Verwaltung von Identität und Zugriff für VMware Cloud on AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Verwaltung von Identität und Zugriff für VMware Cloud on AWS

Table of Contents

Verwaltung von Identität und Zugriff für VMware Cloud on AWS

Richard Milner-Watts, Abdenour Kansab und Chris Porter, Amazon Web Services (AWS)

Vern Bolinius, VMware

Juni 2023 (Dokumentverlauf)

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Identitäts- und Zugangsverwaltung ist das Prinzip, den Systemzugriff nur auf autorisierte Benutzer und Anwendungen zu beschränken, einschließlich der Beschränkung des Zugriffs auf die erforderlichen Netzwerkressourcen. In Cloud-Umgebungen bestehen Identitäts- und Zugriffsverwaltungskontrollen in der Regel aus Richtlinien und Services, die Sie zur Identifizierung, Authentifizierung und Autorisierung von Benutzern, Benutzergruppen und Anwendungen verwenden.

VMware Cloud on AWS unterstützt Ihre VMware vSphere-basierten Workloads in der. AWS Cloud Sie können viele Services und Tools von VMware verwenden, um diese Cloud-Infrastruktur zu konfigurieren, zu verwalten, zu sichern, zu überwachen und zu analysieren. Die Features und Steuerungen, die Sie zur Identitäts- und Zugriffsverwaltung verwenden, variieren je nach Service. Dieses Kapitel enthält bewährte Methoden und Empfehlungen für die Identitäts- und Zugriffsverwaltung für die folgenden VMware-Services:

- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- VMware Cloud Disaster Recovery
- VMware Cloud auf AWS
- VMware Cloud Services Console
- VMware HCX

- VMware NSX
- VMware Site Recovery
- VMware vCenter Server

Dieses Handbuch bietet einen Überblick und bewährte Methoden zum Identitäts- und Zugriffsmanagement für VMware Cloud on AWS und verwandte VMware-Dienste. Es enthält eine kurze Beschreibung der einzelnen Services und erörtert die Überlegungen zum Identitätszugriff und zur Verwaltung dieses Services. Wir geben auch Empfehlungen für die Konfiguration des Dienstes als Teil von VMware Cloud on AWS.

> **Important**
>
> Viele der in diesem Handbuch beschriebenen VMware-Services werden in anderen Cloud- oder On-Premises-VMware-Lösungen verwendet. Die Empfehlungen und bewährten Methoden in diesem Handbuch beziehen sich speziell auf VMware Cloud in AWS. Diese Empfehlungen gelten möglicherweise nicht für andere Umgebungen.

Zielgruppe

Dieser Leitfaden richtet sich an Architekten und Sicherheitsingenieure, die für die Implementierung von VMware Cloud on AWS in ihrer Cloud- oder Hybridumgebung verantwortlich sind.

Gezielte Geschäftsergebnisse

Dieser Leitfaden hilft Ihnen bei folgenden Aufgaben:

1. Machen Sie sich mit den verschiedenen Identitäts- und Zugriffsverwaltungskontrollen für VMware Cloud on AWS und verwandte VMware-Dienste vertraut
2. Machen Sie sich mit den empfohlenen Best Practices vertraut, mit denen Sie VMware Cloud sicher betreiben können AWS
3. Machen Sie sich mit den Optionen vertraut, die für die Verbundauthentifizierung über einen externen Identitätsanbieter verfügbar sind

Identitätsmanagement im Überblick

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware verwendet die folgenden branchenüblichen Konzepte und Identitätshierarchien zur Verwaltung der Identifizierung, Authentifizierung und Autorisierung:

- Benutzer sind die Personen, die in gewisser Weise auf Ihre Umgebung zugreifen. Sie können lokale Benutzer erstellen oder den Verbund verwenden, um Benutzer von einem externen Identitätsanbieter zu authentifizieren. Weitere Informationen finden Sie unter Identitätsverbund und SSO.
- Gruppen bieten einen Mechanismus, um eine Sammlung von Benutzern logisch zu gruppieren. Auf diese Weise können Sie diesen Benutzern konsistente Berechtigungen gewähren und den Verwaltungsaufwand reduzieren. Rollen werden verwendet, um einem Benutzer oder einer Gruppe Berechtigungen zu erteilen. Weitere Informationen finden Sie unter Rollen und Berechtigungen im SDDC (VMware-Dokumentation).
- Organizations in VMware Cloud kontrollieren den Zugriff auf einen oder mehrere VMware-Services. Benutzer und Gruppen müssen einer Organisation angehören, um auf die Services in der Organisation zugreifen zu können. Sie können das Feature Identitätsverwaltung und Verwaltung aktivieren, mit der föderierte Identitäten per Self-Service die Mitgliedschaft bei einer VMware-Organisation beantragen können. Weitere Informationen finden Sie unter VMware Cloud Services Console.

Berechtigungen können Zugriff auf ein bestimmtes Objekt gewähren oder sie können von übergeordneten Objekten vererbt werden. Wenn einem Benutzer oder einer Gruppe mehrere sich überschneidende Berechtigungen zugewiesen werden, gilt die weitestgehende Berechtigung. Weitere Informationen finden Sie unter Hierarchische Vererbung von Berechtigungen (VMware-Dokumentation).

Sie können diese Strukturelemente verwenden, um eine Richtlinie mit den geringsten Berechtigungen einzuführen und logische Zugriffsgrenzen innerhalb Ihrer Infrastruktur auf der Grundlage der

Benutzeranforderungen festzulegen. Geringste Berechtigung ist das Prinzip, Benutzern und Anwendungen nur den Mindestzugriff zu gewähren, der zur Ausführung ihrer Aufgaben erforderlich ist. Im Falle eines unbefugten Zugriffs kann diese branchenweit bewährte Methode dazu beitragen, die Fähigkeit eines Angreifers, Schaden anzurichten oder sensible Daten zu stehlen, einzuschränken. Und selbst für autorisierte Benutzer kann dieses Prinzip verhindern, dass Benutzer auf Daten zugreifen, die sie nicht haben sollten. Wenn Benutzern nur Zugriff auf die erforderlichen Ressourcen gewährt wird, kann dies auch die Produktivität verbessern und den Bedarf an Unterstützung bei der Fehlerbehebung verringern.

Wenn Sie VMware Cloud on verwenden AWS, gibt es zwei Hauptdienste und Tools für die Identitäts- und Zugriffsverwaltung: VMware Cloud Services Console undVMware vCenter Server. Später in diesem Handbuch werden wir diese Services ausführlicher besprechen.

Identitätsverbund und SSO

Viele Unternehmen möchten einen Verbund mit einem externen Identitätsanbieter (IdP) einrichten. Dies ermöglicht Ihnen, Ihren Benutzern ein Single Sign-On (SSO)-Erlebnis zu bieten. Sowohl VMware Cloud als auch vCenter Server unterstützen den Unternehmens-Verbund:

- VMware Cloud unterstützt die auf Security Assertion Markup Language (SAML) 2.0 basierende Sprache IdPs und unterstützt das Lightweight Directory Access Protocol (LDAP). Weitere Informationen finden Sie unter Was ist ein Unternehmensverbund und wie funktioniert er mit VMware Cloud Services (VMware-Dokumentation).
- Wenn Sie vCenter Server auf VMware Cloud on betreiben AWS, wird der Verbund mit vCenter Server mithilfe eines externen IdP derzeit nicht unterstützt. Es kann nur der integrierte IdP verwendet werden, der die Verwendung von Microsoft Active Directory über LDAP unterstützt. Weitere Informationen finden Sie unter Identitätsquellen für vCenter Server mit vCenter Single Sign-On (VMware-Dokumentation).

Einige der anderen verwandten VMware-Services, die in diesem Handbuch behandelt werden, unterstützen auch den direkten Verbund von einem IdP aus. Die Konfiguration des Verbunds in jedem Service schafft jedoch zusätzliche Benutzerverwaltungspunkte und wird schwierig zu verwalten. Stattdessen können Sie Gruppen und Rollen in der VMware Cloud Services Console verwenden, um eine gemeinsame Identitätsquelle zu verwenden und Berechtigungen für andere VMware Cloud-Services zu konfigurieren. Sie können auch den Hybrid Linked Mode konfigurieren, um dieselben Identitäten mit einer On-Premises vCenter-Server-Instance zu verwenden. Dadurch wird die Anzahl der Verbundpunkte und der Identitätsverwaltung auf zwei Services reduziert. Weitere

Informationen zum verknüpften Hybridmodus finden Sie unter Konfiguration des verknüpften Hybrid-Modus (VMware-Dokumentation).

Allgemeine bewährte Methoden

Notice (Hinweis)

Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Important

Viele der in diesem Handbuch beschriebenen VMware-Services werden in anderen Cloud- oder On-Premises-VMware-Lösungen verwendet. Die Empfehlungen und bewährten Methoden in diesem Handbuch beziehen sich speziell auf VMware Cloud in AWS. Diese Empfehlungen gelten möglicherweise nicht für andere Umgebungen.

Beachten Sie die folgenden AWS Empfehlungen für die Verwaltung von Identität und Zugriff auf Ihre VMware-Cloud-Infrastruktur:

- Wenden Sie eine Richtlinie mit der geringsten Berechtigung an. Verwenden Sie die rollenbasierte Zugriffskontrolle (RBAC), um den Benutzern die zur Ausführung ihrer Aufgaben erforderlichen Mindestberechtigungen und den Zugriff zu gewähren.
- Erteilen Sie, wenn möglich, Gruppen und nicht einzelnen Benutzern Berechtigungen.
- Vermeiden Sie es, lokale Benutzer zu konfigurieren. Authentifizieren Sie Benutzer anhand eines externen, verbundenen Identitätsanbieters.
- Konfigurieren der Multi-Faktor-Authentifizierung für alle Benutzer.
- Ihre Passwortrichtlinie sollte Anforderungen an die Passwortstärke und Rotation beinhalten.
- Dokumentieren Sie ein „Break-Glass“-Verfahren für die Übernahme der vollständigen administrativen Kontrolle über die VMware-Organisation und die zugehörigen Services. „Break Glass“, das seinen Namen vom Zerbrechen des Glases zur Auslösung eines Feuermelders hat, bezieht sich auf ein Mittel, mit dem eine Person unter außergewöhnlichen Umständen schnell Administratorzugriff erhalten kann, indem ein zugelassenes und geprüftes Verfahren angewendet wird.

- Wenn Sie über On-Premises-Rechenzentren oder mehrere vCenter-Server-Instances verfügen, verwenden Sie den Hybrid Linked Mode, um Ihre Cloud-vCenter-Server-Instance mit der On-Premises-vCenter-Single-Sign-On-Domain zu verbinden. Auf diese Weise können Sie Ihre Cloud- und On-Premises-Ressourcen über eine einzige vSphere-Client-Oberfläche verwalten.
- Konfigurieren Sie nach Möglichkeit Verwaltungs-Endpunkte wie vCenter Server, HCX Cloud Manager und NSX Manager so, dass sie nur über interne Netzwerke und nicht über das öffentliche Internet zugänglich sind.
- Verwenden Sie keine lokalen Anmeldeinformationen wie das cloudadmin-Konto für administrative Zwecke. Reservieren Sie sich diese Konten für Ihr Break-Glass-Verfahren. Aktionen, die mit lokalen Administratorkonten ausgeführt werden, können keiner bestimmten Person zugeordnet werden, sodass diese Konten verwendet werden könnten, um Änderungen vorzunehmen, ohne dafür verantwortlich zu sein.
- Ändern Sie die Passwörter für lokale Konten wie Root- und Administratorkonten auf starke Werte und speichern Sie diese Anmeldeinformationen sicher in einem geprüften Passwortspeicher. Richten Sie ein Genehmigungsverfahren für die Gewährung des Zugriffs auf diese Passwörter ein.
- Wenn lokale Anmeldeinformationen über einen längeren Zeitraum, z. B. mehrere Monate oder länger, bestehen bleiben, richten Sie ein Verfahren ein, bei dem die Anmeldeinformationen rotiert werden (z. B. wenn Sie VMware HCX verwenden, um ein Netzwerk zu erweitern).

Diese Empfehlungen gelten für alle VMware-Dienstkonfigurationen für VMware Cloud on AWS. Zusätzliche Empfehlungen für die einzelnen Services werden später in diesem Handbuch behandelt.

VMware-Identitätsmanagement-Services

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Wenn Sie VMware Cloud on verwenden AWS, gibt es zwei Hauptdienste und Tools für die Identitäts- und Zugriffsverwaltung: VMware Cloud Services Console undVMware vCenter Server.

VMware Cloud Services Console

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Die VMware Cloud Services Console (VMware-Dokumentation) unterstützt Sie bei der Verwaltung Ihres VMware Cloud-Services-Portfolios, zu dem auch VMware Cloud on gehört AWS. In diesem Service können Sie:

- Entitäten wie Benutzer und Gruppen verwalten
- Organisationen verwalten, die den Zugriff auf andere Cloud-Services wie VMware Cloud Disaster Recovery (VCDR) und die VMware Aria Suite kontrollieren
- Weisen Sie Ressourcen und Services Rollen zu
- Sehen Sie sich die OAuth-Anwendungen an, die Zugriff auf Ihre Organisation haben
- Konfigurieren Sie den Unternehmensverbund für die Organisation
- Aktivieren und implementieren Sie VMware Cloud-Dienste wie VMware Aria und VMware Cloud on AWS
- Abrechnung und Abonnements verwalten

- VMware-Support erhalten

Identität und Zugriff verwalten

Durch die korrekte Einrichtung von Benutzern, Gruppen, Rollen und Organisationen in der VMware Cloud Services Console können Sie eine Zugriffsrichtlinie mit der geringsten Berechtigung implementieren.

Die Sicherung des Zugriffs auf die VMware Cloud Services Console ist von entscheidender Bedeutung, da Administratorbenutzer dieses Services die Berechtigungen in Ihrer gesamten VMware-Cloud-Umgebung ändern und auf vertrauliche Informationen wie Rechnungsinformationen zugreifen können. Um auf alle Konsolenfeatures wie Abrechnung und Support zugreifen zu können, müssen Benutzer außerdem mit einem VMware-Customer-Connect-Profil verknüpft sein (früher bekannt als MyVMware).

In der VMware Cloud Services Console verwenden Sie die folgenden Rollentypen, um Benutzern und Gruppen Berechtigungen zu erteilen:

- Rollen in der Organisation – Diese Rollen beziehen sich direkt auf die VMware-Cloud-Organisation und gewähren Berechtigungen innerhalb der VMware Cloud Services Console. Es gibt zwei Standardrollen. Die Rolle Inhaber der Organisation hat volle Rechte zur Verwaltung der Organisation. Die Rolle Mitglied der Organisation hat Lesezugriff auf die VMware Cloud Services Console. Weitere Informationen finden Sie unter Welche Organisationsrollen sind in VMware Cloud Services verfügbar (VMware-Dokumentation).
- Servicerollen – Mit diesen Rollen können Sie Berechtigungen für die Nutzung eines bestimmten Services zuweisen. Zum Beispiel kann eine Entität mit DR-Administrator-Servicerolle VMware Cloud Disaster Recovery (VCDR) in der dafür vorgesehenen Servicekonsole verwalten. Jedem innerhalb der Organisation verfügbaren Service sind eine oder mehrere Servicerollen zugeordnet. Weitere Informationen zu den verfügbaren Servicerollen finden Sie in der VMware-Dokumentation für den gewünschten Service.

Die VMware Cloud Services Console unterstützt Authentifizierungsrichtlinien. Diese können vorsehen, dass ein Benutzer bei der Anmeldung ein zweites Authentifizierungstoken angeben muss, auch bekannt als Multi-Faktor-Authentifizierung (MFA).

Weitere Informationen zum Verwalten von Identität und Zugriff in diesem Service erhalten Sie unter Identitäts- und Zugriffsverwaltung (VMware-Dokumentation).

AWS Empfehlungen

Zusätzlich zu den Allgemeine bewährte Methoden empfiehlt AWS Folgendes bei der Konfiguration der VMware Cloud Services Console für VMware Cloud in AWS:

- Verwenden Sie beim Erstellen einer Organisation ein VMware-Customer-Connect-Profil und die zugehörige Unternehmens-E-Mail-Adresse, die keiner Einzelperson gehört, z. B. vmwarecloudroot@example.com. Dieses Konto sollte als Service- oder Root-Konto behandelt werden, und Sie sollten die Nutzung überprüfen und den Zugriff auf das E-Mail-Konto einschränken. Konfigurieren Sie sofort den Kontoverbund mit Ihrem Identitätsanbieter (IDP), sodass Benutzer auf die Organisation zugreifen können, ohne dieses Konto zu verwenden. Reservieren Sie dieses Konto für die Verwendung in einem „Break Glass“-Verfahren zur Behebung von Problemen mit dem föderierten IdP.
- Verwenden Sie föderierte Identitäten für die Organisation, um Zugriff auf andere Cloud-Services wie VMware Cloud Disaster Recovery (VCDR) zu gewähren. Verwalten Sie Benutzer oder Verbände nicht einzeln in mehreren Services. Dies vereinfacht die Verwaltung des Zugriffs auf mehrere Services, z. B. wenn Benutzer dem Unternehmen beitreten oder es verlassen.
- Weisen Sie die Rolle Eigentümer der Organisation sparsam zu. Entitäten mit dieser Rolle können sich selbst vollen Zugriff auf alle Aspekte der Organisation und alle zugehörigen Cloud-Services gewähren.

VMware vCenter Server

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware vCenter Server (VMware-Website) ist eine Managementebene für die Verwaltung von VMware-vSphere-Umgebungen. In vCenter Server verwalten Sie die Entitäten, die auf vSphere-Ressourcen wie virtuelle Maschinen zugreifen können, und auf Add-Ons wie VMware HCX und VMware Site Recovery zugreifen können. Sie verwalten vCenter Server über die vSphere-Client-Anwendung. In vCenter Server können Sie:

- Virtuelle Maschinen, VMware-ESXi-Hosts und VMware-vSAN-Speicher verwalten

- vCenter Single Sign On konfigurieren und verwalten

Wenn Sie über On-Premises-Rechenzentren verfügen, können Sie den Hybrid-Linked-Mode verwenden, um Ihre Cloud-vCenter-Server-Instance mit einer On-Premises vCenter-Single-Sign-On-Domain zu verbinden. Wenn die vCenter-Single-Sign-On-Domain mehrere vCenter-Server-Instances enthält, die über den erweiterten verknüpften Modus verbunden sind, sind all diese Instances mit Ihrem Cloud-SDDC verknüpft. In diesem Modus können Sie Ihre On-Premises und Cloud-Rechenzentren von einer einzigen vSphere-Client-Oberfläche aus anzeigen und verwalten, und Sie können Workloads zwischen Ihrem On-Premises-Rechenzentrum und dem Cloud-SDDC migrieren. Weitere Informationen finden Sie unter Konfigurieren des verknüpften Hybrid-Modus (VMware-Dokumentation).

Identität und Zugriff verwalten

In softwaredefinierten Rechenzentren (SDDCs) (VMware-Website) für VMware Cloud on ähnelt die Art und Weise AWS, wie Sie vCenter Server betreiben, einem lokalen SDDC. Der Hauptunterschied besteht darin, dass es sich bei VMware Cloud on um einen verwalteten Dienst handelt. AWS Daher ist VMware für bestimmte Verwaltungsaufgaben verantwortlich, z. B. für die Verwaltung von Hosts, Clustern und die Verwaltung virtueller Maschinen. Weitere Informationen finden Sie unter Was ist in der Cloud anders? und Globale Berechtigungen (VMware-Dokumentation).

Da VMware einige Verwaltungsaufgaben für das SDDC ausführt, benötigt ein Cloud-Administrator weniger Rechte als ein Administrator eines On-Premises-Rechenzentrums. Wenn Sie eine VMware Cloud on AWS SDDC erstellen, wird automatisch ein cloudadmin-Benutzer erstellt und ihm wird die CloudAdminRolle zugewiesen (VMware-Dokumentation). Sie können dieses privilegierte, lokale Benutzerkonto für den Zugriff auf vCenter Server und vCenter Single Sign-On verwenden. Benutzer mit der Servicerolle VMware Cloud on AWS Administrator oder Administrator (Delete Restricted) in der VMware Cloud Services Console können die Anmeldeinformationen für den cloudadmin-Benutzer abrufen. Die CloudAdminRolle hat die maximal möglichen Berechtigungen in vCenter Server für eine VMware Cloud auf AWS SDDC. Weitere Informationen zu dieser Servicerolle finden Sie unter CloudAdmin Privilegien (VMware-Dokumentation). Der cloudadmin-Benutzer ist der einzige lokale Benutzer, der für vCenter Server in VMware Cloud in AWS verfügbar ist. Verwenden Sie eine externe Identitätsquelle, um anderen Benutzern Zugriff zu gewähren.

vCenter Single Sign-On ist ein Authentifizierungsbroker, der eine Infrastruktur für den Austausch von Sicherheitstoken bereitstellt. Wenn sich ein Benutzer bei vCenter Single Sign-On authentifiziert, erhält dieser Benutzer ein Token, mit dem er sich mithilfe von API-Aufrufen bei vCenter Server und anderen Zusatzservices authentifizieren kann. Der cloudadmin-Benutzer kann eine externe Identitätsquelle

für vCenter Server konfigurieren. Weitere Informationen finden Sie unter Identitätsquellen für vCenter Server mit vCenter Single Sign-On (VMware-Dokumentation).

In der VMware Cloud Services Console verwenden Sie drei Rollentypen, um Benutzern und Gruppen Berechtigungen zu erteilen:

- Systemrollen – Sie können diese Rollen nicht bearbeiten oder löschen.
- Beispielrollen – Diese Rollen stellen häufig ausgeführte Kombinationen von Aufgaben dar. Sie können diese Rollen kopieren, bearbeiten oder löschen.
- Benutzerdefinierte Rollen – Wenn die System- und Beispielrollen nicht die gewünschte Zugriffskontrolle bieten, können Sie benutzerdefinierte Rollen im vSphere Client erstellen. Sie können eine vorhandene Rolle duplizieren und ändern, oder Sie können eine neue Rolle erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine benutzerdefinierte vCenter-Server-Rolle (VMware-Dokumentation).

Für jedes Objekt im SDDC-Inventar können Sie einem Benutzer oder einer Gruppe nur eine Rolle zuweisen. Wenn ein Benutzer oder eine Gruppe für ein einzelnes Objekt eine Kombination von integrierten Rollen benötigt, gibt es zwei Optionen. Die erste Option ist die Erstellung einer benutzerdefinierten Rolle mit den erforderlichen Berechtigungen. Die andere Option besteht darin, zwei Gruppen zu erstellen, jeder Gruppe eine integrierte Rolle zuzuweisen und dann den Benutzer beiden Gruppen hinzuzufügen.

AWS Empfehlungen

Zusätzlich zu den Allgemeine bewährte Methoden empfiehlt AWS Folgendes bei der Konfiguration von vCenter Server für VMware Cloud in AWS:

- Verwenden Sie das cloudadmin-Benutzerkonto zur Konfiguration einer externen Identitätsquelle in vCenter Single Sign-On. Weisen Sie die entsprechenden Benutzer aus der externen Identitätsquelle zu, die für administrative Zwecke verwendet werden sollen, und beenden Sie dann die Verwendung von cloudadmin-Benutzer. Bewährte Methoden für die Konfiguration von vCenter Single Sign-On finden Sie unter Informationssicherheit und Zugriff für vCenter Server (VMware-Dokumentation).
- Aktualisieren Sie im vSphere Client die cloudadmin-Anmeldeinformationen für jede vCenter-Server-Instance auf einen neuen Wert, und speichern Sie sie dann sicher. Diese Änderung spiegelt sich nicht in der VMware Cloud Services Console wider. Wenn Sie beispielsweise die

Anmeldeinformationen über die Cloud Services Console anzeigen, wird der ursprüngliche Wert angezeigt.

> **Note**
>
> Wenn die Anmeldeinformationen für dieses Konto verloren gehen, kann der VMware-Support sie zurücksetzen.

- Verwenden Sie nicht das cloudadmin-Konto für den day-to-day Zugriff. Reservieren Sie dieses Konto für die Verwendung im Rahmen eines Break-Glass-Verfahrens.
- Beschränken Sie den Netzwerkzugriff auf vCenter Server auf nur private Netzwerke.

Verwandte VMware-Services

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Kapitel enthält bewährte Methoden und Empfehlungen für das Identitäts- und Zugriffsmanagement für die folgenden VMware-Dienste im Zusammenhang mit VMware Cloud on AWS:

- Services, die über VMware Cloud Services Console verwaltet werden:
  - VMware Cloud auf AWS
  - VMware NSX
  - VMware Aria Operations for Logs
  - VMware Aria Operations for Networks
  - VMware Aria Operations
  - VMware Cloud Disaster Recovery
- Services, die über VMware vCenter Server verwaltet werden:
  - VMware HCX
  - VMware Site Recovery

Dieses Handbuch enthält eine kurze Beschreibung der einzelnen Dienste, erläutert die Identitätszugriffs- und Verwaltungskontrollen für diesen Dienst und enthält AWS Empfehlungen für die Konfiguration dieses Dienstes als Teil von VMware Cloud on AWS.

VMware Cloud auf AWS

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware Cloud on AWS (VMware-Dokumentation) ist ein Service, der gemeinsam von VMware AWS und VMware entwickelt wurde, um Sie bei der Migration und Erweiterung Ihrer lokalen VMware vSphere-basierten Umgebungen auf die. AWS Cloud

Sie können AWS über die VMware Cloud Services Console auf VMware Cloud on zugreifen, wenn Sie zu einer Organisation gehören, die Zugriff auf diesen Service gewährt. In VMware Cloud on AWS können Sie:

- SDDCs erstellen und löschen.
- SDDC-Gruppen verwalten.
- SDDCs einschließlich Netzwerk- und Clusterparametern verwalten.
- Greifen Sie auf die cloudadmin-Benutzeranmeldeinformationen für VMware vCenter Server zu. Weitere Informationen zu diesem Benutzer finden Sie unter VMware vCenter Server in diesem Handbuch.
- Greifen Sie auf die cloudadmin-Benutzeranmeldeinformationen für VMware NSX zu. Weitere Informationen zu diesem Benutzer finden Sie unter VMware NSX in diesem Handbuch.
- Aktivieren und implementieren Sie Zusatzservices innerhalb von SDDCs, wie z. B. VMware Site Recovery und VMware HCX.
- Greifen Sie auf Konsolen für Zusatzservices zu, einschließlich HCX und VMware Site Recovery.

Identität und Zugriff verwalten

Sie verwenden die VMware Cloud Services Console, um Identitäten und den Zugriff auf VMware Cloud on AWS zu verwalten. Für VMware Cloud on sind AWS die folgenden Servicerollen verfügbar:

- Administrator — Diese Rolle hat vollen Zugriff auf VMware Cloud on AWS.

- Administrator (Delete Restricted) — Diese Rolle hat vollen Zugriff auf VMware Cloud on AWS, ausgenommen SDDC-Löschvorgänge.
- NSX-Cloud-Admin
- NSX-Cloud-Auditor

> **Note**
>
> NSX-Cloud-Admin und NSX-Cloud-Auditor stehen im Zusammenhang mit der Verwendung von VMware NSX. Weitere Informationen finden Sie unter VMware NSX.

Für den Zugriff auf ein SDDC im Cloud Services Portal ist eine der beiden Administrator-Rollen erforderlich. Benutzer ohne eine der beiden NSX-Cloud-Rollen können nicht auf die Registerkarte SDDC Networking and Security im Cloud Services Portal zugreifen und haben auch keinen Zugriff auf die NSX-Admin-Anmeldeinformationen.

AWS Empfehlungen

Zusätzlich zu den Allgemeine bewährte Methoden empfiehlt AWS Folgendes bei der Konfiguration von VMware Cloud in AWS:

- Um Administratoren eine Bewertung zu gewähren, verwenden Sie nur die Rolle Administrator (Löschen eingeschränkt). Reservieren Sie die Rolle Administrator für Break-Glass-Zugriff, wenn Sie ein SDDC löschen müssen.
- Erteilen Sie die NSX-Rollen nicht Benutzern, die keinen Zugriff auf Netzwerk- und Firewallkonfigurationen benötigen. Weitere Informationen finden Sie unter VMware NSX in diesem Handbuch.
- Ändern Sie die Passwörter für das lokale cloudadmin-Benutzerkonto auf einen sicheren Wert und speichern Sie diese Anmeldeinformationen sicher in einem geprüften Passwortspeicher. Sie können dieses Passwort in VMware vCenter Server mithilfe des vSphere Web Client ändern.

VMware NSX

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware NSX (VMware-Dokumentation) bietet eine Netzwerkvirtualisierungsebene, die das Open Systems Interconnection (OSI) -Modell von Schicht 2 bis Schicht 7 reproduziert und Feature wie Switching, Routing und Firewalls bietet. Es gibt zwei Versionen von NSX. Die Originalversion (NSX-V) erfordert, dass Sie auch vCenter Server bereitstellen. Die neuere Version (NSX-T) ist von vCenter Server entkoppelt, was die Unterstützung von Hybridarchitekturen ermöglicht. VMware Cloud on AWS verwendet NSX-T.

NSX ist zusammen mit vSphere und vSAN eine Kernkomponente von VMware Cloud on. AWS NSX stellt die gesamte Netzwerkfunktionalität innerhalb eines SDDC bereit und verwaltet die Interaktion zwischen dem Overlay-Netzwerk und den AWS systemeigenen Komponenten, die das Netzwerk-Underlay bilden. NSX ist eng mit anderen Services wie vCenter Server und VMware HCX verknüpft, die NSX-APIs zur Verwaltung von Ressourcen aufrufen.

Mit NSX können Sie:

- Switching und Routing verwalten
- Firewalls, einschließlich der Verwendung einer verteilten Firewall für die Inline-Inspektion zwischen virtuellen Maschinen oder zwischen dem Netzwerk und dem öffentlichen Internet verwalten
- Virtual Private Networks (VPNs) verwalten
- Das Dynamic Host Configuration Protocol (DHCP) und das Domain Name System (DNS) konfigurieren

Sie können über die VMware Cloud Services Console oder über die spezielle NSX Manager-Webbenutzeroberfläche (UI) auf NSX zugreifen. Die NSX-Manager-Web-UI bietet einige zusätzliche Features, die in VMware Cloud Services Console nicht verfügbar sind. Weitere Informationen finden Sie unter SDDC-Netzwerkadministration mit NSX Manager (VMware-Dokumentation).

Beachten Sie Folgendes, wenn Sie in VMware Cloud in AWS auf NSX zugreifen:

- Um über die VMware Cloud Services Console auf NSX zugreifen zu können, muss Ihnen die Rolle „VMware Cloud on Administrator“ zugewiesen worden sein. AWS Sie können auf NSX über die SDDC-Registerkarte Netzwerk und Sicherheit zugreifen. Weitere Informationen zu dieser Rolle finden Sie unter VMware Cloud auf AWS in diesem Handbuch.
- Sie können die Web-UI von NSX Manager öffnen, indem Sie den Link auf der Registerkarte SDDC-Einstellungen oder NSX Manager öffnen auf der Seite SDDC-Zusammenfassung wählen. Weitere Informationen finden Sie unter NSX Manager öffnen (VMware-Dokumentation).
- Wenn das SDDC im Modus Payment Card Industry Data Security Standard (PCI DSS) ist, können sie die Registerkarte Netzwerk und Sicherheit in VMware Cloud Services Console nicht öffnen. Sie müssen die NSX-Manager-Web-UI verwenden.

Identität und Zugriff verwalten

Sie verwenden VMware Cloud Services Console, um Identitäten und den Zugriff auf VMware NSX zu verwalten. Für NSX in VMware Cloud on sind AWS die folgenden Servicerollen verfügbar:

- NSX-Cloud-Admin – Diese Rolle kann die VMware NSX-Funktionalität mit VMware Cloud in AWS verwalten.
- NSX-Cloud-Auditor – Diese Rolle kann NSX-Serviceeinstellungen und -Ereignisse anzeigen, aber keine Änderungen vornehmen.

> **Note**
>
> Trotz ihrer Namen haben diese Rollen nichts mit dem VMware-NSX-Cloud-Service zu tun.

Die folgenden Benutzer können auf NSX zugreifen:

- Der lokale Benutzer cloud_admin, bei dem es sich um einen integrierten und hoch privilegierten lokalen NSX-Benutzer handelt. Benutzer, die Rolle NSX Cloud-Administrator haben, können auf die Anmeldeinformationen für dieses Benutzerkonto zugreifen. Trotz der ähnlichen Namen unterscheidet sich der Benutzer cloud_admin vom lokalen vCenter-Single-Sign-On-Benutzer cloudadmin@vmc.local.
- Anwender, denen entweder die Servicerolle NSX-Cloud-Admin oder die Service-Rolle NSX-Cloud-Auditor in VMware Cloud Services Console zugewiesen wurde. Bei diesen Benutzern kann es sich um Benutzer von VMware Cloud Services Console oder um externe Verbundbenutzer handeln.

- Benutzer, denen über LDAP direkt von einer Identitätsquelle aus Zugriff auf NSX gewährt wurde.

AWS Empfehlungen

Zusätzlich zu den Allgemeine bewährte Methoden empfiehlt AWS Folgendes bei der Konfiguration von NSX für VMware Cloud in AWS:

- Wenn Ihr Unternehmen Benutzer hat, die für die Verwaltung von Netzwerken und Firewalls, aber nicht für die Verwaltung von SDDCs verantwortlich sind, weisen Sie diesen Benutzern eine der NSX-Rollen zu, aber gewähren Sie ihnen nicht die Administrator-Rolle. Diese Benutzer sollten über die NSX-Manager-Web-UI auf NSX zugreifen.
- Ändern Sie die Passwörter für das lokale cloud_admin-Benutzerkonto auf einen sicheren Wert und speichern Sie diese Anmeldeinformationen sicher in einem geprüften Passwortspeicher. Um dieses Passwort zu ändern, müssen Sie sich an den VMware-Support wenden.
- Vermeiden Sie es, externen Benutzern direkt in NSX Zugriff zu gewähren. Richten Sie stattdessen den Unternehmensverbund in VMware Cloud Services Console ein und gewähren Sie dann mithilfe von Rollen und Gruppen Zugriff auf diesen Service.

VMware Aria Operations for Logs

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware Aria Operations for Logs (VMware-Dokumentation), früherVMware vRealize Log Insight Cloud, ist ein Protokollspeicher- und Analysetool, mit dem Sie die von Ihren VMware-SDDCs erzeugten Protokolldaten visualisieren und abfragen können. In VMware Aria Operations for Logs können Sie:

- Mit On-Premises-Instances von vRealize Operations integrieren
- Alle Arten von maschinengenerierten Protokolldaten sammeln und analysieren
- Konfigurieren von Warnungen
- Protokolle von anderen VMware-Services überwachen und analysieren

Es gibt zwei Versionen dieses zentralisierten Protokollverwaltungsservices. VMware vRealize Log Insight ist eine On-Premises-Version, die als Appliance in Ihrem SDDC ausgeführt werden kann. VMware Aria Operations for Logs ist eine software-as-a-service (SaaS-) Version. VMware Cloud on AWS verwendet die Cloud-Version als Standard-Protokollierungsdienst, und dies kann nicht geändert werden. Wenn Sie die On-Premises-Version verwenden, müssen Sie Protokolle von der Cloud-Instance an Ihre On-Premises-Instance weiterleiten.

VMware Aria Operations for Logs ist in VMware Cloud on enthalten AWS. Die mitgelieferte Version hat eine begrenzte Aufnahmekapazität und eine begrenzte Speicherdauer. Bei Bedarf können Sie auf ein Premium-Abonnement upgraden, um diese Limits zu erhöhen. Weitere Informationen finden Sie unter Abonnements und Abrechnung (VMware-Dokumentation).

Identität und Zugriff verwalten

Sie verwenden VMware Cloud Services Console, um Identitäten und den Zugriff auf VMware Aria Operations for Logs zu verwalten. VMware Aria Operations for Logs verwendet dieselben Benutzer, einschließlich föderierter Identitäten und Gruppen, die Sie in VMware Cloud Services Console konfiguriert haben. Um Berechtigungen für diesen Service zu gewähren, können Sie in VMware Aria Operations for Logs eine Servicerolle zuweisen oder eine benutzerdefinierte Rolle konfigurieren. Weitere Informationen finden Sie unter Servicerollen (VMware-Dokumentation).

VMware vRealize Log Insight hat zwei Standardrollen. Die Administrator-Rolle hat vollen Zugriff und volle Kontrolle, und die Benutzer-Rolle hat Lesezugriff und kann Dashboards erstellen. Sie können benutzerdefinierte Rollen verwenden, um nur Zugriff auf bestimmte Datensätze zu gewähren. Diese Datensätze enthalten Filter, die einschränken, welche Protokolldaten dem Benutzer zur Verfügung stehen. Weitere Informationen finden Sie unter Erstellen Sie einen Datensatz(VMware-Dokumentation).

AWS Empfehlungen

Halten Sie sich an die zuvor in diesem Leitfaden beschriebenen Allgemeine bewährte Methoden. Wir haben keine zusätzlichen Empfehlungen für die Identitäts- und Zugriffsverwaltung in diesem Service.

VMware Aria Operations for Networks

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware Aria Operations for Networks, früher VMware vRealize Network Insight Cloud, ist eine SaaS-Version von vRealize Network Insight. VMware vRealize Network Insight (VMware-Dokumentation) hilft Ihnen dabei, die Datenverkehrsflüsse für Ihre Workloads zu verstehen. Sie können diesen Service nutzen, um Netzwerkprobleme zu diagnostizieren und Firewall-Regeln zur Unterstützung der Workload-Segmentierung zu modellieren. In VMware Aria Operations for Networks können Sie:

- Sich Ihre Hybrid- und Multi-Cloud-Umgebungen ansehen
- Problembehandlung und Analyse von Verkehrsströmen durchführen
- Anwendungen erkennen und analysieren
- Abhängigkeiten zwischen Workloads zuordnen

Es gibt drei Versionen dieses Services. VMware vRealize Network Insight ist eine on-premises-only Version. VMware Aria Operations for Networks ist eine SaaS-Version. vRealize Network Insight Universal kann als On-Premises-Lösung oder als verbundene Cloud-SaaS-Lösung bereitgestellt werden. Alle Versionen sind mit VMware Cloud on AWS kompatibel.

Identität und Zugriff verwalten

Sie verwenden VMware Cloud Services Console, um Identitäten und den Zugriff auf VMware Aria Operations for Networks zu verwalten. VMware Aria Operations for Networks verwendet dieselben Benutzer, einschließlich föderierter Identitäten und Gruppen, die Sie in VMware Cloud Services Console konfiguriert haben. Für VMware Aria Operations for Networks sind die folgenden Servicerollen verfügbar:

- Administrator – Diese Rolle hat vollen Zugriff und volle Kontrolle.
- Mitglied – Diese Rolle hat eingeschränkten Zugriff.
- Auditor – Diese Rolle hat nur Lesezugriff.

AWS Empfehlungen

Halten Sie sich an die zuvor in diesem Leitfaden beschriebenen Allgemeine bewährte Methoden. Wir haben keine zusätzlichen Empfehlungen für die Identitäts- und Zugriffsverwaltung in diesem Service.

VMware Aria Operations

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware Aria Operations (VMware-Dokumentation), früher VMware vRealize Operations Cloud, ist eine Betriebsmanagement-Plattform für VMware Cloud in AWS. Dieser Service nutzt künstliche Intelligenz und Machine Learning (KI/ML), um Sie bei der Optimierung, Planung und Skalierung der Anwendungen und Infrastruktur in Ihren Hybrid-Cloud-Bereitstellungen zu unterstützen. In VMware Aria Operations können Sie:

- Sich KI/ML-gestützte Optimierungsempfehlungen für Leistung und Kapazität ansehen
- Konformitäts- und Ressourcenkonfigurationen verwalten
- Auf Tools zugreifen, die Sie bei der Behebung von Problemen unterstützen, z. B. bei der Lösung von Kundenproblemen oder der Reaktion auf Warnmeldungen
- Management Packs (VMware-Dokumentation) zur Erweiterung der Überwachungs-, Problembehebungs- und Abhilfefeatures dieses Services verwenden

Es gibt zwei Versionen dieses Betriebsverwaltungsservices. VMware vRealize Operations ist eine On-Premises-Version, die als Appliance in Ihrem SDDC ausgeführt werden kann. VMware Aria Operations ist eine software-as-a-service (SaaS-) Version von vRealize Operations. Beide Versionen sind mit VMware Cloud on AWS kompatibel. Da es sich bei VMware Cloud on um einen verwalteten Dienst AWS handelt und der Zugriff auf einige Ressourcen eingeschränkt ist, werden nicht alle Funktionen von vRealize Operations unterstützt. Weitere Informationen finden Sie unter Bekannte Einschränkungen(VMware-Dokumentation).

Identität und Zugriff verwalten

Sie verwenden VMware Cloud Services Console, um Identitäten und den Zugriff auf VMware Aria Operations zu verwalten. VMware Aria Operations verwendet dieselben Benutzer, einschließlich verbundener Identitäten und Gruppen, die Sie in VMware Cloud Services Console konfiguriert haben. Um Berechtigungen für diesen Service zu erteilen, können Sie eine Servicerolle zuweisen oder eine benutzerdefinierte Rolle in VMware Aria Operations konfigurieren. Weitere Informationen zu dieser Servicerolle erhalten Sie unter Rollen und Berechtigungen (VMware-Dokumentation).

Es gibt drei integrierte Rollen: Administrator ReadOnly, GeneralUserund bei Bedarf können Sie benutzerdefinierte Rollen erstellen, die bestimmten Berechtigungsanforderungen entsprechen. Sie können Gruppen erstellen, um den Verwaltungsaufwand für die Verwaltung von Berechtigungen für mehrere Benutzer zu minimieren.

Die On-Premises-Version von VMware vRealize Operations unterstützt lokale Benutzer, und sowohl die Cloud- als auch die On-Premises-Version unterstützen Verbundbenutzer. Der Verbund von Benutzern mit einem externen Identitätsanbieter variiert jedoch zwischen der On-Premises- und der Cloud-Version von vRealize Operations. Für die On-Premises-Version können Sie Benutzer von einem externen IdP direkt über LDAP verbinden, oder Sie können die Identitäten verwenden, die Sie in vCenter Server verbunden haben. Für die Cloud-Version verwenden Sie dieselben Benutzer, einschließlich Verbundbenutzer, die Sie in VMware Cloud Services Console konfigurieren.

AWS Empfehlungen

Zusätzlich zu den Allgemeine bewährte Methoden empfiehlt AWS Folgendes bei der Konfiguration von VMware Aria Operations für VMware Cloud in AWS:

- Vermeiden Sie es, Benutzer direkt zu verbinden. Für die Cloud-Version verbinden Sie Anwender in VMware Cloud Services Console und verwenden dann Rollen und Gruppen, um den Zugriff auf diesen Service zu gewähren. Verwenden Sie für die On-Premises-Version dieses Services Identitäten aus einer authentifizierten Quelle oder aktivieren Sie Single Sign-On (SSO). Weitere Informationen finden Sie unter Authentifizierungsquellen und Konfiguration einer Single-Sign-On-Quelle (VMware-Dokumentation).

VMware Cloud Disaster Recovery

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware Cloud Disaster Recovery (VCDR) (VMware-Dokumentation) ist eine DRaaS-Lösung (Disaster Recovery as a Service), die einen mehrstufigen Ansatz für die Notfallwiederherstellung bietet. Sie können die Kosten und den Zeitrahmen für Ihr Recovery Point Objective (RPO) und Recovery Time Objective (RTO) an die Anforderungen eines bestimmten Workloads anpassen. Auf diese Weise können Sie einen zuverlässigen Schutz und eine effiziente Nutzung von Notfallwiederherstellungs-Ressourcen in Einklang bringen. Mit VCDR können Sie:

- Backups von virtuellen Maschinen erstellen
- Backups in einem dauerhaften Cloud-Speicher speichern
- Zwischen flexiblen Bereitstellungsoptionen für Wiederherstellungsziele, von On-Demand bis hin zu Hot-Standby wählen
- Benutzerdefinierte RPOs und RTOs konfigurieren

Identität und Zugriff verwalten

Sie verwenden VMware Cloud Services Console, um Identitäten und den Zugriff auf VMware Cloud Disaster Recovery zu verwalten. VMware Cloud Disaster Recovery verwendet dieselben Benutzer, einschließlich föderierter Identitäten und Gruppen, die Sie in VMware Cloud Services Console konfiguriert haben. Um Berechtigungen für diesen Service zu erteilen, können Sie eine VCDR-Servicerolle zuweisen oder eine benutzerdefinierte Rolle in VMware Cloud Disaster Recovery konfigurieren. Weitere Informationen zu dieser Servicerolle erhalten Sie unter Rollen von VMware Cloud Disaster Recovery (VMware-Dokumentation).

VCDR umfasst mehrere integrierte Rollen, die Sie für den Betrieb des Services verwenden können:

- Administrator – Vollständige Kontrolle, ausgenommen Zugriff auf API-Token.
- Auditor – Schreibgeschützter Zugriff auf die Benutzeroberfläche, ausgenommen Benutzerverwaltung. Zugriff auf Konformitätsberichte.

- DR-Admin – Notfallwiederherstellungspläne erstellen, testen und ausführen.
- Backup-Admin – Verwaltet geschützte Sites und Schutzgruppen. Zugriff für die Wiederherstellung von VMs.
- Plantester – Erstellt Notfallwiederherstellungspläne und führt Testwiederherstellungen durch.
- SDDC-Admin – Verwaltet SDDCs.

AWS Empfehlungen

Halten Sie sich an die zuvor in diesem Leitfaden beschriebenen Allgemeine bewährte Methoden. Wir haben keine zusätzlichen Empfehlungen für die Identitäts- und Zugriffsverwaltung in diesem Service.

VMware HCX

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware HCX (VMware-Dokumentation) ist eine Plattform für Anwendungsmobilität, die Workload-Migrationen zwischen SDDCs ermöglicht. VMware HCX ist in VMware Cloud on enthalten AWS und kann zur Migration von Workloads verwendet werden. Mit VMware HCX können Sie:

- Multi-Site-Meshes zwischen SDDCs konfigurieren
- Netzwerke zwischen HCX-Standorten erweitern
- Virtuelle Maschinen migrieren

Identität und Zugriff verwalten

Sie verwenden VMware vCenter Server, um Identitäten und den Zugriff auf VMware HCX zu verwalten. VMware HCX benötigt Zugriff auf andere VMware-Services, um Ressourcen und Migrationen zu erstellen und zu verwalten, einschließlich Zugriff auf vCenter Server und NSX. VMware HCX besteht aus zwei Komponenten:

- HCX Cloud Manager – In VMware Cloud Services Console aktivieren Sie VMware HCX für das SDDC. Dadurch wird die HCX-Cloud-Manager-Appliance im ausgewählten SDDC installiert. Weitere Informationen finden Sie unter Bereitstellen der HCX Installer OVA im vSphere-Client (VMware-Dokumentation). Nach der Bereitstellung können Sie die vCenter Server cloudadmin-Anmeldeinformationen für den Zugriff auf den HCX-Cloud-Manager-Service verwenden.
- HCX-Anschluss – Sie können die HCX Connector Open Virtualization Archive (OVA)-Datei über den HCX-Cloud-Manager-Service abrufen. Sie verwenden diese Datei, um eine HCX-Cloud-Manager-Appliance auf einer beliebigen vCenter-Server-Instance zu installieren, wodurch diese Instance als Migrationsquelle in VMware HCX eingerichtet wird. Jede HCX-Connector-Instance hat ihre eigenen Administrator- und Root-Anmeldeinformationen.

Nachdem Sie beide Komponentenservices bereitgestellt haben, können Sie über vCenter Server auf VMware HCX zugreifen. Die Gruppe Administratoren vCenter Single Sign-On erhält automatisch die Rolle HCX-Administrator. Durch die Installation von HCX werden vCenter Single Sign-On viele zusätzliche Rollen und Rechte hinzugefügt. Verwenden Sie diese, um detaillierte Zugriffskontrollen für VMware HCX zu erstellen, die auf den verschiedenen Benutzertypen basieren.

AWS Empfehlungen

Zusätzlich zu den Allgemeine bewährte Methoden empfiehlt AWS Folgendes bei der Konfiguration von VMware HCX für VMware Cloud in AWS:

- Verwenden Sie die Gateway-Firewall-Regeln, um den Netzwerkzugriff auf den HCX-Cloud-Manager-Service einzuschränken.
- Speichern Sie die Admin- und Root-Benutzer-Anmeldeinformationen von HCX Connector sicher On-Premises. Erwägen Sie, diese Anmeldeinformationen entsprechend Ihren Unternehmensrichtlinien zu rotieren. VMware verwaltet diese Anmeldeinformationen in Ihrem Namen für HCX Cloud Manager.
- Für eine On-Premises-HCX-Connector-Instance sollten Sie erwägen, benutzerdefinierte HCX-Rollen zu erstellen, die den Anforderungen Ihrer verschiedenen HCX-Benutzertypen entsprechen. Erstellen Sie beispielsweise eine tolerantere Rolle für Benutzer, die HCX einrichten und verwalten, und eine weniger freizügige Rolle für Benutzer, die nur Migrationen verwalten.
- Wenn Sie VMware HCX mit VMware Cloud on koppeln AWS, müssen Sie den Benutzer cloudadmin verwenden. Weitere Informationen finden Sie im Abschnitt Auflösung von HCX — Konnektivitätsdiagnose bei der Standortkopplung (VMware Knowledge Base-Artikel 78340).

- Bei der Kopplung von HCX Cloud mit VMware Cloud on AWS wird die Authentifizierung zwischen VMware Cloud on AWS SDDC und Active Directory nicht unterstützt. Weitere Informationen finden Sie unter [VMC auf AWS] AD wird für die HCX-Cloud-zu-Cloud-Einrichtung nicht unterstützt (VMware Knowledge Base Artikel 90433).

VMware Site Recovery

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware Site Recovery (VMware-Dokumentation) ist eine On-Demand-Lösung für Notfallwiederherstellung as a Service (DRaaS), die auf dem Service VMware Site Recovery Manager für On-Premises-Umgebungen basiert. In VMware Site Recovery können Sie:

- Replikation, Orchestrierung und Automatisierung, um Workloads im Falle eines Standortausfalls zu schützen, implementieren
- Erstellen Sie eine end-to-end Disaster-Recovery-Lösung zum Schutz von SDDCs

Identität und Zugriff verwalten

Sie verwenden VMware vCenter Server, um Identitäten und den Zugriff auf VMware Site Recovery zu verwalten. VMware Site Recovery führt Operationen im Namen von Benutzern durch, z. B. das Replizieren oder Ausschalten einer virtuellen Maschine. Site Recovery verwendet Rollen und Rechte, um sicherzustellen, dass nur Benutzer mit den richtigen Berechtigungen Wiederherstellungsvorgänge durchführen können, z. B. die Ausführung aller Schritte eines Wiederherstellungsplans.

Für Site Recovery sind die folgenden Servicerollen verfügbar:

- SrmAdministrator— Diese Rolle kann alle Konfiguration und Verwaltung von Site Recovery ausführen.
- HmsCloudAdmin— Diese Rolle kann Server auflisten, sie kann sie jedoch nicht hinzufügen oder entfernen.

Wenn Sie Site Recovery in VMware Cloud on einrichten AWS, werden die folgenden Benutzergruppen-Updates automatisch konfiguriert:

1. Eine neue SRM-Administratorgruppe wird erstellt und ihr wird die SrmAdministratorRolle zugewiesen.
2. Eine neue HmsCloudAdministratorsGruppe wird erstellt und ihr wird die HmsCloudAdminRolle zugewiesen.
3. Die CloudAdminGroupGruppe wird sowohl der Gruppe SRM-Administratoren als auch der HmsCloudAdministratorsGruppe hinzugefügt. Dies bietet der CloudAdminGroupGruppe transitive Berechtigungen zur Verwaltung von Site Recovery Manager und vSphere Replication.

Weitere Informationen finden Sie unter Erfahren Sie mehr über die Konfiguration von Berechtigungen für VMware Site Recovery (VMware-Dokumentation).

Wenn Sie Verbundidentitäten für den Zugriff auf vCenter Server verwenden, müssen Sie den verknüpften Hybrid-Modus verwenden, um diesen Gruppen Entitäten hinzuzufügen. Weitere Informationen finden Sie unter Konfigurieren des verknüpften Hybrid-Modus (VMware-Dokumentation).

AWS Empfehlungen

Zusätzlich zu denAllgemeine bewährte Methoden empfiehlt AWS Folgendes bei der Konfiguration von Site Recovery für VMware Cloud in AWS:

- Stellen Sie sicher, dass den Benutzern sowohl auf den Quell- als auch auf der Zielsites dieselben Rollen zugewiesen werden. Dadurch wird sichergestellt, dass geschützte und wiederhergestellte Objekte über identische Berechtigungen verfügen.
- Verwenden Sie den verknüpften Hybrid-Modus, um Site Recovery-Rollenzuweisungen für verbundene Identitäten innerhalb von vCenter Server zu verwalten.
- Site Recovery verwendet private IP-Adressen nur innerhalb des SDDC. In Übereinstimmung mit Allgemeine bewährte Methoden stellen Sie sicher, dass Ihr vCenter von VMware Cloud in AWS auf eine private IP-Adresse aufgelöst wird.

Beispielgruppen und -rollen

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Die folgende Tabelle enthält ein Beispiel für eine Strategie zur Identitäts- und Zugriffsverwaltung für die Verwendung von VMware Cloud in AWS. Es beschreibt die Benutzerpersona, die VMware-Services, auf die die Persona zugreifen muss, die Organisations- und Gruppenmitgliedschaft, die zugewiesenen Rollen und die Art der verwendeten Identität (z. B. lokale Benutzer oder verbundene Identitäten). Verwenden Sie diese Tabelle als Ausgangspunkt, um eine Strategie für Ihr Unternehmen zu entwerfen, die den in diesem Leitfaden empfohlenen bewährten Methoden entspricht.

Benutzerpersona	Abgerufene Services	Name der VMware-Cloud-Beispielgruppe	VMware-Cloud-Servicerollen	vCenter-Single-Sign-On-Beispielgruppenname	vCenter-Single-Sign-On-Rolle	Identitätsquelle
Organisation Break Glass	VMware Cloud Services Console	None	Inhaber der Organisation	Keine	None	Lokaler Benutzer (E-Mail-Adresse des Servicekontos)
VMware-Administrator	VMware Cloud Services Console vCenter Server	`vmware_admins`	Inhaber der Organisation	`vmware_admins`	Administrator	Anbieter von Verbund-Identitäten

Benutzerpersona	Abgerufene Services	Name der VMware-Cloud-Beispielgruppe	VMware-Cloud-Servicerollen	vCenter-Single-Sign-On-Beispielgruppenname	vCenter-Single-Sign-On-Rolle	Identitätsquelle
	HCX Wiederherstellung der Site VCDR vRealize Operations					
Backup-Administrator	vCenter Server	Keine	None	`vmware_backups`	Hauptbenutzer	Anbieter von Verbund-Identitäten
Administrator für Notfallwiederherstellung	vCenter Server VMware Cloud Services Console Wiederherstellung der Site VCDR	`vmware_dr`	Mitglied der Organisation DR-Admin DR-SDDC-Administrator	`vmware_dr`	SrmAdministrator HmsCloudAdmin	Anbieter von Verbund-Identitäten

Benutzerpersona	Abgerufene Services	Name der VMware-Cloud-Beispielgruppe	VMware-Cloud-Servicerollen	vCenter-Single-Sign-On-Beispielgruppenname	vCenter-Single-Sign-On-Rolle	Identitätsquelle
VMware-Betreiber	VMware Cloud Services Console vCenter Server HCX vRealize Operations	`vmware_ops`	Mitglied der Organisation vROps-Administrator	`vmware_ops`	Hauptbenutzer	Anbieter von Verbund-Identitäten
Netzwerkteam	VMware Cloud Services Console vCenter Server	`vmware_networks`	Mitglied der Organisation NSX-Cloud-Admin	`vmware_networks`	Readonly	Anbieter von Verbund-Identitäten

Benutzerpersona	Abgerufene Services	Name der VMware-Cloud-Beispielgruppe	VMware-Cloud-Servicerollen	vCenter-Single-Sign-On-Beispielgruppenname	vCenter-Single-Sign-On-Rolle	Identitätsquelle
Sicherheitsteam	VMware Cloud Services Console vCenter Server HCX (Temporärer Zugriff) Wiederherstellung der Site VCDR vRealize Operations	`vmware_security`	Mitglied der Organisation VROps ReadOnly	`vmware_security`	Readonly	Anbieter von Verbund-Identitäten
Auditoren	VMware Cloud Services Console vCenter Server	`vmware_audit`	Mitglied der Organisation	`vmware_audit`	Readonly	Anbieter von Verbund-Identitäten

Nächste Schritte

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

In diesem Leitfaden wurden die bewährten Methoden behandelt, die wir für die Identitäts- und Zugriffsverwaltung für VMware Cloud on AWS und verwandte VMware-Dienste empfehlen. Diese Empfehlungen sollen Ihnen helfen, Ihre Cloud- und Hybrid-Cloud-Infrastruktur zu schützen und unbefugten Zugriff zu verhindern. Sie sind aber auch so konzipiert, dass sie skalierbar und effizient sind. Durch das Zuweisen von Benutzern zu Gruppen und das anschließende Zuweisen von Rollen zu Gruppen können Sie schneller Berechtigungen gewähren oder einschränken und den Aufwand minimieren, der mit der individuellen Konfiguration von Benutzern verbunden ist. Durch die Verwendung eines Verbunds mit einem externen Identitätsanbieter und vCenter Single Sign-On können Sie Ihren Benutzern außerdem ein nahtloses Single-Sign-On-Erlebnis bieten.

Verwenden Sie die Beispielgruppen und -rollen-Tabelle, um mit der Entwicklung einer Identitäts- und Zugriffsmanagementstrategie zu beginnen, die für Ihr Unternehmen geeignet ist. Nachdem Sie die Empfehlungen in diesem Leitfaden gelesen haben, empfehlen wir Ihnen, die im Abschnitt Ressourcen bereitgestellten Links zu lesen. Diese Ressourcen helfen Ihnen dabei, mehr über die Cloud-Services von VMware und die Konfiguration der in diesem Handbuch beschriebenen bewährten Methoden zu erfahren.

Ressourcen

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Verwandte AWS Ressourcen

- AWS Überblick und Betriebsmodell von VMware Cloud
- Optionen zur Notfallwiederherstellung für Workloads auf VMware Cloud on AWS
- Konfiguration von Speicher-Offload-Optionen für VMware Cloud on AWS
- Stellen Sie mithilfe von VMware Cloud on AWS ein VMware-SDDC bereit AWS
- Migrieren Sie VMware SDDC auf VMware Cloud unter Verwendung von VMware HCX AWS

VMware-Dokumentation

VMware Cloud auf AWS

- Einrichten von Unternehmensverbund für Cloud-Services
- VMware Cloud Services Identity and Access Management

VMware vCenter Server und vCenter Single Sign-On

- Autorisierung in vSphere verstehen
- vSphere-Verwaltung in VMware Cloud auf AWS
- vSphere-Authentifizierung mit vCenter Single Sign-On
- Konfiguration von Identitätsquellen für vCenter Single Sign-On
- Hierarchische Vererbung von Berechtigungen
- Informationssicherheit und Zugriff für vCenter Server
- Erforderliche vSphere-Berechtigungen für allgemeine Aufgaben

VMware NSX

- NSX-Administrationshandbuch
- Informationssicherheit und Zugriff für NSX-T Data Center

VMware HCX

- Benutzerhandbuch für VMware HCX
- Anforderungen an das Benutzerkonto und Rolle für VMware HCX

VMware Aria und vRealize Suite

- Dokumentation zu VMware vRealize Operations
- Rollen und Berechtigungen in vRealize Operations Cloud
- Datenblatt zu VMware vRealize Log Insight
- Erste Schritte mit VMware Aria Operations for Logs
- Leitfaden für VMware Cloud Services
- Benutzerverwaltung in vRealize Network Insight

VMware Site Recovery

- Dokumentation zu VMware Site Recovery
- Rechte, Rollen und Berechtigungen für Site Recovery Manager
- Konfiguration der Berechtigungen für VMware Site Recovery bei VMware Cloud auf AWS

VMware Cloud Disaster Recovery

- Benutzerrollen in VMware Cloud Disaster Recovery

Dokumentverlauf

> **Notice (Hinweis)**
>
> Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Zugriff auf VMware HCX	Wir haben die AWS Empfehlungen für die Konfiguration von VMware HCX für VMware Cloud on AWS aktualisiert.	5. Juni 2023
Erste Veröffentlichung	—	03. November 2022

AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-kompatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2-Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung von AIOps in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Betriebsintegration.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den

öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Cloud-Einführung (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue

Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, die als bösartige Bots bezeichnet werden, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er normalerweise keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen

- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oder AWS CodeCommit. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil

der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Abweichung zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen an historischen Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto

wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder Malware-Angriffe.

Notfallwiederherstellung (DR)

Die Strategie und der Prozess, die Sie zur Minimierung von Ausfallzeiten und Datenverlusten aufgrund einer Katastrophe anwenden. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.
- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu

finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit:AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

FGAC

Weitere Informationen finden Sie unter detaillierter Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

G

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

Industrielles Internet der Dinge (IIoT)

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in derselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für Machine Learning mit AWS.

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

Niedrigere Umgebungen

Siehe Umwelt.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementierung von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Weitere Informationen finden Sie unter Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration

von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Erstellen eines Pfads für eine Organisation.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ODER

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Mit diesen Steuerelementen werden Ressourcen gescannt, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

veröffentlichen/abonnieren (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldeinformationen, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPs definieren Integritätsschutz oder legen Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Services oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, wohingegen Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie

unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der AWS Transit Gateway Dokumentation unter Was ist ein Transit-Gateway.

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems gefährdet.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur gilt als unveränderlich.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

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.