Administratorhandbuch

Amazon WorkSpaces Web

Amazon WorkSpaces Web: Administratorhandbuch

Table of Contents

Was ist Amazon WorkSpaces Web? 1
Begriffe, die Sie bei der Verwendung von WorkSpaces Web beachten sollten 1
Zugehörige Services 3
Architektur 3
Zugriff auf Amazon WorkSpaces Web 4
Einrichten von Amazon WorkSpaces Web 5
Registrieren und Erstellen eines Benutzers 5
So melden Sie sich für ein AWS-Konto an 5
Erstellen eines Administratorbenutzers 6
Erteilen programmgesteuerten Zugriffs 7
Netzwerk und Zugriff 8
VPC-Anforderungen 9
Empfehlungen zur VPC-Einrichtung 21
Unterstützte Availability Zones 22
VPC-Verbindung 24
Client/Benutzer-Verbindung 25
Erste Schritte mit Amazon WorkSpaces Web 28
Schritt 1: Ein Webportal erstellen 28
Konfigurieren von Netzwerkeinstellungen 29
Portaleinstellungen konfigurieren 29
Benutzereinstellungen konfigurieren 31
Identitätsanbieter konfigurieren 32
Überprüfen und starten 43
Schritt 2: Ihr Webportal testen 44
Schritt 3: Ihr Webportal verteilen 44
Nächste Schritte 45
Verwalten Ihres Webportals 46
Webportal-Details anzeigen 46
Ein Webportal bearbeiten 46
Ein Webportal löschen 47
Eine Erhöhung des Service-Kontingents anfordern 47
Das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens steuern 49
Benutzerzugriffsprotokollierung einrichten 50
Beispielprotokolle 51

Ihre Browser-Richtlinie festlegen oder bearbeiten ... 53
Eine benutzerdefinierte Browser-Richtlinie festlegen (Beispiel) ... 53
Bearbeiten Sie die grundlegende Browser-Richtlinie ... 60
Den Eingabemethoden-Editor (IME) konfigurieren ... 61
Die sitzungsinterne Lokalisierung konfigurieren ... 62
IP-Zugriffskontrollen einrichten (optional) ... 65
Eine IP-Zugriffskontrollgruppe erstellen ... 66
Eine IP-Zugriffseinstellung einem Webportal zuordnen ... 67
Eine IP-Zugriffskontrollgruppe bearbeiten ... 68
Einer IP-Zugriffskontrollgruppe löschen ... 68
Erweiterung für Single-Sign-On aktivieren (optional) ... 69
URL-Filterung einrichten ... 71
Sicherheit ... 73
Datenschutz ... 74
Datenverschlüsselung ... 75
Datenschutz für den Datenverkehr zwischen Netzwerken ... 77
Benutzerzugriffsprotokollierung ... 77
Identitäts- und Zugriffsverwaltung ... 78
Zielgruppe ... 78
Authentifizierung mit Identitäten ... 79
Verwalten des Zugriffs mit Richtlinien ... 83
Funktionsweise von Amazon WorkSpaces Web mit IAM ... 86
Beispiele für identitätsbasierte Richtlinien ... 93
Von AWS verwaltete Richtlinien ... 96
Fehlerbehebung ... 104
Verwenden von serviceverknüpften Rollen ... 107
Vorfallreaktion ... 110
Compliance-Validierung ... 111
Ausfallsicherheit ... 112
Sicherheit der Infrastruktur ... 113
Konfigurations- und Schwachstellenanalyse ... 113
Bewährte Methoden für die Gewährleistung der Sicherheit ... 114
Überwachen ... 116
Überwachung mit CloudWatch ... 117
CloudTrail-Protokolle ... 118
Amazon-WorkSpaces-Web-Informationen in CloudTrail ... 119

Erläuterungen der Amazon-WorkSpaces-Web-Protokolldateieinträge 120
Benutzerzugriffsprotokollierung 122
Anleitung für Amazon WorkSpaces Web-Benutzer 123
Browser- und Gerätekompatibilität 123
Zugriff auf das Webportal 124
Anleitung zur Sitzung 124
Starten einer Sitzung 124
Die Symbolleiste verwenden 125
Den Browser verwenden 127
Beenden einer Sitzung 127
Fehlerbehebung 128
Erweiterung für Single Sign-On 129
Kompatibilität 130
Installation 130
Fehlerbehebung 130
Dokumentverlauf 131
..... cxxxv

Was ist Amazon WorkSpaces Web?

Amazon WorkSpaces Web ist ein vollständig verwalteter, auf Linux basierter On-Demand-Service, der den sicheren Browserzugriff auf interne Websites und Software-as-a-Service-Anwendungen (SaaS-Anwendungen) ermöglicht. Greifen Sie von vorhandenen Webbrowsern aus auf den Service zu, ohne den Verwaltungsaufwand für Infrastrukturmanagement, spezielle Clientsoftware oder Lösungen für Virtual Private Network (VPN).

Themen

- Begriffe, die Sie bei der Verwendung von WorkSpaces Web beachten sollten
- Zugehörige Services
- Architektur
- Zugriff auf Amazon WorkSpaces Web

Begriffe, die Sie bei der Verwendung von WorkSpaces Web beachten sollten

Bevor Sie beginnen, mit WorkSpaces Web zu arbeiten, sollten Sie sich mit den folgenden Konzepten vertraut machen.

Identity provider (IdP) (Identitätsanbieter (IdP))

Ein Identitätsanbieter verifiziert die Anmeldeinformationen Ihrer Benutzer. Er stellt dann die Authentifizierungszusicherungen aus, um Zugriff auf einen Dienstanbieter bereitzustellen. Sie können Ihren vorhandenen Identitätsanbieter so konfigurieren, dass er mit WorkSpaces Web kompatibel ist.

Der Prozess zur Konfiguration Ihres Identitätsanbieters (IDP) variiert je nach Identitätsanbieter.

Sie müssen die Metadatendatei des Dienstanbieters zu Ihrem Identitätsanbieter hochladen. Andernfalls können sich Ihre Benutzer nicht anmelden. Sie müssen Ihren Benutzern in Ihrem Identitätsanbieter Zugriff auf die Nutzung von WorkSpaces Web gewähren.

Metadatendokument des Identitätsanbieters

WorkSpaces Web benötigt spezifische Metadaten von Ihrem Identitätsanbieter (IDP), um eine Vertrauensstellung aufzubauen. Sie können diese Metadaten zu WorkSpaces Web hinzufügen,

indem Sie eine von Ihrem Identitätsanbieter heruntergeladene Metadaten-Austauschdatei hochladen.

Dienstanbieter (Service Provider, SP)

Ein Dienstanbieter akzeptiert Authentifizierungsbestätigungen und stellt dem Benutzer einen Service zur Verfügung. WorkSpaces Web fungiert als Dienstanbieter für Benutzer, die von ihrem Identitätsanbieter authentifiziert wurden.

Dienstanbieter-Metadatendokument

Sie müssen die Metadatendetails des Dienstanbieters zur Konfigurationsoberfläche Ihres Identitätsanbieters hinzufügen. Die Einzelheiten dieses Konfigurationsprozesses variieren je nach Anbieter.

SAML 2.0

Ein Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen einem IdP und einem Dienstanbieter.

Virtual Private Cloud (VPC)

Sie können eine vorhandene oder neue VPC, entsprechende Subnetze und Sicherheitsgruppen verwenden, um Ihren Inhalt mit WorkSpaces Web zu verknüpfen.

Subnetze müssen über eine stabile Internetverbindung verfügen. Außerdem müssen die VPC und die Subnetze über eine stabile Verbindung mit allen internen Websites und Websites für Software as a Service (SaaS) verfügen, damit Benutzer auf diese Ressourcen zugreifen können.

Die aufgelisteten VPCs, Subnetze und Sicherheitsgruppen stammen aus derselben Region wie Ihre WorkSpaces-Web-Konsole.

Trust Store (Vertrauensspeicher)

Wenn ein Benutzer, der über WorkSpaces Web auf eine Website zugreift, einen Datenschutzfehler wie NET::ERR_CERT_INVALID erhält, verwendet diese Website möglicherweise ein Zertifikat, das von einer privaten Zertifizierungsstelle (PCA) signiert wurde. Möglicherweise müssen Sie die PCAs in Ihrem Trust Store hinzufügen oder ändern. Wenn Sie auf dem Gerät eines Benutzers ein bestimmtes Zertifikat installieren müssen, um eine Website zu laden, müssen Sie dieses Zertifikat außerdem zu Ihrem Trust Store hinzufügen, damit Ihr Benutzer in WorkSpaces Web auf diese Website zugreifen kann.

Für öffentlich zugängliche Websites sind in der Regel keine Änderungen an einem Trust Store erforderlich.

Webportale

Ein Webportal bietet Ihren Benutzern über ihren Browser Zugriff auf interne Websites und SaaS-Websites. Sie können in jeder unterstützten Region ein Webportal pro Konto erstellen. Wenn Sie eine Limiterhöhung für mehr als ein Portal anfordern möchten, wenden Sie sich an den Support.

Webportal-Endpunkt

Der Webportal-Endpunkt ist der Zugangspunkt, von dem aus Ihre Benutzer Ihr Webportal starten, nachdem sie sich mit dem für das Portal konfigurierten Identitätsanbieter angemeldet haben.

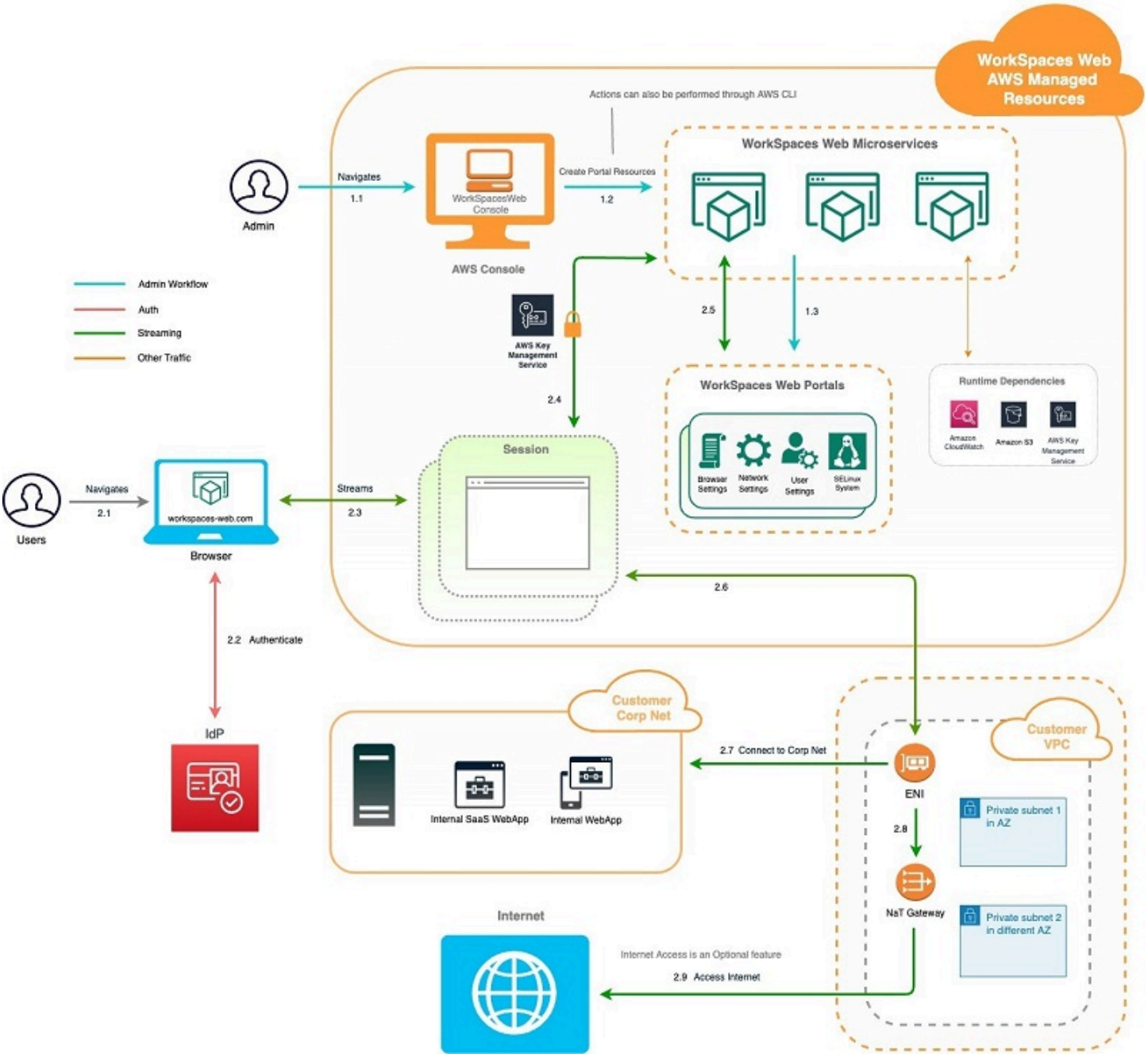
Der Endpunkt ist öffentlich im Internet verfügbar und kann in Ihr Netzwerk eingebettet werden.

Zugehörige Services

WorkSpaces Web ist eine Funktion von Amazon WorkSpaces im AWS-Endbenutzer-Computing-Portfolio. Im Vergleich zu WorkSpaces und AppStream 2.0 wurde WorkSpaces Web speziell für sichere, webbasierte Workloads entwickelt. WorkSpaces Web wird automatisch verwaltet, wobei Kapazität, Skalierung und Images bei Bedarf von AWS bereitgestellt und aktualisiert werden. Sie können beispielsweise Ihren Softwareentwicklern, die Zugriff auf Desktop-Ressourcen benötigen, einen persistenten Workspace-Desktop und den Contact-Center-Benutzern, die nur Zugriff auf eine Handvoll interner Websites und SaaS-Websites (einschließlich solcher, die außerhalb Ihres Netzwerks gehostet werden) auf Desktop-Computern benötigen, Amazon WorkSpaces Web anbieten.

Architektur

Das folgende Diagramm zeigt die WorkSpaces Web-Architektur.



Zugriff auf Amazon WorkSpaces Web

Administratoren greifen über die AWS-WorkSpaces-Web-Konsole, das SDK, die CLI oder die API auf Amazon WorkSpaces Web zu. Ihre Benutzer greifen über den Amazon-WorkSpaces-Web-Endpunkt darauf zu.

Einrichten von Amazon WorkSpaces Web

Bevor Sie Amazon WorkSpaces Web so konfigurieren können, dass es Ihre internen Websites und SaaS-Anwendungen erreicht, müssen Sie die folgenden Voraussetzungen erfüllen.

Themen

- Registrieren und Erstellen eines Benutzers
- Erteilen programmgesteuerten Zugriffs
- Netzwerk und Zugriff

Registrieren und Erstellen eines Benutzers

So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

Nachdem Sie sich für ein AWS-Kontoangemeldet haben, sichern Sie Ihr Root-Benutzer des AWS-Kontos, aktivieren Sie AWS IAM Identity Centerund erstellen Sie einen administrativen Benutzer, damit Sie nicht den Root-Benutzer für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console als Kontobesitzer an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto-E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-AnmeldungBenutzerhandbuch zu .
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen dazu finden Sie unter Aktivieren eines virtuellen MFA-Geräts für den Root-Benutzer Ihres AWS-Konto (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren von IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Im IAM Identity Center gewähren Sie einem administrativen Benutzer administrativen Zugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit dem standardmäßigen IAM-Identity-Center-Verzeichnis konfigurieren im AWS IAM Identity Center-Benutzerhandbuch.

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM-Identity-Center-Benutzer finden Sie unter Anmelden beim AWS-Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmgesteuerten Zugriff, wenn sie außerhalb der AWS Management Console mit AWS interagieren möchten. Die Vorgehensweise, um programmgesteuerten Zugriff zu gewähren, hängt davon ab, welcher Benutzertyp auf zugreift AWS.

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Konfigurieren der AWS CLI für die Verwendung von AWS IAM Identity Center im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs, Tools und AWS-APIs finden Sie unter IAM-Identity-Center-Authentifizierung im Referenzhandbuch zu AWS-SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS-Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Authentifizierung mit IAM-Benutzer-Anmeldeinformationen im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs und Tools finden Sie unter Authentifizierung mit langfristigen Anmeldeinformationen im Referenzhandbuch zu AWS-SDKs und Tools. • Informationen zu AWS-APIs finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Netzwerk und Zugriff

In den folgenden Themen wird erläutert, wie Sie WorkSpaces Web-Streaming-Instances einrichten, damit Benutzer eine Verbindung zu ihnen herstellen können. Außerdem wird erläutert, wie Sie Ihren WorkSpaces Web-Streaming-Instances den Zugriff auf VPC-Ressourcen sowie das Internet ermöglichen.

Themen

• VPC-Anforderungen

- Empfehlungen zur VPC-Einrichtung
- Unterstützte Availability Zones
- VPC-Verbindung
- Client/Benutzer-Verbindung

VPC-Anforderungen

Während der Erstellung des WorkSpaces Webportals wählen Sie eine VPC in Ihrem Konto aus. Sie wählen auch mindestens zwei Subnetze in zwei verschiedenen Availability Zones aus. Diese VPCs und die Subnetze müssen die folgenden Anforderungen erfüllen:

- Die VPC muss über Standard-Tenancy verfügen. VPCs mit dedizierter Mandantenfähigkeit werden nicht unterstützt.
- Aus Gründen der Verfügbarkeit benötigen wir mindestens zwei Subnetze, die in zwei verschiedenen Availability Zones erstellt wurden. Ihre Subnetze müssen über ausreichende IP-Adressen verfügen, um den erwarteten WorkSpaces Web-Datenverkehr zu unterstützen. Konfigurieren Sie jedes Ihrer Subnetze mit einer Subnetzmaske, die genügend Client-IP-Adressen für die maximale Anzahl der gleichzeitigen Sitzungen ermöglicht. Weitere Informationen finden Sie unter Eine neue VPC erstellen und konfigurieren.
- Alle Subnetze müssen eine stabile Verbindung zu allen internen Inhalten haben, entweder im AWS Cloud oder On-Premises, auf die Benutzer mit WorkSpaces Web zugreifen.

Wir empfehlen Ihnen, aus Gründen der Verfügbarkeit und der Skalierung drei Subnetze in unterschiedlichen Availability Zones auszuwählen. Weitere Informationen finden Sie unter Eine neue VPC erstellen und konfigurieren.

WorkSpaces Web weist Streaming-Instances keine öffentliche IP-Adresse zu, um den Internetzugang zu ermöglichen. Sonst wären Ihre Streaming-Instances über das Internet erreichbar. Daher hat keine Streaming-Instance, die mit Ihrem öffentlichen Subnetz verbunden ist, Internetzugang. Wenn Ihr WorkSpaces Webportal Zugriff sowohl auf öffentliche Internetinhalte als auch auf private VPC-Inhalte haben soll, führen Sie die Schritte unter ausAktivieren Sie uneingeschränktes Surfen im Internet (empfohlen).

Eine neue VPC erstellen und konfigurieren

In dieser Sitzung wird beschrieben, wie Sie mit dem VPC-Assistenten eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz erstellen. Im Rahmen dieses Prozesses erstellt

der Assistent ein Internet-Gateway und ein NAT-Gateway. Es wird auch eine benutzerdefinierte Routing-Tabelle erstellt, die dem öffentlichen Subnetz zugeordnet ist. Dann wird die Haupt-Routing-Tabelle aktualisiert, die dem privaten Subnetz zugeordnet ist. Das NAT-Gateway wird automatisch im Subnetz Ihrer VPC erstellt.

Nachdem Sie den Assistenten zum Erstellen einer VPC-Konfiguration verwendet haben, fügen Sie ein zweites privates Subnetz hinzu. Weitere Informationen zu dieser Konfiguration finden Sie unter VPC mit öffentlichen und privaten Subnetzen (NAT).

Schritt 1: Eine Elastic IP-Adresse zuweisen

Bevor Sie Ihre VPC erstellen, müssen Sie eine Elastic IP-Adresse in Ihrer WorkSpaces Webregion zuweisen. Nach der Zuweisung können Sie die Elastic IP-Adresse mit Ihrem NAT-Gateway verknüpfen. Mit einer Elastic IP-Adresse können Sie einen Ausfall bei Streaming-Instances maskieren. Weisen Sie dazu die Adresse einer anderen Instance in Ihrer VPC neu zu. Weitere Informationen finden Sie unter Elastic IP-Adressen.

> **Note**
>
> Für Elastic IP-Adressen, die Sie verwenden, fallen möglicherweise Gebühren an. Weitere Informationen finden Sie unter Seite mit Preisen für Elastic-IP-Adressen.

Wenn Sie noch keine Elastic IP-Adresse haben, führen Sie die folgenden Schritte aus. Wenn Sie eine vorhandene Elastic IP-Adresse verwenden möchten, müssen Sie zunächst sicherstellen, dass sie derzeit nicht einer anderen Instance oder einer Netzwerkschnittstelle zugeordnet ist.

So weisen Sie eine Elastic IP-Adresse zu

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Network & Security die Option Elastic IPs aus.
3. Wählen Sie Allocate new address (Neue Adresse zuordnen) und anschließend Yes, Allocate (Ja, zuordnen) aus.
4. Notieren Sie sich die Elastic IP-Adresse, die auf der Konsole angezeigt wird.
5. Klicken Sie in die im Bereich Elastic IPs in der Ecke oben rechts auf das x-Symbol, um den Bereich zu schließen.

Schritt 2: Eine neuen VPC erstellen

Führen Sie die folgenden Schritte aus, um eine neue VPC mit einem öffentlichen Subnetz und einem privaten Subnetz zu erstellen.

So erstellen Sie eine neue VPC

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich VPC Dashboard (VPC-Dashboard) aus.
3. Wählen Sie VPC Wizard starten.
4. Wählen Sie unter Step 1: Select a VPC Configuration (Schritt 1: Auswählen einer VPC-Konfiguration) die Option VPC with Public and Private Subnets (VPC mit öffentlichen und privaten Subnetzen) und anschließend Select (Auswählen) aus.
5. Konfigurieren Sie unter Step 2: VPC with Public and Private Subnets (Schritt 2: VPC mit öffentlichen und privaten Subnetzen) die VPC wie folgt:

   - Geben Sie für IPv4 CIDR Block (IPv4-CIDR-Block) einen IPv4-CIDR-Block für die VPC ein.
   - Behalten Sie unter IPv6 CIDR Block (IPv6-CIDR-Block) den Standardwert No IPv6 CIDR Block (Kein IPv6-CIDR-Block) bei.
   - Geben Sie unter VPC-Name einen eindeutigen Namen für die VPC ein.
   - Konfigurieren Sie das öffentliche Subnetz wie folgt:
     - Legen Sie unter Public subnet's IPv4 CIDR (IPv4-CIDR für öffentliches Subnetz) den CIDR-Block für das Subnetz ein.
     - Behalten Sie unter Availability Zone den Standardwert No Preference (Keine Einstellung) bei.
     - Geben Sie unter Name für öffentliches Subnetz einen Namen für das Subnetz ein. Beispiel: **`WorkSpaces Web Public Subnet`**
   - Konfigurieren Sie das erste private Subnetz wie folgt:
     - Geben Sie unter Private subnet's IPv4 CIDR (IPv4-CIDR des privaten Subnetzes) den CIDR-Block für das Subnetz an. Notieren Sie sich den von Ihnen angegebenen Wert.
     - Wählen Sie unter Availability Zone eine bestimmte Zone aus und notieren Sie sich die ausgewählte Zone.
     - Geben Sie unter Name für privates Subnetz einen Namen für das Subnetz ein. Beispiel: **`WorkSpaces Web Private Subnet1`**
   - Behalten Sie bei den übrigen Feldern die Standardwerte bei, sofern sie zutreffen.

- Geben Sie bei Elastic-IP-Zuordnungs-ID den Wert ein, der der Elastic-IP-Adresse entspricht, die Sie erstellt haben. Diese Adresse wird dann dem NAT-Gateway zugewiesen. Wenn Sie keine Elastic IP-Adresse haben, erstellen Sie mithilfe der Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
- Geben Sie für Service-Endpunkte einen Amazon-S3-Endpunkt an, wenn für Ihre Umgebung ein solcher erforderlich ist.

  Gehen Sie folgendermaßen vor, um einen Amazon–S3Endpunkt anzugeben:

  1. Wählen Sie Add endpoint (Endpunkt hinzufügen) aus.
  2. Wählen Sie bei Service den Eintrag com.amazonaws.***Region***.s3 aus, wobei *Region* die AWS-Region ist, in der Sie Ihre VPC erstellen.
  3. Wählen Sie für Subnet (Subnetz) die Option Private subnet (Privates Subnetz) aus.
  4. Behalten Sie unter Policy (Richtlinie) den Standardwert Full Access (Voller Zugriff) bei.
- Behalten Sie unter Enable DNS hostnames (DNS-Hostnamen aktivieren) den Standardwert Yes (Ja) bei.
- Behalten Sie bei Hardware tenancy (Hardware-Tenancy) den Standardwert Default (Standard) bei.
- Wählen Sie VPC erstellen aus.
- Es dauert mehrere Minuten, die VPC einzurichten. Wählen Sie nach dem Erstellen der VPC OK aus.

Schritt 3: Ein zweites privates Subnetz hinzufügen

Im vorherigen Schritt haben Sie eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz erstellt. Schließen Sie die folgenden Schritte ab, um Ihrer VPC ein zweites privates Subnetz hinzuzufügen. Es wird empfohlen, ein zweites privates Subnetz in einer anderen Availability Zone als dem ersten privaten Subnetz hinzuzufügen.

So fügen Sie ein zweites privates Subnetz hinzu

1. Wählen Sie im Navigationsbereich Subnetze aus.
2. Wählen Sie das erste private Subnetz aus, das Sie im vorherigen Schritt erstellt haben. Notieren Sie sich auf der Registerkarte Description (Beschreibung) unterhalb der Liste der Subnetze die Availability Zone für dieses Subnetz.
3. Wählen Sie oben links im Subnetzbereich die Option Create Subnet (Subnetz erstellen) aus.

4. Geben Sie unter Name-Tag einen Namen für das private Subnetz ein. Beispiel: **`WorkSpaces Web Private Subnet2`**
5. Wählen Sie für VPC die VPC aus, die Sie im vorherigen Schritt erstellt haben.
6. Wählen Sie unter Availability Zone eine andere Availability Zone als die aus, die Sie für Ihr erstes privates Subnetz verwenden. Die Auswahl einer anderen Availability Zone erhöht die Fehlertoleranz und verhindert Fehler aufgrund unzureichender Kapazität.
7. Geben Sie für IPv4 CIDR block (IPv4-CIDR-Block) einen eindeutigen CIDR-Blockbereich für das neue Subnetz an. Wenn das erste private Subnetz beispielsweise einen IPv4-CIDR-Blockbereich von **`10.0.1.0/24`** hat, können Sie den CIDR-Blockbereich **`10.0.2.0/24`** für das zweite private Subnetz angeben.
8. Wählen Sie Erstellen.
9. Nachdem Ihr Subnetz erstellt wurde, wählen Sie Close (Schließen) aus.

Schritt 4: Die Subnetz-Routing-Tabellen überprüfen und benennen

Nachdem Sie Ihre VPC erstellt und konfiguriert haben, führen Sie die folgenden Schritte aus, um einen Namen für Ihre Routing-Tabellen anzugeben. Sie müssen überprüfen, ob die folgenden Angaben für Ihre Routing-Tabelle korrekt sind:

- Die Routing-Tabelle, die dem Subnetz zugeordnet ist, in dem sich das NAT-Gateway befindet, muss eine Route enthalten, die den Internetdatenverkehr zu einem Internet-Gateway leitet. Dadurch wird sichergestellt, dass Ihr NAT-Gateway Zugriff auf das Internet hat.
- Die Routing-Tabellen, die Ihren privaten Subnetzen zugeordnet sind, müssen so konfiguriert sein, dass der Internetdatenverkehr zum NAT-Gateway geleitet wird. So können die Streaming-Instances innerhalb Ihrer privaten Subnetze mit dem Internet kommunizieren.

So überprüfen und benennen Sie die Subnetz-Routing-Tabellen

1. Wählen Sie im Navigationsbereich die Option Subnetze und dann das öffentliche Subnetz aus, das Sie erstellt haben. Zum Beispiel WorkSpaces Web 2.0 Public Subnet .
2. Wählen Sie auf der Registerkarte Route Table (Routing-Tabelle) die ID der Routing-Tabelle aus. Zum Beispiel rtb-12345678.
3. Wählen Sie die -Routing-Tabelle aus. Wählen Sie unter Name das Bearbeitungssymbol (Stift) aus und geben Sie einen Namen für die Tabelle ein. Geben Sie beispielsweise den Namen

workspacesweb-public-routetable ein. Wählen Sie dann das Häkchen aus, um den Namen zu speichern.

4. Stellen Sie bei weiterhin markierter öffentlicher Routing-Tabelle auf der Registerkarte Routen sicher, dass zwei Routen vorhanden sind: eine für den lokalen Datenverkehr sowie eine weitere, über die der übrige Datenverkehr an das Internet-Gateway für die VPC gesendet wird. In der folgenden Tabelle werden diese beiden Routen beschrieben.

Bestimmungsort	Ziel	Beschreibung
IPv4-CIDR-Block für öffentliches Subnetz (z. B. 10.0.0/20)	Local	Der gesamte Datenverkehr von den Ressourcen, die für IPv4-Adressen im IPv4-CIDR-Block des öffentlichen Subnetzes bestimmt sind. Dieser Datenverkehr wird lokal innerhalb der VPC weitergeleitet.
Datenverkehr, der für alle anderen IPv4-Adressen bestimmt ist, (z. B. 0.0.0.0/0)	Ausgehend (igw-ID)	Datenverkehr, der für alle anderen IPv4-Adressen bestimmt ist, wird an das Internet-Gateway (identifiziert durch igw-ID) weitergeleitet, das vom VPC-Assistenten erstellt wurde.

5. Wählen Sie im Navigationsbereich Subnetze aus. Wählen Sie dann das erste private Subnetz aus, das Sie erstellt haben (zum Beispiel **WorkSpaces Web Private Subnet1**).
6. Wählen Sie auf der Registerkarte Routing-Tabelle die ID der Routing-Tabelle aus.
7. Wählen Sie die -Routing-Tabelle aus. Wählen Sie unter Name das Bearbeitungssymbol (Stift) aus und geben Sie einen Namen für die Tabelle ein. Geben Sie beispielsweise den Namen **workspacesweb-private-routetable** ein. Wählen Sie dann das Häkchen aus, um den Namen zu speichern.
8. Überprüfen Sie auf der Registerkarte Routes (Routen), ob die Routing-Tabelle die folgenden Routen enthält:

Bestimmungsort	Ziel	Beschreibung
IPv4-CIDR-Block für öffentliches Subnetz (z. B. 10.0.0.0/20)	Local	Der gesamte Datenverkehr von den Ressourcen, die für IPv4-Adressen im IPv4-CIDR-Block des öffentlichen Subnetzes bestimmt sind, wird lokal innerhalb der VPC weitergeleitet.
Datenverkehr, der für alle anderen IPv4-Adressen bestimmt ist, (z. B. 0.0.0.0/0)	Ausgehend (nat-ID)	Datenverkehr, der für alle anderen IPv4-Adressen bestimmt ist, wird an das NAT-Gateway weitergeleitet (identifiziert durch nat-ID).
Für S3-Buckets bestimmter Datenverkehr (anwendbar, wenn Sie einen S3-Endpunkt angegeben haben) [pl-ID (com.amazonaws.region.s3)]	Speicher (vpce-ID)	Datenverkehr, der für S3-Buckets bestimmt ist, wird an den S3-Endpunkt weitergeleitet (identifiziert durch vpce-ID).

9. Wählen Sie im Navigationsbereich Subnetze aus. Wählen Sie dann das zweite private Subnetz aus, das Sie erstellt haben (zum Beispiel **`WorkSpaces Web Private Subnet2`**).
10. Stellen Sie auf der Registerkarte Routing-Tabelle sicher, dass es sich bei der ausgewählten Routing-Tabelle um die private Routing-Tabelle handelt (z. B. **`workspacesweb-private-routetable`**). Wenn eine andere Routing-Tabelle angezeigt wird, wählen Sie Bearbeiten aus und wählen Sie stattdessen Ihre private Routing-Tabelle aus.

Aktivieren Sie uneingeschränktes Surfen im Internet (empfohlen)

Gehen Sie folgendermaßen vor, um eine VPC mit einem NAT-Gateway für uneingeschränktes Surfen im Internet zu konfigurieren. Dadurch wird WorkSpaces Webzugriff auf Websites im öffentlichen Internet und auf private Websites gewährt, die in oder mit einer Verbindung zu Ihrer VPC gehostet werden.

So konfigurieren Sie eine VPC mit einem NAT-Gateway für uneingeschränktes Surfen im Internet

Wenn Sie möchten, dass Ihr WorkSpaces Webportal Zugriff sowohl auf öffentliche Internetinhalte als auch auf private VPC-Inhalte hat, gehen Sie folgendermaßen vor:

> **Note**
>
> Wenn Sie bereits eine VPC konfiguriert haben, führen Sie die folgenden Schritte aus, um Ihrer VPC ein NAT-Gateway hinzuzufügen. Informationen zum Erstellen einer neuen VPC finden Sie unter Eine neue VPC erstellen und konfigurieren.

1. Um Ihr NAT-Gateway zu erstellen, führen Sie die Schritte unter Ein NAT-Gateway erstellen aus. Stellen Sie sicher, dass dieses NAT-Gateway über öffentliche Konnektivität verfügt und sich in einem öffentlichen Subnetz in Ihrer VPC befindet.
2. Sie müssen mindestens zwei private Subnetze in verschiedenen Availability Zones angeben. Die Zuweisung Ihrer Subnetze zu verschiedenen Availability Zones trägt zu einer besseren Verfügbarkeit und Fehlertoleranz bei. Informationen zum Erstellen eines zweiten privaten Subnetzes finden Sie unter the section called “Schritt 3: Ein zweites privates Subnetz hinzufügen”.

   > **Note**
   >
   > Um sicherzustellen, dass jede Streaming-Instance Internetzugang hat, fügen Sie Ihrem WorkSpaces Webportal kein öffentliches Subnetz an.

3. Aktualisieren Sie die Routing-Tabelle, die ihren privaten Subnetzen zugeordnet ist, um internetgebundenen Datenverkehr zum NAT-Gateway zu leiten. So können die Streaming-Instances innerhalb Ihrer privaten Subnetze mit dem Internet kommunizieren. Informationen dazu, wie Sie eine Routing-Tabelle einem privaten Subnetz zuordnen, finden Sie in den Schritten unter Routing-Tabellen konfigurieren.

Aktivieren von eingeschränktem Internet-Browsing (mit ausgehendem HTTP-Proxy)

Die empfohlene Netzwerkeinrichtung eines WorkSpaces Webportals besteht darin, private Subnetze mit NAT-Gateway zu verwenden, damit das Portal sowohl öffentliche als auch private Inhalte durchsuchen kann. Weitere Informationen finden Sie unter the section called “Aktivieren

Sie uneingeschränktes Surfen im Internet (empfohlen)". Möglicherweise müssen Sie jedoch die ausgehende Kommunikation von einem WorkSpaces Webportal zum Internet mithilfe eines Web-Proxys steuern. Wenn Sie beispielsweise einen Web-Proxy als Gateway für das Internet verwenden, können Sie präventive Sicherheitskontrollen wie Domain-Zulassungsliste und Inhaltsfilterung implementieren. Dies kann auch die Bandbreitennutzung reduzieren und die Netzwerkleistung verbessern, indem häufig aufgerufene Ressourcen wie Webseiten oder Softwareupdates lokal zwischengespeichert werden. In einigen Anwendungsfällen haben Sie möglicherweise private Inhalte, auf die nur über einen Web-Proxy zugegriffen werden kann.

Möglicherweise sind Sie bereits mit der Konfiguration von Proxy-Einstellungen auf verwalteten Geräten oder auf dem Image Ihrer virtuellen Umgebungen vertraut. Dies stellt jedoch Herausforderungen dar, wenn Sie nicht die Kontrolle über das Gerät haben (z. B. wenn sich Benutzer auf Geräten befinden, die nicht dem Unternehmen gehören oder von diesem verwaltet werden) oder wenn Sie das Image für Ihre virtuelle Umgebung verwalten müssen. Mit WorkSpaces Web können Sie Proxy-Einstellungen mithilfe der in den Webbrowser integrierten Chrome-Richtlinien festlegen. Sie können dies tun, indem Sie einen HTTP-Proxy für ausgehenden Datenverkehr für WorkSpaces Web einrichten.

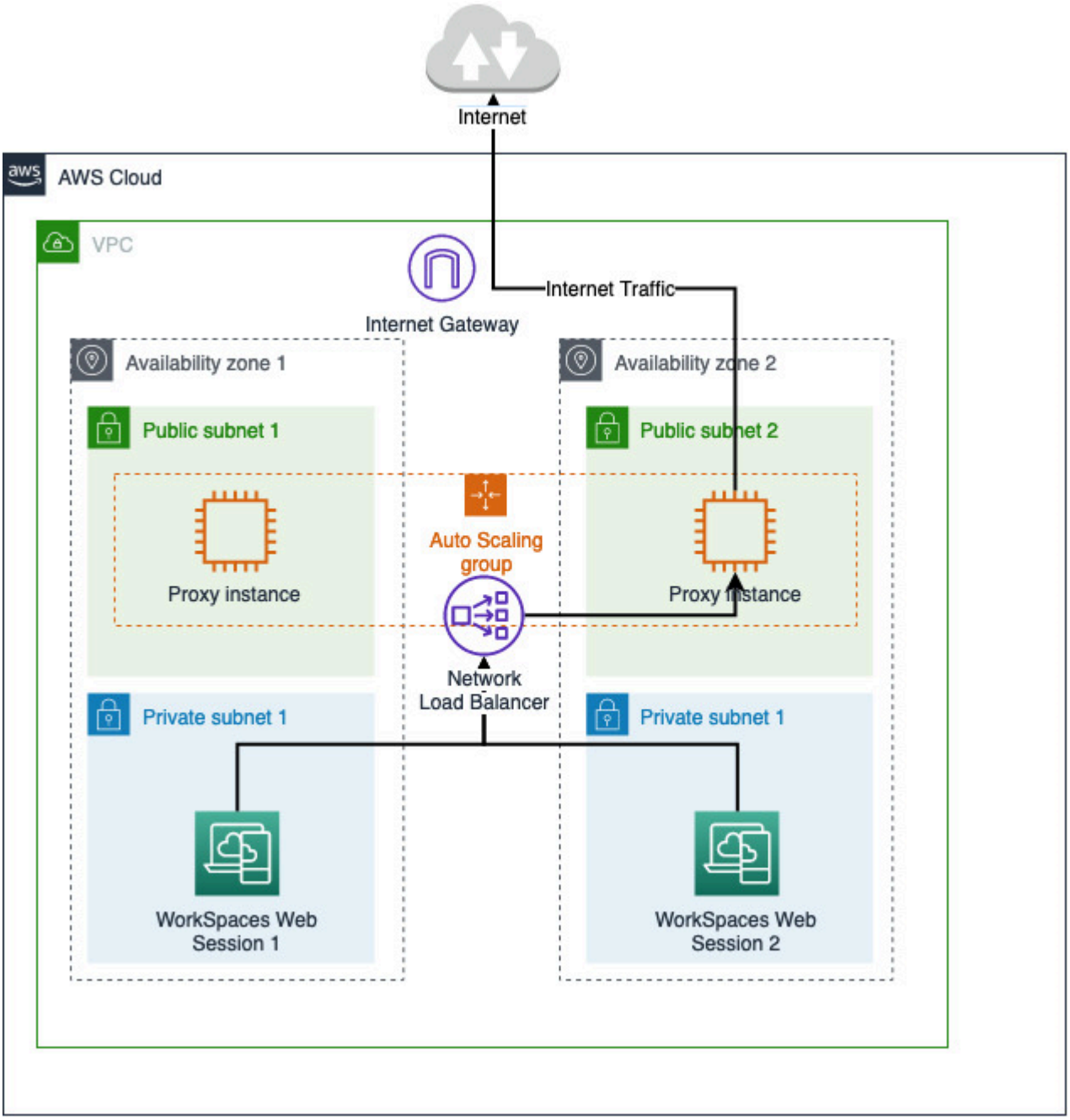
Diese Lösung basiert auf einer empfohlenen ausgehenden VPC-Proxy-Einrichtung. Die Proxy-Lösung basiert auf dem Open-Source-HTTP-Proxy Squid . Anschließend werden WorkSpaces Webbrowser-Einstellungen verwendet, um das WorkSpaces Webportal so zu konfigurieren, dass es eine Verbindung zum Proxy-Endpunkt herstellt. Weitere Informationen finden Sie unter So richten Sie einen ausgehenden VPC-Proxy mit Domain-Whitelisting und Inhaltsfilterung ein.

Diese Lösung bietet Ihnen die folgenden Vorteile:

- Ein ausgehender Proxy, der eine Gruppe von Amazon EC2-Instances mit automatischer Skalierung enthält, die von einem Network Load Balancer gehostet werden. Proxy-Instances befinden sich in einem öffentlichen Subnetz, und jede von ihnen ist mit einer Elastic IP verbunden, sodass sie Zugriff auf das Internet haben.
- Ein WorkSpaces Webportal, das in privaten Subnetzen bereitgestellt wird. Sie müssen kein NAT-Gateway konfigurieren, um den Internetzugang zu ermöglichen. Stattdessen konfigurieren Sie Ihre Browserrichtlinie, sodass der gesamte Internetdatenverkehr über den ausgehenden Proxy geleitet wird. Wenn Sie Ihren eigenen Proxy verwenden möchten, sieht die Einrichtung des WorkSpaces Webportals ähnlich aus.

Architektur

Im Folgenden finden Sie ein Beispiel für eine typische Proxy-Einrichtung in Ihrer VPC. Die Proxy-Amazon EC2-Instance befindet sich in öffentlichen Subnetzen und ist Elastic IP zugeordnet, sodass diese Zugriff auf das Internet haben. Ein Network Load Balancer hostet eine Auto-Scaling-Gruppe von Proxy-Instances. Dadurch wird sichergestellt, dass Proxy-Instances automatisch hochskaliert werden können und der Network Load Balancer der einzelne Proxy-Endpunkt ist, der von WorkSpaces Websitzungen genutzt werden kann.



Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen:

- Sie benötigen eine bereits bereitgestellte VPC mit öffentlichen und privaten Subnetzen, die über mehrere Availability Zones (AZs) verteilt sind. Weitere Informationen zum Einrichten Ihrer VPC-Umgebung finden Sie unter Standard-VPCs.
- Sie benötigen einen einzelnen Proxy-Endpunkt, auf den von privaten Subnetzen aus zugegriffen werden kann, in denen WorkSpaces Websitzungen live sind (z. B. der DNS-Name des Network Load Balancers). Wenn Sie Ihren vorhandenen Proxy verwenden möchten, stellen Sie sicher, dass er auch über einen einzelnen Endpunkt verfügt, auf den Sie von Ihren privaten Subnetzen aus zugreifen können.

Einrichten eines HTTP-Proxys für ausgehenden Datenverkehr für WorkSpaces Web

Gehen Sie folgendermaßen vor, um einen HTTP-Proxy für ausgehenden Datenverkehr für WorkSpaces Web einzurichten.

1. Um einen Beispiel-Proxy für ausgehenden Datenverkehr in Ihrer VPC bereitzustellen, folgen Sie den Schritten unter So richten Sie einen Proxy für ausgehenden Datenverkehr mit Domain-Whitelisting und Inhaltsfilterung ein.
   a. Führen Sie die Schritte unter „Installation (einmalige Einrichtung)“ aus, um die CloudFormation Vorlage in Ihrem Konto bereitzustellen. Stellen Sie sicher, dass Sie die richtige VPC und die richtigen Subnetze als CloudFormation Vorlagenparameter auswählen.
   b. Suchen Sie nach der Bereitstellung den CloudFormation Ausgabeparameter OutboundProxyDomain und OutboundProxyPort. Dies ist der DNS-Name und der Port Ihres Proxys.
   c. Wenn Sie bereits über einen eigenen Proxy verfügen, überspringen Sie diesen Schritt und verwenden Sie den DNS-Namen und den Port Ihres Proxys.
2. Wählen Sie in der WorkSpaces Webkonsole Ihr Portal und dann Bearbeiten aus.
   a. Wählen Sie in den Netzwerkverbindungsdetails die VPC und die privaten Subnetze aus, die Zugriff auf den Proxy haben.
   b. Fügen Sie in den Richtlinieneinstellungen mithilfe eines JSON-Editors die folgende ProxySettings Richtlinie hinzu. Das `ProxyServer` Feld sollte der DNS-Name und der Port Ihres Proxys sein. Weitere Informationen zur ProxySettings Richtlinie finden Sie unter ProxySettings.

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
    }
}
```

3. In Ihrer WorkSpaces Websitzung sehen Sie, dass der Proxy auf die Chrome-Einstellung angewendet wird, die Chrome Proxy-Einstellungen von Ihrem Administrator verwendet.
4. Gehen Sie zu Chrome://policy und auf die Registerkarte Chrome-Richtlinie, um zu bestätigen, dass die Richtlinie angewendet wird.
5. Stellen Sie sicher, dass Ihre WorkSpaces Websitzung erfolgreich Internetinhalte ohne NAT-Gateway durchsuchen kann. Überprüfen Sie in den CloudWatch Protokollen, ob die Squid-Proxy-Zugriffsprotokolle aufgezeichnet werden.

Fehlerbehebung

Nachdem die Chrome-Richtlinie angewendet wurde und Ihre WorkSpaces Websitzung immer noch nicht auf das Internet zugreifen kann, führen Sie die folgenden Schritte aus, um zu versuchen, Ihr Problem zu beheben:

- Stellen Sie sicher, dass der Proxy-Endpunkt von den privaten Subnetzen aus zugänglich ist, in denen sich Ihr WorkSpaces Webportal befindet. Erstellen Sie dazu eine EC2-Instance im privaten Subnetz und testen Sie die Verbindung von der privaten EC2-Instance zu Ihrem Proxy-Endpunkt.
- Stellen Sie sicher, dass der Proxy Internetzugang hat.
- Überprüfen Sie, ob die Chrome-Richtlinie korrekt ist.
  - Bestätigen Sie die folgende Formatierung für das -`ProxyServer`Feld der Richtlinie: `<Proxy DNS name>:<Proxy port>`. Das `https://` Präfix sollte kein `http://` oder enthalten.

- Verwenden Sie in der WorkSpaces Websitzung Chrome, um zu Chrome://Richtlinie zu navigieren, und stellen Sie sicher, dass die ProxySettings Richtlinie erfolgreich angewendet wurde.

Empfehlungen zur VPC-Einrichtung

Die folgenden Empfehlungen können Ihnen dabei helfen, Ihre VPC effektiver und sicherer zu konfigurieren.

VPC-Gesamtkonfiguration

- Stellen Sie sicher, dass Ihre VPC-Konfiguration Ihre Skalierungsanforderungen erfüllen kann.
- Stellen Sie sicher, dass Ihre WorkSpaces Web-Servicekontingente (auch als Limits bezeichnet) ausreichen, um Ihren erwarteten Bedarf zu decken. Um eine Kontingenterhöhung zu beantragen, können Sie die Konsole für Service Quotas unter https://console.aws.amazon.com/servicequotas/ verwenden. Informationen zu Standardkontingenten für WorkSpaces Web finden Sie unter the section called “Eine Erhöhung des Service-Kontingents anfordern”.
- Wenn Sie Ihren Streaming-Sitzungen Zugriff auf das Internet gewähren möchten, empfehlen wir Ihnen, eine VPC mit einem NAT-Gateway in einem öffentlichen Subnetz zu konfigurieren.

Elastic-Network-Schnittstellen

- Jede WorkSpaces Web-Sitzung benötigt während der Streaming-Dauer eine eigene Elastic-Network-Schnittstelle. WorkSpaces Web erstellt so viele Elastic-Network-Schnittstellen (ENIs), wie die maximal gewünschte Kapazität Ihrer Flotte erreicht ist. Standardmäßig liegt das Limit für ENIs pro Region bei 5 000. Weitere Informationen finden Sie unter Netzwerkschnittstellen.

  Bei der Kapazitätsplanung für sehr große Bereitstellungen, z. B. Tausende gleichzeitiger Streaming-Sitzungen, sollten Sie die Anzahl der ENIs berücksichtigen, die für Ihre Spitzennutzung erforderlich sein könnten. Wir empfehlen, dass Sie Ihr ENI-Limit auf oder über dem für Ihr Webportal konfigurierten maximalen Limit für die gleichzeitige Nutzung halten.

Subnets

- Beachten Sie bei der Entwicklung Ihres Plans, Benutzer hochzuskalieren, dass jede WorkSpaces Websitzung eine eindeutige Client-IP-Adresse aus Ihren konfigurierten Subnetzen erfordert. Daher

bestimmt die Größe des Client-IP-Adressraums, der in Ihren Subnetzen konfiguriert ist, die Anzahl der Benutzer, die gleichzeitig streamen können.

- Wir empfehlen, jedes Subnetz mit einer Subnetzmaste zu konfigurieren, die genügend Client-IP-Adressen für die maximale Anzahl der erwarteten gleichzeitigen Benutzer ermöglicht. Überlegen Sie außerdem, ob Sie im Hinblick auf das erwartete Wachstum zusätzliche IP-Adressen hinzufügen. Weitere Informationen finden Sie unter Dimensionierung der VPC und der Subnetze für IPv4.
- Aus Gründen der Verfügbarkeit und Skalierung empfehlen wir, ein Subnetz in jeder eindeutigen Availability Zone zu konfigurieren, die WorkSpaces Web in Ihrer gewünschten Region unterstützt. Weitere Informationen finden Sie unter the section called “Eine neue VPC erstellen und konfigurieren”.
- Zudem muss sichergestellt sein, dass auf die für Ihre Webanwendungen erforderlichen Netzwerkressourcen über Ihre Subnetze zugegriffen werden kann.

Sicherheitsgruppen

- Verwenden Sie Sicherheitsgruppen, um zusätzliche Zugriffssteuerung für Ihre VPC bereitzustellen.

  Mit Sicherheitsgruppen, die zu Ihrer VPC gehören, können Sie den Netzwerkverkehr zwischen WorkSpaces Web-Streaming-Instances und Netzwerkressourcen steuern, die von Webanwendungen benötigt werden. Stellen Sie sicher, dass die Sicherheitsgruppen Zugriff auf die Netzwerkressourcen bieten, die von Ihren Webanwendungen benötigt werden.

Unterstützte Availability Zones

Wenn Sie eine Virtual Private Cloud (VPC) für die Verwendung mit WorkSpaces Web erstellen, müssen sich die Subnetze Ihrer VPC in verschiedenen Availability Zones in der Region befinden, in der Sie WorkSpaces Web starten. Availability Zones sind unabhängige Standorte, die so aufgebaut sind, dass sie von Fehlern in anderen Availability Zones nicht betroffen sind. Indem Instances in separaten Availability Zones gestartet werden, können Sie Ihre Anwendungen vor den Fehlern eines einzelnen Standorts schützen. Jedes Subnetz muss sich vollständig innerhalb einer Availability Zone befinden und darf nicht mehrere Zonen umfassen. Wir empfehlen, für jede unterstützte AZ in der gewünschten Region ein Subnetz zu konfigurieren, um maximale Ausfallsicherheit zu erzielen

Eine Availability Zone wird durch einen Regionscode gefolgt von einem Buchstaben als Bezeichner angegeben, z. B. `us-east-1a`. Um sicherzustellen, dass Ressourcen auf die Availability Zones

einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes AWS-Konto zu. So befindet sich die Availability Zone `us-east-1a` für Ihr AWS-Konto möglicherweise nicht im selben Ort wie `us-east-1a` für ein anderes AWS-Konto.

Um die Availability Zones kontenübergreifend zu koordinieren, müssen Sie die AZ-ID verwenden, die eine eindeutige und konsistente Kennung für eine Availability Zone ist. Beispielsweise ist `use1-az2` eine AZ-ID für die `us-east-1`-Region und hat in jedem AWS-Konto den gleichen Standort.

Mit der Anzeige von AZ-IDs können Sie den Standort von Ressourcen in einem Konto im Verhältnis zu den Ressourcen in einem anderen Konto bestimmen. Wenn Sie beispielsweise ein Subnetz in der Availability Zone mit der AZ-ID `use1-az2` mit einem anderen Konto teilen, steht dieses Subnetz dem Konto in der Availability Zone zur Verfügung, dessen AZ-ID ebenfalls `use1-az2` ist. Die AZ-ID für jede VPC und jedes Subnetz wird in der Amazon VPC-Konsole angezeigt.

WorkSpaces Web ist in einer Teilmenge der Availability Zones für jede unterstützte Region verfügbar. In der folgenden Tabelle sind alle AZ-IDs aufgeführt, die Sie für jede Region verwenden können. Informationen über die Zuordnung von AZ-IDs zu Availability Zones in Ihrem Konto finden Sie unter AZ-IDs für Ihre Ressourcen im AWS RAM-Benutzerhandbuch.

Name der Region	Regionscode	Unterstützte AZ-IDs
USA Ost (Nord-Virginia)	`us-east-1`	`use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6`
USA West (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`
Asia Pacific (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-az3`
Asia Pacific (Seoul)	`ap-northeast-2`	`apne2-az1` , `apne2-az2` , `apne2-az3`
Asien-Pazifik (Singapur)	`ap-southeast-1`	`apse1-az1` , `apse1-az2` , `apse1-az3`
Asien-Pazifik (Sydney)	`ap-southeast-2`	`apse2-az1` , `apse2-az2` , `apse2-az3`

Name der Region	Regionscode	Unterstützte AZ-IDs
Asien-Pazifik (Tokio)	`ap-northeast-1`	`apne1-az1` , `apne1-az2` , `apne1-az4`
Canada (Central)	`ca-central-1`	`cac1-az1`, `cac1-az2`, `cac1-az4`
Europe (Frankfurt)	`eu-central-1`	`euc1-az2`, `euc1-az2`, `euc1-az3`
Europa (Irland)	`eu-west-1`	`euw1-az1`, `euw1-az2`, `euw1-az3`
Europe (London)	`eu-west-2`	`euw2-az1`, `euw2-az2`

Weitere Informationen zu Availability Zones und AZ-IDs finden Sie unter Regionen, Availability Zones und lokale Zonen im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

VPC-Verbindung

Jede WorkSpaces Web-Streaming-Instance verfügt über eine Kundennetzwerkschnittstelle, die Konnektivität zu den Ressourcen in Ihrer VPC sowie zum Internet bietet, wenn private Subnetze mit NAT-Gateway eingerichtet sind.

Für die Internetkonnektivität müssen die folgenden Ports für alle Ziele geöffnet sein. Wenn Sie eine veränderte oder benutzerdefinierte Sicherheitsgruppe verwenden, müssen Sie die erforderlichen Regeln manuell hinzufügen. Weitere Informationen finden Sie unter Regeln zu Sicherheitsgruppen.

> **Note**
>
> Dies gilt für ausgehenden Datenverkehr.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8.433

Client/Benutzer-Verbindung

WorkSpaces Web ist so konfiguriert, dass Streaming-Verbindungen über das öffentliche Internet weitergeleitet werden. Internetkonnektivität ist erforderlich, um Benutzer zu authentifizieren und die Webressourcen bereitzustellen, die WorkSpaces Web für die Funktion benötigt. Sie müssen die in Zulässige Domänen aufgelisteten Domains zulassen, um diesen Datenverkehr zuzulassen.

Die folgenden Themen enthalten Informationen zum Aktivieren von Benutzerverbindungen mit WorkSpaces Web.

Themen

- IP-Adresse und Port-Anforderungen
- Zulässige Domänen

IP-Adresse und Port-Anforderungen

Für den Zugriff auf WorkSpaces Web-Instances benötigen Benutzergeräte ausgehenden Zugriff über die folgenden Ports:

- Port 443 (TCP)
  - Port 443 wird für die HTTPS-Kommunikation zwischen -Benutzergeräten und Streaming-Instances verwendet, wenn die Internet-Endpunkte verwendet werden. Wenn Endbenutzer während Streaming-Sitzungen im Internet surfen, wählt der Web-Browser normalerweise einen Quell-Port im höheren Bereich für das Streamen von Datenverkehr aus. Sie müssen sicherstellen, dass zu diesem Port zurückfließender Datenverkehr zulässig ist.
  - Dieser Port muss für die erforderlichen Domains geöffnet sein, die unter Zulässige Domänen aufgeführt sind.
  - AWS veröffentlicht seine aktuellen IP-Adressbereiche, einschließlich der Bereiche, in die das Session Gateway und die CloudFront Domains aufgelöst werden können, im JSON-Format. Weitere Informationen zum Herunterladen der JSON-Datei und zur Anzeige der aktuellen Bereiche finden Sie unter AWS-IP-Adressbereiche. Wenn Sie verwendenAWS Tools for Windows PowerShell, können Sie auch mit dem Get-AWSPublicIpAddressRange PowerShell Befehl auf dieselben Informationen zugreifen. Weitere Informationen finden Sie unter Abfragen der öffentlichen IP-Adressbereiche für AWS.
- (Optional) Port 53 (UDP)

- Port 53 wird für die Kommunikation zwischen den Benutzergeräten der und Ihren DNS-Servern verwendet.
- Dieser Port ist optional, wenn Sie keine DNS-Server für die Domänennamenauflösung verwenden.
- Der Port muss für die IP-Adressen Ihrer DNS-Server geöffnet sein, damit öffentliche Domain-Namen aufgelöst werden können.

Zulässige Domänen

Damit der Benutzer von seinem lokalen Browser aus auf den WorkSpaces Webservice zugreifen kann, müssen Sie der Zulassungsliste im Netzwerk, von dem aus der Benutzer auf den Service zugreifen möchte, die folgenden Domains und IP-Adressen hinzufügen.

Der *{Region}*-Teil unten sollte durch den Namen der betreibenden AWS-Region ersetzt werden. Zum Beispiel sollte s3.*{region}*.amazonaws.com s3.eu-west-1.amazonaws.com sein, wenn er für Europa (Irland) (eu-west-1) steht.

Kategorie	Domain oder IP-Adresse
WorkSpaces Web-Streaming-Komponente	s3.*{region}*.amazonaws.com s3.amazonaws.com appstream2.*{region}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Web WebApp -Asset	*.workspaces-web.com
WorkSpaces Webauthentifizierung	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Web-Metriken und -Berichte	*.execute-api.*{region}*.amazonaws.com

Kategorie	Domain oder IP-Adresse
	unagi-na.amazon.com

Abhängig von Ihrem konfigurierten Identitätsanbieter müssen Sie möglicherweise auch zusätzlicher Domains auf die Zulassungsliste setzen. Überprüfen Sie die Dokumentation Ihres IdP, um zu ermitteln, welche Domains Sie zulassen müssen, damit WorkSpaces Web diesen Anbieter verwenden kann. Wenn Sie IAM Identity Center verwenden, finden Sie weitere Informationen unter Voraussetzungen für IAM Identity Center.

Erste Schritte mit Amazon WorkSpaces Web

Gehen Sie wie folgt vor, um ein WorkSpaces Web-Webportal zu erstellen und Benutzern über ihre vorhandenen Browser Zugriff auf interne und SaaS-Websites zu gewähren. Sie können in jeder unterstützten Region ein Webportal pro Konto erstellen.

> **Note**
>
> Um eine Erhöhung des Limits für mehr als ein Portal zu beantragen, wenden Sie sich bitte an den Support mit Ihrer AWS-Konto -ID, der Anzahl der anzufordernden Portale und AWS-Region.

Dieser Vorgang dauert mit dem Assistenten zur Erstellung eines Webportals in der Regel fünf Minuten und weitere 15 Minuten, bis das Portal aktiv wird.

Für die Einrichtung eines Webportals fallen keine Kosten an. WorkSpaces Web bietet pay-as-you-go Preise, einschließlich eines niedrigen monatlichen Preises für Benutzer, die den Service aktiv nutzen. Es gibt keine Vorabkosten, Lizenzen oder langfristige Verpflichtungen.

> **Important**
>
> Bevor Sie beginnen, müssen Sie die erforderlichen Voraussetzungen für ein Webportal erfüllen. Weitere Informationen über Webportal-Voraussetzungen finden Sie unter Einrichten von Amazon WorkSpaces Web.

Themen

- Schritt 1: Ein Webportal erstellen
- Schritt 2: Ihr Webportal testen
- Schritt 3: Ihr Webportal verteilen
- Nächste Schritte

Schritt 1: Ein Webportal erstellen

Führen Sie zur Erstellung eines Webportals diese Schritte aus.

Themen

- Konfigurieren von Netzwerkeinstellungen
- Portaleinstellungen konfigurieren
- Benutzereinstellungen konfigurieren
- Identitätsanbieter konfigurieren
- Überprüfen und starten

Konfigurieren von Netzwerkeinstellungen

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Web , dann Webportale und dann Webportal erstellen aus.
3. Führen Sie auf der Seite Schritt 1: Netzwerkverbindung festlegen die folgenden Schritte aus, um eine Verbindung zwischen Ihrer VPC und Ihrem Webportal herzustellen und Ihre VPC und Subnetze zu konfigurieren.

    1. Wählen Sie für Netzwerkdetails eine VPC mit einer Verbindung zu dem Inhalt aus, auf den Ihre Benutzer mit WorkSpaces Web zugreifen sollen.
    2. Wählen Sie bis zu drei private Subnetze aus, die die folgenden Anforderungen erfüllen. Weitere Informationen finden Sie unter Netzwerk und Zugriff.
        - Sie müssen für die Erstellung eines Portals mindestens zwei private Subnetze auswählen.
        - Um eine hohe Verfügbarkeit für Ihr Webportal zu gewährleisten, empfehlen wir Ihnen, die maximale Anzahl von privaten Subnetzen in eindeutigen Availability Zones für Ihre VPC bereitzustellen.
    3. Wählen Sie eine Sicherheitsgruppe aus.

Portaleinstellungen konfigurieren

Führen Sie auf der Seite Schritt 2: Webportaleinstellungen konfigurieren die folgenden Schritte aus, um das Surferlebnis Ihrer Benutzer beim Starten einer Sitzung anzupassen.

1. Geben Sie unter Webportaldetails bei Anzeigename einen identifizierbaren Namen für Ihr Webportal ein.

2. Wählen Sie unter Benutzerzugriffsprotokollierung bei Kinesis-Stream-ID den Amazon-Kinesis-Datenstrom aus, an den Sie Ihre Daten senden möchten. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.
3. Füllen Sie unter Richtlinieneinstellungen folgendes aus:

   - Wählen Sie bei Richtlinienoptionen die Option Visueller Editor oder JSON-Datei-Upload aus. Sie können die Richtlinienkonfigurationsdetails für Ihr Webportal mit beiden Methoden bereitstellen. Weitere Informationen finden Sie unter the section called “Ihre Browser-Richtlinie festlegen oder bearbeiten”.
     - WorkSpaces Web bietet Unterstützung für Chrome-Unternehmensrichtlinien. Sie können Richtlinien entweder mit einem visuellen Editor oder mit einem manuellen Upload für Richtliniendateien hinzufügen und verwalten. Sie können jederzeit zwischen beiden Optionen wechseln.
     - Wenn Sie eine Richtliniendatei hochladen, können Sie die verfügbaren Richtlinien in der Datei in der Konsole sehen. Sie können jedoch nicht alle Richtlinien im visuellen Editor bearbeiten. In der Konsole werden unter Zusätzliche JSON-Richtlinien Richtlinien in Ihrer JSON-Datei aufgeführt, die Sie nicht mit dem visuellen Editor bearbeiten können. Um Änderungen an diesen Richtlinien vorzunehmen, müssen Sie sie manuell bearbeiten.
   - (Optional) Geben Sie unter Startup-URL – optional eine Domain ein, die als Startseite verwendet werden soll, wenn Benutzer ihren Browser starten. Es muss für Ihre VPC eine stabile Verbindung mit dieser URL hergestellt sein.
   - Aktivieren oder deaktivieren Sie Privates Browsing und Löschen des Verlaufs, um dieses Feature während einer Benutzersitzung ein- oder auszuschalten

     > **Note**
     >
     > URLs, die im privaten Modus besucht werden oder bevor ein Benutzer seinen Browserverlauf löscht, können nicht in der Benutzerzugriffsprotokollierung aufgezeichnet werden. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.

   - Unter URL-Filterung können Sie konfigurieren, welche URLs Benutzer während einer Sitzung besuchen können. Weitere Informationen finden Sie unter the section called “URL-Filterung einrichten”.

- (Optional) Geben Sie bei Browserlesezeichen – optional den Anzeigenamen, die Domain und den Ordner für alle Lesezeichen ein, die Ihren Benutzern in ihrem Browser angezeigt werden sollen. Wählen Sie dann Lesezeichen hinzufügen aus.

  > **Note**
  >
  > Domain ist ein Pflichtfeld für Browserlesezeichen.
  > In Chrome finden Nutzer verwaltete Lesezeichen im Ordner Verwaltete Lesezeichen auf der Lesezeichen-Symbolleiste.

- (Optional) Fügen Sie Ihrem Portal Tags hinzu. Sie können Tags verwenden, um nach Ihren -AWS Ressourcen zu suchen oder diese zu filtern. Tags bestehen aus einem Schlüssel und einem optionalen Wert und sind mit Ihrer Portalressource verknüpft.

4. Wählen Sie unter IP-Zugriffskontrolle (optional) aus, ob der Zugriff auf vertrauenswürdige Netzwerke beschränkt werden soll. Weitere Informationen finden Sie unter the section called “IP-Zugriffskontrollen einrichten (optional)”.
5. Wählen Sie Next (Weiter), um fortzufahren.

Benutzereinstellungen konfigurieren

Führen Sie auf der Seite Schritt 3: Benutzereinstellungen auswählen die folgenden Schritte aus, um auszuwählen, auf welche Features Ihre Benutzer während ihrer Sitzung über die obere Navigationsleiste zugreifen können. Wählen Sie dann Weiter aus:

1. Wählen Sie bei Benutzerberechtigungen aus, ob die Erweiterung für Single Sign-On aktiviert werden soll. Weitere Informationen finden Sie unter the section called “Erweiterung für Single-Sign-On aktivieren (optional)”.
2. Wählen Sie bei Zwischenablageberechtigungen die Option Deaktiviert oder Aktiviert aus.
3. Wählen Sie unter Dateiübertragung die Option Deaktiviert oder Aktiviert aus.
4. Wählen Sie bei Auf lokalem Gerät ausdrucken die Option Zulässig oder Nicht zulässig aus.
5. Geben Sie bei Benutzersitzungsdetails Folgendes an:

   - Wählen Sie für Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) die Zeitspanne aus, für die eine Streaming-Sitzung aktiv bleiben kann, nachdem der Benutzer die Verbindung getrennt hat. Wenn Benutzer nach einer Verbindungstrennung oder Netzwerkunterbrechung innerhalb dieses Zeitraums erneut eine Verbindung herstellen

möchten, werden sie wieder mit der vorherigen Sitzung verbunden. Andernfalls werden sie mit einer neuen Sitzung mit einer neuen Streaming-Instance verbunden.

Wenn ein Benutzer die Sitzung beendet, gilt die Zeitüberschreitung beim Trennen nicht. Stattdessen wird der Benutzer aufgefordert, alle geöffneten Dokumente zu speichern, und wird dann sofort von der Streaming-Instance getrennt. Die vom Benutzer verwendete Instance wird dann beendet.

- Wählen Sie für Idle disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung bei Leerlauf in Minuten) die Zeitspanne aus, für die Benutzer im Leerlauf (inaktiv) verbleiben können, bevor sie von ihrer Streaming-Sitzung getrennt werden und bevor das Zeitintervall unter Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) beginnt. Benutzer werden benachrichtigt, bevor sie aufgrund von Inaktivität getrennt werden. Wenn sie versuchen, vor Ablauf des unter Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) angegebenen Zeitintervalls wieder eine Verbindung mit der Streaming-Sitzung herzustellen, werden sie mit ihrer vorherigen Sitzung verbunden. Andernfalls werden sie mit einer neuen Sitzung mit einer neuen Streaming-Instance verbunden. Die Einstellung wird durch den Wert „0“ deaktiviert. Wenn dieser Wert deaktiviert ist, werden Benutzer nicht aufgrund von Inaktivität getrennt.

> **Note**
>
> Benutzer gelten als inaktiv, wenn sie während ihrer Streaming-Sitzung keine Tastatur- oder Mauseingabe mehr machen. Datei-Uploads und -Downloads, Audio-Eingabe, Audio-Ausgabe und Pixeländerungen gelten nicht als Benutzeraktivitäten. Wenn Benutzer nach Ablauf des Zeitintervalls unter Idle disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung bei Leerlauf in Minuten) weiterhin inaktiv sind, wird ihre Verbindung getrennt.

Identitätsanbieter konfigurieren

Führen Sie die folgenden Schritte aus, um Ihren Identitätsanbieter (IdP) zu konfigurieren.

Themen

- Wählen Sie den Identitätsanbietertyp
- Konfigurieren des Standardauthentifizierungstyps
- Konfigurieren des IAM-Identity-Center-Authentifizierungstyps

- Ändern des Identitätsanbietertyps

Wählen Sie den Identitätsanbietertyp

WorkSpaces Web bietet zwei Authentifizierungstypen: Standard und AWS IAM Identity Center. Auf der Seite Identitätsanbieter konfigurieren wählen Sie den Authentifizierungstyp aus, der mit Ihrem Portal verwendet werden soll.

- Verbinden Sie Ihren externen SAML-2.0-Identitätsanbieter (z. B. Okta oder Ping) direkt mit Ihrem Portal für Standard (Standardoption). Weitere Informationen finden Sie unter the section called “Konfigurieren des Standardauthentifizierungstyps”. Der Standardtyp unterstützt sowohl SP-initiierte als auch IdP-initiierte Authentifizierungsabläufe.
- Verbinden Sie für IAM Identity Center (erweiterte Option) das IAM Identity Center mit Ihrem Portal. Um diesen Authentifizierungstyp verwenden zu können, müssen sich Ihr IAM Identity Center und Ihr WorkSpaces Webportal beide im selben befinden AWS-Region. Weitere Informationen finden Sie unter the section called “Konfigurieren des IAM-Identity-Center-Authentifizierungstyps”.

Konfigurieren des Standardauthentifizierungstyps

Verbinden Sie Ihren externen SAML-2.0-Identitätsanbieter (wie Okta oder Ping) direkt mit Ihrem Portal.

Der Standard identitätstypkann (SP-initiiert) und identity-provider-initiated (IdPinitiiert) Anmeldeabläufe mit Ihrem SAML-2.0IdP unterstützen service-provider-initiated.

Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters in WorkSpaces Web

Führen Sie die folgenden Schritte aus, um Ihren Identitätsanbieter zu konfigurieren:

1. Wählen Sie auf der Seite Identitätsanbieter konfigurieren des Erstellungsassistenten die Option Standard aus.
2. Wählen Sie Mit Standard-IdP fortfahren aus.
3. Laden Sie die SP-Metadatendatei herunter und lassen Sie die Registerkarte für einzelne Metadatenwerte geöffnet.
   - Wenn die SP-Metadatendatei verfügbar ist, wählen Sie Metadatendatei herunterladen, um das Metadatendokument des Serviceanbieters (SP) herunterzuladen, und laden Sie die Metadatendatei des Serviceanbieters im nächsten Schritt auf Ihren IdP hoch. Andernfalls können sich Benutzer nicht anmelden.

- Wenn Ihr Anbieter keine SP-Metadatendateien hochlädt, geben Sie die Metadatenwerte manuell ein.

4. Wählen Sie unter SAML-Anmeldetyp auswählen zwischen SP-initiierten und IdP-initiierten SAML-Assertionen oder nur SP-initiierten SAML-Assertionen aus.
   - SP-initiierte und IdP-initiierte SAML-Assertionen ermöglichen es Ihrem Portal, beide Arten von Anmeldeabläufen zu unterstützen. Portale, die IdP initiierte Flows unterstützen, ermöglichen es Ihnen, dem Endpunkt des Service-Identitätsverbunds SAML-Assertionen anzuzeigen, ohne dass Benutzer eine Sitzung starten müssen, indem sie die Portal-URL besuchen.
     - Wählen Sie dies aus, damit das Portal unerwünschteIdP initiierte SAML-Assertions akzeptieren kann.
     - Für diese Option muss ein Standard-Relay-Status in Ihrem SAML-2.0-Identitätsanbieter konfiguriert sein. Der Relay-Statusparameter für Ihr Portal befindet sich in der Konsole unter IdP initiierte SAML-Anmeldung. Sie können ihn auch aus der SP-Metadatendatei unter kopieren`<md:IdPInitRelayState>`.
     - Hinweis
       - Im Folgenden finden Sie das Format des Relay-Status: `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=ExIdentity-Provider`.
       - Wenn Sie den Wert aus der SP-Metadatendatei kopieren und einfügen, stellen Sie sicher, dass Sie `&` zu ändern&. `&` ist ein XML-Escape-Zeichen.
   - Wählen Sie SP-initiierte SAML-Assertions nur für das Portal aus, um nur SP-initiierte Anmeldeabläufe zu unterstützen. Diese Option lehnt unerwünschte SAML-Assertionen von IdP initiierten Anmeldeabläufen ab.

> **Note**
>
> Einige Drittanbieter IdPs ermöglichen es Ihnen, eine benutzerdefinierte SAML-Anwendung zu erstellen, die IdP-initiierte Authentifizierungserlebnisse mithilfe von SP-initiierten Flows bieten kann. Ein Beispiel finden Sie unter Eine Okta-Lesezeichenanwendung hinzufügen.

5. Wählen Sie aus, ob Sie SAML-Anforderungen an diesen Anbieter signieren möchten. Durch die SP-initiierte Authentifizierung kann Ihr IdP überprüfen, ob die Authentifizierungsanforderung vom Portal stammt, wodurch verhindert wird, dass andere Anforderungen von Drittanbietern akzeptiert werden.

a. Laden Sie das Signaturzertifikat herunter und laden Sie es auf Ihren IdP hoch. Dasselbe Signaturzertifikat kann für die einzelne Abmeldung verwendet werden.

b. Aktivieren Sie die signierte Anforderung in Ihrem IdP . Der Name kann je nach IdP unterschiedlich sein.

> **Note**
>
> RSA-SHA256 ist der einzige unterstützte Anforderungs- und Standard-Signaturalgorithmus.

6. Wählen Sie aus, ob Sie die Option Verschlüsselte SAML-Assertions erforderlich aktivieren möchten. Auf diese Weise können Sie die SAML-Assertion verschlüsseln, die von Ihrem IdP stammt. Dadurch kann verhindert werden, dass Daten in SAML-Assertionen zwischen dem IdP und WorkSpaces Web abgefangen werden.

> **Note**
>
> Das Verschlüsselungszertifikat ist in diesem Schritt nicht verfügbar. Sie wird nach dem Start Ihres Portals erstellt. Nachdem Sie das Portal gestartet haben, laden Sie das Verschlüsselungszertifikat herunter und laden Sie es auf Ihren IdP hoch. Aktivieren Sie dann die Assertion-Verschlüsselung in Ihrem IdP (der Name kann je nach IdP unterschiedlich sein.

7. Wählen Sie aus, ob Sie Single Logout aktivieren möchten. Mit einer einzigen Abmeldung können sich Ihre Endbenutzer mit einer einzigen Aktion sowohl von ihrem IdP als auch von der WorkSpaces Web-Sitzung abmelden.

   a. Laden Sie das Signaturzertifikat von WorkSpaces Web herunter und laden Sie es auf Ihren IdP hoch. Dies ist dasselbe Signaturzertifikat, das im vorherigen Schritt für die Anforderungssignierung verwendet wurde.

   b. Für die Verwendung von Single Logout müssen Sie eine Single-Logout-URL in Ihrem SAML-2.0-Identitätsanbieter konfigurieren. Sie finden die Single-Logout-URL für Ihr Portal in der Konsole unter Serviceanbieter (SP)-Details – Einzelne Metadatenwerte anzeigen oder aus der SP-Metadatendatei unter `<md:SingleLogoutService>` .

   c. Aktivieren Sie Single Logout in Ihrem IdP . Der Name kann je nach IdP unterschiedlich sein.

Schritt 2: Konfigurieren Ihres Identitätsanbieters auf Ihrem eigenen IdP

Öffnen Sie eine neue Registerkarte in Ihrem Browser. Schließen Sie dann die folgenden Schritte mit Ihrem Identitätsanbieter ab:

1. Fügen Sie Ihre Portalmetadaten zu Ihrem SAML-IdP hinzu.

   Laden Sie entweder das SP-Metadatendokument, das Sie im vorherigen Schritt heruntergeladen haben, in Ihren IdP hoch oder kopieren Sie die Metadatenwerte und fügen Sie sie in die richtigen Felder in Ihrem IdP ein. Einige Anbieter erlauben keinen Datei-Upload.

   Die Details dieses Prozesses können je nach Anbieter variieren. In der Dokumentation Ihres Anbieters finden Sie Hilfe the section called “Anleitung für bestimmte IdPs” dazu, wie Sie die Portaldetails zu Ihrer IdP-Konfiguration hinzufügen.

2. Bestätigen Sie die NameID für Ihre SAML-Assertion.

   Stellen Sie sicher, dass Ihr SAML-IdP NameID in der SAML-Assertion mit dem Benutzer-E-Mail-Feld auffüllt. NameID und Benutzer-E-Mail werden verwendet, um Ihren SAML-Verbundbenutzer mit dem Portal eindeutig zu identifizieren. Verwenden Sie das persistente SAML-Namen-ID-Format.

3. Optional: Konfigurieren Sie den Relay-Status für die IdP initiierte Authentifizierung.

   Wenn Sie im vorherigen Schritt SP-initiierte und IdP-initiierte SAML-Assertionen akzeptieren ausgewählt haben, führen Sie die Schritte in Schritt 2 von aus, the section called “Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters in WorkSpaces Web” um den Standard-Relay-Status für Ihre IdP-Anwendung festzulegen.

4. Optional: Konfigurieren Sie die Anforderungssignierung . Wenn Sie im vorherigen Schritt SAML-Anforderungen an diesen Anbieter signieren ausgewählt haben, führen Sie die Schritte in Schritt 3 von aus, the section called “Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters in WorkSpaces Web” um das Signaturzertifikat auf Ihren IdP hochzuladen und die Anforderungssignierung zu aktivieren. Einige IdPs wie Okta erfordern möglicherweise, dass Ihre NameID zum Typ „persistent“ gehört, um die Anforderungssignierung zu verwenden. Bestätigen Sie unbedingt Ihre NameID für Ihre SAML-Assertion, indem Sie die oben genannten Schritte ausführen.

5. Optional: Konfigurieren der Assertion-Verschlüsselung . Wenn Sie Verschlüsselte SAML-Assertionen von diesem Anbieter anfordern ausgewählt haben, warten Sie, bis die Portalerstellung abgeschlossen ist, und folgen Sie dann Schritt 4 unter „Metadaten hochladen“ unten, um das

Verschlüsselungszertifikat auf Ihren IdP hochzuladen und die Assertionsverschlüsselung zu aktivieren.

6. Optional: Konfigurieren Sie Single Logout . Wenn Sie Single Logout ausgewählt haben, führen Sie die Schritte in Schritt 5 von aus, the section called “Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters in WorkSpaces Web” um das Signaturzertifikat auf Ihren IdP hochzuladen, Single Logout URL auszufüllen und Single Logout zu aktivieren.
7. Gewähren Sie Ihren Benutzern in Ihrem IdP Zugriff auf die Verwendung von WorkSpaces Web.
8. Laden Sie eine Metadaten-Austauschdatei von Ihrem Identitätsanbieter herunter. Sie laden diese Metadaten im nächsten Schritt in WorkSpaces Web hoch.

Schritt 3: Abschluss der Konfiguration Ihres Identitätsanbieters in WorkSpaces Web

Kehren Sie zur WorkSpaces Webkonsole zurück. Laden Sie auf der Seite Identitätsanbieter konfigurieren des Erstellungsassistenten unter IdP-Metadaten entweder eine Metadatendatei hoch oder geben Sie eine Metadaten-URL von Ihrem IdP ein. Das Portal verwendet diese Metadaten von Ihrem IdP, um Vertrauen zu schaffen.

1. Um eine Metadatendatei hochzuladen, wählen Sie unter IdP-Metadatendokument die Option Datei auswählen aus. Laden Sie die XML-formatierte Metadatendatei von Ihrem Identitätsanbieter hoch, die Sie im vorherigen Schritt heruntergeladen haben.
2. Um eine Metadaten-URL zu verwenden, gehen Sie zu Ihrem IdP, den Sie im vorherigen Schritt eingerichtet haben, und rufen Sie die Metadaten-URL ab. Gehen Sie zurück zur WorkSpaces Webkonsole und geben Sie unter IdP-Metadaten-URL die Metadaten-URL ein, die Sie von Ihrem IdP erhalten haben.
3. Klicken Sie anschließend auf Next.
4. Für Portale, in denen Sie die Option Verschlüsselte SAML-Assertionen von diesem Anbieter anfordern aktiviert haben, müssen Sie das Verschlüsselungszertifikat aus dem Abschnitt mit den Details des Portal-IdP herunterladen und es auf Ihren IdP hochladen. Anschließend können Sie die Option dort aktivieren.

> **Note**
>
> WorkSpaces Web erfordert, dass der Betreff oder die NameID zugeordnet und in der SAML-Assertion innerhalb der Einstellungen Ihres IdP festgelegt wird. Ihr Identitätsanbieter kann diese Zuordnungen automatisch erstellen. Wenn diese Zuordnungen nicht korrekt

konfiguriert sind, können sich Ihre Benutzer nicht beim Webportal anmelden und keine Sitzung starten.
WorkSpaces Web erfordert, dass die folgenden Ansprüche in der SAML-Antwort vorhanden sind. Sie finden *<Ihre SP-Entitäts-ID>* und *<Ihre SP-ACS-URL>* in den Serviceanbieterdetails oder Metadatendokumenten Ihres Portals, entweder über die Konsole oder die CLI.

- Ein -`AudienceRestriction`Anspruch mit einem -`Audience`Wert, der Ihre SP-Entitäts-ID als Ziel der Antwort festlegt. Beispiel:

```
<saml:AudienceRestriction>
    <saml:Audience><Your SP Entity ID></saml:Audience>
</saml:AudienceRestriction>
```

- Ein `Response`-Anspruch mit einem `InResponseTo`-Wert, der der ursprünglichen SAML-Anforderungs-ID entspricht. Beispiel:

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId>">
```

- Ein -`SubjectConfirmationData`Anspruch mit einem `Recipient` Wert Ihrer SP-ACS-URL und einem -`InResponseTo`Wert, der der ursprünglichen SAML-Anforderungs-ID entspricht. Beispiel:

```
<saml:SubjectConfirmation>
    <saml:SubjectConfirmationData ...
        Recipient="<Your SP ACS URL>"
        InResponseTo="<originalSAMLrequestId>"
        />
</saml:SubjectConfirmation>
```

WorkSpaces Webvalidiert Ihre Anforderungsparameter und SAML-Assertions. Für IdP initiierte SAML-Assertionen müssen die Details Ihrer Anforderung als `RelayState` Parameter im Text einer HTTP POST-Anforderung formatiert sein. Der Anforderungstext muss auch Ihre SAML-Assertion als `SAMLResponse` Parameter enthalten. Beide sollten vorhanden sein, wenn Sie den vorherigen Schritt befolgt haben.
Im Folgenden finden Sie einen `POST` Beispieltext für einen IdP initiierten SAML-Anbieter.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

Anleitung für bestimmte IdPs

Um sicherzustellen, dass Sie den SAML-Verbund für Ihr Portal korrekt konfigurieren, finden Sie unter den Links unten eine Dokumentation von häufig verwendeten IdPs.

IdP	Einrichtung der SAML-Anwendung	Benutzerverwaltung	IdP initiierte Authentifizierung	Signieren von Anforderungen	Assertion-Verschlüsselung	Einzelne Abmeldung
Okta	Erstellen von SAML-App-Integrationen	Benutzerverwaltung	SAML-Feldreferenz für den Application Integration Wizard	SAML-Feldreferenz für den Application Integration Wizard	SAML-Feldreferenz für den Application Integration Wizard	SAML-Feldreferenz für den Application Integration Wizard
Entra	Erstellen Ihrer eigenen Anwendung	Schnellstart: Erstellen und Zuweisen eines Benutzerkontos	Aktivieren von Single Sign-On für eine Unternehmensanwendung	Signaturüberprüfung für SAML-Anfragen	Konfigurieren der Microsoft Entra SAML-Token-Verschlüsselung	Single-Sign-Out-SAML-Protokoll
Ping	Hinzufügen einer SAML-Anwendung	Benutzer	Aktivieren des IdP initiierten SSO	Konfigurieren der Anmeldung bei Authentifizierungsanforderungen PingOne für Enterprise	Unterstützt PingOne for Enterprise Verschlüsselung?	SAML-2.0-Einzelabmeldung

IdP	Einrichtung der SAML-Anwendung	Benutzerverwaltung	IdP initiierte Authentifizierung	Signieren von Anforderungen	Assertion-Verschlüsselung	Einzelne Abmeldung
Eine Anmeldung	SAML Custom Connector (Erweitert) (4266907)	OneLogin Manuelles Hinzufügen von Benutzern zu	SAML Custom Connector (Erweitert) (4266907)	SAML Custom Connector (Erweitert) (4266907)	SAML Custom Connector (Erweitert) (4266907)	SAML Custom Connector (Erweitert) (4266907)
IAM Identity Center	Einrichten Ihrer eigenen SAML-2.0-Anwendung	Einrichten Ihrer eigenen SAML-2.0-Anwendung	Einrichten Ihrer eigenen SAML-2.0-Anwendung	N/A	–	N/A

Konfigurieren des IAM-Identity-Center-Authentifizierungstyps

Für den Typ IAM Identity Center (erweitert) verbinden Sie IAM Identity Center mit Ihrem Portal. Wählen Sie diese Option nur aus, wenn Folgendes für Sie zutrifft:

- Ihr IAM Identity Center ist in derselben AWS-Konto und in derselben AWS-Region wie Ihr Webportal konfiguriert.
- Wenn Sie verwenden AWS Organizations, verwenden Sie ein Verwaltungskonto.

Bevor Sie ein Webportal mit dem Authentifizierungstyp IAM Identity Center erstellen, müssen Sie IAM Identity Center als eigenständigen Anbieter einrichten. Weitere Informationen finden Sie unter Erste Schritte mit allgemeinen Aufgaben im IAM Identity Center. Oder Sie können Ihren SAML-2.0-IdP mit IAM Identity Center verbinden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem externen Identitätsanbieter. Andernfalls müssen Sie Ihrem Webportal keine Benutzer oder Gruppen zuweisen.

Wenn Sie IAM Identity Center bereits verwenden, können Sie IAM Identity Center als Anbietertyp auswählen und die folgenden Schritte ausführen, um Benutzer oder Gruppen zu Ihrem Webportal hinzuzufügen, anzuzeigen oder daraus zu entfernen.

> **Note**
>
> Um diesen Authentifizierungstyp verwenden zu können, muss sich Ihr IAM Identity Center im selben AWS-Konto und in demselben AWS-Region wie Ihr WorkSpaces Webportal befinden. Wenn sich Ihr IAM Identity Center in einem separaten AWS-Konto oder befindet AWS-Region, folgen Sie den Anweisungen für den Standardauthentifizierungstyp.
> Weitere Informationen finden Sie unter the section called “Konfigurieren des Standardauthentifizierungstyps”.
> Wenn Sie verwenden AWS Organizations, können Sie WorkSpaces Webportale, die in IAM Identity Center integriert sind, nur über ein Verwaltungskonto erstellen.

So erstellen Sie ein Webportal mit IAM Identity Center

1. Wählen Sie während der Portalerstellung in Schritt 4: Identitätsanbieter konfigurieren die Option ausAWS IAM Identity Center.
2. Wählen Sie Mit IAM Identity Center fortfahren aus.
3. Wählen Sie auf der Seite Benutzer und Gruppen zuweisen die Registerkarte Benutzer und/oder Gruppen aus.
4. Aktivieren Sie das Kontrollkästchen neben dem/den Benutzer(n) oder der Gruppe(n), die Sie dem Portal hinzufügen möchten.
5. Nachdem Sie Ihr Portal erstellt haben, können sich die Benutzer, die Sie zugeordnet haben, mit ihrem Benutzernamen und Passwort bei WorkSpaces Web anmelden.

So verwalten Sie ein Webportal mit IAM Identity Center

1. Nachdem Sie Ihr Portal erstellt haben, wird es in der IAM-Identity-Center-Konsole als konfigurierte Anwendung aufgeführt.
2. Damit Sie auf die Konfiguration dieser Anwendung zugreifen können, wählen Sie in der Seitenleiste Anwendungen aus und suchen Sie nach einer konfigurierten Anwendung mit einem Namen, der dem Anzeigenamen Ihres Webportals entspricht.

> **Note**
>
> Wenn Sie keinen Anzeigenamen eingegeben haben, wird stattdessen die GUID Ihres Portals angezeigt. Die GUID ist die ID, die der Endpunkt-URL Ihres Webportals vorangestellt wird.

So fügen Sie zusätzliche Benutzer und Gruppen einem vorhandenen Webportal hinzu

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Web , Webportale , Ihr Webportal und dann Bearbeiten aus.
3. Wählen Sie Einstellungen für Identitätsanbieter und Weitere Benutzer und Gruppen zuweisen aus. Von hier aus können Sie Ihrem Webportal Benutzer und Gruppen hinzufügen.

> **Note**
>
> Sie können keine Benutzer oder Gruppen über die IAM-Identity-Center-Konsole hinzufügen. Sie müssen dies auf der Bearbeitungsseite Ihres WorkSpaces Webportals tun.

So zeigen Sie Benutzer und Gruppen für Ihr Webportal an oder entfernen sie

- Sie können den Benutzerzugriff auf diese Anwendung mithilfe der Aktionen anzeigen oder entfernen, die in der Tabelle Zugewiesene Benutzer verfügbar sind. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf Anwendungen.

> **Note**
>
> Sie können Benutzer und Gruppen nicht auf der Bearbeitungsseite des WorkSpaces Webportals anzeigen oder entfernen. Sie müssen dies von der Bearbeitungsseite Ihrer IAM-Identity-Center-Konsole aus tun.

Ändern des Identitätsanbietertyps

Gehen Sie wie folgt vor, um den Authentifizierungstyp Ihres Portals jederzeit zu ändern:

- Um von IAM Identity Center zu Standard zu wechseln, führen Sie die Schritte unter austhe section called “Konfigurieren des Standardauthentifizierungstyps”.
- Um von Standard zu IAM Identity Center zu wechseln, führen Sie die Schritte unter austhe section called “Konfigurieren des IAM-Identity-Center-Authentifizierungstyps”.

Die Bereitstellung von Änderungen am Identitätsanbietertyp kann bis zu 15 Minuten dauern und beendet laufende Sitzungen nicht automatisch.

Sie können Änderungen am Identitätsanbietertyp Ihres Portals über anzeigen, AWS CloudTrail indem Sie `UpdatePortal` Ereignisse überprüfen. Der Typ ist in den Anforderungs- und Antwortnutzlasten des Ereignisses sichtbar.

Überprüfen und starten

1. Überprüfen Sie auf der Seite Schritt 5: Überprüfen und starten die Einstellungen, die Sie für Ihr Webportal ausgewählt haben. Sie können Bearbeiten auswählen, um die Einstellungen in einem bestimmten Abschnitt zu ändern. Sie können diese Einstellungen auch später auf der Registerkarte Webportale der Konsole ändern.
2. Wenn Sie fertig sind, wählen Sie Webportal starten aus.
3. Wenn Sie den Status Ihres Webportals anzeigen möchten, wählen Sie Webportale, Ihr Portal und dann Details anzeigen aus.

   Ein Webportal hat einen der folgenden Status:

   - Unvollständig: In der Konfiguration des Webportals fehlen die erforderlichen Identitätsanbieter-Einstellungen.
   - Ausstehend: Das Webportal wendet Änderungen bei seinen Einstellungen an.
   - Aktiv: Das Webportal ist bereit und kann verwendet werden.
4. Warten Sie bis zu 15 Minuten, bis Ihr Portal aktiv wird.

Schritt 2: Ihr Webportal testen

Nachdem Sie ein Webportal erstellt haben, können Sie sich am WorkSpaces Web-Endpunkt anmelden, um Ihre verbundenen Websites wie ein Endbenutzer zu durchsuchen.

Wenn Sie diese Schritte bereits in the section called “Identitätsanbieter konfigurieren” abgeschlossen haben, können Sie diesen Abschnitt überspringen und bei Schritt 3: Ihr Webportal verteilen fortfahren.

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Web , Webportale, Ihr Webportal und dann Details anzeigen aus.
3. Rufen Sie unter Webportal-Endpunkt die angegebene URL für Ihr Portal auf. Der Webportal-Endpunkt ist der Zugangspunkt, von dem aus Ihre Benutzer Ihr Webportal starten, nachdem sie sich mit dem für das Portal konfigurierten Identitätsanbieter angemeldet haben. Er ist öffentlich im Internet verfügbar und kann in Ihr Netzwerk eingebettet werden.
4. Wählen Sie auf der WorkSpaces Web-Anmeldeseite Anmelden, SAML und geben Sie Ihre SAML-Anmeldeinformationen ein.
5. Wenn Sie die Seite Ihre Sitzung wird vorbereitet sehen, wird Ihre WorkSpaces Websitzung gestartet. Schließen oder verlassen Sie diese Seite nicht.
6. Der Webbrowser wird gestartet und zeigt Ihre Startup-URL und jedes andere zusätzliche Verhalten an, das in den Richtlinieneinstellungen Ihres Browsers konfiguriert wurde.
7. Sie können jetzt zu verbundenen Websites navigieren, indem Sie Links auswählen oder URLs in die Adressleiste eingeben.

Schritt 3: Ihr Webportal verteilen

Wenn Sie bereit sind, dass Ihre Benutzer WorkSpaces Web verwenden können, wählen Sie eine der folgenden Optionen, um das Portal zu verteilen:

- Fügen Sie Ihr Portal Ihrem SAML-Anwendungs-Gateway hinzu, damit Benutzer eine Sitzung direkt von ihrem Identitätsanbieter aus starten können. Weitere Informationen finden Sie beispielsweise unter Eine Lesezeichen-App-Integration erstellen.
- Fügen Sie die Portal-URL einer Website hinzu, deren Besitzer Sie sind, und verwenden Sie eine Browserumleitung, um Benutzer zum Webportal weiterzuleiten.
- Senden Sie die Portal-URL per E-Mail an Ihre Benutzer oder übertragen Sie sie auf ein Gerät, das Sie als Browserstartseite oder als Lesezeichen verwalten.

Nächste Schritte

Nachdem Sie Ihr erstes Webportal erstellt haben, können Sie jederzeit Details anzeigen, Details bearbeiten oder das Webportal löschen. Weitere Informationen finden Sie unter Verwalten Ihres Webportals.

Ihr AWS-Konto kann in jeder , in AWS-Region der WorkSpaces Web verfügbar ist, ein Webportal erstellen. Jedes Webportal kann bis zu 25 Benutzerverbindungen gleichzeitig unterstützen. Informationen zur Erhöhung der Anzahl der Portale, die Sie in einer Region erstellen können, oder zur Unterstützung mehrerer gleichzeitiger Sitzungen für ein Portal finden Sie unter the section called “Eine Erhöhung des Service-Kontingents anfordern”.

Verwalten Ihres Webportals

Nachdem Sie Ihr Webportal eingerichtet haben, können Sie dessen Details anzeigen oder bearbeiten sowie das Portal löschen, falls es nicht mehr benötigt wird.

Themen

- Webportal-Details anzeigen
- Ein Webportal bearbeiten
- Ein Webportal löschen
- Eine Erhöhung des Service-Kontingents anfordern
- Das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens steuern
- Benutzerzugriffsprotokollierung einrichten
- Ihre Browser-Richtlinie festlegen oder bearbeiten
- Den Eingabemethoden-Editor (IME) konfigurieren
- Die sitzungsinterne Lokalisierung konfigurieren
- IP-Zugriffskontrollen einrichten (optional)
- Erweiterung für Single-Sign-On aktivieren (optional)
- URL-Filterung einrichten

Webportal-Details anzeigen

So zeigen Sie Webportal-Details an

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Web , Webportale, Ihr Webportal und dann Details anzeigen aus.

Ein Webportal bearbeiten

So bearbeiten Sie ein Webportal

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.

2. Wählen Sie WorkSpaces Web , Webportale, Ihr Webportal und dann Bearbeiten aus.

> **Note**
>
> Änderungen an den Netzwerkeinstellungen oder den Einstellungen für die Zeitüberschreitung beenden sofort alle aktiven Portalsitzungen. Benutzer werden getrennt und müssen sich erneut verbinden, um eine neue Sitzung zu beginnen. Änderungen der Zwischenablageberechtigungen, der Dateiübertragungsberechtigungen oder Auf lokalem Gerät ausdrucken gelten ab der ersten neuen Sitzung. Derzeit aktive Sitzungen werden nicht getrennt. Bei Benutzern, die mit aktiven Sitzungen verbunden sind, werden die Änderungen erst wirksam, wenn sie die Verbindung trennen und eine Verbindung mit einer neuen Sitzung herstellen.

Ein Webportal löschen

So löschen Sie ein Webportal

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Web , Webportale , Ihr Webportal und dann Löschen aus.

Eine Erhöhung des Service-Kontingents anfordern

Wenn Sie Ihr AWS Konto erstellen, legen wir automatisch Standard-Servicekontingente (auch als Limits bezeichnet) für die Ressourcennutzung mit AWS Services fest. WorkSpaces Web legt Kontingente für zwei Arten von Ressourcen fest – Webportale (pro Region) und maximale Anzahl gleichzeitiger Sitzungen (pro Webportal). WorkSpaces Web hat derzeit die folgenden Service Quotas-Limits:

Standardkontingente innerhalb eines AWS-Region nach Konto	Wert
Webportale	1
Maximum gleichzeitiger Sitzungen	25

Ein Webportal ist die grundlegende Ressource in WorkSpaces Web. Es ist die Verbindung zwischen Ihrem SAML-2.0-Identitätsanbieter und Ihrer Netzwerkverbindung zum Internet und Ihren Inhalten. Sie können ein Webportal in jeder erstellen AWS-Region , in der WorkSpaces Web verfügbar ist. Informationen zur aktuellen Verfügbarkeit finden Sie in der Regionstabelle.

Die maximale Anzahl gleichzeitiger Sitzungen ist die höchste Anzahl von Benutzern, die gleichzeitig mit einem bestimmten Webportal verbunden werden. Wenn das Servicekontingentlimit für maximale gleichzeitige Sitzungen nicht angemessen festgelegt ist, stellen Benutzer möglicherweise fest, dass ihre Sitzung nicht verfügbar ist, wenn sie sich bei WorkSpaces Web anmelden. Sie sollten auch sicherstellen, dass Ihre VPC und Subnetze über einen ausreichenden IP-Bereich verfügen, um die maximale Anzahl gleichzeitiger Sitzungen zu unterstützen. Andernfalls können Benutzer möglicherweise keine Verbindung mit einer Sitzung herstellen.

Beispiel: Ein Kunde hat zwei Webportale in USA Ost (Nord-Virginia) und 125 Benutzer. Das erste Webportal (Portal A) hat 25 Benutzer und erfordert keine Service-Quota-Erhöhung. Das zweite Webportal (Portal B) muss für bis zu 100 Benutzer verfügbar sein. Diese Benutzer sind auf zwei Schichten verteilt, und ihre Arbeitszeiten überschneiden sich nicht. Daher müsste der Kunde eine Service-Quota-Erhöhung für Portal B auf eine maximale gleichzeitige Sitzung von 50 Benutzern beantragen.

Sie können eine Erhöhung für eine dieser Service-Quota-Limits beantragen. Weitere Informationen finden Sie unter Anfordern einer Kontingenterhöhung.

So fordern Sie eine Erhöhung Ihrer Service Quota an

1. Öffnen Sie das AWS-Support-Dashboard.
2. Wählen Sie Erhöhung des Servicelimits aus.

> **Important**
>
> WorkSpaces Webservicekontingente betreffen jeweils eine Region. Sie müssen in jeder AWS-Region eine Service-Quota-Erhöhung beantragen, in der Sie mehr Ressourcen benötigen. Weitere Informationen finden Sie unter AWS-Service-Endpunkte.

3. Geben Sie in der Beschreibung des Anwendungsfalls die folgenden Informationen an:

   - Wenn Sie eine Erhöhung der Webportal-Anzahl beantragen, geben Sie diesen Ressourcentyp und Ihre AWS-Konto-ID, die Region, in der Sie die Erhöhung wünschen, und den neuen Grenzwert an.

- Wenn Sie eine Erhöhung der maximal möglichen gleichzeitigen Sitzungen beantragen, geben Sie diesen Ressourcentyp und Ihre AWS-Konto-ID, die Region, in der Sie die Erhöhung wünschen, den ARN des Webportals und den neuen Grenzwert an.

4. (Optional) Um mehrere Service-Quota-Erhöhungen gleichzeitig zu beantragen, füllen Sie eine Anfrage zur Erhöhung des Kontingents im Abschnitt „Anfragen“ aus und wählen Sie dann Weitere Anfrage hinzufügen aus.

Das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens steuern

Wenn ein Benutzer ein WorkSpaces Webportal besucht, kann er sich anmelden, um eine Streaming-Sitzung zu starten. Jede Sitzung beginnt auf der Startseite, sofern sie sich nicht vor weniger als 5 Minuten angemeldet haben. Das Portal sucht nach Identitätsanbieter-Token, um festzustellen, ob der Benutzer beim Starten einer Sitzung zur Eingabe von Anmeldeinformationen aufgefordert werden soll. Ein Benutzer ohne gültiges Identitätsanbieter-Token muss einen Benutzernamen, ein Passwort und (optional) eine Multifaktor-Authentifizierung (MFA) eingeben, um eine Streaming-Sitzung zu starten. Wenn ein Benutzer bereits ein SAML-IdP-Token generiert hat, indem er sich bei seinem Identitätsanbieter oder einer von demselben Identitätsanbieter geschützten App angemeldet hat, wird er nicht nach Anmeldeinformationen gefragt.

Wenn ein Benutzer über ein gültiges SAML-IdP-Token verfügt, kann er auf WorkSpaces Web zugreifen. Sie können das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens steuern.

So steuern Sie das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens

1. Legen Sie die Dauer der Zeitüberschreitung vom Identitätsanbieter bei Ihrem SAML-Identitätsanbieter fest. Wir empfehlen, die Dauer der Zeitüberschreitung vom Identitätsanbieter so zu konfigurieren, dass die kürzeste Zeit gewählt wird, die ein Benutzer benötigt, um seine Aufgaben zu erledigen.

   - Weitere Informationen zu Okta finden Sie unter Eine begrenzte Sitzungsdauer für alle Richtlinien durchsetzen.
   - Weitere Informationen zu Azure AD finden Sie unter Konfigurieren der Sitzungssteuerelemente für Authentifizierung.
   - Weitere Informationen zu Sitzungen finden Sie unter Sitzungen.

- Weitere Informationen zu finden Sie AWS IAM Identity Centerunter Festlegen der Sitzungsdauer.

2. Legen Sie die Inaktivitäts- und Leerlauf-Timeout-Werte Ihres WorkSpaces Webportals fest. Diese Werte steuern die Zeit zwischen der letzten Interaktion eines Benutzers und dem Ende einer WorkSpaces Websitzung aufgrund von Inaktivität. Wenn eine Sitzung endet, verliert ein Benutzer seinen Sitzungsstatus (einschließlich geöffneter Registerkarten, nicht gespeicherter Webinhalte und Verlauf) und kehrt zu Beginn der nächsten Sitzung in einen neuen Status zurück. Weitere Informationen finden Sie in Schritt 5 unter the section called “Schritt 1: Ein Webportal erstellen”.

> **Note**
>
> Wenn bei der Sitzung eines Benutzers eine Zeitüberschreitung auftritt, der Benutzer jedoch immer noch über ein gültiges SAML-IdP-Token verfügt, muss er seinen Benutzernamen und sein Passwort nicht eingeben, um eine neue WorkSpaces Websitzung zu starten. Um zu kontrollieren, wie Token erneut authentifiziert werden, folgen Sie den Anleitungen im vorherigen Schritt.

Benutzerzugriffsprotokollierung einrichten

Sie können die Benutzerzugriffsprotokollierung einrichten, um folgende Benutzerereignisse aufzuzeichnen:

- Sitzungsstart – Markiert den Anfang einer WorkSpaces Web-Sitzung.
- Sitzungsende – Markiert das Ende einer WorkSpaces Websitzung.
- URL-Navigation: Protokolliert die URL, die ein Benutzer lädt.

> **Note**
>
> URL-Navigationsprotokolle werden aus dem Browserverlauf aufgezeichnet. URLs, die nicht im Browserverlauf aufgezeichnet wurden (entweder im Inkognitomodus besucht oder aus dem Browserverlauf gelöscht), werden nicht in Protokollen aufgezeichnet. Es liegt an den Kunden, anhand ihrer Browser-Richtlinie zu entscheiden, ob sie den Inkognitomodus oder das Löschen des Verlaufs deaktivieren möchten.

Darüber hinaus sind für jedes Ereignis die folgenden Informationen enthalten:

- Ereigniszeit
- Username
- Webportal-ARN

Kunden sind dafür verantwortlich, die potenziellen rechtlichen Probleme zu verstehen, die sich aus ihrer Nutzung von WorkSpaces Web ergeben, und sicherzustellen, dass ihre Nutzung von WorkSpaces Web allen geltenden Gesetzen und Vorschriften entspricht. Dazu gehören Gesetze, die die Fähigkeit eines Arbeitgebers regulieren, die Nutzung von WorkSpaces Web durch einen Mitarbeiter zu überwachen, einschließlich Aktivitäten, die innerhalb der Anwendung ausgeführt werden.

Das Aktivieren von Benutzerzugriffsprotokollen in Ihrem WorkSpaces Webportal kann zu Gebühren von Amazon Kinesis Data Streams führen. Weitere Details zu den Preisen finden Sie unter Amazon Kinesis Data Streams – Preise.

Um die Benutzerzugriffsprotokollierung in der WorkSpaces Webkonsole zu aktivieren, wählen Sie unter Benutzerzugriffsprotokollierung die Kinesis-Stream-ID aus, die Sie zum Empfangen von Daten verwenden möchten. Die aufgezeichneten Daten werden direkt in diesen Stream übertragen.

Weitere Informationen zur Erstellung eines Amazon-Kinesis-Datenstroms finden Sie unter Was sind Amazon Kinesis Data Streams?

> **Note**
>
> Um Protokolle von WorkSpaces Web zu empfangen, benötigen Sie einen Amazon Kinesis Data Stream, der mit „amazon-workspaces-web-*“ beginnt. Für Ihren Amazon Kinesis-Datenstrom muss entweder die serverseitige Verschlüsselung deaktiviert sein oder für die Von AWS verwaltete Schlüssel serverseitige Verschlüsselung verwenden.
> Weitere Informationen zur Einstellung der serverseitigen Verschlüsselung in Amazon Kinesis finden Sie unter Wie beginne ich mit serverseitiger Verschlüsselung?.

Beispielprotokolle

Im Folgenden finden Sie ein Beispiel für jedes verfügbare Ereignis, einschließlich Validierung , StartSessionVisitPage, und EndSession.

Die folgenden Felder sind immer für jedes Ereignis enthalten:

- timestamp ist als Epochenzeit in Millisekunden enthalten.
- EventType ist als Zeichenfolge enthalten.
- details ist als weiteres JSON-Objekt enthalten.
- portalArn und userName sind für jedes Ereignis mit Ausnahme von Validation enthalten.

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
```

```
}
```

Ihre Browser-Richtlinie festlegen oder bearbeiten

Mit WorkSpaces Web können Sie eine benutzerdefinierte Browserrichtlinie mithilfe von Chrome-Richtlinien festlegen, die für die neueste stabile Version verfügbar sind. Es gibt mehr als 300 Richtlinien, die Sie auf ein Webportal anwenden können. Weitere Informationen finden Sie unter the section called “Eine benutzerdefinierte Browser-Richtlinie festlegen (Beispiel)” und in der Liste der Chrome Unternehmensrichtlinien.

Wenn Sie die Konsolenansicht verwenden, um ein Webportal zu erstellen, können Sie die folgenden Richtlinien anwenden:

- `StartURL`
- Lesezeichen und Lesezeichenordner
- Aktivieren und Deaktivieren von privatem Browsing
- Löschung des Verlaufs
- URL-Filterung mit `AllowURL` und `BlockURL`

Weitere Informationen über die Verwendung von Richtlinien für die Konsolenansicht finden Sie unter Erste Schritte mit Amazon WorkSpaces Web.

WorkSpaces Web wendet eine grundlegende Browserrichtlinienkonfiguration auf alle Portale zusammen mit allen von Ihnen angegebenen Richtlinien an. Sie können einige dieser Richtlinien mit Ihrer benutzerdefinierten JSON-Datei bearbeiten. Weitere Informationen finden Sie unter the section called “Bearbeiten Sie die grundlegende Browser-Richtlinie”.

Themen

- Eine benutzerdefinierte Browser-Richtlinie festlegen (Beispiel)
- Bearbeiten Sie die grundlegende Browser-Richtlinie

Eine benutzerdefinierte Browser-Richtlinie festlegen (Beispiel)

Sie können jede unterstützte Chrome-Richtlinie für Linux festlegen, indem Sie eine JSON-Datei hochladen. Weitere Informationen zu den Chrome-Richtlinien finden Sie in der Liste der Chrome

Unternehmensrichtlinien. Wählen Sie dort die Linux-Plattform aus. Suchen und überprüfen Sie dann die Richtlinien für die neueste stabile Version.

Im folgenden Beispiel erstellen Sie ein Webportal mit den folgenden Richtlinienkontrollen:

- Lesezeichen einrichten
- Standard-Startseiten einrichten
- Verhindern, dass der Benutzer andere Erweiterungen installiert
- Verhindern, dass der Benutzer den Verlauf löscht
- Verhindern, dass der Benutzer auf den Inkognitomodus zugreift
- Installieren Sie vorab die Erweiterung Okta-Plug-in für alle Sitzungen.

Themen

- Schritt 1: Ein Webportal erstellen
- Schritt 2: Richtlinien sammeln
- Schritt 3: Eine benutzerdefinierte JSON-Richtliniendatei erstellen
- Schritt 4: Ihre Richtlinien zur Vorlage hinzufügen
- Schritt 5: Laden Sie Ihre JSON-Datei für Richtlinien auf Ihr Webportal hoch

Schritt 1: Ein Webportal erstellen

Um Ihre Chrome-Richtlinien-JSON-Datei hochzuladen, müssen Sie ein WorkSpaces Webportal erstellen. Weitere Informationen finden Sie unter the section called “Schritt 1: Ein Webportal erstellen”.

Schritt 2: Richtlinien sammeln

Suchen Sie in den Chrome-Richtlinien nach gewünschten Richtlinien. Sie verwenden dann die Richtlinien, um im nächsten Schritt eine JSON-Datei zu erstellen.

1. Gehen Sie zur Liste der Chrome-Unternehmensrichtlinien.
2. Wählen Sie die Plattform Linux und dann die neueste Chrome-Version aus.
3. Suchen Sie nach den Richtlinien, die Sie festlegen möchten. Suchen Sie in diesem Beispiel nach Erweiterungen, um Richtlinien für deren Verwaltung zu finden. Jede Richtlinie enthält eine Beschreibung, einen Namen für die Linux-Einstellung und einen Beispielwert.

4. Aus den Suchergebnissen gehen 3 Richtlinien hervor, die bei gemeinsamer Verwendung die Unternehmensanforderungen erfüllen:
   - ExtensionSettings – installiert eine Erweiterung beim Start des Browsers.
   - ExtensionInstallBlocklist – verhindert die Installation bestimmter Erweiterungen.
   - ExtensionInstallAllowlist – Ermöglicht die Installation bestimmter Erweiterungen.
5. Zusätzliche Richtlinien erfüllen die verbleibenden Anforderungen;
   - ManagedBookmarks – Fügt Lesezeichen zu Webseiten hinzu.
   - RestoreOnStartupURLs – Konfiguriert, welche Webseiten geöffnet werden, wenn ein neues Browserfenster gestartet wird.
   - AllowDeletingBrowserHistory – Konfiguriert, ob Benutzer ihren Browserverlauf löschen können.
   - IncognitoModeAvailability – Konfiguriert, ob Benutzer auf den Inkognitomodus zugreifen können.

Schritt 3: Eine benutzerdefinierte JSON-Richtliniendatei erstellen

Erstellen Sie eine JSON-Datei mit einem Texteditor, einer Vorlage und den Richtlinien, die Sie im vorherigen Schritt gefunden haben.

1. Öffnen Sie einen Texteditor.
2. Kopieren Sie die folgende Vorlage und fügen Sie ihn in Ihren Texteditor ein:

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
```

```
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
        {
            "value":
            [
                "startup-url"
            ]
        },
        "ExtensionInstallBlocklist": {
            "value": [
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

Schritt 4: Ihre Richtlinien zur Vorlage hinzufügen

Fügen Sie der Vorlage Ihre benutzerdefinierten Richtlinien für jede Unternehmensanforderung hinzu.

1. Richten Sie Lesezeichen-URLs ein.
   a. Fügen Sie unter dem `value`-Schlüssel für jedes hinzuzufügende Lesezeichen die Schlüsselpaare `name` und `url` hinzu.
   b. Setzen Sie `bookmark-url-1` auf `https://www.amazon.com`.
   c. Setzen Sie `bookmark-url-2` auf `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`.

```
    "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. Richten Sie die Startup-URLs ein. Mit dieser Richtlinie können Administratoren die Webseiten festlegen, die angezeigt werden, wenn ein Benutzer ein neues Browserfenster öffnet.
   a. Legen Sie den Wert für `RestoreOnStartup` auf `4` fest. Dadurch wird die `RestoreOnStartup`-Aktion zum Öffnen einer URL-Liste festgelegt. Sie können auch andere Aktionen für Ihre Startup-URLs verwenden. Weitere Informationen finden Sie in der Liste der Chrome-Unternehmensrichtlinien.
   b. Legen Sie `RestoreOnStartupURLs` auf https://www.aboutamazon.com/news fest.

```
 "RestoreOnStartup":
    {
        "value": 4
    },
"RestoreOnStartupURLs":
    {
        "value":
        [
            "https://www.aboutamazon.com/news"
        ]
    },
```

3. Wenn Sie verhindern möchten, dass der Benutzer seinen Browserverlauf löscht, legen Sie `AllowDeletingBrowserHistory` auf `false` fest.

```
 "AllowDeletingBrowserHistory":
    {
        "value": false
    },
```

4. Wenn Sie den Zugriff auf den Inkognitomodus für Ihre Benutzer deaktivieren möchten, legen Sie `IncognitoModeAvailability` auf 1 fest.

```
 "IncognitoModeAvailability":
    {
        "value": 1
    }
```

5. Richten Sie das Okta-Plug-in mit den folgenden Richtlinien ein und setzen Sie es durch:

   - `ExtensionSettings` – installiert eine Erweiterung beim Start des Browsers. Der Erweiterungswert ist auf der Hilfeseite des Okta-Plug-ins verfügbar.
   - `ExtensionInstallBlocklist` – verhindert die Installation bestimmter Erweiterungen. Verwenden Sie einen *-Wert, um standardmäßig alle Erweiterungen zu verhindern.

Administratoren können auf der `ExtensionInstallAllowlist` steuern, welche Erweiterungen zugelassen werden sollen.

- `ExtensionInstallAllowlist` ermöglicht Ihnen die Installation bestimmter Erweiterungen. Da `ExtensionInstallBlocklist` auf `*` festgelegt ist, fügen Sie hier den Okta-Plug-in-Wert hinzu, um dies zuzulassen.

Im Folgenden finden Sie ein Beispiel für eine Richtlinie zum Aktivieren des Okta-Plug-ins:

```
"ExtensionInstallBlocklist": {
    "value": [
        "*",
        ]
},
"ExtensionInstallAllowlist": {
    "value": [
        "glnpjglilkicbckjpbgcfkogebgllemb",
       ]
},
"ExtensionSettings": {
    "value": {
        "glnpjglilkicbckjpbgcfkogebgllemb": {
            "installation_mode": "force_installed",
            "update_url": "https://clients2.google.com/service/update2/crx",
            "toolbar_pin": "force_pinned"
    }
}
```

Schritt 5: Laden Sie Ihre JSON-Datei für Richtlinien auf Ihr Webportal hoch

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Web und dann Webportale aus.
3. Wählen Sie Ihr Webportal und dann Bearbeiten aus.
4. Wählen Sie Richtlinieneinstellungen und anschließend JSON-Datei-Upload aus.
5. Wählen Sie Datei auswählen aus. Navigieren Sie zu Ihrer JSON-Datei, wählen Sie sie aus und laden Sie sie hoch.

6. Wählen Sie Speichern.

Bearbeiten Sie die grundlegende Browser-Richtlinie

Um den Service bereitzustellen, wendet WorkSpaces Web eine Baseline-Browserrichtlinie auf alle Portale an. Diese Basisrichtlinie wird zusätzlich zu den Richtlinien angewendet, die Sie in der Konsolenansicht oder beim JSON-Upload angeben. Im Folgenden finden Sie eine Liste der Richtlinien, die vom Service im JSON-Format angewendet werden:

```
{
    "chromePolicies":
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
            "value": 1
        },
        "URLBlocklist": {
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
        }
    }
}
```

Kunden können an den folgenden Richtlinien keine Änderungen vornehmen:

- `DefaultDownloadDirectory` – diese Richtlinie kann nicht bearbeitet werden. Der Service überschreibt alle Änderungen an dieser Richtlinie.
- `DownloadDirectory` – diese Richtlinie kann nicht bearbeitet werden. Der Service überschreibt alle Änderungen an dieser Richtlinie.

Kunden können die folgenden Richtlinien für ihr Webportal aktualisieren:

- `DownloadRestrictions` – die Standardeinstellung ist auf `1` festgelegt, damit Downloads verhindert werden, die von Chrome Safe Browsing als bösartig eingestuft wurden. Weitere Informationen finden Sie unter Verhindern, dass Benutzer schädliche Dateien herunterladen. Sie können einen Wert von `0` bis `4` festlegen.
- Die Richtlinien `URLAllowlist` und `URLBlocklist` können mithilfe des URL-Filter-Features der Konsolenansicht oder mithilfe des JSON-Uploads erweitert werden. Die Baseline-URLs können jedoch nicht überschrieben werden. Diese Richtlinien sind in einer JSON-Datei, die von Ihrem Webportal heruntergeladen wurde, nicht sichtbar. Wenn Sie jedoch während einer Sitzung „chrome://policy“ aufrufen, zeigt der Remote-Browser die angewendeten Richtlinien an.

Den Eingabemethoden-Editor (IME) konfigurieren

Ein Eingabemethoden-Editor (IME) ist ein Hilfsprogramm, das Endbenutzern Optionen zur Texteingabe in Sprachen bietet, bei denen ein anderes Tastaturlayout als eine QWERTY-Tastatur verwendet wird. IMEs helfen Benutzern bei der Eingabe von Text in Sprachen mit größeren und komplexeren Sprachgruppen wie Japanisch, Chinesisch und Koreanisch. WorkSpaces Websitzungen beinhalten standardmäßig IME-Unterstützung. Benutzer können alternative Sprachen über die IME-Symbolleiste in der Sitzung oder mithilfe von Tastenkombinationen auswählen.

Die folgenden Sprachen werden derzeit von WorkSpaces Webs IME unterstützt:

- Englisch
- Vereinfachtes Chinesisch (Pinyin)
- Traditionelles Chinesisch (Bopomofo)
- Japanisch
- Koreanisch

Wenn Sie eine Sprache aus der IME-Symbolleiste auswählen möchten, führen Sie die folgenden Schritte aus:

1. Wählen Sie das Drop-down-Menü zur Sprachauswahl auf der rechten Seite der schwarzen oberen Bedienfeldleiste aus. In der Standardeinstellung zeigt die Auswahltaste en für Englisch an.
2. Wählen Sie im Drop-down-Menü die gewünschte Sprache aus.
3. Wählen Sie im Untermenü, das nach der Auswahl einer Sprache angezeigt wird, zusätzliche Sprachdetails aus.

Wenn Sie eine Sprache mithilfe von Tastenkombinationen auswählen möchten, verwenden Sie Folgendes:

- Alle IMEs
  - Wenn Sie Shift+Control+Left Alt drücken, können Sie den IME vorwärts durchgehen (bzw. zum richtigen Tastaturlayout wechseln).
- Japanisch
  - Zur Auswahl von Hiragana drücken Sie F6.
  - Zur Auswahl von Katakana drücken Sie F7.
  - Zur Auswahl von Latin drücken Sie F10.
  - Zur Auswahl von Wide Latin drücken Sie F9.
  - Zur Auswahl von Direct Input drücken Sie ALT +, ALT+@, Zenkaku Hankaku.
- Koreanisch
  - Zur Auswahl von Hangul drücken Sie Shift+Space.
  - Zur Auswahl von Hanja drücken Sie F9.

Um die IME-Symbolleiste und das Menü zu entfernen oder die Bildschirmtastatur aus Ihren WorkSpaces Websitzungen zu deaktivieren, wenden Sie sich an AWS Support.

Die sitzungsinterne Lokalisierung konfigurieren

Wenn ein Benutzer eine Sitzung startet, erkennt WorkSpaces Web die lokalen Browser-Sprach- und Zeitzoneneinstellungen des Benutzers und wendet sie auf die Sitzung an. Dies wirkt sich auf die

Anzeigesprache während der Sitzung aus und trägt dazu bei, dass die angezeigte Uhrzeit mit der aktuellen Uhrzeit am Standort des Benutzers übereinstimmt.

Die folgende Liste zeigt die Sprachcodes, die derzeit von WorkSpaces Web unterstützt werden. Wenn der lokale Browser des Benutzers so eingestellt ist, dass er einen nicht unterstützten Sprachcode verwendet, wird für die Sitzung standardmäßig Englisch (en-US) verwendet.

- Deutsch
  - de – Deutsch
  - de-AT – Deutsch (Österreich)
  - de-DE – Deutsch (Deutschland)
  - de-CH – Deutsch (Schweiz)
  - de-LI – Deutsch (Liechtenstein)
- Englisch
  - en – Englisch
  - en-AU – Englisch (australisch)
  - en-CA – Englisch (Kanada)
  - en-IN – Englisch (Indien)
  - en-NZ – Englisch (Neuseeland)
  - en-ZA – Englisch (Südliches Afrika)
  - en-GB – Englisch (Großbritannien und Nordirland)
  - en-US – Englisch (USA)
- Spanisch
  - es – Spanisch
  - es-AR – Spanisch (Argentinien)
  - es-CL – Spanisch (Chile)
  - es-CO – Spanisch (Kolumbien)
  - es-CR – Spanisch (Costa Rica)
  - es-HN – Spanisch (Honduras)
  - es-419 – Spanisch (lateinamerikanisch)
  - es-MX – Spanisch (Mexiko)
  - es-PE – Spanisch (Peru)

  - es-ES – Spanisch (Spanien)
  - es-US – Spanisch (Vereinigte Staaten)
  - es-UY – Spanisch (Uruguay)
  - es-VE – Spanisch (Venezuela)
- Französisch
  - fr – Französisch
  - fr-CA – Französisch (Kanada)
  - fr-FR – Französisch (Frankreich)
  - fr-CH – Französisch (Schweiz)
- Indonesisch
  - id – Indonesisch
  - id-ID – Indonesisch (Indonesien)
- Italienisch
  - it – Italienisch
  - it-IT – Italienisch (Italien)
  - it-CH – Italienisch (Schweiz)
- Japanisch
  - ja – Japanisch
  - ja-JP – Japanisch (Japan)
- Koreanisch
  - ko – Koreanisch
  - ko-KR – Koreanisch (Korea)
- Portugiesisch
  - pt – Portugiesisch
  - pt-BR – Portugiesisch (Brasilien)
  - pt-PT – Portugiesisch (Portugal)
- Chinesisch
  - zh – Chinesisch
  - zh-CN – Chinesisch (China)
  - zh-HK – Chinesisch (Hongkong)

- zh-TW – Chinesisch (Taiwan)

Die Sitzungssprache wird in der folgenden Prioritätsreihenfolge festgelegt:

1. Die ForcedLanguages Richtlinie in den Browsereinstellungen des Webportals. Weitere Informationen finden Sie unter ForcedLanguages.
2. Die lokale Browserspracheinstellung des Endbenutzers.
3. Der Standardwert ist Englisch (en-US).

Die Zeitzone wird durch die lokalen Zeitzoneneinstellungen bestimmt, die im Browser des Endbenutzers angegeben sind. Wenn die Zeitzoneneinstellung nicht gültig ist, wird UTC verwendet.

Die folgenden Komponenten in WorkSpaces Web unterstützen die Lokalisierung:

- WorkSpaces Web-Anmeldeseite
- WorkSpaces Webportal-Statusmeldungen (einschließlich Laden von Nachrichten und Fehlern)
- Chrome-Browser
- Kontextmenü des Systems und das Fenster Speichern unter

Führen Sie einen der folgenden Schritte aus, um die lokalen Browsereinstellungen eines Benutzers festzulegen:

- Wählen Sie in Chrome Einstellungen und dann Sprachen aus. Ordnen Sie die Sprachen dann nach Ihren Wünschen.
- Wählen Sie in Firefox Einstellungen, Allgemein, Sprache und die Sprache aus dem Drop-down-Menü aus.
- Wählen Sie in Edge Einstellungen und dann Sprachen aus. Ordnen Sie die Sprachen dann nach Ihren Wünschen.

IP-Zugriffskontrollen einrichten (optional)

WorkSpaces Mit Web können Sie steuern, von welchen IP-Adressen aus auf Ihr Webportal zugegriffen werden kann. Mit IP–Zugriffseinstellungen können Sie Gruppen vertrauenswürdiger IP-Adressen definieren und verwalten und Benutzern nur dann Zugriff auf ihr Portal gewähren, wenn sie mit einem vertrauenswürdigen Netzwerk verbunden sind.

Standardmäßig ermöglicht WorkSpaces Web Benutzern den Zugriff auf ihr Webportal von überall aus. Eine IP-Zugriffskontrollgruppe fungiert als virtuelle Firewall, die filtert, mit welcher IP-Adresse ein Benutzer eine Verbindung mit dem Webportal herstellen kann. Bei Zuweisung zu Ihrem Webportal erkennen die IP-Zugriffseinstellungen die Benutzer-IP vor der Authentifizierung, um festzustellen, ob sie für eine Verbindung berechtigt sind. Nach der Verbindung überwacht WorkSpaces Web kontinuierlich die IP-Adresse eines Benutzers, um sicherzustellen, dass er über ein vertrauenswürdiges Netzwerk verbunden bleibt. Wenn sich die IP-Adresse eines Benutzers ändert, erkennt und beendet WorkSpaces Web die Sitzung.

Fügen Sie Regeln zu Ihrer IP-Zugriffskontrollgruppe hinzu und ordnen die Gruppe dann Ihrem Webportal zu, um die CIDR-Adressbereiche anzugeben. Sie können jede IP-Zugriffseinstellung mindestens einem Webportal zuordnen. Um die öffentlichen IP-Adressen und IP-Adressbereiche für Ihre vertrauenswürdigen Netzwerke anzugeben, fügen Sie den IP-Zugriffskontrollgruppen Regeln hinzu. Wenn Ihre Benutzer über ein NAT-Gateway oder VPN auf ihr Webportal zugreifen, müssen Sie Regeln erstellen, die den Datenverkehr von den öffentlichen IP-Adressen für das NAT-Gateway oder VPN zulassen.

> **Note**
>
> Kunden sind dafür verantwortlich, die potenziellen rechtlichen Probleme zu verstehen, die sich aus ihrer Nutzung von WorkSpaces Web ergeben, und müssen sicherstellen, dass ihre Nutzung von WorkSpaces Web allen geltenden Gesetzen und Vorschriften entspricht. Dazu gehören Gesetze, die die Fähigkeit eines Arbeitgebers regulieren, die Nutzung von WorkSpaces Web durch einen Mitarbeiter zu überwachen, einschließlich Aktivitäten, die innerhalb der Anwendung ausgeführt werden.

Eine IP-Zugriffskontrollgruppe erstellen

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe zu erstellen.

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im Navigationsbereich IP-Zugriffskontrollen aus.
3. Wählen Sie IP-Zugriffskontrollgruppe erstellen aus.
4. Geben Sie im Dialogfeld IP-Zugriffskontrollgruppe erstellen einen Namen (erforderlich) und eine Beschreibung (optional) für die Gruppe ein.

5. Geben Sie die IP-Adresse oder den CIDR-IP-Bereich ein, den Sie der Quelle zuordnen möchten, und eine Beschreibung (optional).
6. Wählen Sie unter Tags aus, ob ein Schlüsselwertpaar für jede IP-Zugriffskontrollgruppe markiert werden soll.
7. Wenn Sie mit dem Hinzufügen von Regeln und Tags fertig sind, klicken Sie auf Speichern.

Eine IP-Zugriffseinstellung einem Webportal zuordnen

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe einem vorhandenen Webportal zuzuordnen.

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im linken Navigationsbereich die Option Webportale aus.
3. Wählen Sie das Webportal aus und klicken Sie auf Bearbeiten.
4. Wählen Sie unter IP-Zugriffskontrollgruppe die IP-Zugriffskontrollgruppen für das Webportal aus.
5. Wählen Sie Speichern.

Gehen Sie folgendermaßen vor, um bei Erstellung eines Webportals eine IP-Zugriffskontrollgruppe zuzuordnen.

1. Führen Sie in the section called “Portaleinstellungen konfigurieren” die Schritte 1 bis 4 aus, um auf IP-Zugriffskontrolle (optional) zuzugreifen.
2. Wählen Sie IP-Zugriffskontrollen erstellen aus.
3. Geben Sie im Dialogfeld IP-Gruppe erstellen einen Namen (erforderlich) und eine Beschreibung (optional) für die Gruppe ein.
4. Geben Sie die IP-Adresse oder den CIDR-IP-Bereich ein, den Sie der Quelle zuordnen möchten, und eine Beschreibung (optional).
5. Wählen Sie unter Tags aus, ob ein Schlüsselwertpaar für jede IP-Zugriffskontrollgruppe markiert werden soll.
6. Wenn Sie mit dem Hinzufügen von Regeln und Tags fertig sind, wählen Sie IP-Zugriffskontrolle erstellen aus.
7. Ihre IP-Zugriffskontrollgruppe wird beim Start diesem Webportal zugeordnet.

Eine IP-Zugriffskontrollgruppe bearbeiten

Sie können eine Regel für eine IP-Zugriffseinstellung jederzeit löschen. Wenn Sie eine Regel entfernen, die verwendet wurde, um eine Verbindung mit einem Webportal zuzulassen, werden alle Benutzer mit einer aktuellen Sitzung vom Webportal getrennt.

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe zu bearbeiten.

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im Navigationsbereich IP-Zugriffskontrollen aus.
3. Markieren Sie die Gruppe und wählen Sie Edit (Bearbeiten) aus.
4. Bearbeiten Sie die vorhandenen Regeln Quelle und Beschreibung (optional) oder fügen Sie zusätzliche Regeln hinzu.
5. Wählen Sie unter Tags aus, ob ein Schlüsselwertpaar für jede IP-Zugriffskontrollgruppe markiert werden soll.
6. Wenn Sie mit dem Hinzufügen von Regeln und Tags fertig sind, klicken Sie auf Speichern.
7. Wenn Sie eine vorhandene IP-Zugriffseinstellung aktualisiert haben, warten Sie bis zu 15 Minuten, bis die neue oder bearbeitete Regel wirksam wird.

Einer IP-Zugriffskontrollgruppe löschen

Sie können eine Regel für eine IP-Zugriffskontrollgruppe jederzeit löschen. Wenn Sie eine Regel entfernen, die verwendet wurde, um eine Verbindung mit einem Webportal zuzulassen, werden alle Benutzer mit einer aktuellen Sitzung vom Webportal getrennt.

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe zu löschen.

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im Navigationsbereich IP-Zugriffskontrollgruppen aus.
3. Wählen Sie die Gruppe aus und wählen Sie Löschen aus.

Erweiterung für Single-Sign-On aktivieren (optional)

Sie können eine Erweiterung für Ihre Endbenutzer aktivieren, um die Portalanmeldung zu verbessern. Wenn Sie Okta beispielsweise als SAML-2.0-Identitätsanbieter (IDP) Ihres Portals und auch als Identitätsanbieter für die Websites verwenden, die Benutzer während einer Sitzung besuchen sollen, können Sie das Okta-Anmelde-Cookie mit der Erweiterung an die Sitzung übergeben. Wenn Benutzer anschließend eine Website besuchen, für die das Okta-Domain-Cookie erforderlich ist, können sie auf die Website zugreifen, ohne sich während der Sitzung anmelden zu müssen.

Die Erweiterung wird in den Browsern Chrome und Firefox unterstützt. Die Erweiterung ermöglicht die Cookie-Synchronisierung für die zulässigen Domains von der Benutzeranmeldung bis zur Sitzung. Die Erweiterung erfordert nicht, dass sich der Benutzer anmeldet. Sie aktiviert im Hintergrund die Cookie-Synchronisierung, ohne dass der Benutzer nach der Installation irgendwelche Aktionen ausführen muss. Die Erweiterung speichert keine Daten.

Benutzer können die -Erweiterung aus dem Chrome-Webspeicher zu ihrem Chrome-Browser oder aus Add-Ons für zu ihrem FireFox Browser hinzufügen FireFox.

Erweiterungen sind in Chrome in InCognito Fenstern nicht aktiviert. Firefox hat eine Einstellung, die Erweiterungen bei privatem Browsing zulässt. Weitere Informationen finden Sie unter Erweiterungen bei privatem Browsing.

Sie können die vorhandene Benutzereinstellungskonfiguration eines Portals aktualisieren oder dies bei der ersten Erstellung eines Webportals tun. Stellen Sie zunächst fest, welche Domains Sie für Ihren SAML-Identitätsanbieter und Ihre Websites benötigen. Sie können bis zu 10 Domains angeben.

Sie sind dafür verantwortlich, die entsprechende Domain für die zu synchronisierenden Cookies zu testen und zu identifizieren. Möglicherweise sind Änderungen auf der Ebene der Identitätsanbieter- oder Website-Authentifizierung erforderlich, um sicherzustellen, dass Single Sign-On erwartungsgemäß funktioniert.

Informationen dazu, welche Domains mit den gängigsten IdP verwendet werden sollen, finden Sie in der folgenden Tabelle:

IdP und Domains

IdP	Domain
Okta	okta.com

IdP	Domain
Azure-Anzeige	microsoftonline.com
AWS Identity Center	awsapps.com
Eine Anmeldung	onelogin.com
Duo	duosecurity.com

Rufen Sie als Nächstes Ihr Webportal in der Konsole auf. Lassen Sie dann die Erweiterung zu und fügen Sie hinzu, welche Domain-Cookies synchronisiert werden sollen. Gehen Sie wie folgt vor, um ein neues Portal mit der zugelassenen Erweiterung zu erstellen oder ein vorhandenes Portal zu aktualisieren.

Gehen Sie wie folgt vor, um die Erweiterung beim Erstellen eines neuen Webportals zuzulassen:

1. Folgen Sie den Anweisungen unter the section called “Schritt 1: Ein Webportal erstellen”, bis Sie zu the section called “Benutzereinstellungen konfigurieren” gelangen.
2. Wählen Sie für Schritt 1 von the section called “Benutzereinstellungen konfigurieren” unter Benutzerberechtigungen die Option Zugelassen aus, um die Erweiterung für Ihr Webportal zu aktivieren.
3. Geben Sie die Domain für die Cookie-Synchronisierung ein und wählen Sie Neue Domain hinzufügen aus.
4. Führen Sie die Schritte unter the section called “Benutzereinstellungen konfigurieren” aus und schließen Sie die verbleibenden Abschnitte unter the section called “Schritt 1: Ein Webportal erstellen” ab, um Ihr Webportal zu erstellen.

Gehen Sie folgendermaßen vor, um einem vorhandenen Webportal die Erweiterung hinzuzufügen:

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie das zu bearbeitende Webportal aus.
3. Wählen Sie Benutzereinstellungen, Benutzerberechtigungen und Zugelassen aus, um die Erweiterung für Ihr Webportal zu aktivieren.

4. Geben Sie die Domain für die Cookie-Synchronisierung ein und wählen Sie Neue Domain hinzufügen aus.
5. Speichern Sie Ihre Portaländerungen. Die Portale fordern die Benutzer auf, die Erweiterung innerhalb von 15 Minuten zu installieren.

Gehen Sie wie folgt vor, um Domains zu bearbeiten oder die Erweiterung zu entfernen:

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie das zu bearbeitende Webportal aus.
3. Wählen Sie Benutzereinstellungen, Benutzerberechtigungen und Nicht zugelassen aus, um die Erweiterung für Ihr Webportal zu entfernen.
4. Entfernen oder bearbeiten Sie einzelne Domains.
5. Nach dem Entfernen synchronisieren Sitzungen keine Cookies mehr, auch wenn der Benutzer die WorkSpaces Web-Erweiterung in seinem Browser installiert hat.

Einzelheiten zum Benutzererlebnis mit der Erweiterung finden Sie unter the section called “Erweiterung für Single Sign-On”.

URL-Filterung einrichten

Sie können Chrome Policy verwenden, um zu filtern, auf welche URLs Benutzer von ihrem Remote-Browser aus zugreifen können. Chrome Policy bietet zwei Mechanismen zum Filtern von URLs :URLAllowlist und URLBlocklist. Sie können die WorkSpaces Webkonsolenschnittstelle verwenden, um die URL-Filterung als Portaleinstellung zu konfigurieren, oder Sie können sie als Teil Ihrer benutzerdefinierten JSON-Anweisung hinzufügen (entweder im Inline-Editor oder als JSON-Datei-Upload).

So richten Sie die URL-Filterung mithilfe der Konsole ein

1. Öffnen Sie die WorkSpaces Webkonsole unter https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Web , Webportale, Ihr Webportal und dann Details anzeigen aus.
3. Wählen Sie für URL-Filterung eine der folgenden Optionen aus:

- Zugriff auf alle URLs zulassen: Standardmäßig erlaubt ein Webportal den Zugriff auf alle URLs. Sie können bestimmte Websites zur BlockURL-Liste hinzufügen, um zu verhindern, dass Benutzer diese Websites während einer Sitzung besuchen. Wenn Sie beispielsweise www.anycorp.com zur BlockURL-Liste hinzufügen, wird verhindert, dass Benutzer während ihrer Sitzung zu www.anycorp.com navigieren.
- Blockieren des Zugriffs auf alle URLs: Standardmäßig blockiert das Webportal den Zugriff auf alle URLs. Sie können der URL-Zulassungsliste bestimmte Websites hinzufügen, um eine Liste von Websites zu kuratieren, die Benutzer besuchen können, und den Datenverkehr zu anderen Websites blockieren. Erwägen Sie, jede URL als Lesezeichen hinzuzufügen, um den 1-Klick-Zugriff für Benutzer während ihrer Sitzung zu ermöglichen.
- Erweiterte Konfiguration: Wählen Sie diese Option, um allowURL- und blockURLListen parallel zu erstellen. Die URL-Zulassungsliste hat Vorrang vor der URL-Blockliste . Diese Option ermöglicht die URL-Filterung nach Pfad. Sie können beispielsweise www.anycorp.com zur Blockierliste und dann www.anycorp.com/hr zur Zulassungsliste hinzufügen. Auf diese Weise können Benutzer www.anycorp.com/hr, aufrufen, aber sie können nicht auf andere URL-Pfade zugreifen, z. B. www.anycorp.com/finance.

Weitere Hinweise zur Verwendung von Block- und Zulassungs-URLs finden Sie unter Zugriff auf Websites zulassen oder blockieren. Fügen Sie URLs zu diesen Listen hinzu, indem Sie dem Blocklistenfilterformat von Chrome folgen, um die besten Ergebnisse zu erzielen. Weitere Informationen finden Sie unter URL-Blocklistenfilterformat .

So richten Sie die URL-Filterung mit dem JSON-Editor oder dem Datei-Upload ein

1. Wählen Sie im Modul Richtlinieneinstellungen die Option JSON-Editor aus und umgehen Sie das Konsolenbenutzeroberflächenmodul für die Ansicht Editor oder Datei-Upload.

   - Der Editor ermöglicht es Kunden, benutzerdefinierte Richtlinienanweisungen in der Konsole eingebunden zu erstellen. Der Editor hebt Fehler in der JSON-Anweisung während der Richtlinienerstellung hervor.
   - Mit dem Datei-Upload können Kunden eine JSON-Datei hinzufügen, die außerhalb der Konsole erstellt wurde (z. B. aus einem vorhandenen Chrome-Browser exportiert).
2. Weitere Informationen finden Sie unter Chrome-Richtliniendetails für URLAllowlist und URLBlocklist, um eine Zulassungs-/denyURL-Liste für Ihr Webportal ordnungsgemäß zu formatieren. Weitere Informationen finden Sie unter URLAllowlist und URLBlocklist.

Sicherheit in Amazon WorkSpaces Web

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für Amazon WorkSpaces Web gelten, finden Sie unter Im Rahmen des Compliance-Programms zugelassene AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und alle geltenden Gesetze und Vorschriften, die für Ihre Daten gelten.

Diese Dokumentation zeigt Ihnen, wie Sie das Modell der übergreifenden Verantwortlichkeit bei der Verwendung von Amazon WorkSpaces Web einsetzen können. Es zeigt Ihnen, wie Sie Amazon WorkSpaces Web konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS-Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer Amazon-WorkSpaces-Web-Ressourcen unterstützen.

Inhalt

- Datenschutz in Amazon WorkSpaces Web
- Identity and Access Management für Amazon WorkSpaces Web
- Vorfallreaktion in Amazon WorkSpaces Web
- Compliance-Validierung für Amazon WorkSpaces Web
- Ausfallsicherheit in Amazon WorkSpaces Web
- Sicherheit der Infrastruktur in Amazon WorkSpaces Web
- Konfigurations- und Schwachstellenanalyse in Amazon WorkSpaces Web

- Bewährte Methoden für die Sicherheit in Amazon WorkSpaces Web

Datenschutz in Amazon WorkSpaces Web

Das Modell der AWS geteilten gilt für den Datenschutz in Amazon WorkSpaces Web. https://aws.amazon.com/compliance/shared-responsibility-model/ Wie in diesem Modell beschrieben, ist AWS für den Schutz der globalen Infrastruktur verantwortlich, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit WorkSpaces Web oder anderen AWS-Services über die Konsole, APIAWS CLI, oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden,

können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

Amazon WorkSpaces Web sammelt Portalanpassungsdaten wie Browsereinstellungen, Benutzereinstellungen, Netzwerkeinstellungen, Identitätsanbieterinformationen, Vertrauensspeicherdaten und Vertrauensspeicherzertifikatdaten. WorkSpaces Web sammelt auch Browserrichtliniendaten, Benutzereinstellungen (für Browsereinstellungen) und Sitzungsprotokolle. Gesammelte Daten werden in Amazon DynamoDB gespeichert und Amazon S3. WorkSpaces Web verwendet AWS Key Management Service für die Verschlüsselung.

Befolgen Sie die folgenden Richtlinien, um deine Inhalte zu schützen:

- Implementieren Sie den Zugriff mit den geringsten Berechtigungen und erstellen Sie bestimmte Rollen, die für WorkSpaces Web-Aktionen verwendet werden sollen. Verwenden Sie IAM-Vorlagen, um eine Rolle mit Vollzugriff oder Schreibschutz zu erstellen. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien für WorkSpaces Web.
- Schützen Sie Daten durchgängig, indem Sie einen vom Kunden verwalteten Schlüssel bereitstellen, sodass WorkSpaces Web Ihre Daten im Ruhezustand mit den von Ihnen bereitgestellten Schlüsseln verschlüsseln kann.
- Seien Sie vorsichtig, wenn Sie Portal-Domains und Benutzeranmeldedaten teilen:
  - Administratoren müssen sich bei der Amazon- WorkSpaces Konsole anmelden und Benutzer müssen sich beim WorkSpaces Webportal anmelden.
  - Jeder Benutzer im Internet kann auf das Webportal zugreifen, aber er kann keine Sitzung starten, wenn er nicht über die gültigen Benutzeranmeldedaten für das Portal verfügt.
- Benutzer können ihre Sitzungen explizit beenden, indem sie Sitzung beenden auswählen. Dadurch wird die Instance, die die Browsersitzung hostet, verworfen und der Browser wird isoliert.

WorkSpaces Web sichert Inhalte und Metadaten standardmäßig, indem es alle sensiblen Daten mit verschlüsseltAWS KMS. Es erfasst Browserrichtlinien und Benutzereinstellungen, um Richtlinien und Einstellungen während WorkSpaces Websitzungen durchzusetzen. Wenn beim Anwenden vorhandener Einstellungen ein Fehler auftritt, kann ein Benutzer weder auf neue Sitzungen noch auch auf die internen Websites und SaaS-Anwendungen des Unternehmens zugreifen.

Verschlüsselung im Ruhezustand

Verschlüsselung im Ruhezustand ist standardmäßig konfiguriert. Kundenspezifische Daten, die in WorkSpaces Web verwendet werden, werden mit verschlüsseltAWS KMS. WorkSpaces Web bietet Verschlüsselung im Ruhezustand für Ressourcen, die Sie erstellen. Der Service akzeptiert bei der Erstellung einer Ressource einen vom Kunden verwalteten AWS KMS-Schlüssel. Sollte keiner bereitgestellt werden, wird ein eigener AWS-Schlüssel für die Verschlüsselung der ruhenden Ressourcen verwendet. Der Service verschlüsselt das Dokument mit den Browser-Richtlinien, das Sie zur Anpassung Ihrer Browsersitzungen bereitstellen können, sowie die Konfiguration Ihres Identitätsanbieters und die Anzeigenamen für Ihre Portale. Diese Informationen bleiben entweder mit dem vom Kunden verwalteten Schlüssel oder dem eigenen AWS-Schlüssel verschlüsselt, solange sie in unserem Backend gespeichert werden.

Sie können entscheiden, welcher Schlüssel verwendet wird, wenn Sie eine WorkSpaces Web-Ressource erstellen. Wenn Daten verschlüsselt sind, die Teil dieser Ressource sind, akzeptiert WorkSpaces Web das `customerManagedKeyArn` Feld als Teil der `create` API. Der angegebene Schlüssel muss ein symmetrischer AWS KMS-Schlüssel sein, und der Administrator, der die Ressource mit diesem Schlüssel erstellt, muss über die Berechtigungen `kms:Decrypt`, `kms:GenerateDataKey` und `kms:CreateGrant` verfügen. Nachdem eine Ressource mit dem Schlüssel erstellt wurde, kann der Schlüssel nicht mehr entfernt oder geändert werden. Wenn Sie einen vom Kunden verwalteten Schlüssel verwendet haben, muss der Administrator, der auf die Ressource zugreift, über die erforderlichen `kms:Decrypt`- und `kms:GenerateDataKey`-Berechtigungen verfügen. Wenn Sie bei der Verwendung der Konsole die Fehlermeldung erhalten, dass der Zugriff verweigert wurde, stellen Sie sicher, dass der Benutzer, der die Konsole verwendet, über diese Berechtigungen für den verwendeten Schlüssel verfügt.

Sie können Fehler bei der Schlüsselnutzung beheben und sie überprüfen, indem Sie den Status der AWS KMS-Gewährungen überprüfen. Weitere Informationen finden Sie unter Verwalten von Erteilungen. Während der Portalerstellung erstellt WorkSpaces Web eine Erteilung, damit der Service asynchron auf den Schlüssel zugreifen kann. Sie können den Status unserer Schlüsselnutzung überprüfen, indem Sie die Gewährung sowie den Verschlüsselungskontext überprüfen, der bei der Verwendung der Gewährung angegeben wurde. Der Verschlüsselungskontext enthält immer einen Eintrag mit dem Schlüssel `aws:workspaces-web:portal:id` und einem Wert, der Ihrer Portal-ID entspricht. Bei anderen Ressourcen enthält der Verschlüsselungskontext immer einen Eintrag im Format `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` und die entsprechende Ressourcen-ID.

Verschlüsselung während der Übertragung

WorkSpaces Web verschlüsselt Daten während der Übertragung über HTTPS und TLS 1.2. Sie können eine Anfrage an über die Konsole oder WorkSpaces über direkte API-Aufrufe senden. Die übertragenen Anforderungsdaten werden verschlüsselt, indem alles über eine HTTPS- oder TLS-Verbindung gesendet wird. Anforderungsdaten können von der AWSKonsole, AWS Command Line Interfaceoder dem AWS SDK in WorkSpaces Web übertragen werden.

Sowohl die Verschlüsselung während der Übertragung als auch sichere Verbindungen (HTTPS, TLS) sind standardmäßig konfiguriert.

Schlüsselverwaltung

Sie können Ihren eigenen vom Kunden verwalteten AWS KMS-Schlüssel angeben, um Ihre Kundeninformationen zu verschlüsseln. Wenn Sie keinen angeben, verwendet WorkSpaces Web einen AWS eigenen Schlüssel. Sie können Ihren Schlüssel mithilfe des AWS-SDK festlegen.

Datenschutz für den Datenverkehr zwischen Netzwerken

Um Verbindungen zwischen WorkSpaces Web- und On-Premises-Anwendungen zu sichern, verwenden Sie WorkSpaces Web, um Browsersitzungen innerhalb Ihrer eigenen VPC zu starten. Die Verbindung zu On-Premises-Anwendungen ist in Ihrer eigenen VPC konfiguriert und wird nicht von WorkSpaces Web gesteuert.

Um Verbindungen zwischen Konten zu sichern, verwendet WorkSpaces Web eine serviceverknüpfte Rolle, um eine sichere Verbindung zu Kundenkonten herzustellen und Operationen im Namen des Kunden auszuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für WorkSpaces Web.

Benutzerzugriffsprotokollierung

Administratoren können WorkSpaces Websitzungsereignisse aufzeichnen, einschließlich Start-, Stopp- und URL-Aufrufen. Diese Protokolle werden verschlüsselt und sicher über einen Amazon-Kinesis-Datenstrom an Kunden übermittelt. Browserinformationen aus der Benutzerzugriffsprotokollierung werden von AWS nicht gespeichert und sind auch nicht in Sitzungen verfügbar, wenn keine Protokollierung konfiguriert wurde. URL-Besuche im Inkognitomodus oder gelöschte URLs aus dem Browserverlauf werden in der Benutzerzugriffsprotokollierung nicht aufgezeichnet.

Identity and Access Management für Amazon WorkSpaces Web

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer für die Nutzung von WorkSpaces Webressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Funktionsweise von Amazon WorkSpaces Web mit IAM
- Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Web
- Von AWS verwaltete Richtlinien für WorkSpaces Web
- Fehlerbehebung für Amazon WorkSpaces -Web-Identität und -Zugriff
- Verwenden von serviceverknüpften Rollen für WorkSpaces Web

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in WorkSpaces Web.

Service-Benutzer – Wenn Sie den WorkSpaces Web-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere WorkSpaces Web-Features ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in WorkSpaces Web nicht zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung für Amazon WorkSpaces -Web-Identität und -Zugriff.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für WorkSpaces Web-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf WorkSpaces Web. Ihre

Aufgabe besteht darin, zu bestimmen, auf welche WorkSpaces Web-Features und -Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit WorkSpaces Web verwenden kann, finden Sie unter Funktionsweise von Amazon WorkSpaces Web mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf WorkSpaces Web verfassen können. Beispiele für identitätsbasierte WorkSpaces Web-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Web.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuertem Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anfragen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere

Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center-Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir,

temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff: Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff: Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle: Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2: Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt

werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen:Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien:Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Funktionsweise von Amazon WorkSpaces Web mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf WorkSpaces Web zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit WorkSpaces Web verwenden können.

IAM-Funktionen, die Sie mit Amazon WorkSpaces Web verwenden können

IAM-Feature	WorkSpaces Web-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen Überblick über das Zusammenwirken von WorkSpaces Web und anderen -AWSServices mit den meisten IAM-Funktionen finden Sie unter -AWSServices, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für WorkSpaces Web

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für WorkSpaces Web

Beispiele für identitätsbasierte WorkSpaces Web-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Web.

Ressourcenbasierte Richtlinien in WorkSpaces Web

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource

erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für WorkSpaces Web

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der WorkSpaces Web-Aktionen finden Sie unter Von Amazon WorkSpaces Web definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in WorkSpaces Web verwenden das folgende Präfix vor der Aktion:

```
workspaces-web
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "workspaces-web:action1",
      "workspaces-web:action2"
         ]
```

Beispiele für identitätsbasierte WorkSpaces Web-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Web.

Richtlinienressourcen für WorkSpaces Web

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der WorkSpaces Web-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon WorkSpaces Web definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Amazon WorkSpaces Web definierte Aktionen.

Beispiele für identitätsbasierte WorkSpaces Web-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Web.

Richtlinienbedingungsschlüssel für WorkSpaces Web

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der WorkSpaces Web-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon WorkSpaces Web in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon WorkSpaces Web definierte Aktionen.

Beispiele für identitätsbasierte WorkSpaces Web-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Web.

Zugriffssteuerungslisten (ACLs) in WorkSpaces Web

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit WorkSpaces Web

Unterstützt ABAC (Tags in Richtlinien)	Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit WorkSpaces Web

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, unter anderem darüber, welche AWS-Services mit temporären Anmeldeinformationen arbeiten, finden Sie unter AWS-Services, die mit IAM arbeiten im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn

Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für WorkSpaces Web

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für WorkSpaces Web

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die Funktionalität von WorkSpaces Web beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn WorkSpaces Web dazu Anleitungen gibt.

Serviceverknüpfte Rollen für WorkSpaces Web

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon WorkSpaces Web

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von WorkSpaces Webressourcen. Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die AWS-API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von WorkSpaces Web definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Web in der Service-Autorisierungs-Referenz.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der WorkSpaces Webkonsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand WorkSpaces Web-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen:Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS-Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten:Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs:Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten:IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA):Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der WorkSpaces Webkonsole

Um auf die Amazon WorkSpaces Web-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den WorkSpaces Web-Ressourcen in Ihrem aufzulisten und anzuzeigenAWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen weiterhin die WorkSpaces Webkonsole verwenden können, fügen Sie den Entitäten auch die `ReadOnly` AWS von verwaltete Richtlinie WorkSpaces Web `ConsoleAccess` oder hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer

Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Von AWS verwaltete Richtlinien für WorkSpaces Web

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, von AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere von AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken häufige Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu verwalteten AWS-Richtlinien finden Sie unter Verwaltete AWS-Richtlinien im IAM-Leitfaden.

AWS-Services pflegen und Aktualisieren von verwalteten AWS-Richtlinien. Die Berechtigungen in von AWS verwalteten Richtlinien können nicht geändert werden. Services fügen einer von AWS verwalteten Richtlinien möglicherweise gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Services entfernen keine Berechtigungen aus einer von AWS verwalteten Richtlinie, so dass Richtlinien-Aktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

Darüber hinaus unterstützt AWS verwaltete Richtlinien für Auftragsfunktionen, die mehrere Services umfassen. Die von `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS-Services und -Ressourcen. Wenn ein Service ein neues Feature startet, fügt AWS schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS-Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Von AWS verwaltete Richtlinie: AmazonWorkSpacesWebServiceRolePolicy

Sie können die `AmazonWorkSpacesWebServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die WorkSpaces Web die Durchführung von Aktionen in Ihrem Namen ermöglicht. Weitere Informationen finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

Diese Richtlinie gewährt Administratorberechtigungen, die Zugriff auf Services und Ressourcen von AWS ermöglichen, die von Amazon WorkSpaces Web verwendet oder verwaltet werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `WorkSpaces Web` – ermöglicht den Zugriff auf Services und Ressourcen von AWS, die von Amazon WorkSpaces Web verwendet oder verwaltet werden.
- `ec2` – ermöglicht es Prinzipalen, VPCs, Subnetze und Availability Zones zu beschreiben, Netzwerkschnittstellen zu erstellen, zu kennzeichnen, zu beschreiben und zu löschen, eine Adresse zuzuordnen oder zu trennen und Routing-Tabellen, Sicherheitsgruppen und VPC-Endpunkte zu beschreiben.
- `CloudWatch` – ermöglicht es Prinzipalen, Metrikdaten einzugeben.
- `Kinesis` – ermöglicht es Prinzipalen, eine Zusammenfassung der Kinesis-Datenströme zu beschreiben und Datensätze zur Protokollierung von Benutzerzugriffen in Kinesis-Datenströmen abzulegen. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
```

```
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

Von AWS verwaltete Richtlinie: AmazonWorkSpacesWebReadOnly

Sie können die `AmazonWorkSpacesWebReadOnly`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt über die AWS-Managementkonsole, das SDK und die CLI schreibgeschützte Berechtigungen, die den Zugriff auf WorkSpaces Web und seine Abhängigkeiten ermöglichen. Diese Richtlinie beinhaltet keine Berechtigungen, die für die Interaktion mit Portalen erforderlich sind, bei denen `IAM_Identity_Center` als Authentifizierungstyp verwendet wird. Wenn Sie diese Berechtigungen erhalten möchten, kombinieren Sie diese Richtlinie mit `AWSSSOReadOnly`.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `WorkSpaces Web` – bietet über die AWS-Managementkonsole, das SDK und die CLI schreibgeschützten Zugriff auf Amazon WorkSpaces Web und seine Abhängigkeiten.
- `ec2` – ermöglicht es Prinzipalen, VPCs, Subnetze und Sicherheitsgruppen zu beschreiben. Dies wird in der AWS-Managementkonsole in WorkSpaces Web verwendet, um Ihnen Ihre VPCs, Subnetze und Sicherheitsgruppen anzuzeigen, die für die Verwendung mit dem Service verfügbar sind.
- `Kinesis` – ermöglicht Prinzipalen das Aufführen von Amazon-Kinesis-Datenströmen. Dies wird in der AWS-Managementkonsole in WorkSpaces Web verwendet, um Ihnen Kinesis-Datenströmen anzuzeigen, die für die Verwendung mit dem Service verfügbar sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
```

```
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

Updates von WorkSpaces Web für von AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für von AWS verwaltete Richtlinien für WorkSpaces Web, seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

Änderung	Beschreibung	Datum
AmazonWorkSpacesWebServiceRolePolicy – aktualisierte Richtlinie	WorkSpaces Web hat die Richtlinie aktualisiert, um CreateNetworkInterface auf Tags mit aws:RequestTag/WorkspacesWebManaged: true zu beschränken und auf Subnetz- sowie Sicherheitsgruppenressourcen zu reagieren. Außerdem wurde DeleteNetworkInterface auf ENIs beschränken, die mit aws:ResourceTag/Wo	15. Dezember 2022

Änderung	Beschreibung	Datum
	rkspacesWebManaged: true gekennzeichnet sind.	
AmazonWorkSpacesWebReadOnly – aktualisierte Richtlinie	WorkSpaces Web hat die Richtlinie aktualisiert, damit sie jetzt Leseberechtigungen für die Benutzerzugriffsprotokollierung enthält und Kinesis-Datenströme aufführt. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.	2. November 2022
AmazonWorkSpacesWebServiceRolePolicy – aktualisierte Richtlinie	WorkSpaces Web hat die Richtlinie aktualisiert, damit sie eine Zusammenfassung der Kinesis-Datenströme beschreibt und Datensätze zur Protokollierung von Benutzerzugriffen in Kinesis-Datenströmen ablegt. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.	17. Oktober 2022
AmazonWorkSpacesWebServiceRolePolicy – aktualisierte Richtlinie	WorkSpaces Web hat die Richtlinie aktualisiert, damit sie bei der ENI-Erstellung Tags aktualisiert.	6. September 2022

Änderung	Beschreibung	Datum
AmazonWorkSpacesWebServiceRolePolicy – aktualisierte Richtlinie	WorkSpaces Web hat die Richtlinie aktualisiert, um den PutMetricData-API-Berechtigungen den AWS/Usage-Namespace hinzuzufügen.	6. April 2022
AmazonWorkSpacesWebReadOnly – neue Richtlinie	WorkSpaces Web hat eine neue Richtlinie hinzugefügt, um über die AWS-Managementkonsole, das SDK und die CLI schreibgeschützten Zugriff auf Amazon WorkSpaces Web und seine Abhängigkeiten zu bieten.	30. November 2021
AmazonWorkSpacesWebServiceRolePolicy – neue Richtlinie	WorkSpaces Web hat eine neue Richtlinie hinzugefügt, die den Zugriff auf AWS-Services und -Ressourcen ermöglicht, die von Amazon WorkSpaces Web verwendet oder verwaltet werden.	30. November 2021
WorkSpaces Web hat mit der Änderungsverfolgung begonnen	WorkSpaces Web hat mit der Verfolgung von Änderungen für seine AWS-verwalteten Richtlinien begonnen.	30. November 2021

Fehlerbehebung für Amazon WorkSpaces -Web-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit WorkSpaces Web und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in WorkSpaces Web auszuführen

- Ich bin nicht autorisiert, iam durchzuführen:PassRole
- Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine WorkSpaces Webressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in WorkSpaces Web auszuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `workspaces-web:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `workspaces-web:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Ausführen der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an WorkSpaces Web übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in WorkSpaces Web auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine WorkSpaces Webressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob WorkSpaces Web diese Funktionen unterstützt, finden Sie unter Funktionsweise von Amazon WorkSpaces Web mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für WorkSpaces Web

WorkSpaces Web verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit WorkSpaces Web verknüpft ist. Serviceverknüpfte Rollen werden von WorkSpaces Web vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von WorkSpaces Web, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. WorkSpaces Web definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur WorkSpaces Web die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinien. Die Berechtigungsrichtlinie kann mit keiner anderen IAM-Entität verknüpft werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dies schützt Ihre WorkSpaces-Web-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die servicegebundene Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Servicegebundene Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für WorkSpaces Web

WorkSpaces Web verwendet die serviceverknüpfte Rolle `AWSServiceRoleForAmazonWorkSpacesWeb` – WorkSpaces Web verwendet diese serviceverknüpfte Rolle, um für Streaming-Instances und CloudWatch-Metriken auf die Amazon-EC2-Ressourcen von Kundenkonten zuzugreifen.

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonWorkSpacesWeb` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `workspaces-web.amazonaws.com`

Die Rollenberechtigungsrichtlinie `AmazonWorkSpacesWebServiceRolePolicy` erlaubt WorkSpaces Web die Durchführung der folgenden Aktionen für die

angegebenen Ressourcen. Weitere Informationen finden Sie unter the section called "AmazonWorkSpacesWebServiceRolePolicy".

- Aktion: `ec2:DescribeVpcs` für `all AWS resources`
- Aktion: `ec2:DescribeSubnets` für `all AWS resources`
- Aktion: `ec2:DescribeAvailabilityZones` für `all AWS resources`
- Aktion: `ec2:CreateNetworkInterface` mit `aws:RequestTag/WorkSpacesWebManaged: true` in Subnetz- und Sicherheitsgruppenressourcen
- Aktion: `ec2:DescribeNetworkInterfaces` für `all AWS resources`
- Aktion: `ec2:DeleteNetworkInterface` in Netzwerkschnittstellen mit `aws:ResourceTag/WorkSpacesWebManaged: true`
- Aktion: `ec2:DescribeSubnets` für `all AWS resources`
- Aktion: `ec2:AssociateAddress` für `all AWS resources`
- Aktion: `ec2:DisassociateAddress` für `all AWS resources`
- Aktion: `ec2:DescribeRouteTables` für `all AWS resources`
- Aktion: `ec2:DescribeSecurityGroups` für `all AWS resources`
- Aktion: `ec2:DescribeVpcEndpoints` für `all AWS resources`
- Aktion: `ec2:CreateTags` in `ec2:CreateNetworkInterface`-Betrieb mit `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Aktion: `cloudwatch:PutMetricData` für `all AWS resources`
- Aktion: `kinesis:PutRecord` in Kinesis-Datenströmen mit Namen, die mit `amazon-workspaces-web-` beginnen
- Aktion: `kinesis:PutRecords` in Kinesis-Datenströmen mit Namen, die mit `amazon-workspaces-web-` beginnen
- Aktion: `kinesis:DescribeStreamSummary` in Kinesis-Datenströmen mit Namen, die mit `amazon-workspaces-web-` beginnen

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für WorkSpaces Web

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Ihr erstes Portal in der AWS Management Console, der AWS CLI oder der AWS-API erstellen, erstellt Amazon WorkSpaces Web die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Funktionen verwendet.

Wenn Sie diese serviceverknüpfte Rolle löschen und später erneut erstellen müssen, können Sie die Rolle in Ihrem Konto auf dieselbe Weise neu erstellen. Wenn Sie Ihr ersten Portal erstellen, erstellt Amazon WorkSpaces Web die serviceverknüpfte Rolle erneut für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall WorkSpaces Web zu erstellen. Erstellen Sie in der AWS CLI oder der AWS-API eine servicegebundene Rolle mit dem Servicenamen `workspaces-web.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer servicegebundenen Rolle im IAM-Leitfaden. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für WorkSpaces Web

WorkSpaces Web lässt die Bearbeitung der serviceverknüpften Rolle namens `AWSServiceRoleForAmazonWorkSpacesWeb` nicht zu. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für WorkSpaces Web

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der WorkSpaces-Web-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie WorkSpaces-Web-Ressourcen, die von der Rolle AWSServiceRoleForAmazonWorkSpacesWeb verwendet werden

- Wählen Sie eine der folgenden Optionen aus:
  - Wenn Sie die Konsole verwenden, löschen Sie alle Ihre Portale auf der Konsole.
  - Wenn Sie die CLI oder API verwenden, trennen Sie alle Ihre Ressourcen (einschließlich Browsereinstellungen, Netzwerkeinstellungen, Benutzereinstellungen, Trust Stores und Einstellungen für die Benutzerzugriffsprotokollierung) aus Ihren Portalen. Löschen Sie diese Ressourcen und löschen Sie dann die Portale.

So löschen Sie die servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS-API, um die serviceverknüpfte Rolle AWSServiceRoleForAmazonWorkSpacesWeb zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte WorkSpaces-Web-Rollen

WorkSpaces Web unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWSRegionen und Endpunkte.

Vorfallreaktion in Amazon WorkSpaces Web

Sie können Vorfälle erkennen, indem Sie die `SessionFailure` Amazon-CloudWatch-Metrik überwachen. Wenn Sie Warnmeldungen für Vorfälle erhalten möchten, verwenden Sie einen CloudWatch-Alarm für die `SessionFailure`-Metrik. Weitere Informationen finden Sie unter Überwachen von Amazon WorkSpaces Web mit Amazon CloudWatch.

Compliance-Validierung für Amazon WorkSpaces Web

Informationen darüber, ob ein AWS-Service in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services in Geltungsbereich nach Compliance-Programm. Wählen Sie das Compliance-Programm, das Sie interessiert. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Kurzanleitungen für Sicherheit und Compliance: In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

  > **Note**
  >
  > Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS-Compliance-Leitfäden für Kunden: Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von AWS-Services zusammengefasst und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.

- AWS Security Hub: Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager: Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Ausfallsicherheit in Amazon WorkSpaces Web

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter AWSGlobale Infrastruktur.

Folgendes wird derzeit von WorkSpaces Web nicht unterstützt:

- Inhalte zwischen Availability Zones oder Regionen sichern
- Verschlüsselte Sicherungen
- Verschlüsseln von Inhalten, die während der Übertragung zwischen Availability Zones oder Regionen übertragen werden
- Standard-Sicherungen oder automatische Sicherungen

Wenn Sie eine hohe Internetverfügbarkeit konfigurieren möchten, können Sie Ihre VPC-Konfiguration optimieren. Für eine hohe API-Verfügbarkeit können Sie die richtige Menge an TPS anfordern.

Sicherheit der Infrastruktur in Amazon WorkSpaces Web

Als verwalteter Service ist Amazon WorkSpaces Web durch die globale Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon WorkSpaces Web zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

WorkSpaces Web isoliert den Service-Datenverkehr, indem die AWS-Standard-SigV4-Authentifizierung und -Autorisierung auf alle Services angewendet werden. Der Endpunkt der Kundenressource (oder der Endpunkt des Webportals) wird durch Ihren Identitätsanbieter geschützt. Sie können den Datenverkehr weiter isolieren, indem Sie die Multi-Faktor-Autorisierung und andere Sicherheitsmechanismen in Ihrem Identitätsanbieter (IDP) verwenden.

Der gesamte Internetzugriff kann durch die Konfiguration von Netzwerkeinstellungen wie VPC, Subnetz oder Sicherheitsgruppe gesteuert werden. Mehrmandantenfähigkeit und VPC-Endpunkte (PrivateLink) werden derzeit nicht unterstützt.

Konfigurations- und Schwachstellenanalyse in Amazon WorkSpaces Web

WorkSpaces Web aktualisiert und patcht Anwendungen und Plattformen nach Bedarf in Ihrem Namen, einschließlich Chrome und Linux. Sie müssen keine Patches oder Neuerstellungen

durchführen. Es liegt jedoch in Ihrer Verantwortung, WorkSpaces Web gemäß den Spezifikationen und Richtlinien zu konfigurieren und die Nutzung von WorkSpaces Web durch Ihre Benutzer zu überwachen. Alle servicerelevanten Konfigurationen und Schwachstellenanalysen liegen in der Verantwortung von WorkSpaces Web.

Sie können eine Erhöhung des Limits der Ressourcen von WorkSpaces Web beantragen, z. B. für die Anzahl der Webportale und die Anzahl der Benutzer. WorkSpaces Web stellt die Verfügbarkeit des Service und des SLA sicher.

Bewährte Methoden für die Sicherheit in Amazon WorkSpaces Web

Amazon WorkSpaces Web enthält eine Reihe von Sicherheits-Features, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien verwenden können. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Folgendes sind bewährte Methoden für Amazon WorkSpaces Web:

- Wenn Sie potenzielle Sicherheitsereignisse im Zusammenhang mit Ihrer WorkSpaces-Web-Nutzung erkennen möchten, verwenden Sie AWS CloudTrail Amazon CloudWatch, um den Zugriffsverlauf und die Prozessprotokolle zu erkennen und zu verfolgen. Weitere Informationen finden Sie unter Überwachen von Amazon WorkSpaces Web mit Amazon CloudWatch und Protokollieren von Amazon WorkSpaces Web-API-Aufrufen mit AWS CloudTrail.
- Verwenden Sie CloudTrail-Protokolle und CloudWatch-Metriken, um erkennende Steuerelemente zu implementieren und Anomalien zu identifizieren. Weitere Informationen finden Sie unter Überwachen von Amazon WorkSpaces Web mit Amazon CloudWatch und Protokollieren von Amazon WorkSpaces Web-API-Aufrufen mit AWS CloudTrail.
- Sie können die Benutzerzugriffsprotokollierung einrichten, um Benutzerereignisse aufzuzeichnen. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.

Wenn Sie potenzielle Sicherheitsereignisse im Zusammenhang mit Ihrer Nutzung von WorkSpaces verhindern möchten, befolgen Sie diese bewährten Methoden:

- Implementieren Sie den Zugriff mit geringster Berechtigung und erstellen Sie spezifische Rollen, die für WorkSpaces-Webaktionen verwendet werden. Verwenden Sie IAM-Vorlagen, um eine Rolle

mit Vollzugriff oder Schreibschutz zu erstellen. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien für WorkSpaces Web.

- Seien Sie vorsichtig, wenn Sie Portal-Domains und Benutzeranmeldedaten teilen. Jeder Benutzer im Internet kann auf das Webportal zugreifen, aber er kann keine Sitzung starten, wenn er nicht über die gültigen Benutzeranmeldeinformationen für das Portal verfügt. Seien Sie vorsichtig dabei, wie, wann und an wen Sie die Anmeldeinformationen für das Webportal weitergeben.

Überwachen von Amazon WorkSpaces Web

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon WorkSpaces Web und Ihren anderen - AWS Lösungen aufrechtzuerhalten. AWS bietet die folgenden Überwachungstools, um Ihre WorkSpaces Webportale und ihre Ressourcen zu überwachen, Missstände zu melden und ggf. automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie ausgeführt werden, AWS in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen bestimmten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Metriken für Ihre Amazon EC2-Instances CloudWatch verfolgen lassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im Amazon- CloudWatch Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von Amazon EC2-Instances und anderen Quellen aus überwachen CloudTrail, speichern und darauf zugreifen. - CloudWatch Protokolle können Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon- CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und stellt die Protokolldateien in einem von Ihnen angegebenen Amazon S3-Bucket bereit. Sie können feststellen, welche Benutzer und Konten aufgerufen haben AWS, von welcher Quell-IP-Adresse die Aufrufe stammen und wann die Aufrufe erfolgt sind. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

- Überwachen von Amazon WorkSpaces Web mit Amazon CloudWatch
- Protokollieren von Amazon WorkSpaces Web-API-Aufrufen mit AWS CloudTrail
- Benutzerzugriffsprotokollierung

Überwachen von Amazon WorkSpaces Web mit Amazon CloudWatch

Sie können Amazon WorkSpaces Web mit überwachen CloudWatch, das Rohdaten sammelt und sie in lesbare Metriken verarbeitet, die nahezu in Echtzeit vorliegen. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im Amazon- CloudWatch Benutzerhandbuch.

Der `AWS/WorkSpacesWeb`-Namespace enthält die folgenden Metriken.

CloudWatch -Metriken für Amazon WorkSpaces Web

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
`SessionAttempt`	Die Anzahl der Amazon-WorkSpaces Web-Sitzungsversuche.	`PortalId`	Durchschnitt, Summe, Maximum, Minimum	Anzahl
`SessionSuccess`	Die Anzahl der erfolgreichen Amazon WorkSpaces -Web-Sitzungen wird gestartet.	`PortalId`	Durchschnitt, Summe, Maximum, Minimum	Anzahl
`SessionFailure`	Die Anzahl der fehlgeschlagenen Amazon WorkSpaces -Web-Sitzungen wird gestartet.	`PortalId`	Durchschnitt, Summe, Maximum, Minimum	Anzahl

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
`GlobalCpuPercent`	Die CPU-Auslastung der Amazon WorkSpaces Web-Sitzungs-Instance.	`PortalId`	Durchschnitt, Summe, Maximum, Minimum	Prozent
`GlobalMemoryPercent`	Die Speichernutzung (RAM) der Amazon WorkSpaces Web-Sitzungs-Instance.	`PortalId`	Durchschnitt, Summe, Maximum, Minimum	Prozent

> **Note**
>
> Sie können die Metrikstatistik „SampleCount“ für `GlobalCpuPercent` oder anzeigen`GlobalMemoryPercent`, um die Anzahl der gleichzeitigen Sitzungen zu bestimmen, die in Ihrem Portal aktiv sind. Die Datenpunkte werden von jeder Sitzung einmal pro Minute ausgegeben.

Protokollieren von Amazon WorkSpaces Web-API-Aufrufen mit AWS CloudTrail

Amazon WorkSpaces Web ist in AWS CloudTrail integriert. Dieser Service zeichnet die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in Amazon WorkSpaces Web auf. CloudTrail erfasst alle API-Aufrufe für Amazon WorkSpaces Web als Ereignisse. Dazu gehören Aufrufe von der Amazon-WorkSpaces-Web-Konsole und Code-Aufrufe von Amazon-WorkSpaces-Web-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon-S3-Bucket, einschließlich Ereignissen für Amazon WorkSpaces Web, aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an Amazon WorkSpaces Web gestellte

Anforderung, die IP-Adresse, von der die Anforderung gestellt wurde, den Initiator der Anforderung, den Zeitpunkt der Anforderung und weitere Angaben identifizieren.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Amazon-WorkSpaces-Web-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Wenn in Amazon WorkSpaces Web eine Aktivität auftritt, wird sie in einem CloudTrail-Ereignis zusammen mit anderen AWS-Service-Ereignissen im Ereignisverlauf aufgezeichnet. Im Ereignisverlauf können Sie die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, darunter Ereignisse für Amazon WorkSpaces Web, können Sie einen Pfad (Trail) erstellen. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien von mehreren Konten.

Alle Aktionen von Amazon WorkSpaces Web werden von CloudTrail protokolliert und sind in der API-Referenz von Amazon WorkSpaces dokumentiert. Zum Beispiel generieren Aufrufe der Aktionen `CreatePortal`, `DeleteUserSettings` und `ListBrowserSettings` Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anfrage mit Root- oder IAM-Benutzer-Anmeldeinformationen von ausgeführt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Erläuterungen der Amazon-WorkSpaces-Web-Protokolldateieinträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, die Anfrageparameter sowie weitere Details. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die Aktion `ListBrowserSettings` demonstriert.


```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
       "eventSource": "workspaces-web.amazonaws.com",
       "eventName": "ListBrowserSettings",
       "awsRegion": "us-west-2",
       "sourceIPAddress": "127.0.0.1",
       "userAgent": "[]",
       "requestParameters": null,
       "responseElements": null,
       "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
       "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
```

```
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    },
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    }]
}
```

Benutzerzugriffsprotokollierung

Amazon WorkSpaces Web ermöglicht es Kunden, Sitzungsereignisse aufzuzeichnen, einschließlich Start-, Stopp- und URL-Besuchen. Diese Protokolle werden an einen Amazon-Kinesis-Datenstrom übermittelt, den Sie für Ihr Webportal angeben. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.

Anleitung für Amazon WorkSpaces Web-Benutzer

Administratoren verwenden Amazon WorkSpaces Web, um Webportale zu erstellen, die eine Verbindung zu Unternehmenswebsites herstellen, z. B. interne Websites, software-as-a-service (SAAS)-Webanwendungen oder das Internet. Endbenutzer greifen über ihre vorhandenen Webbrowser auf diese Webportale zu, um eine Sitzung zu starten und auf Inhalte zuzugreifen.

Der folgende Inhalt hilft Endbenutzern, die mehr über den Zugriff auf Amazon WorkSpaces Web, das Starten und Konfigurieren einer Sitzung sowie die Verwendung der Symbolleiste und des Webbrowsers erfahren möchten.

Themen

- Browser- und Gerätekompatibilität
- Zugriff auf das Webportal
- Anleitung zur Sitzung
- Fehlerbehebung
- Erweiterung für Single Sign-On

Browser- und Gerätekompatibilität

Amazon WorkSpaces Web wird vom NICE DCV-Webbrowser-Client unterstützt, der in einem Webbrowser ausgeführt wird, sodass keine Installation erforderlich ist. Der Webbrowser-Client wird von gängigen Webbrowsern wie Chrome und Firefox sowie von den wichtigsten Desktop-Betriebssystemen wie Windows, macOS und Linux unterstützt.

Weitere up-to-date Informationen zur Unterstützung von Webbrowser-Clients finden Sie unter Webbrowser-Client.

> **Note**
>
> Webcam-Unterstützung ist derzeit nur in Chromium-basierten Browsern wie Google Chrome und Microsoft Edge verfügbar. Derzeit unterstützen Apple Safari und Mozilla FireFox keine Webcam.

Zugriff auf das Webportal

Ihr Administrator kann den Zugriff auf Ihr Webportal mit den folgenden Optionen gewähren:

- Sie können einen Link aus einer E-Mail oder Website auswählen und sich dann mit Ihren SAML-Identitätsdaten anmelden.
- Sie können sich bei Ihrem SAML-Identitätsanbieter (wie Okta, Ping oder Azure) anmelden und mit einem Klick von der Anwendungsstartseite Ihres SAML-Anbieters aus eine Sitzung starten (z. B. das Okta-Endbenutzer-Dashboard oder das Azure-Myapps-Portal).

Anleitung zur Sitzung

Nachdem Sie sich beim Webportal angemeldet haben, können Sie eine Sitzung starten und während Ihrer Sitzung verschiedene Aktionen ausführen.

Themen

- Starten einer Sitzung
- Die Symbolleiste verwenden
- Den Browser verwenden
- Beenden einer Sitzung

Starten einer Sitzung

Nachdem Sie sich angemeldet haben, um eine Sitzung zu starten, werden die Meldung Sitzung wird gestartet und der Fortschrittsbalken angezeigt. Dies weist darauf hin, dass Amazon WorkSpaces Web eine Sitzung für Sie erstellt. Amazon WorkSpaces Web erstellt im Hintergrund die Instance, startet den verwalteten Webbrowser und wendet Administratoreinstellungen und Browserrichtlinien an.

Wenn Sie sich zum ersten Mal in Ihrem Webportal anmelden, werden blaue Plus-Symbole in der Symbolleiste angezeigt. Dieses Symbol weist darauf hin, dass eine Anleitung verfügbar ist, das Sie durch die in der Symbolleiste verfügbaren Features führt. Mithilfe dieser Symbole können Sie lernen, wie Folgendes tun:

- Erlauben Sie Browserberechtigungen für das Mikrofon, die Webcam und die Zwischenablage, indem Sie das Schlosssymbol neben Ihrem lokalen Browser auswählen und den Schalter neben der Zwischenablage, dem Mikrofon und der Kamera auf Ein umstellen.

  > **Note**
  >
  > Wenn Sie zu Beginn Ihrer ersten Sitzung die Webcam-Berechtigungen aktivieren, wird die Webcam kurzzeitig aktiviert und eine LED auf Ihrem Computer blinkt. Dadurch wird der lokale Browserzugriff auf Ihre Webcam gewährt.

- Aktivieren Sie Amazon WorkSpaces Web, um zusätzliche Überwachungsfenster zu starten, indem Sie das Sperrsymbol in Ihrem Browser auswählen und die Einstellung auf Popups immer zulassen festlegen.

Wenn Sie eine Anleitung erneut starten möchten, können Sie in der Symbolleiste Profil, Hilfe und Anleitung starten auswählen.

Die Symbolleiste verwenden

Wenn Sie die Symbolleiste verschieben möchten, wählen Sie die hellere Leiste im oberen Bereich der Symbolleiste aus, ziehen Sie sie an die gewünschte Position und lassen Sie sie dann los, um sie abzulegen.

Wenn Sie die Symbolleiste minimieren möchten, bewegen Sie den Mauszeiger darüber und wählen Sie die Schaltfläche mit dem Aufwärtspfeil aus, oder klicken Sie zweimal auf die hellere Leiste im oberen Bereich. In der minimierten Ansicht haben Sie mehr Platz auf dem Bildschirm und können mit einem Klick auf die am häufigsten verwendeten Symbole zugreifen.

Um die Symbolleiste am oberen Rand des Bildschirms anzuhängen, wählen Sie Einstellungen , Allgemein und Docked unter Symbolleistenmodus aus.

Die folgende Tabelle enthält eine Beschreibung aller verfügbaren Symbole in der Symbolleiste:

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> Die Symbole für „Zwischenablage“ und „Dateien“ sind standardmäßig ausgeblendet, sofern Ihr Administrator diese Berechtigungen nicht erteilt. Nur Administratoren können die Zwischenablage und Dateien in einem Webportal aktivieren oder deaktivieren. Wenn diese Symbole ausgeblendet sind und Sie darauf zugreifen müssen, wenden Sie sich an Ihren Administrator.

Den Browser verwenden

Wenn Sie Ihre Sitzung starten, zeigt der Browser die Startup-URL an. Dabei handelt es sich um eine URL, die von Ihrem Administrator ausgewählt wurde. Wenn der Administrator keine Startup-URL ausgewählt hat, wird Ihnen die Standardumgebung mit neuen Registerkarten von Google Chrome angezeigt.

Im Browser können Sie Registerkarten öffnen, zusätzliche Browserfenster starten (über das Windows-Symbolleistensymbol oder das Dreipunktmenü des Browsers), eine URL eingeben bzw. in der URL-Leiste suchen oder über verwaltete Lesezeichen zu Websites wechseln. Wenn Sie auf Lesezeichen für das Webportal zugreifen möchten, öffnen Sie den Ordner Verwaltete Lesezeichen in der Lesezeichenleiste (unter der URL-Leiste) oder öffnen Sie den Lesezeichen-Manager über das Dreipunktmenü auf der rechten Seite der URL-Leiste.

Wenn Sie die Größe des Browserfensters ändern oder das Fenster verschieben möchten, ziehen Sie die Leiste mit den Registerkarten von Chrome nach unten. Dadurch steht während der Sitzung auf dem Bildschirm mehr Platz für mehrere Browserfenster zur Verfügung.

> **Note**
>
> Browser-Features wie der Inkognitomodus sind während Ihrer Sitzung möglicherweise nicht verfügbar, wenn Ihr Administrator sie deaktiviert hat.

Beenden einer Sitzung

Wenn Sie eine Sitzung beenden möchten, wählen Sie Profil und Sitzung beenden aus. Nach dem Ende einer Sitzung löscht Amazon WorkSpaces Web alle Daten aus der Sitzung. Nach dem Ende

einer Sitzung sind keine Browserdaten wie geöffnete Websites, Verlauf, Dateien oder Daten aus dem Datei-Explorer verfügbar.

Wenn Sie während einer aktiven Sitzung eine Registerkarte schließen, endet die Sitzung nach einem von Ihrem Administrator festgelegten Zeitraum. Wenn Sie die Registerkarte schließen und das Webportal vor dieser Zeitüberschreitung erneut aufrufen, können Sie der aktuellen Sitzung beitreten und alle Ihre vorherigen Sitzungsdaten anzeigen, z. B. geöffnete Websites und Dateien.

Fehlerbehebung

In meinem Amazon- WorkSpaces Web-Portal kann ich mich nicht anmelden. Ich habe die Fehlermeldung „Ihr Webportal ist noch nicht eingerichtet“ erhalten. Wenden Sie sich an Ihren IT-Administrator, um Hilfe zu erhalten“.

Ihr Administrator muss die Portalerstellung mit einem SAML-2.0-Identitätsanbieter abschließen, damit Sie sich anmelden können. Wenden Sie sich an Ihren Administrator, um Hilfe zu erhalten.

Mein Portal startet keine Sitzung. Ich habe die Fehlermeldung „Sitzung konnte nicht reserviert werden“ erhalten. Es ist ein interner Fehler aufgetreten. Bitte versuchen Sie es erneut.“

Beim Start Ihrer Webportal-Sitzung ist ein Problem aufgetreten. Versuchen Sie erneut, die Sitzung zu starten. Wenn das Problem weiterhin besteht, bitten Sie Ihren Administrator um Hilfe.

Ich kann die Zwischenablage, das Mikrofon oder die Webcam nicht verwenden.

Wenn Sie Browserberechtigungen zulassen möchten, klicken Sie auf das Schlosssymbol neben der URL und schalten Sie den blauen Schalter neben Zwischenablage, Mikrofon, Kamera und Pop-ups und Weiterleitungen um, damit dieses Feature aktiviert wird.

> **Note**
>
> Wenn Ihr Webbrowser die Video- oder Audioeingabe nicht unterstützt, werden diese Optionen nicht in der Symbolleiste angezeigt.

Amazon WorkSpaces Web Echtzeit-Audio-Video (AV) leitet Ihre lokale Webcam-Video- und Mikrofon-Audioeingabe an die Browser-Streaming-Sitzung um. Auf diese Weise können Sie innerhalb Ihrer Streaming-Sitzung mit Chromium-basierten Webbrowsern wie Google Chrome oder Microsoft Edge Ihre lokalen Geräte für Video- und Audiokonferenzen verwenden. Webcam wird derzeit in Browsern, die nicht Chromium-basiert sind, nicht unterstützt.

Informationen zur Konfiguration von Google Chrome finden Sie unter Kamera und Mikrofon verwenden in Chrome.

Mein Webportal öffnet kein zusätzliches Monitorfenster.

Wenn Sie versuchen, zwei Monitore zu starten und am Ende der Adressleiste im oberen Browser ein Symbol für Pop-ups blockiert angezeigt wird, wählen Sie das Symbol und das Optionsfeld neben Pop-ups und Weiterleitungen immer zulassen aus. Wenn Pop-ups zulässig sind, wählen Sie in der Symbolleiste das Symbol für zwei Monitore aus, um ein neues Fenster zu öffnen. Positionieren Sie das Fenster auf Ihrem Monitor neu und ziehen Sie eine Browser-Registerkarte in das Fenster.

Wenn ich versuche, Dateien aus dem Dateibereich herunterzuladen, passiert nichts.

Wenn Sie versuchen, Dateien aus dem Bereich Dateien herunterzuladen und am Ende der Adressleiste im oberen Browser ein Symbol für Pop-ups blockiert angezeigt wird, wählen Sie das Symbol und das Optionsfeld neben Pop-ups und Weiterleitungen immer zulassen aus. Wenn Pop-ups zulässig sind, versuchen Sie erneut, die Dateien herunterzuladen.

Erweiterung für Single Sign-On

Amazon WorkSpaces Web bietet eine Erweiterung für Single Sign-On mit Chrome- und Firefox-Browsern auf Desktop-Computern. Wenn Ihr Administrator die Erweiterung aktiviert hat, werden Sie vom Webportal bei der Anmeldung aufgefordert, die Erweiterung zu installieren.

Amazon WorkSpaces Web hat die -Erweiterung erstellt, um Single Sign-On auf Websites während Ihrer Sitzung zu ermöglichen. Wenn Sie sich beispielsweise mit einem SAML-2.0-Identitätsanbieter (wie Okta oder Ping) bei Ihrem Webportal anmelden und während Ihrer Sitzung eine Website besuchen, die denselben Identitätsanbieter verwendet, kann die Erweiterung den Zugriff auf die Website erleichtern, indem zusätzliche Anmeldeaufforderungen entfernt werden.

Sie müssen die Erweiterung nicht installieren, um auf Ihr Webportal zugreifen zu können, aber sie kann Ihr Erlebnis verbessern, da Sie weniger oft aufgefordert werden, Ihren Benutzernamen und Ihr Passwort einzugeben.

Wenn Sie sich anmelden, sucht die Erweiterung nach den Cookies, die Ihr Administrator für Ihre Sitzung angegeben hat. Alle von der Erweiterung gefundenen Daten, werden im Ruhezustand und während der Übertragung verschlüsselt. Keine dieser Daten wird in Ihrem lokalen Browser gespeichert. Wenn Sie Ihre Sitzung beenden, werden alle Ihre Sitzungsdaten (z. B. geöffnete Registerkarten, heruntergeladene Dateien und Cookies, die an die Sitzung gesendet oder während der Sitzung erstellt wurden) gelöscht.

Kompatibilität

Die Erweiterung funktioniert bei folgenden Geräten:

- Laptops
- Desktop-Computer

Die Erweiterung funktioniert mit folgenden Browsern:

- Chrome
- Firefox

Installation

Folgen Sie bei Anmeldung im Portal der Aufforderung, die Erweiterung für Ihren Chrome- oder Firefox-Browser aus dem Webshop Ihres Browsers zu installieren. Sie müssen dies für jeden Webbrowser nur einmal tun.

Wenn Sie das Gerät wechseln, auf demselben Gerät zu einem anderen Browser wechseln oder die Erweiterung aus Ihrem lokalen Browser löschen, werden Sie beim Start Ihrer nächsten Sitzung aufgefordert, die Erweiterung zu installieren.

Wenn Sie sicherzustellen möchten, dass die Erweiterung erwartungsgemäß funktioniert, verwenden Sie sie auf einer normalen Browser-Registerkarte und nicht im Inkognitomodus (Chrome) oder im privaten Modus (Firefox).

Fehlerbehebung

Wenn Sie die Erweiterung installiert haben, Sie aber während Ihrer Sitzung immer noch zur Anmeldung aufgefordert werden, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie die Amazon WorkSpaces -Web-Erweiterung in Ihrem Browser installiert haben. Falls Sie Ihre Browserdaten gelöscht haben sollten, haben Sie die Erweiterung möglicherweise versehentlich entfernt.
2. Stellen Sie sicher, dass Sie nicht im Inkognitomodus (Chrome) oder im privaten Modus (Firefox) surfen. Diese Modi können zu Problemen mit Erweiterungen führen.
3. Wenn das Problem weiterhin besteht, bitten Sie Ihren Portaladministrator um weitere Hilfe.

Dokumentverlauf für das Amazon WorkSpaces Web-Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für Amazon WorkSpaces Web beschrieben.

Änderung	Beschreibung	Datum
CloudWatch -Metriken	- GlobalCpuPercent und - GlobalMemoryPercent Metriken hinzugefügt.	26. Februar 2024
URL-Filterung einrichten	Sie können Chrome Policy verwenden, um zu filtern, auf welche URLs Benutzer von ihrem Remote-Browser aus zugreifen können.	21. Februar 2024
IdP-Authentifizierungstypen	Sie können entweder den Standard- oder den IAM-Identity-Center-Authentifizierungstyp auswählen.	5. Februar 2024
Erweiterung für Single-Sign-On aktivieren	Sie können eine Erweiterung für Ihre Endbenutzer aktivieren, um die Portalanmeldung zu verbessern.	28. August 2023
Benutzeranleitung für Amazon WorkSpaces Web	Inhalte wurden hinzugefügt, um Endbenutzer zu unterstützen, die mehr über den Zugriff auf Amazon WorkSpaces Web, das Starten und Konfigurieren einer Sitzung und die Verwendung der Symbolleiste und	17. Juli 2023

	des Webbrowsers erfahren möchten.	
IP-Zugriffskontrollen	WorkSpaces Mit Web können Sie steuern, von welchen IP-Adressen aus auf Ihr Webportal zugegriffen werden kann.	31. Mai 2023
Aktualisierung der verwalteten Richtlinien	Aktualisierte AmazonWorkSpacesWebReadOnly verwaltete Richtlinie	15. Mai 2023
Identitätsanbieteraktualisierung konfigurieren	WorkSpaces Web bietet zwei Authentifizierungstypen: Standard und AWS IAM Identity Center	15. März 2023
Aktualisierung der Browser-Richtlinie	Der Abschnitt mit den Browser-Richtlinien wurde aktualisiert und neu strukturiert.	31. Januar 2023
Aktualisierung der verwalteten Richtlinien	Aktualisierte AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie	15. Dezember 2022
Zulassungsliste und Sperrliste	Geben Sie die Zulassungsliste und die Sperrliste an, um eine Liste von Domains anzugeben, auf die Ihre Benutzer zugreifen können oder nicht.	14. November 2022
Aktualisierung der verwalteten Richtlinien	Aktualisierte AmazonWorkSpacesWebReadOnly verwaltete Richtlinie	02. November 2022

Aktualisierung der verwalteten Richtlinien	Aktualisierte AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie	24. Oktober 2022
Benutzerzugriffsprotokollierung	Die Benutzerzugriffsprotokollierung zum Aufnehmen von Benutzerereignissen wurde eingerichtet.	17. Oktober 2022
Netzwerkaktualisierungen	Es wurden verschiedene Aktualisierungen im Abschnitt „Netzwerk und Zugriff“ vorgenommen.	22. September 2022
Aktualisierung der verwalteten Richtlinien	Aktualisierte AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie	6. September 2022
Benutzersitzungen konfigurieren	Den Eingabemethoden-Editor (IME) und die sitzungsinterne Lokalisierung konfigurieren	28. Juli 2022
Netzwerkaktualisierungen	Es wurden verschiedene Aktualisierungen im Abschnitt „Netzwerk und Zugriff“ vorgenommen.	7. Juli 2022
Zeitüberschreitungswerte	Geben Sie das Zeitüberschreitung beim Trennen der Verbindung in Minuten und das Zeitüberschreitung beim Trennen der Verbindung bei Nichtbenutzung in Minuten an.	16. Mai 2022

Verwaltete Richtlinie aktualisiert	Die AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie wurde aktualisiert, um den AWS/Usage-Namespace zu den PutMetricData API-Berechtigungen hinzuzufügen.	6. April 2022
Serviceverknüpfte Rolle	Neue AWSServiceRoleForAmazonWorkSpacesWeb serviceverknüpfte Rolle	30. November 2021
Verwaltete Richtlinie	Neue AmazonWorkSpacesWebReadOnly verwaltete Richtlinie	30. November 2021
Verwaltete Richtlinie	Neue AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie	30. November 2021
Erstversion	Erstveröffentlichung des WorkSpaces Web-Administratorhandbuchs	30. November 2021

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.