstance“. Die Platzhalterinstanz muss sich im gestoppten Zustand befinden. Andernfalls kann AMS die Platzhalter-Instance nicht unter den Starteinstellungen auswählen und Elastic Disaster Recovery kann die Wiederherstellung nicht auf der Platzhalter-Instance durchführen.

Ein Diagramm des Einrichtungs- und Wiederherstellungsprozesses von Elastic Disaster Recovery EC2 auf AMS finden Sie unter [Allgemeine Architektur AWS Elastic Disaster Recovery \(AWS DRS\)](#).

EC2 DR-Schritte mit Elastic Disaster Recovery auf AMS:

1. Erstellen Sie im Zielsubnetz (DR-Site-Subnetz) einen EC2 Platzhalter-AMS-Stack mit den richtigen Tags. Weitere Informationen finden Sie im vorherigen Abschnitt. Wir empfehlen, den Stack mithilfe von CFN-Ingestion zu erstellen, da Sie die Schritte des Zuweisens von Sicherheitsgruppen und des Kennzeichnens der Instance, des EBS-Volumes und anderer Elemente (wie das Hinzufügen der Instance zu einem ELB) im selben Stack kombinieren können.

Typ ändern: Bereitstellung, Aufnahme, Stapel aus Vorlage, Erstellen CloudFormation

2. Stoppen Sie die Platzhalterinstanz.

Typ ändern: Verwaltung, Erweiterte Stack-Komponenten, EC2 Instanz, Stopp

3. Falls nicht in Schritt 1, kennzeichnen Sie die Platzhalterinstanz und ihr EBS-Volume mit dem Schlüssel: "AWSDRS,, Wert:" "AllowLaunchingIntoThisInstance.

Änderungstyp: Verwaltung, Erweiterte Stack-Komponenten, Tag, Update.

4. Verwenden Sie die Platzhalterinstanz aus Schritt 1 als Ziel unter Instanz-ID starten, DRS-Starteinstellungen für den Quellserver. Initiieren Sie den Instance Recovery Drill von der Elastic Disaster Recovery-Konsole für den Quellserver aus.

 Note

Die Platzhalter-Instance-Volumes werden im Konto beibehalten. Um diese Volumes zu löschen, reichen Sie am Ende des Disaster Recovery-Vorgangs einen Änderungstyp Management | Advanced Stack Components | EBS Volume | Delete (ct-3e3h8u0sp5z80) ein.

Elastischer Wiederherstellungsablauf für Disaster Recovery:

- Die Zielinstanz (Platzhalter) muss sich im Status „Gestoppt“ befinden
- Tauschen Sie die Volumes aus und löschen Sie das Quell-Stammvolume (Platzhalter)
- Starten Sie die Instanz
- Führen Sie die Post-Launch-Aktionen aus, um die folgenden Aufgaben abzuschließen:
 - Aktivieren Sie den SSM-Agenten.

- Tauschen Sie die Volumes aus und löschen Sie das Quell-Stammvolume (Platzhalter).
- Starten Sie die Instanz
- Führen Sie das PostLaunchScript SSM-Dokument aus. Dieses Dokument enthält folgende Funktionen:
 1. Verlässt die alte Domain.
 2. Ändert den Hostnamen.
 3. Starten Sie neu. AMS-Bootstrap-Skripts verbinden die Instance beim Start mit der Zieldomäne (DR).

Patchverwaltung in AMS

Themen

- [AMS Patch Orchestrator: ein tagbasiertes Patching-Modell](#)
- [Verwenden von Patch Orchestrator](#)
- [Patchen auf Abruf](#)
- [AMS-Standard-Patching](#)
- [Serviceverpflichtungen für Patches](#)

In AMS ist Patch Management ein Service, der Sie dabei unterstützt, Betriebssystemanbieter-Updates für Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu verwalten. Sie haben die Freiheit, die Häufigkeit und den Prozess des Patchens Ihrer EC2 Amazon-Instances individuell anzupassen.

Sie konfigurieren das Patch-Management während des Onboardings und können es mithilfe des RFC-Prozesses aktualisieren. Stacks, die mit dem Change-Management-System und einer patch-kompatiblen Vorlage (für Amazon EC2, Auto Scaling Scaling-Gruppe, einstufiger oder zweistufiger HA-Stack) erstellt wurden, werden automatisch für das Patch-Management abonniert.

AMS bietet eine Funktion, Patch Orchestrator — tagbasiertes Patchen, für die Konfiguration von Patches.

Definitionen von Patching-Begriffen finden Sie unter. [Die wichtigsten Begriffe von AMS](#)

Important

- Stacks oder die einzelnen Instances eines Stacks können das Patch-Management nicht deaktivieren, wenn die AMS-Vorlage, aus der der Stack erstellt wurde, mit dem Patch-Management kompatibel ist. Derzeit ist das Patchen mit den folgenden Stack-Vorlagen kompatibel:
 - EC2 Amazon-Stack | Erstellen und EC2 Amazon-Stack | Erstellen (mit zusätzlichen Volumes)
 - EC2 Amazon-Instance wurde mit CloudFormation Ingest gestartet
 - Auto Scaling Scaling-Gruppe | Erstellen (die EC2 Amazon-Instances in der Gruppe sind gepatcht)

- Einstufiger Hochverfügbarkeits-Stack | Erstellen und zweistufiger Hochverfügbarkeits-Stack | Erstellen
- Wenn ein andauernder Vorfall einen Stack betrifft, können AMS-Betreiber geplante Patches verschieben oder stornieren.
- Standardmäßig werden alle Instances innerhalb eines bestimmten patch-kompatiblen Stacks direkt gepatcht. Um Auto Scaling Scaling-Gruppen mithilfe des latest/patched AMS-AMI mit einem Amazon Machine Image (AMI) -Ersatz zu patchen, reichen Sie eine Serviceanfrage ein. Aktualisierungen AMIs werden jeden Monat an Konten weitergegeben.

Important

Sie können alternative Patch-Repositorys für verwaltete Knoten angeben. AMS implementiert zwar Ihre angeforderten Patch-Konfigurationen, Sie sind jedoch dafür verantwortlich, die Sicherheit Ihrer ausgewählten Repositorys auszuwählen und zu überprüfen. Sie müssen auch alle Risiken akzeptieren, die sich aus der Nutzung dieser Repositorien ergeben, wie z. B. Risiken in der Lieferkette.

Im Folgenden finden Sie bewährte Methoden für die Sicherheit Ihres Patch-Management-Prozesses:

- Verwenden Sie nur vertrauenswürdige, verifizierte Repository-Quellen
- Verwenden Sie nach Möglichkeit standardmäßig standardmäßige Repositorys von Betriebssystemanbietern
- Prüfen Sie regelmäßig benutzerdefinierte Repository-Konfigurationen

Tip

AMS empfiehlt, Backups für Instances zu aktivieren, die wertvolle Anwendungen oder Dienste enthalten. Hinweise zur Aktivierung von Backups finden Sie unter [Kontinuitätsmanagement in AMS Advanced](#).

AMS Patch Orchestrator: ein tagbasiertes Patching-Modell

Wenn Sie in das neue tagbasierte Patch-Modell von AMS Patch Orchestrator integriert wurden, können Sie Tags verwenden, um Ihre Patch-Konfiguration auf eine bestimmte Gruppe von Ressourcen anzuwenden, die als Patch-Gruppe bezeichnet werden und von einer Instanz bis zu all Ihren Instances reichen. [Informationen zu AMS-Tags finden Sie unter Verwenden von Tags.](#) Anweisungen zur Einrichtung von Patch Orchestrator-Tags finden Sie im folgenden Abschnitt.

Patches werden in den Patchfenstern installiert, die Sie mit [SSM Patch Window](#) | Create definieren. Jedes Patch-Fenster ist ein AWS Systems Manager Manager-Wartungsfenster, das nach einem Zeitplan Ihrer Wahl ausgeführt wird, eine konfigurierte Dauer hat und für eine Patch-Gruppe gilt. Instances, die nicht Teil eines expliziten Patchfensters sind, werden während des Standard-Wartungsfensters gepatcht, das Sie beim Onboarding in Patch Orchestrator definieren.

Important

Wenn mehrere Patch-Wartungsfenster so geplant sind, dass sie gleichzeitig ausgeführt werden, müssen weniger als 1001 Instanzen gleichzeitig verarbeitet werden. Dies ist eine Beschränkung von AWS Systems Manager. AMS empfiehlt mindestens eine Stunde pro fünfzig Instances.

Standardmäßig werden alle vom Hersteller des Betriebssystems (OS) bereitgestellten Patches während eines Wartungsfensters oder eines On-Demand-Patches installiert. Dies wird als Standard-Patch-Baseline bezeichnet. Wenn Sie einschränken möchten, welche Patches installiert werden, können Sie eine benutzerdefinierte Patch-Baseline definieren, indem Sie eine der Patch-Baselines erstellen CTs (per OSes), siehe [Unterkategorie Patchen](#). Sie können beispielsweise eine benutzerdefinierte Patch-Baseline verwenden, sodass nur kritische und wichtige Sicherheitsupdates für eine oder mehrere Patchgruppen installiert werden.

Nachdem Patches auf einer Instanz installiert wurden, wird die Instanz neu gestartet. Patch-Benachrichtigungen werden vor und nach dem Patchen gesendet, und innerhalb von 96 Stunden vor dem geplanten Start wird eine zusätzliche Erinnerung gesendet. Darüber hinaus aktualisiert AMS die Tools zur Infrastrukturverwaltung (z. B. den AWS SSM-Agenten) während des ausgewählten Wartungsfensters.

⚠ Important

AMS hat die monatliche Berichterstattung zur Einhaltung von Patches für Instances mit fehlenden Patches eingestellt und wird keine monatlichen Berichte mehr versenden. Diese Änderung wurde vor dem Hintergrund der kürzlich veröffentlichten Self-Service-Betriebsberichte vorgenommen, die alle 24 Stunden aktualisiert werden, Ihnen bei Bedarf zur Verfügung stehen und die aktuellsten und detailliertesten Daten liefern. Weitere Informationen zu den Berichten finden Sie unter Self-Service-Berichterstattung. Weitere Informationen zu den Berichten finden Sie unter [Self-Service-Berichte](#).

Weitere Informationen zu den Benachrichtigungen finden Sie unter [Patch-Benachrichtigungen](#).

Verwenden von Patch Orchestrator

Aktivieren Sie AMS Patch Orchestrator für Ihr Konto, indem Sie eine Serviceanfrage einreichen, die die folgenden Details enthält:

- Kategorie: Andere
- Betreff: Integriert in Patch Orchestrator
- CC-E-Mails: CC-E-Mail-Adressen erhalten Benachrichtigungen, wenn sich der Status dieses Onboarding-RFC ändert
- Details: Fügen Sie die folgenden Informationen in die E-Mail ein und geben Sie Ihre Werte ein. Beachten Sie, dass das optional ThirdTagKey ist. Empfehlungen und Beispiele finden Sie in der folgenden Tabelle.

```
Default maintenance window Schedule:  
Default Maintenance Window Schedule TimeZone:  
Default Maintenance Window Duration:  
Default Maintenance Window Cutoff:  
Default Patch Backup Retention In Days:  
Default Maintenance Window Notification Emails:  
First Tag Key:  
Second Tag Key:  
Third Tag Key:
```

In der folgenden Tabelle werden das Format und die Empfehlungen für Ihre angegebenen Werte beschrieben.

Patch-Konfigurationen auf Basis von Patch-Orchestrator-Tags

Name des Parameters	Informationen	Empfehlung oder Beispiel
Standardzeitplan für das Wartungsfenster	Der Zeitplan des Standard-Wartungsfensters in Form eines Cron- oder Ratenausdrucks. Beispiel: • <code>cron(0 3 ? * 6L *)</code>: 03:00 Uhr am letzten Freitag im Monat • <code>rate(7 days)</code>: Alle sieben Tage Weitere Informationen zum Erstellen von Cron-Ausdrücken und Links zu Ressourcen für Cron- und Rate-Ausdrücke finden Sie unter Cron- und Rate-Ausdrücke für Wartungsfenster.	Wir empfehlen, das Fenster mindestens einmal pro Monat an einem gleichbleibenden Wochentag laufen zu lassen.
Standard-Wartungsfenster, Zeitplan, Zeitzone	Die Zeitzone, auf der das Standard-Wartungsfenster läuft, im Format Internet Assigned Numbers Authority (IANA).	Beispiel: • Amerika/Los_Angeles • ETC/UTC
Standarddauer des Wartungsfensters	Die Dauer des Standard-Wartungsfensters in Stunden.	Mindestens 1 Stunde pro 50 Instanzen, plus 2 Stunden für den Cutoff.
Standardmäßiger Cutoff für das Wartungsfenster	Die Anzahl der Stunden vor dem Ende des Standard-	Mindestens 2 Stunden.

Name des Parameters	Informationen	Empfehlung oder Beispiel
	Wartungsfensters, in denen keine neuen Patchbefehle gestartet werden. Dieses Intervall ist so gewählt, dass genügend Zeit für den Abschluss des Patches zur Verfügung steht, bevor das Fenster endet.	
Standardmäßige Aufbewahrung von Patch-Backups in Tagen (optional)	Die Standarddauer in Tagen für die Aufbewahrung der EBS-Wiederherstellungspunkte, die vor dem Patchen von Instanzen erstellt wurden.	Wir empfehlen, die Standardinstellung beizubehalten, die 60 ist.
Standard-Benachrichtigungs-E-Mails für das Wartungsfenster	Ein bis fünf E-Mail-Adressen oder Verteilerlisten, um Benachrichtigungen über den Status der standardmäßigen Patches im Wartungsfenster zu erhalten.	Wir empfehlen, Gruppenverteilerlisten anstelle von einzelnen E-Mails zu verwenden.
Erster Tag-Schlüssel	Der erste Tag-Schlüssel, den Sie für die Erstellung Ihrer Patch-Group-Tag-Werte verwenden können.	Zum Beispiel. Appld Geben Sie Null an, wenn Sie bereits Ihre eigenen Patchgruppen mit einem Patchgruppen-Tag definiert haben.
Zweiter Tag-Schlüssel	Der zweite Tag-Schlüssel, den Sie für die Erstellung Ihrer Patch-Group-Tag-Werte verwenden können.	Zum Beispiel Umgebung. Geben Sie Null an, wenn Sie bereits Ihre eigenen Patchgruppen mit einem Patch Group-Tag definiert haben.

Name des Parameters	Informationen	Empfehlung oder Beispiel
Dritter Tag-Schlüssel (optional)	Der optionale dritte Tag-Schlüssel, den Sie für die Erstellung Ihrer Patch-Gruppen-Tag-Werte verwenden können.	Zum Beispiel Group.

Nachdem Sie in das neue Patch-Servicemodell von Patch Orchestrator integriert wurden, gehören alle entsprechend markierten Instanzen in Ihrem Konto zu einer Patch-Gruppe mit einem Patch Group-Tag. Patch Orchestrator verwendet entweder Ihr vorhandenes Patch Group-Tag oder ein von AMS erstelltes Tag, das aus den zwei oder drei verketteten Tag-Werten besteht, die Sie beim Onboarding von Patch Orchestrator angegeben haben. Zum Beispiel `{ } - { } - { }Tag Value 1. Tag Value 2 Tag Value 3` AMS aktualisiert diese von AMS angewandten Patch Group-Tags alle 12 Stunden. Bei Bedarf können Sie die Tagwerte Ihrer Patchgruppe mit den [Änderungstypen Tag | Update \(Überprüfung erforderlich\)](#) oder [Tag | Update \(Überprüfung erforderlich\)](#) aktualisieren.

Wenn Ihre EC2 Amazon-Instance beispielsweise die folgenden Tag-Schlüssel:Wert-Paare hat:

- AppId:MyApplication
- Environment:Production
- Group:1

Beim Onboarding haben Sie die folgenden Tag-Schlüssel angegeben:

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS erstellt das folgende Patch Group-Tag und wendet es auf Ihre Instances an: Patch Group:MyApplication-Production-1.

Note

Patch-Fehlerwarnungen werden nicht für Instances erstellt, deren Betriebssysteme nicht unterstützt werden oder die während des Wartungsfensters gestoppt werden.

Voraussetzungen für Patch Orchestrator

Der Patch Orchestrator-Workflow zielt auf EC2 Amazon-Instances ab, die mit der neuesten Version des System Manager Automation-Dokuments gepatcht wurden: `AWSManagedServices-PatchInstanceFromMaintenanceWindow`

Als Teil des Dokumenten-Workflows wird das Befehlsdokument „AWS-RunPatchBaseline“ für jede EC2 Amazon-Instance aus den Mitgliedern der Patchgruppe ausgeführt. Weitere Informationen finden Sie unter [Über das SSM-Dokument AWS- RunPatchBaseline](#).

Voraussetzungen:

- EC2 Amazon-Instance, die über das von AMS bereitgestellte Amazon Machine Image (AMI) oder auf einem AMI über das CT „Stack from migration partner migrated instance“ (ct-257p9zjk14ija) bereitgestellt wird.
- Ausgangsinternetverbindung aktiviert. Für firewall/proxy Lösungen müssen Windows-Update-Endpunkte, and/or Linux-Repository-Spiegelendpunkte, AWS-Systemmanager-Proxysteinstellungen und Metadaten-Proxykonfiguration zugelassen werden. Weitere Informationen finden [Sie unter SSM-Agent für die Verwendung eines Proxys konfigurieren und Verwenden eines HTTP-Proxys](#)
- Die IAM-Rolle entspricht dem zulässigen Mindestzugriff für den SSM-Dienst oder die IAM-Rolle. `customer-mc-ec2-instance-profile`
- Wir empfehlen 10 GB verfügbaren Root-Partitionsspeicher. Für Linux-Betriebssysteme sind mindestens 2 GB in der `/var` Partition verfügbar.
- Funktionierende und gültige Zertifizierungsstelle für das Herunterladen von Updates.
- Windows Server Update Services (WSUS) — Registrierung, einschließlich, aber nicht beschränkt auf: `DisableWindowsUpdateAccess`, `NoWindowsUpdate`; Automatische Updates dürfen den Betrieb des Windows Update-Prozesses nicht beeinträchtigen.

Validierung:

- Für Linux-Betriebssysteminstanzen, die den Yum Package Manager verwenden, können Sie die Verfügbarkeit von Updates überprüfen, indem Sie folgenden Befehl ausführen `#yum check-update`
- Für Linux OS RedHat 5.7 und neuer, 6.1 und neuer und 7.0 und neuer; EC2 Amazon-Instances, die über das CT „Stack from migration partner migrated instance“ (ct-257p9zjk14ija) auf Ihr AMS-Konto migriert wurden, müssen Sie den Abonnement-Manager-Status für die Aktualisierungsleistung überprüfen.

- Aktivieren Sie unter Windows OS Windows Server Update Services (WSUS). Keine lokale Richtlinie sollte die Fähigkeit von WSUS zum Scannen oder Installieren von Updates blockieren. Sobald Sie sich als Administrator angemeldet haben, können Sie es überprüfen, indem Sie von der Windows Update Service-Konsole aus nach verfügbaren Updates suchen. Windows Server-Betriebssystemversionen, einschließlich 2012R2, 2016 und 2019, verfügen über Standardeinstellungen für Windows Update zum Herunterladen und Installieren. Sie können die gewünschten Einstellungen vor dem Scannen konfigurieren. Bei späteren Betriebssystemversionen kann dieser Vorgang die Installation auslösen. Konfigurieren Sie das gewünschte Verhalten vorher.
- Fordern Sie vom AMS Operations Team eine Validierung an, indem Sie eine Serviceanfrage einreichen: „AWSManagedServices-CheckPatchingPrerequisites Automatisierungsdokument zur Ausführung auf EC2 Amazon-Instance zur Bewertung der Patch-Bereitschaft“.

Note

Patch-Fehlerwarnungen werden nicht für Instances erstellt, deren Betriebssysteme nicht unterstützt werden oder die während des Wartungsfensters gestoppt werden.

Fenster patchen

Instanzen in einer bestimmten Patchgruppe werden in einem oder mehreren Patchfenstern gepatcht. Patchfenster werden nach einem Zeitplan ausgeführt, der als Cron- oder Rate-Ausdruck definiert ist, und haben eine konfigurierbare Dauer, sodass die mit dem Patchen verbundenen Unterbrechungen innerhalb eines bestimmten Zeitintervalls gehalten werden. AMS empfiehlt, mehrere Patchfenster zu erstellen, die alle Ihre Instanzen gemeinsam abdecken, um den spezifischen Patching-Routinen Ihres Unternehmens zu entsprechen, und das standardmäßige Wartungsfenster als Ausweichlösung zu verwenden. Patchfenster werden mit dem RFC-Änderungstyp `Deployment | Patching | SSM-Patchfenster | Create (ct-0e12j07llrxs7)` erstellt. Alle Instanzen, die nicht Teil eines Patchfensters sind, werden während des Standard-Wartungsfensters gepatcht, das beim Onboarding erstellt wurde.

Normalerweise muss ein Patch-Fenster nicht aktualisiert werden, um neue Instanzen aufzunehmen. In der Regel erfolgt dies durch Ändern von Instanz-Tags. Stellen Sie sich zum Beispiel die folgende Abfolge von Ereignissen vor:

1. Zwei Instanzen sind mit `AppId:MyApplication,Environment:Production,` markiert `Group:1`.

Dadurch wird ein Tag für diese Instances erzeugt, vorausgesetzt, Erster Tag-Schlüssel = Appld, Zweiter Tag-Schlüssel = Umgebung, Dritter Tag-Schlüssel = Gruppe und ein Patchfenster für die Patchgruppe MyApplication -Production-1 wird erstellt.

2. Drei weitere Instanzen werden erstellt und mit `AppId:MyApplication,,` gekennzeichnet.
`Environment:Production Group:1`

Dadurch wird ein Tag für die Patchgruppe erzeugt: MyApplication -Production-1.

Es ist keine Änderung am Patchfenster erforderlich, da es alle fünf Instanzen beim nächsten geplanten Start übernimmt.

Eine ausführlichere Erläuterung und eine exemplarische Vorgehensweise zur Verwendung dieses Änderungstyps finden Sie unter [SSM-Patchfenster | Erstellen](#).

Patch-Benachrichtigungen

Important

Ab dem 1. Februar 2025 erhalten AMS-Kunden in ihren verwalteten Konten keine Benachrichtigungen mehr, wenn das Fenster zur Patch-Wartung leer ist.

Die abonnierten E-Mail-Adressen (bis zu fünf) erhalten kurz vor Beginn des Patch-Wartungsfensters eine E-Mail, die der folgenden ähnelt:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
2020-02-21T12:02:18.196Z.
Details:
Maintenance Window AccountId: YOUR_ACCOUNT_ID
Maintenance Window Region:   YOUR_ACCOUNT_REGION
Maintenance Window Id:       THE_MAINTENANCE_WINDOW_ID
Maintenance Window Name:     THE_MAINTENANCE_WINDOW_NAME
Maintenance Window Description: MaintenanceWindow for patching patch
Group PATCH_GROUP_NAME
Maintenance Window Patch Group: PATCH_GROUP_NAME
Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
InstanceId      InstanceName      StackId
```

THE_INSTANCE_ID *THE_INSTANCE_NAME* *THE_STACK_NAME*

A follow-up message with a detailed report is sent as soon as the maintenance window is over.

Please raise a service request if you have any inquiries about AMS Patch Orchestrator by following this URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Am Ende der Patch-Aktivität erhalten die abonnierten E-Mail-Adressen eine E-Mail, die der folgenden ähnelt:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* ended at:
2020-02-21T12:03:20.058Z, with status: SUCCESS.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
Maintenance Window Region: *YOUR_ACCOUNT_REGION*
Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

RfcId	InstanceId	InstanceName	StackId
Status			

THE_RFC_ID *THE_INSTANCE_ID* *THE_INSTANCE_NAME* *THE_STACK_NAME*
STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications by following this URL:

<https://console.aws.amazon.com/managedservices/incident/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Alle 96 Stunden identifiziert das AMS-Patching-System alle bevorstehenden Wartungsfenster mit Patch-Verwaltung innerhalb dieser 96 Stunden und sendet eine Erinnerungsbenachrichtigung an alle abonnierten E-Mail-Adressen, die in dieses 96-Stunden-Fenster fallen. Dies kann nur eine Stunde vor Ablauf des Zeitfensters oder die vollen 96 Stunden sein. Beispiel:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* will start at:
2020-05-06T16:35:36.523Z.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
Maintenance Window Region: *YOUR_ACCOUNT_REGION*
Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
Maintenance Window Schedule: rate(24 hours)
Maintenance Window Timezone: *THE_TIMEZONE*

At this time, these are the instances in the "*PATCH_GROUP_NAME*" Patch Group:

InstanceId	InstanceName	StackId	InstanceState

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Patch-Baselines

Standardmäßig werden alle vom Betriebssystemanbieter bereitgestellten Patches unter Verwendung der AMS-Standard-Patch-Baseline installiert. Wenn Sie einschränken möchten, welche Patches installiert werden, können Sie optional eine Patch-Baseline mit dem RFC-Änderungstyp Deployment | Patching | SSM-Patch-Baseline | Create erstellen erstellen **OS** (CT-ID variiert je nach Betriebssystem).

[Informationen zur Verwendung dieser Änderungstypen finden Sie in der Unterkategorie Patchen.](#)

Für Patch Orchestrator reservierte Tags

Patch Orchestrator generiert außerdem die folgenden Tags, die nicht geändert werden können:

- **AMSPatchGruppe** — Dieses Tag wird für die Generierung von Patch Group-Tagwerten verwendet. Sie sollten die AMSPatch Gruppe nicht ändern. Sie können das Tag „Patch Group“ ändern, wenn Sie einen benutzerdefinierten Wert für „Patch Group“ verwenden möchten. Patch Orchestrator generiert weiterhin einen Wert für AMSPatch Group auf der Grundlage der beim Onboarding bereitgestellten Tag-Schlüssel, ändert jedoch nicht den Tag-Wert „Patch Group“, wenn er von Ihnen auf einen benutzerdefinierten Wert festgelegt wurde. Um die Verwendung eines benutzerdefinierten „Patch Group“-Werts zu beenden, können Sie den Wert von „Patch Group“ so einstellen, dass er dem Wert des Gruppen-Tags entspricht. AMSPatch
- **AMSDefaultPatchGroup** — Dieses Tag gibt mit einem Wert von entweder True oder False an, ob eine Instanz Teil des Standard-Wartungsfensters ist. Wenn die Patch-Gruppe einer Instanz keinem Wartungsfenster zugewiesen ist, wird dieser Wert auf True gesetzt.

Patchen auf Abruf

AMS verfügt über einen Änderungstyp, der mit Ihrer Patch-Baseline zusammenarbeitet, sodass Sie bei Bedarf einen Patch für Instances ausführen können. Dies kann entweder die Standard-Baseline sein, die Sie beim Onboarding festgelegt haben, oder die Patch Orchestrator Systems Manager Manager-Patch-Baseline, die Sie mit dem Änderungstyp Patch-Baseline festgelegt haben (CT-ID variiert je nach Betriebssystem).

Sie können den Änderungstyp für On-Demand-Patching mit oder ohne Patch Orchestrator verwenden.

Informationen zur Verwendung dieses Änderungstyps finden Sie unter [On-Demand-Patching | Ausführen](#).

Note

Sie können Instances, die Teil einer Auto Scaling Scaling-Gruppe sind, nicht in einem On-Demand-Patching-Änderungstyp verwenden.

AMS-Standard-Patching

AMS unterstützt Bestandskunden, die das AMS-Standard-Patching-Modell verwenden, aber dieses Modell ist nicht für Neukunden verfügbar und wird zugunsten von AMS Patch Orchestrator eingestellt.

Typische Patch-Inhalte für AMS-Standard-Patches umfassen Herstellerupdates für unterstützte Betriebssysteme und Software, auf der unterstützte Betriebssysteme vorinstalliert sind (z. B. IIS und Apache Server).

Beim AMS-Onboarding geben Sie die Patchanforderungen, die Richtlinien, die Häufigkeit und die bevorzugten Patchfenster an. Durch diese Konfigurationen können Sie vermeiden, Anwendungen für Infrastruktur-Patches auf einmal offline zu schalten, sodass Sie kontrollieren können, welche Infrastruktur wann gepatcht wird.

Note

Der in diesem Thema beschriebene Patchvorgang gilt nur für Ihre Stacks. Die AMS-Infrastruktur wird in einem separaten Prozess gepatcht. Das AWS Managed Services

Maintenance Window (oder Maintenance Window) führt Wartungsaktivitäten für AWS Managed Services (AMS) durch und findet jeden zweiten Donnerstag im Monat von 15:00 Uhr bis 16:00 Uhr pazifischer Zeit statt. AMS kann das Wartungsfenster 48 Stunden im Voraus ändern. Sie konfigurieren das AMS-Patchfenster beim Onboarding oder genehmigen oder lehnen die monatliche Patch-Service-Benachrichtigung ab.

AMS durchsucht regelmäßig verwaltete EC2 Amazon-Instances nach Updates, die über die Aktualisierungsfunktion des Betriebssystems verfügbar sind. Wir bieten auch regelmäßige Updates für die AMS-Basis Amazon Machine Images (AMIs), die in unserer Umgebung unterstützt werden.

Nach ihrer Validierung werden AMS-AMI-Releases mit allen AMS-Konten geteilt. Sie können die verfügbaren AWS-AMI-Versionen mithilfe des [DescribeImages](#) EC2 Amazon-API-Aufrufs oder der EC2 Amazon-Konsole anzeigen. Informationen zu verfügbaren AMS AMIs finden Sie unter [Finde AMI IDs, AMS](#).

AMS führt Ad-hoc-Patching-Zeitpläne nur dann durch, wenn Sie dies wünschen. Bisher hat AMS eine Benachrichtigung gesendet; derzeit wird keine Benachrichtigung gesendet.

Note

Standardmäßig verwendet AMS Systems Manager, um Patches anzuwenden, indem der Paketmanager (Linux) oder der Systemaktualisierungsdienst (Windows) sein Standard-Repository abfragt, um zu sehen, welche neuen Pakete verfügbar sind. Wenn Sie im Laufe Ihrer day-to-day Operationen mithilfe des Standard-Paketmanagers ein Paket auf einem Linux-Host installiert haben, nimmt dieser Paketmanager auch neue Pakete für diese Software auf, sobald sie verfügbar sind. In einem solchen Fall möchten Sie vielleicht eine Patch-Aktion (in diesem Abschnitt beschrieben) ergreifen, um sich von dieser Instanz abzumelden.

Unterstützte Betriebssysteme

Unterstützte Betriebssysteme (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (voraussichtliches Enddatum des AMS-Supports am 30. Juni 2026)
- Oracle Linux 9.x, 8.x

- RedHat Enterprise Linux (RHEL) 9.x, 8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server für SAP 15 SP3 und höher
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Unterstützte Betriebssysteme () ARM64

- Amazon Linux 2023
- Amazon Linux 2 (voraussichtliches Enddatum des AMS-Supports am 30. Juni 2026)

Unterstützte Patches

AWS Managed Services unterstützt Patches hauptsächlich auf Betriebssystemebene. Die installierten Patches können sich je nach Betriebssystem unterscheiden.

Important

Alle Updates werden von den Remote-Repositorys des Systems Manager Patch Baseline Service heruntergeladen, die auf der Instanz konfiguriert sind und später in diesem Thema beschrieben werden. Die Instanz muss in der Lage sein, eine Verbindung zu den Repositorys herzustellen, damit das Patchen durchgeführt werden kann.

Um den Patch-Baseline-Dienst für Repositorys zu deaktivieren, die Pakete bereitstellen, die Sie selbst verwalten möchten, führen Sie den folgenden Befehl aus, um das Repository zu deaktivieren:

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

Rufen Sie die Liste der aktuell konfigurierten Repositorys mit dem folgenden Befehl ab:

```
yum repolist
```

- Vorkonfigurierte Amazon Linux-Repositorys (normalerweise vier):

Repository-ID	Repository-Name
amzn-main/latest	AMZN-Hauptbasis
amzn-updates/neuestes	AMZN-Updatebasis
epel/x86_64	Zusätzliche Pakete für Enterprise Linux 6 - x86_64
pbis	Aktualisierungen der PBIS-Pakete

- Vorkonfigurierte Repositories für Red Hat Enterprise Linux (fünf für Red Hat Enterprise Linux 7 und fünf für Red Hat Enterprise Linux 6):

Repository-ID	Repository-Name
RHUI-Region- -7/x86_64 client-config-server	Red Hat Update Infrastructure 2.0 Client-Konfigurationsserver
RHUI-Region- /7Server/x86_64 rhel-server-releases	RedHat Enterprise Linux Server 7
RHUI-Region- /7Server/x86_64 rhel-server-releases	RedHat Enterprise Linux Server 7 RH Allgemein () RPMs
epel/x86_64	Zusätzliche Pakete für Enterprise Linux 7 - x86_64
pbis	Aktualisierungen der PBIS-Pakete

Repository-ID	Repository-Name
RHUI-Region- -6 client-config-server	Red Hat aktualisiert die Infrastruktur 2.0
RHUI-Region- rhel-server-releases	RedHat Enterprise Linux Server (6) RPMs

Repository-ID	Repository-Name
RHUI-Region- rhel-server-rh-common	RedHat Enterprise Linux Server 6 RH Allgemein () RPMs
Abstoßen	Zusätzliche Pakete für Enterprise Linux 6 - x86_64
pbis	Aktualisierungen der PBIS-Pakete

- Vorkonfigurierte CentOS 7-Repositorys (normalerweise fünf):

Repository-ID	Repository-Name
base/7/x86_64	CentOS-7 - Basis
Aktualisierungen/7/x86_64	CentOS-7 - Aktualisierungen
Extras/7/x86_64	CentOS-7 - Extras
epel/x86_64	Zusätzliche Pakete für Enterprise Linux 7 - x86_64
pbis	Aktualisierungen der PBIS-Pakete

- Für Microsoft Windows Server werden alle Updates mithilfe des Windows Update Agents erkannt und installiert, der für die Verwendung des Windows Update-Katalogs konfiguriert ist (dies schließt keine Updates von Microsoft Update ein).

Auf Microsoft Windows-Betriebssystemen verwendet Patch Manager die CAB-Datei wsusscn2.cab von Microsoft als Quelle für verfügbare Betriebssystem-Sicherheitsupdates. Diese Datei enthält Informationen über die sicherheitsrelevanten Updates, die von Microsoft veröffentlicht werden. Patch Manager lädt diese Datei regelmäßig von Microsoft herunter und verwendet sie, um die für Windows-Instanzen verfügbaren Patches zu aktualisieren. Die Datei enthält nur Updates, die von Microsoft als sicherheitsrelevant gekennzeichnet wurden. Während die Informationen in der Datei verarbeitet werden, entfernt Patch Manager auch Updates, die durch spätere Updates ersetzt wurden. Daher werden nur die neuesten Updates angezeigt und zur Installation zur Verfügung gestellt. Wenn beispielsweise KB4 012214 ersetzt KB3135456, wird nur KB4 012214 als Update in Patch Manager verfügbar gemacht.

Weitere Informationen zur Datei wsusscn2.cab finden Sie im Microsoft-Artikel [Using WUA to Scan for Updates Offline](#).

Patching und Infrastrukturdesign

AMS verwendet je nach Infrastrukturdesign unterschiedliche Patching-Methoden: veränderbar oder unveränderlich (detaillierte Definitionen finden Sie unter). [Die wichtigsten Begriffe von AMS](#)

Bei veränderlichen Infrastrukturen erfolgt das Patchen mithilfe einer traditionellen In-Place-Methode, bei der Updates direkt auf den EC2 Amazon-Instances einzeln von den Betriebstechnikern von AMS installiert werden. Diese Patching-Methode wird für Stacks verwendet, die keine Auto Scaling Scaling-Gruppen sind und eine einzelne EC2 Amazon-Instance oder einige Instances enthalten. In diesem Szenario würde das Ersetzen des AMI, auf dem die Instance oder der Stack basiert, alle Änderungen zunichte machen, die an diesem System seit der ersten Bereitstellung vorgenommen wurden, sodass dies nicht der Fall ist. Updates werden auf das laufende System angewendet, und es kann aufgrund von Anwendungs- oder Systemneustarts zu Systemausfällen kommen (abhängig von der Stack-Konfiguration). Dies kann mit einer Blue/Green Aktualisierungsstrategie abgemildert werden. Weitere Informationen finden Sie unter [AWS CodeDeploy Stellt Blue/Green Bereitstellungen vor](#).

Bei unveränderlichen Infrastrukturen ist die Patch-Methode der AMI-Ersatz. Unveränderliche Instances werden einheitlich mithilfe eines aktualisierten AMI aktualisiert, das das in der Auto Scaling Scaling-Gruppenkonfiguration angegebene AMI ersetzt. AMS-Versionen werden AMIs jeden Monat aktualisiert (d. h. gepatcht), normalerweise in der Woche, in der Patch Tuesday stattfindet. Im folgenden Abschnitt wird beschrieben, wie das funktioniert.

So funktioniert das AMS-Standard-Patching

AMS verwendet den Systems Manager Run Command-Service für regelmäßig geplante monatliche und nach Bedarf kritische Patches. Dabei gibt es je nach Ihrer Strategie zur Infrastrukturbereitstellung (veränderbar oder unveränderlich) zwei Hauptpatching-Methoden: direkt vor Ort und AMI-Ersatz. In diesem Abschnitt werden der AMS-Patch-Service, die Typen, Methoden und Prozesse beschrieben.

AMS definiert zwei Patch-Typen, die unterschiedlich geplant sind:

- **Kritisches Patchen:** Updates werden so schnell wie möglich installiert, nachdem die Benachrichtigung akzeptiert wurde.

- **Standard-Patches:** Regelmäßige Updates der Betriebssystemhersteller, die monatlich angewendet werden.

Patches werden entweder durch direktes Patchen oder durch AMI-Ersatz (auf Anfrage) installiert.

Scannen aktualisieren

AMS verwendet den [Amazon EC2 Run Command Service](#), um Ihre EC2 Amazon-Stacks zu kontaktieren und die erforderlichen Scan- und Patch-Skripts bereitzustellen. AMS verwendet die native Paketverwaltungskomponente, die bereits auf dem unterstützten Betriebssystem installiert ist, um das gesamte erforderliche Scan- und Patching-Verhalten auf dem EC2 Amazon-Stack durchzuführen. Für Red Hat und Amazon Linux verwendet der Service yum. Für Windows verwendet der Dienst den Windows Update Agent.

Scans werden täglich mit [SSM Maintenance Windows](#) und dem RunPatchBaseline AMS-Standard-AWS-Dokument durchgeführt. Jeder erreichbare EC2 Amazon-Stack wird mithilfe der Update-Repositorys für Linux und Windows gescannt. Der AMS-Patching-Prozess erkennt alle erreichbaren EC2 Amazon-Stacks und führt dann die Scans in einem Batch-Prozess durch, sodass der Stack immer in einem fehlerfreien Zustand bleibt, auch wenn während der Ausführung des Scans ein Fehler auftritt. Die Scanergebnisse werden dann für jeden EC2 Amazon-Stapel gespeichert.

Um die Scanergebnisse für einen Stack oder eine Instance einzusehen, reichen Sie eine Serviceanfrage mit der Stack-ID oder Instance-ID ein.

Das standardmäßige AMS-Patching-Verfahren besteht darin, alle verfügbaren Patches unabhängig von der Patch-Klassifizierung oder dem Schweregrad (z. B. „Kritisch“ oder „Standard“) zu installieren. Eine Ausnahme bilden Patches, die Sie ausdrücklich für den Stack ausgeschlossen haben (Patches, die von AMS als obligatorisch definiert wurden, sollten nicht ausgeschlossen werden).

Sie erhalten 14 Tage vor dem geplanten Wartungsfenster eine Benachrichtigung über den Patch-Service. Auf diese Weise haben Sie Zeit, die vorgeschlagenen Patches zu testen und sie anzunehmen oder abzulehnen. Wenn Sie nicht auf die Benachrichtigung des Patching-Dienstes antworten, werden Ihre Instances nicht gepatcht. Wenn es an der Zeit ist, die Patches zu installieren, erstellt AMS einen Request for Change (RFC) für jeden Stack, und dieser RFC erscheint in der RFC-Liste Ihres Kontos.

AMS hat das Wartungsfenster und den Hinweis konfiguriert

Bei den von AMS konfigurierten Patches hat jedes Konto ein monatliches Wartungsfenster, das Sie beim Onboarding Ihres Kontos festlegen. Das AWS Managed Services Maintenance Window (oder

Maintenance Window) führt Wartungsaktivitäten für AWS Managed Services (AMS) durch und findet jeden zweiten Donnerstag im Monat von 15:00 Uhr bis 16:00 Uhr pazifischer Zeit statt. AMS kann das Wartungsfenster mit einer Vorankündigung von 48 Stunden ändern.

Das Patch-Zeitfenster ist anders. Die ausgehende Serviceanfrage zum Patchen (auch als Servicebenachrichtigung bezeichnet) enthält ein empfohlenes Patchfenster.

 Note

Hinweise zur Beantwortung der Benachrichtigung über den Patchdienst finden Sie unter [Aktionen, die Sie beim AMS-Standard-Patching ergreifen können](#)

Die Benachrichtigung über den Patchdienst wird per E-Mail an die für Ihr Konto hinterlegte Kontakt-E-Mail-Adresse gesendet. Die Benachrichtigung enthält einen Link zur AWS-Support-Konsole, über die Sie darauf antworten können. Sie können auf die Benachrichtigung auch über die AMS-Serviceanforderungsseite antworten. Die Servicemeldung beinhaltet:

- Eine Liste der Updates IDs (CSUs, und OUs) IUs, die für den Stack gelten, und der Updates, die Sie angefordert haben, werden vom Patchen ausgeschlossen (falls vorhanden).
- IDs der Instanzen, die betroffen sein werden.
- Ein empfohlenes Patch-Zeitfenster, in dem die Updates installiert werden. Sie können ein anderes Patchfenster anfordern.
- Eine Bitte, dass Sie das vorgeschlagene Patchen akzeptieren oder zusätzliche Informationen anfordern. AMS gibt Ihnen Zeit, um die Auswirkungen der Updates zu testen und das Patchen zu genehmigen oder abzulehnen oder um den Ausschluss bestimmter Updates zu bitten. Wenn Sie mehr Zeit zum Testen benötigen und möchten, dass die Updates nach dem Testen installiert werden, antworten Sie auf die Servicemeldung und beschreiben Sie, was Sie möchten, oder reichen Sie eine Serviceanfrage für einen neuen Patch-RFC ein, der auf den Details des vorherigen RFC basiert. Wenn Sie überhaupt nicht auf die Servicebenachrichtigung antworten, wird keine Patch-Aktion ergriffen und der RFC wird storniert.

Wenn Sie die Servicebenachrichtigung genehmigen, führt AMS den Patch-RFC aus und installiert die Updates innerhalb des vereinbarten Patchfensters gemäß der Serviceverpflichtung.

Wenn das Patchen abgeschlossen ist, sendet Ihnen AMS in der Serviceanfrage eine Nachricht mit einer Zusammenfassung des Ergebnisses der Patch-Aktivität (d. h. Erfolg oder Fehlschlag).

Patchen vor Ort

In-Place-Patching bezieht sich auf eine Methode, bei der sich AMS bei jeder Stack-Instance anmeldet und Patches anwendet.

In-Place-Patching erfolgt auf veränderlichen Infrastrukturen unter Verwendung von EC2 Amazon-Instances, auf denen ein unterstütztes Betriebssystem ausgeführt wird. Beim Patchen werden alle bis zu diesem Zeitpunkt verfügbaren Updates angewendet, die nicht ausgeschlossen wurden. Wenn kritische Patches veröffentlicht werden, findet ein zusätzlicher kritischer Patching-Prozess statt.

Standard-Patching: direkt vor Ort

Das Standard-Patching erfolgt nach dem vereinbarten Patch-Zeitplan, der in der Patchservice-Benachrichtigung vorgeschlagen wird, und umfasst regelmäßige Patch-Updates, die nicht als kritisch eingestuft werden.

Vor Ablauf des vorgeschlagenen Patch-Fensters und nach Ihrer positiven Antwort auf die Benachrichtigung wird ein Patch-RFC erstellt und in Ihrem RFC-Dashboard angezeigt.

Kritisches Patchen: vor Ort

Wenn ein Betriebssystemanbieter ein wichtiges Sicherheitsupdate veröffentlicht, benachrichtigt AMS Sie über den Patch-RFC, indem es Ihnen gemäß der AMS-Serviceverpflichtung eine Servicebenachrichtigung (an die Kontakt-E-Mail für Ihr Konto) für jeden Stack sendet. Die Servicebenachrichtigung beinhaltet für jedes Update Folgendes:

- Veröffentlichungsdatum aktualisieren
- Kritikalität aktualisieren
- Details aktualisieren (KB-Referenz usw.)
- IDs der betroffenen Stapel

Sie können die in der Benachrichtigung aufgeführten Updates testen und die Patches genehmigen oder ablehnen, indem Sie auf die Servicemeldung antworten. Wenn Sie die Benachrichtigung genehmigen, müssen Sie pro Stapel ein bestimmtes Patchfenster für die Installation der Updates angeben.

 Note

Patchfenster, die innerhalb von 24 Stunden nach der Antwort auf die Servicemeldung liegen, können je nach verfügbarer Kapazität neu geplant werden.

Wenn Sie nicht innerhalb von 10 Tagen antworten oder das vorgeschlagene Patching ablehnen, wird das Patching storniert.

Wenn Sie die Updates nach Ablauf des zulässigen Zeitraums (in der Benachrichtigung angegeben) installieren möchten, reichen Sie eine Serviceanfrage für einen neuen Patch-Zeitplan ein, der auf den Details der vorherigen Benachrichtigung basiert.

Wenn Sie die Servicemeldung genehmigen, installiert AMS die Updates innerhalb des von Ihnen angegebenen Patchfensters entsprechend der Serviceverpflichtung.

Bei mehreren Updates können Sie bestimmte Updates vom Patching ausschließen, indem Sie in Ihrer Antwort auf die Servicemeldung angeben, welche Updates ausgeschlossen werden sollen.

AMS sendet Ihnen für jeden Stack eine Servicebenachrichtigung über das Ergebnis jedes Updates (d. h. Erfolg oder Misserfolg).

Patchen von AMI-Updates (mithilfe von Patched AMIs für Auto Scaling Scaling-Gruppen)

AMI-Ersatz-Patches werden auf unveränderlichen Infrastrukturen durchgeführt, indem die AMI-ID aktualisiert wird, die für die Bereitstellung neuer EC2 Amazon-Instances in einer Auto Scaling Scaling-Gruppe konfiguriert ist.

Amazon Machine Images (AMIs) werden regelmäßig für die unterstützten Betriebssysteme veröffentlicht. Betriebssystemanbieter veröffentlichen in regelmäßigen Abständen neue Patches. AMS verwendet das von Amazon bereitgestellte AMI, aktualisiert es mit den neuesten Patches und fügt dann die entsprechenden Komponenten hinzu, damit es in der AMS-Umgebung betrieben werden kann. Anschließend wird das neue AMS-AMI allen AMS-Kunden zur Verfügung gestellt, indem das AMI mit den Konten geteilt wird. Ihre Auto Scaling Scaling-Gruppen-Stacks können mit diesen neu veröffentlichten AMS monatlich aktualisiert werden. AMIs Die folgende Grafik zeigt, wie Ihre Umgebungen in AMS verwendet AMIs werden.

Auto Scaling Scaling-Gruppen erstellen ihre Instances auf der Grundlage des konfigurierten AMI für die Auto Scaling Scaling-Gruppe. Wenn AMS-Freigaben aktualisiert werden AMIs, haben Sie je nachdem, wie Sie AMI-Updates verwalten, die folgenden Optionen:

- Wenn Sie ein Tool zur Anwendungsbereitstellung verwenden (z. B. UserData, CodeDeploy, usw.), das Ihre Instances nach ihrer Erstellung automatisch anpasst, können Sie wie folgt vorgehen:
 - Antworten Sie auf die Patching-Dienstbenachrichtigung oder reichen Sie eine Serviceanfrage ein, damit das neueste AMS-AMI das Konfigurations-AMI Ihrer aktuellen Auto Scaling Scaling-Gruppe ersetzt. Nachdem die AMI-ID in der Konfiguration Ihrer Auto Scaling Scaling-Gruppen ersetzt wurde, startet AMS fortlaufende Updates Ihrer Instances und Ihre Auto Scaling Scaling-Gruppen-Instance-Konfigurationen (z. B. die Installation von Anwendungen, Boot-Skripts usw.) werden automatisch auf die neuen Instances angewendet, die mit dem neuen AMS AMI erstellt wurden.
- Wenn Sie ein custom/golden AMI in der Konfiguration Ihrer Auto Scaling Scaling-Gruppen verwenden, können Sie:
 - Erstellen Sie eine Instanz mit dem neuen AMS-AMI, passen Sie die Instance an und erstellen Sie ein neues goldenes AMI. Teilen Sie das neue Golden AMI über die EC2 Amazon-Konsole mit AMS und senden Sie eine Serviceanfrage an AMS, um die Konfiguration Ihrer Auto Scaling Scaling-Gruppen für die Verwendung Ihres neuen benutzerdefinierten AMI zu aktualisieren.
 - Teilen Sie Ihr bestehendes goldenes AMI mithilfe der EC2 Amazon-Konsole mit AMS und reichen Sie eine Serviceanfrage für AMS ein, um Ihr goldenes AMI zu aktualisieren. Zu diesem Zweck erstellt AMS eine Instance aus Ihrem Golden AMI, wendet die Patches auf diese Instance an, erstellt ein neues Golden AMI für Sie und aktualisiert dann die Konfiguration Ihrer Auto Scaling Scaling-Gruppen, um das neue AMI zu verwenden. Der Nachteil dabei ist, dass AMS nicht testen kann, ob Ihr neues benutzerdefiniertes AMI so funktioniert, wie Sie es möchten. Stattdessen sollten Sie die mit dem neuen AMI erstellte Instance testen und sicherstellen, dass alles ordnungsgemäß funktioniert, bevor Sie ein neues goldenes AMI erstellen, es teilen und AMS auffordern, Ihre Auto Scaling Scaling-Gruppen zu aktualisieren. AMS empfiehlt diese Option nicht.

Standard-Patching: AMI-Updates

Jeden Monat veröffentlicht AMS neue Amazon Machine Images (AMIs) mit Serviceverbesserungen und neuen Patches, die für die gelten AMIs.

 Note

Neue AMS AMIs werden nach dem Patch Tuesday von der aktualisierten Version von AWS generiert. AMS testet sie dann, bevor sie verfügbar gemacht werden. Nach dem neuen AMIs bestandenen Test wurden die AMS-Aktien AMIs auf verwaltete Konten umgestellt.

Kritisches Patchen: AMI-Updates

Bei Bedarf stellt AMS AMIs aktualisierte Updates mit wichtigen Sicherheitspatches bereit, die seit der letzten monatlichen AMI-Version veröffentlicht wurden.

Das Verfahren für kritische Sicherheitsupdates für unveränderliche Infrastrukturen ist identisch mit dem monatlichen AMI-Prozess für unveränderliche Infrastrukturen, mit der Ausnahme, dass außerhalb des normalen Zeitplans (Patch Tuesday) ein neues AMS-AMI erstellt wird, das auf der Veröffentlichung neuer kritischer Updates basiert. AMS stellt ein neues AMI mit den kritischen Sicherheitspatches gemäß den für Ihr Konto definierten Service Level Agreements (SLAs) zur Verfügung. AMS-Updates von Auto Scaling Scaling-Gruppen nur auf Anfrage. Verwenden Sie eine Serviceanfrage, um AMI-Ersatzanfragen einzureichen.

Fehler beim AMS-Standard-Patchen

Im Falle fehlgeschlagener Updates führt AMS eine Analyse durch, um die Ursache des Fehlers zu ermitteln, und teilt Ihnen das Ergebnis der Analyse mit. Wenn der Fehler auf AMS zurückzuführen ist, wiederholen wir die Updates, sofern der Fehler innerhalb des Wartungsfensters liegt. Andernfalls erstellt AMS Servicemeldungen für das fehlgeschlagene Instance-Update und wartet auf Ihre Anweisungen.

Bei Ausfällen, die auf Ihr System zurückzuführen sind, können Sie eine Serviceanfrage mit einem neuen Patch-RFC einreichen, um die Instances zu aktualisieren.

Aktionen, die Sie beim AMS-Standard-Patching ergreifen können

Sie können nicht nur neue Produkte testen AMIs, sondern auch verschiedene Maßnahmen ergreifen, um das Patchen Ihrer Infrastruktur zu verwalten:

- Wenn das Testen der Updates länger gedauert hat, als es das Patchfenster erlaubt hat, können Sie AMS auffordern, die stornierten Updates zu installieren, wenn Sie bereit sind, indem Sie eine

Serviceanfrage einreichen (verwenden Sie die Details in der ursprünglichen Servicebenachrichtigung als Grundlage).

- Sie können beantragen, dass ein wichtiges Update (IU) oder ein anderes Update (OU) vor dem nächsten automatischen Aktualisierungsfenster installiert wird, indem Sie eine Serviceanfrage mit einer Liste der Updates, der entsprechenden Instanzen und gegebenenfalls weiteren Details einreichen. Da dieser CT nicht automatisiert ist, dauert es länger, ihn zu planen und auszuführen. Überprüfen Sie die Service-Level-Ziele (SLOs) für den entsprechenden Zeitpunkt. Weitere Informationen finden Sie unter [AMS-Servicelevel-Ziele \(SLOs\)](#).

Darüber hinaus können Sie vorhandene, gepatchte AMS verwenden, um benutzerdefinierte AMIs zu erstellen. Weitere Informationen finden Sie unter [AMI | Create](#).

Note

Sie können vor dem nächsten Wartungsfenster kein neues AMS-AMI auf der Grundlage eines wichtigen Updates oder eines anderen Updates anfordern, da der AMS-AMI-Freigabeprozess zum Vorteil aller AMS-Kunden einem einheitlichen Rhythmus folgt.

Ändert, was rauskommt patched/opting

Wenn das Patchen von AMS konfiguriert ist, können Sie in Ihrer Antwort auf die Benachrichtigung zum Patch-Service oder in einer Serviceanfrage ändern, welche Ressourcen gepatcht werden. Sie haben die folgenden Möglichkeiten:

- Definieren Sie pro Stack und Betriebssystem eine Liste von Patches, die von der Problembehebung ausgeschlossen werden sollen.
- Definieren Sie eine Liste von Ressourcen, die von bestimmten Patches oder allen Patches ausgeschlossen werden sollen.
- Definieren Sie eine Liste von Ressourcen, die immer von allen Patches ausgeschlossen werden sollen.
- Definieren Sie eine Liste von Ressourcen, die an einem bestimmten Tag und zu einer bestimmten Uhrzeit gepatcht werden sollen (gut, wenn Sie kein Wartungsfenster definiert haben).

Um einen oder mehrere Patches auszuschließen, reichen Sie eine Serviceanfrage ein oder antworten Sie mithilfe der im Folgenden bereitgestellten Vorlage auf die Benachrichtigung über den Patch-

Service. Reichen Sie keinen RFC ein. Geben Sie in der Anfrage den oder die Patch-Namen an, die Sie ausschließen möchten, und warum. Nehmen Sie diese Informationen wie folgt in eine Serviceanfrage auf:

- Name: Der Name des Patches. Bei Windows-Patches ist dies der KB-Name, z. KB3145384 B. Bei Linux-Patches ist dies der Paketname, z. openssh-6.6.1p1-25.61.amzn1.x86_64 B.
- Grund: Ein Kommentar, der angibt, warum der Patch ausgeschlossen wurde.
- Ablaufzeit: Der date/time Zeitpunkt, an dem der Ausschluss abläuft.

Wenn ein ausgeschlossener Patch bereits installiert ist, wird er entfernt.

Die Anfrage wird von einem Mitarbeiter geprüft, der mit Ihnen darüber spricht, ob der Ausschluss dieser Patches ein erhebliches Sicherheitsrisiko darstellt. Das Ablaufdatum ausgeschlossener Patches wird ebenfalls ausgehandelt. Nach dem vereinbarten Ablaufdatum läuft der Ausschluss ab und der Patch wird bei allen nachfolgenden Patches installiert.

Patches auf der Ausschlussliste werden weiterhin in den Scanergebnissen angezeigt, sofern zutreffend.

Note

Im Gegensatz zu Windows sind Linux-Patches versionsspezifisch. Diese Unterscheidung ist wichtig, da neue Versionen eines ausgeschlossenen Patches nicht automatisch ausgeschlossen werden. Es liegt in Ihrer Verantwortung, AMS darüber zu informieren, dass neue Versionen eines Linux-Patches ausgeschlossen werden, falls Sie dies wünschen.

Vorlagen für Antworten auf Patchservice-Benachrichtigungen

Sie müssen auf Benachrichtigungen des Patching-Dienstes im angegebenen Format antworten, damit das Patchen auf Ihren Instances durchgeführt werden kann. Sie sollten dies tun, wenn Sie bei AMS noch kein Wartungsfenster festgelegt haben.

Wenn Sie auf eine Servicemeldung antworten, verwenden Sie das angegebene Format.

Wenn kein Wartungsfenster festgelegt ist, teilen Sie uns wie folgt mit, wann ein Patch installiert werden muss:

UTC	StartTime	StackId	InstanceId (Optional)

2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

Wenn Sie ein festgelegtes Wartungsfenster haben und möchten, dass bestimmte Ressourcen von bestimmten Patches ausgeschlossen werden, verwenden Sie das folgende Format:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>
stack-123456789014	i-1234566783	<i>PATCH</i>
stack-123456789015	i-1234566782	<i>PATCH</i>

Wenn Sie ein festgelegtes Wartungsfenster haben und möchten, dass bestimmte Ressourcen immer von allen Patches ausgeschlossen werden, verwenden Sie das folgende Format:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL
stack-123456789015	i-1234566782	ALL

Vorbereitung für das Patchen

Um Ihre Umgebung auf automatisiertes Patchen vorzubereiten, empfehlen wir Folgendes:

- Stellen Sie sicher, dass Sie über ein vollständiges Inventar aller Instanzen verfügen, die gepatcht werden sollen.
- Stellen Sie sicher, dass Ihre Ressourcen im Rahmen Ihrer Geschäftskontinuitätsstrategie regelmäßig gesichert werden. Zusätzliche Backups werden als Teil der Patch-Sequenz erstellt und diese werden automatisch gemäß Ihrer konfigurierten Patch Orchestrator-Aufbewahrungsrichtlinie gelöscht (Standard ist 60 Tage).
- Stellen Sie sicher, dass alle relevanten Lizenzen auf dem neuesten Stand sind.
- Ändern Sie Ihre Stack-Wartungsfenster so, dass das Patchen gestaffelt wird, sodass Test-Stacks vor Produktionsstapeln gepatcht werden. Auf diese Weise werden alle Fehler beim Patchen in den Test-Stacks gefunden und können identifiziert werden, bevor die Produktions-Stacks gepatcht werden.

Patch-Einstellungen anzeigen

Um herauszufinden, wie Ihre aktuelle Patching-Konfiguration aussieht, können Sie wie folgt vorgehen:

- Senden Sie zusammen mit der Anfrage eine Serviceanfrage an AMS.
- Warten Sie auf eine Patch-Service-Benachrichtigung. Die Patching-Benachrichtigung informiert Sie über alle Patches, die installiert werden müssen, und über alle Instanzen, die gepatcht werden müssen, und schlägt außerdem ein Patch-Fenster vor.

Sie können eine Serviceanfrage einreichen, um Folgendes zu ändern:

- Scan-Intervall: Die Zeitspanne in Minuten zwischen Konformitätsscans, die an Instanzen dieses Stacks durchgeführt wurden.

Die Standardeinstellung ist 240 (4 Stunden).

- NotificationWindow: Wie weit im Voraus (in Minuten) vor einer geplanten Änderung (Patch) die Benachrichtigung an Sie gesendet werden soll. Die Standardeinstellung ist 10080 (7 Tage).

AMS-Standard-Patching FAQs

Dieser Abschnitt enthält Antworten auf einige häufig gestellte Fragen.

- F: Wie deaktiviere ich das weltweite Patchen?

A: Um das Patchen global zu deaktivieren, reichen Sie eine Serviceanfrage ein. Beachten Sie, dass Sie die obligatorischen AMS-Patches nicht abbestellen können. Alle Stacks werden weiterhin gescannt, damit wir über Sicherheitslücken berichten können.

- F: Wie schließe ich bestimmte Stacks vom Patchen aus?

A: Um bestimmte Stacks dauerhaft vom Patchen auszuschließen, reichen Sie eine Serviceanfrage ein. Um bestimmte Stacks von einem bestimmten Patch-Zyklus auszuschließen, antworten Sie auf die bevorstehende Patching-Benachrichtigung mit der Liste der Stacks, die ausgeschlossen werden sollen. Weitere Informationen finden Sie unter [Ändert, was rauskommt patched/optiming](#) . Beachten Sie, dass Sie sich von obligatorischen Patches nicht abmelden können.

- F: Was passiert, wenn ich eine Benachrichtigung über einen Patch-Service nicht genehmige?

A: Sie haben 14 Tage Zeit, um eine Standard-Patch-Serviceanfrage zu genehmigen, und 10 Tage, um eine kritische Patching-Benachrichtigung zu genehmigen. Wenn Sie die Serviceanfrage nicht innerhalb der Frist genehmigen, wird die Serviceverpflichtung für nichtig erklärt und es erfolgt kein Patching. Im Fall von obligatorischen Patches werden Patches unabhängig von der Antwort auf die Serviceanfrage installiert.

- F: Wie schließe ich bestimmte Patches und Pakete von der Installation aus?

A: Um bestimmte Patches oder Pakete dauerhaft auszuschließen, reichen Sie eine Serviceanfrage ein. Um bestimmte Patches oder Pakete aus einem bestimmten Patch-Zyklus auszuschließen, antworten Sie auf die bevorstehende Patchmeldung mit der Liste der auszuschließenden Patches oder Pakete. Details hierzu finden Sie unter [Ändert, was rauskommt patched/opting](#). Beachten Sie, dass Sie sich von obligatorischen Patches nicht abmelden können.

- F: Was passiert, wenn ein System aufgrund eines Patches ausfällt?

A: AMS überwacht jedes System. AMS sendet Ihnen eine Servicebenachrichtigung über das Ergebnis jedes Updates (d. h. Erfolg oder Misserfolg) pro Stack und Instanz. Wenn ein Fehler erkannt wird, untersucht AMS die Instance und stellt sie wieder her. Anschließend versucht ein AMS-Betriebsingenieur, das Patch manuell durchzuführen. Weitere Informationen finden Sie unter [Fehler beim AMS-Standard-Patchen](#).

- F: Welche Updates werden von AMS verwaltet?

A: AMS verwaltet Updates auf Betriebssystemebene, über die AMS vom Anbieter informiert wird. Weitere Informationen finden Sie unter [Unterstützte Patches](#).

- F: Welche Updates werden nicht von AMS verwaltet?

A: Updates auf Anwendungsebene werden nicht von AMS verwaltet.

- F: Wie werden Auto Scaling Scaling-Gruppen aktualisiert?

A: Auto Scaling Scaling-Gruppen werden in der Auto Scaling Scaling-Gruppenkonfiguration mit einem AMI-Ersatz aktualisiert und führen ein fortlaufendes Update durch. Bei einem fortlaufenden Update wird die HealthyHostThreshold Einstellung Ihrer Patching-Konfiguration berücksichtigt, die festlegt, wie viele EC2 Amazon-Instances in einem Stack während des Patchens aktiv bleiben müssen. Weitere Informationen finden Sie unter [Patchen von AMI-Updates \(mithilfe von Patched AMIs für Auto Scaling Scaling-Gruppen\)](#).

- F: Wie kann ich Updates außerhalb des normalen Zyklus installieren lassen?

A: Für Updates auf Betriebssystemebene, die Sie außerhalb des normalen Patching-Zeitplans installieren möchten, reichen Sie mithilfe der Patch-Benachrichtigung, die Sie erhalten haben, eine Serviceanfrage ein. Dies kann passieren, wenn das Testen eines vorgeschlagenen Patches länger als 21 Tage (für einen Standard-Patch) oder 14 Tage (für einen kritischen Patch) gedauert hat. Out-of-band Patches können für eigenständige EC2 Amazon-Instances direkt durchgeführt werden.

- F: Wie werden neu bereitgestellte Stacks oder Instances gepatcht?

A: Wenn Sie eine neue EC2 Amazon-Stack-Instance oder Auto Scaling Scaling-Gruppe erstellen, sollten Sie immer das neueste AMS-AMI angeben, auf dem bereits die neuesten Patches enthalten sind. Bei veränderlichen Infrastrukturen sollte Inline-Patching durchgeführt werden, sobald der Stack bereitgestellt ist.

Serviceverpflichtungen für Patches

Auf der Grundlage Ihrer Art der Infrastrukturbereitstellung und der Wichtigkeit des Updates bieten wir Serviceversprechen für wichtige Sicherheitsupdates für veränderliche und unveränderliche Infrastrukturen sowie für wichtige Updates für veränderliche und unveränderliche Infrastrukturen.

Standard-Patching

Dies sind AMS-Serviceverpflichtungen für Standard-Patching.

Standard-Patching, veränderbare Infrastruktur (In-Place-Patching)

Veranstaltung/Aktion	Messung des Leistungsversprechens
Wichtige Updates werden in einem Monat veröffentlicht.	Die Uhr beginnt
Vierzehn Tage nach Erstellung der Standard-Patch-Benachrichtigung informiert AMS Sie per Servicebenachrichtigung und per E-Mail für jeden Stack über bevorstehende geplante Patches. Die Servicemeldung beinhaltet: • Eine Liste der Updates IDs (CSUs und IUs), die für den Stack relevant (erforderlich und nicht angewendet) sind, sowie der Updates, die vom Patchen ausgeschlossen sind • IDs der betroffenen Stacks • Das Wartungsfenster, in dem die Updates installiert werden	Die Uhr stoppt, nachdem die Servicebenachrichtigung gesendet wurde.
Sie testen die Auswirkungen der Updates und genehmigen oder lehnen den RFC ab. Wenn Sie nicht innerhalb von 14 Tagen antworten oder das Patchen in Ihrer Antwort auf die Servicebenachrichtigung ablehnen, werden keine Maßnahmen ergriffen. Wenn der Test länger als 14 Tage dauert und Sie möchten, dass die Updates nach Ablauf der 14-tägigen Frist installiert werden, reichen Sie eine Serviceanfrage für einen neuen Patch-RFC ein, der auf den Details des vorherigen RFC basiert.	Wenn Sie nicht innerhalb von 14 Tagen zustimmen oder nicht antworten, wird die ausstehende Änderung storniert und die Serviceverpflichtung für die Updates gilt nicht.

Veranstaltung/Aktion	Messung des Leistungsversprechens
Wenn Sie die Servicemeldung innerhalb von 14 Tagen genehmigen, wendet AMS die Aktualisierungen an. Sie können sich dafür entscheiden, bestimmte Updates aus einem RFC auszuschließen, indem Sie in Ihrer Antwort auf die Servicemeldung angeben, welche Updates ausgeschlossen werden sollen.	Die Uhr beginnt, wenn Sie die Servicebenachrichtigung innerhalb von 14 Tagen nach Erhalt genehmigen. Die Uhr stoppt, nachdem versucht wurde, das Update zu installieren.
AMS sendet Ihnen eine Servicebenachrichtigung über das Ergebnis jeder Aktualisierung, die versucht wurde. Die Servicemeldung enthält die folgenden Details: • EC2 Amazon-Instanz-ID • Update 1 erfolgreich/gescheitert: ARN a1, ARN a2... • Update 2 erfolgreich/gescheitert: ARN b1, ARN b2... • Aktualisierung N erfolgreich/Fehlgeschlagen: ARN c1, ARN c2...	Nicht zutreffend.
Im Falle fehlgeschlagener Updates führt AMS eine Analyse durch, um die Ursache des Fehlers zu ermitteln, und teilt Ihnen das Ergebnis der Analyse mit. Wenn der Fehler auf AMS zurückzuführen ist, versucht AMS erneut, die Updates innerhalb des Wartungsfensters durchzuführen. Andernfalls erstellt AMS Servicemeldungen für die fehlgeschlagene Kombination aus Instanz und Update und wartet in einem Wartungsfenster auf Ihre Anweisungen.	Nicht zutreffend.

Veranstaltung/Aktion	Messung des Leistungsversprechens
Bei Ausfällen, die Ihnen zuzuschreiben sind, reichen Sie eine Serviceanfrage für einen neuen Patch-RFC ein, um die Instanzen zu aktualisieren.	Nicht zutreffend.

Kritisches Patchen

Dies sind AMS-Serviceverpflichtungen für wichtige Sicherheitsupdates.

Kritische Sicherheitsupdates, veränderbare Infrastruktur

Veranstaltung/Aktion	Messung des Leistungsversprechens
CSU ist veröffentlicht.	Die Uhr beginnt
AMS benachrichtigt Sie über den Patch-RFC durch eine Servicebenachrichtigung (die auch eine E-Mail sendet) für jeden Stack. Die Servicebenachrichtigung beinhaltet: • Aktualisiert das Veröffentlichungsdatum • Aktualisiere die Kritikalität • Details aktualisieren: KB-Referenz usw. • IDs der betroffenen Stapel	Die Uhr stoppt, nachdem die Servicebenachrichtigung gesendet wurde.
Sie testen die im RFC aufgeführten Updates und genehmigen oder lehnen den RFC innerhalb von 10 Tagen ab, indem Sie auf die Servicemeldung antworten. Sie geben ein bestimmtes Wartungsfenster (pro Stack) für die Installation der Updates an. Die angegebenen Wartungsfenster, die innerhalb von 24 Stunden nach der Antwort auf die Servicemeldung liegen, können je nach verfügbarer Kapazität neu geplant werden.	Wenn Sie nicht innerhalb von 14 Tagen zustimmen oder nicht antworten, wird die ausstehende Änderung storniert und die Serviceverpflichtung für das Update gilt nicht.

Veranstaltung/Aktion	Messung des Leistungsversprechens
Wenn Sie nicht innerhalb von 10 Tagen antworten oder den Patch-RFC ablehnen, wird die ausstehende Aktion abgebrochen. Wenn Sie die Updates nach Ablauf der 14-tägigen Frist anwenden möchten, reichen Sie eine Serviceanfrage für einen neuen Patch-RFC ein, der auf den Details des vorherigen RFC basiert.	
Wenn Sie die Servicemeldung genehmigen, wendet AMS die Aktualisierungen an. Bei mehreren Updates können Sie sich dafür entscheiden, bestimmte Updates von der Änderung auszuschließen, indem Sie in Ihrer Antwort auf die Servicemeldung angeben, welche Updates ausgeschlossen werden sollen.	Wenn das gewünschte Wartungsfenster nicht innerhalb des Zeitrahmens liegt, wird die Servicezusage für das Update nur verpasst, wenn der RFC nicht innerhalb des gewünschten Wartungsfensters ausgeführt wird.
AMS sendet Ihnen eine Servicebenachrichtigung über das Ergebnis jedes Updates, das angewendet wurde. Die Servicemeldung enthält die folgenden Details: • EC2 Amazon-Instanz-ID • Aktualisierung erfolgreich: ARN a1, ARN a2... • Aktualisierung fehlgeschlagen: ARN c1, ARN c2...	Nicht zutreffend.

Veranstaltung/Aktion	Messung des Leistungsversprechens
Im Falle fehlgeschlagener Updates führt AMS eine Analyse durch, um die Ursache des Fehlers zu ermitteln, und teilt Ihnen das Ergebnis der Analyse mit. Wenn der Fehler auf AMS zurückzuführen ist, versucht AMS erneut, die Updates innerhalb des Wartungsfensters durchzuführen. Andernfalls erstellt AMS Servicemeldungen für die fehlgeschlagene Kombination aus Instanz und Update und wartet in einem neuen Wartungsfenster auf Ihre Anweisungen.	Nicht zutreffend.
Bei Ausfällen, die Ihnen zuzuschreiben sind, reichen Sie eine Serviceanfrage für einen neuen Patch-RFC ein, um die Instanzen zu aktualisieren.	Nicht zutreffend.

Kritische Sicherheitsupdates, unveränderliche Infrastruktur

Veranstaltung/Aktion	Messung des Leistungsversprechens
CSU ist veröffentlicht.	Die Uhr beginnt
AMS informiert Sie in einer Servicemeldung über Folgendes: • Veröffentlichungsdatum aktualisieren • Kritikalität aktualisieren • Details aktualisieren (KB-Referenz usw.) • AMS Amazon Machine Images (AMI) betroffen • Voraussichtliches Veröffentlichungsdatum und -uhrzeit für neue Updates AMIs	Die Uhr läuft weiter.

Veranstaltung/Aktion	Messung des Leistungsversprechens
AMS-Versionen wurden AMIs im verwalteten Konto aktualisiert.	Die Uhr stoppt.
Wenn Sie die Servicemeldung genehmigen, wendet AMS die Updates an. AMS benachrichtigt Sie durch eine Servicebenachrichtigung und per E-Mail über die in Ihrem Konto AMIs geteilten Informationen.	Nicht zutreffend.
Wenn das Testen der neuen AMIs Version länger als die zugewiesene Zeit (eine Woche) dauert, können Sie eine Serviceanfrage an AMS senden, um Ihre Auto Scaling Scaling-Gruppen mit dem neuen AMS-AMI (wie es ist) zu aktualisieren. Wenn Sie das neue AMS-AMI mit Ihren Konfigurationen ändern möchten, verwenden Sie einen RFC mit dem Management Other Other Update CT (ct-0xdawir96cy7k), um anzufordern, dass wir Ihre Auto Scaling Scaling-Gruppen aktualisieren.	Nicht zutreffend.

Berichte und Optionen

AWS Managed Services (AMS) sammelt Daten aus verschiedenen nativen AWS-Services, um Mehrwertberichte zu wichtigen AMS-Angeboten bereitzustellen.

AMS bietet zwei Arten von detaillierten Berichten:

- **Berichte auf Anfrage:** Sie können bestimmte Berichte ad hoc über Ihren Cloud Service Delivery Manager (CSDM) anfordern. Diese Berichte haben kein Limit, da Sie sie während des Onboardings oder bei kritischen Ereignissen möglicherweise mehrmals anfordern müssen. Beachten Sie jedoch, dass diese Berichte nicht so konzipiert sind, dass sie nach einem Zeitplan wie wöchentliche Berichte bereitgestellt werden. Um Ihre Bedürfnisse besser zu verstehen oder weitere Informationen zur Verwendung von Self-Service-Berichten zu erhalten, wenden Sie sich an Ihren CSDM.
- **Self-Service-Berichte:** Mit den Self-Service-Berichten von AMS können Sie Daten beliebig oft direkt abfragen und analysieren. Verwenden Sie Self-Service-Berichte, um von der AMS-Konsole aus auf Berichte zuzugreifen und Datensätze über S3-Buckets (ein Bucket pro Konto) zu melden. Auf diese Weise können Sie die Daten in Ihr bevorzugtes Business Intelligence (BI) -Tool integrieren, sodass Sie Berichte an Ihre Anforderungen anpassen können.

Themen

- [Berichte auf Anfrage](#)
- [Self-Service-Berichte](#)

Berichte auf Anfrage

Themen

- [AMS-Patchberichte](#)
- [AMS Backup-Berichte](#)
- [Berichte von Top Talkers zur Vermeidung von Vorfällen und Überwachung](#)
- [Bericht „Einzelheiten zu Abrechnungsgebühren“](#)
- [Trusted Remediator-Berichte](#)

AMS sammelt Daten aus verschiedenen nativen AWS-Services, um Mehrwertberichte zu wichtigen AMS-Angeboten bereitzustellen. Eine Kopie dieser Berichte erhalten Sie bei Ihrem Cloud Service Delivery Manager (CSDM).

AMS-Patchberichte

Verfügbare Berichte

- [Bericht mit Zusammenfassung der Details zur Patch-Instanz](#)
- [Bericht mit den Patch-Details](#)
- [Bericht für Instanzen, bei denen Patches verpasst wurden](#)
- [SSM-Abdeckungsbericht wird gepatcht](#)

Bericht mit Zusammenfassung der Details zur Patch-Instanz

Der Bericht „Zusammenfassung der Patch-Instanzdetails“ enthält Instanzdetails, die für Instances gesammelt wurden, die in die Berichterstattung aufgenommen wurden. Dieser Informationsbericht hilft dabei, alle eingebundenen Instances, den Kontostatus, die Instanzdetails, den Umfang des Wartungsfensters, die Ausführungszeit des Wartungsfensters, die Stack-Details und den Plattformtyp zu ermitteln. Dieser Bericht enthält Folgendes:

1. Daten zu den Produktions- und Nichtproduktionsinstanzen eines Kontos. Hinweis: Die Produktions- und Nichtproduktionsphase wird aus dem Kontonamen und nicht aus den Instanz-Tags abgeleitet.
2. Daten zur Verteilung der Instances nach Plattformtyp. Hinweis: Der Plattformtyp „N/A“ gibt an, wenn die Plattforminformationen nicht abgerufen werden AWS Systems Manager können.
3. Daten zur Verteilung des Status der Instances und zur Anzahl der ausgeführten, angehaltenen oder beendeten Instances.

Name des Felds	Definition
Datum/Uhrzeit melden	Datum und Uhrzeit der Berichtsgenerierung.
Konto-ID	AWS-Konto-ID, zu der die Instance-ID gehört
Kontoname	AWS-Kontoname

Name des Felds	Definition
Produktionskonto	Kennung der AMS-Produktkonten, die keine Produkte sind, je nachdem, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält. Beispiel: PROD, NONPROD, Nicht verfügbar
Status des Kontos	AMS-Kontostatus. Zum Beispiel: AKTIV, INAKTIV
Verpflichtung zum AMS-Kontoservice	PREMIUM, ZUZÜGLICH
Landezone	Flagge für den Landezonentyp des Kontos. Zum Beispiel: MALZ, NON-MALZ
Zugangsbeschränkungen	Regionen, auf die der Zugriff beschränkt ist. Zum Beispiel: US SOIL
Instanz-ID	ID der EC2 Instanz
Instance-Name	Name der EC2 Instanz
Plattformtyp der Instanz	Typ des Betriebssystems (OS). Zum Beispiel: Windows, Linux usw.
Name der Instanzplattform	Name des Betriebssystems (OS). Zum Beispiel: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer
Stack-Name	Name des Stacks, der die Instanz enthält
Typ des Stapels	AMS-Stack (AMS-Infrastruktur innerhalb des Kundenkontos) oder Kunden-Stack (AMS-verwaltete Infrastruktur, die Kundenanwendungen unterstützt). Beispiele: AMS, CUSTOMER
Name der Auto-Scaling-Gruppe	Name der Auto Scaling Group (ASG), die die Instance enthält

Name des Felds	Definition
Instanz-Patch-Gruppe	Name der Patchgruppe, der verwendet wird, um Instanzen zu gruppieren und dasselbe Wartungsfenster anzuwenden. Wenn die Patch-Gruppe nicht zugewiesen ist, lautet der Wert „Nicht zugewiesen“
Typ der Instanz-Patchgruppe	Typ der Patchgruppe. STANDARD: Standard-Patchgruppe mit dem Standard-Wartungsfenster, das durch das <code>AMSDefaultPatchGroup:True</code> Tag auf der Instanz bestimmt wird. KUNDE: Vom Kunden erstellte Patchgruppe. NOT_ASSIGNED: Keine Patchgruppe zugewiesen
Instance-Status	Status innerhalb des EC2 Instanzlebenszyklus. Beispiele: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING. Weitere Informationen finden Sie unter Instanzlebenszyklus.
Geltungsbereich des Wartungsfensters	Wenn es für diese Instanz ein future Wartungsfenster gibt. Beispiele: COVERED oder NOT_COVERED
Wartungsfenster, Ausführung, Datum/Uhrzeit	Das nächste Mal wird das Wartungsfenster voraussichtlich ausgeführt. Falls NULL, Ausführung in einem Fenster, d. h. nicht wiederkehrend

Bericht mit den Patch-Details

Der Bericht mit den Patch-Details von AWS Managed Services (AMS) bietet Patch-Details und deckt das Wartungsfenster für verschiedene Instanzen ab, darunter:

1. Daten zu Patch-Gruppen und ihren Typen.
2. Daten zu Wartungsfenstern, Dauer, Stichtag, future Daten der Ausführung von Wartungsfenstern (Zeitplan) und betroffenen Instanzen in jedem Fenster.
3. Daten zu allen Betriebssystemen unter dem Konto und Anzahl der Instanzen, auf denen das Betriebssystem installiert ist.

Name des Felds	Definition
Datum/Uhrzeit melden	Datum und Uhrzeit der Berichtsgenerierung.
Konto-ID	AWS-Konto-ID, zu der die Instance-ID gehört
Kontoname	AWS-Kontoname
Instanz-ID	ID der EC2 Instanz
Produktionskonto	Kennung der AMS-Produktkonten, die keine Produkte sind, je nachdem, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält. Wenn keine Daten verfügbar sind, lautet der Wert „Nicht verfügbar“
Status des Kontos	AMS-Kontostatus. Zum Beispiel: AKTIV, INAKTIV
Plattformtyp der Instanz	Typ des Betriebssystems (OS). Zum Beispiel: Windows, Linux
Name der Instanzplattform	Name des Betriebssystems (OS). Zum Beispiel: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer
Typ des Stapels	AMS-Stack (AMS-Infrastruktur innerhalb eines Kundenkontos) oder Kunden-Stack (AMS-verw

Name des Felds	Definition
	altete Infrastruktur, die Kundenanwendungen unterstützt). Zum Beispiel: AMS, CUSTOMER
Instanz-Patch-Gruppe	Name der Patchgruppe, der verwendet wird, um Instanzen zu gruppieren und dasselbe Wartungsfenster anzuwenden. Wenn die Patch-Gruppe nicht zugewiesen ist, lautet der Wert „Nicht zugewiesen“
Typ der Instanz-Patchgruppe	Typ der Patchgruppe. STANDARD: Standard-Patchgruppe mit standardmäßigem Wartungsfenster, bestimmt durch das <code>AMSDefaultPatchGroup:True</code> Tag auf der Instanz KUNDE: Vom Kunden erstellte Patchgruppe NICHT ZUGEWIESEN: Es wurde keine Patchgruppe zugewiesen
Instance-Status	Status innerhalb des EC2 Instanzlebenszyklus. Zum Beispiel: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Weitere Informationen finden Sie unter Instanzlebenszyklus.
ID des Wartungsfensters	Kennung des Wartungsfensters
Status des Wartungsfensters	Mögliche Werte sind ENABLED oder DISABLED.
Typ des Wartungsfensters	Typ des Wartungsfensters

Name des Felds	Definition
Wartungsfenster: Datum und Uhrzeit der nächsten Ausführung	Das nächste Mal wird das Wartungsfenster voraussichtlich ausgeführt. Falls NULL, Ausführung in einem Fenster, d. h. nicht wiederkehrend
Wartungsfenster für die letzte Ausführung	Der letzte Zeitpunkt, zu dem das Wartungsfenster ausgeführt wurde
Dauer des Wartungsfensters (Stunden)	Die Dauer des Wartungsfensters in Stunden
Umfang des Wartungsfensters	Der Umfang des Wartungsfensters
Patch-Baseline-ID	Die Patch-Baseline ist derzeit an die Instanz angehängt
Patch-Status	Allgemeiner Status der Patch-Konformität. Zum Beispiel: COMPLIANT, NON_COMPLIANT. Wenn mindestens ein Patch fehlt, gilt die Instanz als nicht konform, andernfalls als konform.
Konform — Insgesamt	Anzahl der kompatiblen Patches (alle Schweregrade)
Nicht konform — Insgesamt	Anzahl der nicht konformen Patches (alle Schweregrade)
Konform — Kritisch	Anzahl der kompatiblen Patches mit dem Schweregrad „kritisch“
Konform — Hoch	Anzahl der kompatiblen Patches mit dem Schweregrad „hoch“
Konform — Mittel	Anzahl der kompatiblen Patches mit dem Schweregrad „mittel“

Name des Felds	Definition
Konform — Niedrig	Anzahl der kompatiblen Patches mit dem Schweregrad „niedrig“
Konform — informativ	Anzahl der kompatiblen Patches mit dem Schweregrad „informativ“
Konform — Nicht spezifiziert	Anzahl der kompatiblen Patches mit dem Schweregrad „nicht spezifiziert“
Nicht konform — Kritisch	Anzahl der nicht konformen Patches mit dem Schweregrad „kritisch“
Nicht konform — Hoch	Anzahl der nicht konformen Patches mit dem Schweregrad „hoch“
Nicht konform — Mittel	Anzahl der nicht konformen Patches mit dem Schweregrad „mittel“
Nicht konform — Niedrig	Anzahl der nicht konformen Patches mit dem Schweregrad „niedrig“
Nicht konform — Informativ	Anzahl der nicht konformen Patches mit dem Schweregrad „informativ“
Nicht konform — Nicht spezifiziert	Anzahl der nicht konformen Patches mit dem Schweregrad „nicht spezifiziert“

Bericht für Instanzen, bei denen Patches verpasst wurden

Der Bericht AWS Managed Services (AMS) -Instances That Missed Patches enthält Details zu Instances, die während der Ausführung des letzten Wartungsfensters Patches verpasst haben, darunter:

1. Daten zu fehlenden Patches auf Patch-ID-Ebene.
2. Daten zu allen Instances, bei denen mindestens ein Patch fehlt, zusammen mit Attributen wie Schweregrad des Patches, Tage ohne Patches, Bereich und Veröffentlichungsdatum des Patches.

Name des Felds	Definition
Datum/Uhrzeit melden	Datum und Uhrzeit der Berichtsgenerierung.
Konto-ID	AWS-Konto-ID, zu der die Instance-ID gehört
Kontoname	AWS-Kontoname
Produktionskonto	Kennung der AMS-Produktkonten und der Konten anderer Hersteller, je nachdem, ob der Kontoname den Wert „PROD“, „NONPROD“ enthält.
Status des Kontos	AMS-Kontostatus. Zum Beispiel: AKTIV oder INAKTIV
Dienststufe für AMS-Konten	PREMIUM oder PLUS
Instance-ID	ID der EC2 Instanz
Plattformtyp der Instanz	Typ des Betriebssystems (OS). Zum Beispiel: Windows
Instance-Status	Status des EC2 Instanzlebenszyklus. Zum Beispiel: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Weitere Informationen finden Sie unter Instance-Lebenszyklus .
Patch-ID	ID des veröffentlichten Patches. Beispiel: KB3172729
Schweregrad des Patch	Schweregrad des Patches pro Herausgeber. Zum Beispiel: KRITISCH, WICHTIG, MÄSSIG, NIEDRIG, NICHT SPEZIFIZIERT
Patch-Klassifizierung	Klassifizierung der Patches pro Herausgeber. Zum Beispiel: CRITICALUPDATES,

Name des Felds	Definition
	SECURITYUPDATES, UPDATEROLLUPS, UPDATES, FEATUREPACKS
Datum und Uhrzeit der Patch-Veröffentlichung (UTC)	Veröffentlichungsdatum des Patches pro Herausgeber
Status der Patch-Installation	Installationsstatus des Patches auf der Instanz pro SSM. Zum Beispiel: INSTALLIERT, FEHLT, NICHT ZUTREFFEND
Tage ohne Patches	Anzahl der Tage, an denen die Instanz seit dem letzten SSM-Scan nicht gepatcht wurde
Zeitraum für Tage ohne Patches	Ungepatchte Tage. Zum Beispiel: <30 TAGE, 30-60 TAGE, 60-90 TAGE, 90+ TAGE

SSM-Abdeckungsbericht wird gepatcht

Der Bericht AMS Patching SSM Coverage informiert Sie darüber, ob auf den EC2 Instances im Konto der SSM-Agent installiert ist oder nicht.

Name des Felds	Definition
Name des Kunden	Kundenname für Situationen, in denen es mehrere Unterkunden gibt
Region der Ressource	AWS Region, in der sich die Ressource befindet
Account name (Kontoname)	Der Name des Kontos
AWS Konto-ID	Die ID des AWS Kontos
Ressourcen-ID	ID der EC2 Instanz
Ressourcenname	Name der EC2 Instanz

Name des Felds	Definition
Konforme Flagge	Gibt an, ob auf der Ressource der SSM-Agent installiert ist („Compliant“) oder nicht („NON_COMPLIANT“)

AMS Backup-Berichte

Verfügbare Berichte

- [Bericht über Erfolg- und Fehlschlag des Backup-Jobs](#)
- [Bericht „Backup-Zusammenfassung“](#)
- [Summary/Coverage Backup-Bericht](#)

Bericht über Erfolg- und Fehlschlag des Backup-Jobs

Der Success/Failure Backup-Job-Bericht enthält Informationen über Backups, die in den letzten Wochen ausgeführt wurden. Um den Bericht anzupassen, geben Sie die Anzahl der Wochen an, für die Sie Daten abrufen möchten. Die Standardanzahl von Wochen ist 12. In der folgenden Tabelle sind die im Bericht enthaltenen Daten aufgeführt:

Name des Felds	Definition
AWS-Konto-ID	AWS-Konto-ID, zu der die Ressource gehört
Kontoname	AWS-Kontoname
Backup-Job-ID	Die ID des Backup-Jobs
Ressourcen-ID	Die ID der gesicherten Ressource
Ressourcentyp	Der Typ der Ressource, die gesichert wird
Region der Ressource	Die AWS Region der gesicherten Ressource
Backup-Status	Der Status des Backups. Weitere Informationen finden Sie unter Status von Backup-Jobs

Name des Felds	Definition
ID des Wiederherstellungspunkts	Die eindeutige Kennung des Wiederherstellungspunkts
Statusmeldung	Beschreibung der Fehler oder Warnungen, die während des Backup-Jobs aufgetreten sind
Größe des Backup	Größe des Backups in GB
ARN für den Wiederherstellungspunkt	Der ARN des erstellten Backups
Alter des Wiederherstellungspunkts in Tagen	Anzahl der Tage, die seit der Erstellung des Wiederherstellungspunkts vergangen sind
Weniger als 30 Tage alt	Indikator für Backups, die weniger als 30 Tage alt sind

Bericht „Backup-Zusammenfassung“

Name des Felds	Definition
Name des Kunden	Kundenname für Situationen, in denen mehrere Unterkunden
Backup-Monat	Monat des Backups
Jahr des Backup	Jahr des Backups
Ressourcentyp	Der Typ der Ressource, die gesichert wird
Anzahl der Ressourcen	Die Anzahl der Ressourcen, die gesichert wurden
Anzahl der Wiederherstellungspunkte	Anzahl der unterschiedlichen Schnappschüsse
Backups, die weniger als 30 Tage alt sind	Die Anzahl der Backups, die weniger als 30 Tage alt sind

Name des Felds	Definition
Maximales Alter des Wiederherstellungspunkts	Das älteste Alter des Wiederherstellungspunkts seit Tagen
Mindestalter des Wiederherstellungspunkts	Das letzte Alter des Wiederherstellungspunkts in Tagen

Summary/Coverage Backup-Bericht

Der Summary/Coverage Backup-Bericht listet auf, wie viele Ressourcen derzeit durch keinen AWS Backup Plan geschützt sind. Besprechen Sie mit Ihrem CDSM einen geeigneten Plan, um die Abdeckung nach Möglichkeit zu erhöhen und das Risiko eines Datenverlusts zu verringern.

Name des Felds	Definition
Name des Kunden	Kundenname für Situationen, in denen mehrere Unterkunden
Region	AWS Region, in der sich die Ressource befindet
Account name (Kontoname)	Der Name des Kontos
AWS Konto-ID	Die ID des AWS Kontos
Ressourcentyp	Typ der Ressource. Ressourcen werden unterstützt von AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EFS EC2 FSx, RDS und S3)
ARN-Ressourcen	ARN der Ressource
Ressourcen-ID	ID der Ressource
Abdeckung	Gibt an, ob die Ressource abgedeckt ist oder nicht („COVERED“ oder „NOT_COVERED“)
Anzahl der Ressourcen	Anzahl der unterstützten Ressourcen im Konto

Name des Felds	Definition
perc_coverage	Prozentsatz der unterstützten Ressourcen, für die in den letzten 30 Tagen ein Backup ausgeführt wurde.

Berichte von Top Talkers zur Vermeidung von Vorfällen und Überwachung

Verfügbare Berichte

- [Bericht über verhinderte Vorfälle](#)
- [Bericht „Monitoring Top Talkers“](#)

Bericht über verhinderte Vorfälle

Der Bericht über verhinderte Vorfälle listet die CloudWatch Amazon-Alarme auf, die automatisch behoben wurden, wodurch ein möglicher Vorfall verhindert wurde. Weitere Informationen finden Sie unter [Automatische Problembehebung](#). In der folgenden Tabelle sind die in diesem Bericht enthaltenen Informationen aufgeführt:

Name des Felds	Definition
execution_start_time_utc	Datum, an dem die Automatisierung ausgeführt wurde
Kundenname	Kundenname des Kontos
Konto_Bezeichnung	Der Name des Kontos
AwsAccountId	Die ID des AWS-Kontos
Dokumentname	Der Name des ausgeführten SSM-Dokuments oder der ausgeführten Automatisierung
Dauer in Minuten	Die Länge der Automatisierung in Minuten
Region	AWS Region, in der sich die Ressource befindet

Name des Felds	Definition
automation_execution_id	Die ID der Ausführung
automation_execution_status	Der Status der Ausführung

Bericht „Monitoring Top Talkers“

Der Bericht Monitoring Top Talkers zeigt die Anzahl der CloudWatch Amazon-Alerts, die in einem bestimmten Zeitraum generiert wurden, und bietet Visualisierungen der Ressourcen, die die meisten Alerts generieren. Dieser Bericht hilft Ihnen dabei, Ressourcen zu identifizieren, die die meisten Alerts generieren. Diese Ressourcen eignen sich möglicherweise für die Durchführung einer Ursachenanalyse zur Behebung des Problems oder zur Änderung der Alarmschwellenwerte, um unnötige Auslöser zu verhindern, wenn kein echtes Problem vorliegt. In der folgenden Tabelle sind die in diesem Bericht enthaltenen Informationen aufgeführt:

Name des Felds	Definition
Kundenname	Name des Kunden
AccountId	Die ID des AWS Kontos
Kategorie der Warnung	Die Art der ausgelösten Warnung
Beschreibung	Beschreibung der Warnung
Ressourcen-ID	ID der Ressource, die die Warnung ausgelöst hat
Ressourcenname	Name der Ressource, die die Warnung ausgelöst hat
Region	AWS Region, in der sich die Ressource befindet
Status des Vorfalls	Aktueller Status des durch den Alarm ausgelösten Vorfalls

Name des Felds	Definition
Erstes Auftreten	Das erste Mal, dass die Warnung ausgelöst wurde
Jüngstes Ereignis	Der letzte Zeitpunkt, zu dem die Warnung ausgelöst wurde
Anzahl der Alarme	Anzahl der Alarme, die zwischen dem ersten und dem letzten Ereignis generiert wurden

Bericht „Einzelheiten zu Abrechnungsgebühren“

Der Bericht mit den Einzelheiten zu den Rechnungsgebühren von AWS Managed Services (AMS) enthält Einzelheiten zu den AMS-Abrechnungsgebühren mit verknüpften Konten und den jeweiligen AWS-Services, darunter:

- Gebühren auf AMS-Serviceebene, Prozentsätze zur Erhöhung der Gebühren, AMS-Servicestufen auf Kontoebene und AMS-Gebühren.
- Verknüpfte Konten und Nutzungsgebühren AWS

Name des Felds	Definition
Monat der Abrechnung	Der Monat und das Jahr, in dem der Service in Rechnung gestellt wurde
Konto-ID des Zahlers	Die 12-stellige ID, die das Konto identifiziert, das für die Zahlung der AMS-Gebühren verantwortlich ist
ID des verknüpften Kontos	Die 12-stellige ID, die das AMS-Konto identifiziert, das Dienste in Anspruch nimmt, die Kosten verursachen
AWS Name des Dienstes	Der AWS Dienst, der verwendet wurde

Name des Felds	Definition
AWS Gebühren	Die AWS Gebühren für den AWS unter Dienstname aufgeführten AWS Dienstnamen
Preisplan	Der Name des Preisplans, der mit dem verknüpften Konto verknüpft ist
Proportion erhöhen	Der Uplift-Prozentsatz (als Dezimalzahl V.WXYZ) basierend auf pricing_plan, SLA und AWS-Service
Angepasste Gebühren AWS	AWS Nutzung angepasst an AMS
Erhöhte AWS-Gebühren	Der Prozentsatz der AWS-Gebühren, die für AMS berechnet werden sollen; $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
EC2 Instances, die RDS ausgeben	Ausgaben für EC2 und RDS-Instances
AMS-Gebühren	AMS-Gebühren insgesamt für das Produkt; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Anteilige Mindestgebühr	Der Betrag, den wir berechnen, um den vertraglichen Mindestbetrag zu erreichen
Mindestgebühr	AMS-Mindestgebühren (falls zutreffend)
Gesamtbetrag der AMS-Gebühren für verknüpfte Konten	Summe aller Gebühren für das linked_account
AMS-Gebühren für das Konto des Zahlers	Summe aller Gebühren für das Konto des Zahlers

Trusted Remediator-Berichte

Verfügbare Berichte

- [Bericht „Trusted Remediator Remediation — Zusammenfassung“](#)

- [Bericht mit der Zusammenfassung der Trusted Remediator-Konfiguration](#)
- [Trusted Advisor Überprüfen Sie den zusammenfassenden Bericht](#)

Bericht „Trusted Remediator Remediation — Zusammenfassung“

Der Bericht „Trusted Remediator Remediation Status“ enthält Informationen zu den Behebungen, die während früherer Behebungszyklen durchgeführt wurden. Die Standardanzahl von Wochen ist 1. Um den Bericht anzupassen, geben Sie die Anzahl der Wochen auf der Grundlage Ihres Behebungszeitplans an.

Name des Felds	Definition
Datum	Das Datum, an dem die Daten gesammelt wurden.
Konto-ID	Die AWS Konto-ID, zu der die Ressource gehört
Kontoname	Der AWS Kontoname
Überprüfen Sie die Kategorie	Die AWS Trusted Advisor Scheck-Kategorie
Überprüfen Sie den Namen	Der Name der behobenen Prüfung Trusted Advisor
Prüf-ID	Die ID des korrigierten Schecks Trusted Advisor
Ausführungsmodus	Der Ausführungsmodus, der für die spezifische Trusted Advisor Prüfung konfiguriert wurde
OpsItem ID	Die ID der Datei, die von Trusted Advisor für die Behebung OpsItem erstellt wurde
OpsItem Status	Der Status von „OpsItem Erstellt von“ zum Trusted Advisor Zeitpunkt der Meldung
Ressourcen-ID	Der ARN der Ressource, die für die Problembhebung erstellt wurde

Bericht mit der Zusammenfassung der Trusted Remediator-Konfiguration

Der Bericht mit der Zusammenfassung der Trusted Remediator-Konfiguration enthält Informationen zu den aktuellen Trusted Remediator-Wiederherstellungskonfigurationen für jede Prüfung. Trusted Advisor

Name des Felds	Definition
Datum	Das Datum, an dem die Daten gesammelt wurden.
Konto-ID	Die AWS Konto-ID, für die die Konfiguration gilt
Kontoname	Der AWS Kontoname
Überprüfen Sie die Kategorie	Die AWS Trusted Advisor Scheck-Kategorie
Überprüfen Sie den Namen	Der Name der behebten Trusted Advisor Prüfung, für die die Konfiguration gilt
Prüf-ID	Die ID der standardisierten Trusted Advisor Prüfung, für die die Konfiguration gilt
Ausführungsmodus	Der Ausführungsmodus, der für die spezifische Trusted Advisor Prüfung konfiguriert wurde
Auf Automatisiert überschreiben	Das Tag-Muster, falls konfiguriert, um den Ausführungsmodus auf Automatisiert zu überschreiben
Auf Manuell überschreiben	Das Tag-Muster, falls konfiguriert, um den Ausführungsmodus auf Manuell zu überschreiben

Trusted Advisor Überprüfen Sie den zusammenfassenden Bericht

Der Bericht „Zusammenfassung der Trusted Advisor Schecks“ enthält Informationen zu den aktuellen Trusted Advisor Prüfungen. In diesem Bericht werden Daten nach jedem wöchentlichen

Behebungsplan gesammelt. Die Standardanzahl von Wochen ist 1. Um den Bericht anzupassen, geben Sie die Anzahl der Wochen an, die auf Ihrem Behebungszyklus basieren.

Name des Felds	Definition
Datum	Das Datum, an dem die Daten gesammelt wurden.
Konto-ID	Die AWS Konto-ID, für die die Konfiguration gilt
Name des Kunden	Der AWS Kontoname
Überprüfen Sie die Kategorie	Die AWS Trusted Advisor Scheck-Kategorie
Überprüfen Sie den Namen	Der Name der behebten Trusted Advisor Prüfung, für die die Konfiguration gilt
Prüf-ID	Die ID der standardisierten Trusted Advisor Prüfung, für die die Konfiguration gilt
Status	Der Warnungsstatus der Prüfung. Mögliche Status sind ok (grün), Warnung (gelb), Fehler (rot) oder not_available
Markierte Ressourcen	Die Anzahl der AWS Ressourcen, die durch den Scheck gekennzeichnet (aufgelistet) wurden. Trusted Advisor
Ignorierte Ressourcen	Die Anzahl der AWS Ressourcen, die ignoriert wurden, Trusted Advisor weil Sie sie als unterdrückt markiert haben.
Ressourcen im kritischen Zustand	Die Anzahl der Ressourcen im kritischen Zustand
Ressourcen im Warnstatus	Die Anzahl der Ressourcen im Warnstatus

Self-Service-Berichte

Die Self-Service-Berichte (SSR) von AWS Managed Services (AMS) sind eine Funktion, die Daten von verschiedenen systemeigenen AWS Services sammelt und Zugriff auf Berichte zu wichtigen AMS-Angeboten bietet. SSR bietet Informationen, die Sie zur Unterstützung von Betrieb, Konfigurationsmanagement, Bestandsmanagement, Sicherheitsmanagement und Compliance verwenden können.

Verwenden Sie SSR, um über die AMS-Konsole auf die Berichte und Berichtsdatensätze über Amazon S3 S3-Buckets (ein Bucket pro Konto) zuzugreifen. Sie können die Daten in Ihr bevorzugtes Business Intelligence (BI) -Tool einbinden, um die Berichte an Ihre individuellen Bedürfnisse anzupassen. AMS erstellt diesen S3-Bucket (S3-Bucket-Name: (ams-reporting-data-a<Account_ID>)) in Ihrer primären AWS Region, und die Daten werden von der AMS-Steuerebene gemeinsam genutzt, die in der Region us-east-1 gehostet wird.

Important

Um auf diese Funktion zugreifen zu können, müssen Sie über eine der folgenden Rollen verfügen:

- Landezone für mehrere Konten: AWSManagedServicesReadOnlyRole
- Landingzone für ein Konto: Kunde__Rolle ReadOnly

Important

Verwenden von benutzerdefinierten Schlüsseln mit AWS Glue

Um Ihre AWS Glue Metadaten mit einem vom Kunden verwalteten KMS-Schlüssel zu verschlüsseln, müssen Sie die folgenden zusätzlichen Schritte ausführen, damit AMS Daten aus dem Konto aggregieren kann:

1. Öffnen Sie die AWS Key Management Service Konsole unter <https://console.aws.amazon.com/kms> und wählen Sie dann Customer Managed Keys aus.
2. Wählen Sie die Schlüssel-ID aus, die Sie zur Verschlüsselung der AWS Glue Metadaten verwenden möchten.
3. Wählen Sie die Registerkarte Aliase und dann Alias erstellen aus.

4. Geben Sie `AmsReportingFlywheelCustomKey` in das Textfeld ein und wählen Sie dann Alias erstellen aus.

Themen

- [Interne API-Operationen](#)
- [Patch-Bericht \(täglich\)](#)
- [Backup-Bericht \(täglich\)](#)
- [Zwischenfallbericht \(wöchentlich\)](#)
- [Abrechnungsbericht \(monatlich\)](#)
- [Aggregierte Berichte](#)
- [Dashboards für AMS-Selfservice-Berichte](#)
- [Datenaufbewahrungsrichtlinie](#)
- [Offboard von SSR](#)

Interne API-Operationen

Wenn Sie API-Operationen überwachen, werden Ihnen möglicherweise Aufrufe der folgenden rein internen Operationen angezeigt:

- `GetDashboardUrl`
- `ListReportsV2`

Interner API-Vorgang: `GetDashboardUrl`

Dieser Vorgang erscheint in den Systemprotokollen, wenn er von der AMS-Konsole aufgerufen wird. Es gibt keinen anderen Anwendungsfall. Es ist nicht für Ihren direkten Gebrauch verfügbar.

Gibt die eingebettete Dashboard-URL für den entsprechenden Bericht zurück. Dieser Vorgang akzeptiert einen `dashboardName` zurückgegebenen Wert von `ListReports`.

Erforderliche Syntax

```
HTTP/1.1 200
Content-type: application/json
{
```



```
"dashboardName": "string"
}
```

Elemente anfordern

dashboardName: Der Name des QuickSight Dashboards, für das die URL angefordert wird. Der Dashboard-Name wird in ListReports V2 zurückgegeben.

Typ: Zeichenfolge

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück. Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

url: Gibt die QuickSight URL für die angeforderte URL zurückdashboardName.

Typ: Zeichenfolge

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unter [Häufige Fehler](#).

BadRequestException:

Die eingereichte Anfrage ist nicht gültig. Zum Beispiel, wenn die Eingabe unvollständig oder falsch ist. Einzelheiten finden Sie in der beigefügten Fehlermeldung.

HTTP Status Code: 400

NotFoundException:

Die angeforderte Ressource wurde nicht gefunden. Stellen Sie sicher, dass der Anfrage-URI korrekt ist.

HTTP Status Code: 404

TooManyRequestsException:

Die Anfrage hat ihr Drosselungslimit erreicht. Versuchen Sie es nach dem angegebenen Zeitraum erneut.

HTTP-Statuscode: 429

UnauthorizedException:

Die Anfrage wurde abgelehnt, da der Anrufer nicht über ausreichende Berechtigungen verfügt.

HTTP-Statuscode: 401

Interner API-Betrieb: ListReports V2

Diese API erscheint in den Systemprotokollen, wenn sie von der AMS-Konsole aufgerufen wird. Sie hat keinen anderen Anwendungsfall. Es ist nicht für Ihren direkten Gebrauch verfügbar.

Gibt eine Liste von Betriebsberichten zurück, die für ein bestimmtes Konto verfügbar sind.

Erforderliche Syntax

Die Anfrage hat keinen Anfragetext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdateTime": "string",
    }
  ],
  "reportsType": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück. Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

reportsList: Die Liste der verfügbaren Betriebsberichte.

Typ: Anordnung von Dashboard-Objekten

reportsType: Gibt an, ob ein Bericht für mehrere Konten aggregiert ist oder nicht.

Typ: Zeichenfolge

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unter [Häufige Fehler](#).

BadRequestException:

Die eingereichte Anfrage ist nicht gültig. Beispielsweise ist die Eingabe unvollständig oder falsch. Einzelheiten finden Sie in der beigefügten Fehlermeldung.

HTTP Status Code: 400

NotFoundException:

Die angeforderte Ressource wurde nicht gefunden. Stellen Sie sicher, dass der Anfrage-URI korrekt ist.

HTTP Status Code: 404

TooManyRequestsException:

Die Anfrage hat ihr Drosselungslimit erreicht. Versuchen Sie es nach dem angegebenen Zeitraum erneut.

HTTP-Statuscode: 429

UnauthorizedException:

Die Anfrage wurde abgelehnt, da der Anrufer nicht über ausreichende Berechtigungen verfügt.

HTTP-Statuscode: 401

Patch-Bericht (täglich)

Verfügbare Berichte

-
- [Einzelheiten zum Patch](#)
- [Instanzen, bei denen Patches ausgelassen wurden](#)

Dies ist ein informativer Bericht, anhand dessen alle in Patch Orchestrator (PO) integrierten Instanzen, Kontostatus, Instanzdetails, Umfang des Wartungsfensters, Ausführungszeit des Wartungsfensters, Stackdetails und Plattformtyp identifiziert werden können.

Dieser Datensatz bietet:

- Daten zu den Produktions- und Nichtproduktionsinstanzen eines Kontos. Die Produktions- und Nichtproduktionsphase wird vom Kontonamen und nicht von den Instanz-Tags abgeleitet.
- Daten zur Verteilung der Instanzen nach Plattformtyp. Der Plattformtyp „N/A“ tritt auf, wenn AWS Systems Manager (SSM) die Plattforminformationen nicht abrufen kann.
- Daten zur Verteilung des Status der Instanzen, zur Anzahl der laufenden, angehaltenen oder beendeten Instanzen.

Name des Konsolenfeldes	Feldname des Datensatzes	Definition
Zugriffsbeschränkungen	access_restrictions	Regionen, auf die der Zugriff beschränkt ist
Konto-ID	aws_account_id	AWS Konto-ID, zu der die Instanz-ID gehört
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdige Konto, das von Ihnen aktiviert wurde. AWS Organizations
Kontoname	Konto_Bezeichnung	AWS Kontoname
Status des Kontos	account_status	AMS-Kontostatus
	account_sla	Verpflichtung zum AMS-Konto service
Kontotyp	malz_role	MALZ-Rolle
Name der Auto-Scaling-Gruppe	instanz_asg_name	Name der Auto Scaling Group (ASG), die die Instance enthält
Instanz-ID	instance_id	ID der EC2 Instanz

Name des Konsolenfeldes	Feldname des Datensatzes	Definition
Instance-Name	Instanzname	Name der Instanz EC2
Instanz-Patch-Gruppe	instance_patch_group	Name der Patch-Gruppe, die verwendet wird, um Instanzen zu gruppieren und dasselbe Wartungsfenster anzuwenden
Typ der Instanz-Patchgruppe	instance_patch_group_type	Typ der Patch-Gruppe
Plattformtyp der Instanz	instance_platform_type	Typ des Betriebssystems (OS)
Name der Instanzplattform	instance_platform_name	Name des Betriebssystems (OS)
Instance-Status	instance_state	Status innerhalb des Instanzenlebenszyklus EC2
Instanz-Tags	ec2_tags	Die mit der EC2 Amazon-Instance-ID verknüpften Tags
Landezone	malz_flag	Flagge für ein Konto im Zusammenhang mit Malz
Geltungsbereich des Wartungsfensters	mw_covered_flag	Wenn für eine Instanz mindestens ein Wartungsfenster mit einem future Ausführungsdatum aktiviert ist, gilt sie als abgedeckt, andernfalls als nicht abgedeckt
Wartungsfenster, Ausführungsdatum/Uhrzeit	früheste_window_execution_time	Das nächste Mal wird das Wartungsfenster voraussichtlich ausgeführt

Name des Konsolenfeldes	Feldname des Datensatzes	Definition
Wartungsfenster, Ausführung, Datum/Uhrzeit	früheste_window_execution_time	Das nächste Mal wird das Wartungsfenster voraussichtlich ausgeführt
Produktionskonto	prod_account	Kennung der AMS-Prod- und Nicht-Prod-Konten, abhängig davon, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält.
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Stack-Name	instance_stack_name	Name des Stacks, der die Instanz enthält
Typ des Stapels	instance_stack_type	AMS-Stack (AMS-Infrastruktur innerhalb des Kundenkontos) oder Kunden-Stack (AMS-verwaltete Infrastruktur, die Kundenanwendungen unterstützt)

Einzelheiten zum Patch

Dieser Bericht enthält Patch-Details und deckt das Wartungsfenster für verschiedene Instanzen ab.

Dieser Bericht enthält:

- Daten zu Patchgruppen und ihren Typen.
- Daten zu Wartungsfenstern, Dauer, Stichtag, future Daten der Ausführung von Wartungsfenstern (Zeitplan) und betroffenen Instanzen in jedem Fenster.
- Daten zu allen Betriebssystemen unter dem Konto und Anzahl der Instanzen, auf denen das Betriebssystem installiert ist.

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Konto-ID	aws_account_id	AWS Konto-ID, zu der die Instanz-ID gehört
Kontoname	Konto_Bezeichnung	AWS Kontoname
Kontostatus	account_status	AMS-Kontostatus
Konform — Kritisch	compliant_critical	Anzahl der kompatiblen Patches mit dem Schweregrad „kritisch“
Konform — Hoch	compliant_high	Anzahl der kompatiblen Patches mit dem Schweregrad „hoch“
Konform — Mittel	compliant_medium	Anzahl der kompatiblen Patches mit dem Schweregrad „mittel“
Konform — Niedrig	compliant_low	Anzahl der kompatiblen Patches mit dem Schweregrad „niedrig“
Konform — informativ	compliant_informational	Anzahl der kompatiblen Patches mit dem Schweregrad „informativ“
Konform — Nicht spezifiziert	compliant_nicht spezifiziert	Anzahl der kompatiblen Patches mit dem Schweregrad „nicht spezifiziert“
Konform — Insgesamt	compliant_total	Anzahl der kompatiblen Patches (alle Schweregrade)

Name des Felds	Feldname des Datensatzes	Definition
Instanz-ID	instance_id	ID der EC2 Instanz
Instance-Name	Instanzname	Name der Instanz EC2
	account_sla	Dienststufe für AMS-Konten
Plattformtyp der Instanz	instance_platform_type	Typ des Betriebssystems (OS)
Name der Instanzplattform	instance_platform_name	Name des Betriebssystems (OS)
Typ der Instanz-Patchgruppe	instance_patch_group_type	DEFAULT: Standard-Patchgruppe mit standardmäßigem Wartungsfenster, bestimmt durch das Tag:TRUE auf der Instanz AMSDefault PatchGroup KUNDE: Der Kunde hat die Patchgruppe erstellt NOT_ASSIGNED: Keine Patch-Gruppe zugewiesen
Instanz-Patch-Gruppe	instance_patch_group	Name der Patch-Gruppe, die verwendet wird, um Instanzen zu gruppieren und dasselbe Wartungsfenster anzuwenden
Instance-Status	instance_state	Status innerhalb des Instanzenlebenszyklus EC2
Instanz-Tags	ec2_tags	Die mit der EC2 Amazon-Instance-ID verknüpften Tags

Name des Felds	Feldname des Datensatzes	Definition
Wartungsfenster für die letzte Ausführung	last_execution_window	Der letzte Zeitpunkt, zu dem das Wartungsfenster ausgeführt wurde
ID des Wartungsfensters	Fenster-ID	Wartungsfenster-ID
Status des Wartungsfensters	window_state	Status des Wartungsfensters
Typ des Wartungsfensters	Fenstertyp	Typ des Wartungsfensters
Wartungsfenster: Datum und Uhrzeit der nächsten Ausführung	window_next execution_time	Beim nächsten Mal wird das Wartungsfenster voraussichtlich ausgeführt
Dauer des Wartungsfensters (Stunden)	Dauer des Fensters	Die Dauer des Wartungsfensters in Stunden
Geltungsbereich des Wartungsfensters	mw_covered_flag	Wenn für eine Instanz mindestens ein Wartungsfenster mit einem future Ausführungsdatum aktiviert ist, gilt sie als abgedeckt, andernfalls als nicht abgedeckt
Nicht konform — Kritisch	noncompliant_critical	Anzahl der nicht konformen Patches mit dem Schweregrad „kritisch“
Nicht konform — Hoch	noncompliant_high	Anzahl der nicht konformen Patches mit dem Schweregrad „hoch“
Nicht konform — Mittel	noncompliant_medium	Anzahl der nicht konformen Patches mit dem Schweregrad „mittel“

Name des Felds	Feldname des Datensatzes	Definition
Nicht konform — Niedrig	noncompliant_low	Anzahl der nicht konformen Patches mit dem Schweregrad „niedrig“
Nicht konform — Informativ	nicht konform _informativ	Anzahl der nicht konformen Patches mit dem Schweregrad „informativ“
Nicht konform — Nicht spezifiziert	nicht konform _nicht spezifiziert	Anzahl der nicht konformen Patches mit dem Schweregrad „nicht spezifiziert“
Nicht konform — Insgesamt	noncompliant_total	Anzahl der nicht konformen Patches (alle Schweregrade)
Patch-Baseline-ID	Patch_Baseline_ID	Die Patch-Baseline ist derzeit an die Instanz angehängt
Patch-Status	Status des Patches	Allgemeiner Status der Patch-Konformität. Fehlt mindestens ein Patch, gilt die Instanz als nicht konform, andernfalls als konform.
Produktionskonto	prod_account	Kennung der AMS-Prod- und Nicht-Prod-Konten, abhängig davon, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält.
Typ des Stapels	instance_stack_type	AMS-Stack (AMS-Infrastruktur innerhalb des Kundenkontos) oder Kunden-Stack (AMS-verwaltete Infrastruktur, die Kundenanwendungen unterstützt)

Name des Felds	Feldname des Datensatzes	Definition
	window_next_exec_yyyy	Jahr als Teil von window_next_execution_time
	window_next_exec_mm	Teil des Monats window_next_execution_time
	Window_Next_Exec_D	Teil des Tages von window_next_execution_time
	window_next_exec_HHMM	Stunde:Minute Teil von window_next_execution_time

Instanzen, bei denen Patches ausgelassen wurden

Dieser Bericht enthält Einzelheiten zu Instanzen, bei denen während der Ausführung des letzten Wartungsfensters Patches verpasst wurden.

Dieser Bericht enthält:

- Daten zu fehlenden Patches auf Patch-ID-Ebene.
- Daten zu allen Instances, bei denen mindestens ein Patch fehlt, und Attribute wie Schweregrad des Patches, Tage ohne Patches, Bereich und Veröffentlichungsdatum des Patches.

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung
Konto-ID	aws_account_id	AWS Konto-ID, zu der die Instanz-ID gehört
Kontoname	Konto_Bezeichnung	AWS Kontoname
Kundenname Elternteil	Kundenname_Elternteil	

Name des Felds	Feldname des Datensatzes	Definition
Name des Kunden	Kundenname	
Produktionskonto	prod_account	Bezeichner der AMS-Prod- oder Non-Prod-Konten, je nachdem, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält.
Status des Kontos	account_status	AMS-Kontostatus
Kontotyp	Kontotyp	
	account_sla	Dienststufe für AMS-Konten
Instanz-ID	instance_id	ID deiner EC2 Instanz
Instance-Name	Instanzname	Name Ihrer Instanz EC2
Plattformtyp der Instanz	instance_platform_type	Typ des Betriebssystems (OS)
Instance-Status	instance_state	Status innerhalb des Instanzlebenszyklus EC2
Instanz-Tags	ec2_tags	Die mit der EC2 Amazon-Instance-ID verknüpften Tags
Patch-ID	Patch-ID	ID des veröffentlichten Patches
Schweregrad des Patch	patch_sev	Schweregrad des Patches pro Herausgeber
Patch-Klassifizierung	patch_class	Klassifizierung der Patches nach dem Patch-Herausgeber
Datum und Uhrzeit der Patch-Veröffentlichung (UTC)	release_dt_utc	Veröffentlichungsdatum des Patches pro Herausgeber

Name des Felds	Feldname des Datensatzes	Definition
Status der Patch-Installation	Installationsstatus	Installieren Sie den Status des Patches auf der Instanz pro SSM
Tage ohne Patches	days_ungepatched	Anzahl der Tage, an denen die Instanz seit dem letzten SSM-Scan nicht gepatcht wurde
Zeitraum für Tage ohne Patches	days_unpatched_bucket	Ungepatchte Tage

Backup-Bericht (täglich)

Der Backup-Bericht deckt primäre und sekundäre (falls zutreffend) Regionen ab. Er deckt den Status der Backups (Erfolg/Fehlschlag) und Daten zu den erstellten Snapshots ab.

Dieser Bericht enthält:

- Status des Backup
- Anzahl der aufgenommenen Schnappschüsse
- Wiederherstellungspunkt
- Backup-Plan und Tresorinformationen

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Konto-ID	aws_account_id	AWS-Konto-ID, zu der die Instance-ID gehört

Name des Felds	Feldname des Datensatzes	Definition
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdige Konto, das von Ihnen aktiviert wurde. AWS Organizations
Kontoname	Konto_Bezeichnung	AWS-Kontoname
Konto-SLA	account_sla	Verpflichtung zum AMS-Konto service
	malz_flag	Flagge für ein Konto im Zusammenhang mit Malz
	malz_role	MALZ-Rolle
	Zugangsbeschränkungen	Regionen, auf die der Zugriff beschränkt ist
Startdatum und Uhrzeit des geplanten Backup-Snapshots	start_by_dt_utc	Zeitstempel, zu dem der Start des Snapshots geplant ist
Aktuelles Startdatum und Uhrzeit des Backup-Snapshots	creation_dt_utc	Zeitstempel, zu dem der Snapshot tatsächlich beginnt
Datum und Uhrzeit der Fertigstellung des Backup-Snapshots	completion_dt_utc	Zeitstempel, wenn der Snapshot abgeschlossen ist
Ablaufdatum/Uhrzeit des Backup-Snapshots	expiration_dt_utc	Zeitstempel, wenn der Snapshot abläuft
Status des Backup-Jobs	backup_job_status	Status des Snapshots
Art des Backup	Sicherungstyp	Art der Sicherung
ID des Backup-Auftrags	Backup_Job-ID	Die eindeutige Kennung des Backup-Jobs

Name des Felds	Feldname des Datensatzes	Definition
Backup-Größe in Byte	backup_size_in_bytes	Die Backup-Größe in Byte
Backup-Plan ARN	backup_plan_arn	Der Backup-Plan ARN
ID des Backup-Plans	backup_plan_id	Eindeutige Kennung des Backup-Plans
Name des Sicherungsplans	backup_plan_name	Der Name des Backup-Plans
Version des Backup-Plans	backup_plan_version	Die Version des Backup-Plans
ID der Backup-Regel	backup_rule_id	Die ID der Backup-Regel
Backup-Tresor-ARN	backup_vault_arn	Backup-Tresor-ARN
Name des Sicherungstresors	Name des Backup-Tresors	Der Name des Backup-Tresors
IAM-Rolle ARN	iam_role_arn	Die IAM-Rolle ARN
Instanz-ID	instance_id	Eindeutige Instanz-ID
Instance-Status	instance_state	Instance-Status
Instanz-Tags	ec2_tags	Die mit der Instanz-ID verknüpften EC2 Tags
ARN-Ressourcen	resource_arn	Der Name der Amazon-Ressource
Ressourcen-ID	resource_id	Die eindeutige Ressourcen-ID
Region der Ressource	resource_region	Die primären (und gegebenenfalls sekundären) Regionen der Ressource.
Ressourcentyp	resource_type	Der Typ der Ressource

Name des Felds	Feldname des Datensatzes	Definition
ARN für den Wiederherstellungspunkt	recovery_point_arn	Der ARN des Wiederherstellungspunkts
ID des Wiederherstellungspunkts	Wiederherstellungspunkt-ID	Die eindeutige Kennung des Wiederherstellungspunkts
Status des Wiederherstellungspunkts	recovery_point_status	Status des Wiederherstellungspunkts
Löschen des Wiederherstellungspunkts nach Tagen	recovery_point_delete_after_days	Löschen des Wiederherstellungspunkts nach Tagen
Der Erholungspunkt wird nach Tagen in den Kühlraum verschoben	recovery_point_move_to_cold_storage_after_days	Anzahl der Tage nach dem Fertigstellungsdatum, an denen der Backup-Snapshot in den Cold Storage verschoben wird
Verschlüsselungsstatus des Wiederherstellungspunkts	recovery_point_is_encrypted	Verschlüsselungsstatus des Wiederherstellungspunkts
ARN für den Wiederherstellungspunkt-Verschlüsselungsschlüssel	recovery_point_encryption_key_arn	Verschlüsselungsschlüssel ARN für den Wiederherstellungspunkt
Stapel-ID	stack_id	Eindeutige Kennung für den Cloudformation-Stack
Stack-Name	stack_name	Stack-Name
Schlagwort: AMS-Standard-Patchgruppe	tag_ams_default_patch_group	Tag-Wert: AMS-Standard-Patchgruppe
Schlagwort: App-ID	tag_app_id	Tag-Wert: App-ID
Schlagwort: App-Name	tag_app_name	Tag-Wert: App-Name
Schlagwort: Backup	tag_backup	Tagwert: Backup

Name des Felds	Feldname des Datensatzes	Definition
Schlagwort: Compliance-Framework	tag_compliance_framework	Tag-Wert: Compliance-Framework
Schlagwort: Kostenstelle	tag_cost_center	Tag-Wert: Kostenstelle
Schlagwort: Kunde	tag_customer	Tag-Wert: Kunde
Schlagwort: Datenklassifizierung	tag_data_classification	Tag-Wert: Datenklassifizierung
Tag: Umgebungstyp	tag_environment_type	Tag-Wert: Umgebungstyp
Tag: Öffnungszeiten	tag_hours_of_operation	Tag-Wert: Betriebsstunden
Schlagwort: Besizerteam	tag_owner_team	Tag-Wert: Besizerteam
Schlagwort: E-Mail des Eigentümerteams	tag_owner_team_email	Tag-Wert: E-Mail-Adresse des Eigentümerteams
Schlagwort: Patch-Gruppe	tag_patch_group	Tag-Wert: Patch-Gruppe
Schlagwort: Support-Priorität	tag_support_priority	Tag-Wert: Support-Priorität
Status des Volumens	volume_state	Status des Volumens

Zwischenfallbericht (wöchentlich)

Dieser Bericht enthält die aggregierte Liste der Vorfälle zusammen mit ihrer Priorität, ihrem Schweregrad und ihrem aktuellen Status, einschließlich:

- Daten zu Supportfällen, die im verwalteten Konto als Vorfälle eingestuft wurden
- Vorfallinformationen, die zur Visualisierung der Vorfallkennzahlen für das verwaltete Konto erforderlich sind
- Daten zu den Kategorien von Vorfällen und zum Status der Behebung jedes Vorfalls

Sowohl Visualisierungen als auch Daten sind für den wöchentlichen Vorfalbericht verfügbar.

- Auf die Visualisierung kann über die AMS-Konsole im Konto über die Seite Berichte zugegriffen werden.
- Auf den Datensatz mit dem folgenden Schema kann über den S3-Bucket im verwalteten Konto zugegriffen werden.
- Verwenden Sie die bereitgestellten Datumsfelder, um Vorfälle nach Monat, Quartal, Woche oder and/or Tag zu filtern, an dem der Vorfall erstellt oder gelöst wurde.

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Konto-ID	aws_account_id	AWS Konto-ID, zu der der Vorfall gehört.
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Kontoname	Konto_Bezeichnung	AWS Kontoname.
Fallnummer	case_id	Die ID des Vorfalls.
Monat der Erstellung	erstellter_Monat	Der Monat, in dem der Vorfall erstellt wurde.
Priorität	priority	Die Priorität des Vorfalls.
Schweregrad	severity	Die Schwere des Vorfalls.
Status	Status	Der Status des Vorfalls.
Kategorie	yuma_category	Die Kategorie des Vorfalls.
Tag der Erstellung	erstellter_Tag	Der Tag, an dem der Vorfall im Format erstellt wurde. YYYY-MM-DD

Name des Felds	Feldname des Datensatzes	Definition
Woche erstellt	created_wk	Die Woche, in der der Vorfall im Format YYYY-WW erstellt wurde. Sonntag bis Samstag werden als Anfang und Ende einer Woche gezählt. Die Woche dauert von 01 bis 52. Woche 01 ist immer die Woche, die den ersten Tag des Jahres enthält. Beispielsweise befinden sich 2023-12-31 und 2024-01-01 in Woche 2024-01.
Quartal erstellt	created_qtr	Das Quartal, in dem der Vorfall im Format YYYY-Q erstellt wurde. 01/01 bis 03/31 sind als Q1 definiert usw.
Tag der Lösung	resolved_day	Der Tag, an dem der Vorfall im Format behoben wurde. YYYY-MM-DD
Gelöste Woche	resolved_wk	Die Woche, in der der Vorfall gelöst wurde, im Format YYYY-WW. Sonntag bis Samstag werden als Anfang und Ende einer Woche gezählt. Die Woche dauert von 01 bis 52. Woche 01 ist immer die Woche, die den ersten Tag des Jahres enthält. Beispielsweise befinden sich 2023-12-31 und 2024-01-01 in Woche 2024-01.

Name des Felds	Feldname des Datensatzes	Definition
Monat, der gelöst wurde	Resolved_month	Der Monat, in dem der Vorfall behoben wurde, im Format YYYY-MM.
Quartal gelöst	resolved_qtr	Das Quartal, in dem der Vorfall gelöst wurde, im Format YYYY-Q. 01/01 bis 03/31 sind als Q1 definiert usw.
Gruppierungsregel wurde erstellt	grouping_rule	Die Gruppierungsregel, die für den Vorfall gilt. Entweder „no_grouping“ oder „instance_grouping“.
Instanz IDs	instance_ids	Die mit dem Vorfall verknüpfte Instanz.
Anzahl der Alerts	Anzahl_der_Warnmeldungen	Die Anzahl der Warnmeldungen, die mit diesem Vorfall verknüpft sind. Wenn Sie die Gruppierung aktiviert haben, kann diese Zahl größer als 1 sein. Wenn Sie die Gruppierung nicht aktiviert haben, wird sie immer 1 sein.
Erstellt um	created_at	Der Zeitstempel, zu dem der Vorfall erstellt wurde.
Alarm ARNs	alarm_arns	Der Amazon-Ressourcenname („arn“) der Alarme, die mit Ihrem Vorfall verknüpft sind.

Name des Felds	Feldname des Datensatzes	Definition
Verwandte Alarme	verwandte Alarme	Die für Menschen lesbaren Namen aller Alarme, die mit dem Vorfall in Verbindung stehen.

Abrechnungsbericht (monatlich)

Einzelheiten zu den Abrechnungsgebühren

Dieser Bericht enthält Einzelheiten zu den AMS-Abrechnungsgebühren für verknüpfte Konten und die jeweiligen AWS-Services.

Dieser Bericht enthält:

- Daten zu AMS-Gebühren auf Serviceniveau, prozentuale Erhöhungsquoten, AMS-Servicestufen auf Kontoebene und AMS-Gebühren.
- Daten zu verknüpften Konten und AWS-Nutzungsgebühren.

Important

Der monatliche Abrechnungsbericht ist nur in Ihrem Management Payer Account (MPA) oder Ihrem definierten Gebührenkonto verfügbar. Dies sind die Konten, an die Ihre monatliche AMS-Rechnung gesendet wird. Wenn Sie diese Konten nicht finden können, wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM), um Unterstützung zu erhalten.

Name des Felds	Feldname des Datensatzes	Definition
Rechnungsdatum	date	Monat und Jahr der abgerechneten Dienstleistung
Konto-ID des Zahlers	payer_account_id	Die 12-stellige ID, die das Konto identifiziert, das für die

Name des Felds	Feldname des Datensatzes	Definition
		Zahlung der AMS-Gebühren verantwortlich ist
ID des verknüpften Kontos	linked_account_id	Die 12-stellige ID, die das AMS-Konto identifiziert, das Dienste in Anspruch nimmt, die zu hohen Kosten führen
AWS Name des Dienstes	product_name	Der AWS Dienst, der verwendet wurde
AWS Gebühren	aws_charges	Die AWS Gebühren für den AWS Dienstnamen in AWS Service Name
Preisplan	Preisplan	Der mit dem verknüpften Konto verknüpfte Preisplan
AMS Service Group	tier_uplifting_groups	Gruppencode für den AMS-Service, der den Prozentsatz der Erhöhung festlegt
Verhältnis der Erhöhung	prozentualer Anstieg	Der prozentuale Anstieg (als Dezimalzahl V.WXYZ), basierend auf pricing_plan, SLA und Service AWS
Angepasste Gebühren AWS	adjusted_aws_usage	AWS Nutzung für AMS angepasst
Erhöhte Gebühren AWS	uplifted_aws_charges	Der Prozentsatz der Gebühren, die für AMS berechnet werden müssen AWS ; adjusted_aws_charges * uplift_percent

Name des Felds	Feldname des Datensatzes	Definition
EC2 Instanzen, die RDS ausgeben	instances_ec2_rds_spend	Ausgaben für und RDS-Instanzen EC2
Gebühren für Reserved Instances	ris_charges	Gebühren für Reserved Instances
Die Gebühren für Reserved Instances wurden angehoben	uplifted_ris	Der Prozentsatz der Reserved Instance-Gebühren, die für AMS berechnet werden müssen; $\text{ris\_charges} * \text{uplift\_percent}$
Gebühren für den Savings Plan	sp_charges	SavingsPlan Nutzungsggebühren
Erhöhte Sparplangebühren	uplifted_sp	Der Prozentsatz der Sparplangebühren, die für AMS berechnet werden müssen; $\text{sp\_charges} * \text{uplift\_percent}$
AMS-Gebühren	ams_charges	Summe der AMS-Gebühren für das Produkt; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Anteilige Mindestgebühr	anteiliges Minimum	Der Betrag, den wir berechnen, um den vertraglichen Mindestbetrag zu erreichen
Gesamter AMS-Betrag der Gebühren für verknüpfte Konten	linked_account_total ams_charges	Summe aller Gebühren für den Linked_Account

Name des Felds	Feldname des Datensatzes	Definition
AMS-Gebühren insgesamt auf dem Konto des Zahlers	payer_account_total ams_charges	Summe aller Gebühren für das Konto des Zahlers
Mindestgebühr	Mindestgebühren	AMS-Mindestgebühren (falls zutreffend)
discount für Reserved Instance und Savings Plan	adj_ri_sp_charges	RI/SP discount to be applied against RI/SP Gebühren (unter bestimmten Umständen anwendbar)

Aggregierte Berichte

Aggregierte Self-Service-Berichte (SSR) bieten Ihnen einen Überblick über bestehende Self-Service-Berichte, die auf Unternehmensebene kontenübergreifend aggregiert wurden. Auf diese Weise erhalten Sie Einblick in wichtige Betriebskennzahlen wie Patch-Compliance, Backup-Abdeckung und Vorfälle für alle Konten, die in Ihrem Unternehmen von AMS verwaltet werden. AWS Organizations

Aggregierte SSR ist in allen kommerziellen Bereichen verfügbar, in AWS-Regionen denen AWS Managed Services verfügbar sind. Eine vollständige Liste der verfügbaren Regionen finden Sie in der [Regionentabelle](#).

Aktivieren Sie aggregierte Berichte

[Sie müssen aggregiertes SSR von einem Verwaltungskonto aus verwalten. AWS Organizations](#) Das Verwaltungskonto ist das AWS Konto, mit dem Sie Ihre Organisation erstellt haben.

Um Aggregated SSR für ein AWS Organizations Verwaltungskonto zu aktivieren, das in AMS integriert ist, greifen Sie auf Ihre AMS-Konsole zu und navigieren Sie zu Berichte. Wählen Sie in der top-right-hand Ecke Organization Access aus, um den Bereich [AWS Managed Services Console: Organization View](#) zu öffnen. In diesem Bereich können Sie die Aggregated SSR-Funktionalität verwalten.

AWS Organizations Verwaltungskonten, die nicht in AMS integriert sind, haben keinen Zugriff auf die AMS-Konsole. Um Aggregated SSR für ein AWS Organizations Verwaltungskonto zu aktivieren,

das nicht bei AMS integriert ist, authentifizieren Sie sich zunächst bei Ihrem AWS-Konto, navigieren Sie dann zur [AWS Konsole](#) und suchen Sie nach Managed Services. Dadurch wird die AMS-Marketingseite geöffnet. Wählen Sie auf dieser Seite in der Navigationsleiste den Link Organization Access aus, um die AWS Managed Services Services-Konsole zu öffnen: Organization View, in der Sie die Aggregated SSR-Funktionalität verwalten können.

Wenn Sie zum ersten Mal auf die [AWS Managed Services Console: Organization View](#) zugreifen, führen Sie die folgenden Schritte aus:

1. Wenn Sie es noch nicht eingerichtet haben AWS Organizations, wählen Sie in Ihrer Konsole die Option Aktivieren AWS Organizations aus. Weitere Informationen zur Einrichtung AWS Organizations finden Sie im [AWS Organizations Benutzerhandbuch](#). Sie können diesen Schritt überspringen, wenn Sie ihn bereits verwenden AWS Organizations.
2. Um den Aggregated Self-Service Reporting Service zu aktivieren, wählen Sie auf der Konsole die Option Vertrauenswürdigen Zugriff aktivieren aus.
3. (Optional) Registrieren Sie einen delegierten Administrator, um Lesezugriff für die Organisationsansicht zu erhalten.

Zeigen Sie als delegierter Administrator aggregierte Berichte an

Ein delegierter Administrator ist das Konto, das Sie für den Lesezugriff auf die aggregierten Berichte auswählen. Der delegierte Administrator muss ein bei AMS registriertes Konto sein und das einzige Konto sein, das Lesezugriff auf aggregierte Berichte hat.

Um einen delegierten Administrator auszuwählen, geben Sie die Konto-ID in Schritt 3 in der AWS Managed Services Console ein: Organization View. Sie können jeweils nur ein delegiertes Administratorkonto registrieren. Beachten Sie, dass das delegierte Administratorkonto ein von AMS verwaltetes Konto sein muss.

Um ein delegiertes Administratorkonto zu aktualisieren, navigieren Sie zur [AWS Managed Services Console: Organization View](#) und wählen Sie Delegierten Administrator entfernen aus. Die Konsole fordert Sie auf, eine neue Konto-ID einzugeben, um sich als delegierter Administrator zu registrieren.

Lesen Sie aggregierte Berichte

Wenn Sie keinen delegierten Administrator registrieren und Ihr AWS Organizations Verwaltungskonto bei AMS angemeldet ist, erhält das AWS Organizations Verwaltungskonto standardmäßig Lesezugriff auf die aggregierten Berichte. Wenn das AWS Organizations Verwaltungskonto nicht von AMS

verwaltet wird, müssen Sie ein delegiertes Administratorkonto wählen, um Lesezugriff auf die aggregierten Berichte zu haben.

Zu jedem Zeitpunkt hat nur ein einziges Konto, das bei AMS integriert ist, Lesezugriff auf die aggregierten Berichte, entweder das AWS Organizations Verwaltungskonto oder der registrierte delegierte Administrator. Alle anderen Mitgliedskonten in Ihrer Organisation (und bei AMS integriert) haben weiterhin nur Zugriff auf Einzelkontenberichte für jedes einzelne Konto.

[Nachdem Sie Aggregated SSR aktiviert haben, navigieren Sie zu Ihren Berichten.](#) Alle Ihre vorhandenen Self-Service-Berichte werden in diesem Abschnitt aufgeführt, und ein blaues Tag gibt an, dass sie aggregiert wurden. Beachten Sie, dass Sie von dem Konto aus auf die AMS-Konsole zugreifen müssen, das Sie für den Lesezugriff auf die aggregierten Berichte ausgewählt haben. Dies ist entweder das AWS Organizations Verwaltungskonto oder das delegierte Administratorkonto.

Nachdem Sie Aggregated SSR aktiviert haben, sind aggregierte Berichte ab dem nächsten Berichtszyklus verfügbar.

Deaktivieren Sie aggregierte Berichte

Um Aggregated SSR zu deaktivieren, öffnen Sie die [AWS Managed Services Console: Organization View](#). Wählen Sie Vertrauenswürdigen Zugriff deaktivieren aus. Nachdem Sie den vertrauenswürdigen Zugriff für Aggregated SSR deaktiviert haben, werden Ihre AMS-Selfservice-Berichte nicht mehr auf Organisationsebene kontenübergreifend aggregiert. Beachten Sie auch, dass die Deaktivierung ab dem nächsten Berichtszyklus wirksam wird.

Nach der Deaktivierung von Aggregated SSR dauert es eine Wartezeit, bis die Berichte in Ihrer AMS-Konsole als Einzelkonto-Berichte angezeigt werden. Diese Verzögerung ist darauf zurückzuführen, dass die Deaktivierung der Funktion ab dem nächsten Berichtszyklus wirksam wird.

Dashboards für AMS-Selfservice-Berichte

AMS Self-Service Reports bietet zwei Dashboards: und. [Resource Tagger-Dashboard](#) [Dashboard „Regeln für Sicherheitskonfigurationen“](#)

Resource Tagger-Dashboard

Das AMS Resource Tagger Dashboard bietet detaillierte Informationen zu den Ressourcen, die von Resource Tagger unterstützt werden, sowie zum aktuellen Status der Tags, die Resource Tagger so konfiguriert ist, dass sie auf diese Ressourcen angewendet werden.

Resource Tagger-Abdeckung nach Ressourcentyp

Dieser Datensatz besteht aus einer Liste von Ressourcen, deren Tags von Resource Tagger verwaltet werden.

Die Ressourcenabdeckung nach Ressourcentyp wird in Form von vier Liniendiagrammen visualisiert, die die folgenden Kennzahlen beschreiben:

- **Ressourcenanzahl:** Die Gesamtzahl der Ressourcen in der Region, aufgeschlüsselt nach Ressourcentyp.
- **Ressourcen, denen verwaltete Tags fehlen:** Die Gesamtzahl der Ressourcen in der Region, aufgeschlüsselt nach Ressourcentyp, für die verwaltete Tags erforderlich sind, die aber nicht von Resource Tagger markiert wurden.
- **Nicht verwaltete Ressourcen:** Die Gesamtzahl der Ressourcen in der Region, aufgeschlüsselt nach Ressourcentyp, auf die Resource Tagger keine verwalteten Tags angewendet hat. Dies bedeutet in der Regel, dass diese Ressourcen keiner Resource Tagger-Konfiguration entsprechen oder dass sie ausdrücklich von Konfigurationen ausgeschlossen sind.
- **Verwaltete Ressourcen:** Gegenstück zur Metrik „Nicht verwaltete Ressourcen“ (Anzahl der Ressourcen — Nicht verwaltete Ressourcen).

In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung (UTC-Zeit)
AWS-Konto ID	aws_account_id	AWS-Konto AUSWEIS
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdige Konto, das von Ihnen aktiviert wurde. AWS Organizations
Region	Region	AWS-Region
Ressourcentyp	resource_type	Dieses Feld identifiziert den Ressourcentyp. Es sind nur

Feldname	Name des Datensatz-Felds	Definition
		Ressourcentypen enthalten , die von Resource Tagger unterstützt werden.
Anzahl der Ressourcen	resource_count	Anzahl der Ressourcen (des angegebenen Ressourcentyps), die in dieser Region bereitgestellt werden.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	Anzahl der Ressourcen (des angegebenen Ressourcentyps), für die gemäß den Konfigurationsprofilen verwaltete Tags erforderlich sind, die aber noch nicht von Resource Tagger markiert wurden.
UnmanagedResources	unmanaged_resource_count	Anzahl der Ressourcen (des angegebenen Ressourcentyps), auf die vom Resource Tagger keine verwalteten Tags angewendet wurden. In der Regel entsprechen diese Ressourcen keinem Resource Tagger-Konfigurationsblock oder sind ausdrücklich aus Konfigurationsblöcken ausgeschlossen.

Einhaltung der Resource Tagger-Konfigurationsregeln

Dieser Datensatz besteht aus einer Liste von Ressourcen in einem AWS-Region, sortiert nach Ressourcentyp, auf die ein bestimmtes Konfigurationsprofil angewendet wurde. Es wird als Liniendiagramm visualisiert.

In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung (UTC-Zeit)
AWS-Konto ID	aws_account_id	AWS-Konto AUSWEIS
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Region	Region	AWS-Region
Ressourcentyp	resource_type	Dieses Feld identifiziert den Ressourcentyp. Es sind nur Ressourcentypen enthalten , die von Resource Tagger unterstützt werden.
ID des Konfigurationsprofils	configuration_profile_id	Die ID des Resource Tagger-Konfigurationsprofils. Ein Konfigurationsprofil wird verwendet, um Richtlinien und Regeln zu definieren, die zum Taggen Ihrer Ressourcen verwendet werden.
MatchingResourceCount	resource_count	Anzahl der Ressourcen (des angegebenen Ressourcentyps), die der ID des Resource Tagger-Konfigurationsprofils entsprechen. Damit eine Ressource dem Konfigurationsprofil entspricht, muss das Profil aktiviert sein

Feldname	Name des Datensatz-Felds	Definition
		und die Ressource muss der Regel des Profils entsprechen.

Resource Tagger-konforme Ressourcen

Dieser Datensatz besteht aus einer Liste von Ressourcen, die für eine einzelne Resource Tagger-Konfiguration nicht konform sind. Bei diesen Daten handelt es sich um eine tägliche Momentaufnahme der Ressourcen-Compliance. Sie zeigen den Status der Kundenressourcen zum Zeitpunkt der Übermittlung dieser Berichte an die Kundenkonten (es gibt keine historische Ansicht). Es wird als Pivot-Tabelle visualisiert, die aus Ressourcen besteht, die für eine bestimmte Konfiguration nicht konform sind.

In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung (UTC-Zeit)
AWS-Konto ID	aws_account_id	AWS-Konto AUSWEIS
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdige Konto, das von Ihnen aktiviert wurde. AWS Organizations
Region	Region	AWS-Region
Ressourcentyp	resource_type	Dieses Feld identifiziert den Ressourcentyp. Es sind nur Ressourcentypen enthalten , die von Resource Tagger unterstützt werden.

Feldname	Name des Datensatz-Felds	Definition
Ressourcen-ID	resource_id	Die eindeutige Kennung für Ressourcen, die von Resource Tagger unterstützt werden.
Status der Abdeckung	Deckungsstatus	Dieses Feld gibt an, ob die Ressource anhand der Resource Tagger-Konfigurations-ID als konfiguriert gekennzeichnet ist.
ID des Konfigurationsprofils	configuration_profile_id	Die ID des Resource Tagger-Konfigurationsprofils. Ein Konfigurationsprofil wird verwendet, um Richtlinien und Regeln zu definieren, die zum Taggen Ihrer Ressourcen verwendet werden.

Dashboard „Regeln für Sicherheitskonfigurationen“

Das Security Config Rules Dashboard bietet einen detaillierten Einblick in die Ressourcen- und AWS Config Regelkonformität von AMS-Konten. Sie können den Bericht nach dem Schweregrad der Regel filtern, um die wichtigsten Ergebnisse zu priorisieren. In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
AWS-Konto ID	AWS-Konto AUSWEIS	Die Konto-ID, die mit verwandten Ressourcen verknüpft ist.
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations

Feldname	Name des Datensatz-Felds	Definition
Datum/Uhrzeit melden	Datum des Berichts	Datum und Uhrzeit der Berichtsgenerierung.
Kundenname	Name des Kunden	Der Name des Kunden.
Konto_Bezeichnung	Kontoname	Der mit der Konto-ID verknüpfte Name
resource_id	Ressourcen-ID	Ein Bezeichner für eine Ressource.
resource_region	Region der Ressource	Der AWS-Region Ort, an dem sich die Ressource befindet.
resource_type	Ressourcentyp	Der Ressourcentyp AWS-Service oder.
Ressourcenname	Ressourcenname	Der Name der Ressource.
resource_ams_flag	AMS-Flagge der Ressource	Wenn die Ressource im Besitz von AMS ist, ist dieses Flag auf TRUE gesetzt. Wenn sich die Ressource im Besitz des Kunden befindet, ist dieses Flag auf FALSE gesetzt. Wenn der Eigentümer nicht bekannt ist, wird dieses Kennzeichen auf UNKNOWN gesetzt.
config_rule	Konfigurationsregel	Der nicht anpassbare Name für die Konfigurationsregel.
config_rule_description	Beschreibung der Konfigurationsregel	Eine Beschreibung der Konfigurationsregel.

Feldname	Name des Datensatz-Felds	Definition
source_identifizier	Quellen-ID	Ein eindeutiger Bezeichner für die verwaltete Konfigurationsregel und kein Bezeichner für eine benutzerdefinierte Konfigurationsregel.
compliance_flag	Konformitätskennzeichnung	Zeigt an, ob die Ressourcen den Konfigurationsregeln entsprechen oder nicht.
rule_type	Regeltyp	Gibt an, ob die Regel vordefiniert oder benutzerdefiniert ist.
exception_flag	Ausnahme-Flag	Das Ausnahmerkennzeichen für Ressourcen zeigt die Risikobereitschaft gegenüber einer Ressource an, die den Vorschriften nicht entspricht. Wenn das Ausnahmerkennzeichen für eine Ressource den Wert TRUE hat, ist die Ressource ausgenommen. Wenn das Ausnahme-Flag NULL ist, ist die Ressource nicht ausgenommen.
cal_dt	Datum	Das Bewertungsdatum der Regel.
Beschreibung der Abhilfemaßnahme	Beschreibung der Problembhebung	Eine Beschreibung, wie die Einhaltung von Regeln behoben werden kann.

Feldname	Name des Datensatz-Felds	Definition
severity	Schweregrad	Der Schweregrad der Konfigurationsregel gibt die Auswirkungen einer Nichteinhaltung an.
customer_action	Aktion des Kunden	Maßnahmen, die Sie zur Behebung dieser Regel benötigen.
Empfehlung	Empfehlung	Eine Beschreibung dessen, wonach die Konfigurationsregel sucht.
remediation_category	Kategorie „Problembehebung“	Die Standardmaßnahmen, die AMS ergreift, wenn diese Regel nicht mehr konform ist.

Datenaufbewahrungsrichtlinie

AMS SSR hat für jeden Bericht eine Richtlinie zur Aufbewahrung von Daten eingeführt. Nach Ablauf des Berichtszeitraums werden die Daten gelöscht und sind nicht mehr verfügbar.

Name des Berichts	SSR-Konsole zur Datenspeicherung	Datenspeicherung SSR S3-Bucket
Zusammenfassung der Instanzdetails (Patch Orchestrator)	2 Monate	2 Jahre
Einzelheiten zum Patch	2 Monate	2 Jahre
Instanzen, bei denen während der Ausführung des Wartungsfensters Patches übersehen wurden	2 Monate	2 Jahre

Name des Berichts	SSR-Konsole zur Datenspeicherung	Datenspeicherung SSR S3-Bucket
Einzelheiten zu den AMS-Abrechnungsgebühren	2 Jahre	2 Jahre
Täglicher Backup-Bericht	1 Monat	2 Jahre
Wöchentlicher Zwischenfallbericht	2 Monate	2 Jahre
Dashboard mit Regeln für Sicherheitskonfigurationen	3 Monate	2 Jahre
Resource Tagger-Dashboard	1 Jahr	2 Jahre

Offboard von SSR

Um den SSR-Dienst zu verlassen, erstellen Sie über die AMS-Konsole eine Serviceanfrage (SR). Nachdem Sie die SR eingereicht haben, hilft Ihnen ein Betriebstechniker von AMS bei der Auslagerung von SSR. Geben Sie in der SR den Grund an, aus dem Sie aussteigen möchten.

Um ein Konto auszulagern und die Ressourcen zu bereinigen, erstellen Sie über die AMS-Konsole eine SR. Nachdem Sie die SR eingereicht haben, hilft Ihnen ein AMS Operations Engineer beim Löschen des SSR Amazon S3 S3-Buckets.

Wenn Sie das Board von AMS verlassen, werden Sie automatisch von der AMS SSR-Konsole aus ausgebucht. AMS beendet automatisch das Senden von Daten an Ihr Konto. AMS löscht Ihren SSR S3-Bucket im Rahmen des Offboarding-Prozesses.

Vorfallberichte, Serviceanfragen und Abrechnungsfragen in AMS

Themen

- [Vorfallmanagement](#)
- [Verwaltung von Serviceanfragen](#)
- [Fragen zur Abrechnung](#)

Mit AWS Managed Services (AMS) können Sie jederzeit über die AMS-Konsole Hilfe bei betrieblichen Problemen und Anfragen anfordern. Die Betriebstechniker von AMS stehen Ihnen rund um die Uhr zur Verfügung, um auf Ihre Vorfälle und Serviceanfragen zu reagieren, wobei die Reaktionszeit von Service Level Agreements (SLAs) und Service Level Objectives (SLOs) abhängig von Ihrem ausgewählten Konto Service Tier (Plus, Premium) ist. Die Betriebsingenieure von AMS benachrichtigen Sie mithilfe derselben Mechanismen proaktiv über wichtige Warnmeldungen und Fragen.

Vorfallmanagement

Themen

- [Was ist Incident Management?](#)
- [Verpflichtungen im Bereich Incident Management](#)
- [Beispiele für das Incident-Management](#)

Vorfälle sind AWS-Service Leistungsprobleme, die sich auf Ihre verwaltete Umgebung auswirken, wie von AWS Managed Services (AMS) oder Ihnen festgestellt. Vorfälle, die vom AMS-Team identifiziert wurden, werden zunächst als „Ereignisse“ empfangen. Dabei handelt es sich um eine Änderung des Systemstatus, die durch die Überwachung erfasst wird. Wenn ein konfigurierter Schwellenwert überschritten wird, löst das Ereignis einen Alarm aus, der auch als Warnung bezeichnet wird. Das AMS-Betriebsteam bestimmt, ob das Ereignis keine Auswirkungen hat, ob es sich um einen Vorfall (eine Betriebsunterbrechung oder -verschlechterung) oder um ein Problem (die zugrunde liegende Ursache für einen oder mehrere gelöste Vorfälle) handelt.

Das AMS-Team erhält auch Vorfälle, die Sie über das Support Center oder programmgesteuert mithilfe der [AWS-Support-API](#) mit dem Servicecode identifiziert haben. `sentinel-report-incident`

Nachdem Ihr Vorfall beim AMS-Betriebsteam eingegangen ist, wird er überprüft, um sicherzustellen, dass der Vorfall nicht besser als Serviceanfrage eingestuft wird. Sollte der Fall als Serviceanfrage eingestuft werden, wird er sofort neu klassifiziert und das AMS-Serviceanfrageteam übernimmt den Vorgang, und Sie werden benachrichtigt. Wenn der Vorfall vom empfangenden Betreiber behoben werden kann, werden unverzüglich Maßnahmen ergriffen, um den Vorfall zu lösen. Die Mitarbeiter von AMS ziehen interne Unterlagen zu Rate, um eine Lösung zu finden, und leiten den Vorfall bei Bedarf an andere Support-Mitarbeiter weiter, bis der Vorfall behoben ist. Um bei jedem Schritt der Problembehebung auf dem Laufenden zu bleiben, müssen Sie die Option CC-E-Mails ausfüllen. Wenn Sie die Verbindung über einen Verbund herstellen möchten, melden Sie sich an, bevor Sie dem Link in der von AMS gesendeten E-Mail folgen. Nach der Behebung dokumentiert das AMS-Betriebsteam den Vorfall und die Lösung für die future Verwendung.

Wenn zur Behebung eines Vorfalls Änderungen an der Infrastruktur erforderlich sind, ist möglicherweise eine Sicherheitsüberprüfung erforderlich. Zu den Infrastrukturänderungen, die möglicherweise eine Sicherheitsüberprüfung erfordern, gehören Änderungen im Zusammenhang mit IAM oder ressourcenbasierten Richtlinien oder Risikogenehmigungen. Für diese Art von Vorfällen muss ein AMS Operations Engineer einen RFC erstellen, bevor er die Änderung vornimmt, und Sie müssen diesem RFC zustimmen. Wenn die Lösung des Vorfalls beispielsweise die Aktualisierung einer IAM-Richtlinie erfordert, wird eine AMS-Sicherheitsüberprüfung durchgeführt, und dann erstellt ein AMS Operations Engineer einen RFC mit den Komponenten Management | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie aktualisieren (ct-27tuth19k52b4) und wartet, bis Sie den RFC genehmigen, bevor Sie fortfahren.

Note

AMS ermöglicht jetzt die Lösung von Vorfällen, bei denen Infrastrukturänderungen ohne den zusätzlichen Schritt der RFC-Genehmigung vorgenommen werden müssen. Wenn die zur Behebung des Vorfalls erforderlichen Änderungen KEINE Sicherheitsüberprüfung erfordern (die Änderung bezieht sich nicht auf IAM, ressourcenbasierte Richtlinien oder Risikogenehmigungen), kann AMS die Änderungen auf der Grundlage Ihrer im Rahmen des Vorfalls erhaltenen Genehmigung vornehmen, ohne dass eine separate Genehmigung in einem RFC erforderlich ist.

[Definitionen von Begriffen für das Incident-Management finden Sie unter Wichtige Begriffe von AMS.](#)

Informationen zum Eskalationspfad von Vorfällen finden Sie unter [Hilfe erhalten](#).

Eine Beschreibung der Reaktion von AMS auf Vorfälle finden Sie unter [AMS-Reaktion auf Vorfälle](#).

Was ist Incident Management?

Incident Management ist der Prozess, den AMS verwendet, um aktive Vorfälle aufzuzeichnen, darauf zu reagieren, den Fortschritt zu kommunizieren und darüber zu informieren.

Das Ziel des Incident-Management-Prozesses besteht darin, sicherzustellen, dass der normale Betrieb Ihres Managed Services so schnell wie möglich wiederhergestellt wird, die Auswirkungen auf das Geschäft minimiert werden und alle betroffenen Parteien auf dem Laufenden gehalten werden.

Beispiele für Vorfälle sind unter anderem der Verlust oder die Verschlechterung der Netzwerkkonnektivität, ein Prozess oder eine API, die nicht reagiert, oder eine geplante Aufgabe, die nicht ausgeführt wird (z. B. ein fehlgeschlagenes Backup).

Die folgende Grafik zeigt den Arbeitsablauf eines Vorfalls, den Sie AMS gemeldet haben.

Diese Grafik zeigt den Arbeitsablauf eines Vorfalls, der Ihnen von AMS gemeldet wurde.

Priorität des Vorfalls

Incidents, die im AWS Support Center, in der Konsole oder in der Support API (SAPI) erstellt wurden, haben andere Klassifizierungen als Incidents, die in der AMS-Konsole erstellt wurden.

- **Niedrig:** Nicht kritische Funktionen Ihres Geschäftsservices oder Ihrer Anwendung, die sich auf AWS- oder AMS-Ressourcen beziehen, sind betroffen.
- **Mittel:** Ein Unternehmensservice oder eine Anwendung, die sich auf AWS and/or AMS-Ressourcen bezieht, ist mäßig beeinträchtigt und funktioniert in einem heruntergestuften Zustand.
- **Hoch:** Ihr Unternehmen ist erheblich beeinträchtigt. Kritische Funktionen Ihrer Anwendung im Zusammenhang mit AWS and/or AMS-Ressourcen sind nicht verfügbar. Reserviert für die kritischsten Ausfälle, die Produktionssysteme betreffen.

Note

Die AWS-Supportkonsole bietet fünf Prioritätsstufen für Vorfälle, die wir in die drei AMS-Stufen übersetzen.

Problem im Vergleich zu Vorfall

Wenn AMS der Ansicht ist, dass ein Vorfall auf einen größeren Defekt oder eine Fehlkonfiguration hinweist und erneut auftreten könnte, wird der Vorfall nicht nur als Vorfall, sondern als Problem betrachtet. In solchen Fällen führt AMS Analysen des Problems durch und unterbreitet Vorschläge zur Lösung des Problems.

Verpflichtungen im Bereich Incident Management

Leistungszusagen für das Incident-Management

Ereignis oder Aktion	Messung des Leistungsversprechens
Fall 1: Es wird ein Ereignis mit bekannten Auswirkungen ausgelöst. AMS eröffnet einen Vorfall und informiert Sie.	Die Frist für die Reaktion auf Vorfälle und die Behebung von Vorfällen beginnt, wenn:
Fall 2: AMS kontaktiert Sie, um die Auswirkungen des Ereignisses zu bestätigen. Sie bestätigen, dass es sich bei dem Ereignis um einen Vorfall handelt.	Fall 1: AMS verursacht einen Vorfall.
Fall 3: Sie stellen ein Problem fest und reichen einen Vorfallbericht ein.	Fall 2: Sie bestätigen, dass es sich bei der Warnung um einen Vorfall handelt.
	Fall 3: Sie melden einen Vorfall.
Wenn Sie den Vorfall einreichen, sendet AMS eine Antwort, um ihn zu bestätigen.	Die Serviceversprechen hängen von der Priorität des verursachten Vorfalls ab.
Wenn AMS den Vorfall in Ihrem Namen erstellt, wird keine separate Antwort auf den Vorfall gesendet.	Die Zeit für die Behebung des Vorfalls läuft weiter.
	Die Zeit für die Reaktion auf Vorfälle endet, wenn AMS die Bestätigung des Vorfalls sendet.

Ereignis oder Aktion	Messung des Leistungsversprechens
	 Note Die Zeit, die Sie damit verbringen, auf Eingaben von Ihnen zu warten, wird bei der Berechnung der Zeit für die Behebung von Vorfällen nicht berücksichtigt. Bei Vorfällen, die AMS erstellt, entspricht die erste Reaktionszeit dem Zeitpunkt, zu dem die erste Benachrichtigung über den Vorfall an Sie erstellt wurde.

Ereignis oder Aktion	Messung des Leistungsversprechens
AMS überprüft den Zustand der betreffenden Ressourcen/Dienste, um zu überprüfen, ob: • Ein von AMS festgestelltes Ereignis oder ein vom Kunden eingereichter Vorfall gilt als Vorfall und • der Vorfall ist korrekt priorisiert und Wenn ein von Ihnen eingereichter Vorfall nicht korrekt priorisiert wurde, ordnet AMS ihm eine neue Priorität zu. Wenn AMS die Priorität eines Vorfalls ändert, erhalten Sie eine Benachrichtigung zusammen mit den Gründen für die Änderung der Priorität. In bestimmten Fällen gilt ein von Ihnen eingereichtes Problem je nach Ursache möglicherweise nicht als Vorfall. In diesen Fällen schließt AMS den Vorfall ab und sendet Ihnen eine Benachrichtigung mit der Begründung. Unabhängig von der Kategorie der Ereignisse arbeitet AMS mit Ihnen zusammen, um Ihnen bei Bedarf weiterzuhelfen. Informationen zu den Regeln für die Kategorisierung von Vorfällen finden Sie unter. Priorität des Vorfalls	Falls sich die Priorität des Vorfalls ändert, gilt die Serviceversicherung für die neue Priorität ; die Uhr tickt weiter. In Fällen, in denen ein Vorfall abgeschlossen wird, weil er nicht der Definition eines Vorfalls entspricht, gelten keine Serviceversprechen; die Uhr bleibt stehen.

Ereignis oder Aktion	Messung des Leistungsversprechens
AMS bearbeitet den Vorfall, um ihn im Rahmen der Serviceverpflichtung zu lösen. Wenn AMS in bestimmten Fällen feststellt, dass nicht verfügbare Stacks oder Ressourcen nicht rechtzeitig behoben werden können, bietet AMS die Wiederherstellung der Infrastruktur als Option zur Lösung an. Die Wiederherstellung der Infrastruktur beinhaltet die erneute Bereitstellung vorhandener Stacks auf der Grundlage der Vorlagen der betroffenen Stacks und die Initiierung einer Datenwiederherstellung auf der Grundlage des letzten bekannten Wiederherstellungspunkts (EBS/RDS-Snapshot), sofern von Ihnen nichts anderes angegeben wurde. Kurzlebige Daten auf einzelnen Instanzen gehen verloren. EC2 Wenn Sie eine Wiederherstellung der Infrastruktur nicht wie von AWS empfohlen autorisieren, haben Sie keinen Anspruch auf eine Servicegutschrift für das zugehörige Incident Resolution Time Service Commitment.	Die Uhr stoppt, wenn: - AMS hat alle Dienste oder Ressourcen, die sich auf diesen Vorfall beziehen, auf den Status „Nicht verfügbar“ zurückgesetzt, oder - eine Wiederherstellung der Infrastruktur wurde gestartet.
Gelegentlich benötigt AMS eine Klarstellung von Ihnen oder eine Aktivität von Ihnen, um die Behebung von Vorfällen voranzutreiben, es sei denn, Sie haben eine vordefinierte, genehmigte Maßnahme. Daher besteht eine Kommunikation zwischen AMS und Ihnen, um Vorfälle zu lösen	Die Uhr stoppt, wenn: AMS auf eine Antwort oder Aktion von Ihnen wartet. Die Uhr wird neu gestartet, wenn: AMS die Antwort von Ihnen erhält oder die von AMS von Ihnen geforderte Aktion abgeschlossen ist.

 Note

Eine vollständige Liste der Serviceversprechen finden Sie im [AMS Service Level Agreement](#).

Beispiele für das Incident-Management

Beispiele für das Incident-Management.

Themen

- [Testen von Vorfällen](#)
- [Meldung von Vorfällen](#)
- [Überwachung und Aktualisierung von Vorfällen](#)
- [Verwaltung von Vorfällen mit der AWS-Support-API](#)
- [Reaktion auf AMS-generierte Vorfälle](#)

Die folgenden Beispiele beschreiben die Verwendung der AMS-Konsole zum Einreichen eines Vorfalls. Nach der Übermittlung arbeitet das AMS-Team mit Ihnen zusammen, um den Vorfall gemäß Ihrem Service Level Agreement (SLA) zu lösen.

Testen von Vorfällen

Beim Testen von AMS-Incident-Einsendungen bitten wir Sie, in den Betrefftext dieses Kennzeichen aufzunehmen: AMSTestNoOpsActionRequired. Dieses Kennzeichen informiert AMS darüber, dass die Übermittlung des Vorfalls nur zu Testzwecken dient. Wenn die Betriebstechniker von AMS diese Markierung sehen, werden sie in keiner Weise auf die Meldung des Vorfalls reagieren.

Meldung von Vorfällen

Verwenden Sie die AMS-Konsole, um einen Vorfall zu melden. Es ist wichtig, für jedes neue Problem oder jede neue Frage einen neuen Vorfall zu erstellen. Bei der Eröffnung von Fällen, die sich auf alte Anfragen beziehen, ist es hilfreich, die entsprechende Fallnummer anzugeben, damit wir auf frühere Korrespondenz zurückgreifen können.

Note

Wenn die Fallkorrespondenz vom ursprünglichen Problem abweicht, bittet Sie ein AMS-Mitarbeiter möglicherweise, einen neuen Vorfall zu melden.

Um einen Vorfall über die AMS-Konsole zu melden:

1. Wählen Sie in der linken Navigationsleiste Incidents

Die Liste der Vorfälle wird geöffnet:

Wenn Ihre Vorfalldatei leer ist, setzt die Option Filter löschen den Filter auf den Status Beliebig zurück.

Wenn Sie wissen, dass Sie Telefon oder Chat verwenden möchten, klicken Sie im Support Center auf Incident erstellen, um die Seite Incident Create in der Support Center-Konsole zu öffnen, die automatisch mit dem AMS-Servicetyp gefüllt wird.

Important

- Telefonanrufe, die mit initiiert wurden, Support werden aufgezeichnet, um die Reaktionszeit zu verbessern. Wenn der Anruf unterbrochen wird, müssen Sie über das Support Center zurückrufen. Es gibt keine Möglichkeit, AWS Sie zurückzurufen.
- Der Telefon- und Chat-Support ist darauf ausgelegt, bei Supportfällen, Vorfällen und Serviceanfragen zu helfen, nicht bei RFC- oder Sicherheitsproblemen.
- Verwenden Sie bei RFC-Problemen die Korrespondenzoption auf der entsprechenden RFC-Detailseite, um einen AMS-Techniker zu kontaktieren.
- Erstellen Sie bei Sicherheitsproblemen eine Support-Anfrage mit hoher Priorität (P1 oder P2). Die Live-Chat-Funktion ist nicht für Sicherheitsereignisse vorgesehen.

2. Wenn Sie nach einem vorhandenen Vorfall suchen möchten, wählen Sie in der Drop-down-Liste einen Vorfalldatenfilter aus.

- Alle Vorfälle, die noch nicht behoben wurden.
- Ein neuer Vorfall, der noch nicht zugewiesen wurde.
- Ein Vorfall, der zugewiesen wurde.
- Ein Vorfall, den Sie erneut aufgegriffen haben.

- Ein zugewiesener, komplizierter Vorfall.
- Vorfälle, für die vor dem nächsten Schritt Ihr Feedback erforderlich ist.
- Vorfälle, zu denen Sie kürzlich Informationen übermittelt haben.
- Ein Vorfall, der abgeschlossen ist.
- Alle Vorfälle auf dem Konto.

3. Wählen Sie Erstellen aus.

Die Seite „Vorfall erstellen“ wird geöffnet:

4. Wählen Sie eine Priorität aus:

- Niedrig: Nicht kritische Funktionen Ihres Unternehmensdienstes oder Ihrer Anwendung im Zusammenhang mit AWS/AMS-Ressourcen sind betroffen.
- Mittel: Ein Unternehmensdienst oder eine Anwendung, die sich auf AWS/AMS-Ressourcen bezieht, ist mäßig beeinträchtigt und funktioniert in einem eingeschränkten Zustand.
- Hoch: Ihr Unternehmen ist erheblich beeinträchtigt. Kritische Funktionen Ihrer Anwendung im Zusammenhang mit AWS/AMS-Ressourcen sind nicht verfügbar. Reserviert für die kritischsten Ausfälle, die Produktionssysteme betreffen.

5. Wählen Sie eine Kategorie aus.

 Note

Wenn Sie die Incident-Funktionalität testen möchten, fügen Sie Ihrem Incident-Titel das Kennzeichen „Keine Aktion“ (AMSTestNoOpsActionRequired) hinzu.

6. Geben Sie Informationen ein für:

- Betreff: Ein aussagekräftiger Titel für den Vorfallbericht.
- CC-E-Mails: Eine Liste mit E-Mail-Adressen für Personen, die Sie über den Bericht und die Lösung des Vorfalls informieren möchten.
- Einzelheiten: Eine umfassende Beschreibung des Vorfalls, der betroffenen Systeme und des erwarteten Ergebnisses der Lösung. Beantworten Sie die voreingestellten Fragen oder löschen Sie sie und geben Sie alle relevanten Informationen ein.

Um einen Anhang hinzuzufügen, wählen Sie Anlage hinzufügen, suchen Sie nach der gewünschten Anlage und klicken Sie auf Öffnen. Um den Anhang zu löschen, klicken Sie auf das Symbol Löschen:

7. Wählen Sie Absenden aus.

Es öffnet sich eine Detailseite mit Informationen zu dem Vorfall — wie Typ, Betreff, Erstellt, ID und Status — sowie ein Korrespondenzbereich, der die Beschreibung der von Ihnen erstellten Anfrage enthält.

Klicken Sie auf Antworten, um einen Korrespondenzbereich zu öffnen und zusätzliche Informationen oder Statusaktualisierungen bereitzustellen.

Klicken Sie auf Fall schließen, wenn der Vorfall gelöst wurde.

Klicken Sie auf Mehr laden, wenn mehr Korrespondenz vorhanden ist, als auf eine Seite passt.

Vergessen Sie nicht, die Kommunikation zu bewerten!

Ihr Vorfall wird auf der Seite mit der Liste der Vorfälle angezeigt.

YouTube Video: [Wie melde ich einen Vorfall von der AWS Managed Services Services-Konsole aus?](#)

Überwachung und Aktualisierung von Vorfällen

Sie können Vorfallberichte und Serviceanfragen, beides sogenannte Fälle, mithilfe der AMS-Konsole oder programmgesteuert mithilfe der API aktualisieren, überwachen und überprüfen. Support Informationen zur Verwendung der Support API finden Sie unter [DescribeCases](#)Bedienung.

Gehen Sie wie folgt vor, um einen Fall, einen Vorfall oder eine Serviceanfrage mithilfe der AMS-Konsole zu überwachen.

1. Suchen Sie im Dashboard „Vorfallberichte“ oder „Serviceanfragen“ der AMS-Konsole nach einem Fall und wählen Sie den Betreff aus, um eine Detailseite mit dem aktuellen Status und den Korrespondenzen zu öffnen.

Wenn ein gemeldeter Vorfall oder eine Serviceanfrage vom AMS-Betriebsteam aktualisiert wird, erhalten Sie eine E-Mail und einen Link zu dem Vorfall in der AMS-Konsole, sodass Sie darauf antworten können. Sie können auf die Korrespondenz mit einem Vorfall nicht antworten, indem Sie auf die E-Mail antworten.

 Important

Sie müssen eine E-Mail-Adresse eingegeben haben, um Benachrichtigungen über Statusänderungen im Zusammenhang mit einer Serviceanfrage oder einem Vorfall zu erhalten. Benachrichtigungen werden nur an die E-Mail-Adresse gesendet, die dem Fall bei der Erstellung hinzugefügt wurde.

Der Link in der Benachrichtigungs-E-Mail funktioniert nur, wenn Sie einen E-Mail-Server in Ihrem AMS-Verbundnetzwerk verwenden. Sie können jedoch auf die Korrespondenz antworten, indem Sie Ihre AMS-Konsole aufrufen und die Seite mit den Falldetails verwenden.

2. Wenn die Liste viele Fälle enthält, können Sie die Option Filter verwenden:

- Alle geöffnet (Standard): Verwenden Sie diesen Filter, um alle Fälle zu sehen, die nicht gelöst wurden.
- Nicht zugewiesen: Verwenden Sie diese Option, wenn Sie den Fall gerade eingereicht haben und keine Benachrichtigung erhalten haben, dass sich der Status des Falls geändert hat. Hinweis: Vorfälle und Serviceanfragen werden je nach der eingereichten Priorität (Vorfälle) oder Ihrem Service Level Agreement (Serviceanfragen) unterschiedlich schnell bearbeitet.
- Öffnen: Verwenden Sie diese Option, wenn Sie die Benachrichtigung erhalten haben, dass es sich bei dem Fall um die Aktion „Ausstehend bei Amazon“ handelt. Dies bedeutet, dass der Fall zugewiesen wurde, die Bearbeitung jedoch noch nicht begonnen hat.
- Erneut geöffnet: Verwenden Sie diese Option, wenn Sie die Benachrichtigung erhalten haben, dass der Fall nach der Bearbeitung erneut geöffnet wurde.
- In Bearbeitung: Verwenden Sie diese Option, wenn Sie die Benachrichtigung erhalten haben, dass ein Mitarbeiter mit der Bearbeitung des Falls begonnen hat.
- Ausstehende Bearbeitung durch den Kunden: Verwenden Sie diese Option, wenn Sie von Ihrer Seite eine Aufforderung zum Tätigwerden erhalten haben.
- Kundenaktion abgeschlossen: Verwenden Sie diese Option, wenn Sie eine Benachrichtigung erhalten haben, dass Ihre Maßnahme in Bezug auf den Fall bearbeitet wurde.

- Gelöst: Dient zum Anzeigen von Fällen, von denen Sie wissen, dass sie gelöst wurden. Gelöste Fälle werden zwölf Monate lang in der Historie gespeichert.
 - Beliebiger Status: Verwenden Sie diesen Filter, um alle Fälle unabhängig vom Status anzuzeigen.
3. Um den aktuellen Status zu überprüfen, aktualisieren Sie die Seite.
 4. Wenn es so viele Korrespondenzen gibt, dass nicht alle auf der Seite angezeigt werden, wählen Sie „Mehr laden“.
 5. Um den Status des Falls zu aktualisieren, wählen Sie Antworten, geben Sie die neue Korrespondenz ein und klicken Sie dann auf Absenden.
 6. Um den Fall abzuschließen, nachdem er zu Ihrer Zufriedenheit gelöst wurde, wählen Sie Fall schließen.

Stellen Sie sicher, dass Sie den Service anhand der 1-5 Sterne bewerten, damit AMS weiß, wie es uns geht!

Verwaltung von Vorfällen mit der AWS-Support-API

Die [AWS-Support-API](#) ermöglicht es Ihnen, Vorfälle zu erstellen und ihnen während der Untersuchung Ihrer Probleme und Interaktionen mit AWS-Supportmitarbeitern Korrespondenz hinzuzufügen. Die AWS-Support-API modelliert einen Großteil des Verhaltens des [AWS Support Centers](#). Weitere Informationen darüber, wie Sie diesen AWS-Support-Service nutzen können, finden Sie unter [Programmieren eines AWS-Supportfalls](#).

Note

Wenn Sie die AWS Support API oder SAPI für AMS Advanced-Vorfälle verwenden, verwenden Sie diesen Servicecode: `sentinel-report-incident`.

Reaktion auf AMS-generierte Vorfälle

AMS überwacht Ihre Ressourcen proaktiv. Weitere Informationen finden Sie unter [Überwachung und Ereignismanagement](#). Manchmal identifiziert AMS einen Vorfall und erstellt ihn, meistens, um Sie über einen Vorfall zu informieren. Falls Sie Maßnahmen ergreifen müssen, um einen Vorfall zu lösen, sendet AMS eine Benachrichtigung an die Kontaktinformationen, die Sie für das Konto angegeben haben. Sie reagieren auf diesen Vorfall genauso wie auf jeden anderen Vorfall. In der Regel würden

Sie auf Vorfälle über die AMS-Konsole reagieren. In einigen Fällen ist eine Kontaktaufnahme per E-Mail oder Telefon erforderlich.

Note

AMS sendet Mitteilungen an Ihre primäre E-Mail-Adresse in Ihrem AWS-Konto. Wir empfehlen, einen alternativen Operations-Kontakt-E-Mail-Alias hinzuzufügen, um den Incident-Management-Prozess zu vereinfachen. Dies wird während des AMS-Onboarding-Prozesses und der zugehörigen Onboarding-Dokumentation behandelt. Wenn Sie AMS während des Onboardings Kontakte zur Verfügung gestellt haben, die nicht auf Ressourcen basieren (über die Sie Ihren CSDM informiert haben), werden diese Kontakte verwendet. Sie könnten Ihnen beispielsweise eine Kontaktliste mit dem Namen "SecurityContacts" zur Verfügung stellen, die Sie für sicherheitsrelevante CSDMs/CAs Vorfälle oder Benachrichtigungen verwenden können. Ihre Kontakt-Stichwörter instances/resources werden für von AMS generierte Vorfälle verwendet, sofern Sie CSDM Ihre Zustimmung zur Verwendung von Tag-Informationen gegeben haben.

[Weitere Informationen zu diesem Benachrichtigungsdienst finden Sie unter Benachrichtigungen.](#)

Verwaltung von Serviceanfragen

Themen

- [Wann sollte eine Serviceanfrage verwendet werden](#)
- [So funktioniert die Verwaltung von Serviceanfragen](#)
- [Testen einer Serviceanfrage in AMS](#)
- [Eine Serviceanfrage in AMS erstellen](#)
- [Überwachung und Aktualisierung von Serviceanfragen in AMS](#)
- [Beantwortung von AMS-generierten Serviceanfragen](#)

Serviceanfragen sind Mitteilungen an AMS, die von Ihnen erstellt wurden, um Informationen oder Rat einzuholen. Ein gutes Beispiel für eine Standard-Serviceanfrage ist Beratung oder Hilfe bei der Konfiguration eines AMS-Dienstes wie Alarm Manager, Patch Orchestrator usw. Sie können auch Serviceanfragen von AMS erhalten. Diese werden als ausgehende Serviceanfragen oder Servicebenachrichtigungen bezeichnet. Eine Liste Ihrer Serviceanfragen und ausgehenden

Serviceanfragen (Servicebenachrichtigungen), die Ihnen von AMS gesendet wurden, finden Sie auf der Seite Serviceanfragen der AMS-Konsole.

Weitere Informationen zu ausgehenden Serviceanfragen finden Sie unter. [Beantwortung von AMS-generierten Serviceanfragen](#)

Sie erstellen eine AWS Managed Services (AMS) -Serviceanfrage mithilfe der AMS-Konsole oder programmgesteuert mithilfe der Support API. [Einzelheiten zur Verwendung der API finden Sie unter Support API](#). Wählen Sie für AMS den `sentinel-service-request` Servicecode aus.

Nachdem Ihre Serviceanfrage beim AMS Operations Team eingegangen ist, wird sie gemäß Ihrem Service Level Agreement priorisiert. Um bei jedem Schritt des Prozesses zur Lösung von Serviceanfragen auf dem Laufenden zu bleiben, müssen Sie die Option CC-E-Mails ausfüllen. Wenn Sie die Verbindung über einen Verbund herstellen möchten, melden Sie sich an, bevor Sie dem Link in der von AMS gesendeten E-Mail folgen.

Verwenden Sie die Seite „Serviceanfrage erstellen“ der AMS-Konsole, um die folgenden Aufgaben auszuführen:

- Eine Serviceanfrage erstellen und aktualisieren
- Rufen Sie eine Liste mit detaillierten Informationen zu all Ihren aktuellen Serviceanfragen ab
- Grenzen Sie Ihre Suche nach Serviceanfragen nach Datum und Vorfallkennungen ein, einschließlich Anfragen, die gelöst wurden
- Fügen Sie Mitteilungen und Dateianhänge zu Ihren Anfragen hinzu und fügen Sie E-Mail-Empfänger für die Fallkorrespondenz hinzu
- Bearbeiten Sie Serviceanfragen
- Bewerten Sie die Kommunikation mit Serviceanfragen

Wann sollte eine Serviceanfrage verwendet werden

Die folgenden Beispiele beschreiben eine Serviceanfrage:

- AMS oder AWS allgemeine Anleitung
- Fragen im Zusammenhang mit Patch MW
- Fragen zum Backup-Zeitplan
- Fragen zur Funktionalität von AWS Diensten

Im Folgenden finden Sie Beispiele dafür, was in einer Serviceanfrage nicht angesprochen werden sollte:

- Probleme beim Zugriff
- Patch-Fehler
- Backup-Fehler
- RFC-Fehler oder RFC, der eine Betriebsunterbrechung verursacht (Verwenden Sie Incident für Betriebsunterbrechung)
- RFC-Fragen oder zusätzliche Eingaben oder Änderung des RFC-Bereichs (Verwenden Sie bidirektionale RFC-Korrespondenz)

So funktioniert die Verwaltung von Serviceanfragen

Serviceanfragen werden vom AMS-Betriebsteam auf Abruf bearbeitet.

Nachdem Ihre Serviceanfrage beim AMS Operations Team eingegangen ist, wird sie überprüft, um sicherzustellen, dass die Anfrage nicht besser als Vorfall eingestuft wird. Sollte es als Vorfall eingestuft werden, wird es sofort neu klassifiziert, das AMS Incident Management Team übernimmt die Aufgabe und Sie werden benachrichtigt.

Wenn die Serviceanfrage durch die Einreichung eines RFC gelöst werden kann, sendet Ihnen der überprüfende Mitarbeiter eine E-Mail mit der Aufforderung, den entsprechenden RFC einzureichen (Einzelheiten werden bereitgestellt).

Wenn der AMS-Betreiber die Serviceanfrage lösen kann, werden sofort entsprechende Schritte unternommen. Wenn es sich bei der Serviceanfrage beispielsweise um Architekturberatung oder andere Informationen handelt, verweist der Betreiber Sie auf die entsprechenden Ressourcen oder beantwortet die Frage direkt.

Wenn bei der Analyse Ihrer Serviceanfrage ein Fehler oder eine Funktionsanfrage festgestellt wird, sendet AMS Ihnen im Rahmen der Serviceanfrage eine Benachrichtigung. Da es keine voraussichtliche Ankunftszeit für Funktionsanfragen oder Bugfixes gibt, ist die ursprüngliche Serviceanfrage geschlossen. Wenden Sie sich an Ihren CSDM, wenn Sie weitere Fragen zur ursprünglichen Serviceanfrage haben.

Wenn die Serviceanfrage außerhalb des Geltungsbereichs von AMS liegt, sendet der Betreiber die Anfrage entweder an Ihren Cloud Service Delivery Manager, damit dieser mit Ihnen kommunizieren

kann, oder an das entsprechende AWS Betriebsteam, zusammen mit einer E-Mail an Sie, in der Sie darüber informiert werden, welche Schritte unternommen werden.

Die Serviceanfrage ist erst gelöst, wenn Sie angegeben haben, dass Sie mit dem Ergebnis zufrieden sind.

 Note

Wir empfehlen in jedem Fall, eine Kontakt-E-Mail-Adresse, einen Namen und eine Telefonnummer anzugeben, um die Kommunikation zu erleichtern.

Testen einer Serviceanfrage in AMS

Beim Testen von AMS-Serviceanfragen bitten wir Sie, in den Betrefftext dieses Kennzeichen aufzunehmen: `AMSTestNoOpsActionRequired`um AMS darüber zu informieren, dass die Serviceanfrage nur zu Testzwecken dient. Wenn die Betriebstechniker von AMS diese Kennzeichnung sehen, antworten sie nicht auf die Serviceanfrage.

Eine Serviceanfrage in AMS erstellen

So erstellen Sie eine Serviceanfrage mit der AWS Managed Services (AMS) -Konsole:

1. Wählen Sie in der linken Navigationsleiste Serviceanfragen aus.

Die Liste der Serviceanfragen wird geöffnet.

Wenn Ihre Liste mit Serviceanfragen leer ist, setzt die Option Filter löschen den Filter auf den Status Beliebig zurück.

Wenn Sie wissen, dass Sie Telefon oder Chat verwenden möchten, klicken Sie im Support Center auf Serviceanfrage erstellen, um die Seite Serviceanfrage erstellen in der Support Center-Konsole zu öffnen, die automatisch mit dem AMS-Servicetyp gefüllt wird.

 Note

Telefonanrufe, die mit dem Support Center eingeleitet wurden, werden aufgezeichnet, um die Reaktion zu verbessern. Wenn der Anruf unterbrochen wird, müssen Sie über das Support Center zurückrufen. Es gibt keine Möglichkeit, AWS Sie zurückzurufen.

 Important

Der Telefon- und Chat-Support ist darauf ausgelegt, Ihnen bei Supportfällen, Vorfällen und Serviceanfragen zu helfen. Verwenden Sie bei RFC-Problemen die Korrespondenzoption auf der entsprechenden RFC-Detailseite, um einen AMS-Techniker zu kontaktieren.

2. Wenn Sie nach einer vorhandenen Serviceanfrage suchen möchten, wählen Sie in der Dropdownliste einen Statusfilter für Serviceanfragen aus.

- Alle Serviceanfragen, die noch nicht gelöst wurden.
- Eine neue Serviceanfrage, die noch nicht zugewiesen wurde.
- Eine Serviceanfrage, die zugewiesen wurde.
- Eine Serviceanfrage, die Sie erneut geöffnet haben.
- Eine zugewiesene, komplizierte Serviceanfrage.
- Serviceanfragen, für die Ihr Feedback vor dem nächsten Schritt erforderlich ist.
- Serviceanfragen, für die Sie kürzlich Informationen eingereicht haben.
- Eine Serviceanfrage, die abgeschlossen wurde.
- Alle Serviceanfragen im Konto.

3. Wählen Sie Erstellen aus.

Die Seite Serviceanfrage erstellen wird geöffnet.

4. Wählen Sie eine Kategorie aus.

Note

Wenn Sie die Funktionalität für Serviceanfragen testen möchten, fügen Sie dem Titel Ihrer Serviceanfrage das Kennzeichen „Keine Aktion“ hinzu `AMSTestNoOpsActionRequired`.

5. Geben Sie Informationen ein für:

- **Betreff:** Dadurch wird ein Link zu den Details der Serviceanfrage auf der Listenseite erstellt.
- **CC-E-Mails:** Diese E-Mails erhalten zusätzlich zu Ihren Standard-E-Mail-Kontakten Korrespondenz.
- **Einzelheiten:** Geben Sie hier so viele Informationen wie möglich an.

Um eine Anlage hinzuzufügen, wählen Sie Anlage hinzufügen, suchen Sie nach der gewünschten Anlage und klicken Sie auf Öffnen. Um den Anhang zu löschen, klicken Sie auf das Symbol Löschen:

6. Wählen Sie Absenden aus.

Es öffnet sich eine Detailseite mit Informationen zur Serviceanfrage — wie Typ, Betreff, Erstellt, ID und Status — sowie ein Korrespondenzbereich, der die Beschreibung der von Ihnen erstellten Anfrage enthält.

Darüber hinaus wird Ihre Serviceanfrage auf der Listenseite mit der Serviceanfrage angezeigt. Verwenden Sie diese Option, wenn Sie eine Warnung erhalten, aber noch nichts von AMS gehört haben.

Klicken Sie auf Antworten, um einen Korrespondenzbereich zu öffnen und zusätzliche Informationen oder Statusmeldungen bereitzustellen.

Klicken Sie auf „Fall lösen“, wenn die Serviceanfrage gelöst wurde.

Klicken Sie auf Mehr laden, um weitere Korrespondenzen anzuzeigen, die nicht auf die erste Seite passen.

Vergessen Sie nicht, die Kommunikation zu bewerten!

Für abrechnungsbezogene Anfragen erstellen Sie in der Support Center-Konsole einen Serviceanforderungsfall.

YouTube Video: [Wie und wann werden Serviceanfragen von der AWS-Konsole aus gestellt und was sind die Service Level-Ziele?](#)

Überwachung und Aktualisierung von Serviceanfragen in AMS

Sie können Vorfälleberichte und Serviceanfragen, die auch als Fälle bezeichnet werden, mithilfe der AMS-Konsole oder programmgesteuert mithilfe der API aktualisieren, überwachen und überprüfen. Support Informationen zur Verwendung der Support API finden Sie unter [DescribeCases](#)Bedienung.

Gehen Sie wie folgt vor, um einen Fall, einen Vorfall oder eine Serviceanfrage mithilfe der AMS-Konsole zu überwachen.

1. Suchen Sie im Dashboard „Vorfälleberichte“ oder „Serviceanfragen“ der AMS-Konsole nach einem Fall und wählen Sie den Betreff aus, um eine Detailseite mit dem aktuellen Status und den Korrespondenzen zu öffnen.

Wenn ein gemeldeter Vorfall oder eine Serviceanfrage vom AMS-Betriebsteam aktualisiert wird, erhalten Sie eine E-Mail und einen Link zu dem Vorfall in der AMS-Konsole, sodass Sie darauf antworten können. Sie können auf die Korrespondenz mit einem Vorfall nicht antworten, indem Sie auf die E-Mail antworten.

Important

Sie müssen eine E-Mail-Adresse eingegeben haben, um Benachrichtigungen über Statusänderungen im Zusammenhang mit einer Serviceanfrage oder einem Vorfall zu

erhalten. Benachrichtigungen werden nur an die E-Mail-Adresse gesendet, die dem Fall bei der Erstellung hinzugefügt wurde.

Der Link in der Benachrichtigungs-E-Mail funktioniert nur, wenn Sie einen E-Mail-Server in Ihrem AMS-Verbundnetzwerk verwenden. Sie können jedoch auf die Korrespondenz antworten, indem Sie Ihre AMS-Konsole aufrufen und die Seite mit den Falldetails verwenden.

2. Wenn die Liste viele Fälle enthält, können Sie die Option Filter verwenden:

- Alle geöffnet (Standard): Verwenden Sie diesen Filter, um alle Fälle zu sehen, die nicht gelöst wurden.
- Nicht zugewiesen: Verwenden Sie diese Option, wenn Sie den Fall gerade eingereicht haben und keine Benachrichtigung erhalten haben, dass sich der Status des Falls geändert hat. Hinweis: Vorfälle und Serviceanfragen werden je nach der eingereichten Priorität (Vorfälle) oder Ihrem Service Level Agreement (Serviceanfragen) unterschiedlich schnell bearbeitet.
- Öffnen: Verwenden Sie diese Option, wenn Sie die Benachrichtigung erhalten haben, dass es sich bei dem Fall um die Aktion „Ausstehend bei Amazon“ handelt. Dies bedeutet, dass der Fall zugewiesen wurde, die Bearbeitung jedoch noch nicht begonnen hat.
- Erneut geöffnet: Verwenden Sie diese Option, wenn Sie die Benachrichtigung erhalten haben, dass der Fall nach der Bearbeitung erneut geöffnet wurde.
- In Bearbeitung: Verwenden Sie diese Option, wenn Sie die Benachrichtigung erhalten haben, dass ein Mitarbeiter mit der Bearbeitung des Falls begonnen hat.
- Ausstehende Bearbeitung durch den Kunden: Verwenden Sie diese Option, wenn Sie von Ihrer Seite eine Aufforderung zum Tätigwerden erhalten haben.
- Kundenaktion abgeschlossen: Verwenden Sie diese Option, wenn Sie eine Benachrichtigung erhalten haben, dass Ihre Maßnahme in Bezug auf den Fall bearbeitet wurde.
- Gelöst: Dient zum Anzeigen von Fällen, von denen Sie wissen, dass sie gelöst wurden. Gelöste Fälle werden zwölf Monate lang in der Historie gespeichert.
- Beliebiger Status: Verwenden Sie diesen Filter, um alle Fälle unabhängig vom Status anzuzeigen.

3. Um den aktuellen Status zu überprüfen, aktualisieren Sie die Seite.

4. Wenn es so viele Korrespondenzen gibt, dass nicht alle auf der Seite angezeigt werden, wählen Sie „Mehr laden“.

5. Um den Status des Falls zu aktualisieren, wählen Sie Antworten, geben Sie die neue Korrespondenz ein und klicken Sie dann auf Absenden.

6. Um den Fall abzuschließen, nachdem er zu Ihrer Zufriedenheit gelöst wurde, wählen Sie Fall schließen.

Stellen Sie sicher, dass Sie den Service anhand der 1-5 Sterne bewerten, damit AMS weiß, wie es uns geht!

Beantwortung von AMS-generierten Serviceanfragen

Das AMS-Patchmanagement sendet Serviceanfragen (auch bekannt als Servicebenachrichtigung) vor dem von Ihnen festgelegten Wartungsfenster an Sie. Weitere Informationen finden Sie unter [AMS-Wartungsfenster](#). [AMS sendet Ihnen auch Servicemeldungen, wenn die Möglichkeit besteht, dass Ihre Infrastruktur durch einen AWS Service beeinträchtigt wird oder wenn eine EC2 Instanz in Ihrem Konto neu gestartet werden muss. Weitere Informationen finden Sie unter Dienstbenachrichtigungen.](#)

Note

AMS sendet Mitteilungen an die primäre E-Mail-Adresse Ihres AWS Kontos, die Sie angegeben haben. Wir empfehlen, einen alternativen Operations-Kontakt-E-Mail-Alias hinzuzufügen, um den Verwaltungsprozess für Serviceanfragen oder Servicebenachrichtigungen zu vereinfachen. Das Hinzufügen dieser E-Mails wird während des AMS-Onboarding-Prozesses und der zugehörigen Onboarding-Dokumentation behandelt.

Fragen zur Abrechnung

Gehen Sie wie folgt vor, um eine abrechnungsbezogene Frage einzureichen:

1. Öffnen Sie das [AWS -Support Center zu Hause #/](https://console.aws.amazon.com/support/). <https://console.aws.amazon.com/support/>
2. Wählen Sie Konto und Abrechnung.
3. Wählen Sie Create case (Fall erstellen) aus.
4. Wählen Sie Konto und Abrechnung aus und folgen Sie dann den Anweisungen, um Ihren Fall einzureichen.

Betrieb auf Abruf

Operations on Demand (OOD) ist eine Funktion von AWS Managed Services (AMS), die den Standardumfang Ihres AMS-Betriebsplans erweitert, indem sie Betriebsdienste bereitstellt, die derzeit nicht nativ in den [AMS-Betriebsplänen](#) oder AWS angeboten werden. Nach der Auswahl wird das Katalogangebot durch eine Kombination aus Automatisierung und hochqualifizierten AMS-Ressourcen bereitgestellt. Es gibt keine langfristigen Verpflichtungen oder zusätzlichen Verträge, sodass Sie Ihr bestehendes AMS sowie Ihre AWS Betriebsabläufe und Kapazitäten nach Bedarf erweitern können. Sie erklären sich damit einverstanden, monatliche Stundenblöcke (OOD-Blöcke), 20 Stunden pro Block, zu erwerben.

Sie können aus dem Katalog der standardisierten Angebote auswählen und über eine Serviceanfrage ein neues OOD-Engagement einleiten. Zu den OOD-Angeboten gehören beispielsweise die Unterstützung bei der Wartung von Amazon EKS, dem Betrieb und der AWS Control Tower Verwaltung von SAP-Clustern. Je nach Nachfrage und den am häufigsten auftretenden betrieblichen Anwendungsfällen werden regelmäßig neue Katalogangebote hinzugefügt.

OOD ist sowohl für die Betriebspläne AMS Advanced als auch für AMS Accelerate verfügbar und in allen Ländern verfügbar, in [AWS-Regionen](#) denen AMS verfügbar ist.

AMS führt das Kundensicherheitsrisikomanagement (CSRM) durch und implementiert gleichzeitig die von Ihnen gewünschten Änderungen. Weitere Informationen zum CSRM-Prozess finden Sie unter Sicherheitsüberprüfungen für [Änderungsanträge](#).

Angebotskatalog für Operations on Demand

Operations on Demand (OOD) bietet Ihnen die in der folgenden Tabelle beschriebenen Dienste.

Note

Definitionen der wichtigsten Begriffe finden Sie in der AWS Managed Services Services-Dokumentation [Wichtige Begriffe](#).

Betriebsplan	Titel	Beschreibung	Erwartete Ergebnisse

AMS Accelerate	Wartung des Amazon EKS-Clusters	AMS entlastet Ihre Container-Entwickler, indem es die laufende Wartung Ihrer Amazon Elastic Kubernetes Service (Amazon EKS) -Bereitstellungen übernimmt. AMS führt die zur Aktualisierung eines Clusters erforderlichen end-to-end Verfahren durch und adressiert dabei die Komponenten der Kontrollebene, der Add-Ons und der Knoten. AMS führt die Aktualisierung der verwalteten Knotentypen sowie eines kuratierten Satzes von Amazon EKS- und Kubernetes-Add-Ons durch.	Kundenteams halfen bei den zugrundeliegenden Betriebsarbeiten zur Aktualisierung von Amazon EKS-Clustern.

AMS Accelerate	AMI-Gebäude und Verkauf	AMS bietet seinen Kunden die laufende Verwaltung des Aufbaus und Verkaufs von AMI. Unsere Techniker führen monatliche Releases von abonnierten AMIs, On-Demand-Releases AMIs für neue Patch-Aktivitäten durch, verwalten Änderungen mithilfe von Runbooks und überwachen AMI-Builds mithilfe von Monitoring. CloudWatch Wir bieten auch Unterstützung bei der Fehlerbehebung und detaillierte Berichte für alle Benutzer, die in bestimmten Konten AMIs verwendet werden. Für dieses Angebot müssen AMI-Build-Pipelines über EC2 Image Builder bereitgestellt werden. AMS unterstützt keine anderen Automatisierungen oder Dienste, die mit EC2 Image Builder interagieren.	Die Sicherheitsslage der Kunden verbesserte sich und der Zeitaufwand der Kunden für Gebäude und Verkauf wurde AMIs reduziert.

AMS Accelerate	Kuratierte Ausführung von Änderungen	Arbeiten Sie mit unseren erfahrenen Betriebsingenieuren zusammen, um Ihre Geschäftsanforderungen in validierte Änderungsanforderungen umzusetzen, die sicher in Ihrer AWS Umgebung ausgeführt werden können. Nutzen Sie unseren einzigartigen Automatisierungsansatz und unser Wissen über bewährte betriebliche Verfahren (z. B. Folgenabschätzung, Rollbacks, Zwei-Personen-Regel), unabhängig davon, ob es sich um eine einfache Änderung im großen Maßstab oder um eine komplexe Maßnahme mit nachgelagerten Auswirkungen handelt.	Kunden helfen uns bei der Definition, Erstellung und Ausführung von individuellen Änderungsanforderungen. Änderungen können manuell oder automatisiert (CloudFormation, SSM) erfolgen. Beinhaltet bei Bedarf eine Beratung Support zur Konfiguration. Nicht für Änderungen am Anwendungscode, für die Installation/Bereitstellung von Anwendungen, für die Datenmigration oder für Änderungen der Betriebssystemkonfiguration vorgesehen.

AMS Accelerate	AWS Network Firewall Operationen	AMS arbeitet mit Ihnen zusammen, um Ihre Firewall zu integrieren und die Richtlinien und Regeln für den laufenden Firewall-Betrieb zu implementieren und zu verwalten. Zu diesem Zweck nutzen unsere Techniker unsere betrieblichen Best Practices und Automatisierung, um standardisierte Richtlinien und Regeln zu konfigurieren, und indem sie die Überwachung aktivieren, um Änderungen zu erkennen, die außerhalb des Automatisierungsprozesses vorgenommen wurden. AMS benachrichtigt Sie schnell über unerwünschte Änderungen und bietet Optionen, um diese auf Anfrage einzubeziehen oder das Konto auf eine frühere Konfiguration zurückzusetzen, um die Gesamtstabilität Ihrer Systeme zu gewährleisten.	Die Kundenteams helfen bei der Reduzierung des Verwaltungsaufwands, indem sie unbeabsichtigte Änderungen an der Netzwerk-Firewall schnell erkennen, was zu einer verbesserten Problembewertung und einer kürzeren Ursachanalyse sowohl für erwartete als auch für unerwartete Probleme führte.

AMS Accelerate	AWS Control Tower Betriebsabläufe	Kontinuierlicher Betrieb und Verwaltung Ihrer AWS Control Tower landing zone, einschließlich AWS Transit Gateway, und AWS Organizations Bereitstellung einer umfassenden Landezonenlösung. Wir kümmern uns um den Verkauf von Konten, das SCP- und OU-Management, die Behebung von Störungen, die SSO-Benutzerverwaltung und AWS Control Tower Upgrades mit unserer Bibliothek an benutzerdefinierten Steuerungen und Leitplanken.	Die Kundenteams helfen bei einigen der zugrunde liegenden Betriebsarbeiten wie Management AWS Control Tower, AWS Transit Gateway und AWS Organizations.

AMS Accelerate	AWS landing zone Beschleunigen Sie den Betrieb	AMS sorgt für den laufenden Betrieb der AWS Landezonen, die über den AWS Landing Zone Accelerator (LZA) eingerichtet wurden. Unsere Techniker kümmern sich um Änderungen an Konfigurationsdateien, das AWS Control Tower (CT) -Umgebungsmangement (Kontoverkauf, OU-Erstellung, CT-Guardrails), die Verwaltung der Service Control Policy (SCP), die Erkennung und Behebung von CT-Driften, das Netzwerkkonfigurationsmanagement sowie Updates für CT und das LZA-Framework. AWS LZA bietet die Möglichkeit, eine sichere AWS Umgebung mit mehreren Konten einzurichten und zu verwalten. Dabei kommen bewährte betriebliche Verfahren und Dienste zum Einsatz, wie z. AWS Control Tower	Die Kundenteams unterstützen den laufenden Betrieb und die Verwaltung der AWS Landing Zone Accelerator-Lösung.

AMS Accelerate	SAP-Cluster-Assistent	Dedizierte Alarmierung, Überwachung, Cluster-Patching, Sicherung und Behebung von Zwischenfällen für Ihre SAP-Cluster. Mit diesem Katalogelement können Sie Ihrem SAP-Betriebsteam einen Teil der laufenden operativen Arbeit abnehmen, sodass es sich auf das Kapazitätsmanagement und die Leistungsoptimierung konzentrieren kann.	SAP-Teams von Kunden oder Partnern haben uns bei einigen der zugrunde liegenden Betriebsarbeiten unterstützt. Der Kunde muss jedoch weitere SAP-Funktionen wie Kapazitätsmanagement, Leistungsoptimierung, DBA und SAP-Basisadministration bereitstellen.

AMS Accelerate	SQL Server im laufenden Betrieb EC2	AMS arbeitet mit Ihnen zusammen, um den laufenden Betrieb Ihrer auf EC2 Instances bereitgestellten SQL Server-Datenbanken zu integrieren, zu implementieren und zu verwalten. Unsere Techniker nutzen unsere betrieblichen Best Practices und Automatisierung, um Ihre Datenbankteams zu entlasten, indem sie Aufgaben wie Backup und Patching übernehmen, den AMS-Betriebssupport auf SQL Server-Patching ausweiten, um clusterfähige fortlaufende Updates, Sicherungs- und Wiederherstellungsservices im Einklang mit unserer Ransomware-Abwehrstrategie und die Überwachung der Einhaltung der vom Kunden bereitgestellten Sicherungs- und Patchkontrollen zu überwachen.	SQL Server-Kunden helfen beim Auslagern von Patching- und Backup-Datenbankoperationen, um die Ausfallsicherheit und den Sicherheitsstatus ihrer Workloads zu verbessern und zusätzlich die Lizenzkosten zu optimieren, indem sie ihre eigenen Lizenzen (BYOL) einführen EC2.

AMS Advanced	Wartung des Amazon EKS-Clusters	AMS entlastet Ihre Container-Entwickler, indem es sich um die laufende Wartung und Integrität Ihrer Amazon Elastic Kubernetes Service (Amazon EKS) -Bereitstellungen kümmert. AMS führt die zur Aktualisierung eines Clusters erforderlichen end-to-end Verfahren durch und adressiert dabei die Komponenten der Kontrollebene, der Add-Ons und der Knoten. AMS führt die Aktualisierung der verwalteten Knotentypen sowie eines kuratierten Satzes von Amazon EKS- und Kubernetes-Add-Ons durch.	Kundenteams helfen bei den zugrunde liegenden Betriebsarbeiten zur Aktualisierung von Amazon EKS-Clustern.
AMS für Fortgeschrittene	Vorrangige RFC-Ausführung	Eigene Kapazität eines AMS Operations Engineers, der die Ausführung Ihrer Änderungsanträge (RFC) priorisiert. Alle Einsendungen erhalten eine höhere Anzahl an Antworten, und die Prioritätsreihenfolge kann angepasst werden, indem Sie über einen Amazon Chime Chime-Besprechungsraum direkt mit den Technikern interagieren.	Kunden erhalten eine Antwort innerhalb von 8 Stunden für RFCs.

AMS Advanced und AMS Accelerate	Upgrade eines älteren Betriebssystems	Vermeiden Sie eine Instanzmigration, indem Sie Instanzen auf eine unterstützte Betriebssystemversion aktualisieren. Wir können ein direktes Upgrade für Ihre ausgewählten Instanzen durchführen und dabei die Automatisierungs- und Upgrade-Funktionen der Softwareanbieter nutzen (z. B. Microsoft Windows 2008 R2 auf Microsoft Windows 2012 R2). Dieser Ansatz ist ideal für ältere Anwendungen, die nicht einfach auf einer neuen Instanz neu installiert werden können, und bietet zusätzlichen Schutz vor bekannten und nicht abgemilderten Sicherheitsbedrohungen auf älteren Betriebssystemversionen. Die folgenden Betriebssysteme werden für direkte Upgrades unterstützt: • Microsoft Windows 2012 R2 auf Microsoft Windows 2016 und höher • Microsoft Windows 2016 bis Microsoft Windows 2022 und höher • Von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 • Von Red Hat Enterprise Linux 8 auf Red Hat Enterprise Linux 9 • Von Oracle Linux 7 auf Oracle Linux 8	Diese Lösung wird für Anwendungen bereitgestellt, die nicht mehr auf einer neuen Instance neu installiert werden können (z. B. verlorener Quellcode, ausgefallener ISV usw.). Sie können fehlgeschlagene Upgrades in ihren ursprünglichen Zustand zurückversetzen. Aus betrieblicher Sicht ist ein Rollback vorzuziehen, da dadurch die Instance in einen Zustand versetzt wird, der mit den neuesten Sicherheitspatches besser unterstützt werden kann.

Themen

- [AMS Operations on Demand anfordern](#)
- [Änderungen an den Operations on Demand-Angeboten vornehmen](#)

AMS Operations on Demand anfordern

AWS Managed Services (AMS) Operations on Demand (OOD) ist für alle verfügbar AWS-Konten , die bei AMS integriert wurden. Um Operations on Demand nutzen zu können, fordern Sie zusätzliche Informationen von Ihrem Cloud Service Delivery Manager (CSDM), Solutions Architect (SA), Account Manager oder Cloud Architect (CA) an. Die verfügbaren OOD-Angebote sind in der vorherigen Tabelle des [Operations on Demand-Angebotskatalogs](#) aufgeführt. Reichen Sie nach Abschluss des Auftragsumfangs eine Serviceanfrage an AMS Operations ein, um einen Auftrag für OOD einzuleiten.

Jede OOD-Serviceanfrage muss die folgenden detaillierten Informationen zum Auftrag enthalten:

- Die angeforderten spezifischen OOD-Angebote und für jedes spezifische OOD-Angebot:
 - Die Anzahl der Blöcke (ein Block entspricht 20 Stunden Betriebsressourcenzeit in einem bestimmten Kalendermonat, die zum jeweils aktuellen Standardtarif für AWS das jeweilige Operations on Demand-Angebot berechnet werden), die dem jeweiligen OOD-Angebot zugewiesen werden sollen.
 - Die Konto-ID für jedes AWS Managed Services Services-Konto, für das das spezifische OOD-Angebot angefordert wird.

OOD-Serviceanfragen müssen von Ihnen über einen der folgenden Kanäle eingereicht werden:

- Das AWS Managed Services Services-Konto, das die entsprechenden Operations on Demand-Angebote erhält, oder
- Ein AWS Managed Services Services-Konto, bei dem es sich um ein AWS Organizations Verwaltungskonto im Modus mit allen Funktionen handelt, und zwar im Namen aller Mitgliedskonten, bei denen es sich um AWS Managed Services Services-Konten handelt.

Nach Eingang der OOD-Serviceanfrage überprüft AMS Operations die Konten und aktualisiert sie mit deren Genehmigung, teilweiser Genehmigung oder Ablehnung.

Sobald die Serviceanfrage für das OOD-Angebot genehmigt wurde, stimmen sich AMS und Sie ab, um mit dem Auftrag zu beginnen. Es werden keine OOD-Angebote initiiert, bis die Serviceanfrage genehmigt und ein Startdatum für den Auftrag vereinbart wurde.

AMS verwendet eine monatliche Abonnementzuweisung von OOD-Blöcken. Wir weisen die genehmigte Anzahl von Blöcken monatlich zu, beginnend mit dem Startdatum des Engagements, bis Sie mit einer neuen Serviceanfrage die Abmeldung beantragen. OOD-Blöcke sind für einen Kalendermonat gültig. Ungenutzte Blöcke oder Blockteile werden nicht auf future Monate übertragen oder übertragen.

Ihnen wird jeden Monat mindestens ein OOD-Block in Rechnung gestellt, unabhängig von der Anzahl der tatsächlich genutzten Stunden. Jeder zusätzliche zugewiesene OOD-Block, für den keine Stunden genutzt wurden, wird nicht in Rechnung gestellt.

Änderungen an den Operations on Demand-Angeboten vornehmen

Um Änderungen an laufenden Aufträgen für Operations on Demand (OOD) -Angebote zu beantragen, reichen Sie eine Serviceanfrage ein, die folgende Informationen enthält:

- Die angeforderte (n) Änderung (en) und
- Das Datum, an dem die Änderungen in Kraft treten sollen.

Nach Erhalt der OOD-Serviceanfrage prüft AMS Operations die Anfrage und gibt entweder deren Zustimmung oder bittet den zuständigen CSDM, gemeinsam mit Ihnen den Umfang und die Auswirkungen der Änderung zu ermitteln. Wenn festgestellt wird, dass für die Änderung eine Überprüfung des Umfangs mit dem CSDM erforderlich ist, müssen Sie eine zweite OOD-Serviceanfrage einreichen, um den geänderten Auftrag nach Abschluss der Scoping-Maßnahme einzuleiten.

Nach der Genehmigung wird und bleibt die zuletzt geänderte Blockzuweisung aktiv und ersetzt alle vorherigen Blockzuweisungen, sofern mit Ihnen nichts anderes vereinbart wurde. AWS

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen in den einzelnen Versionen des AMS Advanced User Guide beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

- API-Version: 2019-05-21
- Neu oder aktualisiert CTs und exemplarische Vorgehensweisen: Verlauf des Referenzdokuments vom Typ [AMS Advanced Change Type](#).
- Neues AMS AMIs: [AMS Amazon-Maschinenbilder \(AMIs\)](#)

Änderung	Beschreibung	Datum
Die Tabelle für AWS Identity and Access Management (IAM) im Abschnitt Standards teurelemente in AMS Advanced wurde aktualisiert	Die Informationen in der Tabelle zu den IAM-Richtlinien und dem Zugriff auf Amazon S3 S3-Buckets wurden aktualisiert.	25. September 2025
Der Schritt für abrechnungsbezogene Anfragen wurde aktualisiert	Der Schritt zum Erstellen von Serviceanfragen für abrechnungsbezogene Anfragen wurde im Abschnitt Serviceanfrage in AMS erstellen aktualisiert.	25. September 2025
Die Informationen für E-Mail-Benachrichtigungen für Änderungstypen wurden aktualisiert	Die Informationen und das Beispiel für das Hinzufügen von E-Mail-Benachrichtigungen für Änderungstypen wurden im Abschnitt RFC-E-Mail-Benachrichtigungen konfigurieren (Konsole) aktualisiert.	25. September 2025
Der Änderungstyp wurde aktualisiert	Der Abschnitt zur automatischen Kennzeichnung der	25. September 2025

AMS-Infrastruktur wurde mit dem Änderungstyp für das Taggen von AMS-Ressourcen aktualisiert.

[Häufig gestellte Fragen zu aktualisierten virtuellen Maschinen Import/Export in AWS Managed Services](#)

Der RFC, mit dem ein Instanzprofil angefordert wurde, wurde aktualisiert, damit Tools Befehle von der Instanz aus ausführen können.

24. September 2025

[Aktualisierter Request for Change \(RFC\) für den Start einer SUSE Linux Enterprise Server for SAP Applications SP6 15-Instanz SP6](#)

Schritt 2 unter So starten Sie eine neue SUSE Linux Enterprise Server for SAP Applications SP6 15-Instanz mit dem richtigen RFC aktualisiert.

22. September 2025

[Aktualisierter Änderungsantrag \(RFC\)](#)

Der Abschnitt mit häufig gestellten Fragen zu AWS Managed Services wurde mit dem richtigen RFC aktualisiert AWS Elastic Disaster Recovery , um die erforderlichen IAM-Rollen in Ihrem Konto zu erstellen.

22. September 2025

[Es wurden 4 neue Trusted Advisor Kostenoptimierungsprüfungen hinzugefügt, die von Trusted Remediator unterstützt werden](#)

Die folgenden Kostenoptimierungsprüfungen wurden hinzugefügt:

- c1z7kmr00n — Amazon-Empfehlungen zur Kostenoptimierung für Instances EC2
- c1z7kmr02n — Empfehlungen zur Amazon EBS-Kostenoptimierung für Volumen
- c1z7kmr03n — Empfehlungen zur Amazon RDS-Kostenoptimierung für DB-Instances
- c1z7kmr05n — Empfehlungen zur Kostenoptimierung für Funktionen AWS Lambda

22. September 2025

[Der Hinweis für Availability Zones wurde aktualisiert \(AZs\)](#)

Die Informationen zu Sicherheitsgruppen in AMS wurden aktualisiert.

5. September 2025

[Der Änderungstyp wurde aktualisiert](#)

Der Abschnitt mit häufig gestellten Fragen zu Amazon FSx in AWS Managed Services wurde aktualisiert und der Typ wurde geändert, um das Managed AD für das Anwendungskonto freizugeben.

5. September 2025

Der Änderungstyp wurde
aktualisiert

Der Abschnitt mit häufig gestellten Fragen zu Amazon DocumentDB in AWS Managed Services wurde aktualisiert und enthält nun die Option „Löschen APIs“.

5. September 2025

Der Änderungstyp wurde
aktualisiert

Der Abschnitt mit häufig gestellten Fragen zu Alexa for Business in AWS Managed Services wurde aktualisiert. Der Typ wurde für die Installation und den Betrieb Ihres Alexa for Business-Gateways auf zwei IAM-Benutzer mit beschränktem Zugriff geändert.

5. September 2025

Der Änderungstyp wurde
aktualisiert

AppStream Version 2.0 im Abschnitt mit häufig gestellten Fragen zu AWS Managed Services wurde aktualisiert. Hier können Sie den Typ ändern, um eine IAM-Rolle zu erstellen und auszuwählen, die auf allen Flottenstreaming-Instances verfügbar sein wird

5. September 2025

Der Änderungstyp wurde aktualisiert

Der Abschnitt mit häufig gestellten Fragen zu AWS Managed Services wurde aktualisiert EventBridge und enthält nun den Änderungstyp, um eine EventBridge Servicерolle anzufordern, bevor EventBridge sie zum Auslösen anderer AWS Ressourcen verwendet wird.

5. September 2025

Die Unterstützung Trusted Advisor für Sicherheitschecks wurde durch Trusted Remediator aktualisiert

Die unterstützten vorkonfigurierten Parameter und Einschränkungen für die Prüfung Hs4Ma3G108 aktualisiert — CloudTrail Trails sollten in Amazon Logs integriert werden CloudWatch

5. September 2025

Die Unterstützung Trusted Advisor für Sicherheitschecks wurde durch Trusted Remediator aktualisiert

Die Trusted Advisor Sicherheitsüberprüfung wurde aktualisiert, sodass Version 2 von Hs4Ma3G184 hinzugefügt wurde. Die Protokollierung von Application Load Balancern und Classic Load Balancern sollte aktiviert sein

5. September 2025

Aktualisierte Prüfungen der Trusted Advisor betrieblichen Exzellenz, unterstützt durch den Bereich Trusted Remediator

Der Abschnitt „Trusted Advisor Operational Excellence Checks, die von Trusted Remediator unterstützt werden“ wurde aktualisiert und um die neue unterstützte Prüfung c1fd6b96l4 Amazon S3 Access Logs Enabled hinzugefügt.

28. August 2025

<u>Der Änderungstyp wurde aktualisiert</u>	Ändern Sie den Typ für die benutzerdefinierte IAM-Rolle.	25. August 2025
<u>Der Abschnitt „Using CloudWatch Application Insights for .Net“ und „SQL Server“ im AMS-Bereich wurde aktualisiert</u>	Der Änderungstyp wurde für die Verwendung von CloudWatch Application Insights überarbeitet.	25. August 2025
<u>Aktualisierter Änderungsantrag (RFC)</u>	Änderungsanforderung (RFC) zum Hinzufügen weiterer Tags zum Amazon S3 S3-Bucket.	25. August 2025
<u>Aktualisierter Änderungsantrag (RFC)</u>	Änderungsantrag (RFC) zur Kennzeichnung aller Ressourcen, die von AMS zu Verwaltungszwecken erstellt wurden.	25. August 2025
<u>Der Abschnitt mit häufig gestellten Fragen zu Lambda im AWS Managed Services wurde aktualisiert</u>	Überarbeiteter Änderungstyp für den Zugriff auf andere AWS Services zur Erstellung von Ereignisquellen.	25. August 2025
<u>Der Abschnitt mit häufig gestellten Fragen zu Lambda im AWS Managed Services wurde aktualisiert</u>	Überarbeiteter Änderungstyp zur Bereitstellung von Lambda-Funktionen.	25. August 2025
<u>Der Abschnitt Sicherheitsgruppen erstellen, ändern oder löschen wurde aktualisiert</u>	Der Änderungstyp wurde überarbeitet, um eine Sicherheitsgruppe außerhalb von Stacks und VPCs zu erstellen.	25. August 2025

[Der Bereich Trusted Remediator wurde aktualisiert und enthält nun neue Inhalte für Compute Optimizer](#)

Der Abschnitt Trusted Remediator wurde aktualisiert und enthält nun neue Inhalte für unterstützte Empfehlungen. AWS Compute Optimizer

18. August 2025

[Der Link zum TOC-Glossar wurde entfernt](#)

[AWS Glossar.](#)

8. August 2025

[Präzise Empfehlung für die Art der Änderung](#)

Um Ihre Kundenmetrik in Ihr Anwendungsüberwachungssystem zu integrieren, bitten Sie AMS, ein Amazon SNS SNS-Thema für die Metrik zu erstellen, indem Sie einen RFC mit Deployment | Monitoring and Notification | SNS | Create CT (ct-3dfnglm4ombbs) einreichen.

8. August 2025

[Präzise Empfehlung für die Art der Änderung](#)

Um Platzhalter-Instance-Volumes zu löschen, reichen Sie Folgendes ein: Management | Advanced Stack Components | EBS-Volume | Änderungstyp löschen (ct-3e3h8u0sp5z80).

8. August 2025

[Neue SecureChannelFailure Überwachungswarnungen: und Broken Secure Channel](#)

[Automatische Behebung von Warnmeldungen aus der Basisüberwachung in AMS AMS.](#)

8. August 2025

Neue Trusted Remediator-Prüfungen	Trusted Advisor Kostenoptimierungsprüfungen werden durch Trusted Trusted Advisor Remediator-Sicherheitsprüfungen unterstützt, die von Trusted Remediator r AWSManagedServices-TerminateEC Hs4Ma3G120—2, Hs4Ma3G230—2 und c18d2gz150—2 InstanceStoppedForPeriodOfTime unterstützt werden. AWSManagedServices-TrustedRemediator EnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	8. August 2025
Aktualisierung des IAM-Standards in Punkt 3.2	Der Wortlaut wurde geklärt und die Erwähnung von Tagging gestrichen.	25 Juli 2025
Aktualisierung der Optionen zur Deaktivierung von Alarmen	Wenn Sie ein Tag hinzufügen, können Sie sich von zwei weiteren Benachrichtigungen abmelden.	25 Juli 2025
Der Self-Service Provisioning Service ist veraltet	Der CloudEndure Self-Service Provisioning Service wurde zugunsten von eingestellt. AWS Application Migration Service	25 Juli 2025
Neue Funktion für Backups	Passen Sie Benachrichtigungen in Backup-Tresoren mit einem neuen Tag an.	25 Juli 2025

<u>Die Tabelle der Steuerelemente wurde aktualisiert</u>	Einige doppelte Steuerelemente im Tabellenabschnitt AMS-STD-002 - AWS Identity and Access Management (IAM) wurden entfernt.	26. Juni 2025
<u>Die Voraussetzungen für den SSP-Dienst AWS Transfer Family wurden aktualisiert</u>	Dem Abschnitt mit den Voraussetzungen wurden Informationen hinzugefügt.	26. Juni 2025
<u>Beispiel für eine aktualisierte IAM-Richtlinie</u>	Aktualisiertes Beispiel für eine IAM-Richtlinie mit mehr Einschränkungen, wie empfohlen.	26. Juni 2025
<u>Aktualisiertes AMI wird unterstützt OSES</u>	Ubuntu Linux 24.04 wurde unter Ubuntu Linux 22.04 hinzugefügt und alle Verweise auf geändert. SP5 SP6	26. Juni 2025
<u>Self-Service-Bereitstellungsdienst, veraltet MediaStore</u>	Veraltungshinweis für hinzugefügt. AWS Elemental MediaStore	26. Juni 2025
<u>Self-Service-Bereitstellungsservice, Amazon Inspector Classic ist veraltet</u>	Veraltungshinweis für Amazon Inspector Classic hinzugefügt.	26. Juni 2025
<u>Self-Service-Bereitstellungsservice, Amazon Connect ist veraltet</u>	Veraltungshinweis für Amazon Connect hinzugefügt.	26. Juni 2025
<u>Der Abschnitt für unterstützte Konfigurationen in AMS wurde aktualisiert</u>	Die unterstützten Konfigurationen für unterstützte Betriebssysteme und Betriebssysteme mit unterstütztem Ende des Support (EOS) in AMS wurden aktualisiert.	25. Juni 2025

Self-Service-Bereitstellungsdienst, veraltet WorkDocs	Seite und Verweise auf „veraltet“ wurden entfernt. WorkDocs	19. Juni 2025
Patch-Management: Wichtiger Sicherheitshinweis für alternative Patch-Repositorys	Wichtiger Sicherheitshinweis und bewährte Methoden für die Verwendung alternativer Patch-Repositorys in AMS.	10. Juni 2025
Unterstützte Betriebssystem-Updates	Von AMS Advanced unterstützte Betriebssysteme wurden aktualisiert, einige hinzugefügt, andere entfernt.	22. Mai 2025
Nur intern APIs	Nur intern, die in einigen APIs Protokollen vorkommen. CloudWatch	22. Mai 2025
Aktualisierungen für AMS Trusted Remediator	Wie verwendet man einen neuen Parameter, <code>preconfigured-parameters</code> , um Trusted Advisor Prüfungen in Trusted Remediator anzupassen.	22. Mai 2025
Aktualisierungen der SSP Amazon Elastic Container Registry	Weitere Rollen werden automatisch bereitgestellt, wenn Sie den Amazon ECR-Service einbinden.	8. Mai 2025

Häufig gestellte Fragen und Updates zu AMS Advanced Trusted Remediator.

Verschiedene Aktualisierungen der unterstützten Trusted Advisor Prüfungen , häufig gestellte Fragen zu Trusted Remediator (hinzugefügt „Welche Ressourcen stellt Trusted Remediator für Ihre Konten bereit?“) und mehr. Siehe auch [Trusted Advisor Prüfungen, die von Trusted Remediator unterstützt werden.](#)

8. Mai 2025

Aktualisierung der AMS Advanced Standard-Sicherheitskontrollen.

Es wurden Steuerelemente für die gemeinsame Nutzung von Sicherheitsgruppen hinzugefügt.

8. Mai 2025

Geschützte Namespaces von AMS Advanced.

AMS hat EPSMarket placeSubscriptionRole Namespaces geschützt und hinzugefügt. EPS

24. April 2025

Speicherorte für AMS Advanced-Protokolle.

Zusätzliche Protokollspeicherorte hinzugefügt.

24. April 2025

Aktualisierung der Voraussetzungen für den AMS Advanced Self-Service Provisioning-Modus für AppStream Version 2.0

Eine Voraussetzung für AppStream 2.0 wurde hinzugefügt: Sie müssen einen Amazon S3 S3-Bucket -Namen angeben, wenn Sie den Bereitstellungs-RFC für den Service einreichen.

24. April 2025

<u>AMS Advanced Neue Amazon RDS-Warnung zur automatischen Problembehebung.</u>	Warn-ID: - 0224, wird ausgelöst, wenn der angeforderte zugewiesene Speicherplatz den konfigurierten maximalen Speicherschwellenwert erreicht oder überschreitet.	27. März 2025
<u>AMS Advanced AWS hat den Neukundenzugang zu Amazon CloudSearch mit Wirkung zum 25. Juli 2024 geschlossen.</u>	Bestandskunden können den Service weiterhin nutzen, es wird jedoch keine neuen Funktionen geben.	27. März 2025
<u>AMS Advanced AWS hat den Zugang für Neukunden mit Wirkung zum AWS CodeCommit 25. Juli 2024 geschlossen.</u>	Bestandskunden können den Service weiterhin nutzen, es wird jedoch keine neuen Funktionen geben.	27. März 2025
<u>Trusted Remediator ist jetzt verfügbar.</u>	Trusted Remediator, eine AWS Managed Services Services-Lösung, die die Behebung von AWS Trusted Advisor Prüfungen automatisiert, ist jetzt verfügbar.	19. März 2025
<u>AMS Advanced Neue RDS-Warnung für automatische Korrekturen.</u>	RDS-EVENT-0224 hinzugefügt.	17. März 2025
<u>AMS Advanced Neue Funktion: Benachrichtigungen bei Vorfällen.</u>	Sie können AppRegistry damit Anwendungen erstellen und die Benachrichtigungen zu Vorfällen für diese Anwendungen anpassen.	13. März 2025

[AMS-Update zum Schwellenwert für die RDS-Alarmüberwachung.](#)

Der Alarmschwellenwert für die durchschnittliche RDS-CPU-Auslastung wurde von 75 auf 90% geändert.

20. Februar 2025

[Aktualisierte Self-Service-Berichte mit neuen Datenoptionen für die Anzeige aggregierter Berichte](#)

Trusted AWS Organization account enabled by the customerFür die folgenden Self-Service-Berichte wurden die neuen Datenoptionen „Feldname:“Admin Account ID, „Datensatz-Feldname:“**aws_admin_account_id** und „Definition:“ hinzugefügt:

28. Januar 2025

- Patch-Bericht (täglich)
- Backup-Bericht (täglich)
- Vorfallbericht (wöchentlich)

[Update zum AWS Batch SSP](#)

Sie können den folgenden RFC für die Bereitstellung AWS Batch in Ihrem AMS-Konto verwenden: Management | AWS-Service | Self-Provisioned Service | Add (ct-1w8z66n899dct).

28. Januar 2025

[Neue AMS-Funktion: Aggregierte Self-Service-Berichte](#)

Aggregierte Self-Service-Berichte (SSR) bieten Ihnen einen Überblick über bestehende Self-Service-Berichte, die auf Organisationsebene kontenübergreifend aggregiert wurden.

21. Januar 2025

[Aktualisierung des Abschnitts
Forecast SSP](#)

Hinweis hinzugefügt: AWS hat den Zugang für Neukunden zu Amazon Forecast mit Wirkung zum 29. Juli 2024 geschlossen. Bestandskunden von Amazon Forecast können den Service weiterhin wie gewohnt nutzen.

10. Januar 2025

[Aktualisierung des Abschnitts mit AMS-geschützten
Namespaces](#)

Ein fehlender geschützter Namespace (*mc, *MC und *Mc) wurde zur Liste der AMS-geschützten Namespaces hinzugefügt.

9. Januar 2025

[Update zum Abschnitt So
funktioniert die Überwachung](#)

Es wurden Informationen zu einer neuen Funktion hinzugefügt, mit der Warnmeldungen nach Ressourcen oder Instanz-ID statt nach Vorfall konfiguriert werden.

8. Januar 2025

[Aktualisiert: Tag-basierter
Update-Inhalt](#)

Ein Tippfehler im Schlüsselnamen wurde behoben und der falsche Pfad zur Konfigurationsdatei korrigiert.

6. Januar 2025

[Aktualisiert: AMS AMI Notes](#)

Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.

21. November 2024

[Die Tabelle mit den Operations On Demand-Angeboten wurde aktualisiert](#)

Die folgenden Betriebssysteme werden für direkte Upgrades unterstützt:

11. November 2024

- Microsoft Windows 2016 bis Microsoft Windows 2022 und höher

[Die Tabelle mit den Operations On Demand-Angeboten wurde aktualisiert](#)

Die folgenden Betriebssysteme werden für direkte Upgrades unterstützt:

1. November 2024

- Microsoft Windows 2012 R2 auf Microsoft Windows 2016 und höher
- Von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8
- Von Red Hat Enterprise Linux 8 auf Red Hat Enterprise Linux 9
- Von Oracle Linux 7 auf Oracle Linux 8

[Unterstützte Konfigurationen wurden aktualisiert](#)

Die unterstützten Oracle Linux-Betriebssysteme wurden auf 9.0-9.3, 8.0-8.9, 7.5-7.9 aktualisiert.

24. Oktober 2024

Aktualisierte AMS Amazon Machine Images (AMIs)

Windows-basiert aktualisiert, AMIs um Windows 2012 und 2012 R2 zu entfernen. Die Linux-Version wurde aktualisiert AMIs , um mehrere AMIS zu entfernen, die nicht mehr unterstützt werden, und um Folgendes hinzuzufügen:

24. Oktober 2024

- Amazon Linux (2ARM64)
- RHEL 9
- SUSE Linux Enterprise Server 15 SP5

Sie können jetzt mehrere E-Mail-Adressen in tagbasierte Benachrichtigungen aufnehmen.

In tagbasierten Benachrichtigungen werden jetzt mehrere E-Mail-Adressen unterstützt.

20. September 2024

Abschnitt „Sicherheitsüberprüfungen“ für Änderungsanfragen hinzugefügt.

Es wurde ein neuer Abschnitt hinzugefügt, der Einzelheiten zur Sicherheitsüberprüfung von Änderungsanträgen enthält.

17. September 2024

Ein neuer Abschnitt wurde hinzugefügt.

Ein neuer Abschnitt, in dem beschrieben wird, wie Sicherheitsüberprüfungen von Änderungsanträgen in AMS Advanced durchgeführt werden, ist jetzt verfügbar.

12. September 2024

Neuer Service, der von AMS Advanced unterstützt wird.

AWS Resilience Hub wird jetzt von AMS Advanced unterstützt.

30. August 2024

[Neue Dienste, die von AMS Advanced unterstützt werden.](#)

Fünf neue Dienste werden jetzt von AMS Advanced unterstützt:

21. August 2024

- Amazon Bedrock
- Amazon Kendra
- Amazon Quantum Ledger Database (Amazon QLDB)
- AWS Service Catalog AppRegistry
- Amazon Managed Service für Prometheus

[Eine neue Netzwerkstandardkonfiguration für Endpoint Security ist jetzt verfügbar.](#)

Die Update-Quelle ist jetzt in den EPS-Standardnetzwerkeinstellungen enthalten.

21. August 2024

[Aktualisiert: AMS AMI Notes](#)

Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.

30. Juli 2024

[AMS unterstützt jetzt Amazon Route 53 Resolver DNS Firewall.](#)

AMS unterstützt jetzt Amazon Route 53 Resolver DNS Firewall

30. Juli 2024

[AWS DataSync SSPS-Aktualisierung](#)

AWS DataSync benötigt nicht mehr das Präfix „datasync-“ für Amazon S3 S3-Bucket-Namen.

30. Juli 2024

[Dashboard mit Regeln für Sicherheitskonfigurationen](#)

Das Security Config Rules Dashboard ist jetzt in der Self-Service-Berichterstattung verfügbar.

24. Juli 2024

<u>AMS unterstützt jetzt Oracle Linux 8.9, RHEL 8.10 und RHEL 9.4.</u>	AMS unterstützt jetzt Oracle Linux 8.9, RHEL 8.10 und RHEL 9.4.	5. Juli 2024
<u>Amazon Bedrock ist jetzt im Self-Service-Bereitstellung smodus verfügbar</u>	Sie können Amazon Bedrock jetzt im AMS SSP-Modus anfordern.	27. Juni 2024
<u>DNS-Firewall-Ereignisse mit Amazon Route 53 Resolver in der Reaktion auf Sicherheitsvorfälle</u>	AMS überwacht jetzt DNS-Firewall-Ereignisse von Amazon Route 53 Resolver in Security Incident Response	21. Juni 2024
<u>Es wurden zusätzliche Informationen zur Aktivierung der AMS-Funktion „Bring Your Own EPS“ (BYOEPS) hinzugefügt.</u>	Es wurden zusätzliche Informationen zur Aktivierung der AMS-Funktion „Bring Your Own EPS“ (BYOEPS) hinzugefügt.	5. Juni 2024
<u>Aktualisiert: AMS AMI Notes</u>	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	23. Mai 2024
<u>Informationen zur Verwendung einer benutzerdefinierten Rolle AWS Amplify im Self-Service-Bereitstellungsmodus hinzugefügt (nur MALZ-Umgebungen).</u>	Es wurden Anweisungen hinzugefügt, wie MALZ-Umgebungen eine benutzerdefinierte Rolle AWS Amplify im Self-Service-Bereitstellungsmodus verwenden können.	23. Mai 2024
<u>Amazon Kendra ist jetzt im Self-Service-Bereitstellung smodus verfügbar.</u>	Amazon Kendra ist jetzt im Self-Service-Bereitstellung smodus verfügbar.	23. Mai 2024

<u>AMS Advanced unterstützt zusätzliche Betriebssysteme.</u>	AMS Advanced unterstützt Red Hat Enterprise Linux (RHEL) 9.x und Ubuntu 20.04 und 22.04.	25. April 2024
<u>AMS Advanced unterstützt die ARM64 Architektur für Amazon Linux 2.</u>	AMS Advanced unterstützt die ARM64 Architektur für Amazon Linux 2.	25. April 2024
<u>Der Bereich Offboard für Landingzone-Konten mit mehreren Konten (MALZ) wurde aktualisiert.</u>	Es wurden detaillierte Informationen zum Offboarding von Anwendungs- und Core-Konten aus der landing zone für mehrere Konten hinzugefügt.	11. April 2024
<u>Aktualisiert: Beschreibung der Verwaltung von Serviceanfragen.</u>	Die Beschreibung der Verwaltung von Serviceanfragen wurde im Thema Servicebeschreibung aktualisiert.	21. März 2024
<u>Aktualisiert: Abschnitt „Serviceverpflichtungen für das Incident-Management“.</u>	Es wurde ein Link zum AMS Service Level Agreement hinzugefügt.	21. März 2024
<u>Aktualisiert: Abschnitt „So funktioniert die Verwaltung von Serviceanfragen“.</u>	Es wurde klargestellt, wie AMS mit Serviceanfragen umgeht, die eine Funktionsanfrage oder einen Fehler enthalten.	21. März 2024
<u>Aktualisiert: Holen Sie sich den Support-Bereich.</u>	Der Bereich „Support anfordern“ wurde aktualisiert und enthält nun einen neuen Abschnitt mit Fragen zur Rechnungsstellung.	21. März 2024

Aktualisiert: Automatisierte IAM-Bereitstellung von AMS	Automatisiertes AMS IAM-Provisioning mit Informationen zur benutzerdefinierten Sperrliste aktualisiert	21. März 2024

Frühere Aktualisierungen

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation des AMS Advanced-Handbuchs vor März 2024 beschrieben.

Änderungen	Beschreibung	Link
Februar 2024		
Unterstützte Betriebssysteme wurden aktualisiert	Die unterstützten Betriebssysteme wurden um SUSE Linux Enterprise Server 15 SP5 aktualisiert.	Siehe Unterstützte Konfigurationen
Hinweis zu Warnmeldungen aus der Basisüberwachung in AMS hinzugefügt.	Es wurde ein Hinweis hinzugefügt, der darauf hinweist, dass der Alarm für die Nutzung von Volumes EC2 ohne Root-Rechte standardmäßig deaktiviert ist.	Siehe Warnmeldungen aus der Basisüberwachung in AMS
Ein neuer Abschnitt AMS Event Router wurde zur Überwachung und Ereignisverwaltung hinzugefügt.	Es wurde ein neuer Abschnitt hinzugefügt, der den AMS Advanced Event Router behandelt.	Siehe Verwenden von Amazon EventBridge Managed Rules in AMS
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	Siehe AMIs. csv-and-notes.02.2024

Änderungen	Beschreibung	Link
Februar 2024		
Ein neuer Abschnitt für die Rolle, die mit dem Amazon EventBridge Rule Service verknüpft ist, für AMS Advanced hinzugefügt	Im Abschnitt Infrastruktursicherheit wurde ein neuer Abschnitt für die Rolle „Amazon EventBridge Rule Service“ für AMS Advanced hinzugefügt.	Siehe Rolle im Zusammenhang mit dem Amazon EventBridge Rule Service für AMS Advanced
Der Abschnitt Self-Servicing-Bereitstellungsmodus wurde aktualisiert	Ein neuer Abschnitt für den neuen Amazon Inspector im Self Servicing Provision Mode wurde hinzugefügt.	Siehe Amazon Inspector Classic (AMS SSPS)
Januar 2024		
Der Abschnitt zur Verwaltung geplanter Ereignisse (PEM) wurde aktualisiert	Zusätzliche Informationen und eine häufig gestellte Frage zum Management von geplanten Ereignissen (PEM) wurden hinzugefügt.	Siehe Verwaltung geplanter Ereignisse in AWS Managed Services
Ein neuer Abschnitt für die auto Installation des SSM-Agenten wurde hinzugefügt	In der automatisierten EC2 Instanzkonfiguration wurde ein neuer Abschnitt für die auto Installation des SSM-Agenten hinzugefügt.	Siehe Automatische Installation des SSM-Agenten
Hinzugefügt AWS Resilience Hub (AMS SSPS)	Ein neuer SSPS-Dienst wurde hinzugefügt.	Siehe Verwenden Sie AMS SSP zur Bereitstellung AWS Resilience Hub in Ihrem AMS-Konto

Änderungen	Beschreibung	Link
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	Siehe AMIs. csv-and-notes.01.2024
Dezember 2023		
Der Direct Change-Modus in AMS wurde aktualisiert	Dem Direct Change-Modus in AMS wurde ein neuer Unterabschnitt, Anwendungsfälle im Direct Change-Modus, hinzugefügt.	Siehe Direkter Änderungsmodus in AMS
Aktualisiert AWS Amplify (AMS SSPS)	Die häufig gestellten Fragen wurden aktualisiert, um klarzustellen, dass für die Beantragung von Amplify eine Risikoakzeptanz erforderlich ist.	Siehe Verwenden Sie AMS SSP zur Bereitstellung AWS Amplify in Ihrem AMS-Konto
Neu AWS Elastic Disaster Recovery (AMS SSPS)	Ein neuer SSPS-Dienst wurde hinzugefügt	Siehe Verwenden Sie AMS SSP zur Bereitstellung AWS Elastic Disaster Recovery in Ihrem AMS-Konto
Neuer Amazon Managed Service für Prometheus (AMS SSPS)	Ein neuer SSPS-Service wurde hinzugefügt	Siehe Verwenden Sie AMS SSP, um Amazon Managed Service für Prometheus in Ihrem AMS-Konto bereitzustellen
Der Abschnitt „Funktionsweise des Kontinuitätsmanagements“ wurde aktualisiert.	Ein neuer Unterabschnitt, AMS-Backup-Überwachung und Berichterstattung, wurde hinzugefügt.	Siehe So funktioniert Kontinuitätsmanagement

Änderungen	Beschreibung	Link
Neuer Amazon DevOps Guru (AMS SSPS)	Ein neuer SSPS-Service wurde hinzugefügt	Siehe Verwenden Sie AMS SSP, um Amazon DocumentDB (mit MongoDB-Kompatibilität) in Ihrem AMS-Konto bereitzustellen
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	Siehe AMIs. csv-and-notes1.12.2023
November 2023		
Amazon CloudWatch Synthetics (AMS SSPS) wurde aktualisiert	Es wurde aktualisiert FAQs und verwendet nun die richtigen Rollennamen.	Siehe Verwenden Sie AMS SSP, um Amazon CloudWatch Synthetics in Ihrem AMS-Konto bereitzustellen
Aktualisierter Self-Service-Bereitstellungsmodus von Amazon API Gateway	Dem API-Gateway-Abschnitt wurde eine zusätzliche Rolle hinzugefügt. <code>customer_apigateway_cloudwatch_role</code>	Siehe Verwenden Sie AMS SSP, um Amazon API Gateway in Ihrem AMS-Konto bereitzustellen
Dem Self-Service Provisioning-Modus wurde ein neuer Dienst hinzugefügt	Zum Abschnitt Self-Service Provisioning-Modus hinzugefügt AWS Service Catalog AppRegistry	Siehe Verwenden Sie AMS SSP zur Bereitstellung AWS Service Catalog AppRegistry in Ihrem AMS-Konto
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	Siehe AMIs. csv-and-notes1.11.2023

Änderungen	Beschreibung	Link
September 2023		
Ein Hinweis zur Verwendung von Patch Orchestrator wurde hinzugefügt	Der folgende Hinweis wurde dem Abschnitt „Patch Orchestrator verwenden“ hinzugefügt: „Patch-Fehlerwarnungen werden nicht für Instanzen erstellt, deren Betriebssysteme nicht unterstützt werden oder die während des Wartungsfensters gestoppt werden“	Siehe Patchverwaltung in AMS
Datenverschlüsselung mit zusätzlichen Diensten aktualisiert	Dienste zur Datenverschlüsselung in AMS hinzugefügt.	Siehe Datenschutz in AMS
Den RFC-Fehlermeldungen wurde ein neuer Absatz hinzugefügt.	Es wurde ein neuer Absatz hinzugefügt, um den Link „Serviceanfrage erstellen“ hinzuzufügen.	Siehe Behebung von RFC-Fehlern in AMS
Die IAM-Rollenamen wurden korrigiert.	Der IAM-Rollenname <code>customer_emr_cluster_autosc</code> <code>aling_role</code> wurde korrigiert.	Siehe Self-Service-Bereitstellungsmodus in AMS
Die Basisinformationen zur Überwachung wurden aktualisiert	Der Verweis auf zwei veraltete Alarmer wurde entfernt. RDSRead LatencyAlarm RDSWrite LatencyAlarm	Siehe Warnmeldungen aus der Basisüberwachung in AMS
August 2023		

Änderungen	Beschreibung	Link
Hinzugefügt: Antwort auf Sicherheitsvorfälle von AMS	Dokumentation zur Verwendung von AMS Security Incident Response hinzugefügt.	Siehe Reaktion auf Sicherheitsvorfälle in AMS
Juli 2023		
Hinzugefügt: Automatisierte IAM-Bereitstellung	Dokumentation zur Verwendung von Automated IAM Provisioning hinzugefügt.	Siehe Automatisierte IAM-Bereitstellung AMS
Aktualisiert: Tabelle mit Zugriffsrollen	Fehlende Rollen für AMS Access hinzugefügt.	Siehe Zugriff auf das AMS-Kundenkonto (IAM-Rollen)
Juni 2023		
Aktualisiert: Liste der überwachten RDS-Warnmeldungen.	Die Liste der RDS-Warnmeldungen für die AMS-Basisüberwachung wurde aktualisiert. 9 neue RDS-Warntypen wurden hinzugefügt und 3 bestehende RDS-Warntypen wurden entfernt.	Siehe Warnmeldungen aus der Basisüberwachung in AMS .
Aktualisiert: Tabelle mit Zugriffsrollen	Neue Rollen für AMS Security.	Siehe Zugriff auf das AMS-Kundenkonto (IAM-Rollen)
Mai 2023		
Aktualisiert: Richtlinie zum Startdatum der Serviceabrechnung.	Die Definitionen des Startdatums der Abrechnung wurden aktualisiert.	Siehe Die wichtigsten Begriffe von AMS .
April 2023		

Änderungen	Beschreibung	Link
Aktualisiert: Monatlicher Self-Service-Bericht zur Abrechnung.	Hinweis hinzugefügt: Die monatlichen Abrechnungsberichte sind nur in einem Management Payer-Konto (AMS Advanced-Landzone für mehrere Konten) verfügbar, aber sie sind für alle verknüpften AMS Accelerate-verwalteten Konten verfügbar.	Siehe Abrechnungsbericht (monatlich) .
Aktualisiert: Der Inhalt „Standard-Patching“ wurde entfernt	AMS verwendet Patch Orchestrator.	Patchverwaltung in AMS
Aktualisiert: Was ist AMS?	Einige Themen wurden zuvor unter Was ist AMS? verschoben um Teil der AMS-Servicebeschreibung zu werden.	Service description (Service-Beschreibung)
Aktualisiert: Offboarding-Landingzone für mehrere Konten	Verschiedene Klarstellungen vorgenommen.	Offboard von AMS-Landingzone-Konten mit mehreren Konten
Aktualisiert: AWS Transfer Family (AMS SSPS)	Link zum Tutorial zur Einrichtung der Übertragung hinzugefügt.	Verwenden Sie AMS SSP zur Bereitstellung AWS Transfer Family in Ihrem AMS-Konto
Aktualisierter Inhalt: Self-Service-Bereitstellung	Gemäß den gesetzlichen Bestimmungen von AWS wurde CodeSuite "" durch „Code-Services“ ersetzt.	Verwenden Sie AMS SSP, um AMS Code-Dienste in Ihrem AMS-Konto bereitzustellen
Aktualisierter Inhalt: CloudWatch Metriken und Alarmer	Link zum Beispiel hinzugefügt: Zählt das Vorkommen eines Begriffs .	Benutzerdefinierte CloudWatch Metriken und Alarmer in AMS erstellen

Änderungen	Beschreibung	Link
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes04.2023
März 2023		
Aktualisierter Inhalt: Offboarding von AMS	Es wurde geklärt, welche Ressourcen gelöscht werden, wenn Landingzone-Konten mit mehreren Konten offline sind	Offboard von AMS-Landingzone-Konten mit mehreren Konten
Aktualisiert: AMS AMIs	Link zur AMI-ZIP-Datei für jeden Monat im Abschnitt Dokumentenverlauf hinzugefügt.	Dokumentenverlauf
Aktualisiert: Automatische Problembehebung	Die LVM-Unterstützung für EC2 Volumenautomatisierung wurde entfernt.	Automatische AMS-Behebung von Warnmeldungen
Aktualisiert: Patch RACI	Verschiedene Aktualisierungen und Klarstellungen für das RACI zum Patchen.	AMS-Verantwortungsmatrix (RACI)
Aktualisierter Inhalt: Self-Service-Bereitstellung	Ein FAQ-Aufzählungsfeld wurde hinzugefügt. Um einen neuen AWS Datasync-Agenten zu starten, ist keine WIGS-Aufnahme erforderlich.	Self-Service-Bereitstellung smodus in AMS

Änderungen	Beschreibung	Link
Aktualisierter Inhalt: Self-Service-Bereitstellung	Ein FAQ-Aufzählungsfeld wurde hinzugefügt. Um einen neuen AWS Datasync-Agenten zu starten, ist keine WIGS-Aufnahme erforderlich.	Self-Service-Bereitstellung smodus in AMS
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes.03.2023
Februar 2023		
Aktualisierter Inhalt: Offboarding von AMS	Es wurde geklärt, wie Landingzone-Umgebungen mit mehreren Konten und Anwendungskonten VPCs ausgegliedert werden	Offboard-AMS-Konten
Aktualisierter Inhalt: Finden ARNs	describe-table DynamoDB-CLI für die Suche nach einem DynamoDB-Tabellen-ARN hinzugefügt	Suchen Sie Amazon-Resourcennamen (ARNs) in AMS

Änderungen	Beschreibung	Link
Aktualisierter Inhalt: Self-Service Provisioning	Die AMS-Option "CodeSuite" wurde entfernt, da es sich nicht um eine tatsächliche SSPS handelt. Sie können weiterhin den Typ Verwaltung AWS Dienst Selbst bereitgestellter Dienst Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) ändern und die drei Dienste anfordern:, und. CodeBuild CodeDeploy CodePipeline AMS stellt Ihrem Konto dann die folgenden IAM-Rollen zur Verfügung:, und. customer_codebuild_service_role customer_codedeploy_service_role aws_code_pipeline_service_role Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.	Self-Service-Bereitstellung smodus in AMS
Aktualisierter Inhalt: Secrets Manager Manager-Update	Die Rollen, die für die landing zone mit mehreren Konten (MALZ) und die landing zone für einzelne Konten (SALZ) benötigt wurden, wurden korrigiert.	Häufig gestellte Fragen zum Teilen von Schlüsseln mit Secrets Manager
Aktualisierter Inhalt: Automatische Behebung von Warnmeldungen durch AMS	Unterstützung für Logical Volume Manager (LVM) - Volumes hinzugefügt.	EC2 Automatisierung der Behebung der Volumennutzung

Änderungen	Beschreibung	Link
Aktualisierter Inhalt: AMS Amazon Machine Images (AMIs)	Der Abschnitt Offboarding AMS AMIs mit Beispielcode zum Entfernen AMIs aus Ihrem Konto wurde hinzugefügt.	AMS Amazon-Maschinenbilder (AMIs)
Aktualisierter Inhalt: IAM-Benutzerrolle	Die IAM-Richtlinie wurde aktualisiert: AMSBilling Richtlinie.	IAM-Benutzerrolle in AMS
Neuer Inhalt: Nicht unterstützt OSes	Es wurden Informationen darüber hinzugefügt, welche Dienste AMS für nicht unterstützte Betriebssysteme anbietet (OSes).	Funktionen für nicht unterstützte Betriebssysteme in AMS
Aktualisierter Inhalt: Berichte auf Abruf	Bestimmte On-Demand -Berichte sind in AMS Advanced nicht verfügbar und wurden fälschlicherweise als verfügbar angezeigt.	Berichte auf Anfrage
Aktualisierter Inhalt: Offboarding von AMS-Konten	Die Anweisungen für das Offboarding von MALZ-Anwendungskonten wurden klargestellt.	Externe AMS-Anwendungskonten
Aktualisierter Inhalt: Secrets Manager	Die Namen der IAM-Rollen, die für die Verwendung von Secrets Manager erforderlich sind, wurden korrigiert.	Häufig gestellte Fragen zu Secrets Manager in AWS Managed Services

Änderungen	Beschreibung	Link
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes02.2023
Januar 2023		
Neuer Inhalt: AWS Device Farm (AMS SSPS)	Ein neuer SSPS-Dienst wurde hinzugefügt: AWS Device Farm.	Verwenden Sie AMS SSP zur Bereitstellung AWS Device Farm in Ihrem AMS-Konto
Aktualisiert: unterstützte Windows-Versionen	Unterstützung für Windows Server 2022 hinzugefügt.	AMS Amazon-Maschinenbilder (AMIs), Unterstützte Konfigurationen und AMS AMI-Benachrichtigungen mit SNS
Aktualisiert: Kontinuitätsmanagement	Die Regeln im Standard-AMS-Backup-Plan wurden aktualisiert.	Standard-Backup-Pläne, landing zone für mehrere Konten
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes.01.2023
Dezember 2022		
Aktualisiert: Bastionen verwenden	Fehlerhafter Link behoben.	Zugreifen auf Instanzen mithilfe von Bastionen

Änderungen	Beschreibung	Link
Aktualisiert: Resource Scheduler	Es wurden mehrere Verbesserungen vorgenommen und Links AWS zum Instance Scheduler hinzugefügt, um mehr Kontext zu bieten.	Ressourcenplaner für AWS Managed Services
Aktualisiert: Windows AMIs und unterstützte Konfigurationen (für neue Windows AMIs)	Der AMS-AMI-Inhalt wurde von EC2 Launch (Windows Server 2016 und höher) zu EC2 Launch (Windows Server 2016 und Windows Server 2019) hinzugefügt und EC2 LaunchV2 (Windows Server 2022 und höher) hinzugefügt. Windows-basiert AMIs von Microsoft Windows Server (2012, 2012 R2, 2016 und 2019) auf Microsoft Windows Server (2012, 2012 R2, 2016, 2019 und 2022) aktualisiert.	AMS Amazon-Maschinenbilder (AMIs) und Service description (Service-Beschreibung)
Aktualisiert: Abschnitt „Resourced Scheduler“	Verbesserte Methoden für die Bereitstellung und Anpassung von AMS Resource Scheduler.	Ressourcenplaner für AWS Managed Services
Aktualisiert: AMS einrichten: privates und öffentliches DNS	Das DNS-Architekturdiagramm wurde aktualisiert.	Privates und öffentliches DNS einrichten
Aktualisiert: MALZ-Netzwerkarchitektur	Das Diagramm wurde aktualisiert und eine Anleitung für Accelerate-Anwendungskonten hinzugefügt.	MALZ Netzwerkarchitektur

Änderungen	Beschreibung	Link
Aktualisiert: Einrichtung: Verwendung von Tags	Neuer Hinweis: Benutzerdefiniertes Tagging wird nur für MALZ-Anwendungskonten unterstützt, nicht für Kernkonten.	Automatisches Tagging der AMS-Infrastruktur
Aktualisiert: Zugriffsverwaltung : Bastionen verwenden	Die Einführung wurde aktualisiert und umfasst nun auch RDP-Bastionen.	Kosteneinsparung bei Bastionen in der Single-Account-Landezone (SALZ)
Aktualisiert: AMS-Standardeinstellungen: Warnmeldungen	EC2 Instance: Non-Root-Volume Usage wurde zur Warnungstabelle hinzugefügt.	Warnmeldungen aus der Basisüberwachung in AMS
Aktualisiert: Continuity Management	Es wurden Hinweise zu kontinuierlichen Backups hinzugefügt.	So funktioniert Kontinuitätsmanagement
Aktualisiert: Automatisierte EC2 Instanzkonfiguration	Unterstützung für PowerBroker Identity Service (PBIS) und On Instance Code (OIC) hinzugefügt.	Automatisches Aktualisieren von PBIS auf Linux-Instances und Automatisches Aktualisieren von Code auf Linux-Instances
Aktualisiert: Self-Service Provisioning für Secrets Manager	Das CT für das Hinzufügen von Secrets Manager zu Ihrem Konto wurde aktualisiert (unter FAQs).	Verwenden Sie AMS SSP zur Bereitstellung AWS Secrets Manager in Ihrem AMS-Konto
Aktualisiert: Protokollverwaltung	Die Liste der Protokolle auf EC2 Systemebene wurde aktualisiert.	Amazon Elastic Compute Cloud (Amazon EC2) — Protokolle auf Systemebene

Änderungen	Beschreibung	Link
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes.12.2022
November 2022		
Aktualisiert: AMS Amazon Machine Images (AMIs)	Die unterstützten SUSE Linux-Versionen wurden aktualisiert.	AMS Amazon-Maschinenbilder (AMIs)
Aktualisiert: MALZ-Konten	Es wurde eine Anleitung zum Löschen eines vom Kunden verwalteten Anwendungskontos hinzugefügt.	Vom Kunden verwaltete Anwendungskonten
Aktualisiert: AMS einrichten	customer-ams-amazon2-security-enhanced hinzugefügt.	AMS AMI-Benachrichtigungen mit SNS
Aktualisiert: So funktioniert die Überwachung	Die Erläuterung der Servicemeldungen und Vorfallberichte wurde aktualisiert.	So funktioniert die Überwachung
Aktualisiert: Kontotypen für MALZ-Anwendungen	Die Erklärung der Kontotypen wurde verbessert.	Arten von Anwendungskonten
Aktualisiert: Entwicklermodus	Es wurde eine Warnung zum Entwicklermodus hinzugefügt.	Bevor Sie mit dem AMS-Entwicklermodus beginnen
Aktualisiert: Verwaltung geplanter Ereignisse	Der Abschnitt: Typen von PEM wurde hinzugefügt	Verwaltung geplanter Ereignisse in AWS Managed Services
Aktualisiert: Amazon Machine Images (AMIs)	Die unterstützten SUSE Linux-Versionen wurden aktualisiert	AMS Amazon-Maschinenbilder (AMIs)

Änderungen	Beschreibung	Link
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes1.11.2022

Oktober 2022

Neu: Automatisierte Instanzkonfiguration	In einem neuen Abschnitt wird der Prozess der automatisierten Instanzkonfiguration beschrieben.	Automatisierte Instanzkonfiguration in AMS Advanced
Neu: Für einige SSPS ist nur manuelles CT zulässig	Der Self-Service-Bereitstellungsdienst für mehr als 50 wurde aktualisiert und verwendet FAQs nun den manuellen CT und nicht den automatisierten CT für das Hinzufügen von SSPS.	Self-Service-Bereitstellungsmodus in AMS
Update: AMS einrichten	Den Amazon EC2 IAM-Instanzprofilen für MALZ wurden zwei Richtlinien hinzugefügt.	EC2 IAM-Instanzprofil
Neu: Bibliothek mit benutzerdefinierten Detektiv- und Präventionsregeln.	Es wurden eine Reihe von Beispielrichtlinien zur Servicesteuerung (SCPs) und präventive Konfigurationsregelkontrollen hinzugefügt, die auf unseren Erfahrungen mit mehreren Kunden basieren.	Kuratierte Regeln SCPs und Konfigurationsregeln

Änderungen	Beschreibung	Link
Update: Warnung AWS Backup	Es wurde eine Warnung hinzugefügt: „Bearbeiten Sie keine AMS-Backup-Pläne, da Ihre Änderungen verloren gehen könnten. Erstellen Sie stattdessen neue Backup-Pläne mit ct-2hyozbpa0sx0m für Ihre benutzerdefinierten Konfigurationen.“	So funktioniert Kontinuitätsmanagement
AWS Backup Update: Vorsicht	Es wurde ein Hinweis zum Hinzufügen neuer IAM-Rollen zu Ihrem Verband hinzugefügt.	Bereitstellung von IAM-Ressourcen in AMS Advanced
Update: Verwaltung der Überwachung	Benachrichtigungen generieren Vorfallberichte, keine Serviceanfragen.	So funktioniert die Überwachung
Update: Bringen Sie Ihr eigenes EPS mit	Gilt sowohl für SALZ als auch für MALZ.	AMS bring dein eigenes EPS mit
Update: Accelerate Application-Konto	Es wurde klargestellt, dass es sich bei Ihrem Accelerate-Konto um ein Anwendungskonto handelt.	Arten von Anwendungskonten
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes.10.2022
September 2022		

Änderungen	Beschreibung	Link
Aktualisiert: CLI-Befehlsbeispiele für die Suche nach Ressourcen	Es wurde ein neues Beispiel hinzugefügt und es wurde angegeben, dass die --region Option möglicherweise benötigt wird.	Finden der benötigten Daten (SKMS), AMS
Aktualisiert: Bereitstellung von IAM-Rollen	IAM-Rollen können jetzt mit dem erstellt und verwaltet werden. AWSManagedServicesCloudFormationAdminRole	Stapel im Direct Change-Modus erstellen
Aktualisiert: Technische Standards von AMS	AMS-STD-007-Protokollierung : (#20) Die Weiterleitungsanforderungen wurden geklärt.	Sicherheit und Compliance
Aktualisiert: So funktioniert Continuity Management	Die Formulierung des Start Backup-Jobs wurde überarbeitet und lautet nun „auf Anfrage“ statt „vorhanden“.	So funktioniert Continuity Management
Aktualisiert: Sicherheit und Compliance	Beschreibung und Anleitung für den AMS-STD-007-Standard Nummer 20: Weiterleitung von Protokollen zwischen Konten wurden aktualisiert.	Sicherheit und Compliance
Aktualisiert: Anwendungsfälle für das Change-Management	Ein defekter Link zum alten Change Management-Benutzerhandbuch wurde entfernt.	Anwendungsfälle des Change-Managements
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes.09.2022

Änderungen	Beschreibung	Link
11. August 2022		

Änderungen	Beschreibung	Link
Aktualisiert: Die Kapitelüberschriften wurden aus Gründen der Einheitlichkeit und Lesbarkeit einige Themenunterabschnitte in passendere Abschnitte verschoben	„MALZ-Netzwerkarchitektur“ und „SALZ-Netzwerkarchitektur“ sind jetzt beide Unterabschnitte des übergeordneten Abschnitts „Netzwerkarchitektur“, früher der Abschnitt „AMS-Netzwerkarchitektur“ „Modi für das Change-Management“ ist die neue Überschrift für „Change Management“ „Standardeinstellungen“ ist jetzt ein Unterabschnitt von „AMS einrichten“ „AD FS-Beanspruchungsregel und SAML-Einstellungen“ (früher „ActiveDirectory Federation Services (ADFS)-Beanspruchungsregel und SAML-Einstellungen“) ist jetzt ein Unterabschnitt von „AMS einrichten“ „Zugriffsverwaltung“ ist die neue Überschrift für „Zugriff in AMS“ und wurde im Inhaltsverzeichnis nach oben verschoben „Finden der benötigten Daten“ ist die neue Überschrift für	Was ist AWS Managed Services?

Änderungen	Beschreibung	Link
	„Wissensmanagement im Bereich Service“ „Berichte und Optionen“ ist die neue Überschrift für „AMS Reporting“ und befindet sich weiter unten im Inhaltsverzeichnis „Operations on Demand“ ist jetzt das letzte Thema im Inhaltsverzeichnis	
Aktualisiert: Suchen und ARN, Neu: Suchen nach einer Ressource mit einem ARN	Beide Verfahren wurden aus Gründen der Nützlichkeit komplett neu geschrieben.	Suchen Sie Amazon-Ressourcennamen (ARNs) in AMS und Finden Sie Ressourcen nach ARN in AMS .
Aktualisiert: Verbinden Sie Ihre CMA mit Transit Gateway	Die Automatisierung unterstützt nicht das Hinzufügen von Routen zu Kernroutendomänen und das Verfahren musste aktualisiert werden.	Verbinden Sie Ihre CMA mit Transit Gateway
Aktualisiert: Preisgestaltung der MALZ-Basiskomponenten	Alle Preise sind in US-Dollar angegeben und mit Dollarzeichen formatiert.	Grundkomponenten der AMS-Umgebung
Aktualisiert: AMS AMI Notes	Die Zip-Datei enthält Hinweise zu den neuesten AMS Amazon-Maschinenimages (AMIs) und eine CSV-Datei der neuesten Version AMIs.	AMIs. csv-and-notes.08.2022
14. Juli 2022		

Änderungen	Beschreibung	Link
Aktualisiert: Self-Service-Berichterstattung	Es wurden Anweisungen zum Verschlüsseln von AWS Glue Metadaten mit KMS-Schlüsseln hinzugefügt.	Self-Service-Berichte
Aktualisiert: AMS-Basisüberwachung	DeleteRecoveryPoint Backup-Warnung hinzugefügt.	Warnmeldungen aus der Basisüberwachung in AMS
Aktualisiert: Unterstützte Betriebssysteme	Datum für das Ende des Support für Amazon Linux 2 hinzugefügt.	Unterstützte Konfigurationen
Aktualisiert: Self-Service-Bereitstellung	Eine Voraussetzung für den AWS Transfer SSPS wurde hinzugefügt.	Verwenden Sie AMS SSP zur Bereitstellung AWS Transfer Family in Ihrem AMS-Konto
Aktualisiert: AMS Reporting	Hinweis zu Opt-in-Regionen hinzugefügt.	Berichte und Optionen
Aktualisiert: RFC-Korrespondenz und Anhang	Die zulässigen Textdateitypen wurden klargestellt. Insbesondere müssen YAML-Dateien auf .yaml (nicht .yml) enden.	Fügen Sie RFC-Korrespondenz und Anlagen hinzu (Konsole)
21. Juni 2022		
Aktualisierter Inhalt	Der AMS-Modus, der früher als „Change Management-Modus“ oder „Standard-CM-Modus“ bekannt war, ist jetzt als „RFC-Modus“ bekannt. Der Bereich Modi wurde erweitert.	Übersicht der Modi.
Neuer Alarm	Ein AWS Backup Alarm wurde hinzugefügt.	Warnmeldungen aus der Basisüberwachung in AMS
16. Juni 2022		

Änderungen	Beschreibung	Link
Neuer Inhalt	Verwaltung von Vorfällen. Vorfälle, die kein Sicherheitsrisiko darstellen, können jetzt von AMS mit Ihrer Zustimmung im Vorfallbericht behoben werden und benötigen keinen separaten RFC und keine separate Genehmigung.	Vorfallmanagement
Aktualisierter Inhalt	MALZ: Das Diagramm der Netzwerkarchitektur wurde aktualisiert. Updates: Das VPC-Peering für das Masterkonto VPC to Shared Services VPC sollte entfernt werden, da es nicht existiert.	Architektur von Netzwerken
	Self-Service Provisioned Service (SSPS) von Sagemaker. Das Update wurde mit einer neuen IAM-Rolle aktualisiert, die beim Onboarding für Sagemaker hinzugefügt wurde.	Verwenden Sie AMS SSP, um Amazon SageMaker AI in Ihrem AMS-Konto bereitzustellen

Änderungen	Beschreibung	Link
	Zur Liste der für SNS-Benachrichtigungen AMIs unterstützen Benachrichtigungen : customer-ams-sles 12, customer-ams-sles 15, customer-ams-amazon 1-sicherheitserweitert, customer-ams-rhel 8, customer-ams-rhel 8-sicherheitserweitert, 18, 2012, 2019 und 2019 mit erweiterter Sicherheit hinzugefügt. customer-ams-ubuntu customer-ams-windows customer-ams-windows customer-ams-windows customer-ams-rhel Die Versionen 6 und 6 mit erweiterter Sicherheit wurden entfernt. customer-ams-rhel AMIs	AMS AMI-Benachrichtigungen mit SNS
	Eskalations-E-Mails wurden entfernt.	Hilfe zu AWS Managed Services erhalten
	Die Themenliste wurde unter die ersten Absätze verschoben.	Was ist AWS Managed Services?
	Aktualisierte Serviceprotokolle mit besseren Links für Load-Balancing-Logs, ebenfalls neu formatiert.	Aggregierte AMS-Servic ceprotokolle

Änderungen	Beschreibung	Link
EKS Self-Service Provisioning Service (SSPS). Es wurden Informationen zur Aktivierung der Verschlüsselung von Envelope Secrets in Ihrem Cluster hinzugefügt.	Verwenden Sie AMS SSP, um Amazon EKS AWS Fargate in Ihrem AMS-Konto bereitzustellen	
09. Juni 2022		
Aktualisierter Inhalt, Hilfe erhalten	E-Mails mit dem Eskalationspfad wurden entfernt. AMS bietet Kommunikationsmethoden in Form von Störungsbberichten, Serviceanfragen und RFCs.	Hilfe zu AWS Managed Services erhalten
12. Mai 2022		
Neue Inhalte, Abonnementmodell Operations on Demand (OOD)	AMS hat das Onboarding von Operations on Demand vom aktuellen Anmelde- und Verlängerungsmodell auf ein Abonnementzuweisungsgs- und Standard-Opt-In-Modell umgestellt. Wenn Sie ein AMS-Konto einrichten, sind Sie jetzt automatisch bei Operations on Demand registriert.	Betrieb auf Abruf
14. April 2022		
Neue Inhalte, Kostenoptimierung	AMS gibt Empfehlungen zur Kostenoptimierung.	Kostenoptimierung in AWS Managed Services

Änderungen	Beschreibung	Link
Aktualisierter Inhalt, Accelerate Account in MALZ	Ein falscher Rollenname (CustomerDefaultAdminRole) wurde auf den richtigen Rollennamen (AccelerateDefaultAdminRole) aktualisiert.	AMS Accelerate-Konten Abschnitt „Zugriff auf Ihr Accelerate-Konto“.
Aktualisierter Inhalt, AMS greift auf IAM-Rollen zu	Es wurden weitere AMS IAM-Rollen hinzugefügt, die für den Zugriff auf Ihre Konten verwendet werden.	Warum und wann AMS auf Ihr Konto zugreift Abschnitt „Zugriff auf IAM-Rollen für AMS-Kundenkonten“.
Aktualisierter Inhalt, AMS-Backup-Pläne	Von AMS verwaltete Backup-Pläne hinzugefügt.	AMS-Backup-Pläne und AMS-Backup-Tresore
Aktualisierter Inhalt, AWS Secrets Manager	Die häufig gestellten Fragen wurden aktualisiert.	Verwenden Sie AMS SSP zur Bereitstellung AWS Secrets Manager in Ihrem AMS-Konto
Aktualisierter Inhalt, Onboarding im Direct Change Mode (DCM)	AMS unterstützt das Onboarding von Service Catalog-Kunden in DCM nicht.	Erste Schritte mit dem Direct Change-Modus
Aktualisierter Inhalt, Servicebeschreibung	Der Abschnitt „Unterstützte Dienste“ wurde klargestellt: • Amazon EKS auf AWS Fargate -> Amazon Elastic Kubernetes Service auf Fargate • Amazon ECS für Fargate -> Amazon Elastic Container Service auf AWS Fargate • Amazon Kinesis -> Amazon Kinesis Data Streams	Unterstützte AWS Dienste

Änderungen	Beschreibung	Link
Aktualisierter Inhalt, Offboarding von MALZ-Konten	Aktualisiert, um auf neue Änderungstypen für Offboarding-Anwendungskonten hinzuweisen.	Externe AMS-Anwendungskonten
Aktualisierter Inhalt, Incident-Management im Entwicklermodus	Die Beschreibung der Incident-SLA wurde aktualisiert auf: AMS SLA gilt nicht für Ressourcen, die außerhalb von AMS Change Management erstellt oder aktualisiert wurden (einschließlich Entwicklermodus). Daher werden Ressourcen, die im Entwicklermodus aktualisiert oder erstellt wurden, automatisch auf die Stufe P3 heruntergestuft, und der Support erfolgt nach bestem Wissen.	Vorfallmanagement im AMS-Entwicklermodus
Aktualisierter Inhalt, DCM-Onboarding	Die RFC-Vorlage für das neue DCM enthält jetzt ein Feld für Ihren SAML-Provider-ARN.	Erste Schritte mit dem Direct Change-Modus
Aktualisierter Inhalt, DCM für CloudFormation	Die Anweisungen zum Erstellen und Aktualisieren von CloudFormation Stacks enthalten jetzt YAML-Beispiele.	AMS-Transformation
Aktualisierter Inhalt, MALZ Tools-Account	Es gibt eine neue IAM-Rolle für Migrationen: AWSManagedServicesMigrationRole	AWS Service zur Anwendungsmigration (AWS MGN) und Zugriff auf das neue AMS Tools-Konto aktivieren

Änderungen	Beschreibung	Link
Neue Inhalte, Landingzone-Konten mit mehreren Konten	Sie können ein Accelerate-Konto in Ihrem AMS-Verwaltungskonto mit mehreren Konten für die landing zone erstellen.	AMS Accelerate-Konten
Aktualisierter Inhalt, API/CLI SDK-Installation	In den Installationsanweisungen wurden der falsche Dateiname für Mac/Linux Installationen und ein falscher Befehl aufgeführt. Dieses Problem wurde behoben.	Verwenden der AMS-API und CLI
Aktualisierter Inhalt, Accelerate Account in MALZ	Es gab einen falschen Regelnamen (Customer DefaultAdminRole), er wurde auf den richtigen aktualisiert (AccelerateDefaultAdminRole).	AMS Accelerate-Konten , Abschnitt „Zugriff auf Ihr Accelerate-Konto“
Aktualisierter Inhalt, Überwachung	Die Überwachung der Root-Nutzung wurde von 85 auf 95% revidiert.	Warnmeldungen aus der Basisüberwachung in AMS
Aktualisierter Inhalt, AMI-Benachrichtigungen	Sie können viele Arten von SNS-Benachrichtigungen für neue AMS AMIs erstellen . Wir haben Informationen zur Erstellung verschiedener Typen hinzugefügt.	AMS AMI-Benachrichtigungen mit SNS
Aktualisierter Inhalt, AMS-StandardEinstellungen	Verweise auf Macie Classic wurden entfernt und durch Macie ersetzt.	Warnmeldungen aus der Basisüberwachung in AMS

Änderungen	Beschreibung	Link
Aktualisierter Inhalt, für AMS reservierte Präfixe	Die Liste der reservierten Präfixe wurde alphabetisch sortiert.	Reservierte AMS-Präfixe
Aktualisierter Inhalt, Servicebeschreibung	Die Funktionsbereiche zum Änderungsmanagement und zur Self-Service-Bereitstellung wurden mit weiteren Informationen zu den AMS-Modi aktualisiert.	Funktionen des erweiterten Betriebsplans AMS von AWS Managed Services (AMS)
Aktualisierter Inhalt, AWS Secrets Manager	Schlüssel mit Secrets Manager teilen.	10. Februar 2022
Neue Inhalte, Self-Service-Bereitstellung, Amazon Connect	Es wurde eine häufig gestellte Frage hinzugefügt, in der es darum geht, das Hinzufügen einer Länderliste für ausgehende oder eingehende Anrufe anzufordern.	10. Februar 2022
Neue Inhalte, Self-Service-Bereitstellung, Amazon EKS auf Fargate	Es wurde eine häufig gestellte Einschränkung hinzugefügt, dass die Bereitstellung von EKS-Clustern über das AWS Cloud Development Kit (CDK) oder CloudFormation Ingest in AMS nicht unterstützt wird.	10. Februar 2022

Änderungen	Beschreibung	Link
Inhalt geändert, Entwickle rmodus	Korrektur: Sie verwenden keinen RFC oder eine Serviceanfrage, um Ihrer Verbundlösung Benutzer zuzuweisen, Sie tun dies je nach Ihrer Lösung selbst.	10. Februar 2022
Geänderter Inhalt, Direct Change-Modus (DCM)	Beachten Sie, dass IAM in DCM nicht unterstützt wird.	10. Februar 2022
	DCM, beachten Sie die von uns durchgeführten Validierungen.	10. Februar 2022
	DCM, klären Sie die Einschränkungen der verschiedenen Rollen ab.	10. Februar 2022
Geänderter Inhalt, Überwachung der Basiswarnungen	Die Ressourcenwarnungen für Redshift-Cluster wurden geändert.	10. Februar 2022
Geänderter Inhalt, Self-Service-Berichterstattung	Es wurde der exakte S3-Bucket-Name (ams-reporting-data-a<Account_ID>) hinzugefügt, den Kunden zum Abrufen der Berichte verwenden können.	10. Februar 2022

Änderungen	Beschreibung	Link
Inhalt geändert, Inhalt aktualisiert, sodass er auf automatisierte Änderungstypen statt auf manuelle Änderungen verweist. Verwaltung Andere Andere (MOO)	Der Inhalt der Anwendungskontos für mehrere Konten (MALZ) wurde aktualisiert und verweist nun auf automatisierte Änderungstypen (drei, „Den TGW-Anhang einer Routentabelle zuordnen“, „Routen in den TGW-Routentabellen erstellen“, um eine Verbindung zu dieser VPC herzustellen“ und „Konfiguration Ihrer VPC-Routentabellen so, dass sie auf das AMS Multi-Account Landing Zone-Transit-Gateway zeigen“). Empfangen von Warnmeldungen, die von AMS generiert wurden Tag-basierte Warnmeldungen	10. Februar 2022
Geänderter Inhalt: AMS AMIs.	Es wurden neue Informationen zur erweiterten Sicherheit hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Konfigurationen AMS Amazon-Maschinenbilder (AMIs), und Verbesserte Sicherheit AMIs	27. Januar 2022

Änderungen	Beschreibung	Link
Neuer Inhalt: Self-Service-Bereitstellung.	Amazon Fsx für OpenZFS hinzugefügt. Siehe Verwenden Sie AMS SSP, um Amazon FSx für OpenZFS in Ihrem AMS-Konto bereitzustellen.	27. Januar 2022
Geänderter Inhalt: Code-Deploy Self-Service Provisioning Service (SSPS).	Zusätzlicher Rollename und zusätzlicher Hinweis zur Einschränkung. Weitere Informationen finden Sie unter. Verwenden Sie AMS SSP zur Bereitstellung AWS CodeDeploy in Ihrem AMS-Konto	27. Januar 2022
Geänderter Inhalt: Die Links wurden aktualisiert.	Fehlerhafte Links behoben: AMS-AMIs, Suchen Ihrer Einstellungen, Suchen einer Stack-ID, Suchen einer VPC-ID, ListVpcSummaries ListStackSummaries, und GetStack APIs. Ein Beispiel finden Sie unter Finden Sie den Stack IDs in AMS.	13. Januar 2022
Geänderter Inhalt: EKS-Unterstützung für Fargate	Einschränkung hinzugefügt zu FAQs: Das Erstellen oder Verwalten von EC2 Knotengruppen mit EKS wird nicht unterstützt. Siehe Verwenden Sie AMS SSP, um Amazon EKS AWS Fargate in Ihrem AMS-Konto bereitzustellen.	13. Januar 2022

Änderungen	Beschreibung	Link
Geänderter Inhalt: CloudFormation, Direct Change Mode (DCM)	Es wurden Anweisungen zum Erstellen oder Aktualisieren von CF-Stacks mit hinzugefügt. AmsStackTransform Siehe Stapel im Direct Change-Modus erstellen .	13. Januar 2022
Geänderter Inhalt: Einheitlichkeit der Dienstnamen AWS	AMS-Verweise, die AWS-Services exakt den offiziellen AWS Titeln oder Metadaten entsprechen. Zuvor gab es geringfügige Abweichungen, die den Musterabgleich erschwerten. Ein Beispiel finden Sie unter Verwenden Sie AMS SSP, um Alexa for Business in Ihrem AMS-Konto bereitzustellen .	13. Januar 2022
Geänderter Inhalt: Self-Service-Bereitstellung von Elastic Container Registry (ECR)	Es wurde ein FAQ-Eintrag zur Verwendung von ECR zur Verwaltung von Benutzerberechtigungen hinzugefügt. Siehe Verwenden Sie AMS SSP, um Amazon Elastic Container Registry in Ihrem AMS-Konto bereitzustellen .	13. Januar 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.