AWS Whitepaper

Bewährte Methoden für die Bereitstellung von WorkSpaces

Bewährte Methoden für die Bereitstellung von WorkSpaces: AWS Whitepaper

Table of Contents

Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces

Veröffentlichungsdatum: 1. Juni 2022 (Dokumentversionen)

Überblick

In diesem Whitepaper wird eine Reihe von bewährten Methoden für die Bereitstellung von beschrieben WorkSpaces. Das Whitepaper behandelt Netzwerküberlegungen, Verzeichnisservices und Benutzerauthentifizierung, Sicherheit sowie Überwachung und Protokollierung.

Dieses Whitepaper ermöglicht auch den schnellen Zugriff auf relevante Informationen und richtet sich an Netzwerkingenieure, Verzeichnisingenieure oder Sicherheitsingenieure.

Einführung

Amazon WorkSpaces ist ein verwalteter Desktop-Computing-Service in der Cloud. Amazon WorkSpaces eliminiert den Aufwand für die Beschaffung oder Bereitstellung von Hardware oder die Installation komplexer Software und bietet ein Desktop-Erlebnis entweder mit wenigen Klicks auf AWS Management Console, über die Amazon Web Services (AWS)-Befehlszeilenschnittstelle (CLI) oder über die Anwendungsprogrammierschnittstelle (API). Mit Amazon können WorkSpacesSie innerhalb weniger Minuten einen Microsoft-Windows- oder Amazon-Linux-Desktop starten, mit dem Sie eine sichere, zuverlässige und schnelle Verbindung zu Ihrer Desktop-Software herstellen und von On-Premises oder von einem externen Netzwerk aus darauf zugreifen können. Sie haben folgende Möglichkeiten:

- Nutzen Sie Ihr vorhandenes, On-Premises-Microsoft Active Directory (AD), indem Sie AWS Directory Service verwenden: Active Directory Connector (AD Connector).
- Erweitern Sie Ihr Verzeichnis auf die - AWS Cloud.
- Erstellen Sie ein verwaltetes Verzeichnis mit AWS Directory Service Microsoft AD oder Simple AD, um Ihre Benutzer und zu verwalten WorkSpaces.
- Nutzen Sie Ihren On-Premises- oder Cloud-gehosteten RADIUS-Server mit AD Connector, um Multi-Faktor-Authentifizierung (MFA) für Ihr bereitzustellen WorkSpaces.

Sie können die Bereitstellung von Amazon WorkSpaces mithilfe der CLI oder API automatisieren, mit der Sie Amazon WorkSpaces in Ihre vorhandenen Bereitstellungsworkflows integrieren können.

Aus Sicherheitsgründen können Sie zusätzlich zur integrierten Netzwerkverschlüsselung, die der Amazon- WorkSpaces Service bereitstellt, auch die Verschlüsselung im Ruhezustand für Ihr aktivieren WorkSpaces. Weitere Informationen finden Sie im Abschnitt Verschlüsselt WorkSpaces dieses Dokuments.

Sie können Anwendungen in Ihrem bereitstellen, WorkSpaces indem Sie Ihre vorhandenen On-Premises-Tools wie Microsoft System Center Configuration Manager (SCCM), Puppet Enterprise oder Ansible verwenden.

Die folgenden Abschnitte enthalten Details zu Amazon WorkSpaces, erläutern, wie der Service funktioniert, beschreiben, was Sie zum Starten des Services benötigen, und teilen Ihnen mit, welche Optionen und Funktionen Sie verwenden können.

WorkSpaces -Anforderungen

Der Amazon WorkSpaces -Service erfordert drei Komponenten, um erfolgreich bereitgestellt zu werden:

- WorkSpaces Clientanwendung – Ein von Amazon unterstütztes Client WorkSpaces-Gerät. Weitere Informationen finden Sie unter Erste Schritte mit Ihrem WorkSpace.

  Sie können Personal Computer over Internet Protocol (PCoIP) Zero Clients auch verwenden, um eine Verbindung zu herzustellen WorkSpaces. Eine Liste der verfügbaren Geräte finden Sie unterPCoIP Zero Clients für Amazon WorkSpaces.
- Ein Verzeichnisservice zur Authentifizierung von Benutzern und zur Bereitstellung des Zugriffs auf ihre WorkSpace – Amazon arbeitet WorkSpaces derzeit mit AWS Directory Service und Microsoft AD zusammen. Sie können Ihren On-Premises-AD-Server mit AWS Directory Service verwenden, um Ihre vorhandenen Unternehmensbenutzeranmelde informationen mit Amazon zu unterstützen WorkSpaces.
- Amazon Virtual Private Cloud (Amazon VPC), in der Sie Ihr Amazon ausführen können WorkSpaces – Sie benötigen mindestens zwei Subnetze für eine Amazon WorkSpaces-Bereitstellung, da jedes AWS Directory-Service-Konstrukt zwei Subnetze in einer Multi-AZ-Bereitstellung benötigt.

Überlegungen zu Netzwerken

Jede WorkSpace ist dem spezifischen Amazon VPC- und AWS Directory Service-Konstrukt zugeordnet, mit dem Sie sie erstellt haben. Alle AWS Directory-Service-Konstrukte (Simple AD, AD Connector und Microsoft AD) benötigen zwei Subnetze, die jeweils in verschiedenen Availability Zones (AZs) betrieben werden. Subnetze sind einem Directory-Service-Konstrukt dauerhaft zugeordnet und können nach der Erstellung nicht mehr geändert werden. Aus diesem Grund müssen Sie unbedingt die richtigen Subnetzgrößen bestimmen, bevor Sie das Directory-Services-Konstrukt erstellen. Berücksichtigen Sie sorgfältig Folgendes, bevor Sie die Subnetze erstellen:

- Wie viele benötigen WorkSpaces Sie im Laufe der Zeit?
- Was ist das erwartete Wachstum?
- Welche Arten von Benutzern müssen Sie unterbringen?
- Wie viele AD-Domains möchten Sie verbinden?
- Wo befinden sich Ihre Unternehmenskonten?

Amazon empfiehlt, Benutzergruppen oder Personas basierend auf der Art des Zugriffs und der Benutzerauthentifizierung zu definieren, die Sie im Rahmen Ihres Planungsprozesses benötigen. Antworten auf diese Fragen sind hilfreich, wenn Sie den Zugriff auf bestimmte Anwendungen oder Ressourcen einschränken müssen. Definierte Benutzerrollen können Ihnen helfen, den Zugriff mithilfe von AWS Directory Service, Netzwerkzugriffskontrolllisten, Routing-Tabellen und VPC-Sicherheitsgruppen zu segmentieren und einzuschränken. Jedes AWS Directory-Service-Konstrukt verwendet zwei Subnetze und wendet die gleichen Einstellungen auf alle an WorkSpaces , die von diesem Konstrukt aus starten. Sie können beispielsweise eine Sicherheitsgruppe verwenden, die für alle gilt, die an einen AD Connector WorkSpaces angefügt sind, um anzugeben, ob MFA erforderlich ist oder ob ein Endbenutzer lokalen Administratorzugriff auf sein haben kann WorkSpace.

> **Note**
>
> Jeder AD Connector stellt eine Verbindung zu Ihrem vorhandenen Enterprise Microsoft AD her. Um diese Funktion zu nutzen und eine Organisationseinheit (OU) anzugeben, müssen Sie Ihren Directory Service so konstruieren, dass er Ihre Benutzerrollen berücksichtigt.

VPC-Design

In diesem Abschnitt werden bewährte Methoden für die Dimensionierung Ihrer VPC und Subnetze, den Datenverkehrsfluss und die Auswirkungen auf das Design von Verzeichnisservices beschrieben.

Hier sind einige Dinge, die Sie beim Entwerfen der VPC, der Subnetze, Sicherheitsgruppen, Routing-Richtlinien und Netzwerkzugriffskontrolllisten (ACLs) für Ihr Amazon berücksichtigen sollten, WorkSpaces damit Sie Ihre WorkSpaces Umgebung für Skalierbarkeit, Sicherheit und Benutzerfreundlichkeit erstellen können:

- VPC – Wir empfehlen, eine separate VPC speziell für Ihre WorkSpaces Bereitstellung zu verwenden. Mit einer separaten VPC können Sie die erforderlichen Leitlinien für Governance und Sicherheit für Ihre angeben, WorkSpaces indem Sie eine Trennung des Datenverkehrs einrichten.
- Directory Services – Jedes AWS Directory Service Konstrukt erfordert ein Paar von Subnetzen, die eine hochverfügbare Verzeichnisserviceaufteilung zwischen AZs bieten.
- Subnetzgröße – WorkSpaces Bereitstellungen sind an ein Verzeichniskonstrukt gebunden und befinden sich in derselben VPC wie Ihr gewähltes AWS Directory Service, können sich jedoch in verschiedenen VPC-Subnetzen befinden. Einige Überlegungen:
  - Subnetzgrößen sind dauerhaft und können sich nicht ändern. Sie sollten genügend Platz für zukünftiges Wachstum lassen.
  - Sie können eine Standardsicherheitsgruppe für die von Ihnen ausgewählten angeben AWS Directory Service. Die Sicherheitsgruppe gilt für alle WorkSpaces , die dem spezifischen AWS Directory Service Konstrukt zugeordnet sind.
  - Sie können mehrere Instances von dasselbe Subnetz AWS Directory Service verwenden.

Berücksichtigen Sie zukünftige Pläne, wenn Sie Ihre VPC entwerfen. Sie können beispielsweise Verwaltungskomponenten wie einen Antivirenserver, einen Patch-Managementserver oder einen AD- oder RADIUS-MFA-Server hinzufügen. Es lohnt sich, zusätzliche verfügbare IP-Adressen in Ihrem VPC-Design zu planen, um solche Anforderungen zu erfüllen.

Ausführliche Anleitungen und Überlegungen zum VPC-Design und zur Dimensionierung von Subnetzen finden Sie in der re:Invent-Präsentation Wie Amazon.com zu Amazon wechselt WorkSpaces.

Netzwerkschnittstellen

Jede WorkSpaces hat zwei Elastic Network-Schnittstellen (ENIs), eine Verwaltungsnetzwerkschnittstelle (`eth0`) und eine primäre Netzwerkschnittstelle (`eth1`). AWS verwendet die Verwaltungsnetzwerkschnittstelle zur Verwaltung der WorkSpace – es ist die Schnittstelle, auf der Ihre Client-Verbindung beendet wird. AWS verwendet einen privaten IP-Adressbereich für diese Schnittstelle. Damit das Netzwerk-Routing ordnungsgemäß funktioniert, können Sie diesen privaten Adressraum nicht in einem Netzwerk verwenden, das mit Ihrer WorkSpaces VPC kommunizieren kann.

Eine Liste der privaten IP-Bereiche, die pro Region verwendet werden, finden Sie unter Amazon WorkSpaces Details.

> **Note**
>
> Amazon WorkSpaces und die zugehörigen Verwaltungsnetzwerkschnittstellen befinden sich nicht in Ihrer VPC und Sie können die Verwaltungsnetzwerkschnittstelle oder die Amazon Elastic Compute Cloud (Amazon EC2)-Instance-ID in Ihrem nicht anzeigen AWS Management Console (siehe Figure 5Figure 6, und Figure 7). Sie können jedoch die Sicherheitsgruppeneinstellungen Ihrer primären Netzwerkschnittstelle (`eth1`) in der -Konsole anzeigen und ändern. Die primäre Netzwerkschnittstelle jeder WorkSpace wird auf Ihre ENI-Amazon EC2Ressourcenkontingente angerechnet. Für große Bereitstellungen von Amazon müssen Sie ein Support-Ticket über die öffnen WorkSpaces, AWS Management Console um Ihre ENI-Kontingente zu erhöhen.

Datenverkehrsfluss

Sie können den Amazon- WorkSpaces Datenverkehr in zwei Hauptkomponenten aufteilen:

- Der Datenverkehr zwischen dem Client-Gerät und dem Amazon- WorkSpaces Service.
- Der Datenverkehr zwischen dem Amazon- WorkSpaces Service und dem Kundennetzwerkverkehr.

Im nächsten Abschnitt werden beide Komponenten behandelt.

Client-Gerät zu WorkSpace

Unabhängig von seinem Standort (lokal oder remote) verwendet das Gerät, auf dem der Amazon WorkSpaces-Client ausgeführt wird, dieselben beiden Ports für die Konnektivität mit dem Amazon-WorkSpaces Service. Der Client verwendet Port 443 (HTTPS-Port) für alle Authentifizierungs- und sitzungsbezogenen Informationen sowie Port 4172 (PCoIP-Port) mit Transmission Control Protocol (TCP) und User Datagram Protocol (UDP), um Pixel-Streaming an eine bestimmte WorkSpace und Netzwerkzustandsprüfungen durchzuführen. Der Datenverkehr auf beiden Ports ist verschlüsselt. Port 443-Datenverkehr wird für Authentifizierungs- und Sitzungsinformationen verwendet und verwendet TLS für die Verschlüsselung des Datenverkehrs. Pixel-Streaming-Datenverkehr verwendet AES-256-bitVerschlüsselung für die Kommunikation zwischen dem Client und `eth0` der über WorkSpacedas Streaming-Gateway. Weitere Informationen finden Sie im Sicherheit Abschnitt dieses Dokuments.

Wir veröffentlichen pro Region IP-Bereiche unserer PCoIP-Streaming-Gateways und Endpunkte für Netzwerkzustandsprüfungen. Sie können ausgehenden Datenverkehr auf Port 4172 von Ihrem Unternehmensnetzwerk auf das AWS Streaming-Gateway und die Endpunkte für die Netzwerkintegritätsprüfung beschränken, indem Sie nur ausgehenden Datenverkehr auf Port 4172 zu den spezifischen AWS Regionen zulassen, in denen Sie Amazon verwenden WorkSpaces. Informationen zu den IP-Bereichen und Endpunkten für die Netzwerkintegritätsprüfung finden Sie unter IP-Bereiche für Amazon WorkSpaces PCoIP Gateway.

Der Amazon- WorkSpaces Client verfügt über eine integrierte Netzwerkstatusprüfung. Dieses Dienstprogramm zeigt Benutzern, ob ihr Netzwerk eine Verbindung mithilfe eines Statusindikators unten rechts in der Anwendung unterstützen kann. Die folgende Abbildung zeigt eine detailliertere Ansicht des Netzwerkstatus, auf den Sie zugreifen können, indem Sie oben rechts im Client Netzwerk auswählen.

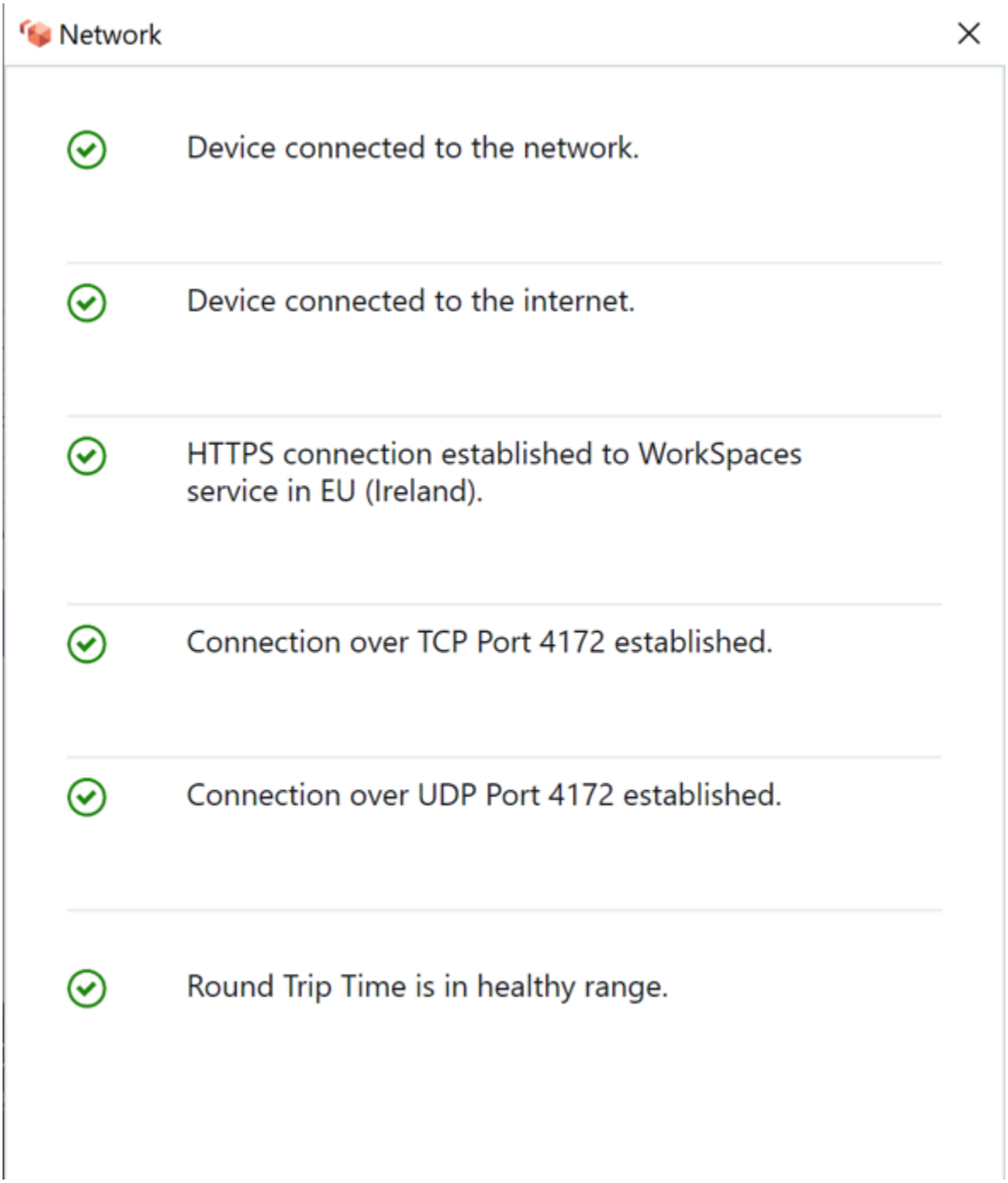


Abbildung 1: WorkSpaces Client: Netzwerkprüfung

Ein Benutzer initiiert eine Verbindung von seinem Client zum Amazon- WorkSpaces Service, indem er seine Anmeldeinformationen für das Verzeichnis bereitstellt, das vom Directory-Service-Konstrukt verwendet wird, in der Regel sein Unternehmensverzeichnis. Die Anmeldeinformationen werden über HTTPS an die Authentifizierungs-Gateways des Amazon- WorkSpaces Services in der Region gesendet, in der sich das WorkSpace befindet. Das Authentifizierungs-Gateway des Amazon-

WorkSpaces Services leitet dann den Datenverkehr an das spezifische AWS Directory-Service-Konstrukt weiter, das Ihrem zugeordnet ist WorkSpace.

Wenn Sie beispielsweise den AD Connector verwenden, leitet der AD Connector die Authentifizierungsanforderung direkt an Ihren AD-Service weiter, der On-Premises oder in einer AWS VPC sein könnte. Weitere Informationen finden Sie im Abschnitt AD-DS-Bereitstellungsszenarien in diesem Dokument. Der AD Connector speichert keine Authentifizierungsinformationen und fungiert als zustandsloser Proxy. Daher ist es zwingend erforderlich, dass AD Connector über Konnektivität zu einem AD-Server verfügt. Der AD Connector bestimmt, mit welchem AD-Server eine Verbindung hergestellt werden soll, indem die DNS-Server verwendet werden, die Sie beim Erstellen des AD Connectors definieren.

Wenn Sie einen AD Connector verwenden und MFA für das Verzeichnis aktiviert haben, wird das MFA-Token vor der Verzeichnisdienstauthentifizierung überprüft. Wenn die MFA-Validierung fehlschlägt, werden die Anmeldeinformationen des Benutzers nicht an Ihren AWS Directory Service weitergeleitet.

Sobald ein Benutzer authentifiziert wurde, beginnt der Streaming-Datenverkehr mit Port 4172 (PCoIP-Port) über das AWS Streaming-Gateway zur WorkSpace. Sitzungsbezogene Informationen werden während der gesamten Sitzung weiterhin über HTTPS ausgetauscht. Der Streaming-Datenverkehr verwendet die erste ENI auf der WorkSpace (`eth0` auf der WorkSpace), die nicht mit Ihrer VPC verbunden ist. Die Netzwerkverbindung vom Streaming-Gateway zur ENI wird von verwaltet AWS. Im Falle eines Verbindungsfehlers von den Streaming-Gateways zur WorkSpaces Streaming-ENI wird ein CloudWatch Ereignis generiert. Weitere Informationen finden Sie im Abschnitt Überwachung oder Protokollierung mit Amazon CloudWatch in diesem Dokument.

Die Datenmenge, die zwischen dem Amazon- WorkSpaces Service und dem Client gesendet wird, hängt vom Grad der Pixelaktivität ab. Um ein optimales Benutzererlebnis zu gewährleisten, empfehlen wir, dass die Round-Trip-Zeit (RTT) zwischen dem WorkSpaces Client und der AWS Region, in der WorkSpaces sich Ihr befindet, weniger als 100 Millisekunden (ms) beträgt. In der Regel bedeutet dies, dass sich Ihr WorkSpaces Client weniger als zweitausend Kilometer von der Region befindet, in der gehostet WorkSpace wird. Die Webseite Connection Health Check kann Ihnen helfen, die optimale AWS Region für die Verbindung mit dem Amazon- WorkSpaces Service zu ermitteln.

Amazon WorkSpaces Service zu VPC

Nachdem eine Verbindung von einem Client zu einem authentifiziert WorkSpace und Streaming-Datenverkehr initiiert wurde, zeigt Ihr WorkSpaces Client entweder einen Windows- oder Linux-Desktop (Ihr Amazon WorkSpace) an, der mit Ihrer Virtual Private Cloud (VPC) verbunden ist, und Ihr Netzwerk sollte zeigen, dass Sie diese Verbindung hergestellt haben. Der primären Elastic Network Interface (ENI) WorkSpacevon `eth1`wird eine IP-Adresse vom Dynamic Host Configuration Protocol (DHCP)-Service zugewiesen, die von Ihrer VPC bereitgestellt wird, in der Regel aus denselben Subnetzen wie Ihr AWS Directory Service. Die IP-Adresse bleibt für die WorkSpace Dauer der Lebensdauer des bei WorkSpace. Die ENI in Ihrer VPC hat Zugriff auf jede Ressource in der VPC und auf jedes Netzwerk, das Sie mit Ihrer VPC verbunden haben (über ein VPC-Peering, eine - AWS Direct Connect Verbindung oder eine VPN-Verbindung).

Der ENI-Zugriff auf Ihre Netzwerkressourcen wird durch die Routing-Tabelle des Subnetzes und der Standardsicherheitsgruppe bestimmt, die Ihr AWS Directory Service für jede konfiguriert WorkSpace, sowie durch alle zusätzlichen Sicherheitsgruppen, die Sie der ENI zuweisen. Sie können der ENI, die auf Ihre VPC ausgerichtet ist, jederzeit Sicherheitsgruppen hinzufügen, indem Sie die AWS Management Console oder verwenden AWS CLI. (Weitere Informationen zu Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihr WorkSpaces.) Zusätzlich zu Sicherheitsgruppen können Sie Ihre bevorzugte hostbasierte Firewall auf einem bestimmten verwenden, WorkSpace um den Netzwerkzugriff auf Ressourcen innerhalb der VPC zu beschränken.

Es wird empfohlen, Ihre DHCP-Optionsliste mit der/den DNS Server-IP(s) und vollqualifizierten Domainnamen zu erstellen, die für Ihr Active Directory spezifisch für Ihre Umgebung autoritativ sind, und diese benutzerdefinierten DHCP-Optionsliste dann der von Amazon verwendeten Amazon VPC zuzuweisen WorkSpaces. Standardmäßig verwendet Amazon Virtual Private Cloud (Amazon VPC) AWS DNS anstelle Ihres Verzeichnisservice-DNS. Durch die Verwendung eines DHCP-Optionssatzes wird eine ordnungsgemäße DNS-Namensauflösung und konsistente Konfiguration Ihrer internen DNS-Namenserver nicht nur für Ihr WorkSpaces, sondern auch für alle unterstützenden Workloads (Workloads) oder Instance(s) sichergestellt, die Sie möglicherweise für Ihre Bereitstellung geplant haben.

Wenn DHCP-Optionen angewendet werden, gibt es zwei wichtige Unterschiede in Bezug darauf, wie sie auf angewendet werden WorkSpaces , im Vergleich dazu, wie sie mit herkömmlichen EC2-Instances angewendet werden:

- Der erste Unterschied besteht darin, wie DNS-Suffixe der DHCP-Option angewendet werden. Für jeden WorkSpace sind DNS-Einstellungen für seinen Netzwerkadapter konfiguriert, wobei die

Optionen Primäre und verbindungsspezifische DNS-Suffixe anfügen und übergeordnete Suffixe der primären DNS-Suffix-Optionen anfügen aktiviert sind. Die Konfiguration wird mit dem DNS-Suffix aktualisiert, das in dem AWS von Ihnen registrierten und WorkSpace standardmäßig mit dem verknüpften Directory Service konfiguriert ist. Wenn sich das DNS-Suffix, das im verwendeten DHCP-Optionssatz konfiguriert ist, unterscheidet, wird es hinzugefügt und auf alle zugehörigen angewendet WorkSpaces.

- Der zweite Unterschied besteht darin, dass die konfigurierten DNS-IPs der DHCP-Option nicht auf den angewendet werden, WorkSpace da der Amazon- WorkSpaces Service die IP-Adressen der Domain-Controller des konfigurierten Verzeichnisses priorisiert.

Alternativ können Sie eine privat gehostete Route-53-Zone konfigurieren, um eine Hybrid- oder Split-DNS-Umgebung zu unterstützen und eine ordnungsgemäße DNS-Auflösung für Ihre Amazon-WorkSpaces Umgebung zu erhalten. Weitere Informationen finden Sie unter Hybrid Cloud DNS-Optionen für VPC und AWS Hybrid DNS mit Active Directory .

> **Note**
>
> Jeder WorkSpace muss die IP-Tabelle aktualisieren, wenn ein neuer oder anderer DHCP-Optionssatz auf die VPC angewendet wird. Zur Aktualisierung können Sie ipconfig /renew ausführen oder eine WorkSpace(s) in der VPC neu starten, die mit Ihrem aktualisierten DHCP-Optionssatz konfiguriert ist. Wenn Sie AD Connector verwenden und die IP-Adressen Ihrer verbundenen IP-Adressen/Domain-Controller aktualisieren, müssen Sie dann den Bollight-`DomainJoinDNS`Registrierungsschlüssel auf Ihrem aktualisieren WorkSpaces. Es wird empfohlen, dies über ein GPO zu tun. Der Pfad zu diesem Registrierungsschlüssel ist `HKLM:\SOFTWARE\Amazon\Skylight`. Der Wert dieses Werts `REG_SZ` wird nicht aktualisiert, wenn die DNS-Einstellungen des AD Connectors geändert werden und VPC DHCP Options Sets diesen Schlüssel ebenfalls nicht aktualisiert.

Die Abbildung im Abschnitt AD-DS-Bereitstellungsszenarien dieses Whitepapers zeigt den beschriebenen Datenverkehrsfluss.

Wie zuvor erläutert, priorisiert der Amazon- WorkSpaces Service die Domain-Controller-IP-Adressen des konfigurierten Verzeichnisses für die DNS-Auflösung und ignoriert die in Ihrem DHCP-Optionssatz konfigurierten DNS-Server. Wenn Sie eine genauere Kontrolle über Ihre DNS-Servereinstellungen für Ihr Amazon benötigen WorkSpaces, können Sie die Anweisungen zum

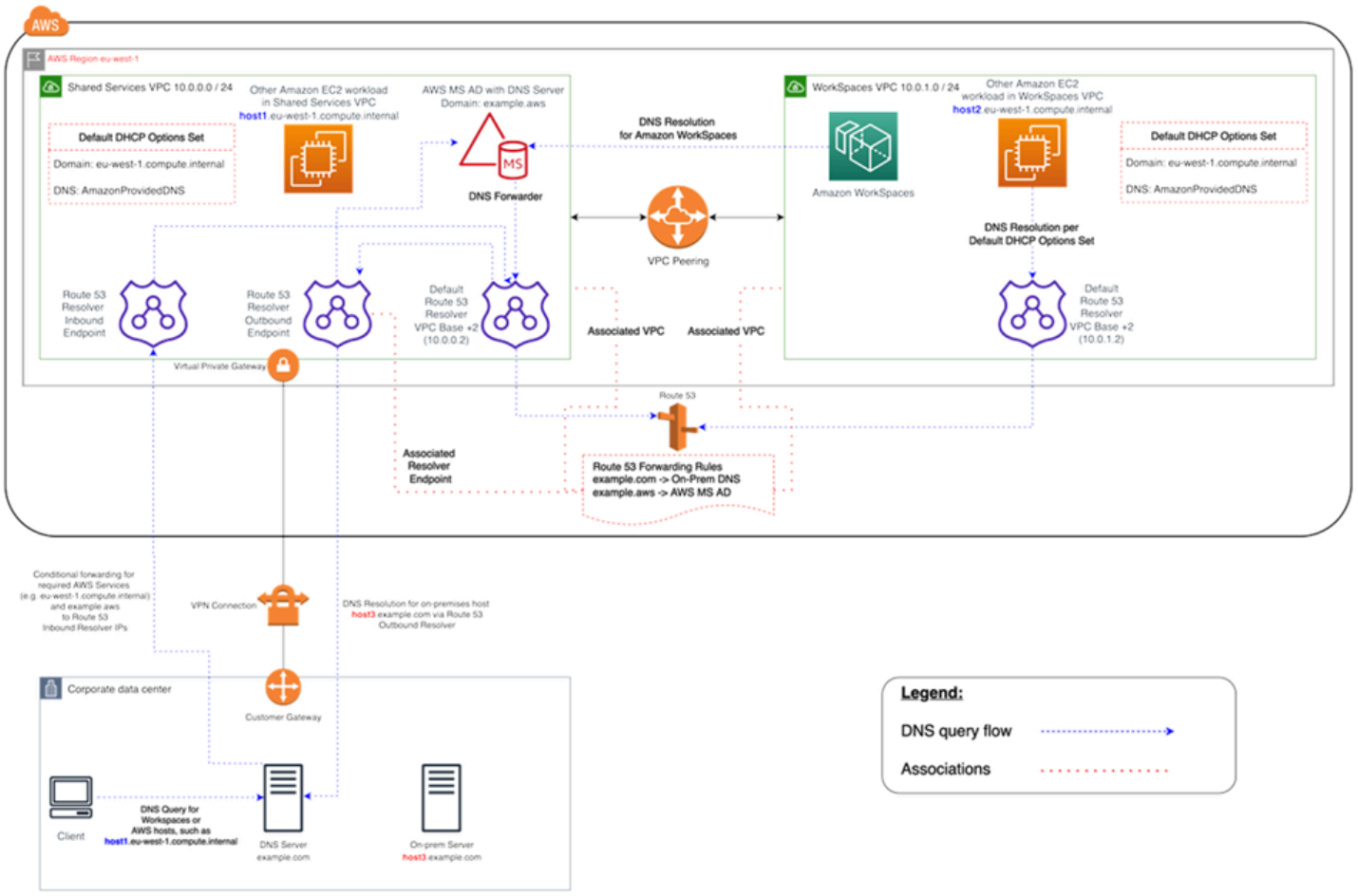
Aktualisieren von DNS-Servern für Amazon WorkSpaces im Handbuch DNS-Server für Amazon aktualisieren WorkSpaces des Amazon- WorkSpaces Administratorhandbuchs verwenden.

Wenn Sie andere -Services in auflösen WorkSpaces müssen und wenn Sie die standardmäßigen DHCP-Optionen verwenden AWS, die mit Ihrer VPC festgelegt sind, muss Ihr Domain-Controller-DNS-Service in dieser VPC daher so konfiguriert sein, dass er DNS-Weiterleitung verwendet, die auf den Amazon-DNS-Server mit der IP-Adresse auf der Basis Ihres VPC-CIDR plus zwei verweist. Das heißt, wenn Ihr VPC-CIDR 10.0.0.0/24 ist, konfigurieren Sie die DNS-Weiterleitung so, dass der standardmäßige Route-53-DNS-Resolver bei 10.0.0.0.2 verwendet wird. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html

Falls Ihre eine DNS-Auflösung von Ressourcen in Ihrem On-Premises-Netzwerk WorkSpaces benötigen, können Sie einen ausgehenden Route-53-Resolver-Endpunkt verwenden, eine Route-53-Weiterleitungsregel erstellen und diese Regel den VPCs zuordnen, die diese DNS-Auflösung benötigen. Wenn Sie die Weiterleitung auf Ihrem Domain-Controller-DNS-Service an den standardmäßigen Route-53-DNS-Resolver Ihrer VPC konfiguriert haben, wie im vorherigen Absatz beschrieben, finden Sie den DNS-Auflösungsprozess im Abschnitt Auflösen von DNS-Abfragen zwischen VPCs und in Ihrem Netzwerkhandbuch für Amazon Route 53-Entwicklerhandbuch.

Wenn Sie den standardmäßigen DHCP-Optionssatz verwenden und andere Hosts in Ihren VPCs, die nicht Teil Ihrer Active-Directory-Domain sind, in der Lage sein müssen, Hostnamen in Ihrem Active-Directory-Namespace aufzulösen, können Sie diesen ausgehenden Route-53-Resolver-Endpunkt verwenden und eine weitere Route-53-Weiterleitungsregel hinzufügen, die DNS-Abfragen für Ihre Active-Directory-Domain an Ihre Active-Directory-DNS-Server weiterleitet. Diese Route-53-Weiterleitungsregel muss dem ausgehenden Route-53-Resolver-Endpunkt zugeordnet sein, der Ihren Active-Directory-DNS-Service erreichen kann, sowie allen VPCs, die Sie aktivieren möchten, um DNS-Datensätze in Ihrer WorkSpaces Active-Directory-Domain aufzulösen.

Ebenso kann ein Route 53 Resolver Inbound Endpoint verwendet werden, um die DNS-Auflösung von DNS-Datensätzen Ihrer WorkSpaces Active-Directory-Domain aus Ihrem On-Premises-Netzwerk zu ermöglichen.



Beispiel für eine Auflösung in Abbildung 2: WorkSpaces DNS mit Route-53-Endpunkten

- Ihr Amazon WorkSpaces verwendet den AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)-DNS-Service für die DNS-Auflösung. Der AWS Managed Microsoft AD DNS-Service löst die `example.aws` Domain auf und leitet alle anderen DNS-Abfragen an den standardmäßigen Route 53 DNS Resolver an die VPC-CIDR-Basis-IP-Adresse +2 weiter, um die DNS-Auflösung zu aktivieren

  Die Shared Services VPC enthält einen Route 53 Outbound Resolver-Endpunkt, der zwei Route 53-Weiterleitungsregeln zugeordnet ist. Eine dieser Regeln leitet DNS-Abfragen für die `example.com` Domain an die On-Premises-DNS-Server weiter. Die zweite Regel leitet DNS-Abfragen für Ihre AWS Managed Microsoft AD Domain `example.aws` an Ihren Active-Directory-DNS-Service in der VPC für freigegebene Services weiter.

  Mit dieser Architektur WorkSpaces kann Ihr Amazon DNS-Abfragen für Folgendes auflösen:

  - Ihre AWS Managed Microsoft AD Domain `example.aws`.

  - EC2-Instances in der Domäne, die mit Ihrem standardmäßigen DHCP-Optionssatz (z. B. `host1.eu-west-1.compute.internal`) konfiguriert sind, sowie andere AWS Services oder Endpunkte.
  - Hosts und Services in Ihrer On-Premises-Domain, z. B. `host3.example.com`.
- • Die anderen EC2-Workloads in der Shared Services VPC (`host1.eu-west-1.compute.internal`) und in der WorkSpaces VPC (`host2.eu-west-1.compute.internal`) können die gleichen DNS-Auflösungen wie Ihr haben WorkSpaces, solange die Route 53-Weiterleitungsregeln beiden VPCs zugeordnet sind. Die DNS-Auflösung für die `example.aws` Domain wird in diesem Fall über den standardmäßigen Route 53 DNS Resolver an der VPC-CIDR-Basis-IP-Adresse +2 geleitet, die sie gemäß den konfigurierten und zugehörigen Route 53-Weiterleitungsregeln über den ausgehenden Route 53 Resolver-Endpunkt an den WorkSpaces Active Directory-DNS-Service weiterleitet.
- • Schließlich kann ein On-Premises-Client auch dieselbe DNS-Auflösung durchführen, da der On-Premises-DNS-Server mit bedingten Weiterleitungen für die `eu-west-1.compute.internal` Domains `example.aws` und konfiguriert ist und DNS-Abfragen für diese Domains an die eingehenden Endpunkt-IP-Adressen des Route 53 Resolvers weiterleitet.

Beispiel für eine typische Konfiguration

Betrachten wir ein Szenario, in dem Sie zwei Arten von Benutzern haben und Ihr AWS Directory Service ein zentralisiertes AD für die Benutzerauthentifizierung verwendet:

- Mitarbeiter, die vollen Zugriff von überall aus benötigen (z. B. Mitarbeiter in Vollzeit) – Diese Benutzer haben vollen Zugriff auf das Internet und das interne Netzwerk und werden durch eine Firewall von der VPC an das On-Premises-Netzwerk weitergeleitet.
- Auftragnehmer, die nur eingeschränkten Zugriff innerhalb des Unternehmensnetzwerks haben sollten (z. B. Auftragnehmer und Berater) – Diese Benutzer haben eingeschränkten Internetzugang über einen Proxyserver auf bestimmte Websites in der VPC und eingeschränkten Netzwerkzugriff in der VPC und auf das On-Premises-Netzwerk.

Sie möchten Mitarbeitern in Echtzeit die Möglichkeit geben, auf ihrem lokalen Administratorzugriff WorkSpace zur Installation von Software zu haben, und Sie möchten die Zwei-Faktor-Authentifizierung mit MFA erzwingen. Außerdem möchten Sie den Mitarbeitern in Echtzeit den Zugriff auf das Internet ermöglichen, ohne Einschränkungen durch ihre WorkSpace.

Bei Auftragnehmern möchten Sie den lokalen Administratorzugriff blockieren, damit sie nur bestimmte vorinstallierte Anwendungen verwenden können. Sie möchten restriktive Netzwerkzugriffskontrollen mithilfe von Sicherheitsgruppen für diese anwenden WorkSpaces. Sie müssen die Ports 80 und 443 nur für bestimmte interne Websites öffnen und ihren Zugriff auf das Internet vollständig blockieren.

In diesem Szenario gibt es zwei völlig unterschiedliche Arten von Benutzern mit unterschiedlichen Anforderungen für den Netzwerk- und Desktopzugriff. Es ist eine bewährte Methode, ihre WorkSpaces unterschiedlich zu verwalten und zu konfigurieren. Sie müssen zwei AD Connectors erstellen, einen für jede Benutzerpersona. Jeder AD Connector benötigt zwei Subnetze, die über genügend IP-Adressen verfügen, um Ihre WorkSpaces Schätzungen des Nutzungswachstums zu erfüllen.

> **Note**
>
> Jedes AWS VPC-Subnetz verbraucht zu Verwaltungszwecken fünf IP-Adressen (die ersten vier und die letzte IP-Adresse) und jeder AD Connector verbraucht eine IP-Adresse in jedem Subnetz, in dem er bestehen bleibt.

Weitere Überlegungen zu diesem Szenario sind:

- AWS VPC-Subnetze sollten private Subnetze sein, damit der Datenverkehr, z. B. der Internetzugang, entweder über ein NAT-Gateway (Network Address Translation), einen Proxy-NAT-Server in der Cloud gesteuert oder über Ihr On-Premises-Datenverkehrsmanagementsystem zurückgeleitet werden kann.
- Für den gesamten VPC-Datenverkehr, der für das On-Premises-Netzwerk bestimmt ist, ist eine Firewall vorhanden.
- Microsoft-AD-Server und die MFA-RADIUS-Server sind entweder On-Premises (siehe Szenario 1: Verwenden von AD Connector zur Proxy-Authentifizierung an On-Premises-AD-DS in diesem Dokument) oder Teil der AWS Cloud-Implementierung (siehe Szenario 2 und Szenario 3, AD-DS-Bereitstellungsszenarien in diesem Dokument).

Da allen eine Form des Internetzugangs gewährt WorkSpaces wird und sie in einem privaten Subnetz gehostet werden, müssen Sie auch öffentliche Subnetze erstellen, die über ein Internet-Gateway auf das Internet zugreifen können. Sie benötigen ein NAT-Gateway für die Mitarbeiter, das ihnen den Zugriff auf das Internet ermöglicht, und einen Proxy-NAT-Server für die Berater und Auftragnehmer, um ihren Zugriff auf bestimmte interne Websites zu beschränken. Um Ausfälle zu

planen, Hochverfügbarkeit zu entwerfen und die Gebühren für den AZ-übergreifenden Datenverkehr zu begrenzen, sollten Sie zwei NAT-Gateways und NAT- oder Proxy-Server in zwei verschiedenen Subnetzen in einer Multi-AZ-Bereitstellung haben. Die beiden AZs, die Sie als öffentliche Subnetze auswählen, stimmen mit den beiden AZs überein, die Sie für Ihre WorkSpaces Subnetze in Regionen mit mehr als zwei Zonen verwenden. Sie können den gesamten Datenverkehr von jeder WorkSpaces AZ an das entsprechende öffentliche Subnetz weiterleiten, um die AZ-übergreifenden Datenverkehrsgebühren zu begrenzen und eine einfachere Verwaltung zu ermöglichen. Die folgende Abbildung zeigt die VPC-Konfiguration.

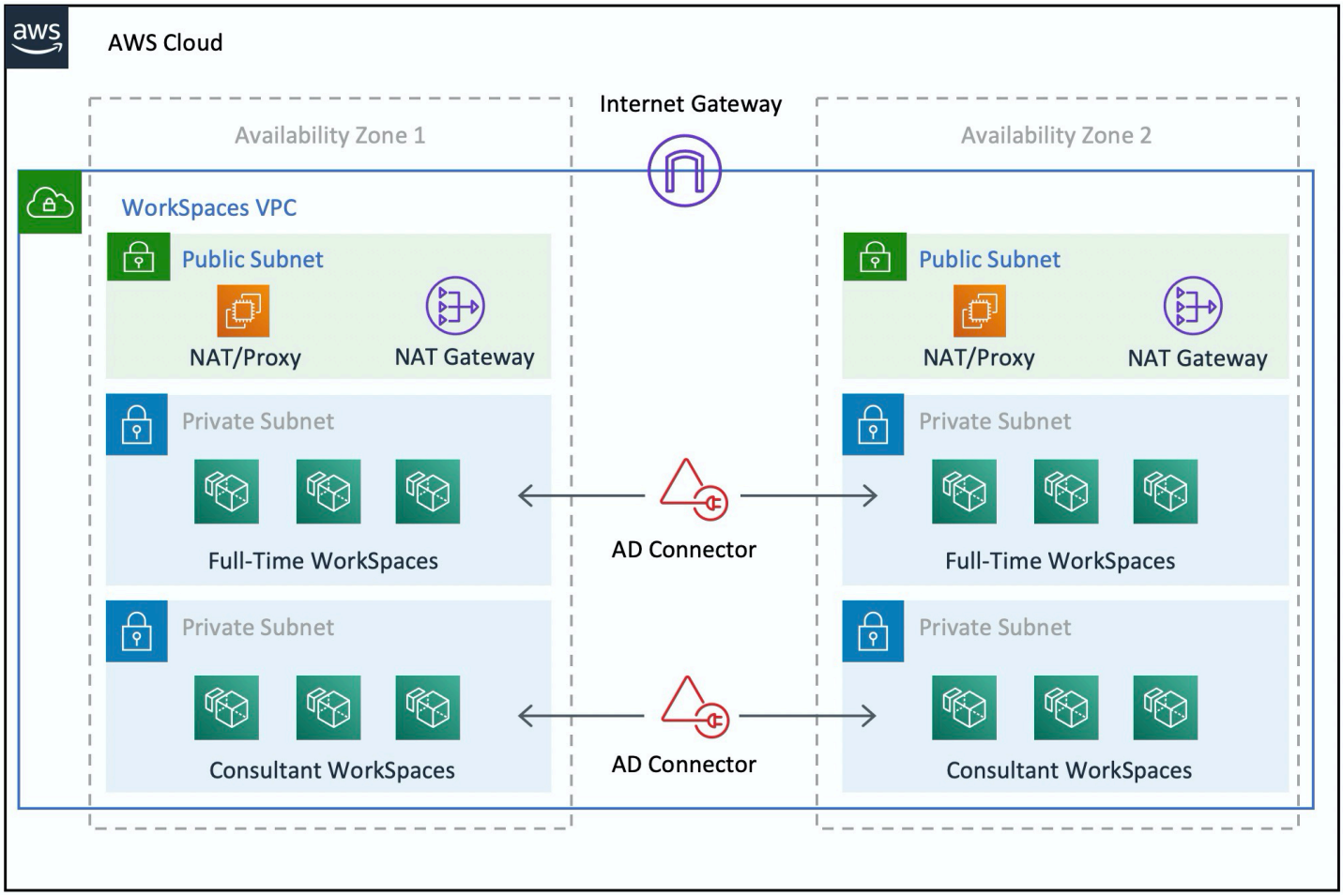


Abbildung 3: High-Level-VPC-Design

In den folgenden Informationen wird beschrieben, wie Sie die beiden verschiedenen WorkSpaces Typen konfigurieren:

So konfigurieren Sie WorkSpaces für Vollzeit-Mitarbeiter:

1. Wählen Sie in der Amazon WorkSpaces -Managementkonsole in der Menüleiste die Option Verzeichnisse aus.

2. Wählen Sie das Verzeichnis aus, in dem sich Ihre Mitarbeiter befinden.
3. Wählen Sie Local Administrator Setting aus.

Wenn Sie diese Option aktivieren, WorkSpace verfügen alle neu erstellten über lokale Administratorrechte. Um Internetzugang zu gewähren, konfigurieren Sie NAT für ausgehenden Internetzugang von Ihrer VPC aus. Um MFA zu aktivieren, müssen Sie einen RADIUS-Server, Server-IPs, Ports und einen vorinstallierten Schlüssel angeben.

Im Fall von Arbeitskräften WorkSpace kann WorkSpacesder eingehende Datenverkehr zum auf das Remote Desktop Protocol (RDP) aus dem Helpdesk-Subnetz beschränkt werden, indem eine Standardsicherheitsgruppe über die AD-Connector-Einstellungen angewendet wird.

So konfigurieren Sie WorkSpaces für Auftragnehmer und Berater:

1. Deaktivieren Sie in der Amazon- WorkSpaces Managementkonsole Internet Access und die Einstellung Lokaler Administrator.
2. Fügen Sie im Abschnitt Sicherheitsgruppeneinstellungen eine Sicherheitsgruppe hinzu, um eine Sicherheitsgruppe für alle neuen WorkSpaces zu erzwingen, die unter diesem Verzeichnis erstellt wurden.

Beschränken Sie für Berater den ausgehenden und eingehenden Datenverkehr auf WorkSpaces, WorkSpaces indem Sie eine Standardsicherheitsgruppe über die AD-Connector-Einstellungen auf alle anwenden, die dem AD Connector WorkSpaces zugeordnet sind. Die Sicherheitsgruppe verhindert ausgehenden Zugriff vom WorkSpaces auf alles andere als HTTP- und HTTPS-Datenverkehr sowie eingehenden Datenverkehr zum RDP vom Helpdesk-Subnetz im On-Premises-Netzwerk.

> **Note**
>
> Die Sicherheitsgruppe gilt nur für die ENI, die sich in der VPC befindet (`eth1` auf der WorkSpace), und der Zugriff auf die WorkSpace vom WorkSpaces Client aus ist aufgrund einer Sicherheitsgruppe nicht eingeschränkt. Die folgende Abbildung zeigt das endgültige WorkSpaces VPC-Design.

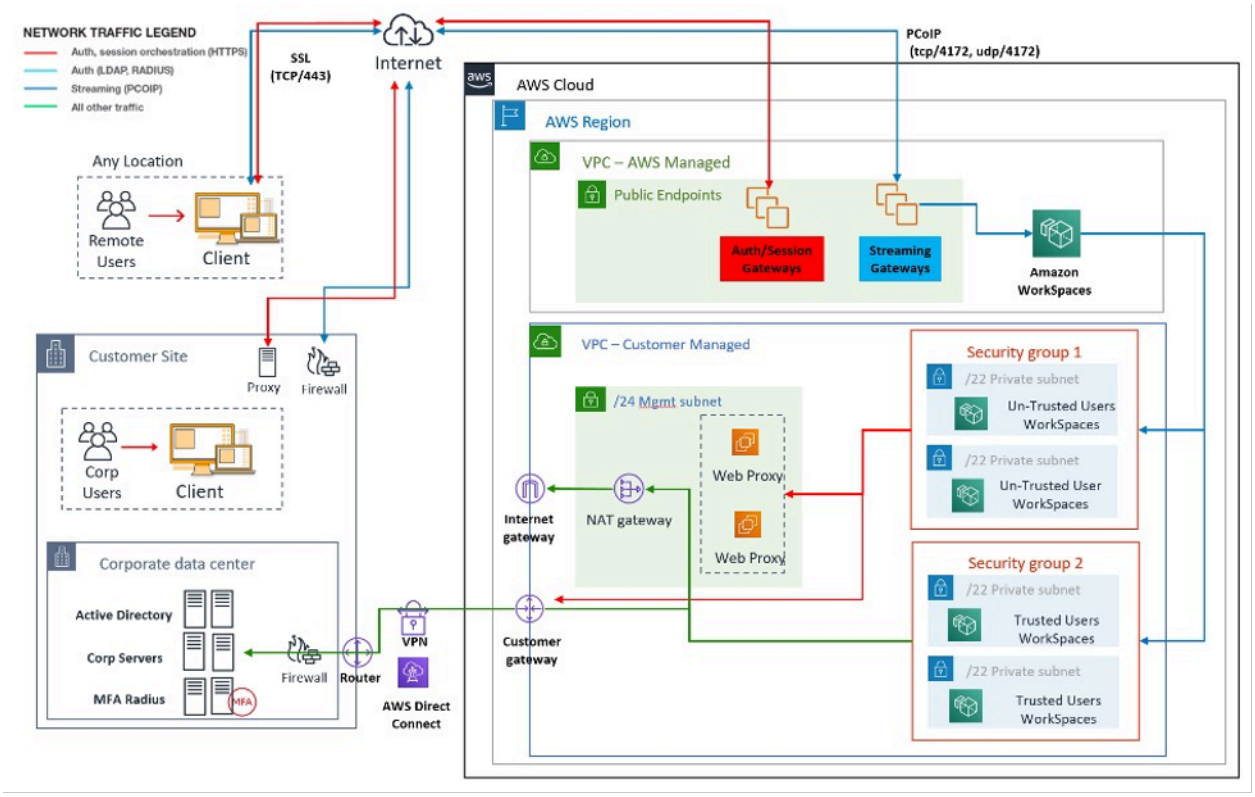


Abbildung 4: WorkSpaces Entwurf mit Benutzerpersonas

AWS Directory Service

Wie in der Einführung erwähnt, AWS istDirectory Service eine Kernkomponente von Amazon WorkSpaces. Mit AWS Directory Service können Sie drei Arten von Verzeichnissen mit Amazon erstellen WorkSpaces:

- AWS Managed Microsoft AD ist ein verwaltetes Microsoft AD, das von Windows Server 2012 R2 unterstützt wird. AWS Managed Microsoft AD ist in der Standard- oder Enterprise Edition verfügbar.
- Simple AD ist ein eigenständiger, Microsoft-AD-kompatibler, verwalteter Verzeichnisservice, der von Samba 4 unterstützt wird.
- AD Connector ist ein Verzeichnis-Proxy zum Umleiten von Authentifizierungsanforderungen und Benutzer- oder Gruppen-Lookups an Ihr vorhandenes On-Premises-Microsoft-AD.

Im folgenden Abschnitt werden Kommunikationsabläufe für die Authentifizierung zwischen dem Amazon WorkSpaces Brokerage Service und AWS Directory Service, bewährte Methoden für die Implementierung WorkSpaces mit AWS Directory Service und erweiterte Konzepte wie MFA beschrieben. Außerdem werden Konzepte der Infrastrukturarchitektur für Amazon WorkSpaces in

großem Umfang, Anforderungen an Amazon VPC und AWS Directory Service erörtert, einschließlich der Integration mit lokalen Microsoft AD Domain Services (AD DS).

AD-DS-Bereitstellungsszenarien

Das Sichern von Amazon WorkSpaces ist der AWS Directory Service, und das richtige Design und die richtige Bereitstellung des Verzeichnisservices ist von entscheidender Bedeutung. Die folgenden sechs Szenarien bauen auf den Active Directory Domain Services im AWS Schnellstarthandbuch auf und beschreiben die bewährten Bereitstellungsoptionen für AD DS bei Verwendung mit Amazon WorkSpaces. Im Abschnitt Überlegungen zum Entwurf dieses Dokuments werden die spezifischen Anforderungen und bewährten Methoden für die Verwendung von AD Connector für beschrieben WorkSpaces, was ein integraler Bestandteil des gesamten WorkSpaces Entwurfskonzepts ist.

- Szenario 1: Verwenden von AD Connector zur Proxy-Authentifizierung an On-Premises-AD-DS – In diesem Szenario ist die Netzwerkkonnektivität (VPN/Direct Connect) für den Kunden vorhanden, wobei die gesamte Authentifizierung über AWS Directory Service (AD Connector) an den On-Premises-AD-DS des Kunden weitergeleitet wird.
- Szenario 2: Erweitern von On-Premises-AD-DS in AWS (Replikat) – Dieses Szenario ähnelt Szenario 1, aber hier wird ein Replikat des Kunden-AD-DS AWS in Kombination mit AD Connector bereitgestellt, wodurch die Latenz von Authentifizierungs-/Abfrageanforderungen an AD DS und den globalen AD-DS-Katalog reduziert wird.
- Szenario 3: Eigenständige isolierte Bereitstellung mit AWS Directory Service in der AWS Cloud – Dies ist ein isoliertes Szenario und beinhaltet keine Konnektivität zum Kunden zur Authentifizierung. Dieser Ansatz verwendet AWS Directory Service (Microsoft AD) und AD Connector. Obwohl dieses Szenario für die Authentifizierung nicht auf die Konnektivität mit dem Kunden angewiesen ist, wird bei Bedarf Anwendungsdatenverkehr über VPN oder Direct Connect bereitgestellt.
- Szenario 4: AWS Microsoft AD und eine bidirektionale transitive Vertrauensstellung zu On-Premises – Dieses Szenario umfasst den AWS Managed Microsoft AD Service (MAD) mit einer bidirektionalen transitiven Vertrauensstellung zum On-Premises Microsoft AD Forest.
- Szenario 5: AWS Microsoft AD unter Verwendung einer Shared-Services-VPC – In diesem Szenario wird AWS Managed Microsoft AD in einer Shared-Services-VPC verwendet, um als Identitätsdomäne für mehrere AWS Services (Amazon EC2, Amazon usw.) verwendet zu werden, während der AD Connector verwendet wird WorkSpaces, um LDAP-Benutzerauthentifizierungsanforderungen (Lightweight Directory Access Protocol) an die AD-Domain-Controller weiterzuleiten.

- Szenario 6: AWS Microsoft AD, Shared Services VPC und One-Way Trust to On-Premises AD – Dieses Szenario ähnelt Szenario 5, umfasst jedoch unterschiedliche Identitäts- und Ressourcendomänen, die eine unidirektionale Vertrauensstellung zu On-Premises verwenden.

Sie müssen bei der Auswahl Ihres Bereitstellungsszenarios für Active Directory Domain Services (ADDS) mehrere Überlegungen berücksichtigen. In diesem Abschnitt wird die Rolle von AD Connector mit Amazon erläutert WorkSpacesund einige wichtige Überlegungen bei der Auswahl eines ADDS-Bereitstellungsszenarios behandelt. Weitere Hinweise zum Entwurf und zur Planung von ADDS in finden AWSSie im Active Directory Domain Services on AWS Design and Planning Guide.

Die Rolle des AWS AD Connectors mit Amazon WorkSpaces

Der AWS AD Connector ist ein - AWS Directory-Service, der als Proxy-Service für ein Active Directory fungiert. Es speichert oder speichert keine Benutzeranmeldeinformationen, sondern leitet Authentifizierungs- oder Suchanfragen an Ihr Active Directory weiter – On-Premises oder auf AWS. Sofern Sie nicht verwenden AWS Managed Microsoft AD, ist dies auch die einzige Möglichkeit, Ihr Active Directory (On-Premises oder erweitert auf AWS) für die Verwendung mit Amazon WorkSpaces () zu registrierenWorkSpaces.

Ein AD Connector kann auf Ihr On-Premises-Active-Directory, auf ein Active Directory verweisen, das auf AWS (AD-Domain-Controller auf Amazon EC2) erweitert wurde, oder auf ein AWS Managed Microsoft AD.

Der AD Connector spielt eine wichtige Rolle, wobei die meisten Bereitstellungsszenarien in den folgenden Abschnitten behandelt werden. Die Verwendung des AD Connectors mit WorkSpaces bietet eine Reihe von Vorteilen:

- Wenn es auf Ihr Unternehmens-Active-Directory verweist, können sich Ihre Benutzer mit ihren vorhandenen Unternehmensanmeldeinformationen bei WorkSpaces und anderen -Services wie Amazon WorkDocs anmelden.
- Sie können bestehende Sicherheitsrichtlinien (Passwortablauf, Kontosperren usw.) konsistent anwenden, unabhängig davon, ob Ihre Benutzer auf Ressourcen in Ihrer On-Premises-Infrastruktur oder in der zugreifen AWS Cloud, z. B. WorkSpaces.
- Der AD Connector ermöglicht eine einfache Integration mit Ihrer vorhandenen RADIUS-basierten MFA-Infrastruktur, um eine zusätzliche Sicherheitsebene zu bieten.
- Es ermöglicht die Trennung Ihrer Benutzer. Sie ermöglicht beispielsweise die Konfiguration einer Reihe von WorkSpaces Optionen pro Geschäftseinheit oder Persona, da mehrere AD Connectors

zur Benutzerauthentifizierung auf dieselben Domain Controller (DNS-Server) von Active Directory verweisen können:

- Zieldomäne oder Organisationseinheit für die gezielte Anwendung von Active-Directory-Gruppenrichtlinienobjekten (GPOs)
- Verschiedene Sicherheitsgruppen zur Steuerung des Datenverkehrsflusses zu/von WorkSpaces
- Verschiedene Zugriffskontrolloptionen (zulässige Client-Geräte) und IP-Zugriffskontrollgruppen (Zugriff auf IP-Bereiche beschränken)
- Selektive Aktivierung von lokalen Administratorberechtigungen
- Verschiedene Self-Service-Berechtigungen
- Selektive Durchsetzung der Multi-Factor Authentication (MFA)
- Platzierung Ihrer WorkSpaces Elastic Network Interfaces (ENI) in verschiedenen VPCs oder Subnetzen zur Isolierung

Mehrere AD Connectors ermöglichen es auch, eine größere Anzahl von Benutzern zu unterstützen, wenn Sie die Leistungsgrenze eines einzelnen kleinen oder großen AD Connectors erreichen. Weitere Informationen finden Sie im Größe von AWS Managed Microsoft AD Abschnitt .

Die Verwendung von AD Connectors mit WorkSpaces ist kostenlos, sofern Sie mindestens einen aktiven WorkSpaces Benutzer in einem kleinen AD Connector und mindestens 100 aktive WorkSpaces Benutzer in einem großen AD Connector haben. Weitere Informationen finden Sie auf der Seite AWS Directory Services – Preise.

Die Bedeutung Ihrer Netzwerkverbindung zu AWS mit einem On-Premises-Active-Directory

WorkSpaces stützt sich auf die Konnektivität zu Ihrem Active Directory. Daher ist die Verfügbarkeit der Netzwerkverbindung zu Ihrem Active Directory von entscheidender Bedeutung. Wenn Ihre Netzwerkverbindung in Szenario 1 beispielsweise ausgefallen ist, können sich Ihre Benutzer nicht authentifizieren und können daher ihre nicht verwenden WorkSpaces.

Wenn ein On-Premises-Active-Directory als Teil des Szenarios verwendet werden soll, müssen Sie Ausfallsicherheit, Latenz und Datenverkehrskosten Ihrer Netzwerkverbindung zu berücksichtigen AWS. Bei einer WorkSpaces Bereitstellung in mehreren Regionen kann dies mehrere Netzwerkverbindungen in verschiedenen AWS Regionen umfassen oder mehrere AWS Transit Gatewayen mit Peering zwischen ihnen, um Ihren AD-Datenverkehr an die VPC mit Konnektivität zu Ihrem On-Premises-AD weiterzuleiten. Diese Überlegungen zu Netzwerkverbindungen gelten für

die meisten in den folgenden Abschnitten beschriebenen Szenarien, sind aber besonders wichtig für Szenarien, in denen Ihr AD-Datenverkehr von AD Connectors und die Netzwerkverbindung durchlaufen WorkSpaces muss, um Ihr On-Premises-Active-Directory zu erreichen. Szenario 1 hebt einige der Einschränkungen hervor.

Verwenden der Multi-Faktor-Authentifizierung mit WorkSpaces

Wenn Sie die Multi-Factor Authentication (MFA) mit verwenden möchten WorkSpaces, müssen Sie einen AWS AD Connector oder einen verwenden AWS Managed Microsoft AD, da nur diese Services die Registrierung des Verzeichnisses für die Verwendung mit WorkSpaces und Konfiguration von RADIUS zulassen. Für die Platzierung Ihrer RADIUS-Server gelten die im Die Bedeutung Ihrer Netzwerkverbindung zu AWS mit einem On-Premises-Active-Directory Abschnitt beschriebenen Überlegungen zur Netzwerkverbindung.

Trennen von Konto und Ressourcendomäne

Aus Sicherheitsgründen oder aus Gründen der besseren Verwaltbarkeit kann es sinnvoll sein, die Kontodomäne von der Ressourcendomäne zu trennen. Platzieren Sie beispielsweise die WorkSpaces Computerobjekte in einer separaten Ressourcendomäne, während die Benutzer Teil der Kontodomäne sind. Eine Implementierung wie diese kann verwendet werden, um einer Partnerorganisation zu ermöglichen, mithilfe WorkSpaces von AD-Gruppenrichtlinien in der Ressourcen-Domain zu verwalten, ohne die Kontrolle zu entziehen oder Zugriff auf die Konto-Domain zu gewähren. Dies kann durch die Verwendung von zwei Active Directories mit einer konfigurierten Active Directory Trust erreicht werden. In den folgenden Abschnitten wird dies ausführlicher behandelt:

- Szenario 4: AWS Microsoft AD und eine bidirektionale transitive Vertrauensstellung zu On-Premises
- Szenario 6: AWS Microsoft AD, VPC für gemeinsam genutzte Services und eine unidirektionale Vertrauensstellung zu On-Premises

Große Active-Directory-Bereitstellungen

Sie müssen sicherstellen, dass Active-Directory-Standorte und -Services entsprechend konfiguriert sind. Dies ist besonders wichtig, wenn Ihr Active Directory aus einer großen Anzahl von Domain-Controllern an verschiedenen geografischen Standorten besteht. Ihr Windows WorkSpaces verwendet den standardmäßigen Microsoft-Mechanismus, um ihren Domain-Controller für die

Active-Directory-Website zu ermitteln, der sie zugewiesen sind. Dieser DC Locator-Prozess basiert auf DNS und kann erheblich verlängert werden, falls in der Anfangsphase des DC Locator-Prozesses eine langwierige Liste von Domain-Controllern mit unspezifischer Priorität und Gewichtung zurückgegeben wird. Wenn Ihr an einen suboptimalen Domain-Controller „angeheftet“ WorkSpaces wird, kann die gesamte nachfolgende Kommunikation mit diesem Domain-Controller unter Umständen an einer erhöhten Netzwerklatenz und einer geringeren Bandbreite leidet, wenn Netzwerkverbindungen über große Bereiche übertragen werden. Dies verlangsamt jede Kommunikation mit dem Domain-Controller, einschließlich der Verarbeitung einer potenziell großen Anzahl von Gruppenrichtlinienobjekten (GPOs) und Dateiübertragungen vom Domain-Controller. Abhängig von der Netzwerktopologie können sich auch Ihre Netzwerkkosten erhöhen, da die zwischen WorkSpaces und Domain-Controllern ausgetauschten Daten möglicherweise unnötigerweise einen kostengünstigeren Netzwerkpfad durchlaufen. In den Überlegungen zum Design Abschnitten VPC-Design und finden Sie Anleitungen zu DHCP und DNS mit Ihrem VPC-Design sowie Active Directory-Standorte und -Services.

Verwenden von Microsoft Azure Active Directory oder Active Directory Domain Services mit WorkSpaces

Wenn Sie Microsoft Azure Active Directory mit verwenden möchten WorkSpaces, können Sie Azure AD Connect verwenden, um Ihre Identität mit Ihrem lokalen Active Directory oder mit Ihrem Active Directory in AWS (Domain Controller auf Amazon EC2 oder) zu synchronisieren AWS Managed Microsoft AD. Auf diese Weise können Sie jedoch nicht WorkSpaces mit Ihrem Azure Active Directory verbunden werden. Weitere Informationen finden Sie in der Microsoft Hybrid Identity-Dokumentation in der Microsoft Azure-Dokumentation.

Wenn Sie Ihr WorkSpaces mit Ihrem Azure Active Directory verbinden möchten, müssen Sie Microsoft Azure Active Directory Domain Services (Azure AD DS) bereitstellen, Konnektivität zwischen AWS und Azure herstellen und einen AWS AD Connector verwenden, der auf Ihre Azure AD DS Domain Controller verweist. Weitere Informationen zur Einrichtung finden Sie im Blogbeitrag Hinzufügen Ihrer WorkSpaces zu Azure AD mithilfe von Azure Active Directory Domain Services.

Wenn Sie AWS Directory Services mit verwenden WorkSpaces, müssen Sie die Größe Ihrer WorkSpaces Bereitstellung und das erwartete Wachstum berücksichtigen, um die AWS Directory Service angemessen zu dimensionieren. Dieser Abschnitt enthält Anleitungen zur Dimensionierung der AWS Directory Service für die Verwendung mit WorkSpaces. Wir empfehlen Ihnen auch, die Abschnitte Bewährte Methoden für AD Connector und Bewährte Methoden für AWS Managed Microsoft AD im AWS Directory Service -Administratorhandbuch zu lesen.

Größe von AD Connector mit WorkSpaces

Der Active Directory Connector (AD Connector) ist in zwei Größen verfügbar: Small und Large. Obwohl es keine erzwungenen Benutzer- oder Verbindungslimits gibt, empfehlen wir, einen kleinen AD Connector für bis zu 500 WorkSpaces berechtigte Benutzer und einen großen AD Connector für bis zu 5000 WorkSpaces berechtigte Benutzer zu verwenden. Sie können Anwendungslasten auf mehrere AD Connector verteilen, um sie an Ihre Leistungsanforderungen anzupassen. Wenn Sie beispielsweise 1 500 WorkSpaces Benutzer unterstützen müssen, können Sie Ihre WorkSpaces gleichmäßig auf drei kleine AD Connector verteilen, die jeweils 500 Benutzer unterstützen. Wenn sich alle Ihre Benutzer in derselben Domain befinden, kann AD Connector alle auf denselben Satz von DNS-Servern verweisen, die Ihre Active-Directory-Domain auflösen.

Beachten Sie, dass Sie, wenn Sie mit einem kleinen AD Connector begonnen haben und Ihre WorkSpaces Bereitstellung im Laufe der Zeit wächst, ein Supportticket ausstellen können, damit sich die Größe Ihres AD Connectors von klein zu groß ändert, um die größere Anzahl WorkSpaces berechtigter Benutzer zu bewältigen.

Größe von AWS Managed Microsoft AD

AWS Managed Microsoft AD Mit können Sie Microsoft Active Directory als verwalteten Service ausführen. Sie können beim Starten des Services zwischen Standard Edition und Enterprise Edition wählen. Die Standard Edition wird für kleine und mittelgroße Unternehmen mit bis zu 5 000 Benutzern empfohlen und unterstützt bis zu 30 000 Verzeichnisobjekte wie Benutzer, Gruppen und Computer. Die Enterprise Edition wurde für die Unterstützung von bis zu 500.000 Verzeichnisobjekten entwickelt und bietet auch ein zusätzliches Feature, z. B. die Multi-Region-Replikation .

Wenn Sie mehr als 500.000 Verzeichnisobjekte unterstützen müssen, sollten Sie die Bereitstellung von Domain-Controllern für Microsoft Active Directory auf Amazon EC2 in Betracht ziehen. Die Größe dieser Domain-Controller finden Sie im Dokument Kapazitätsplanung für Active Directory Domain Services von Microsoft.

Szenario 1: Verwenden des AD-Konnektors zur Proxy-Authentifizierung an den On-Premises-Active-Directory-Service

Dieses Szenario richtet sich an Kunden, die ihren On-Premises-AD-Service nicht auf erweitern möchten AWSoder bei denen eine neue Bereitstellung von AD DS keine Option ist. Die folgende Abbildung zeigt auf hoher Ebene, jede der Komponenten und den Ablauf der Benutzerauthentifizierung.

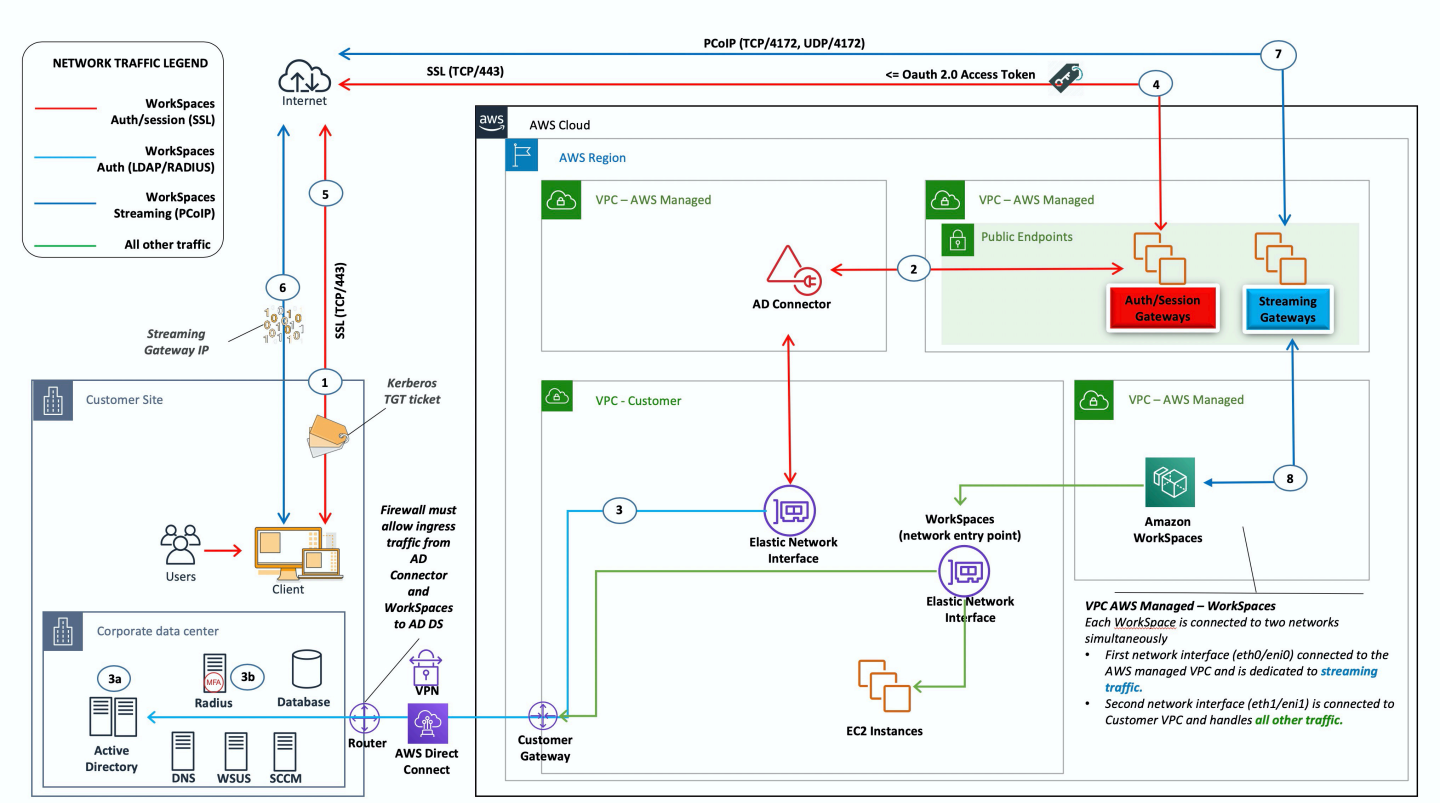


Abbildung 5: AD Connector zu On-Premises Active Directory

In diesem Szenario wird AWS der -Directory-Service (AD Connector) für alle Benutzer- oder MFA-Authentifizierungen verwendet, die über den AD Connector an den On-Premises-AD-DS des Kunden weitergeleitet werden (siehe folgende Abbildung). Einzelheiten zu den Protokollen oder der Verschlüsselung, die für den Authentifizierungsprozess verwendet werden, finden Sie im Sicherheit Abschnitt dieses Dokuments.

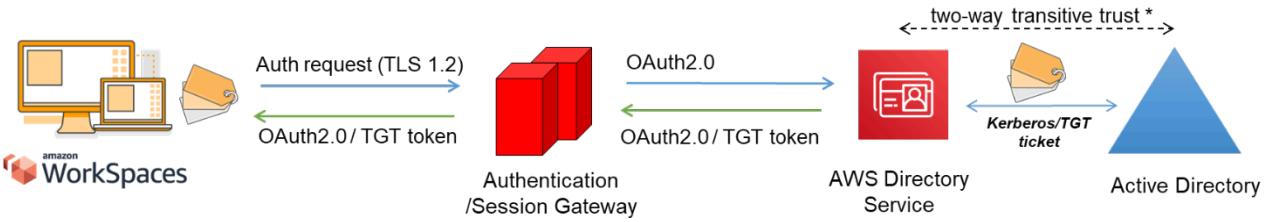


Abbildung 6: Benutzerauthentifizierung über das Authentication Gateway

Szenario 1 zeigt eine Hybridarchitektur, in der der Kunde möglicherweise bereits über Ressourcen in verfügt AWS, sowie über Ressourcen in einem On-Premises-Rechenzentrum, auf das über Amazon zugegriffen werden kann WorkSpaces. Der Kunde kann seine vorhandenen On-Premises-AD-DS- und RADIUS-Server für die Benutzer- und MFA-Authentifizierung nutzen.

Diese Architektur verwendet die folgenden Komponenten oder Konstrukte:

AWS

- Amazon VPC – Erstellen einer Amazon VPC mit mindestens zwei privaten Subnetzen über zwei AZs hinweg.
- DHCP Options Set – Erstellen eines Amazon VPC DHCP Options Set. Auf diese Weise können vom Kunden angegebene Domänennamen und Domänennamenserver (DNS) (On-Premises-Services) definiert werden. Weitere Informationen finden Sie unter DHCP-Optionssätze.
- Amazon Virtual Private Gateway – Aktivieren Sie die Kommunikation mit Ihrem eigenen Netzwerk über einen IPsec-VPN-Tunnel oder eine AWS Direct Connect -Verbindung.
- AWS Directory Service – AD Connector wird in einem Paar privater Amazon-VPC-Subnetze bereitgestellt.
- Amazon WorkSpaces – WorkSpaces werden in denselben privaten Subnetzen wie der AD Connector bereitgestellt. Weitere Informationen finden Sie im Abschnitt Active Directory: Standorte und Services dieses Dokuments.

Customer

- Netzwerkkonnektivität – Unternehmens-VPN- oder Direct-Connect-Endpunkte.
- AD DS – Unternehmens-AD DS.
- MFA (optional) – Unternehmens-RADIUS-Server.
- Endbenutzergeräte – Endbenutzergeräte für Unternehmen oder Bring Your Own License (BYOL), die für den Zugriff auf den Amazon- WorkSpaces Service verwendet werden (wie Windows, Macs, iPads, Android-Tablets, Null-Clients und Chromebooks). Weitere Informationen finden Sie in dieser Liste der Clientanwendungen für unterstützte Geräte und Webbrowser.

Diese Lösung eignet sich zwar hervorragend für Kunden, die AD DS nicht in der Cloud bereitstellen möchten, bietet jedoch einige Einschränkungen:

- Abhängigkeit von der Konnektivität – Wenn die Konnektivität zum Rechenzentrum verloren geht, können sich Benutzer nicht bei ihrem jeweiligen anmelden WorkSpaces, und bestehende Verbindungen bleiben während der Lebensdauer des Kerberos/Ticket-Granting Ticket (TGT) aktiv.

- Latenz – Wenn Latenz über die Verbindung besteht (dies ist bei VPN häufiger als bei Direct Connect der Fall), dauert die WorkSpaces Authentifizierung und alle AD-DS-bezogenen Aktivitäten, wie z. B. die Durchsetzung von Gruppenrichtlinien (GPO), mehr Zeit.
- Datenverkehrskosten – Die gesamte Authentifizierung muss den VPN- oder Direct-Connect-Link durchlaufen und hängt daher vom Verbindungstyp ab. Dies ist entweder die Datenübertragung von Amazon EC2 ins Internet oder die Datenübertragung von außen (Direct Connect).

> **Note**
>
> AD Connector ist ein Proxy-Service. Es speichert oder speichert keine Benutzeranmeldeinformationen. Stattdessen werden alle Authentifizierungs-, Such- und Verwaltungsanfragen von Ihrem AD bearbeitet. In Ihrem Verzeichnisservice ist ein Konto mit Delegierungsrechten erforderlich, das berechtigt ist, alle Benutzerinformationen zu lesen und der Domain einen Computer hinzuzufügen.

Im Allgemeinen hängt die WorkSpaces Erfahrung stark vom Active-Directory-Authentifizierungsprozess ab, der in der vorherigen Abbildung gezeigt wurde. In diesem Szenario hängt die WorkSpaces Authentifizierungserfahrung stark von der Netzwerkverbindung zwischen dem Kunden-AD und der WorkSpaces VPC ab. Der Kunde sollte sicherstellen, dass der Link hochverfügbar ist.

Szenario 2: Erweitern von On-Premises-AD-DS in AWS (Replikat)

Dieses Szenario ähnelt Szenario 1. In diesem Szenario wird jedoch ein Replikat des Kunden AD DS AWS in Kombination mit AD Connector bereitgestellt. Dies reduziert die Latenz von Authentifizierungs- oder Abfrageanforderungen an AD DS, die auf Amazon Elastic Compute Cloud (Amazon EC2) ausgeführt werden. Die folgende Abbildung zeigt eine allgemeine Ansicht der einzelnen Komponenten und des Ablaufs der Benutzerauthentifizierung.

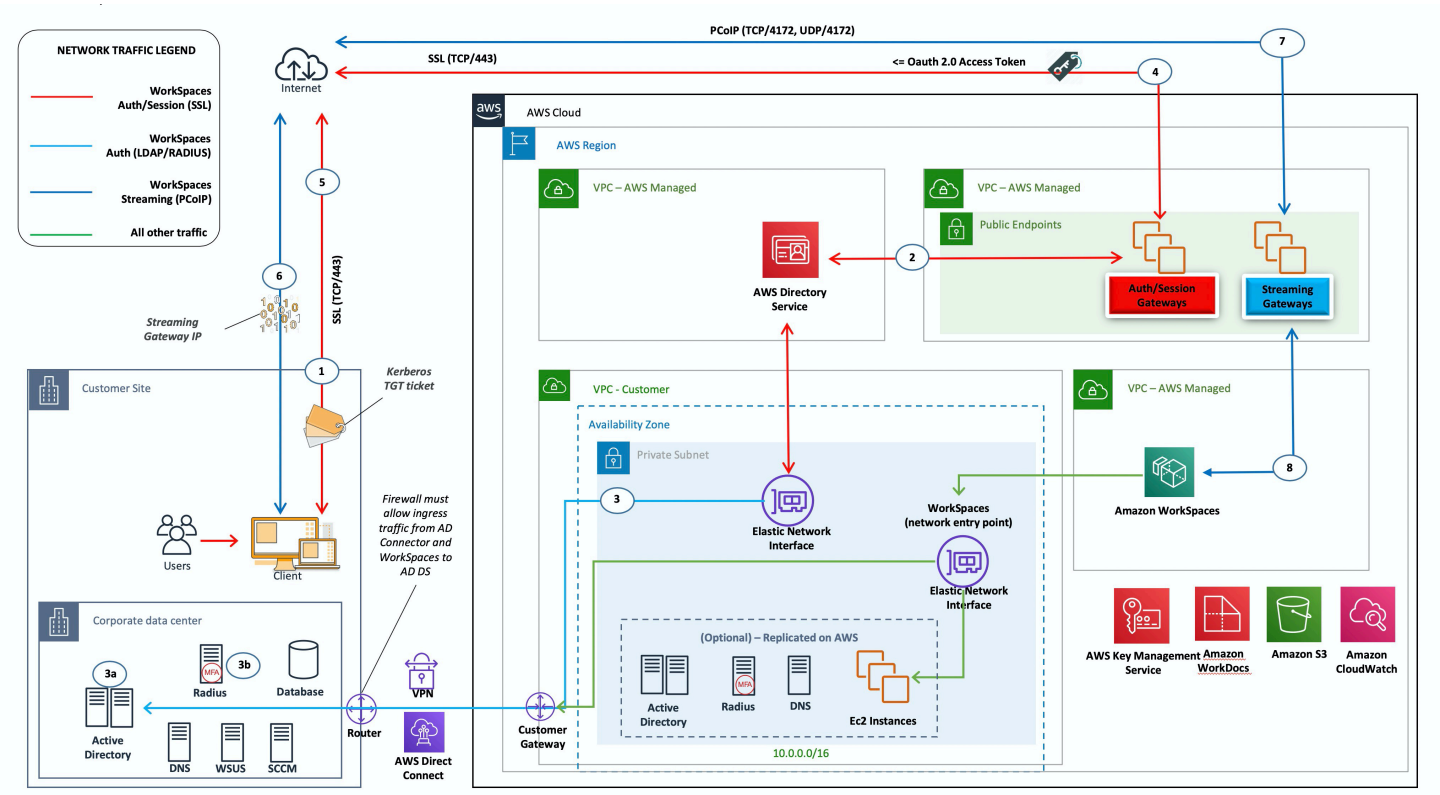


Abbildung 7: Erweitern der Active-Directory-Domäne des Kunden auf die Cloud

Wie in Szenario 1 wird AD Connector für alle Benutzer- oder MFA-Authentifizierungen verwendet, die wiederum an den AD DS des Kunden weitergeleitet werden (siehe vorherige Abbildung). In diesem Szenario wird das Kunden-AD DS in AZs auf Amazon EC2-Instances bereitgestellt, die zu Domain-Controllern in der On-Premises-AD-Gesamtstruktur des Kunden hochgestuft werden und in der - AWS Cloud ausgeführt werden. Jeder Domain-Controller wird in privaten VPC-Subnetzen bereitgestellt, um AD DS in der AWS Cloud hochverfügbar zu machen. Bewährte Methoden für die Bereitstellung von AD DS in AWSfinden Sie im Abschnitt Überlegungen zum Design dieses Dokuments.

Nach der Bereitstellung von WorkSpaces Instances haben sie Zugriff auf die cloudbasierten Domain-Controller für sichere Verzeichnisservices und DNS mit niedriger Latenz. Der gesamte Netzwerkverkehr, einschließlich AD-DS-Kommunikation, Authentifizierungsanforderungen und AD-Replikation, wird entweder innerhalb der privaten Subnetze oder über den Kunden-VPN-Tunnel oder Direct Connect gesichert.

Diese Architektur verwendet die folgenden Komponenten oder Konstrukte:

AWS

- Amazon VPC – Erstellung einer Amazon VPC mit mindestens vier privaten Subnetzen über zwei AZs hinweg – zwei für den Kunden AD DS, zwei für AD Connector oder Amazon WorkSpaces.
- DHCP Options Set – Erstellen eines Amazon VPC DHCP-Optionssatzes. Auf diese Weise kann der Kunde einen bestimmten Domänennamen und DNSs (AD DS Local) definieren. Weitere Informationen finden Sie unter DHCP-Optionssätze.
- Amazon Virtual Private Gateway – Aktivieren Sie die Kommunikation mit einem kundeneigenen Netzwerk über einen IPsec-VPN-Tunnel oder eine - AWS Direct Connect Verbindung.
- Amazon EC2
  - DS-Domain-Controller für Kundenunternehmen, die auf Amazon EC2-Instances in dedizierten privaten VPC-Subnetzen bereitgestellt werden.
  - RADIUS-Server für MFA auf Amazon EC2-Instances in dedizierten privaten VPC-Subnetzen (optional).
- AWS Directory Services – AD Connector wird in einem Paar privater Amazon-VPC-Subnetze bereitgestellt.
- Amazon WorkSpaces – WorkSpaces werden in denselben privaten Subnetzen wie der AD Connector bereitgestellt. Weitere Informationen finden Sie im Abschnitt Active Directory: Sites and Services dieses Dokuments.

Customer

- Netzwerkkonnektivität – Unternehmens-VPN oder - AWS Direct Connect Endpunkte.
- AD DS – Corporate AD DS (erforderlich für die Replikation).
- MFA (optional) – Unternehmens-RADIUS-Server.
- Endbenutzergeräte – Unternehmens- oder BYOL-Endbenutzergeräte (wie Windows, Macs, iPads, Android-Tablets, Null-Clients und Chromebooks), die für den Zugriff auf den Amazon- WorkSpaces Service verwendet werden. Weitere Informationen finden Sie in der Liste der Clientanwendungen für unterstützte Geräte und Webbrowser. Diese Lösung hat nicht die gleichen Einschränkungen wie Szenario 1. Amazon WorkSpaces und AWS Directory Service verlassen sich nicht auf die bestehende Konnektivität.

- Abhängigkeit von der Konnektivität – Wenn die Konnektivität zum Kundenrechenzentrum verloren geht, können Endbenutzer weiterhin arbeiten, da die Authentifizierung und optional eMFA lokal verarbeitet werden.
- Latenz – Mit Ausnahme des Replikationsverkehrs ist die gesamte Authentifizierung lokal und mit geringer Latenz. Weitere Informationen finden Sie im Abschnitt Active Directory: Standorte und Services dieses Dokuments.
- Datenverkehrskosten – In diesem Szenario ist die Authentifizierung lokal, wobei nur die AD-DS-Replikation den VPN- oder Direct-Connect-Link durchqueren muss, wodurch die Datenübertragung reduziert wird.

Im Allgemeinen wird die WorkSpaces Erfahrung verbessert und ist nicht stark von der Konnektivität zu den On-Premises-Domain-Controllern abhängig, wie in der vorherigen Abbildung gezeigt. Dies ist auch der Fall, wenn ein Kunde WorkSpaces auf Tausende von Desktops skalieren möchte, insbesondere im Zusammenhang mit globalen AD-DS-Katalogabfragen, da dieser Datenverkehr für die WorkSpaces Umgebung lokal bleibt.

Szenario 3: Eigenständige isolierte Bereitstellung mit AWS Directory Service in der AWS Cloud

In diesem Szenario, das in der folgenden Abbildung dargestellt ist, wird AD DS in der AWS Cloud in einer eigenständigen isolierten Umgebung bereitgestellt. AWS Directory Service wird ausschließlich in diesem Szenario verwendet. Anstatt AD DS vollständig zu verwalten, können sich Kunden bei Aufgaben wie dem Aufbau einer hochverfügbaren Verzeichnistopologie, der Überwachung von Domain-Controllern und der Konfiguration von Backups und Snapshots auf AWS Directory Service verlassen.

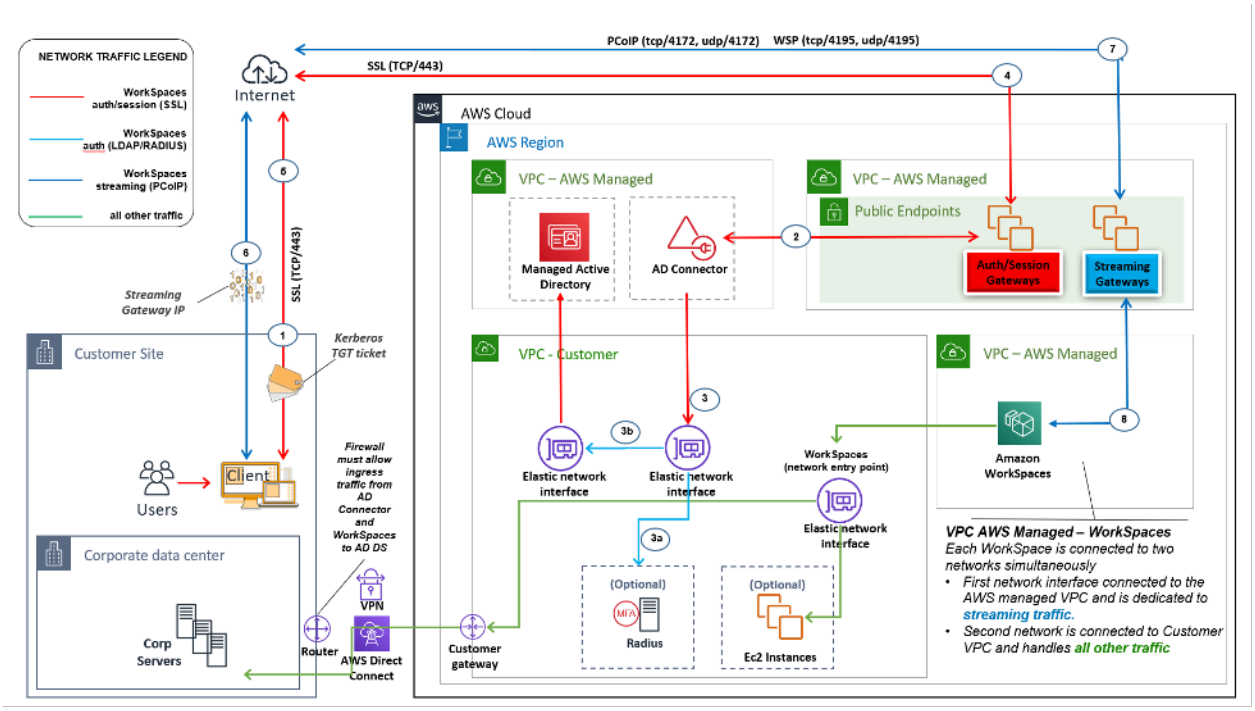


Abbildung 8: Nur Cloud: AWS Directory Services (Microsoft AD)

Wie in Szenario 2 wird AD DS (Microsoft AD) in dedizierten Subnetzen bereitgestellt, die sich über zwei AZs erstrecken, wodurch AD DS in der AWS Cloud hochverfügbar wird. Zusätzlich zu Microsoft AD wird AD Connector (in allen drei Szenarien) für die WorkSpaces Authentifizierung oder MFA bereitgestellt. Dadurch wird sichergestellt, dass Rollen oder Funktionen innerhalb der Amazon VPC getrennt werden. Dies ist eine bewährte Standardmethode. Weitere Informationen finden Sie im Abschnitt Überlegungen zum Design dieses Dokuments.

Szenario 3 ist eine standardmäßige All-In-Konfiguration, die gut für Kunden geeignet ist, die die Bereitstellung, das Patchen, die hohe Verfügbarkeit und die Überwachung des AWS Directory Service AWS verwalten möchten. Das Szenario eignet sich aufgrund seines Isolationsmodus auch gut für den Nachweis von Konzepten, Labor- und Produktionsumgebungen.

Zusätzlich zur Platzierung von AWS Directory Service zeigt diese Abbildung den Fluss des Datenverkehrs von einem Benutzer zu einem Workspace und wie der Workspace mit dem AD-Server und dem MFA-Server interagiert.

Diese Architektur verwendet die folgenden Komponenten oder Konstrukte.

AWS

- Amazon VPC – Erstellen einer Amazon VPC mit mindestens vier privaten Subnetzen in zwei AZs – zwei für AD DS Microsoft AD , zwei für AD Connector oder WorkSpaces.
- DHCP-Optionssatz – Erstellen eines Amazon VPC DHCP-Optionssatzes. Auf diese Weise kann ein Kunde einen bestimmten Domänennamen und DNS (Microsoft AD) definieren. Weitere Informationen finden Sie unter DHCP-Optionssätze.
- Optional: Amazon Virtual Private Gateway – Aktivieren Sie die Kommunikation mit einem kundeneigenen Netzwerk über einen IPsec-VPN-Tunnel (VPN) oder eine - AWS Direct Connect Verbindung. Verwenden Sie für den Zugriff auf On-Premises-Backend-Systeme.
- AWS Directory Service – Microsoft AD wird in einem dedizierten Paar von VPC-Subnetzen (AD DS Managed Service) bereitgestellt.
- Amazon EC2 – Vom Kunden „optionale“ RADIUS-Server für MFA.
- AWS Directory Services – AD Connector wird in einem Paar privater Amazon-VPC-Subnetze bereitgestellt.
- Amazon WorkSpaces – WorkSpaces werden in denselben privaten Subnetzen wie der AD Connector bereitgestellt. Weitere Informationen finden Sie im Abschnitt Active Directory: Sites and Services dieses Dokuments.

Customer

- Optional: Netzwerkkonnektivität – Unternehmens-VPN oder - AWS Direct Connect Endpunkte.
- Endbenutzergeräte – Unternehmens- oder BYOL-Endbenutzergeräte (wie Windows, Macs, iPads, Android-Tablets, Null-Clients und Chromebooks), die für den Zugriff auf den Amazon-WorkSpaces Service verwendet werden. Weitere Informationen finden Sie in dieser Liste der Clientanwendungen für unterstützte Geräte und Webbrowser.

Wie Szenario 2 hat dieses Szenario keine Probleme mit der Abhängigkeit von der Konnektivität zum On-Premises-Rechenzentrum des Kunden, der Latenz oder den Datenübertragungskosten (außer wenn der Internetzugang für WorkSpaces innerhalb der VPC aktiviert ist), da es sich dabei standardmäßig um ein isoliertes oder reines Cloud-Szenario handelt.

Szenario 4: AWS Microsoft AD und eine bidirektionale transitive Vertrauensstellung zu On-Premises

In diesem Szenario, das in der folgenden Abbildung dargestellt ist, wird AWS Managed AD in der AWS Cloud bereitgestellt, die eine bidirektionale transitive Vertrauensstellung zum On-Premises-AD des Kunden hat. Benutzer und WorkSpaces werden in Managed AD erstellt, wobei die AD-Vertrauensstellung den Zugriff auf Ressourcen in der On-Premises-Umgebung ermöglicht.

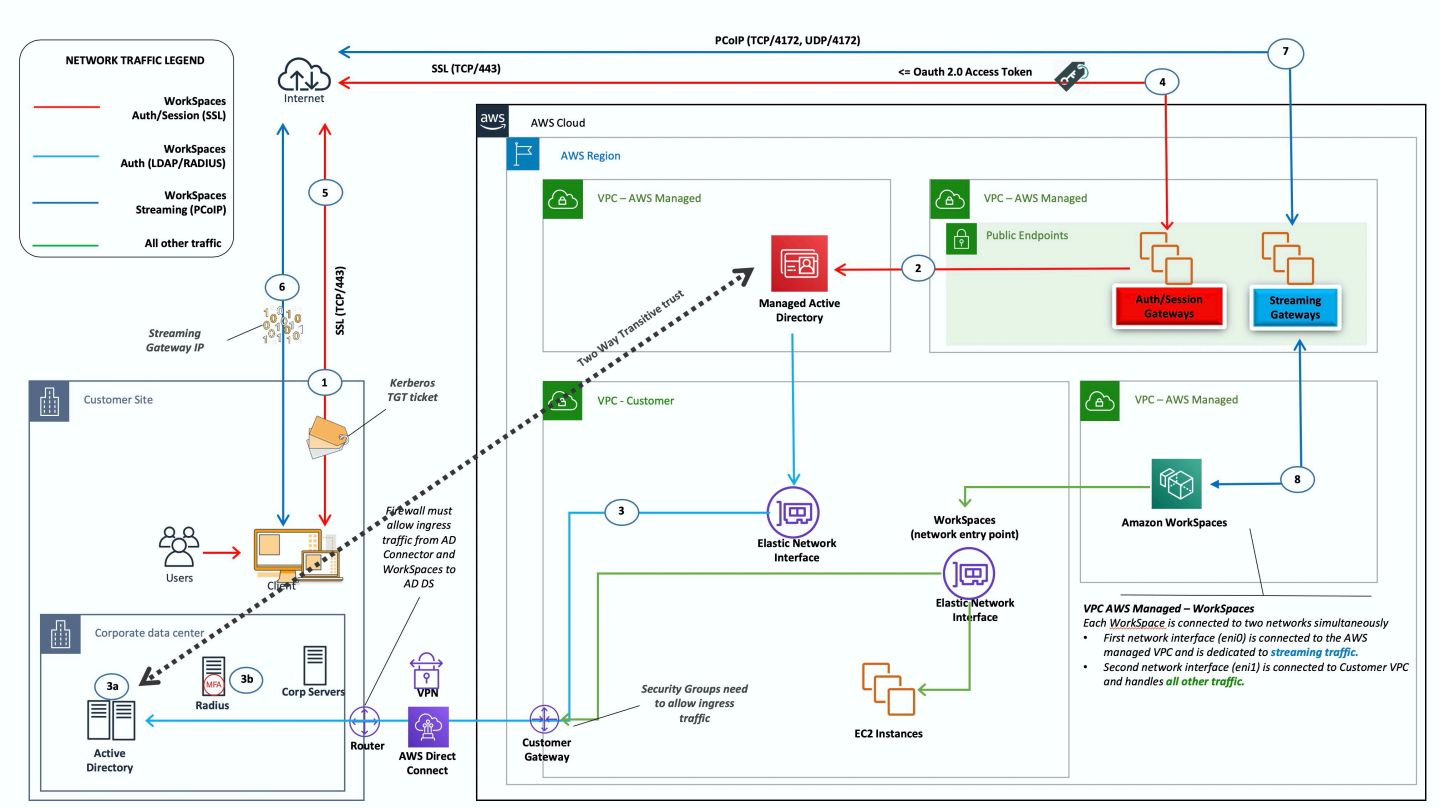


Abbildung 9: AWS Microsoft AD und eine bidirektionale transitive Vertrauensstellung zu On-Premises

Wie in Szenario 3 wird AD DS (Microsoft AD) in dedizierten Subnetzen bereitgestellt, die sich über zwei AZs erstrecken, wodurch AD DS in der AWS Cloud hochverfügbar wird.

Dieses Szenario eignet sich gut für Kunden, die über einen vollständig verwalteten AWS Directory Service verfügen möchten, einschließlich Bereitstellung, Patching, Hochverfügbarkeit und Überwachung ihrer AWS Cloud. In diesem Szenario können WorkSpaces Benutzer auch auf AD-verbundene Ressourcen in ihren vorhandenen Netzwerken zugreifen. In diesem Szenario muss eine Domain-Vertrauensstellung vorhanden sein. Sicherheitsgruppen und Firewall-Regeln müssen die Kommunikation zwischen den beiden aktiven Verzeichnissen ermöglichen.

Zusätzlich zur Platzierung von AWS Directory Service gibt die vorherige Abbildung Aufschluss über den Datenverkehr von einem Benutzer zu einem Workspace und die Interaktion des Workspace mit dem AD-Server und dem MFA-Server.

Diese Architektur verwendet die folgenden Komponenten oder Konstrukte.

AWS

- Amazon VPC – Erstellen einer Amazon VPC mit mindestens vier privaten Subnetzen in zwei AZs – zwei für AD DS Microsoft AD, zwei für AD Connector oder WorkSpaces.
- DHCP-Optionssatz – Erstellen eines Amazon VPC DHCP-Optionssatzes. Auf diese Weise kann ein Kunde einen bestimmten Domänennamen und DNS (Microsoft AD) definieren. Weitere Informationen finden Sie unter DHCP-Optionssätze.
- Optional: Amazon Virtual Private Gateway – Aktivieren Sie die Kommunikation mit einem kundeneigenen Netzwerk über einen IPsec-VPN-Tunnel (VPN) oder eine - AWS Direct Connect Verbindung. Verwenden Sie für den Zugriff auf On-Premises-Backend-Systeme.
- AWS Directory Service – Microsoft AD wird in einem dedizierten Paar von VPC-Subnetzen (AD DS Managed Service) bereitgestellt.

- Amazon EC2 – Optionale RADIUS-Server für MFA vom Kunden.
- Amazon WorkSpaces – WorkSpaces werden in denselben privaten Subnetzen wie der AD Connector bereitgestellt. Weitere Informationen finden Sie im Abschnitt Active Directory: Sites and Services dieses Dokuments.

Customer

- Netzwerkkonnektivität – Unternehmens-VPN oder - AWS Direct Connect Endpunkte.
- Endbenutzergeräte – Unternehmens- oder BYOL-Endbenutzergeräte (wie Windows, Macs, iPads, Android-Tablets, Null-Clients und Chromebooks), die für den Zugriff auf den Amazon- WorkSpaces Service verwendet werden. Weitere Informationen finden Sie in der Liste der Clientanwendungen für unterstützte Geräte und Webbrowser.

Diese Lösung erfordert Konnektivität zum On-Premises-Rechenzentrum des Kunden, damit der Vertrauensprozess ausgeführt werden kann. Wenn WorkSpaces Benutzer Ressourcen im On-

Premises-Netzwerk verwenden, müssen die Kosten für Latenz und ausgehende Datenübertragung berücksichtigt werden.

Szenario 5: AWS Microsoft AD unter Verwendung eines freigegebenen Services Virtual Private Cloud (VPC)

In diesem Szenario, das in der folgenden Abbildung dargestellt ist, wird ein AWS Managed AD in der AWS Cloud bereitgestellt, das Authentifizierungsservices für Workloads bereitstellt, die entweder bereits in gehostet werden AWS oder als Teil einer umfassenderen Migration geplant sind. Die bewährte Methode besteht darin, Amazon WorkSpaces in einer dedizierten VPC zu haben. Kunden sollten auch eine bestimmte AD-OU erstellen, um die WorkSpaces Computerobjekte zu organisieren.

Um WorkSpaces mit einer VPC für freigegebene Services bereitzustellen, die Managed AD hostet, stellen Sie einen AD Connector (ADC) mit einem in Managed AD erstellten Bol-Servicekonto bereit. Das Servicekonto benötigt Berechtigungen zum Erstellen von Computerobjekten in der WorkSpaces angegebenen Organisationseinheit im freigegebenen Services Managed AD.

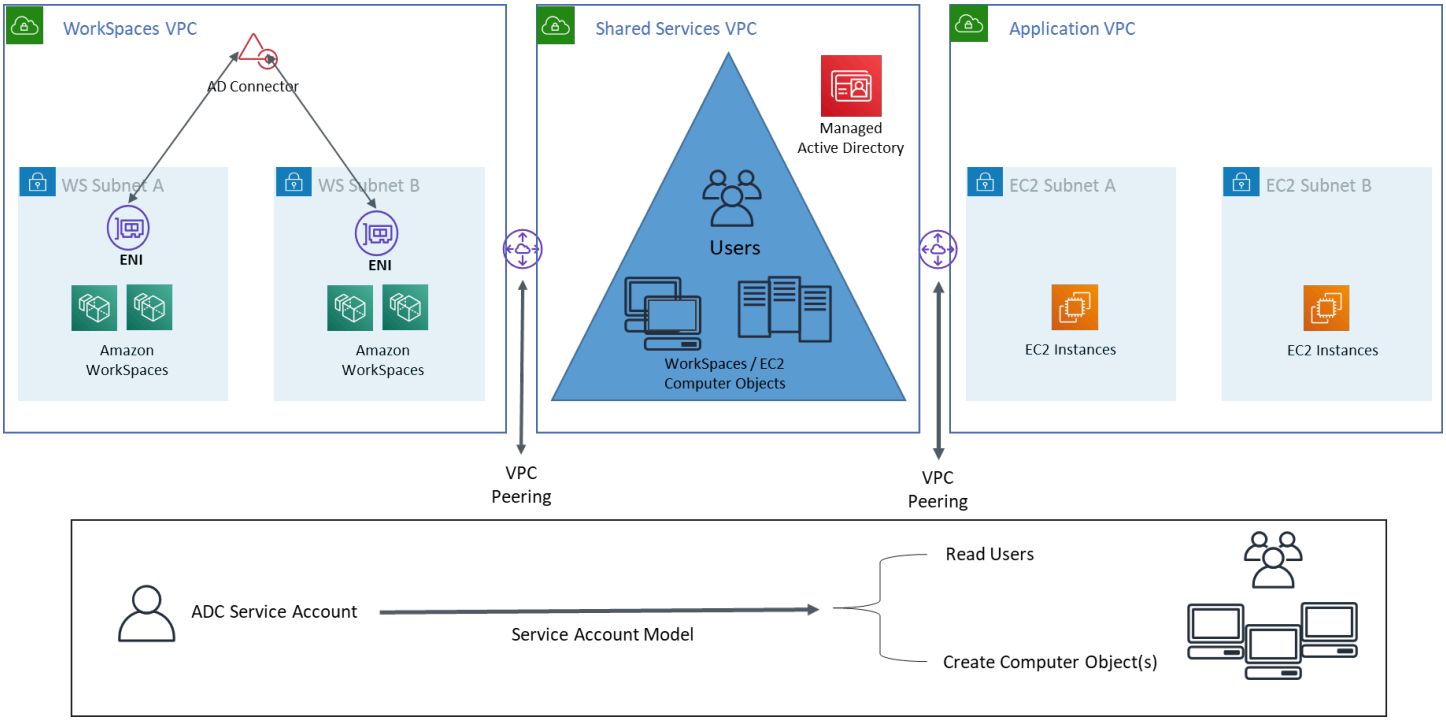


Abbildung 10: AWS Microsoft AD unter Verwendung einer VPC für gemeinsam genutzte Services

Diese Architektur verwendet die folgenden Komponenten oder Konstrukte.

AWS

- Amazon VPC – Erstellen einer Amazon VPC mit mindestens zwei privaten Subnetzen in zwei AZs (zwei für AD Connector und WorkSpaces).
- DHCP-Optionssatz – Erstellen eines Amazon VPC DHCP-Optionssatzes. Auf diese Weise kann ein Kunde einen bestimmten Domänennamen und DNS (Microsoft AD) definieren. Weitere Informationen finden Sie unter DHCP-Optionssätze.
- Optional: Amazon Virtual Private Gateway – Aktivieren Sie die Kommunikation mit einem kundeneigenen Netzwerk über einen IPsec-VPN-Tunnel (VPN) oder eine - AWS Direct Connect Verbindung. Verwenden Sie für den Zugriff auf On-Premises-Backend-Systeme.
- AWS Directory Service – Microsoft AD, das in einem dedizierten Paar von VPC-Subnetzen (AD DS Managed Service), AD Connector bereitgestellt wird
- AWS Transit Gateway/VPC Peering – Aktivieren Sie die Konnektivität zwischen Workspaces VPC und der Shared Services VPC
- Amazon EC2 – Optionale RADIUS-Server für MFA.
- Amazon WorkSpaces – WorkSpaces werden in denselben privaten Subnetzen wie der AD Connector bereitgestellt. Weitere Informationen finden Sie im Abschnitt Active Directory: Standorte und Services dieses Dokuments.

Customer

- Netzwerkkonnektivität – Unternehmens-VPN oder - AWS Direct Connect Endpunkte.
- Endbenutzergeräte – Unternehmens- oder BYOL-Endbenutzergeräte (wie Windows, Macs, iPads, Android-Tablets, Null-Clients und Chromebooks), die für den Zugriff auf den Amazon- WorkSpaces Service verwendet werden. Weitere Informationen finden Sie in der Liste der Clientanwendungen für unterstützte Geräte und Webbrowser.

Szenario 6: AWS Microsoft AD, VPC für gemeinsam genutzte Services und eine unidirektionale Vertrauensstellung zu On-Premises

Dieses Szenario verwendet, wie in der folgenden Abbildung gezeigt, ein vorhandenes On-Premises-Active-Directory für Benutzer und führt ein separates Managed Active Directory in AWS Cloud ein,

um die mit dem verknüpften Computerobjekte zu hosten WorkSpaces. In diesem Szenario können die Computerobjekte und Active-Directory-Gruppenrichtlinien unabhängig vom Unternehmens-Active-Directory verwaltet werden.

Dieses Szenario ist nützlich, wenn ein Drittanbieter Windows im Namen WorkSpaces eines Kunden verwalten möchte, da er es dem Dritten ermöglicht, die mit ihm verknüpften - WorkSpaces und - Richtlinien zu definieren und zu kontrollieren, ohne dem Drittanbieter Zugriff auf das Kunden-AD gewähren zu müssen. In diesem Szenario wird eine bestimmte Active-Directory-Organisationseinheit (OU) erstellt, um die WorkSpaces Computerobjekte im Shared Services AD zu organisieren.

> **Note**
>
> Amazon Linux WorkSpaces benötigt eine bidirektionale Vertrauensstellung, damit sie erstellt werden können.

Um Windows WorkSpaces mit den Computerobjekten bereitzustellen, die in der Shared Services VPC erstellt wurden, die Managed Active Directory mithilfe von Benutzern aus der Kundenidentitätsdomäne hostet, stellen Sie einen Active Directory Connector (ADC) bereit, der auf das Unternehmens-AD verweist. Verwenden Sie ein im Unternehmens-AD (Identitätsdomäne) erstelltes microSD-Servicekonto, das über delegierte Berechtigungen zum Erstellen von Computerobjekten in der Organisationseinheit (OU) verfügt, die für Windows WorkSpaces im Shared Services Managed AD konfiguriert wurde und über Leseberechtigungen für das Unternehmens-Active Directory (Identitätsdomäne) verfügt.

Um sicherzustellen, dass die Domain Locator-Funktion WorkSpaces Benutzer auf der gewünschten AD-Site für die Identitäts-Domain authentifizieren kann, benennen Sie die AD-Sites beider Domains für die Amazon WorkSpaces Subnets identisch gemäß der Microsoft-Dokumentation. Es hat sich bewährt, sowohl Identitätsdomänen als auch Shared Services Domain AD Domain Controller in derselben AWS Region wie Amazon zu haben WorkSpaces.

Ausführliche Anweisungen zur Konfiguration dieses Szenarios finden Sie im Implementierungshandbuch zum Einrichten einer unidirektionalen Vertrauensstellung für Amazon WorkSpaces mit AWS Directory Services.

In diesem Szenario richten wir eine einseitige transitive Vertrauensstellung zwischen dem AWS Managed Microsoft AD in der Shared Services VPC und dem On-Premises-AD ein. Abbildung 11 zeigt die Vertrauens- und Zugriffsrichtung und wie AWS AD Connector das AD-Connector-Servicekonto verwendet, um Computerobjekte in der Ressourcendomäne zu erstellen.

Eine Gesamtstruktur-Vertrauensstellung wird gemäß Microsoft-Empfehlung verwendet, um sicherzustellen, dass die Kerberos-Authentifizierung wann immer möglich verwendet wird. Ihre WorkSpaces erhalten Gruppenrichtlinienobjekte (GPOs) von Ihrer Ressourcen-Domain in der AWS Managed Microsoft AD. Darüber hinaus WorkSpaces führen Sie die Kerberos-Authentifizierung mit Ihrer Identitätsdomäne durch. Damit dies zuverlässig funktioniert, empfiehlt es sich, Ihre Identitätsdomäne auf zu erweitern, AWS wie oben bereits erläutert. Wir empfehlen, den Leitfaden Bereitstellen von Amazon WorkSpaces mithilfe einer One-Way-Trust-Ressourcendomäne mit AWS Directory Service Implementierung für weitere Details zu lesen.

Sowohl der AD Connector als auch Ihr WorkSpacesmüssen mit den Domain-Controllern Ihrer Identitätsdomäne und Ihrer Ressourcendomäne kommunizieren können. Weitere Informationen finden Sie unter IP-Adresse und Port-Anforderungen für WorkSpaces im Amazon- WorkSpaces Administratorhandbuch.

Wenn Sie mehrere AD Connectors verwenden, hat es sich bewährt, dass jeder der AD Connectors sein eigenes AD Connector Service-Konto verwendet.

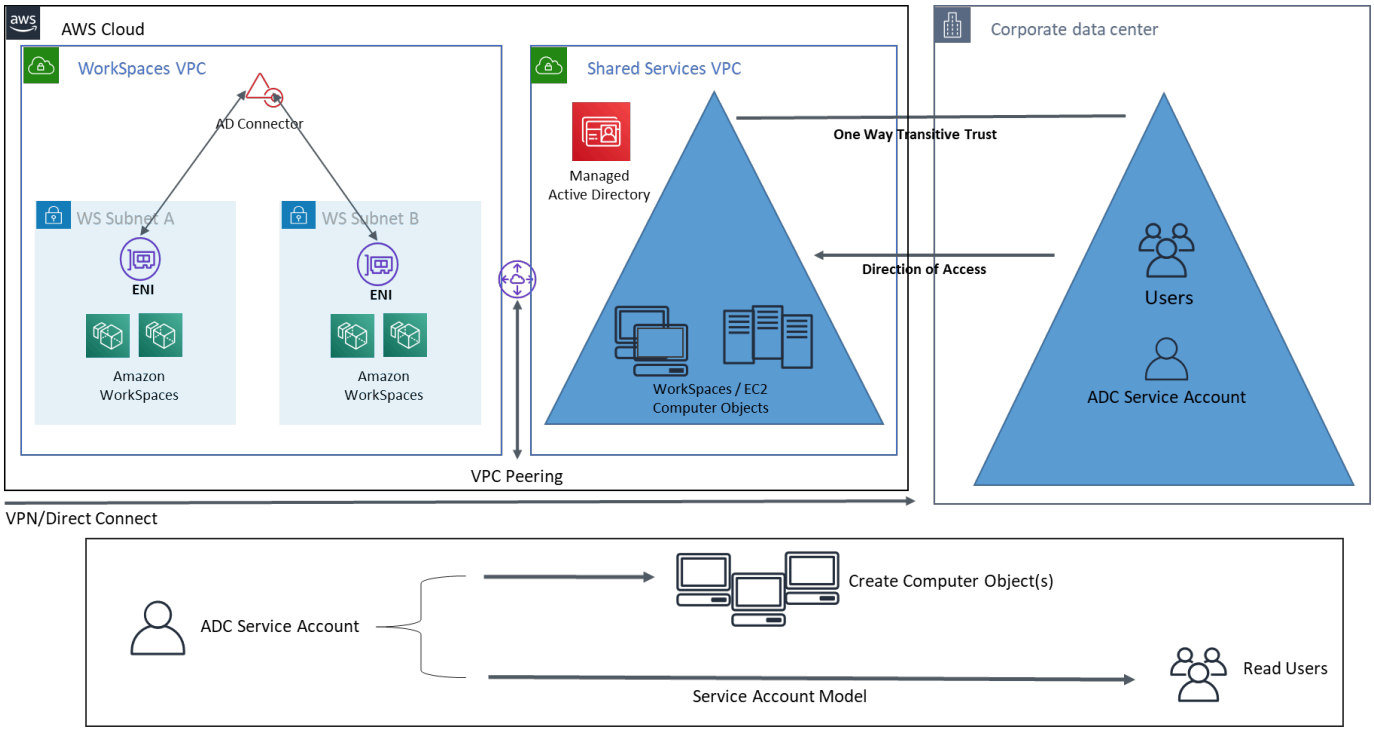


Abbildung 11: AWS Microsoft, VPC für gemeinsam genutzte Services und eine unidirektionale Vertrauensstellung zu AD On-Premises

Diese Architektur verwendet die folgenden Komponenten oder Konstrukte:

AWS

- Amazon VPC – Erstellen einer Amazon VPC mit mindestens zwei privaten Subnetzen in zwei AZs – zwei für AD Connector und WorkSpaces.
- DHCP-Optionssatz – Erstellen eines Amazon VPC DHCP-Optionssatzes. Auf diese Weise kann ein Kunde einen bestimmten Domänennamen und DNS (Microsoft AD) definieren. Weitere Informationen finden Sie unter DHCP-Optionssätze.
- Optional: Amazon Virtual Private Gateway – Aktivieren Sie die Kommunikation mit einem kundeneigenen Netzwerk über einen IPsec-VPN-Tunnel (VPN) oder eine - AWS Direct Connect Verbindung. Verwenden Sie für den Zugriff auf On-Premises-Backend-Systeme.
- AWS Directory Service – Microsoft AD wird in einem dedizierten Paar von VPC-Subnetzen (AD DS Managed Service), AD Connector bereitgestellt.
- Transit Gateway/VPC Peering – Aktivieren Sie die Konnektivität zwischen Workspaces VPC und der Shared Services VPC.
- Amazon EC2 – Vom Kunden „optionale“ RADIUS-Server für MFA.
- Amazon WorkSpaces – WorkSpaces werden in denselben privaten Subnetzen wie der AD Connector bereitgestellt. Weitere Informationen finden Sie im Abschnitt Active Directory: Sites and Services dieses Dokuments.

Customer

- Netzwerkkonnektivität – Unternehmens-VPN oder - AWS Direct Connect Endpunkte.
- Endbenutzergeräte – Unternehmens- oder BYOL-Endbenutzergeräte (wie Windows, Macs, iPads, Android-Tablets, Null-Clients und Chromebooks), die für den Zugriff auf den Amazon-WorkSpaces Service verwendet werden. Weitere Informationen finden Sie in dieser Liste der Clientanwendungen für unterstützte Geräte und Webbrowser.

Verwenden von Multi-Region AWS Managed Active Directory mit Amazon WorkSpaces

AWS Directory Service for Microsoft Active Directory (MAD) ist ein vollständig verwaltetes Microsoft Active Directory (AD), das mit Amazon gekoppelt werden kann WorkSpaces. Kunden entscheiden sich für AWS Managed Microsoft AD, da es über integrierte Hochverfügbarkeit, Überwachung und Backups verfügt. AWS Die verwaltete Microsoft AD Enterprise Edition fügt die Möglichkeit

hinzu, die Multi-Region-Replikation zu konfigurieren. Diese Funktion konfiguriert automatisch regionsübergreifende Netzwerkkonnektivität, stellt Domain-Controller bereit und repliziert alle Active-Directory-Daten in mehreren Regionen. Dadurch wird sichergestellt, dass Windows- und Linux-Workloads in diesen Regionen eine Verbindung zu AWS MAD herstellen und MAD mit geringer Latenz und hoher Leistung verwenden können. Replizierte MAD-Regionen können nicht direkt bei registriert WorkSpaces werden, aber ein repliziertes MAD-Verzeichnis kann bei registriert werden, WorkSpaces indem ein AD Connector (ADC) so konfiguriert wird, dass er auf Ihre replizierten Domain-Controller verweist.

Die bewährte Methode bei der Bereitstellung von AD Connectors mit MAD besteht darin, einen AD Connector für jede Geschäftseinheit in Ihrer WorkSpaces Umgebung zu erstellen. Auf diese Weise können Sie jede Geschäftseinheit mit einer bestimmten Organisationseinheit in Active Directory abgleichen. Anschließend können Sie AD-Gruppenrichtlinienobjekte auf Ebene der Organisationseinheit zuweisen, die direkt mit der betreffenden Geschäftseinheit übereinstimmen.

Architektur

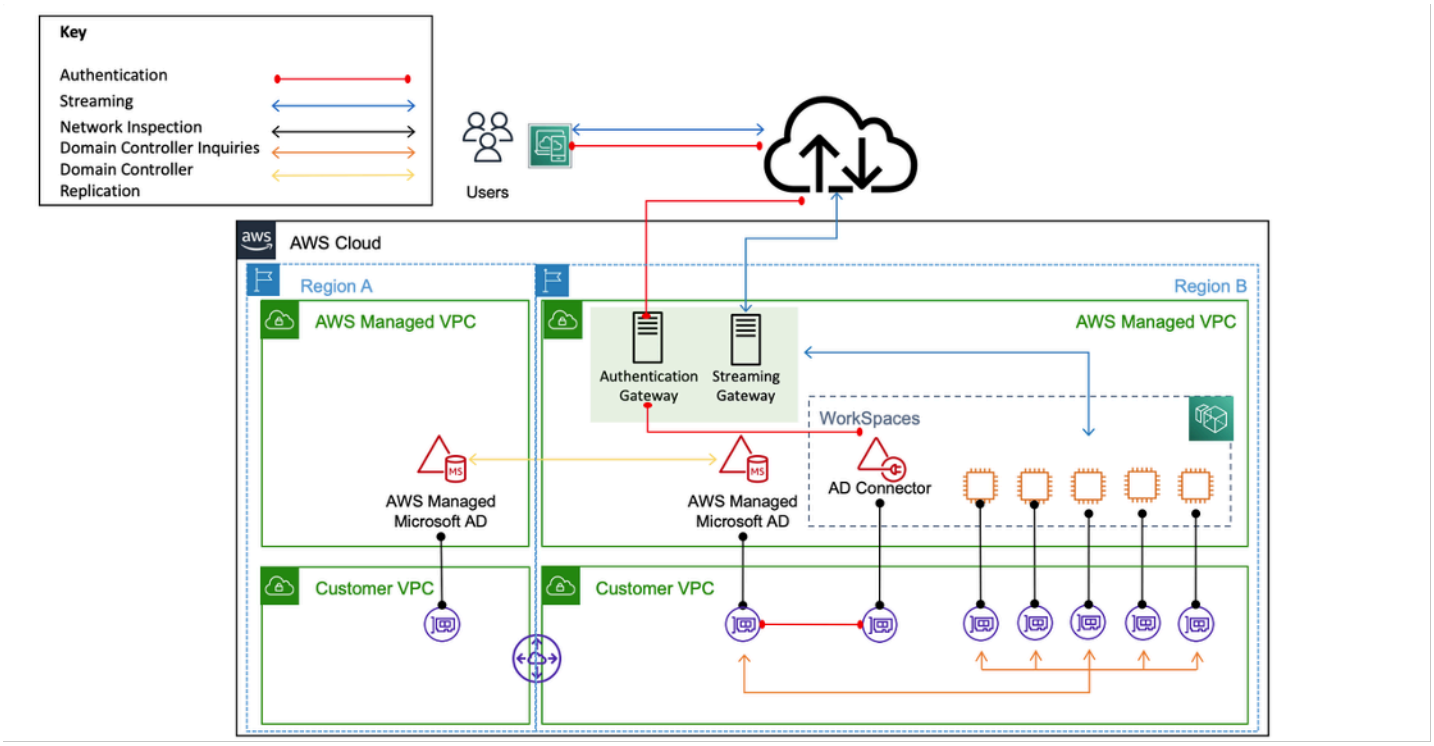


Abbildung 12: Beispielarchitektur für die Registrierung einer replizierten MAD-Region in einem WorkSpace

Implementierung

Um Ihre replizierte MAD-Region in zu registrieren WorkSpaces, müssen Sie einen AD Connector erstellen, der auf Ihre MAD-Domain-Controller-IPs verweist. Sie finden Ihre MAD-Domain-Controller-IP-Adressen, indem Sie zum Navigationsbereich der AWS Directory-Service-Konsole gehen, Verzeichnisse und dann die richtige Verzeichnis-ID auswählen. Um diese AD Connectors zu erstellen, folgen Sie diesem Handbuch. Sobald sie erstellt wurden, können Sie sie für registrieren WorkSpaces. Bevor Sie WorkSpaces in Ihrer neuen Region bereitstellen, stellen Sie sicher, dass Sie die DHCP-Optionsliste Ihrer VPCs aktualisiert haben. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/dhcp_options_set.html

Überlegungen zum Design

Eine funktionale AD-DS-Bereitstellung in der - AWS Cloud erfordert ein gutes Verständnis sowohl von Active-Directory-Konzepten als auch von bestimmten AWS -Services. In diesem Abschnitt werden wichtige Designüberlegungen bei der Bereitstellung von AD DS für Amazon WorkSpaces, bewährte VPC-Methoden für AWS Directory Service, DHCP- und DNS-Anforderungen, AD-Connector-Spezifika sowie AD-Standorte und -Services erörtert.

VPC-Design

Wie zuvor im Abschnitt Netzwerküberlegungen dieses Dokuments erörtert und für die Szenarien 2 und 3 früher dokumentiert, sollten Kunden AD DS in der AWS Cloud in einem dedizierten Paar privater Subnetze, über zwei AZs hinweg und getrennt von AD Connector oder WorkSpaces Subnetzen bereitstellen. Dieses Konstrukt bietet hochverfügbaren Zugriff mit geringer Latenz auf AD-DS-Services für WorkSpacesund behält gleichzeitig die bewährten Standardmethoden der Trennung von Rollen oder Funktionen innerhalb der Amazon VPC bei.

Die folgende Abbildung zeigt die Trennung von AD DS und AD Connector in dedizierte private Subnetze (Szenario 3). In diesem Beispiel befinden sich alle Services in derselben Amazon VPC.

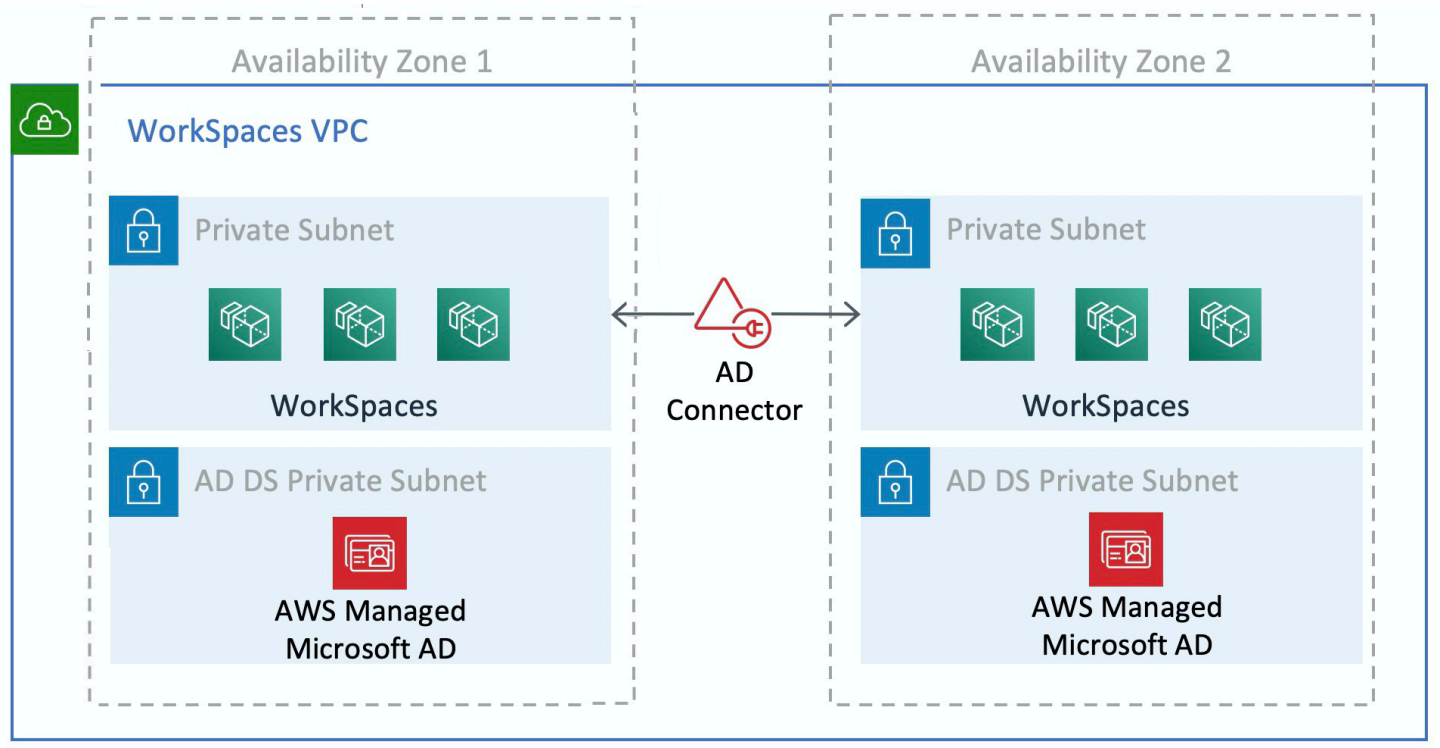


Abbildung 13: AD-DS-Netzwerktrennung

Die folgende Abbildung zeigt ein Design ähnlich Szenario 1. In diesem Szenario befindet sich der On-Premises-Teil jedoch in einer dedizierten Amazon VPC.

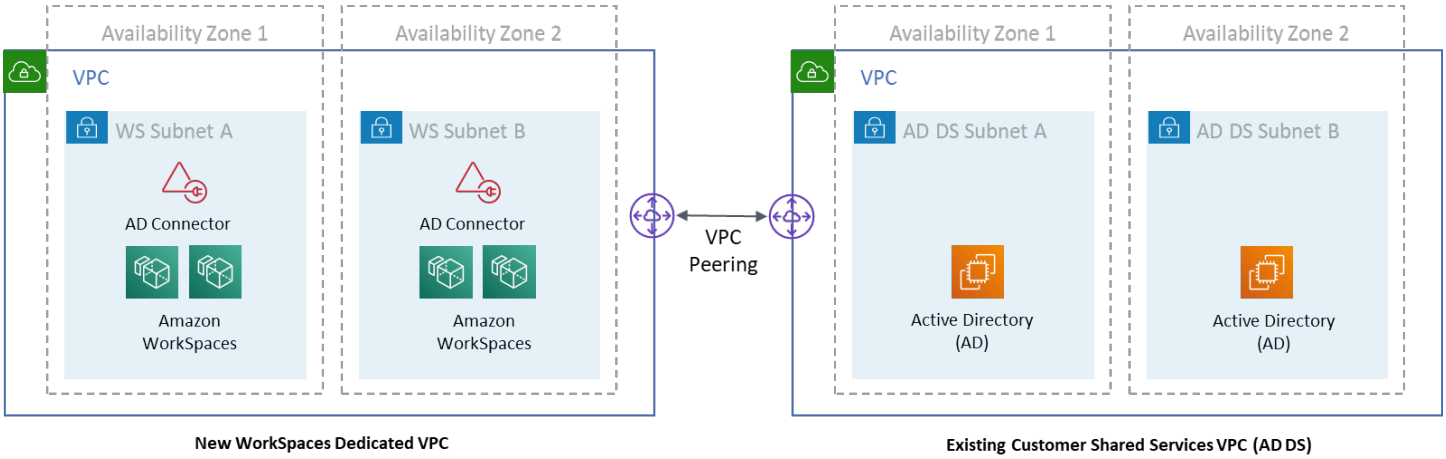


Abbildung 14: Dedicated WorkSpaces VPC

> **Note**
>
> Für Kunden mit einer vorhandenen AWS Bereitstellung, in der AD DS verwendet wird, wird empfohlen, ihre WorkSpaces in einer dedizierten VPC zu platzieren und VPC-Peering für die AD-DS-Kommunikation zu verwenden.

Zusätzlich zur Erstellung dedizierter privater Subnetze für AD DS benötigen Domain-Controller und Mitgliedsserver mehrere Sicherheitsgruppenregeln, um Datenverkehr für -Services wie AD-DS-Replikation, Benutzerauthentifizierung, Windows-Zeitservices und verteiltes Dateisystem (DFS) zuzulassen.

> **Note**
>
> Die bewährte Methode besteht darin, die erforderlichen Sicherheitsgruppenregeln auf die WorkSpaces privaten Subnetze zu beschränken und im Fall von Szenario 2 die bidirektionale AD-DS-Kommunikation On-Premises zur und von der AWS Cloud zu ermöglichen, wie in der folgenden Tabelle gezeigt.

Tabelle 1 – Bidirektionale AD-DS-Kommunikation zur und von der AWS Cloud

Protokoll	Port	Verwenden Sie	Bestimmungsort
TCP	53, 88, 135, 139, 389, 445, 464, 636	Auth (primär)	Active Directory (privates Rechenzentrum oder Amazon EC2)*
TCP	49 152 – 65 535	RPC-Hochports	Active Directory (privates Rechenzentrum oder Amazon EC2) **
TCP	3268-3269	Vertrauensstellungen	Active Directory (privates Rechenzentrum oder Amazon EC2)*
TCP	9389	Remote Microsoft Windows PowerShell (optional)	Active Directory (privates Rechenzentrum oder Amazon EC2)*
UDP	53, 88, 123, 137, 138, 389, 445, 464	Auth (primär)	Active Directory (privates Rechenzentrum oder Amazon EC2)*
UDP	1812	Auth (MFA) (optional)	RADIUS (privates Rechenzentrum oder Amazon EC2)*

Weitere Informationen finden Sie unter Portanforderungen für Active Directory und Active Directory Domain Services und Serviceübersicht und Netzwerkportanforderungen für Windows.

step-by-step Anleitungen zur Implementierung von Regeln finden Sie unter Hinzufügen von Regeln zu einer Sicherheitsgruppe im Amazon Elastic Compute Cloud-Benutzerhandbuch.

VPC-Design: DHCP und DNS

Bei einer Amazon VPC werden Dynamic Host Configuration Protocol (DHCP)-Services standardmäßig für Ihre Instances bereitgestellt. Standardmäßig stellt jede VPC einen internen DNS-Server (Domain Name System) bereit, auf den über den CIDR-Adressraum (Classless Inter-Domain Routing) +2 zugegriffen werden kann und der über einen standardmäßigen DHCP-Optionssatz allen Instances zugewiesen wird.

DHCP-Optionssätze werden innerhalb einer Amazon VPC verwendet, um Bereichsoptionen zu definieren, z. B. den Domänennamen oder die Namenserver, die Kunden-Instances über DHCP übergeben werden sollen. Die korrekte Funktionalität von Windows-Services innerhalb einer Kunden-VPC hängt von dieser DHCP-Bereichsoption ab. In jedem der zuvor definierten Szenarien erstellen Kunden einen eigenen Bereich, der den Domainnamen und die Namenserver definiert, und weisen ihn zu. Dadurch wird sichergestellt, dass mit der Domain verbundene Windows-Instances oder für die Verwendung des AD-DNS konfiguriert WorkSpaces sind.

Die folgende Tabelle ist ein Beispiel für einen benutzerdefinierten Satz von DHCP-Bereichsoptionen, die erstellt werden müssen, damit Amazon WorkSpaces und AWS Directory Services ordnungsgemäß funktionieren.

Tabelle 2 – Benutzerdefinierter Satz von DHCP-Bereichsoptionen

Parameter	Wert
Namens-Tag	Erstellt ein Tag, bei dem key = name und value auf eine bestimmte Zeichenfolge festgelegt sind Beispiel: example.com
Domainname	example.com
Domainnamenserver	DNS-Serveradresse, getrennt durch Kommas Beispiel: 192.0.2.10, 192.0.2.21
NTP-Server	Lassen Sie dieses Feld leer
NetBIOS-Namenserver	Geben Sie dieselben durch Kommas getrennte n IPs wie für die Domainnamenserver ein

Parameter	Wert
	Beispiel: 192.0.2.10, 192.0.2.21
NetBIOS-Knotentyp	2

Weitere Informationen zum Erstellen eines benutzerdefinierten DHCP-Optionssatzes und zum Zuordnen zu einer Amazon VPC finden Sie unter Arbeiten mit DHCP-Optionssätzen im Amazon Virtual Private Cloud-Benutzerhandbuch.

In Szenario 1 wäre der DHCP-Bereich das On-Premises-DNS oder AD DS. In den Szenarien 2 oder 3 wäre dies jedoch der lokal bereitgestellte Verzeichnisservice (AD DS auf Amazon EC2 oder AWS Directory Services: Microsoft AD). Es wird empfohlen, dass jeder Domain-Controller, der sich in der -AWS Cloud befindet, ein globaler Katalog und ein Directory-integrierter DNS-Server ist.

Active Directory: Standorte und Services

Für Szenario 2 sind Standorte und Services kritische Komponenten für die richtige Funktion von AD DS. Die Standorttopologie steuert die AD-Replikation zwischen Domain-Controllern innerhalb desselben Standorts und über Standortgrenzen hinweg. In Szenario 2 sind mindestens zwei Standorte vorhanden: On-Premises und Amazon WorkSpaces in der Cloud.

Die Definition der richtigen Standorttopologie gewährleistet die Client-Affinität, was bedeutet, dass Clients (in diesem Fall WorkSpaces) ihren bevorzugten lokalen Domain-Controller verwenden.

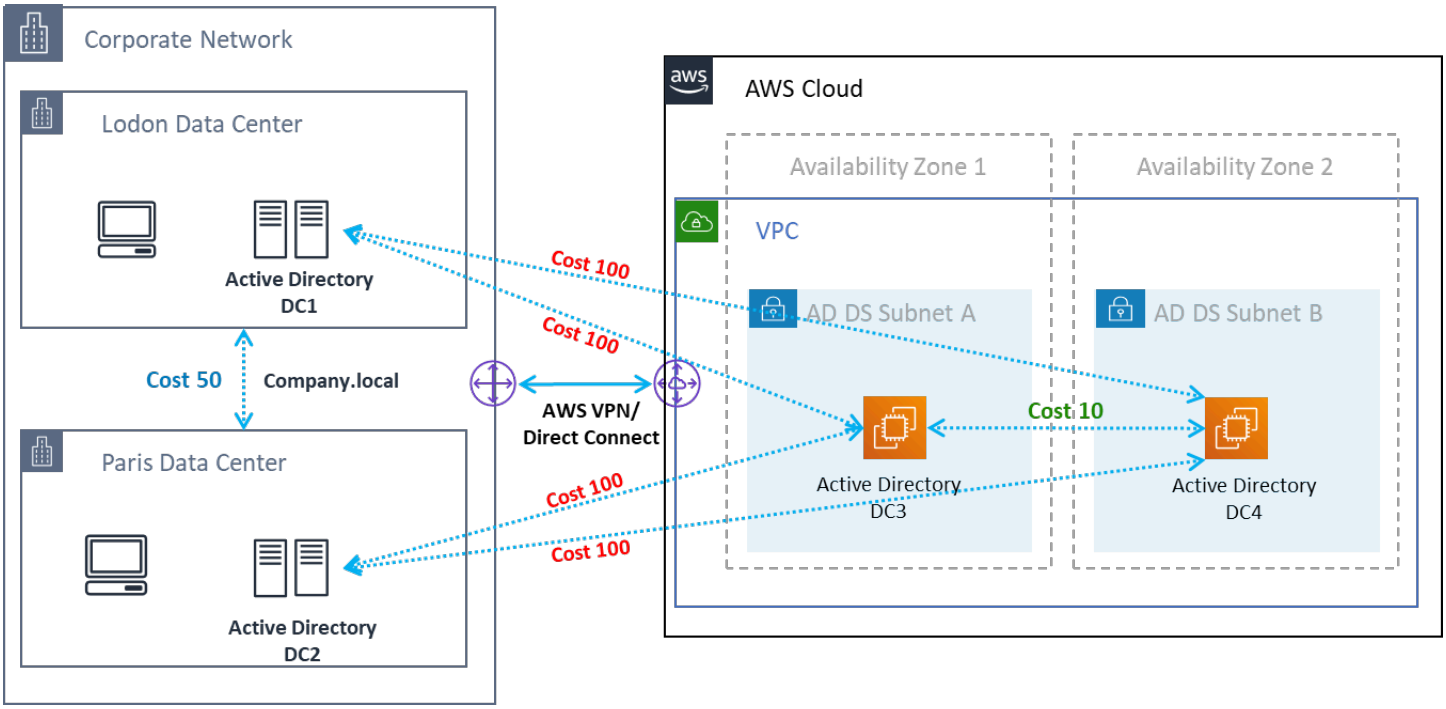


Abbildung 15: Active-Directory-Standorte und -Services: Client-Affinität

Bewährte Methode: Definieren Sie hohe Kosten für Website-Links zwischen On-Premises-AD-DS und der AWS Cloud. Die folgende Abbildung zeigt, welche Kosten den Website-Links zugewiesen werden müssen (Kosten 100), um eine standortunabhängige Client-Affinität sicherzustellen.

Diese Zuordnungen tragen dazu bei, dass der Datenverkehr – wie AD-DS-Replikation und Client-Authentifizierung – den effizientesten Pfad zu einem Domain-Controller verwendet. In den Szenarien 2 und 3 trägt dies dazu bei, eine geringere Latenz und einen übergreifenden Datenverkehr sicherzustellen.

Protokoll

Amazon WorkSpaces Streaming Protocol (WSP) ist ein cloudnatives Streaming-Protokoll, das ein konsistentes Benutzererlebnis über globale Entfernungen und unzuverlässige Netzwerke hinweg ermöglicht. WSP entkoppelt das Protokoll von durch Auslagern WorkSpaces von Metrikanalyse, Kodierung, Codec-Nutzung und -Auswahl. WSP verwendet Port TCP/UDP 4195. Bei der Entscheidung, ob das WSP-Protokoll verwendet wird oder nicht, gibt es mehrere wichtige Fragen, die vor der Bereitstellung beantwortet werden sollten. Bitte lesen Sie die Entscheidungsmatrix unten:

Frage	WSP	PCoIP
Benötigen die identifizierten WorkSpaces Benutzer bidirektionales Audio/Video?	•	
Wird null Clients als Remote-Endpunkt (lokales Gerät) verwendet?		•
Wird Windows oder macOS für den Remote-Endpunkt verwendet?	•	•
Wird Ubuntu 18.04 für den Remote-Endpunkt verwendet?		•
Greifen die Benutzer WorkSpaces über Webzugriff auf Amazon zu?		•
Wird die Smartcard-Unterstützung (PIC/CAC) vor der Sitzung oder während der Sitzung benötigt?	•	
Wird in WorkSpaces der Region China (Ningxia) verwendet?		•
Wird Smartcard-Vorauthentifizierung oder Sitzungsunterstützung erforderlich sein?	•	
Verwenden Endbenutzer unzuverlässige Verbindungen mit hoher Latenz oder niedriger Bandbreite?	•	

Die vorherigen Fragen sind entscheidend, um das Protokoll zu bestimmen, das verwendet werden soll. Weitere Informationen zu den empfohlenen Protokollanwendungsfällen finden Sie hier . Das verwendete Protokoll kann auch zu einem späteren Zeitpunkt mit der Amazon WorkSpaces -Migrate-Funktion geändert werden. Weitere Informationen zur Verwendung dieser Funktion finden Sie hier.

Bei der Bereitstellung WorkSpaces mit WSP sollten die WSP Gateways einer Zulassungsliste hinzugefügt werden, um die Konnektivität zum Service sicherzustellen. Darüber hinaus sollte die Round-Trip-Zeit (RTT) für Benutzer, die sich WorkSpaces über WSP mit einem verbinden, unter 250 ms liegen, um eine optimale Leistung zu erzielen. Verbindungen mit einem RTT zwischen 250 ms und 400 ms werden beeinträchtigt. Wenn die Verbindung des Benutzers dauerhaft beeinträchtigt ist, wird empfohlen, nach Möglichkeit ein Amazon WorkSpaces in einer serviceunterstützten Region bereitzustellen, die dem Endbenutzer am nächsten ist.

Multifaktor-Authentifizierung (MFA)

Die Implementierung von MFA erfordert WorkSpaces , dass Amazon entweder mit einem Active Directory Connector (AD Connector) oder AWS Managed Microsoft AD (MAD) als Directory Service konfiguriert wird und über einen RADIUS-Server verfügt, auf den der Directory Service im Netzwerk zugreifen kann. Simple Active Directory unterstützt MFA nicht.

Im vorherigen Abschnitt werden Überlegungen zur Bereitstellung von Active Directory und Directory Services für AD sowie zu RADIUS-Designoptionen in jedem Szenario behandelt.

MFA – Zwei-Faktor-Authentifizierung

Nachdem MFA aktiviert wurde, müssen Benutzer ihren Benutzernamen, ihr Passwort und ihren MFA-Code für die Authentifizierung auf ihren jeweiligen WorkSpaces Desktops dem WorkSpaces Client bereitstellen.

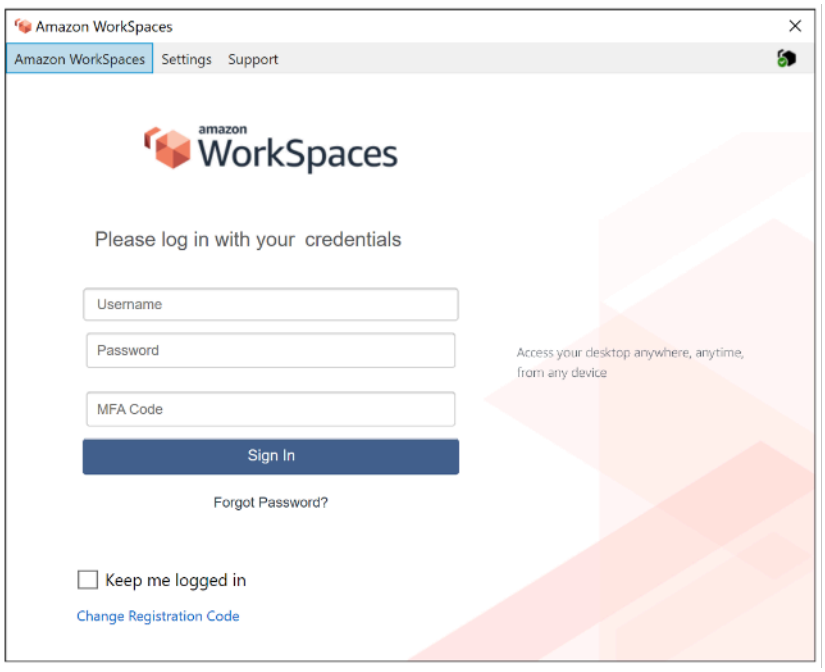


Abbildung 16: WorkSpaces Client mit aktivierter MFA

> **Note**
>
> Der AWS Directory Service unterstützt keine selektive oder kontextbezogene MFA: Dies ist eine globale Einstellung pro Verzeichnis. Wenn eine selektive MFA pro Benutzer erforderlich ist, müssen die Benutzer durch einen AD Connector getrennt werden, der auf dasselbe Quell-Active Directory verweisen kann.

WorkSpaces MFA erfordert einen oder mehrere RADIUS-Server. In der Regel handelt es sich dabei um vorhandene Lösungen, die Sie möglicherweise bereits bereitgestellt haben, z. B. RSA oder Gemalto. Alternativ können RADIUS-Server in Ihrer VPC auf EC2-Instances bereitgestellt werden (im Abschnitt AD-DS-Bereitstellungsszenarien dieses Dokuments finden Sie Architekturoptionen). Wenn Sie eine neue RADIUS-Lösung bereitstellen, gibt es mehrere Implementierungen, z. B. FreeRADIUS, zusammen mit SaaS-Angeboten wie Bol Security oder Okta MFA.

Es hat sich bewährt, mehrere RADIUS-Server zu nutzen, um sicherzustellen, dass Ihre Lösung ausfallsicher ist. Bei der Konfiguration Ihres Directory Service für MFA können Sie mehrere IP-Adressen eingeben, indem Sie sie durch ein Komma trennen (z. B. 192.0.0.0,192.0.0.12). Die Directory-Services-MFA-Funktion versucht die erste angegebene IP-Adresse und wechselt zur zweiten IP-Adresse, falls die Netzwerkkonnektivität nicht mit der ersten hergestellt werden kann. Die Konfiguration von RADIUS für eine hochverfügbare Architektur ist für jeden Lösungssatz einzigartig.

Die übergreifende Empfehlung besteht jedoch darin, die zugrunde liegenden Instances für Ihre RADIUS-Funktion in verschiedenen Availability Zones zu platzieren. Ein Konfigurationsbeispiel ist Bol Security und für Okta MFA können Sie mehrere Okta RADIUS-Serveragenten auf die gleiche Weise bereitstellen.

Ausführliche Schritte zum Aktivieren Ihres AWS Directory Service für MFA finden Sie unter AD Connector und AWS Managed Microsoft AD.

Notfallwiederherstellung/Geschäftskontinuität

WorkSpaces Regionsübergreifende Umleitung

Amazon WorkSpaces ist ein regionaler Service, der Kunden Remote-Desktop-Zugriff bietet. Abhängig von den Anforderungen an Geschäftskontinuität und Notfallwiederherstellung (BC/DR) benötigen einige Kunden ein nahtloses Failover in eine andere Region, in der der WorkSpaces Service verfügbar ist. Diese BC/DR-Anforderung kann mithilfe der Option für WorkSpaces regionsübergreifende Umleitung erreicht werden. Es ermöglicht Kunden, einen vollqualifizierten Domainnamen (FQDN) als WorkSpaces Registrierungscode zu verwenden.

Eine wichtige Überlegung besteht darin, zu bestimmen, zu welchem Zeitpunkt eine Umleitung zu einer Failover-Region erfolgen soll. Die Kriterien für diese Entscheidung sollten auf Ihrer Unternehmensrichtlinie basieren, aber das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) enthalten. Ein Well-Architected- WorkSpaces Architekturdesign sollte das Potenzial für einen Serviceausfall beinhalten. Die Zeittoleranz für die normale Wiederherstellung des Geschäftsbetriebs wird auch bei der Entscheidung berücksichtigt.

Wenn sich Ihre Endbenutzer bei WorkSpaces mit einem FQDN als WorkSpaces Registrierungscode anmelden, wird ein DNS-TXT-Datensatz aufgelöst, der eine Verbindungskennung enthält, die das registrierte Verzeichnis bestimmt, an das der Benutzer weitergeleitet wird. Die Anmeldestartseite des WorkSpaces Clients wird dann basierend auf dem registrierten Verzeichnis angezeigt, das der zurückgegebenen Verbindungskennung zugeordnet ist. Auf diese Weise können Administratoren ihre Endbenutzer basierend auf Ihren DNS-Richtlinien für den FQDN zu verschiedenen WorkSpaces Verzeichnissen weiterleiten. Diese Option kann mit öffentlichen oder privaten DNS-Zonen verwendet werden, vorausgesetzt, die privaten Zonen können vom Client-Computer aufgelöst werden. Die regionsübergreifende Umleitung kann manuell oder automatisiert sein. Beide Failovers können erreicht werden, indem der TXT-Datensatz geändert wird, der die Verbindungskennung enthält, auf die das gewünschte Verzeichnis verwiesen werden soll.

Während Sie Ihre BC/DR-Strategie entwickeln, ist es wichtig, die Benutzerdaten zu berücksichtigen, da die WorkSpaces regionsübergreifende Umleitungsoption keine Benutzerdaten synchronisiert und auch keine WorkSpaces Bilder synchronisiert. Ihre WorkSpaces Bereitstellungen in verschiedenen AWS Regionen sind unabhängige Entitäten. Sie müssen daher zusätzliche Maßnahmen ergreifen, um sicherzustellen, dass Ihre WorkSpaces Benutzer auf ihre Daten zugreifen können, wenn eine Umleitung zu einer sekundären Region stattfindet. Für die Replikation von Benutzerdaten stehen viele Optionen zur Verfügung, z. B. WorkSpaces, Windows FSx (DFS Share) oder Dienstprogramme von Drittanbietern, um Daten-Volumes zwischen Regionen zu synchronisieren. Ebenso müssen Sie sicherstellen, dass Ihre sekundäre Region Zugriff auf die erforderlichen WorkSpaces Images hat, z. B. indem Sie die Images regionsübergreifend kopieren. Weitere Informationen finden Sie unter Regionsübergreifende Umleitung für Amazon WorkSpaces im Amazon- WorkSpaces Administratorhandbuch und im Beispiel im Diagramm.

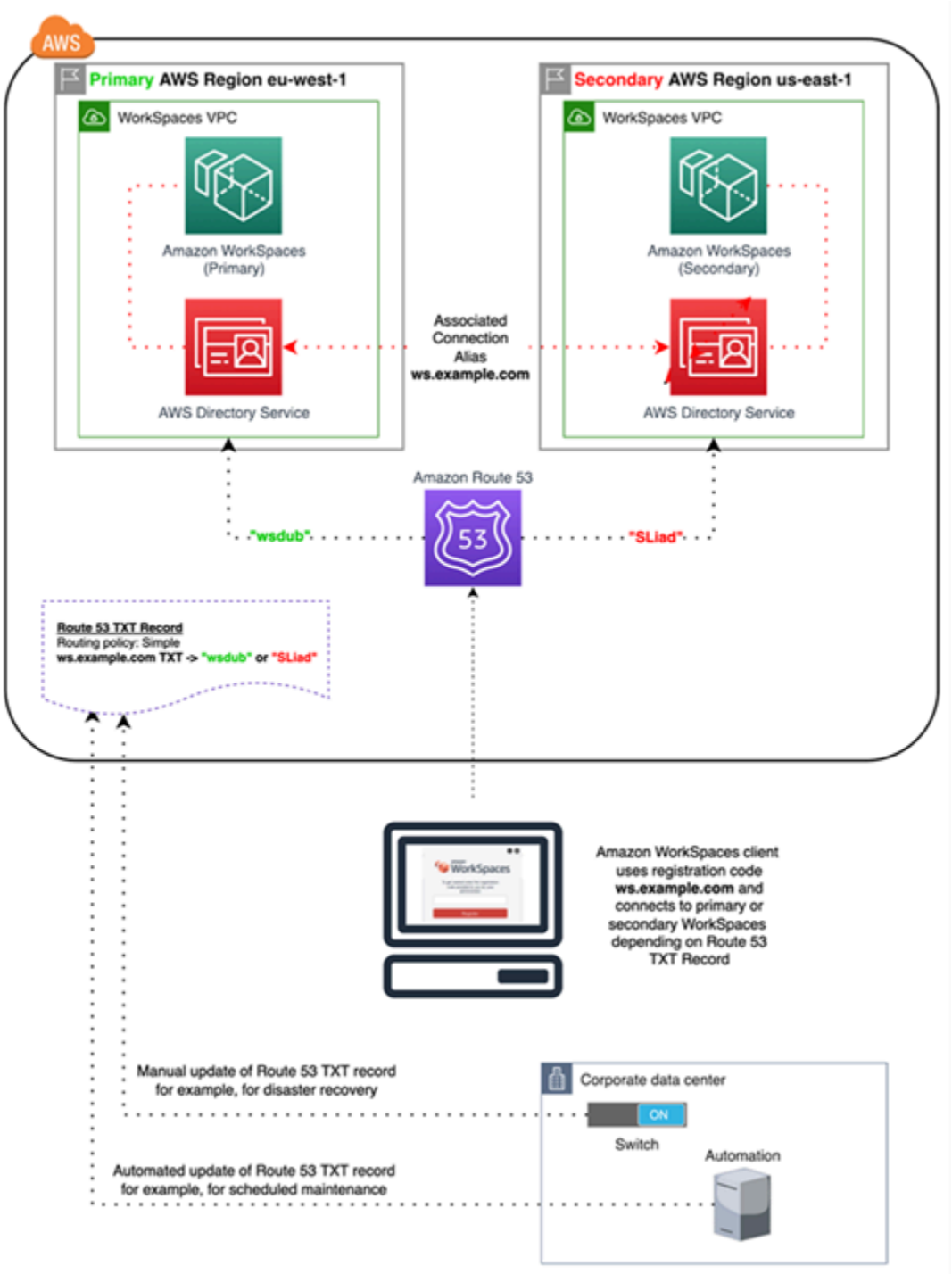


Abbildung 17: Beispiel für eine WorkSpaces regionsübergreifende Umleitung mit Amazon Route 53

WorkSpaces Schnittstellen-VPC-Endpunkt (AWS PrivateLink) – API-Aufrufe

WorkSpaces Öffentliche Amazon-APIs werden auf unterstütztAWS PrivateLink. AWS PrivateLink erhöht die Sicherheit von Daten, die mit cloudbasierten Anwendungen geteilt werden, indem die Offenlegung von Daten im öffentlichen Internet reduziert wird. WorkSpaces Der API-Datenverkehr kann innerhalb einer VPC mithilfe eines Schnittstellenendpunkts gesichert werden. Dabei handelt es sich um eine Elastic Network-Schnittstelle mit einer privaten IP-Adresse aus dem IP-Adressbereich Ihres Subnetzes, die als Eintrittspunkt für Datenverkehr dient, der für einen unterstützten Service bestimmt ist. Auf diese Weise können Sie über private IP-Adressen privat auf - WorkSpaces API-Services zugreifen.

Durch die Verwendung von PrivateLink mit WorkSpaces öffentlichen APIs können Sie REST-APIs auch sicher für Ressourcen innerhalb Ihrer VPC oder für Ressourcen bereitstellen, die über mit Ihren Rechenzentren verbunden sind AWS Direct Connect.

Sie können den Zugriff auf ausgewählte Amazon VPCs und VPC-Endpunkte einschränken und den kontoübergreifenden Zugriff mithilfe ressourcenspezifischer Richtlinien aktivieren.

Stellen Sie sicher, dass die Sicherheitsgruppe, die der Endpunktnetzwerkschnittstelle zugeordnet ist, die Kommunikation zwischen der Endpunktnetzwerkschnittstelle und den Ressourcen in Ihrer VPC ermöglicht, die mit dem Service kommunizieren. Wenn die Sicherheitsgruppe eingehenden HTTPS-Datenverkehr (Port 443) von Ressourcen in der VPC einschränkt, können Sie möglicherweise keinen Datenverkehr über die Endpunkt-Netzwerkschnittstelle senden. Ein Schnittstellenendpunkt unterstützt nur TCP-Verkehr.

- Für Endpunkte wird nur IPv4-Datenverkehr unterstützt.
- Wenn Sie einen Endpunkt erstellen, können Sie ihm eine Endpunktrichtlinie zuweisen, die den Zugriff auf den Service, mit dem Sie eine Verbindung herstellen, steuert.
- Die Anzahl der Endpunkte, die Sie pro VPC erstellen können, ist kontingentiert.
- Endpunkte werden nur innerhalb derselben Region unterstützt. Sie können keinen Endpunkt zwischen einer VPC und einem Service in einer anderen Region erstellen.

Benachrichtigung erstellen, um Warnungen zu Schnittstellenendpunktereignissen zu erhalten – Sie können eine Benachrichtigung erstellen, um Warnungen zu bestimmten Ereignissen zu erhalten, die auf Ihrem Schnittstellenendpunkt auftreten. Um eine Benachrichtigung zu erstellen, müssen Sie

dieser ein Amazon SNS-Thema zuordnen. Sie können das SNS-Thema abonnieren, um eine E-Mail-Benachrichtigung zu erhalten, wenn ein Endpunktereignis auftritt.

Erstellen einer VPC-Endpunktrichtlinie für Amazon WorkSpaces – Sie können eine Richtlinie für Amazon-VPC-Endpunkte für Amazon erstellen, WorkSpaces um Folgendes anzugeben:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Verbinden Ihres privaten Netzwerks mit Ihrer VPC – Um die Amazon WorkSpaces -API über Ihre VPC aufzurufen, müssen Sie eine Verbindung von einer Instance innerhalb der VPC herstellen oder Ihr privates Netzwerk mithilfe eines Amazon Virtual Private Network (VPN) oder mit Ihrer VPC verbinden AWS Direct Connect. Weitere Informationen zu Amazon VPN finden Sie unter VPN-Verbindungen im Amazon Virtual Private Cloud-Benutzerhandbuch. Weitere Informationen zu AWS Direct Connectfinden Sie unter Erstellen einer Verbindung im AWS Direct Connect - Benutzerhandbuch.

Weitere Informationen zur Verwendung der Amazon WorkSpaces -API über einen VPC-Schnittstellenendpunkt finden Sie unter Infrastruktursicherheit in Amazon WorkSpaces.

Smartcard-Unterstützung

Smartcard-Unterstützung ist sowohl für Microsoft Windows als auch für Amazon Linux verfügbar WorkSpaces. Smartcard-Unterstützung über Common Access Card (CAC) und Personal Identity Verification (PIV) sind ausschließlich über Amazon unter WorkSpaces Verwendung des WorkSpaces Streaming Protocol (WSP) verfügbar. Die Smartcard-Unterstützung auf WSP WorkSpaces bietet eine erhöhte Sicherheitslage für die Authentifizierung von Benutzern auf von der Organisation genehmigten Verbindungsendpunkten mit bestimmter Hardware in Form von Smartcard-Lesern. Es ist wichtig, sich zunächst mit dem Umfang der Unterstützung für Smartcards vertraut zu machen und zu bestimmen, wie Smartcards in bestehenden und zukünftigen WorkSpaces Bereitstellungen funktionieren würden.

Es ist eine bewährte Methode, zu bestimmen, welche Art von Smartcard-Unterstützung erforderlich ist: Authentifizierung vor der Sitzung oder Authentifizierung während der Sitzung. Die Authentifizierung vor der Sitzung ist nur zum Zeitpunkt dieses Schreibens in AWS GovCloud (USA-West), USA Ost (Nord-Virginia), USA West (Oregon), Europa (Irland), Asien-Pazifik (Tokio) und

Asien-Pazifik (Sydney) verfügbar. Die Smartcard-Authentifizierung während der Sitzung ist allgemein verfügbar und enthält einige Überlegungen, wie z. B.:

- Verfügt Ihre Organisation über eine Smartcard-Infrastruktur, die in Ihr Windows Active Directory integriert ist?
- Ist Ihr Online Certificate Status Protocol (OCSP) Responder Public Internet zugänglich?
- Werden Benutzerzertifikate mit User Principal Name (UPN) im Feld Subject Alternative Name (SAN) ausgestellt?
- Weitere Überlegungen finden Sie in den Abschnitten Sitzung und Vorsitzung.

Die Smartcard-Unterstützung wird über die Gruppenrichtlinie aktiviert. Es hat sich bewährt, die administrative Vorlage für Amazon WorkSpaces Group Policy für WSP zum zentralen Speicher Ihrer Active-Directory-Domain hinzuzufügen, die von Amazon WorkSpaces Directory(ies) verwendet wird. Wenn Sie diese Richtlinie auf eine vorhandene Amazon- WorkSpaces Bereitstellung anwenden, WorkSpaces erfordert alles die Aktualisierung der Gruppenrichtlinie und einen Neustart, damit die Änderung für alle Benutzer wirksam wird, da es sich um eine computerbasierte Richtlinie handelt.

Stammzertifizierungsstelle

Die Art der Portabilität von Amazon- WorkSpaces Client und -Benutzer erfordert die Notwendigkeit, das Stammzertifizierungsstellenzertifikat von Drittanbietern remote an den vertrauenswürdigen Stammzertifikatspeicher jedes Geräts zu übermitteln, das Benutzer für die Verbindung mit ihrem Amazon verwenden WorkSpaces. AD-Domain-Controller und Benutzergeräte mit Smartcards müssen den Root-CAs vertrauen. Lesen Sie die Richtlinien von Microsoft zur Aktivierung von Drittanbieter-CAs, um weitere Informationen zu den genauen Anforderungen zu erhalten.

In AD-Domain-verbundenen Umgebungen erfüllen diese Geräte diese Anforderung durch Gruppenrichtlinien, die Root-CA-Zertifikate verteilen. In Szenarien, in denen Amazon WorkSpaces Client von non-domain-joined Geräten verwendet wird, muss eine alternative Bereitstellungsmethode für die Root-CAs von Drittanbietern bestimmt werden, z. B. Intune .

Sitzung

Die Authentifizierung während der Sitzung vereinfacht und sichert die Anwendungsauthentifizierung, nachdem Amazon- WorkSpaces Benutzersitzungen bereits gestartet wurden. Wie bereits erwähnt, WorkSpaces deaktiviert das Standardverhalten für Amazon Smartcards und muss über

die Gruppenrichtlinie aktiviert werden. Aus Sicht der Amazon- WorkSpaces Verwaltung ist die Konfiguration speziell für Anwendungen erforderlich, die die Pass-Through-Authentifizierung (z. B. Webbrowser) durchlaufen. Für AD Connectors und Directory(s) sind keine Änderungen erforderlich.

Die gängigsten Anwendungen, die Authentifizierung während der Sitzung erfordern, sind Webbrowser wie Mozilla Firefox und Google Chrome. Mozilla Firefox erfordert eine eingeschränkte Konfiguration für die Smartcard-Unterstützung während der Sitzung. Amazon Linux WSP WorkSpaces erfordert eine zusätzliche Konfiguration für die Smartcard-Unterstützung während der Sitzung sowohl für Mozilla Firefox als auch für Google Chrome.

Es hat sich bewährt, sicherzustellen, dass die CAs vor der Fehlerbehebung in den persönlichen Zertifikatspeicher des Benutzers geladen werden, da der Amazon WorkSpaces Client möglicherweise keine Berechtigungen für den lokalen Computer hat. Verwenden Sie außerdem OpenSC, um Smartcard-Geräte zu identifizieren, wenn Sie bei der Authentifizierung bei Smartcards vermuten, dass es während der Sitzung zu Problemen kommt. Schließlich wird ein OCSP-Responder (Online Certificate Status Protocol) empfohlen, um den Sicherheitsstatus der Anwendungsauthentifizierung durch eine Zertifikatswiderrufsprüfung zu verbessern.

Vorsitzung

Für die Unterstützung der Authentifizierung vor der Sitzung ist Windows WorkSpaces Client Version 3.1.1 und höher oder macOS WorkSpaces Client Version 3.1.5 und höher erforderlich. Die Authentifizierung vor der Sitzung mit Smartcards unterscheidet sich grundsätzlich von der Standardauthentifizierung, sodass sich der Benutzer sowohl durch Einfügen der Smartcard als auch durch Eingabe eines PIN-Codes authentifizieren muss. Bei diesem Authentifizierungstyp ist die Dauer der Benutzersitzungen durch die Lebensdauer des Kerberos-Tickets begrenzt. Ein vollständiges Installationshandbuch finden Sie hier .

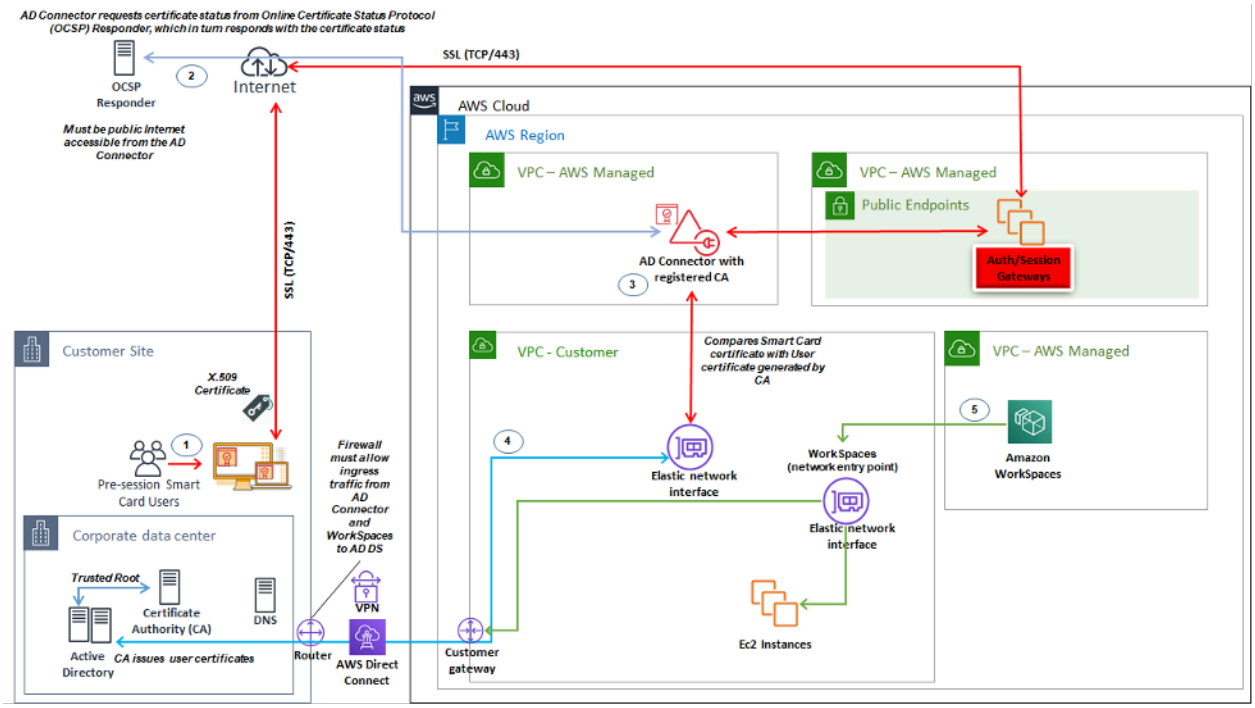


Abbildung 18: Übersicht über die Authentifizierung vor der Sitzung

1. Der Benutzer öffnet Amazon WorkSpaces Client, fügt eine Smartcard ein und gibt seine PIN ein. Die PIN wird von Amazon WorkSpaces Client verwendet, um das X.509-Zertifikat zu entschlüsseln, das dem AD Connector über das Authentication Gateway als Proxy zugestellt wird.
2. AD Connector validiert das X.509-Zertifikat anhand der öffentlich zugänglichen OCSP-Responder-URL, die in den Verzeichniseinstellungen angegeben ist, um sicherzustellen, dass das Zertifikat nicht widerrufen wurde.
3. Wenn das Zertifikat gültig ist, setzt der Amazon WorkSpaces Client den Authentifizierungsprozess fort, indem er den Benutzer auffordert, seine PIN ein zweites Mal einzugeben, um das X.509-Zertifikat und den Proxy für den AD Connector zu entschlüsseln, wo es dann zur Validierung mit den Stamm- und Zwischenzertifikaten des AD Connectors abgeglichen wird.
4. Sobald die Validierung des Zertifikats erfolgreich abgeglichen wurde, wird Active Directory vom AD Connector verwendet, um den Benutzer zu authentifizieren, und es wird ein Kerberos-Ticket erstellt.
5. Das Kerberos-Ticket wird zur Authentifizierung und WorkSpace zum Starten der WSP-Sitzung an Amazon des Benutzers übergeben.

OCSP Responder muss öffentlich zugänglich sein, da die Verbindung über das AWS verwaltete Netzwerk und nicht über das vom Kunden verwaltete Netzwerk hergestellt wird. Daher gibt es in diesem Schritt kein Routing zu privaten Netzwerken.

Die Eingabe des Benutzernamens ist nicht erforderlich, da die Benutzerzertifikate, die AD Connector vorgelegt werden, die userPrincipalName (UPN) des Benutzers im Feld subjectAltName (SAN) des Zertifikats enthalten. Es hat sich bewährt, alle Benutzer, die eine Authentifizierung vor der Sitzung mit Smartcards benötigen, zu automatisieren, ihre AD-Benutzerobjekte so zu aktualisieren, dass sie sich mit erwartetem UPN im Zertifikat mit authentifizieren PowerShell, anstatt dies einzeln in Microsoft-Managementkonsolen durchzuführen.

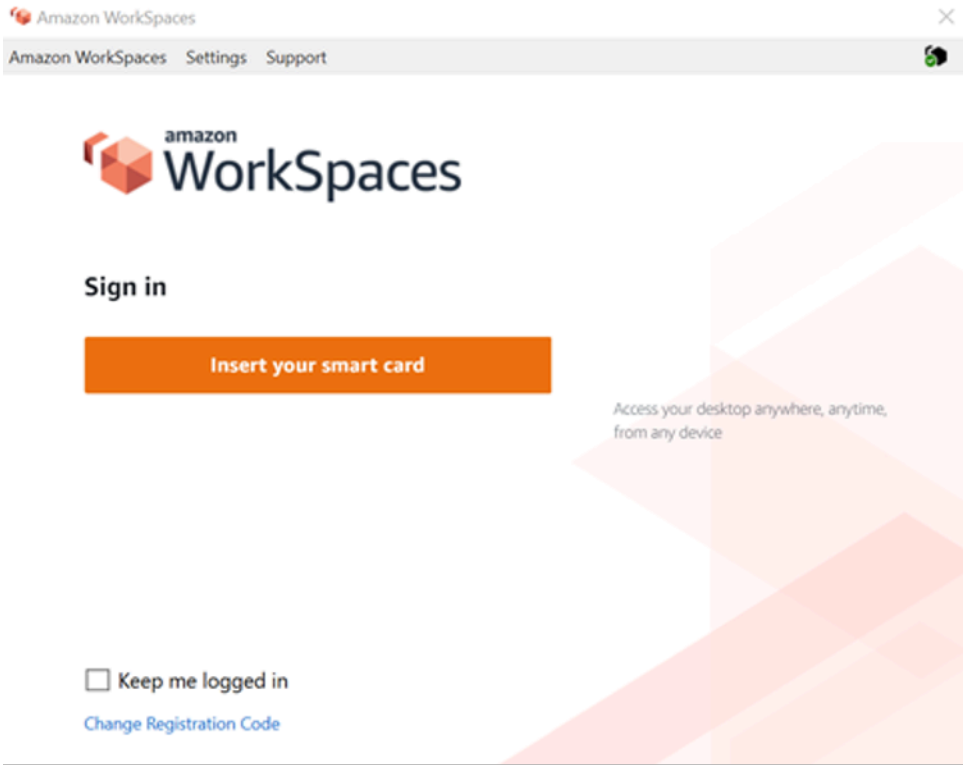


Abbildung 19: WorkSpaces Anmelden in der Konsole

Client-Bereitstellung

Der Amazon WorkSpaces Client (Version 3.X+) verwendet standardisierte Konfigurationsdateien, die von Administratoren zur Vorkonfiguration des WorkSpaces Clients ihres Benutzers genutzt werden können. Der Pfad für die beiden Hauptkonfigurationsdateien finden Sie unter:

BS	Pfad der Konfigurationsdatei
Windows	C:\Users\USERNAME\AppData\Local\Amazon Web Services\Amazon WorkSpaces
macOS	/Benutzer/USERNAME/Bibliothek/Anwendungsunterstützung/Amazon Web Services/Amazon WorkSpaces
Linux (Ubuntu 18.04)	/home/ubuntu/.local/share/Amazon Web Services/Amazon WorkSpaces/

Innerhalb dieser Pfade finden Sie die beiden Konfigurationsdateien. Die erste Konfigurationsdatei ist UserSettings.json, mit der Objekte wie aktuelle Registrierung, Proxy-Konfiguration, Protokollierungsebene und die Möglichkeit zum Speichern der Registrierungsliste festgelegt werden. Die zweite Konfigurationsdatei ist RegistrationList.json. Diese Datei enthält alle WorkSpaces Verzeichnisinformationen, die der Client verwenden soll, um dem richtigen WorkSpaces Verzeichnis zuzuordnen. Durch die Vorkonfiguration des RegistrationListJSON werden alle Registrierungscodes innerhalb des Clients für den Benutzer ausgefüllt.

> **Note**
>
> Wenn Ihre Benutzer WorkSpaces Client-Version 2.5.11 ausführen, wird proxy.cfg für Client-Proxy-Einstellungen verwendet und client_settings.ini legt die Protokollebene sowie die Möglichkeit zum Speichern der Registrierungsliste fest. Die Standard-Proxy-Einstellung verwendet das, was im Betriebssystem festgelegt ist.

Da diese Dateien standardisiert sind, können Administratoren den WorkSpaces Client herunterladen, alle zutreffenden Einstellungen festlegen und dann dieselben Konfigurationsdateien an alle Endbenutzer übertragen. Damit die Einstellungen wirksam werden, muss der Client gestartet werden, nachdem die neuen Konfigurationen festgelegt wurden. Wenn Sie die Konfiguration ändern, während der Client ausgeführt wird, wird keine der Änderungen innerhalb des Clients festgelegt.

Die letzte Einstellung, die für WorkSpaces Benutzer festgelegt werden kann, ist die automatische Aktualisierung des Windows-Clients. Dies wird nicht über Konfigurationsdateien gesteuert, sondern über die Windows-Registrierung. Wenn eine neue Version des Clients veröffentlicht

wird, können Sie einen Registrierungsschlüssel erstellen, um diese Version zu überspringen. Dies kann nicht durch Erstellen eines Zeichenfolgenregistrierungseintrags SkipThisVersion mit einem Wert der vollständigen Versionsnummer im folgenden Pfad festgelegt werden: Computer \HKEY_CURRENT_USER\Software\Amazon Web Services. microSD\Amazon WorkSpaces \WinSparkle Diese Option ist auch für macOS verfügbar. Die Konfiguration befindet sich jedoch in einer plist-Datei, für deren Bearbeitung eine spezielle Software erforderlich ist. Wenn Sie diese Aktion trotzdem ausführen möchten, können Sie dazu einen SUSkippedVersion-Eintrag in der Domäne com.amazon.workspaces hinzufügen, der sich unter befindet: /Users/USERNAME/Library/ Preferences

Amazon- WorkSpaces Endpunktauswahl

Auswählen eines Endpunkts für Ihr WorkSpaces

Amazon WorkSpaces bietet Unterstützung für mehrere Endpunktgeräte, von Windows-Desktops bis hin zu iPads und Chromebooks. Sie können die verfügbaren Amazon- WorkSpaces Clients von der Amazon Workspaces-Website herunterladen. Die Auswahl des richtigen Endpunkts für Ihre Benutzer ist eine wichtige Entscheidung. Wenn Ihre Benutzer die Verwendung von bidirektionalem Audio/ Video benötigen und das WorkSpaces Streaming-Protokoll verwenden, müssen sie den Windows- oder macOS-Client verwenden. Stellen Sie für alle Clients sicher, dass die IP-Adressen und Ports, die unter IP-Adresse und Port-Anforderungen für Amazon WorkSpaces aufgeführt sind, explizit konfiguriert wurden, um sicherzustellen, dass der Client eine Verbindung zum Service herstellen kann. Hier sind einige zusätzliche Überlegungen, die Ihnen bei der Auswahl eines Endpunktgeräts helfen:

- Windows – Um den Windows-Amazon- WorkSpaces Client verwenden zu können, muss der 4.x-Client den 64-Bit-Microsoft-Windows-8.1-, Windows-10-Desktop ausführen. Benutzer können den Client nur für ihr Benutzerprofil ohne Administratorrechte auf dem lokalen Computer installieren. Systemadministratoren können den Client mit Gruppenrichtlinien, Microsoft Endpoint Manager Configuration Manager (MEMCM) oder anderen Tools zur Anwendungsbereitstellung, die in einer Umgebung verwendet werden, auf verwalteten Endpunkten bereitstellen. Der Windows-Client unterstützt maximal vier Displays und eine maximale Auflösung von 3840x2160.
- macOS – Um den neuesten macOS-Amazon- WorkSpaces Client bereitzustellen, müssen macOS-Geräte macOS 10.12 (Sierra) oder höher ausführen. Sie können eine ältere Version des WorkSpaces Clients bereitstellen, um eine Verbindung zu PCoIP herzustellen WorkSpaces , wenn auf dem Endpunkt OSX 10.8.1 oder höher ausgeführt wird. Der macOS-Client unterstützt bis zu zwei Monitore mit 4K-Auflösung oder vier Monitore mit WUXGA-Auflösung (1920 x 1200).

- Linux – Der Amazon WorkSpaces -Linux-Client benötigt 64-Bit-Ubuntu 18.04 (AMD64), um ausgeführt zu werden. Wenn Ihre Linux-Endpunkte diese Betriebssystemversion nicht ausführen, wird der Linux-Client nicht unterstützt. Bevor Sie Linux-Clients bereitstellen oder Benutzern ihren Registrierungscode zur Verfügung stellen, stellen Sie sicher, dass Sie den Linux-Clientzugriff auf Verzeichnisebene aktivieren, da dies standardmäßig deaktiviert ist und Benutzer erst dann eine Verbindung von Linux-Clients herstellen können, wenn er aktiviert ist. WorkSpaces Der Linux-Client unterstützt bis zu zwei Monitore mit 4K-Auflösung oder vier Monitore mit WUXGA-Auflösung (1920 x 1200).
- iPad – Die Amazon WorkSpaces iPad-Clientanwendung unterstützt PCoIP WorkSpaces. Die unterstützten iPads sind iPad2 oder höher mit iOS 8.0 oder höher, iPad Retina mit iOS 8.0 und höher, iPad Mini mit iOS 8.0 und höher und iPad Pro mit iOS 9.0 und höher. Stellen Sie sicher, dass das Gerät, von dem aus die Benutzer eine Verbindung herstellen, diese Kriterien erfüllt. Die iPad-Clientanwendung unterstützt viele verschiedene Formen. (Weitere Informationen finden Sie in einer vollständigen Liste der unterstützten Trichter.) Die Amazon WorkSpaces iPad-Clientanwendung unterstützt auch die Swiftpoint GT ProPoint, und - PadPoint Machbarkeit. Die Swiftpoint-TRACPOINT PenPoint - und - GoPoint Matken werden nicht unterstützt.
- Android/Chromebook – Wenn Sie ein Android-Gerät oder Chromebook als Endpunkt für Ihre Endbenutzer bereitstellen möchten, müssen einige Überlegungen berücksichtigt werden. Stellen Sie sicher, dass WorkSpaces die Benutzer eine Verbindung zu PCoIP WorkSpaces herstellen, da dieser Client nur PCoIP WorkSpaces unterstützt. Dieser Client unterstützt nur eine einzige Anzeige. Wenn Benutzer Multi-Monitor-Unterstützung benötigen, verwenden Sie einen anderen Endpunkt. Wenn Sie ein Chromebook bereitstellen möchten, stellen Sie sicher, dass das bereitgestellte Modell die Installation von Android-Anwendungen unterstützt. Die vollständige Funktionsunterstützung wird nur auf dem Android-Client und nicht auf dem Legacy-Chromebook-Client unterstützt. Dies ist in der Regel nur eine Überlegung für Chromebooks, die vor 2019 erstellt wurden. Android-Unterstützung wird sowohl für Tablets als auch für Mobiltelefone bereitgestellt, solange auf Android OS 4.4 und höher ausgeführt wird. Es wird jedoch empfohlen, dass das Android-Gerät OS 9 oder höher ausführt, um den neuesten WorkSpace Android-Client zu verwenden. Wenn auf Ihren Chromebooks die WorkSpaces Client-Version 3.0.1 oder höher ausgeführt wird, können Ihre Benutzer jetzt die Self-Service-WorkSpaces Funktionen nutzen. Darüber hinaus können Sie als Administrator Zertifikate für vertrauenswürdige Geräte verwenden, um den WorkSpaces Zugriff auf vertrauenswürdige Geräte mit gültigen Zertifikaten einzuschränken.
- Webzugriff – Benutzer können über einen Webbrowser von jedem Standort WorkSpaces aus auf ihr Windows zugreifen. Dies ist ideal für Benutzer, die ein gesperrtes Gerät oder ein restriktives Netzwerk verwenden müssen. Statt eine herkömmliche Remote-Zugriffslösung zu verwenden und

die entsprechende Client-Anwendung zu installieren, können Benutzer über die Website auf ihre Arbeitsressourcen zugreifen. Benutzer können den WorkSpaces Webzugriff verwenden, um eine Verbindung zu non-graphics-based Windows PCoIP WorkSpaces herzustellen, auf dem Windows 10 oder Windows Server 2016 mit Desktop-Erfahrung ausgeführt wird. Benutzer müssen eine Verbindung mit Chrome 53 oder höher oder Firefox 49 oder höher herstellen. Für WSP-basierte können Benutzer den WorkSpaces Webzugriff verwenden WorkSpaces, um eine Verbindung zu nicht-grafischen Windows-basierten herzustellen WorkSpaces. Diese Benutzer müssen eine Verbindung mit Microsoft Edge 91 oder höher oder Google Chrome 91 oder höher herstellen. Die minimal unterstützte Bildschirmauflösung beträgt 960 x 720 mit einer maximal unterstützten Auflösung von 2560 x 1600. Mehrere Monitore werden nicht unterstützt. Für ein optimales Benutzererlebnis wird nach Möglichkeit empfohlen, dass Benutzer eine Betriebssystemversion des Clients verwenden.

- PCoIP Zero Client – Sie können PCoIP-Zero-Clients für Endbenutzer bereitstellen, denen PCoIP WorkSpaces zugewiesen ist oder denen PCoIP zugewiesen wird. Der Tera2-Zero-Client muss über eine Firmware-Version von 6.0.0 oder höher verfügen, um eine direkte Verbindung mit dem herzustellen WorkSpace. Um die Multi-Faktor-Authentifizierung mit Amazon verwenden zu können WorkSpaces, muss das Tera2-Zero-Client-Gerät Firmware-Version 6.0.0 oder höher ausführen. Support und Fehlerbehebung für die Zero-Client-Hardware sollten Sie beim Hersteller durchführen.
- I OS – Sie können I OS auf Endpunktgeräten verwenden, um eine Verbindung zu PCoIP basierend auf herzustellen WorkSpaces , solange die Firmwareversion 11.04.280 oder höher ist. Die unterstützten Funktionen entsprechen heute denen des vorhandenen Linux-Clients. Bevor Sie I OS-Clients bereitstellen oder Benutzern ihren Registrierungscode zur Verfügung stellen, stellen Sie sicher, dass Sie den Linux-Clientzugriff auf WorkSpaces Verzeichnisebene aktivieren, da dies standardmäßig deaktiviert ist und Benutzer erst dann eine Verbindung von I OS-Clients herstellen können, wenn er aktiviert ist. Der I OS-Client unterstützt bis zu zwei Monitore mit 4K-Auflösung oder vier Monitore mit WUXGA-Auflösung (1920x1200).

Web-Zugriffsclient

Der Web-Access-Client ist für gesperrte Geräte konzipiert und bietet Zugriff auf Amazon, WorkSpaces ohne dass Clientsoftware bereitgestellt werden muss. Der Web-Access-Client wird nur in Einstellungen empfohlen, in denen es sich bei Amazon um ein Windows-Betriebssystem (OS) WorkSpaces handelt, und die für begrenzte Benutzerworkflows verwendet werden, z. B. für eine Freiraumumgebung. Die meisten Anwendungsfälle profitieren von dem Funktionssatz, der vom Amazon- WorkSpaces Client verfügbar ist. Der Web-Access-Client wird nur in bestimmten

Anwendungsfällen empfohlen, in denen Geräte und Netzwerkeinschränkungen eine alternative Verbindungsmethode erfordern.

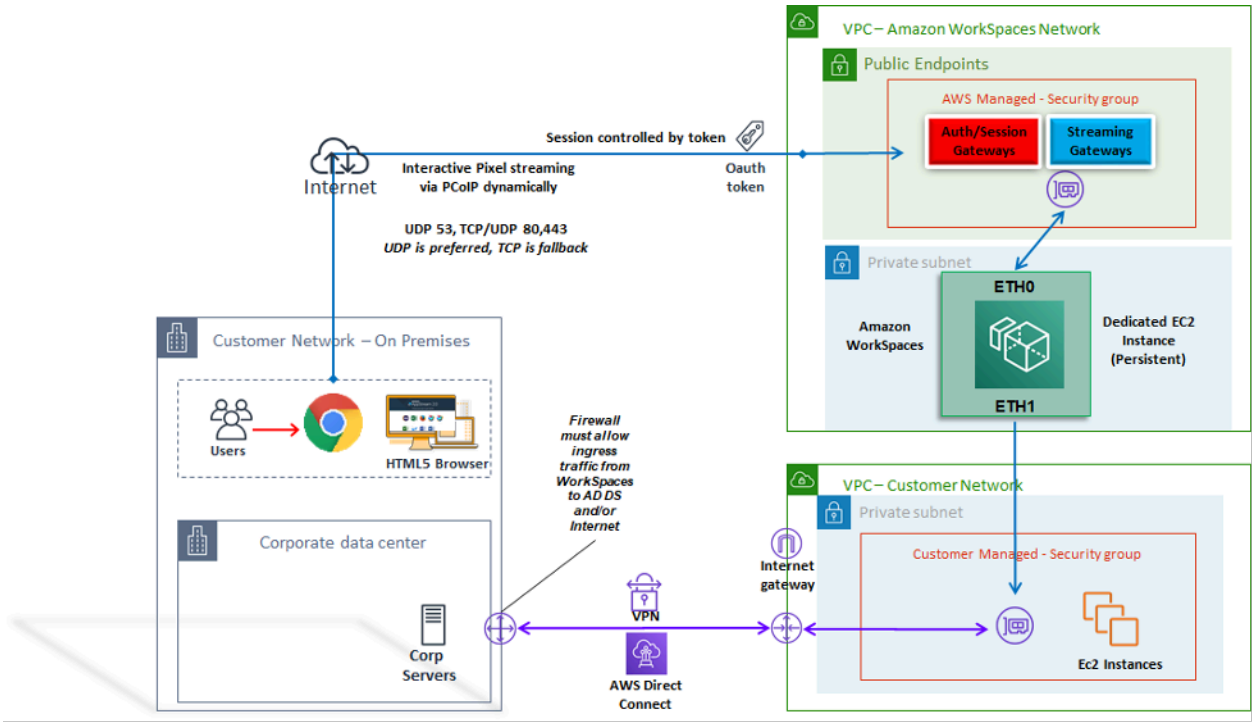


Abbildung 20: Web-Access-Client-Architektur

Wie im Diagramm gezeigt, hat der Web-Access-Client unterschiedliche Netzwerkanforderungen, um die Sitzung an Benutzer zu streamen. Web Access ist für Windows entweder WorkSpaces über das PCoIP- oder das WSP-Protokoll verfügbar. DNS und HTTP/HTTPS sind für die Authentifizierung und Registrierung bei den WorkSpaces Gateways erforderlich. Für die WorkSpaces Verwendung des WSP-Protokolls muss die direkte Verbindung von UDP/TCP 4195 zu den IP-Adressbereichen des WSP-Gateways geöffnet werden. Streaming-Datenverkehr wird keinem festen Port zugewiesen, wie er mit dem vollständigen Amazon- WorkSpaces Client ist. Stattdessen wird er dynamisch zugewiesen. UDP ist für Streaming-Datenverkehr vorzuziehen. Der Webbrowser greift jedoch auf TCP zurück, wenn UDP eingeschränkt ist. In Umgebungen, in denen TCP/UDP-Port 4172 blockiert ist und aufgrund organisatorischer Einschränkungen nicht entsperrt werden kann, bietet der Web-Access-Client eine alternative Verbindungsmethode für Benutzer.

Standardmäßig ist der Web-Access-Client auf Verzeichnisebene deaktiviert. Um Benutzern den Zugriff auf ihr Amazon WorkSpaces über einen Webbrowser zu ermöglichen, verwenden Sie entweder die , AWS Management Console um die Verzeichniseinstellungen zu aktualisieren, oder verwenden Sie programmgesteuert die -WorkspaceAccessProperties API, um zu Zulassen

DeviceTypeWeb zu ändern. Darüber hinaus muss der Administrator sicherstellen, dass die Gruppenrichtlinieneinstellungen nicht mit den Anmeldeanforderungen in Konflikt stehen.

Amazon- WorkSpaces Tags

```
Tags enable you to associate metadata with AWS resources. Tags can be used with Amazon
 WorkSpaces to registered directories,
  bundles, IP Access Control Groups, or images. Tags assist with cost allocation to
 internal cost centers. Before using tags with Amazon WorkSpaces,
  refer to the Tagging Best Practices whitepaper.

Tag restrictions
```

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 127 Unicode-Zeichen
- Maximale Wertlänge: 255 Unicode-Zeichen
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = _ : / @. Verwenden Sie keine führenden oder nachgestellten Leerzeichen.
- Verwenden Sie nicht die Präfixe aws: oder aws:workspaces: in Ihren Tag-Namen oder -Werten, da sie für die AWS Verwendung reserviert sind. Tag-Namen oder Werte mit diesen Präfixen können nicht bearbeitet oder gelöscht werden.

Ressourcen, die Sie markieren können

- Sie können Tags zu den folgenden Ressourcen hinzufügen, wenn Sie sie erstellen: WorkSpaces, importierte Images und IP-Zugriffskontrollgruppen.
- Sie können Tags zu vorhandenen Ressourcen der folgenden Typen hinzufügen: WorkSpaces, registrierte Verzeichnisse, benutzerdefinierte Pakete, Images und IP-Zugriffskontrollgruppen.

  Verwenden des Kostenzuordnungs-Tags

Um Ihre WorkSpaces Ressourcen-Tags im Cost Explorer anzuzeigen, aktivieren Sie die Tags, die Sie auf Ihre WorkSpaces Ressourcen angewendet haben, indem Sie den Anweisungen unter

Aktivieren benutzerdefinierter Kostenzuordnungs-Tags im Benutzerhandbuch für AWS Billing and Cost Management und Kostenmanagement folgen.

Obwohl Tags 24 Stunden nach der Aktivierung angezeigt werden, kann es vier bis fünf Tage dauern, bis Werte, die diesen Tags zugeordnet sind, im Cost Explorer angezeigt werden. Um Kostendaten in Cost Explorer anzuzeigen und bereitzustellen, müssen WorkSpaces für Ressourcen, die markiert wurden, während dieser Zeit Gebühren anfallen. Cost Explorer zeigt nur Kostendaten aus dem Zeitpunkt an, an dem die Tags vorwärts aktiviert wurden. Derzeit sind keine Verlaufsdaten verfügbar.

Verwalten von Tags

Um die Tags für eine vorhandene Ressource mit der zu aktualisieren AWS CLI, verwenden Sie die Befehle create-tags und delete-tags. Für Massenaktualisierungen und zur Automatisierung der Aufgabe für eine große Anzahl von WorkSpaces Ressourcen bietet Amazon WorkSpaces Unterstützung für AWS Resource Groups Tag Editor. AWS Resource Groups Tag Editor ermöglicht Ihnen das Hinzufügen, Bearbeiten oder Löschen von AWS Tags aus Ihrem WorkSpaces zusammen mit Ihren anderen AWS Ressourcen.

Amazon WorkSpaces -Servicekontingente

Service Quotas erleichtern die Suche nach dem Wert eines bestimmten Kontingents, auch als Limit bezeichnet. Sie können auch alle Kontingente für einen bestimmten Service nachschlagen.

So zeigen Sie Ihre Kontingente für an WorkSpaces

1. Navigieren Sie zur Service Quotas-Konsole .
2. Wählen Sie im linken Navigationsbereich AWS Services aus.
3. Wählen Sie Amazon WorkSpaces aus der Liste aus oder geben Sie Amazon WorkSpaces in das Type-Ahead-Suchfeld ein.
4. Um zusätzliche Informationen zu einem Kontingent anzuzeigen, z. B. seine Beschreibung und den Amazon-Ressourcennamen (ARN), wählen Sie den Kontingentnamen aus.

Amazon WorkSpaces stellt verschiedene Ressourcen bereit, die Sie in Ihrem Konto in einer bestimmten Region verwenden können, darunter WorkSpaces, Images, Pakete, Verzeichnisse, Verbindungsaliase und IP-Kontrollgruppen. Wenn Sie Ihr Amazon Web Services-Konto erstellen, werden Standardkontingente (auch als Limits bezeichnet) für die Anzahl der Ressourcen festgelegt, die Sie erstellen können.

Sie können die Service Quotas-Konsole verwenden, um die Standard-Service Quotas anzuzeigen oder Kontingenterhöhungen für anpassbare Kontingente anzufordern.

Weitere Informationen finden Sie unter Anzeigen von Service Quotas und Anfordern einer Kontingenterhöhung im Benutzerhandbuch für Service Quotas.

Automatisieren der Amazon- WorkSpaces Bereitstellung

Mit Amazon können WorkSpacesSie innerhalb weniger Minuten einen Microsoft-Windows- oder Amazon-Linux-Desktop starten und sich von On-Premises- oder einem externen Netzwerk sicher, zuverlässig und schnell mit Ihrer Desktop-Software verbinden und darauf zugreifen. Sie können die Bereitstellung von Amazon automatisieren WorkSpaces , damit Sie Amazon WorkSpaces in Ihre vorhandenen Bereitstellungsworkflows integrieren können.

Allgemeine WorkSpaces Automatisierungsmethoden

Kunden können eine Reihe von Tools verwenden, um eine schnelle Amazon- WorkSpaces Bereitstellung zu ermöglichen. Die Tools können verwendet werden, um die Verwaltung von zu vereinfachen WorkSpaces, Kosten zu senken und eine agile Umgebung zu ermöglichen, die schnell skaliert und verschoben werden kann.

AWS CLI und API

Es gibt Amazon WorkSpaces -API-Operationen, mit denen Sie sicher und skalierbar mit dem Service interagieren können. Alle öffentlichen APIs sind mit dem AWS CLI SDK und Tools für verfügbar PowerShell, während private APIs wie die Image-Erstellung nur über die verfügbar sind AWS Management Console. Berücksichtigen Sie bei der Berücksichtigung von Betriebsmanagement und Business Self-Service für Amazon WorkSpaces, dass WorkSpaces APIs technisches Fachwissen und Sicherheitsberechtigungen erfordern.

API-Aufrufe können mit dem AWS SDK erfolgen. AWS Tools for Windows PowerShell und AWS Tools for PowerShell Core sind PowerShell Module, die auf Funktionen basieren, die vom AWS SDK for .NET bereitgestellt werden. Mit diesen Modulen können Sie Skriptoperationen für AWS Ressourcen über die PowerShell Befehlszeile erstellen und in vorhandene Tools und Services integrieren. API-Aufrufe können es Ihnen beispielsweise ermöglichen, den WorkSpaces Lebenszyklus automatisch zu verwalten, indem Sie in AD integrieren, um WorkSpaces basierend auf der AD-Gruppenmitgliedschaft eines Benutzers Bereitstellung und Außerbetriebnahme durchzuführen.

AWS CloudFormation

AWS CloudFormation Mit können Sie Ihre gesamte Infrastruktur in einer Textdatei modellieren. Diese Vorlage wird zur einzigen Informationsquelle für Ihre Infrastruktur. Auf diese Weise können Sie Infrastrukturkomponenten standardisieren, die in Ihrer gesamten Organisation verwendet werden, was die Compliance von Konfigurationen und eine schnellere Fehlerbehebung ermöglicht.

AWS CloudFormation stellt Ihre Ressourcen sicher und wiederholbar bereit, sodass Sie Ihre Infrastruktur und Anwendungen aufbauen und neu erstellen können. Sie können verwenden, CloudFormation um Umgebungen in Betrieb zu nehmen und außer Betrieb zu nehmen, was nützlich ist, wenn Sie eine Reihe von Konten haben, die Sie wiederholbar erstellen und außer Betrieb nehmen möchten. Berücksichtigen Sie bei der Berücksichtigung von Betriebsmanagement und Business Self-Service für Amazon WorkSpaces, dass AWS CloudFormation technisches Fachwissen und Sicherheitsberechtigungen erfordert.

Self-Service- WorkSpaces Portal

Kunden können Build-on WorkSpaces -API-Befehle und andere - AWS Services verwenden, um ein WorkSpaces Self-Service-Portal zu erstellen. Dies hilft Kunden dabei, den Prozess zur Bereitstellung und Rückforderung WorkSpaces in großem Umfang zu optimieren. Mithilfe eines WorkSpaces Portals können Sie es Ihren Mitarbeitern ermöglichen, ihre eigenen WorkSpaces mit einem integrierten Genehmigungsworkflow bereitzustellen, für den kein IT-Eingreifen für jede Anfrage erforderlich ist. Dadurch werden die IT-Betriebskosten gesenkt und Endbenutzer können WorkSpaces schneller mit beginnen. Der zusätzliche integrierte Genehmigungsworkflow vereinfacht den Desktop-Genehmigungsprozess für Unternehmen. Ein dediziertes Portal kann ein automatisiertes Tool für die Bereitstellung von Windows- oder Linux-Cloud-Desktops bieten und es Benutzern ermöglichen, ihre neu zu erstellen, neu zu starten oder zu migrieren WorkSpace, sowie eine Möglichkeit zum Zurücksetzen von Passwörtern bereitzustellen.

Es gibt geführte Beispiele für die Erstellung von Self-Service- WorkSpaces Portalen, auf die im Abschnitt Weitere Lesungen dieses Dokuments verwiesen wird. AWS Partner stellen vorkonfigurierte WorkSpaces Verwaltungsportale über die bereitAWS Marketplace.

Integration mit Enterprise IT Service Management

Wenn Unternehmen Amazon WorkSpaces als virtuelle Desktop-Lösung in großem Umfang einsetzen, müssen IT Service Management (ITSM)-Systeme implementiert oder in diese integriert werden. Die ITSM-Integration ermöglicht Self-Service-Angebote für Bereitstellung und Betrieb.

Mit dem Service Catalog können Sie häufig bereitgestellte AWS Services und bereitgestellte Softwareprodukte zentral verwalten. Dieser Service hilft Ihrer Organisation dabei, konsistente Governance- und Compliance-Anforderungen zu erfüllen und gleichzeitig Benutzern zu ermöglichen, nur die genehmigten AWS Services bereitzustellen, die sie benötigen. Der Service Catalog kann verwendet werden, um ein Self-Service-Lebenszyklusmanagement-Angebot für Amazon WorkSpaces aus IT-Service-Management-Tools wie zu aktivierenServiceNow.

WorkSpaces Bewährte Methoden für die Bereitstellungsautomatisierung

Sie sollten Well Architected-Prinzipien bei der Auswahl und Gestaltung der WorkSpaces Bereitstellungsautomatisierung berücksichtigen.

- Design für Automatisierung – Design, um den geringstmöglichen manuellen Eingriff in den Prozess zu ermöglichen, um Wiederholbarkeit und Skalierung zu ermöglichen.
- Entwurf für Kostenoptimierung – Durch die automatische Erstellung und Rückgewinn von können Sie den Verwaltungsaufwand reduzieren WorkSpaces, der erforderlich ist, um Ressourcen bereitzustellen und ungenutzte oder ungenutzte Ressourcen zu entfernen, um unnötige Kosten zu verursachen.
- Design zur Effizienz – Minimieren Sie die Ressourcen, die zum Erstellen und Beenden von benötigt werden WorkSpaces. Stellen Sie nach Möglichkeit Tier-0-Self-Service-Funktionen für das Unternehmen bereit, um die Effizienz zu verbessern.
- Design für Flexibilität – Erstellen Sie einen konsistenten Bereitstellungsmechanismus, der mehrere Szenarien verarbeiten kann und mit demselben Mechanismus skaliert werden kann (angepasst mit getaggten Anwendungsfällen und Profilkennungen).
- Entwurf für Telefonie – Entwerfen Sie Ihre - WorkSpaces Operationen so, dass die richtige Autorisierung und Validierung zum Hinzufügen oder Entfernen von Ressourcen möglich ist.
- Design für Skalierbarkeit – Das pay-as-you Go-Modell, das Amazon WorkSpaces verwendet, kann zu Kosteneinsparungen führen, indem Ressourcen nach Bedarf erstellt und entfernt werden, wenn sie nicht mehr benötigt werden.
- Design für Sicherheit – Entwerfen Sie Ihre - WorkSpaces Operationen so, dass die richtige Autorisierung und Validierung zum Hinzufügen oder Entfernen von Ressourcen möglich ist.
- Design für Supportfähigkeit – Entwerfen Sie Ihre WorkSpaces -Operationen so, dass sie Mechanismen und Prozesse für Nicht- Support und Wiederherstellung ermöglichen.

Amazon- WorkSpaces Patching und direkte Upgrades

Mit Amazon können WorkSpacesSie Patches und Updates mit vorhandenen Tools von Drittanbietern wie Microsoft System Center Configuration Manager (SCCM), Puppet Enterprise oder Ansible verwalten. Die direkte Bereitstellung von Sicherheitspatches unterhält in der Regel einen monatlichen Patch-Zyklus mit zusätzlichen Prozessen für die Eskalation oder schnelle Bereitstellung. Im Falle von direkten Betriebssystem-Upgrades oder Feature-Updates sind jedoch oft besondere Überlegungen erforderlich.

WorkSpace Wartung

Amazon WorkSpaces verfügt über ein Standard-Wartungsfenster, in dem Amazon- WorkSpaces Agent-Updates und alle verfügbaren Betriebssystem-Updates WorkSpace installiert. WorkSpaces ist während des geplanten Wartungsfensters nicht für Benutzerverbindungen verfügbar.

- AlwaysOn WorkSpaces Das Standard-Wartungsfenster ist 00:00 bis 04:00 Uhr in der Zeitzone des WorkSpace, jeden Sonntagmorgen.

- Die Zeitzonenumleitung ist standardmäßig aktiviert und kann das Standardfenster so überschreiben, dass es der lokalen Zeitzone des Benutzers entspricht.
- Sie können die Zeitzonenumleitung für Windows mithilfe von Gruppenrichtlinien deaktivieren WorkSpaces. Sie können die Zeitzonenumleitung für Linux deaktivieren WorkSpaces, indem Sie die PCoIP-Agent-Konfiguration verwenden.

- AutoStop WorkSpaces werden einmal im Monat automatisch gestartet, um wichtige Updates zu installieren. Ab dem dritten Montag des Monats und für bis zu zwei Wochen ist das Wartungsfenster jeden Tag von etwa 00:00 bis 05:00 Uhr in der Zeitzone der AWS Region für die geöffnet WorkSpace. kann an einem beliebigen Tag im Wartungsfenster gewartet WorkSpace werden.

- Obwohl Sie die Zeitzone, die für die Wartung von verwendet wird, nicht ändern können AutoStop WorkSpaces, können Sie das Wartungsfenster für Ihr deaktivieren AutoStop WorkSpaces.

- Manuelle Wartungsfenster können basierend auf Ihrem bevorzugten Zeitplan festgelegt werden, indem Sie den Status von WorkSpace auf ADMIN_MAINTENANCE setzen.

- Der AWS CLI Befehl modify-workspace-state kann verwendet werden, um den WorkSpace Status in ADMIN_MAINTENANCE zu ändern.

Amazon Linux WorkSpaces

Überlegungen, Voraussetzungen und vorgeschlagene Muster für die Verwaltung von Updates und Patches auf WorkSpaces benutzerdefinierten Amazon-Linux-Images finden Sie im Whitepaper Bewährte Methoden zur Vorbereitung Ihrer Amazon- WorkSpaces für-Linux-Images.

Linux-Patching-Voraussetzungen und -Überlegungen

- Amazon Linux-Repositorys werden in Amazon Simple Storage Service (Amazon S3)-Buckets gehostet, auf die über öffentliche, über das Internet zugängliche Endpunkte oder private Endpunkte zugegriffen werden kann. Wenn Ihr Amazon Linux WorkSpaces keinen Internetzugang hat, lesen Sie bitte diesen Prozess, um Updates zugänglich zu machen: Wie kann ich yum aktualisieren oder Pakete ohne Internetzugang auf meinen EC2-Instances installieren, auf denen Amazon Linux 1 oder Amazon Linux 2 ausgeführt wird?
- Sie können das Standard-Wartungsfenster für Linux nicht konfigurieren WorkSpaces. Wenn eine Anpassung dieses Fensters erforderlich ist, kann der manuelle Wartungsvorgang verwendet werden.

Amazon-Windows-Patching

Standardmäßig WorkSpaces ist Ihr Windows so konfiguriert, dass Updates von Windows Update empfangen werden, die Internetzugriff von Ihrer WorkSpaces VPC erfordern. Informationen zum Konfigurieren Ihrer eigenen Mechanismen für automatische Updates für Windows finden Sie in der Dokumentation für Windows Server Update Services (WSUS) und Configuration Manager .

Direktes Upgrade für Amazon Windows

- Wenn Sie ein Image aus einem Windows 10 erstellen möchten WorkSpace, beachten Sie, dass die Image-Erstellung auf Windows 10-Systemen, die von einer früheren Version aktualisiert wurden (einem Windows-Feature/Versions-Upgrade), nicht unterstützt wird. Kumulative Windows- oder Sicherheitsupdates werden jedoch vom Prozess der WorkSpaces Image-Erstellung und -Erfassung unterstützt.

- Benutzerdefinierte Abbilder für Windows 10 Bring Your Own License (BYOL) sollten mit der aktuell unterstützten Version von Windows auf einer VM als Quelle für den BYOL-Importprozess beginnen: Weitere Informationen finden Sie in der BYOL-Importdokumentation.

Voraussetzungen für das direkte Upgrade von Windows

- Wenn Sie Windows-10-Upgrades mithilfe der Active-Directory-Gruppenrichtlinie oder SCCM verschoben oder angehalten haben, aktivieren Sie Betriebssystem-Upgrades für Ihr Windows 10 WorkSpaces.
- Wenn die ein WorkSpace ist AutoStop WorkSpace, ändern Sie die AutoStop Zeit auf mindestens drei Stunden, um das Upgrade-Fenster zu berücksichtigen.
- Beim direkten Upgrade-Prozess wird das Benutzerprofil neu erstellt, indem eine Kopie des Standardbenutzers erstellt wird (C:\Users\Default). Verwenden Sie nicht das Standardbenutzerprofil, um Anpassungen vorzunehmen. Es wird empfohlen, stattdessen Anpassungen am Benutzerprofil über Gruppenrichtlinienobjekte (GPOs) vorzunehmen. Über GPOs vorgenommene Anpassungen können einfach geändert oder rückgängig gemacht werden und sind weniger anfällig für Fehler.
- Beim In-Place-Upgradeprozess kann nur ein Benutzerprofil gesichert und neu erstellt werden. Wenn Sie mehrere Benutzerprofile auf Laufwerk D haben, löschen Sie alle Profile mit Ausnahme des Profils, das Sie benötigen.

Überlegungen zum direkten Upgrade von Windows

- Der direkte Upgrade-Prozess verwendet zwei Registrierungsskripts (enable-inplace-upgrade.ps1 und update-pvdrivers.ps1), um die erforderlichen Änderungen an Ihrem vorzunehmen WorkSpaces und die Ausführung des Windows Update-Prozesses zu ermöglichen. Diese Änderungen beinhalten das Erstellen eines temporären Benutzerprofils auf Laufwerk C anstelle von Laufwerk D. Wenn ein Benutzerprofil bereits auf Laufwerk D vorhanden ist, verbleiben die Daten in diesem ursprünglichen Benutzerprofil auf Laufwerk D.
- Sobald das direkte Upgrade bereitgestellt wurde, müssen Sie die Benutzerprofile auf dem Laufwerk D wiederherstellen, um sicherzustellen, dass Sie Ihr neu erstellen oder migrieren können WorkSpaces, und um potenzielle Probleme mit der Umleitung von Benutzer-Shell-Ordnern zu vermeiden. Sie können dies tun, indem Sie den PostUpgradeRestoreProfileOnD-Registrierungsschlüssel verwenden, wie auf der BYOL-Upgrade-Referenzseite beschrieben.

Amazon WorkSpaces -Sprachpakete

Amazon- WorkSpaces Pakete, die das Windows-10-Desktop-Erlebnis bieten, unterstützen Englisch (USA), Französisch (Canadisch), Koreanisch und Japanisch. Sie können jedoch zusätzliche Sprachpakete für Spanisch, Italienisch, Portugiesisch und viele weitere Sprachoptionen hinzufügen. Weitere Informationen finden Sie unter Wie erstelle ich ein neues Windows- WorkSpace Image mit einer anderen Clientsprache als Englisch?.

Amazon- WorkSpaces Profilverwaltung

Amazon WorkSpaces trennt das Benutzerprofil vom Basisbetriebssystem (OS), indem alle Profilschreibvorgänge auf ein separates Amazon Elastic Block Store (Amazon EBS)-Volume umgeleitet werden. In Microsoft Windows wird das Benutzerprofil in D:\Users\username gespeichert. In Amazon Linux wird das Benutzerprofil in /home gespeichert. Das EBS-Volume wird automatisch alle 12 Stunden erstellt. Der Snapshot wird automatisch in einem von AWS verwalteten S3-Bucket gespeichert, der für den Fall verwendet wird, dass ein Amazon neu erstellt oder wiederhergestellt WorkSpace wird.

Für die meisten Organisationen ist das Vorhandensein automatischer Snapshots alle 12 Stunden gegenüber der vorhandenen Desktop-Bereitstellung ohne Backups für Benutzerprofile überlegen. Kunden können jedoch eine genauere Kontrolle über Benutzerprofile benötigen, z. B. Migration vom Desktop zu WorkSpaces, zu einem neuen Betriebssystem/einer neuen AWS Region, Unterstützung für DR usw. Für Amazon sind alternative Methoden für die Profilverwaltung verfügbar WorkSpaces.

Ordnerumleitung

Die Ordnerumleitung ist zwar ein gängiges Designüberlegung bei Architekturen der virtuellen Desktop-Infrastruktur (VDI), ist jedoch weder eine bewährte Methode noch sogar eine gängige Anforderung in Amazon- WorkSpaces Designs. Der Grund dafür ist, dass Amazon WorkSpaces eine persistente Lösung für Desktop as a Service (DaaS) ist, bei der Anwendungs- und Benutzerdaten standardmäßig erhalten bleiben.

Es gibt bestimmte Szenarien, in denen die Ordnerumleitung für Benutzer-Shell-Ordner (z. B. D:\Users\username\Desktop, die an \\Server\RedirectionShare$\username\Desktop umgeleitet werden) erforderlich ist, z. B. sofortiges Recovery Point Objective (RPO) für Benutzerprofildaten in Notfallwiederherstellungsumgebungen (DR).

Bewährte Methoden

Die folgenden bewährten Methoden sind für eine robuste Ordnerumleitung aufgeführt:

- Hosten Sie die Windows-Dateiserver in derselben AWS Region und AZ, in der Amazon gestartet WorkSpaces wird.
- Stellen Sie sicher, dass die Regeln für eingehenden Datenverkehr der AD-Sicherheitsgruppe die Windows File Server-Sicherheitsgruppe oder private IP-Adressen enthalten. Andernfalls stellen Sie sicher, dass die On-Premises-Firewall denselben TCP- und UDP-Port-basierten Datenverkehr zulässt.
- Stellen Sie sicher, dass Regeln für eingehenden Datenverkehr von Windows File Server-Sicherheitsgruppen TCP 445 (SMB) für alle Amazon- WorkSpaces Sicherheitsgruppen enthalten.
- Erstellen Sie eine AD-Sicherheitsgruppe für Amazon- WorkSpaces Benutzer, um den Zugriff von Benutzern auf die Windows-Dateifreigabe zu autorisieren.
- Verwenden Sie DFS Namespace (DFS-N) und DFS Replication (DFS-R), um sicherzustellen, dass Ihre Windows-Dateifreigabe agil ist und nicht an einen bestimmten Windows-Dateiserver gebunden ist. Alle Benutzerdaten werden automatisch zwischen Windows-Dateiservern repliziert.
- Fügen Sie „$“ an das Ende des Freigabenamens an, um die Benutzerdaten des Freigabe-Hostings beim Durchsuchen der Netzwerkfreigaben im Windows Explorer vor der Ansicht zu verbergen.
- Erstellen Sie die Dateifreigabe gemäß den Anweisungen von Microsoft für umgeleitete Ordner: Bereitstellen der Ordnerumleitung mit Offline-Dateien. Folgen Sie genau den Anweisungen für Sicherheitsberechtigungen und GPO-Konfigurationen.
- Wenn Ihre Amazon- WorkSpaces Bereitstellung Bring Your Own License (BYOL) ist, müssen Sie auch die Deaktivierung von Offline-Dateien gemäß den Anweisungen von Microsoft angeben: Deaktivieren von Offline-Dateien für einzelne umgeleitete Ordner.
- Installieren und führen Sie Data Deduplication (allgemein als „Dedupe“ bezeichnet) aus, wenn Ihr Windows File Server Windows Server 2016 oder höher ist, um den Speicherverbrauch zu reduzieren und die Kosten zu optimieren. Weitere Informationen finden Sie unter Installieren und Aktivieren der Datendeduplizierung und Ausführen der Datendeduplizierung.
- Sichern Sie Ihre Windows File Server-Dateifreigaben mithilfe vorhandener organisatorischer Backup-Lösungen.

Objekt, das Sie vermeiden sollten

- Verwenden Sie keine Windows File Server, auf die nur über eine Wide Area Network (WAN)-Verbindung zugegriffen werden kann, da das SMB-Protokoll nicht für diese Verwendung konzipiert ist.
- Verwenden Sie nicht dieselbe Windows-Dateifreigabe, die für Home Directories verwendet wird, um das Risiko zu verringern, dass Benutzer versehentlich ihre User-Shell-Ordner löschen.
- Die Aktivierung von Volume Shadow Copy Service (VSS) wird zwar empfohlen, um die Dateiwiederherstellung zu vereinfachen, allein jedoch nicht die Notwendigkeit, die Windows File Server-Dateifreigaben zu sichern.

Weitere Überlegungen

- Amazon FSx for Windows File Server bietet einen verwalteten Service für Windows-Dateifreigaben und vereinfacht den Betriebsaufwand der Ordnerumleitung, einschließlich automatischer Sicherungen.
- Verwenden Sie AWS Storage Gateway für SMB File Share, um Ihre Dateifreigaben zu sichern, wenn es keine Lösung für das Organisations-Backup gibt.

Profileinstellungen

Gruppenrichtlinien

Eine gängige bewährte Methode in Microsoft-Windows-Bereitstellungen für Unternehmen besteht darin, Benutzerumgebungseinstellungen über Gruppenrichtlinienobjekt (GPO)- und Gruppenrichtlinieneinstellungen (GPP) zu definieren. Einstellungen wie Tastenkombinationen, Laufwerkszuordnungen, Registrierungsschlüssel und Drucker werden über die Gruppenrichtlinien-Managementkonsole definiert. Zu den Vorteilen der Definition der Benutzerumgebung über GPOs gehören unter anderem:

- Zentralisiertes Konfigurationsmanagement
- Benutzerprofil definiert durch AD-Sicherheitsgruppenmitgliedschaft oder OU-Platzierung
- Schutz vor dem Löschen von Einstellungen
- Automatisieren der Profilerstellung und Personalisierung bei der ersten Anmeldung

- Einfache zukünftige Aktualisierung

> **Note**
>
> Folgen Sie den bewährten Methoden von Microsoft zur Optimierung der Gruppenrichtlinienleistung.

Gruppenrichtlinien für interaktive Anmeldungsbanner dürfen nicht verwendet werden, da sie auf Amazon nicht unterstützt werden WorkSpaces. Banner werden auf dem Amazon WorkSpaces Client über AWS Supportanfragen angezeigt. Außerdem dürfen Wechselgeräte nicht über Gruppenrichtlinien blockiert werden, da sie für Amazon erforderlich sind WorkSpaces.

GPOs können zur Verwaltung von Windows verwendet werden WorkSpaces. Weitere Informationen finden Sie unter Verwalten Ihrer Windows- WorkSpaces.

Amazon- WorkSpaces Volumes

Jede Amazon WorkSpaces -Instance enthält zwei Volumes: ein Betriebssystem-Volume und ein Benutzer-Volume.

- Amazon Windows WorkSpaces – Das Laufwerk C:\ wird für das Betriebssystem (OS) verwendet und das Laufwerk D:\ ist ein Benutzer-Volume. Das Benutzerprofil befindet sich auf dem Benutzervolume (AppData, Dokumente, Bilder, Downloads usw.).
- Amazon Linux WorkSpaces – Bei einem Amazon Linux- wird WorkSpacedas System-Volume (/dev/xvda1) als Stammordner gemountet. Das Benutzer-Volume gilt für Benutzerdaten und Anwendungen; /dev/xvdf1 wird als /home bereitgestellt.

Für Betriebssystem-Volumes können Sie eine Startgröße für dieses Laufwerk von 80 GB oder 175 GB auswählen. Für Benutzer-Volumes können Sie eine Startgröße von 10 GB, 50 GB oder 100 GB auswählen. Beide Volumes können bei Bedarf auf bis zu 2TB erhöht werden. Um das Benutzervolumen jedoch über 100 GB hinaus zu erhöhen, muss das Betriebssystem-Volume 175 GB betragen. Volume-Änderungen können nur einmal alle sechs Stunden pro Volume durchgeführt werden. Weitere Informationen zum Ändern der WorkSpaces Volume-Größe finden Sie im Abschnitt Ändern eines WorkSpace im -Administratorhandbuch.

WorkSpaces Bewährte Methoden für -Volumes

Bei der Planung einer Amazon- WorkSpaces Bereitstellung wird empfohlen, die Mindestanforderungen für die Betriebssysteminstallation, direkte Upgrades und zusätzliche Kernanwendungen zu berücksichtigen, die dem Image auf dem Betriebssystem-Volume hinzugefügt werden. Für das Benutzer-Volume wird empfohlen, mit einer kleineren Festplattenzuweisung zu beginnen und die Größe des Benutzer-Volumes nach Bedarf schrittweise zu erhöhen. Durch die Minimierung der Größe der Datenträger-Volumes werden die Kosten für die Ausführung der gesenkt WorkSpace.

> **Note**
>
> Während eine Volume-Größe erhöht werden kann, kann sie nicht verringert werden.

Amazon- WorkSpaces Protokollierung

In einer Amazon- WorkSpaces Umgebung gibt es viele Protokollquellen, die zur Behebung von Problemen und zur Überwachung der WorkSpaces Gesamtleistung erfasst werden können.

Amazon WorkSpaces Client 3.x Auf jedem Amazon- WorkSpaces Client befinden sich die Client-Protokolle in den folgenden Verzeichnissen:

- Windows – %LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
- macOS – ~/Library/"Anwendungsunterstützung"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
- Linux (Ubuntu 18.04 oder höher) – /opt/workspacesclient/workspacesclient

Es gibt viele Instances, in denen Diagnose- oder Debugging-Details für eine WorkSpaces Sitzung clientseitig erforderlich sein können. Erweiterte Client-Protokolle können auch aktiviert werden, indem der ausführbaren Workspaces-Datei ein „-l3“ hinzugefügt wird. Beispielsweise:

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

Amazon WorkSpaces -Service

Der Amazon WorkSpaces -Service ist in Amazon CloudWatch Metrics, CloudWatch Events und integriert CloudTrail. Diese Integration ermöglicht die Anmeldung der Leistungsdaten und API-Aufrufe beim zentralen AWS Service.

Bei der Verwaltung einer Amazon- WorkSpaces Umgebung ist es wichtig, bestimmte CloudWatch Metriken ständig zu überwachen, um den Gesamtzustand der Umgebung zu bestimmen. Metriken

Während für Amazon andere CloudWatch Metriken verfügbar sind WorkSpaces (siehe Überwachen Ihrer WorkSpaces mithilfe von CloudWatch Metriken), helfen die drei folgenden Metriken bei der Aufrechterhaltung der WorkSpace Instance-Verfügbarkeit:

- Unhealthy – Die Anzahl der WorkSpaces , die einen fehlerhaften Status zurückgegeben haben.
- SessionLaunchTime – Die Zeit, die zum Initiieren einer WorkSpaces Sitzung benötigt wird.
- InSessionLatency – Die Round-Trip-Zeit zwischen dem WorkSpaces Client und der WorkSpace.

Weitere Informationen zu WorkSpaces Protokollierungsoptionen finden Sie unter Protokollieren von Amazon WorkSpaces -API-Aufrufen mit CloudTrail. Die zusätzlichen CloudWatch Ereignisse helfen bei der Erfassung der clientseitigen IP der Benutzersitzung, wann der Benutzer eine Verbindung mit der WorkSpaces Sitzung hergestellt hat und welcher Endpunkt während der Verbindung verwendet wurde. All diese Details helfen bei der Isolierung oder Lokalisierung von vom Benutzer gemeldeten Problemen während der Fehlerbehebungssitzungen.

> **Note**
>
> Einige CloudWatch Metriken sind nur mit AWS Managed AD verfügbar.

Container und Windows-Subsystem für Linux auf Amazon WorkSpaces

Container und Amazon WorkSpaces

Endbenutzer-Computing wird häufig von Kunden erreicht, die Container-Workloads mit Amazon bedienen möchten WorkSpaces. Dies ist nach Möglichkeit nicht die bevorzugte oder empfohlene Lösung. Kunden, die die potenziellen Kosten und betrieblichen Einsparungen von Containern nutzen möchten, wird dringend empfohlen, Amazon Elastic Container Service (Amazon ECS) und/oder Amazon Elastic Kubernetes Service (Amazon EKS) zu bewerten.

In Fällen, in denen Kundenanforderungen die Aktivierung von Containern mit Amazon vorschreiben WorkSpaces, wurde eine technische Anleitung veröffentlicht, die die Verwendung von Docker ermöglicht. Kunden sollten darüber informiert werden, dass dies andere nachfolgende Services erfordert und dass im Vergleich zu entkoppelten, nativen Containerservices höhere Kosten und Komplexität anfallen.

Windows-Subsystem für Linux

Mit der Einführung von Windows Server 2019 als zugrunde liegendem Betriebssystem für Amazon sind Kunden sehr darauf bemüht WorkSpaces, das Windows-Subsystem für Linux (WSL), insbesondere WSL2, zu implementieren. Da WSL2 eine virtuelle Maschine (Hyper-V) aufruft, um ihre Funktionen auszuführen, kann es nicht auf Amazon ausgeführt werden WorkSpaces, die von AWS Hypervisoren verwaltet werden. Kunden sollten wissen, dass aus diesem Grund nur WSL1 verfügbar sein wird, und die Unterschiede zwischen WSL1 und WSL2 verstehen.

Amazon- WorkSpaces Migration

Mit der Amazon- WorkSpaces Migrationsfunktion können Sie Ihre Benutzer-Volume-Daten in ein neues Paket integrieren. Sie können diese Funktion verwenden, um:

- Migrieren Sie Ihr WorkSpaces von der Windows 7-Umgebung zur Windows 10-Desktop-Umgebung.
- Migrieren Sie von einer PCoIP WorkSpace zu einem WorkSpaces Streaming-Protokoll (WSP WorkSpace).
- Migrieren Sie WorkSpaces von einem öffentlichen oder benutzerdefinierten Paket zu einem anderen. Sie können beispielsweise von GPU-fähigen Paketen (Graphics und GraphicsPro) zu nicht GPU-fähigen Paketen und umgekehrt migrieren.

Migrationsprozess

Mit der WorkSpaces Migration können Sie das Ziel WorkSpaces -Bundle angeben. Der Migrationsprozess erstellt das WorkSpace mithilfe eines neuen Root-Volumes aus dem Ziel-Bundle-Image neu und das Benutzer-Volume aus dem neuesten ursprünglichen Snapshot des Benutzer-Volumes. Bei der Migration wird aus Gründen der Kompatibilität ein neues Benutzerprofil generiert. Die Daten in Ihrem alten Benutzerprofil, die nicht in das neue Profil verschoben werden können, werden in einem .notMigrated-Ordner gespeichert.

Während der Migration bleiben die Daten auf dem Benutzer-Volume (Laufwerk D) erhalten, aber alle Daten auf dem Stamm-Volume (C:\Laufwerk) gehen verloren. Dies bedeutet, dass keine der installierten Anwendungen, Einstellungen und Änderungen an der Registrierung beibehalten werden. Der alte Benutzerprofilordner wird mit dem NotMigrated Suffix umbenannt und ein neues Benutzerprofil wird erstellt.

Der Migrationsprozess dauert bis zu einer Stunde pro WorkSpace. Wenn der Migrationsworkflow den Prozess nicht abschließen kann, setzt der Service den vor der Migration automatisch WorkSpace auf seinen ursprünglichen Zustand zurück, wodurch das Risiko eines Datenverlusts minimiert wird.

Alle dem Original zugewiesenen Tags WorkSpace werden während der Migration übertragen. Der Ausführungsmodus des WorkSpace bleibt erhalten. Das migrierte WorkSpace hat eine neue WorkSpace ID, einen neuen Computernamen und eine neue IP-Adresse. Migrationsverfahren

Sie können WorkSpaces mithilfe des Befehls migrate-workspace oder der Amazon- WorkSpaces API über die Amazon- WorkSpaces Konsole, AWS CLI die migrieren. Alle Migrationsanforderungen

werden in die Warteschlange gestellt, und der Service drosselt automatisch die Gesamtzahl der Migrationsanforderungen, wenn zu viele vorhanden sind. Migrationslimits

- Sie können nicht zu einem öffentlichen oder benutzerdefinierten Windows 7-Desktopumgebungsbundle migrieren.
- Sie können nicht zu BYOL-Windows-7-Paketen migrieren.
- Sie können BYOL WorkSpaces nur zu anderen BYOL-Paketen migrieren.
- Sie können ein , das aus öffentlichen oder benutzerdefinierten Paketen WorkSpace erstellt wurde, nicht zu einem BYOL-Paket migrieren.
- Die Migration von Linux WorkSpaces wird derzeit nicht unterstützt.
- In AWS Regionen, die mehr als eine Sprache unterstützen, können Sie WorkSpaces zwischen Sprachpaketen migrieren.
- Die Quell- und Zielbundles müssen unterschiedlich sein. (In Regionen, die mehr als eine Sprache unterstützen, können Sie jedoch auf dasselbe Windows-10-Paket migrieren, solange sich die Sprachen unterscheiden.) Wenn Sie Ihre WorkSpace mit demselben Paket aktualisieren möchten, erstellen Sie stattdessen die neu WorkSpace.
- Sie können nicht WorkSpaces zwischen Regionen migrieren.
- WorkSpaces kann nicht migriert werden, wenn sie sich im ADMIN_MAINTENANCE-Modus befinden.

Kosten

Während des Monats, in dem die Migration stattfindet, werden Ihnen anteilige Beträge sowohl für das neue als auch für das ursprüngliche berechnet WorkSpaces. Wenn Sie beispielsweise am 10. Mai WorkSpace A zu WorkSpace B migrieren, wird Ihnen vom 1. Mai bis zum 10. Mai WorkSpace A in Rechnung gestellt, und Ihnen wird vom 11. Mai bis zum 30. Mai WorkSpace B in Rechnung gestellt.

WorkSpaces Bewährte Methoden für die Migration

Bevor Sie eine migrieren WorkSpace, gehen Sie wie folgt vor:

- Sichern Sie alle wichtigen Daten auf Laufwerk C an einem anderen Speicherort. Alle Daten auf Laufwerk C werden während der Migration gelöscht.
- Stellen Sie sicher, dass die WorkSpace migrierte mindestens 12 Stunden alt ist, um sicherzustellen, dass ein Snapshot des Benutzer-Volumes erstellt wurde. Auf der Seite Migrieren WorkSpaces in der Amazon- WorkSpaces Konsole können Sie auf den Zeitpunkt des letzten

Snapshots verweisen. Alle Daten, die nach dem letzten Snapshot erstellt wurden, gehen während der Migration verloren.

- Um potenziellen Datenverlust zu vermeiden, stellen Sie sicher, dass sich Ihre Benutzer von ihrem abmelden und sich erst wieder anmelden WorkSpaces, nachdem der Migrationsprozess abgeschlossen ist.
- Stellen Sie sicher, dass die , die WorkSpaces Sie migrieren möchten, den Status VERFÜGBAR, GEstoppT oder FEHLER haben.
- Stellen Sie sicher, dass Sie über genügend IP-Adressen für die WorkSpaces verfügen, die Sie migrieren. Während der Migration werden dem neue IP-Adressen zugewiesen WorkSpaces.
- Wenn Sie Skripts verwenden, um zu migrieren WorkSpaces, migrieren Sie sie in Batches von nicht mehr als 25 WorkSpaces gleichzeitig.

Well-Architected Framework

AWS Well-Architected hilft Cloud-Architekten beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Infrastruktur für ihre Anwendungen und Workloads. Es beschreibt die wichtigsten Konzepte, Entwurfsprinzipien und bewährten Architekturmethoden für das Entwerfen und Ausführen von Workloads in der Cloud. Es basiert auf fünf wichtigen Säulen:

- Operational Excellence
- Sicherheit
- Zuverlässigkeit
- Leistungseffizienz
- Kostenoptimierung

Beim Entwerfen einer Amazon- WorkSpaces Umgebung ist es wichtig, diese wichtigsten Säulen zu bewerten, um die Reifebereitstellungsstufe zu bestimmen und zusätzliche Funktionen zu entdecken, die mit dem Amazon verwendet werden können WorkSpaces. Es gibt zwar allgemeine Leitlinien für das AWS Well-Architect Framework , aber im Folgenden finden Sie einige wichtige Fragen, die in die Planungsphase Ihrer WorkSpaces Bereitstellung aufgenommen werden können, um sicherzustellen, dass jede der fünf Säulen berücksichtigt wird.

Allgemeines

- Was ist der Geschäftstreiber für dieses Projekt?

Operational Excellence

- Wie trennen Sie die Zugriffskontrolle zwischen Benutzern und verschiedenen Administratorgruppen?

Sicherheit

1. Was sind die Sicherheits- und Compliance-Anforderungen, die für den Betrieb von berücksichtigt werden WorkSpaces müssen?
2. Gibt es Einschränkungen beim Routing zu externen IP-Adressen?

3. Sind die erforderlichen WorkSpaces Ports durch die Unternehmens-Firewall zulässig?
4. Wird oder wird die Multi-Faktor-Authentifizierung mit dieser Bereitstellung verwendet?
5. Wie viele Benutzeridentitäten und Autorisierungsanforderungen haben Sie heute?

Zuverlässigkeit

1. Was ist die Datenaufbewahrungsrichtlinie für Desktops?
2. Was ist das Recovery Point Objective (RPO) für Endbenutzerdaten?
3. Was ist das Recovery Time Objective (RTO) für Endbenutzerdaten?

Kostenoptimierung

1. Wurden die WorkSpaces Pakete für den Benutzerfall und die Anwendungen richtig dimensioniert?
2. Verarbeiten die Benutzer WorkSpaces mehr als 82 Stunden pro Monat?

Die obigen Fragen stellen zwar keine vollständige Liste der Elemente dar, die berücksichtigt werden sollten, sie bieten jedoch einige übergreifende Anleitungen, die Sie bei einer Well-Architected-WorkSpacesAmazon-Bereitstellung unterstützen.

Sicherheit

In diesem Abschnitt wird erläutert, wie Sie Daten mithilfe von Verschlüsselung sichern, wenn Sie Amazon- WorkSpaces Services verwenden. Es beschreibt die Verschlüsselung während der Übertragung und im Ruhezustand sowie die Verwendung von Sicherheitsgruppen zum Schutz des Netzwerkzugriffs auf die WorkSpaces. Dieser Abschnitt enthält auch Informationen dazu, wie Sie den Zugriff auf Endgeräte mithilfe WorkSpaces von vertrauenswürdigen Geräten und IP-Zugriffskontrollgruppen steuern können.

Weitere Informationen zur Authentifizierung (einschließlich MFA-Unterstützung) im AWS Directory Service finden Sie in diesem Abschnitt.

Verschlüsselung während der Übertragung

Amazon WorkSpaces verwendet Kryptografie, um die Vertraulichkeit in verschiedenen Kommunikationsphasen (bei der Übertragung) sowie Daten im Ruhezustand (verschlüsselt) zu schützen WorkSpaces. Die Prozesse in jeder Phase der Verschlüsselung, die von Amazon WorkSpaces während der Übertragung verwendet wird, werden in den folgenden Abschnitten beschrieben.

Informationen zur Verschlüsselung im Ruhezustand finden Sie im Abschnitt Verschlüsselt WorkSpaces dieses Dokuments.

Registrierung und Aktualisierungen

Die Desktop-Client-Anwendung kommuniziert mit Amazon für Updates und Registrierungen mithilfe von HTTPS.

Authentifizierungsphase

Der Desktop-Client initiiert die Authentifizierung, indem er Anmeldeinformationen an das Authentifizierungs-Gateway sendet. Die Kommunikation zwischen dem Desktop-Client und dem Authentifizierungs-Gateway verwendet HTTPS. Wenn die Authentifizierung am Ende dieser Phase erfolgreich ist, gibt das Authentifizierungs-Gateway über dieselbe HTTPS-Verbindung ein OAuth-2.0-Token an den Desktop-Client zurück.

> **Note**
>
> Die Desktop-Client-Anwendung unterstützt die Verwendung eines Proxyservers für Port-443-(HTTPS)-Datenverkehr, für Updates, Registrierung und Authentifizierung.

Nach Erhalt der Anmeldeinformationen vom Client sendet das Authentifizierungs-Gateway eine Authentifizierungsanforderung an AWS Directory Service. Die Kommunikation vom Authentifizierungs-Gateway zu AWS Directory Service erfolgt über HTTPS, sodass keine Benutzeranmeldeinformationen im Klartext übertragen werden.

Authentifizierung – Active Directory Connector (ADC)

AD Connector verwendet Kerberos, um eine authentifizierte Kommunikation mit On-Premises-AD herzustellen, sodass es an LDAP binden und nachfolgende LDAP-Abfragen ausführen kann. Clientseitige LDAPS-Unterstützung in Bol ist auch für die Verschlüsselung von Abfragen zwischen Microsoft AD und AWS Anwendungen verfügbar. Bevor Sie clientseitige LDAPS-Funktionalität implementieren, überprüfen Sie die Voraussetzungen für clientseitiges LDAPS .

Der AWS Directory Service unterstützt auch LDAP mit TLS. Es werden keine Benutzeranmeldeinformationen im Klartext übertragen. Für mehr Sicherheit ist es möglich, eine WorkSpaces VPC über eine VPN-Verbindung mit dem On-Premises-Netzwerk (in dem sich AD befindet) zu verbinden. Bei Verwendung einer AWS Hardware-VPN-Verbindung können Kunden die Verschlüsselung während der Übertragung einrichten, indem sie Standard-IPSEC (Internet Key Exchange (IKE) und IPSEC-SAs) mit symmetrischen AES-128- oder AES-256-Verschlüsselungsschlüsseln, SHA-1 oder SHA-256 für Integritäts-Hash und DH-Gruppen (2,14-18, 22, 23 und 24 für Phase 1; 1,2,5, 14-18, 22, 23 und 24 für Phase 2) unter Verwendung von Perfect Forward Secrecy (PFS) verwenden.

Broker-Phase

Nach dem Empfang des OAuth-2.0-Tokens (vom Authentifizierungs-Gateway, falls die Authentifizierung erfolgreich war) fragt der Desktop-Client Amazon- WorkSpaces Services (Broker Connection Manager) über HTTPS ab. Der Desktop-Client authentifiziert sich selbst, indem er das OAuth-2.0-Token sendet. Daher erhält der Client die Endpunktinformationen des WorkSpaces Streaming-Gateways.

Streaming-Phase

Der Desktop-Client fordert auf, eine PCoIP-Sitzung mit dem Streaming-Gateway zu öffnen (mit dem OAuth-2.0-Token). Diese Sitzung ist mit AES-256 verschlüsselt und verwendet den PCoIP-Port für die Kommunikationssteuerung (4172/TCP).

Mit dem OAuth2.0-Token fordert das Streaming-Gateway die benutzerspezifischen WorkSpaces Informationen vom Amazon WorkSpaces-Service über HTTPS an.

Das Streaming-Gateway empfängt auch das TGT vom Client (das mit dem Passwort des Client-Benutzers verschlüsselt ist). Durch die Verwendung von Kerberos-TTT-Pass-Through initiiert das Gateway eine Windows-Anmeldung auf dem WorkSpace, wobei das abgerufene Kerberos-TTT des Benutzers verwendet wird.

Das initiiert WorkSpace dann eine Authentifizierungsanforderung an den konfigurierten AWS Directory Service unter Verwendung der Kerberos-Standardauthentifizierung.

Nachdem erfolgreich angemeldet WorkSpace wurde, wird das PCoIP-Streaming gestartet. Die Verbindung wird vom Client auf Port TCP 4172 mit dem Rückverkehr auf Port UDP 4172 initiiert. Darüber hinaus erfolgt die erste Verbindung zwischen dem Streaming-Gateway und einem WorkSpaces Desktop über die Verwaltungsschnittstelle über UDP 55002. (Informationen zu IP-Adressen- und Portanforderungen für Amazon WorkSpaces finden Sie in der Dokumentation. Der anfängliche ausgehende UDP-Port ist 55002.) Die Streaming-Verbindung, die die Ports 4172 (TCP und UDP) verwendet, wird mit 128- und 256-Bit-Verschlüsselungen von AES verschlüsselt, aber standardmäßig auf 128-Bit. Kunden können dies aktiv in 256-Bit ändern, entweder mit PCoIP-spezifischen AD-Gruppenrichtlinieneinstellungen für Windows WorkSpacesoder mit der Datei pcoip-agent.conf für Amazon Linux WorkSpaces. Weitere Informationen zur Gruppenrichtlinienverwaltung für Amazon WorkSpacesfinden Sie in der Dokumentation .

Netzwerkschnittstellen

Jede Amazon WorkSpace verfügt über zwei Netzwerkschnittstellen, die als primäre Netzwerkschnittstelle und Verwaltungsnetzwerkschnittstelle bezeichnet werden.

Die primäre Netzwerkschnittstelle bietet Konnektivität zu Ressourcen innerhalb der Kunden-VPC, z. B. Zugriff auf AWS Directory Service, das Internet und das Unternehmensnetzwerk des Kunden. Es ist möglich, Sicherheitsgruppen an diese primäre Netzwerkschnittstelle anzufügen. Konzeptionell werden die Sicherheitsgruppen anhand des Umfangs der deployment: WorkSpaces security-Gruppe und der ENI-Sicherheitsgruppen unterschieden, die dieser ENI zugeordnet sind.

Verwaltungsnetzwerkschnittstelle

Die Verwaltungsnetzwerkschnittstelle kann nicht über Sicherheitsgruppen gesteuert werden. Kunden können jedoch eine hostbasierte Firewall auf verwenden, WorkSpaces um Ports zu blockieren oder den Zugriff zu steuern. Wir empfehlen nicht, Einschränkungen für die Verwaltungsnetzwerkschnittstelle anzuwenden. Wenn ein Kunde beschließt, hostbasierte Firewall-Regeln hinzuzufügen, um diese Schnittstelle zu verwalten, sollten einige Ports geöffnet sein, damit der Amazon- WorkSpaces Service den Zustand und die Zugänglichkeit für die verwalten kann WorkSpace. Weitere Informationen finden Sie unter Netzwerkschnittstellen im Amazon Workspaces Administration Guide.

WorkSpaces Sicherheitsgruppen

Eine Standardsicherheitsgruppe wird pro AWS Directory Service erstellt und automatisch an alle angefügt WorkSpaces , die zu diesem spezifischen Verzeichnis gehören.

Amazon nutzt WorkSpaceswie viele andere - AWS Services Sicherheitsgruppen. Amazon WorkSpaces erstellt zwei AWS Sicherheitsgruppen, wenn Sie ein Verzeichnis beim WorkSpaces Service registrieren. Eine für Verzeichniscontroller directoryId _controllers und eine für WorkSpaces in Verzeichnis directoryId _workspacesMembers . Löschen Sie keine dieser Sicherheitsgruppen, sonst WorkSpaces wird Ihr beeinträchtigt. Standardmäßig ist der Ausgang der Sicherheitsgruppe des WorkSpaces Mitglieds auf 0.0.0.0/0 geöffnet. Sie können einem Verzeichnis eine WorkSpaces Standardsicherheitsgruppe hinzufügen. Nachdem Sie eine neue Sicherheitsgruppe mit einem WorkSpaces Verzeichnis verknüpft haben, wird die neue Sicherheitsgruppe für neue WorkSpaces , die Sie starten, oder vorhandene , WorkSpaces die Sie neu erstellen, verwendet. Sie können diese neue Standardsicherheitsgruppe auch zu vorhandenen hinzufügen, WorkSpaces ohne sie neu zu erstellen. Wenn Sie einem WorkSpaces Verzeichnis mehrere Sicherheitsgruppen zuordnen, WorkSpaces aggregieren Sie die Regeln aus jeder Sicherheitsgruppe in einem einzigen Regelsatz. Wir empfehlen, Ihre Sicherheitsgruppenregeln so weit wie möglich zu verdichten. Weitere Informationen zu Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihre VPC im Amazon-VPC-Benutzerhandbuch.

Weitere Informationen zum Hinzufügen einer Sicherheitsgruppe zu einem WorkSpaces Verzeichnis oder vorhandenen WorkSpacefinden Sie im WorkSpaces Admin-Handbuch.

Einige Kunden möchten Ports und Ziele einschränken, die der WorkSpaces Datenverkehr verlassen kann. Um den ausgehenden Datenverkehr von der einzuschränken WorkSpaces, müssen Sie

sicherstellen, dass Sie bestimmte Ports belassen, die für die Servicekommunikation erforderlich sind. Andernfalls können sich Ihre Benutzer nicht bei ihrer anmelden WorkSpaces.

WorkSpaces verwendet die Elastic Network Interface (ENI) in der Kunden-VPC für die Kommunikation mit den Domain-Controllern während der WorkSpace Anmeldung. Damit sich Ihre Benutzer WorkSpaces erfolgreich bei ihrem anmelden können, müssen Sie den folgenden Ports den Zugriff auf Ihre Domain-Controller oder die CIDR-Bereiche erlauben, die Ihre Domain-Controller in der Sicherheitsgruppe _workspacesMembers enthalten.

- TCP/UDP 53 – DNS
- TCP/UDP 88 – Kerberos-Authentifizierung
- TCP/UDP 389 – LDAP
- TCP/UDP 445 – SMB
- TCP 3268-3269 – Globaler Katalog
- TCP/UDP 464 – Kerberos-Passwortänderung
- TCP 139 – Netlogon
- UDP 137-138 – Netlogon
- UDP 123 – NTP
- TCP/UDP 49152-65535 Flüchtige Ports für RPC

Wenn Sie auf andere Anwendungen, das Internet oder andere Standorte zugreifen WorkSpaces müssen, müssen Sie diese Ports und Ziele in CIDR-Notation innerhalb der Sicherheitsgruppe _workspacesMembers zulassen. Wenn Sie diese Ports und Ziele nicht hinzufügen, WorkSpaces erreicht nichts anderes als die oben aufgeführten Ports. Eine letzte Überlegung: Standardmäßig hat eine neue Sicherheitsgruppe keine Regeln für eingehenden Datenverkehr. Aus diesem Grund ist kein eingehenden Verkehr von einem anderen Host zu Ihrer Instance erlaubt, bis Sie der Sicherheitsgruppe Regeln für eingehenden Verkehr hinzufügen. Die obigen Schritte sind nur erforderlich, wenn Sie entweder den WorkSpaces ausgehenden Datenverkehr von einschränken möchten oder Eingangsregeln nur auf die Ressourcen oder CIDR-Bereiche beschränkt haben möchten, die Zugriff darauf haben sollen.

> **Note**
>
> Eine neu zugeordnete Sicherheitsgruppe wird nur angefügt, die nach der Änderung WorkSpaces erstellt oder neu erstellt wurde.

ENI-Sicherheitsgruppen

Da es sich bei der primären Netzwerkschnittstelle um eine reguläre ENI handelt, kann sie mithilfe der verschiedenen AWS Verwaltungstools verwaltet werden. Weitere Informationen finden Sie unter Elastic Network Interfaces. Navigieren Sie zur WorkSpace IP-Adresse (auf der WorkSpaces Seite in der Amazon- WorkSpaces Konsole) und verwenden Sie diese IP-Adresse dann als Filter, um die entsprechende ENI zu finden (im Abschnitt Netzwerkschnittstellen der Amazon EC2-Konsole).

Sobald sich die ENI befindet, kann sie direkt von Sicherheitsgruppen verwaltet werden. Berücksichtigen Sie bei der manuellen Zuweisung von Sicherheitsgruppen zur primären Netzwerkschnittstelle die Portanforderungen von Amazon WorkSpaces. Weitere Informationen finden Sie unter Netzwerkschnittstellen im Administrationshandbuch für Amazon Workspaces.

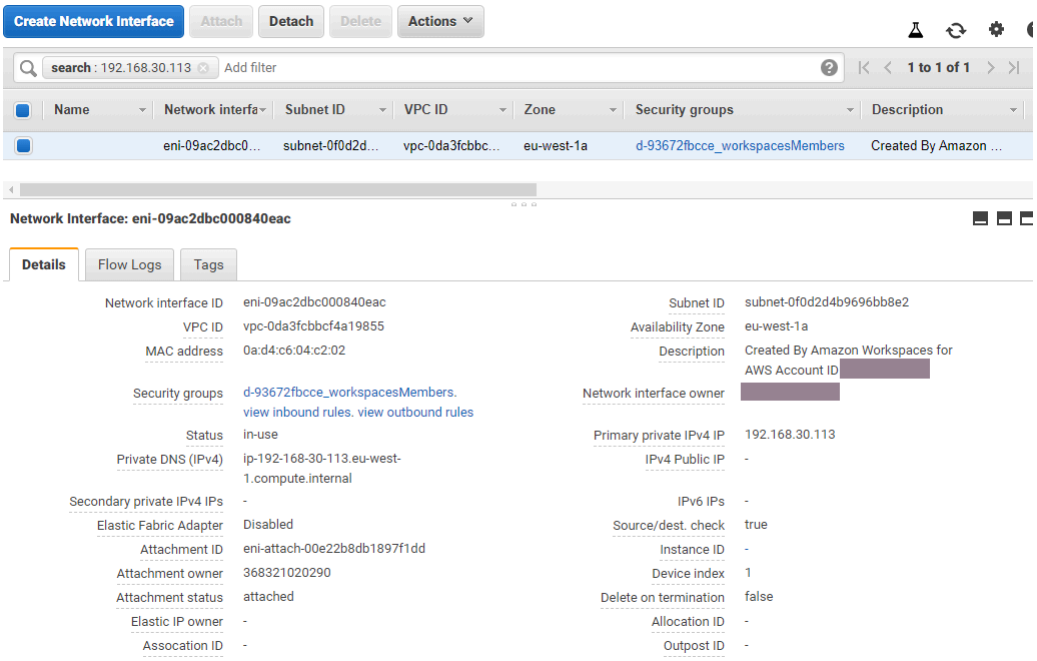


Abbildung 21: WorkSpaces Client mit aktivierter MFA

Netzwerk-Zugriffskontrolllisten (ACLs) (BP5)

Aufgrund der zusätzlichen Komplexität bei der Verwaltung noch einer anderen Firewall werden Netzwerk-ACLs häufig in sehr komplexen Bereitstellungen verwendet und im Allgemeinen nicht als bewährte Methode verwendet. Wenn Netzwerk-ACLs an die Subnetze in der VPC angefügt werden, konzentriert sich ihre Funktion auf Layer 3 (Netzwerk) des OSI-Modells. Da Amazon in Directory Services entwickelt WorkSpaces wurde, müssen zwei Subnetze definiert werden. Netzwerk-

ACLs werden getrennt von Directory Services verwaltet, und es ist sehr wahrscheinlich, dass eine Netzwerk-ACL nur einem der WorkSpaceszugewiesenen Subnetze zugewiesen wird.

Wenn eine zustandslose Firewall erforderlich ist, sind Netzwerk-ACLs eine bewährte Methode für die Sicherheit. Stellen Sie sicher, dass alle Änderungen an Netzwerk-ACLs, die über die Standardeinstellungen hinausgehen, als bewährte Methode pro Subnetz validiert werden. Wenn die Netzwerk-ACLs nicht wie vorgesehen funktionieren, sollten Sie VPC-Flow-Protokolle verwenden, um den Datenverkehr zu analysieren.

AWS Netzwerk-Firewall

AWS Network Firewall bietet Funktionen, die über das hinausgehen, was native Sicherheitsgruppen und Netzwerk-ACLs bieten, jedoch zu Kosten. Wenn Kunden nach der Möglichkeit gefragt ~~haben~~, die Sicherheit in Bezug auf Netzwerkverbindungen wie Server Name Inspection (SNI) für HTTPS-basierte Websites, Intrusion Detection und Prevent sowie eine Zulassungs- und Ablehnungsliste für Domainnamen zu erhöhen, mussten sie keine alternativen Firewalls auf der finden AWS Marketplace. Die Komplexität bei der Bereitstellung dieser Firewalls führte zu Herausforderungen, die über das hinausgehen, was Standard-EUC-Administratoren sind. AWS Die Netzwerk-Firewall bietet eine native AWS Erfahrung und aktiviert gleichzeitig Schutzmechanismen der Ebenen 3 bis 7. Die Verwendung von AWS Network Firewall in Verbindung mit NAT Gateway ist eine bewährte Methode, wenn Organisationen keine anderen Mittel (vorhandene On-Premises-Lizenzierung für Firewalls von Drittanbietern, die in die Cloud übertragen werden können, oder separate Teams, die Firewalls verwalten) haben, um alle EUC-Netzwerkschutzmaßnahmen abzudecken. NAT Gateway ist bei AWS Network Firewall ebenfalls kostenlos.

Bereitstellungen von AWS Network Firewall sind auf das bestehende EUC-Design ausgelegt. Einzelne VPC-Designs können eine vereinfachte Architektur mit Subnetzen für Firewall-Endpunkte und separaten Überlegungen zum Internet-Egress-Routing erreichen, während mehrere VPC-Designs von einer konsolidierten Inspektions-VPC mit Firewall- und Transit-Gateways-Endpunkten profitieren.

Designszenarien

Szenario 1: Grundlegende Instance-Sperre

Die WorkSpaces Standardsicherheitsgruppe lässt keinen eingehenden Datenverkehr zu, da Sicherheitsgruppen standardmäßig verweigert und zustandsbehaftet werden. Das bedeutet, dass keine zusätzlichen Konfigurationen konfiguriert werden müssen, um die WorkSpaces Instances selbst

weiter zu sichern. Berücksichtigen Sie die Regeln für ausgehenden Datenverkehr, die den gesamten Datenverkehr zulassen, und ob dies dem Anwendungsfall entspricht. Beispielsweise kann es am besten sein, den gesamten ausgehenden Datenverkehr zu Port 443 für jede Adresse zu verweigern, und bestimmte IP-Bereiche, die Port-Anwendungsfälle wie 389 für LDAP, 636 für LDAPS, 445 für SMB unter anderem erfüllen. Beachten Sie jedoch, dass die Komplexität der Umgebung mehrere Regeln erfordert und daher besser über Netzwerk-ACLs oder eine Firewall-Appliance bedient werden kann.

Szenario 2: Eingehende Ausnahmen

Es ist zwar keine konstante Anforderung, es kann jedoch vorkommen, dass der Netzwerkdatenverkehr in initiiert wird WorkSpaces. Zum Beispiel erfordert das Ausprobieren von Instances, wenn der WorkSpaces Client keine Verbindung herstellen kann, eine alternative Remote-Konnektivität. In diesen Fällen empfiehlt es sich, eingehendes TCP 3389 vorübergehend für die Sicherheitsgruppe der Kunden-ENI WorkSpacedes zu aktivieren.

Ein anderes Szenario sind Organisationsskripte, die Befehle für Bestands- oder Automatisierungsfunktionen ausführen, die von einer zentralen Instance initiiert werden. Die Sicherung des Datenverkehrs auf diesem Port von diesen spezifischen zentralisierten Instances auf dem Inbound kann dauerhaft konfiguriert werden. Es hat sich jedoch bewährt, dies für die zusätzliche Sicherheitsgruppe zu tun, die an die Verzeichniskonfiguration angehängt ist, da sie auf mehrere Bereitstellungen im AWS Konto angewendet werden kann.

Schließlich gibt es etwas Netzwerkverkehr, der nicht zustandsbehaftet ist und erfordert, dass in den Ausnahmen für eingehenden Datenverkehr kurzlebige Ports angegeben werden. Wenn Abfragen und Skripts fehlschlagen, empfiehlt es sich, flüchtige Ports zumindest vorübergehend zuzulassen und gleichzeitig die Ursache für den Verbindungsfehler zu ermitteln.

Szenario 3: Einzelne VPC-Inspektion

Vereinfachte Bereitstellungen von WorkSpaces (z. B. eine einzelne VPC ohne Skalierungspläne) erfordern keine separate VPC zur Überprüfung, sodass die Verbindung zu anderen VPCs mit VPC-Peering vereinfacht werden kann. Für Firewall-Endpunkte müssen jedoch separate Subnetze mit für diese Endpunkte konfiguriertem Routing sowie Internet Gateway (IGW)-Ausgangs-Routing erstellt werden, andernfalls müssten sie nicht konfiguriert werden. Vorhandene Bereitstellungen verfügen möglicherweise nicht über den verfügbaren IP-Speicherplatz, wenn alle Subnetze den gesamten VPC-CIDR-Block verwenden. In diesen Fällen kann Szenario 4 besser sein, da die Bereitstellung bereits über ihr ursprüngliches Design hinaus skaliert wurde.

Szenario 4: Zentralisierte Überprüfung

Wird in mehreren EUC-Bereitstellungen in einer - AWS Region bevorzugt, wodurch die Verwaltung der zustandsbehafteten und zustandslosen Regeln der AWS Network Firewall vereinfacht wird. Vorhandene VPC-Peers werden durch Transit Gateways ersetzt, da dieses Design die Verwendung von Transit Gateway-Anhängen sowie das Inspektions-Routing erfordert, das nur über diese Anhänge konfiguriert werden kann. Ein höherer Grad an Kontrolle wird auch über diese Konfiguration geübt und ermöglicht Sicherheit über die WorkSpaces Standardumgebung hinaus.

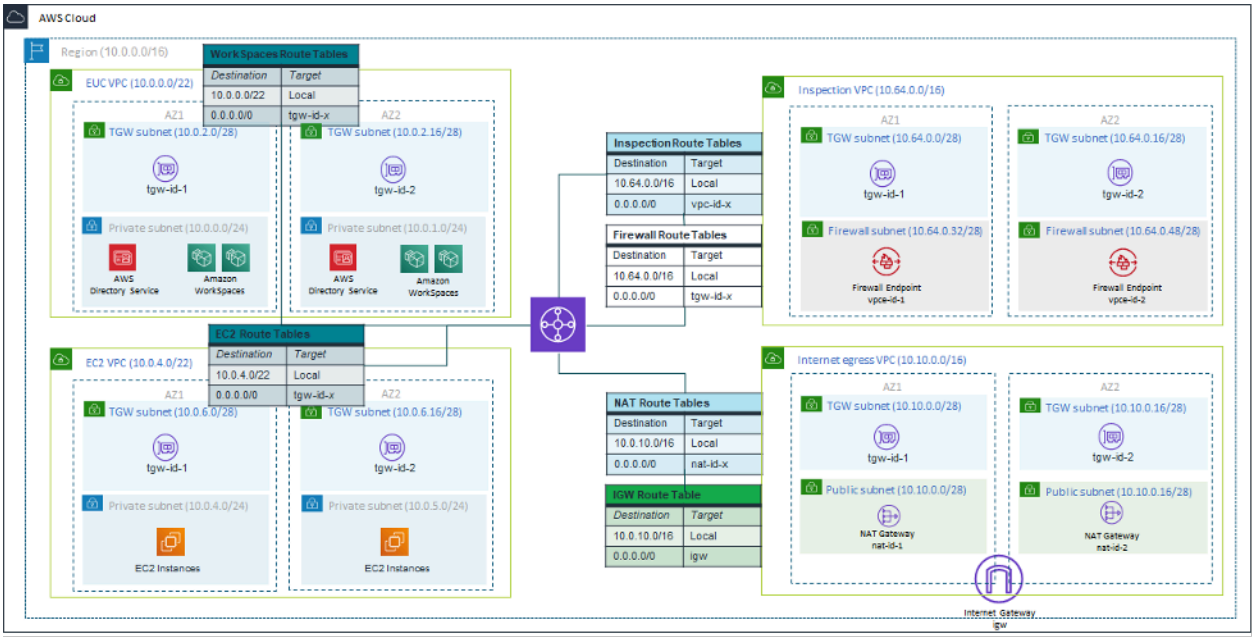


Abbildung 22: Beispielarchitektur mit Transit-Gateway-Anhängen

Verschlüsselt WorkSpaces

Jedem Amazon WorkSpace wird ein Root-Volume (C: Laufwerk für Windows WorkSpaces, Root für Amazon Linux WorkSpaces) und ein Benutzer-Volume (D: Laufwerk für Windows WorkSpaces, /home für Amazon Linux) bereitgestellt WorkSpaces. Die verschlüsselte WorkSpaces Funktion ermöglicht die Verschlüsselung eines oder beider Volumes.

Was ist verschlüsselt?

Die im Ruhezustand gespeicherten Daten, Festplatteneingabe/-ausgabe (I/O) auf dem Volume und Snapshots, die aus verschlüsselten Volumes erstellt wurden, werden alle verschlüsselt.

Wann erfolgt die Verschlüsselung?

Die Verschlüsselung für eine WorkSpace sollte beim Starten (Erstellen) der WorkSpace. WorkSpaces Volumes nur beim Start angegeben werden: Nach dem Start kann der Volume-Verschlüsselungsstatus nicht geändert werden. Die folgende Abbildung zeigt die Amazon-WorkSpaces Konsolenseite zur Auswahl der Verschlüsselung beim Start eines neuen WorkSpace.

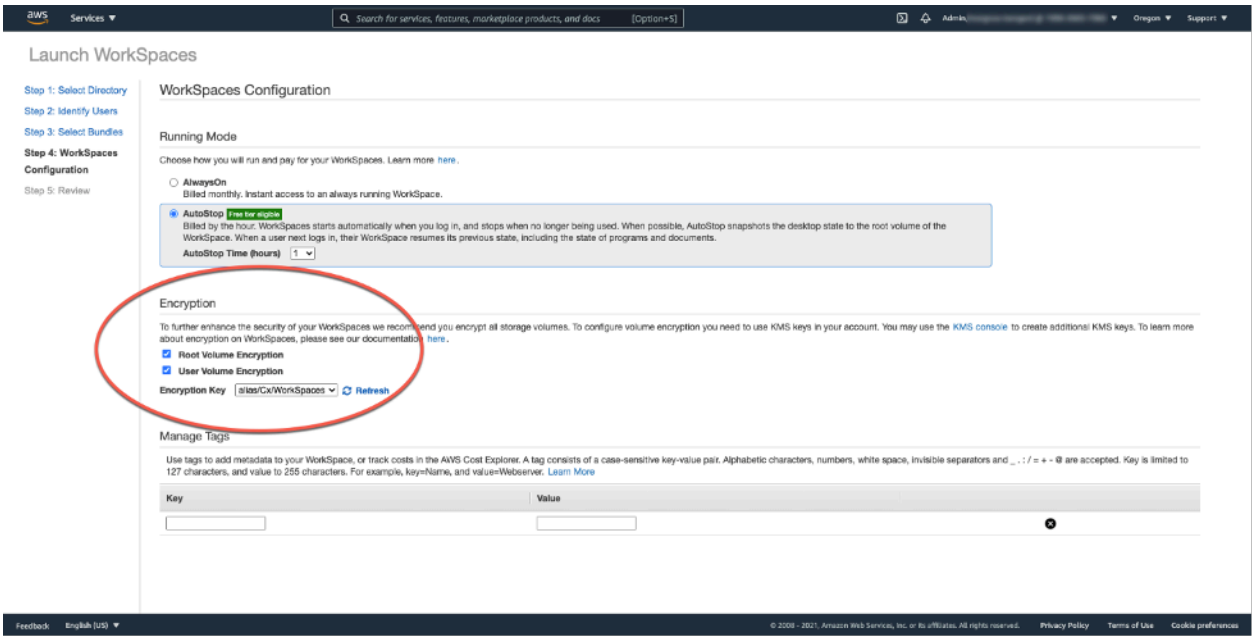


Abbildung 23: Verschlüsseln von WorkSpace Root-Volumes

Wie wird ein neuer WorkSpace verschlüsselt?

Ein Kunde kann die WorkSpaces Option Verschlüsselt entweder über die Amazon- WorkSpaces Konsole oder die oder mithilfe der Amazon WorkSpaces -API auswählen AWS CLI, wenn ein Kunde ein neues startet WorkSpace.

Zum Verschlüsseln der Volumes WorkSpaces verwendet Amazon einen CMK von AWS Key Management Service (AWS KMS). Ein Standard AWS KMS -CMK wird erstellt, wenn ein zum ersten Mal in einer Region gestartet WorkSpace wird. (CMKs haben einen Regionsbereich.)

Ein Kunde kann auch einen vom Kunden verwalteten CMK zur Verwendung mit verschlüsselten erstellen WorkSpaces. Der CMK wird verwendet, um die Datenschlüssel zu verschlüsseln, die vom Amazon- WorkSpaces Service zur Verschlüsselung jedes der WorkSpace Volumes verwendet werden. (In strikter Weise verschlüsselt Amazon EBS die Volumes). Aktuelle CMK-Limits finden Sie unter AWS KMS Ressourcenkontingente.

> **Note**
>
> Das Erstellen benutzerdefinierter Images aus einem verschlüsselten WorkSpace wird nicht unterstützt. Außerdem kann die WorkSpaces Bereitstellung mit aktivierter Root-Volume-Verschlüsselung bis zu einer Stunde dauern.

Eine detaillierte Beschreibung des WorkSpaces Verschlüsselungsprozesses finden Sie unter Wie Amazon WorkSpaces verwendet AWS KMS. Überlegen Sie, wie die Verwendung von CMK überwacht wird, um sicherzustellen, dass eine Anforderung für einen verschlüsselten korrekt bedient WorkSpace wird. Weitere Informationen zu AWS KMS Schlüsseln und Datenschlüsseln finden Sie auf der AWS KMS Seite .

Optionen für die Zugriffskontrolle und vertrauenswürdige Geräte

Amazon WorkSpaces bietet Kunden Optionen zum Verwalten, auf welche Client-Geräte zugreifen kann WorkSpaces. Kunden können den WorkSpaces Zugriff nur auf vertrauenswürdige Geräte beschränken. Der Zugriff auf WorkSpaces kann von macOS- und Microsoft Windows-PCs mithilfe digitaler Zertifikate erlaubt werden. Es kann auch den Zugriff für iOS-, Android-, Chrome OS-, Linux- und Null-Clients sowie den WorkSpaces Web Access-Client zulassen oder blockieren. Mit diesen Funktionen kann es die Sicherheitslage weiter verbessern.

Die Optionen für die Zugriffskontrolle sind für neue Bereitstellungen aktiviert, damit Benutzer WorkSpaces von Clients unter Windows, MacOS, iOS, Android, ChromeOS und Zero Clients auf ihre zugreifen können. Der Zugriff über Web Access oder einen Linux- WorkSpaces Client ist für eine neue WorkSpaces Bereitstellung standardmäßig nicht aktiviert und muss aktiviert werden.

Wenn es Beschränkungen für den Zugriff auf Unternehmensdaten von vertrauenswürdigen Geräten (auch als verwaltete Geräte bezeichnet) gibt, kann der WorkSpaces Zugriff auf vertrauenswürdige Geräte mit gültigen Zertifikaten beschränkt werden. Wenn diese Funktion aktiviert ist, WorkSpaces verwendet Amazon die zertifikatbasierte Authentifizierung, um festzustellen, ob ein Gerät vertrauenswürdig ist. Wenn die WorkSpaces Clientanwendung nicht überprüfen kann, ob ein Gerät vertrauenswürdig ist, blockiert sie Versuche, sich anzumelden oder erneut eine Verbindung vom Gerät herzustellen.

Unterstützung für vertrauenswürdige Geräte ist für die folgenden Clients verfügbar:

- Amazon WorkSpaces -Android-Client-App auf Google Play, die auf Android- und Android-kompatiblen Chrome-Betriebssystemgeräten ausgeführt wird

- Amazon- WorkSpaces macOS-Client-App auf macOS-Geräten
- Amazon WorkSpaces -Windows-Client-App auf Windows-Geräten

Weitere Informationen zum Steuern, welche Geräte auf zugreifen können WorkSpaces, finden Sie unter WorkSpaces Zugriff auf vertrauenswürdige Geräte beschränken.

> **Note**
>
> Zertifikate für vertrauenswürdige Geräte gelten nur für Amazon WorkSpaces -Windows-, macOS- und Android-Clients. Diese Funktion gilt nicht für den Amazon- WorkSpaces Web-Access-Client oder Clients von Drittanbietern, einschließlich, aber nicht beschränkt auf Teradici-PCoIP-Software und mobile Clients, Teradici-PCoIP-Zero-Clients, RDP-Clients und Remote-Desktop-Anwendungen.

IP-Zugriffskontrollgruppen

Mithilfe von IP-Adressen-basierten Kontrollgruppen können Kunden Gruppen vertrauenswürdiger IP-Adressen definieren und verwalten und Benutzern WorkSpaces nur dann Zugriff auf ihre gewähren, wenn sie mit einem vertrauenswürdigen Netzwerk verbunden sind. Diese Funktion hilft Kunden, mehr Kontrolle über ihren Sicherheitsstatus zu erhalten.

IP-Zugriffskontrollgruppen können auf WorkSpaces Verzeichnisebene hinzugefügt werden. Es gibt zwei Möglichkeiten, um mit der Verwendung von IP-Zugriffskontrollgruppen zu beginnen.

- Seite „IP-Zugriffskontrollen“ – Über die - WorkSpaces Managementkonsole können IP-Zugriffskontrollgruppen auf der Seite „IP-Zugriffskontrollen“ erstellt werden. Regeln können diesen Gruppen hinzugefügt werden, indem die IP-Adressen oder IP-Bereiche eingegeben werden, von denen aus auf sie zugegriffen werden WorkSpaces kann. Diese Gruppen können dann auf der Seite Update Details zu Verzeichnissen hinzugefügt werden.
- Workspace-APIs – WorkSpaces APIs können verwendet werden, um Gruppen zu erstellen, zu löschen und anzuzeigen, Zugriffsregeln zu erstellen oder zu löschen oder Gruppen aus Verzeichnissen hinzuzufügen und zu entfernen.

Eine detaillierte Beschreibung der Verwendung von IP-Zugriffskontrollgruppen mit dem Amazon-WorkSpaces Verschlüsselungsprozess finden Sie unter IP-Zugriffskontrollgruppen für Ihr WorkSpaces.

Überwachung oder Protokollierung mit Amazon CloudWatch

Die Überwachung von Netzwerken, Servern und Protokollen ist ein integraler Bestandteil jeder Infrastruktur. Kunden, die Amazon bereitstellen, WorkSpaces müssen ihre Bereitstellungen überwachen, insbesondere den Gesamtzustand und den Verbindungsstatus einzelner WorkSpaces.

Amazon- CloudWatch Metriken für WorkSpaces

CloudWatch -Metriken für WorkSpaces sollen Administratoren zusätzliche Einblicke in den Gesamtzustand und den Verbindungsstatus einzelner bieten WorkSpaces. Metriken sind pro verfügbar WorkSpaceoder für alle WorkSpaces in einer Organisation innerhalb eines bestimmten Verzeichnisses aggregiert.

Diese Metriken können wie alle CloudWatch Metriken in der AWS Management Console (in der folgenden Abbildung dargestellt), über die CloudWatch APIs aufgerufen und durch CloudWatch Alarme und Tools von Drittanbietern überwacht werden.

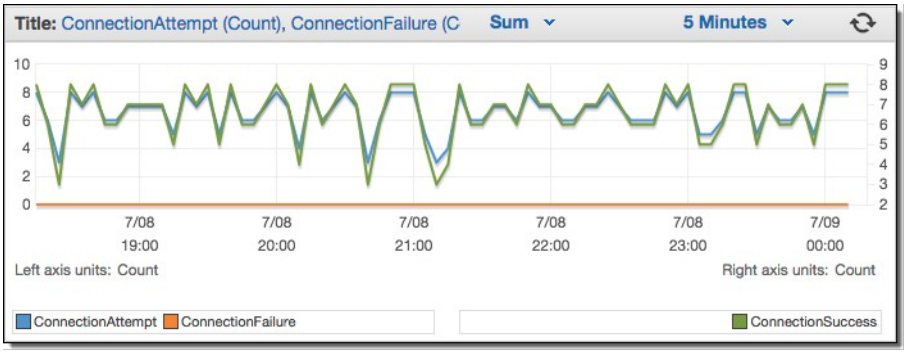


Abbildung 24: CloudWatch Metriken: ConnectionAttempt / ConnectionFailure

Standardmäßig sind die folgenden Metriken aktiviert und ohne zusätzliche Kosten verfügbar:

- Verfügbar – WorkSpaces , die auf eine Statusprüfung reagieren, werden in dieser Metrik gezählt.
- Fehlerhaft – WorkSpaces , die nicht auf dieselbe Statusprüfung reagieren, werden in dieser Metrik gezählt.
- ConnectionAttempt – Die Anzahl der Verbindungsversuche zu einem WorkSpace.
- ConnectionSuccess – Die Anzahl der erfolgreichen Verbindungsversuche.

- ConnectionFailure – Die Anzahl der erfolglosen Verbindungsversuche.
- SessionLaunchTime – Die Zeit, die benötigt wird, um eine Sitzung zu initiieren, gemessen vom WorkSpaces Client.
- InSessionLatency – Die Round-Trip-Zeit zwischen dem WorkSpaces Client und WorkSpaces, gemessen und gemeldet vom Client.
- SessionDisconnect – Die Anzahl der vom Benutzer initiierten und automatisch geschlossenen Sitzungen.

Darüber hinaus können Alarme erstellt werden, wie in der folgenden Abbildung gezeigt.

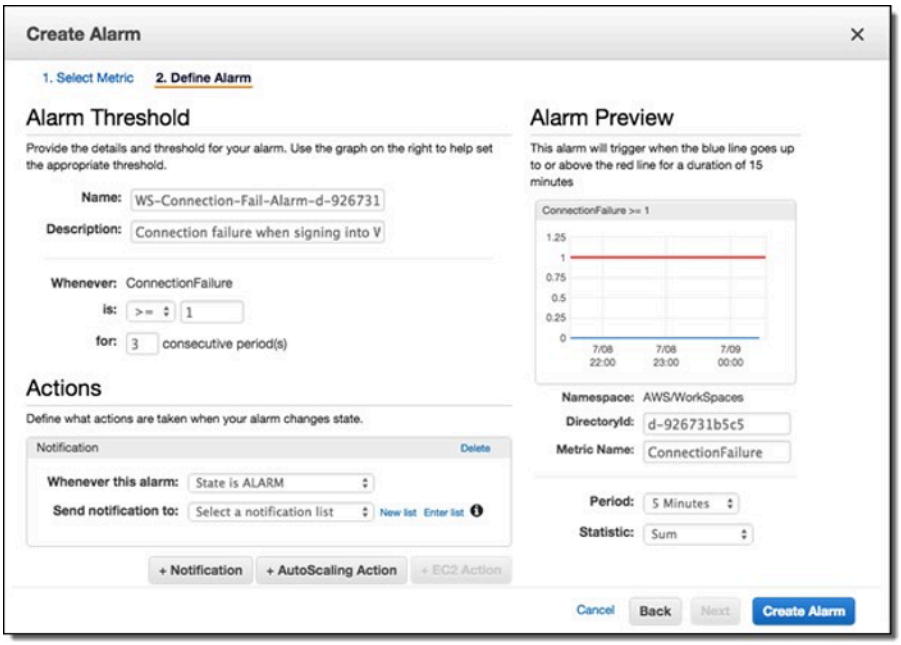


Abbildung 25: Erstellen eines CloudWatch Alarms für WorkSpaces Verbindungsfehler

Amazon CloudWatch Events für WorkSpaces

Ereignisse von Amazon CloudWatch Events können verwendet werden, um erfolgreiche Anmeldungen bei anzuzeigen, zu suchen, herunterzuladen, zu archivieren, zu analysieren und darauf zu reagieren WorkSpaces. Der Service kann Client-WAN-IP-Adressen, Betriebssystem-, WorkSpaces ID- und Verzeichnis-ID-Informationen für die Anmeldung von Benutzern bei überwachen WorkSpaces. Sie kann beispielsweise Ereignisse für die folgenden Zwecke verwenden:

- Speichern oder archivieren Sie WorkSpaces Anmeldeereignisse als Protokolle für zukünftige Referenzen, analysieren Sie die Protokolle, um nach Mustern zu suchen, und ergreifen Sie basierend auf diesen Mustern Maßnahmen.

- Verwenden Sie die WAN-IP-Adresse, um zu bestimmen, von wo aus Benutzer angemeldet sind, und verwenden Sie dann Richtlinien, um Benutzern nur Zugriff auf Dateien oder Daten von zu gewähren WorkSpaces , die die Zugriffskriterien des CloudWatch Ereignistyps WorkSpaces Zugriff erfüllen.
- Verwenden Sie Richtlinien-Steuerelemente, um den Zugriff auf Dateien und Anwendungen von nicht autorisierten IP-Adressen zu blockieren.

Weitere Informationen zur Verwendung von - CloudWatch Ereignissen finden Sie im Amazon CloudWatch Events-Benutzerhandbuch. Weitere Informationen zu CloudWatch Ereignissen für WorkSpacesfinden Sie unter Überwachen Ihrer WorkSpaces mit Cloudwatch Events.

YubiKey -Unterstützung für Amazon WorkSpaces

Um eine zusätzliche Sicherheitsebene hinzuzufügen, entscheiden sich Kunden häufig dafür, Tools und Websites mit Multifaktor-Authentifizierung zu sichern. Einige Kunden entscheiden sich dafür, dies mit einem Yubico- zu tun YubiKey. Amazon WorkSpaces unterstützt sowohl Einmalpasscodes (OTP) als auch FIDO-U2F-Authentifizierungsprotokoll mit YubiKeys.

Amazon unterstützt WorkSpaces derzeit den OTP-Modus und es sind keine zusätzlichen Schritte erforderlich, die ein Administrator oder Endbenutzer benötigt, um einen YubiKey mit OTP zu verwenden. Der Benutzer kann seine YubiKey an seinen Computer anfügen, sicherstellen, dass die Tastatur in der ausgerichtet ist WorkSpace (insbesondere in dem Feld, in dem das OTP eingegeben werden muss), und den Kontakt „Lift“ auf der anfassenYubiKey. Der YubiKey gibt das OTP automatisch in das ausgewählte Feld ein.

Um den FIDO-U2F-Modus mit YubiKey und zu verwenden WorkSpaces, sind zusätzliche Schritte erforderlich. Stellen Sie sicher, dass Ihren Benutzern eines dieser unterstützten YubiKey Modelle ausgestellt wird, um die U2F-Umleitung mit zu verwenden WorkSpaces:

- YubiKey 4
- YubiKey 5 NAT
- YubiKey 5 Nano
- YubiKey 5C
- YubiKey 5C Nano
- YubiKey 5 NAT

So aktivieren Sie die USB-Umleitung für YubiKey U2F

Standardmäßig ist die USB-Umleitung für PCoIP WorkSpaces deaktiviert. Um den U2F-Modus mit verwenden zu können YubiKeys, müssen Sie sie aktivieren.

1. Stellen Sie sicher, dass Sie die neueste WorkSpaces administrative Gruppenrichtlinienvorlage für PCoIP (32-Bit) oder die WorkSpaces administrative Gruppenrichtlinienvorlage für PCoIP (64-Bit) installiert haben.
2. Öffnen Sie bei einer Verzeichnisverwaltung WorkSpace oder einer Amazon EC2-Instance, die mit Ihrem WorkSpaces Verzeichnis verbunden ist, das Gruppenrichtlinienverwaltungstool (gpmc.msc) und navigieren Sie zu PCoIP-Sitzungsvariablen .
3. Um dem Benutzer zu erlauben, Ihre Einstellung zu überschreiben, wählen Sie Überschreibbare Administratorstandardwerte aus. Wählen Sie andernfalls Keine überschreibbaren Administratorstandards aus.
4. Öffnen Sie die Einstellung USB in der PCoIP-Sitzung aktivieren/deaktivieren.
5. Wählen Sie Aktiviert und anschließend OK aus.
6. Öffnen Sie die Einstellung PCoIP-USB-Geräte für zulässige und unzulässige Geräte konfigurieren.
7. Wählen Sie Aktiviert aus und konfigurieren Sie unter USB-Autorisierungstabelle eingeben (maximal zehn Regeln) die Regeln für die Zulassungsliste Ihres USB-Geräts.
   a. Autorisierungsregeln – 110500407. Dieser Wert ist eine Kombination aus einer Vendor-ID (VID) und einer Produkt-ID (PID). Das Format für eine VID/PID-Kombination ist `1xxxxyyyy`, wobei `xxxx` die VID im Hexadezimalformat und die PID im Hexadezimalformat `yyyy` ist. In diesem Beispiel ist 1050 die VID und 0407 die PID. Weitere YubiKey USB-Werte finden Sie unter YubiKey USB-ID-Werte.
8. Konfigurieren Sie unter USB-Autorisierungstabelle eingeben (maximal zehn Regeln) Ihre USB-Geräte-Blocklistenregeln.
   a. Geben Sie für Nicht-autorisiert-Regel eine leere Zeichenfolge ein. Das bedeutet, dass nur USB-Geräte in der Autorisierungsliste zulässig sind.

> **Note**
>
> Sie können maximal 10 USB-Autorisierungsregeln und maximal 10 USB-Nicht-autorisiert-Regeln definieren. Verwenden Sie den senkrechten Strich (|), um mehrere Regeln voneinander zu trennen. Ausführliche Informationen zu den Autorisierungs-/Nichtautorisierungsregeln finden Sie unter Teradici PCoIP Standard Agent für Windows.

9. Wählen Sie OK aus.
10. Die Änderung der Gruppenrichtlinieneinstellung wird nach der nächsten Aktualisierung der Gruppenrichtlinien für die WorkSpace und nach dem Neustart der WorkSpace Sitzung wirksam. Führen Sie einen der folgenden Schritte aus, um die Gruppenrichtlinienänderungen anzuwenden:
    a. Starten Sie die neu WorkSpace (wählen Sie in der Amazon- WorkSpaces Konsole die und WorkSpacedann Aktionen , Neustart aus WorkSpaces).
    b. Geben Sie in einer administrativen Eingabeaufforderung gpupdate /force ein.
11. Nachdem die Einstellung wirksam ist, können alle unterstützten USB-Geräte zu umgeleitet werden, WorkSpaces es sei denn, es sind Einschränkungen über die Einstellung für USB-Geräteregeln konfiguriert.

Sobald Sie die USB-Umleitung für YubiKey U2F aktiviert haben, können Sie Ihre YubiKey mit dem F Bol-U2F-Modus verwenden.

Kostenoptimierung

Self-Service- WorkSpace Verwaltungsfunktionen

In Amazon können Self-Service- WorkSpace Verwaltungsfunktionen für Benutzer aktiviert werden WorkSpaces, um ihnen mehr Kontrolle über ihre Erfahrung zu geben. Wenn Sie Benutzern Self-Service-Funktionen gewähren, kann die Workload Ihrer IT-Support-Mitarbeiter für Amazon reduziert werden WorkSpaces. Wenn Self-Service-Funktionen aktiviert sind, können Benutzer eine oder mehrere der folgenden Aufgaben direkt über ihren Windows-, macOS- oder Linux-Client für Amazon ausführen WorkSpaces:

- Speichern Sie die Anmeldeinformationen auf ihrem Client. Auf diese Weise können sich Benutzer wieder mit ihrem verbinden, WorkSpace ohne ihre Anmeldeinformationen erneut einzugeben.
- Starten Sie ihr neu WorkSpace.
- Erhöhen Sie die Größe der Root- und Benutzer-Volumes auf ihrem WorkSpace.
- Ändern Sie den Datenverarbeitungstyp (Paket) für ihre WorkSpace.
- Wechseln Sie den Ausführungsmodus ihrer WorkSpace.
- Erstellen Sie ihre neu WorkSpace.

Es gibt keine laufenden Auswirkungen auf die Kosten, wenn Benutzern die Optionen Neustart und Neuerstellung für ihr gewährt werden WorkSpaces. Benutzer sollten sich darüber im Klaren sein, dass eine Neuerstellung ihres dazu führen WorkSpace wird, dass ihr WorkSpace bis zu eine Stunde lang nicht verfügbar ist, wenn der Neuerstellungsprozess stattfindet.

Optionen zum Erhöhen der Volume-Größe, Ändern des Datenverarbeitungstyps und Wechseln des Ausführungsmodus können zusätzliche Kosten für verursachen WorkSpaces. Eine bewährte Methode besteht darin, Self-Service zu aktivieren, um den Workload für das Support-Team zu reduzieren. Self-Service für zusätzliche Kostenelemente sollte innerhalb eines Workflow-Prozesses zugelassen werden, der sicherstellt, dass die Autorisierung für zusätzliche Gebühren erhalten wurde. Dies kann über ein dediziertes Self-Service-Portal für WorkSpacesoder durch Integration in bestehende ITSM-Services (Information Technology Service Manage) erfolgen, z. B. ServiceNow.

Ausführlichere Informationen finden Sie unter Aktivieren von Self-Service- WorkSpace Verwaltungsfunktionen für Ihre Benutzer. Ein Beispiel für die Aktivierung eines strukturierten Portals

für Benutzer-Self-Service finden Sie unter Automatisieren von Amazon WorkSpaces mit einem Self-Service-Portal.

Amazon WorkSpaces Cost Optimizer

Die Amazon WorkSpaces -Cost-Optimizer-Lösung analysiert alle Ihre Amazon- WorkSpaces Nutzungsdaten. Abhängig von Ihrer Nutzung konvertiert es die automatisch WorkSpace in die kostengünstigste Fakturierungsoption (stündlich oder monatlich). Diese Lösung hilft Ihnen, Ihre - WorkSpace Nutzung zu überwachen und die Kosten zu optimieren, und verwendet , AWS CloudFormation um die erforderlichen AWS Services automatisch bereitzustellen und zu konfigurieren, um die Nutzung alle 24 Stunden zu analysieren und einzelne zu konvertieren WorkSpaces. Die neueste Version, 2.4, bietet Kunden die Flexibilität, die Lösung in einer vorhandenen VPC bereitzustellen und optional für Region und Beendigung zu konfigurieren. Außerdem wurde die Genauigkeit der Berechnungen der Fakturierungsstunde für Metadaten WorkSpaces und erweiterte Berichterstellungsmetadaten verbessert. Wenn Sie zuvor eine frühere Version (v2.2.1 oder niedriger) dieser Lösung bereitgestellt haben, folgen Sie der Update-Stack-Dokumentation, um den Amazon WorkSpaces -Cost-Optimizer- CloudFormation Stack zu aktualisieren, um die neueste Version des Frameworks der Lösung zu erhalten.

Der Ausführungsmodus eines WorkSpace bestimmt seine sofortige Verfügbarkeit und Abrechnung. Im Folgenden finden Sie den aktuell ausgeführten WorkSpaces Ausführungsmodus:

AlwaysOn – Wird verwendet, wenn eine feste monatliche Gebühr für die unbegrenzte Nutzung von bezahlt wird WorkSpaces. Dieser Modus eignet sich am besten für Benutzer, die ihr WorkSpace als primären Desktop verwenden und WorkSpace jederzeit sofortigen Zugriff auf ein benötigen, das ausgeführt wird.

AutoStop – Wird verwendet, wenn Sie nach WorkSpaces Stunde bezahlen. In diesem Modus WorkSpaces stoppen Sie nach einem bestimmten Inaktivitätszeitraum und der Status von Apps und Daten wird gespeichert. Um die automatische Stoppzeit festzulegen, verwenden Sie AutoStop Zeit (Stunden). Dieser Modus eignet sich am besten für Benutzer, die nur Teilzeitzugriff auf ihre benötigen WorkSpaces.

Eine bewährte Methode besteht darin, die Nutzung zu überwachen und den Ausführungsmodus von Amazon so einzustellen, dass WorkSpaceser mit einer Lösung wie dem Amazon WorkSpaces Cost Optimizer die kostengünstigste ist. Diese Lösung stellt eine Amazon CloudWatch-Ereignisregel bereit, die alle 24 Stunden eine -AWS LambdaFunktion aufruft.

Diese Lösung kann einzelne an jedem Tag, nachdem sie den Schwellenwert erreicht hat, WorkSpaces von einem stündlichen Fakturierungsmodell in ein monatliches Fakturierungsmodell umwandeln. Wenn die Lösung eine WorkSpace von der stündlichen Fakturierung in die monatliche Fakturierung umwandelt, konvertiert die Lösung die WorkSpace zurück in die stündliche Fakturierung erst zu Beginn des nächsten Monats und nur, wenn die Nutzung unter dem Schwellenwert lag. Das Abrechnungsmodell kann jedoch jederzeit manuell über die AWS Management Console oder die Amazon WorkSpaces -API geändert werden. Die AWS CloudFormation Vorlage der Lösung enthält Parameter, die diese Konvertierungen ausführen und die Ausführung der Lösung im Testlaufmodus ermöglichen, um Berichte über die Empfehlungen bereitzustellen.

Abmelden mit Tags

Um zu verhindern, dass die Lösung einen WorkSpace zwischen Fakturierungsmodellen konvertiert, wenden WorkSpace Sie ein Ressourcen-Tag mithilfe des Tag-Schlüssels Skip_Convert und eines beliebigen Tag-Werts auf den an. Diese Lösung protokolliert markierte WorkSpaces, konvertiert jedoch nicht die markierte WorkSpaces. Entfernen Sie das Tag jederzeit, um die automatische Konvertierung für diese fortzusetzen WorkSpace. Weitere Informationen finden Sie unter Amazon WorkSpaces Cost Optimizer.

Aktivieren von Regionen

Standardmäßig überwacht diese Lösung WorkSpaces in allen verfügbaren AWS Regionen, indem sie nach Verzeichnissen sucht, die bei Amazon WorkSpaces im selben AWS Konto registriert sind. Sie können in der Eingabeparameter Liste der AWS Regionen eine durch Komma getrennte Liste der AWS Regionen angeben, die Sie überwachen möchten, um die zu überwachenden Regionen einzuschränken.

Bereitstellung in einer vorhandenen VPC

Diese Lösung erfordert eine VPC, um die ECS-Aufgabe auszuführen. Standardmäßig erstellt die Lösung eine neue VPC, aber Sie können in einer vorhandenen VPC bereitstellen, indem Sie die Subnetz-IDs und die Sicherheitsgruppen-ID als Teil des Eingabeparameters angeben. Ihr aktuelles Subnetz verfügt über eine Route zum Internet, damit die ECS-Aufgabe das in einem öffentlichen Amazon ECR-Repository gehostete Docker-Image abrufen kann.

Beendigung des ungenutzten WorkSpaces

Mit dieser Lösung können Sie ungenutzt WorkSpaces am letzten Tag des Monats beenden, wenn alle Kriterien erfüllt sind. Sie können sich für dieses Feature anmelden, indem Sie den

TerminateUnusedWorkSpaces Eingabeparameter in die CloudFormation Vorlage ändern. Eine bewährte Methode besteht darin, diese Funktion für einige Monate im Modus „War Run“ auszuführen und die monatlichen Berichte zu überprüfen, um die für die Beendigung WorkSpaces markierten zu überprüfen.

Amazon Connect-Optimierung für Amazon WorkSpaces

Die Endbenutzererfahrung für Kontaktcenter-Kundendienstmitarbeiter muss oberste Priorität haben, denn wenn ihr Audio beeinträchtigt ist, führt dies zu einer schlechten Anruferfahrung für den Kunden, den sie bedienen. Wenn Sie eine Kontaktcenter-Lösung auf einem Remote-Desktop ausführen, wird die Audioleistung immer auf einen messbaren Umfang beeinträchtigt, wenn der Sprachverkehr nicht über die Netzwerkverbindung priorisiert wird. Diese Auswirkung ist auf das Audio zurückzuführen, das vom Audioendpunkt zur virtuellen Sitzung fließt und dann über das Streaming-Protokoll komprimiert wird, das an den Endbenutzer übermittelt werden soll. Dieses zusätzliche Routing führt dazu, dass das Audio durch Netzwerkengpässe eine Leistungseinbußen aufweist.

Ein Ansatz zur Vermeidung dieses Verhaltens besteht darin, das Audio aus der Sitzung herauszuteilen, d. h. alle Ressourcen des Kontaktcenter-Kundendienstmitarbeiters bleiben während der Sitzung, während der Audiostrom aus der Sitzung bleibt. Diese Aufteilung ermöglicht es dem Audio, vom Audioendpunkt direkt an den Endbenutzer zu streamen, während alle anderen Anrufressourcen, einschließlich der PII, die der Agent anzeigt, in einer sicheren Sitzung verbleiben. Diese Audiooptimierung gilt als bewährte Methode, da sie sicherstellt, dass das Anruferlebnis des Kunden so gut wie möglich ist.

Amazon Connect bietet eine Streams-API, mit der Administratoren ihr Contact Control Panel (CCP) an ihre Geschäftsanforderungen anpassen können. Eine der Optionen, die ein Administrator hat, besteht darin, zu steuern, ob das benutzerdefinierte CCP Audio für den Anruf empfangen kann. Mit diesen Einstellungen können wir ein geteiltes CCP konfigurieren; ein reines Audio-CCP für außerhalb der Sitzung und ein medienloses CCP für die Sitzung. Sobald Administratoren diese benutzerdefinierten CCPs konfiguriert haben, können sie die Audiooptimierung von Amazon Connect für WorkSpaces nutzen. Da CCPs im Browser bereitgestellt werden, können Administratoren mit dieser Einstellung ihre reine Audio-CCP-URL für das WorkSpaces Verzeichnis bereitstellen. Nach der Konfiguration öffnet WorkSpacesder WorkSpaces Client bei WorkSpaces erfolgreicher Authentifizierung bei seinen die bereitgestellte reine Audio-CCP-URL im lokalen Standardbrowser des Kundendienstmitarbeiters. Diese Aktion ermöglicht es dem Audio, direkt zum lokalen Computer des Kundendienstmitarbeiters zu fließen, während das medienlose CCP alles andere innerhalb der sicheren WorkSpaces Sitzung verarbeitet.

Architekturdiagramm

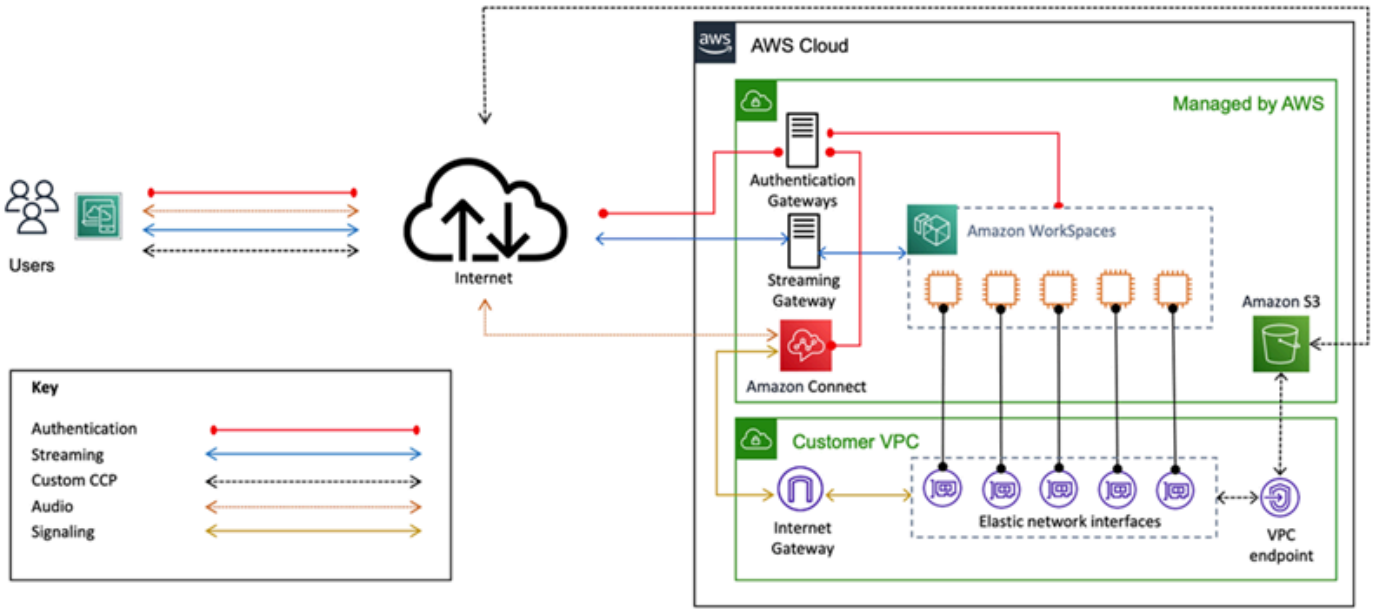


Abbildung 26 – Amazon Connect und WorkSpaces Architekturdiagramm

Fehlerbehebung

Häufige Verwaltungs- und Clientprobleme, wie Fehlermeldungen wie Ihr Gerät kann keine Verbindung zum WorkSpaces Registrierungsservice herstellen oder kann keine Verbindung zu einem WorkSpace mit einem interaktiven Anmeldebanner herstellen, finden Sie auf den Seiten Client- und Admin istratorfehlerbehebungim Amazon- WorkSpaces Administratorhandbuch. https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-troubleshooting.html#troubleshooting-specific-issues

Themen

- AD Connector kann keine Verbindung zu Active Directory herstellen
- Fehlerbehebung bei einem Fehler bei der Erstellung eines WorkSpace benutzerdefinierten Images
- Fehlerbehebung für ein als fehlerhaft WorkSpace markiertes Windows
- Sammeln eines WorkSpaces Support-Protokoll-Bundles zum Debuggen
- So überprüfen Sie die Latenz zur nächstgelegenen AWS Region

AD Connector kann keine Verbindung zu Active Directory herstellen

Damit AD Connector eine Verbindung zum On-Premises-Verzeichnis herstellen kann, muss die Firewall für das On-Premises-Netzwerk bestimmte Ports für die CIDRs für beide Subnetze in der VPC geöffnet haben. Siehe Szenario 1: Verwenden von AD Connector zur Proxy-Authentifizierung an den On-Premises-Active-Directory-Service. Führen Sie die folgenden Schritte aus, um zu testen, ob diese Bedingungen erfüllt sind.

So testen Sie die Verbindung:

1. Starten Sie eine Windows-Instance in der VPC und stellen Sie eine VPC-Verbindung über RDP her. Die weiteren Schritte werden in der VPC-Instance ausgeführt.
2. Laden Sie die DirectoryServicePortTest Testanwendung herunter und entpacken Sie sie. Der Quellcode und die Microsoft Visual Studio-Projektdateien sind enthalten, um die Testanwendung bei Bedarf zu ändern.
3. Führen Sie in einer Windows-Eingabeaufforderung die DirectoryServicePortTest Testanwendung mit den folgenden Optionen aus:

```
DirectoryServicePortTest.exe -d <domain_name>
```

```
-ip <server_IP_address> -tcp "53,88,135,139,389,445,464,636,49152" -udp
 "53,88,123,137,138,389,445,464" <domain_name>
```

<domain_name**>** – Der vollqualifizierte Domänenname, der zum Testen der Gesamtstruktur und der Domänenfunktionsebenen verwendet wird. Wenn der Domänenname ausgeschlossen ist, werden die Funktionsebenen nicht getestet.

<server_IP_address**>** – Die IP-Adresse eines Domain-Controllers in der On-Premises-Domain. Die Ports werden anhand dieser IP-Adresse getestet. Wenn die IP-Adresse ausgeschlossen ist, werden die Ports nicht getestet.

Dieser Test bestimmt, ob die erforderlichen Ports von der VPC zur Domain geöffnet sind. Die Testanwendung prüft zudem die mindestens erforderlichen Gesamtstruktur- und Funktionsebenen der Domäne.

Fehlerbehebung bei einem Fehler bei der Erstellung eines WorkSpace benutzerdefinierten Images

Wenn ein Windows- oder Amazon Linux- gestartet und angepasst WorkSpace wurde, kann ein benutzerdefiniertes Image aus diesem erstellt werden WorkSpace. Ein benutzerdefiniertes Image enthält das Betriebssystem, die Anwendungssoftware und die Einstellungen für die WorkSpace.

Überprüfen Sie die Anforderungen zum Erstellen eines benutzerdefinierten Windows-Images oder die Anforderungen zum Erstellen eines benutzerdefinierten Amazon Linux-Images. Die Image-Erstellung erfordert, dass alle Voraussetzungen erfüllt sind, bevor die Image-Erstellung gestartet werden kann.

Um zu bestätigen, dass Windows die Anforderungen für die Image-Erstellung WorkSpace erfüllt, empfehlen wir, den Image Checker auszuführen. Der Image Checker führt eine Reihe von Tests an der durch, WorkSpace wenn ein Image erstellt wird, und bietet Anleitungen zur Behebung gefundener Probleme. Ausführliche Informationen finden Sie unter Installieren und Konfigurieren des Image Checkers.

Nachdem die alle Tests WorkSpace bestanden hat, wird die Meldung „Validierung erfolgreich“ angezeigt. Sie können jetzt ein benutzerdefiniertes Paket erstellen. Beheben Sie andernfalls alle Probleme, die zu Testfehlern und Warnungen führen, und wiederholen Sie die Ausführung des Image Checkers, bis der alle Tests WorkSpace bestanden hat. Alle Fehler und Warnungen müssen behoben werden, bevor ein Image erstellt werden kann.

Weitere Informationen finden Sie in den Tipps zur Behebung von Problemen, die vom Image Checker erkannt wurden.

Fehlerbehebung für ein als fehlerhaft WorkSpace markiertes Windows

Der Amazon- WorkSpaces Service überprüft regelmäßig den Zustand eines , WorkSpace indem er ihm eine Statusanforderung sendet. Die WorkSpace wird als fehlerhaft markiert, wenn eine Antwort nicht WorkSpace rechtzeitig von der empfangen wird. Häufige Ursachen für diesen Fehler sind:

- Eine Anwendung auf dem WorkSpace blockiert die Netzwerkverbindung zwischen dem Amazon WorkSpaces-Service und dem WorkSpace.
- Hohe CPU-Auslastung auf dem WorkSpace.
- Der Computername des WorkSpace wird geändert.
- Der Agent oder Service, der auf den Amazon- WorkSpaces Service reagiert, befindet sich nicht im Ausführungsstatus.

Die folgenden Schritte zur Fehlerbehebung können die in einen WorkSpace fehlerfreien Zustand versetzen:

- Starten Sie zunächst die WorkSpaceüber die Amazon- WorkSpaces Konsole neu. Wenn der Neustart des das Problem WorkSpace nicht behebt, verwenden Sie entweder RDP oder stellen WorkSpace Sie über SSH eine Verbindung zu einem Amazon Linux her.
- Wenn die von einem anderen Protokoll nicht erreichbar WorkSpace ist, erstellen Sie die von der Amazon-Konsole WorkSpaceaus neu. WorkSpaces
- Wenn keine WorkSpaces Verbindung hergestellt werden kann, überprüfen Sie Folgendes:

Überprüfen der CPU-Auslastung

Verwenden Sie Open Task Manager, um festzustellen, ob der eine hohe CPU-Auslastung WorkSpace aufweist. Wenn dies der Fall ist, versuchen Sie einen der folgenden Schritte zur Fehlerbehebung, um das Problem zu beheben:

1. Halten Sie alle Services an, die eine hohe CPU-Menge verbrauchen.

2. Passen Sie die Größe der WorkSpace auf einen Datenverarbeitungstyp an, der größer ist als der derzeit verwendete.
3. Starten Sie die neu WorkSpace.

> **Note**
>
> Informationen zur Diagnose einer hohen CPU-Auslastung und Anleitungen, wenn die obigen Schritte das Problem mit der hohen CPU-Auslastung nicht beheben, finden Sie unter Wie diagnostiziere ich eine hohe CPU-Auslastung auf meiner EC2-Windows-Instance, wenn meine CPU nicht gedrosselt wird?

Überprüfen des Computernamens des WorkSpace

Wenn der Computername des Workspace geändert wurde, ändern Sie ihn wieder in den ursprünglichen Namen:

1. Öffnen Sie die Amazon- WorkSpaces Konsole und erweitern Sie dann die Option Unhealthy, WorkSpace um Details anzuzeigen.
2. Kopieren Sie den Computernamen.
3. Stellen Sie WorkSpace über RDP eine Verbindung mit dem her.
4. Öffnen Sie eine Eingabeaufforderung und geben Sie dann den Hostnamen ein, um den aktuellen Computernamen anzuzeigen.
   a. Wenn der Name mit dem Computernamen aus Schritt 2 übereinstimmt, fahren Sie mit dem nächsten Abschnitt zur Fehlerbehebung fort.
   b. Wenn die Namen nicht übereinstimmen, geben Sie sysdm.cpl ein, um die Systemeigenschaften zu öffnen, und folgen Sie dann den verbleibenden Schritten in diesem Abschnitt.
5. Wählen Sie Ändern und fügen Sie dann den Computernamen aus Schritt 2 ein.
6. Geben Sie bei Aufforderung die Anmeldeinformationen des Domain-Benutzers ein.
7. Vergewissern Sie sich, dass sich im Ausführungsstatus SkyLightWorkspaceConfigService befindet
   a. Überprüfen Sie unterServices, ob der WorkSpace Service ausgeführt SkyLightWorkspaceConfigServicewird. Wenn dies nicht der Fall ist, starten Sie den Service.

Überprüfen von Firewall-Regeln

Vergewissern Sie sich, dass die Windows-Firewall und alle ausgeführten Firewalls von Drittanbietern über Regeln verfügen, die die folgenden Ports zulassen:

- Eingehendes TCP auf Port 4172: Stellen Sie die Streaming-Verbindung her.
- Eingehendes UDP auf Port 4172: Stream-Benutzereingabe.
- Eingehendes TCP auf Port 8200: Verwalten und Konfigurieren der WorkSpace.
- Ausgehendes UDP auf Port 55002: PCoIP-Streaming.

Wenn die Firewall zustandslose Filterung verwendet, öffnen Sie die kurzlebigen Ports 49152-65535, um die Rückgabekommunikation zu ermöglichen.

Wenn die Firewall zustandsbehaftete Filterung verwendet, ist der flüchtige Port 55002 bereits geöffnet.

Sammeln eines WorkSpaces Support-Protokoll-Bundles zum Debuggen

Bei der Behebung von WorkSpaces Problemen ist es erforderlich, das Protokollpaket vom betroffenen WorkSpace und dem Host, auf dem der WorkSpaces Client installiert ist, zu sammeln. Es gibt zwei grundlegende Kategorien von Protokollen:

- Serverseitige Protokolle: Die WorkSpace ist in diesem Szenario der Server, daher handelt es sich um Protokolle, die auf der WorkSpace selbst existieren.
- Clientseitige Protokolle: Protokolliert auf dem Gerät, das der Endbenutzer zum Herstellen einer Verbindung mit dem verwendet WorkSpace.

- Nur Windows- und macOS-Clients schreiben Protokolle lokal.
- Null-Clients und iOS-Clients protokollieren nicht.
- Android-Protokolle werden im lokalen Speicher verschlüsselt und automatisch in das WorkSpaces Client-Engineering-Team hochgeladen. Nur dieses Team kann die Protokolle für Android-Geräte überprüfen.

Serverseitige WSP-Protokolle

Alle WSP-Komponenten schreiben ihre Protokolldateien in einen von zwei Ordnern:

- Primärer Standort: `C:\ProgramData\Amazon\WSP\` und `C:\ProgramData\NICE\dcv\log\`
- Speicherort des Archivs: `C:\ProgramData\Amazon\WSP\TRANSMITTED\`

Ändern der Ausführlichkeit von Protokolldateien unter Windows

Sie können die Ausführlichkeitsstufe der Protokolldatei für WSP Windows WorkSpaces im großen Maßstab konfigurieren, indem Sie die Gruppenrichtlinieneinstellung für die Ausführlichkeitsstufe der Protokolldatei konfigurieren.

Um die Ausführlichkeit der Protokolldatei für einzelne zu ändern WorkSpaces, konfigurieren Sie den `h_log_verbosity_options` Schlüssel mit dem Windows-Registrierungs-Editor:

1. Öffnen Sie den Windows-Registrierungseditor als Administrator.
2. Navigieren Sie zu `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. Wenn der `WSP` Schlüssel nicht vorhanden ist, klicken Sie mit der rechten Maustaste und wählen Sie Neu > Schlüssel und benennen Sie ihn `WSP`.
4. Navigieren Sie zu `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP`.
5. Wenn der `h_log_verbosity_options` Wert nicht vorhanden ist, klicken Sie mit der rechten Maustaste und wählen Sie Neu > DWORD und benennen Sie ihn `h_log_verbosity_options`.
6. Klicken Sie auf das neue `h_log_verbosity_options` DWORD und ändern Sie den Wert je nach erforderlicher Ausführlichkeitsstufe in eine der folgenden Zahlen:
   - 0 – Fehler
   - 1 – Warnung
   - 2 – Informationen
   - 3 – Debuggen
7. Klicken Sie auf OK und schließen Sie den Windows Registrierungs-Editor.
8. Starten Sie die neu WorkSpace.

Serverseitige PCoIP-Protokolle

Alle PCoIP-Komponenten schreiben ihre Protokolldateien in einen von zwei Ordnern:

- Primärer Standort: `C:\ProgramData\Teradici\PCoIPAgent\logs`
- Archivspeicherort: `C:\ProgramData\Teradici\logs`

Wenn Sie mit AWS Support an einem komplexen Problem arbeiten, ist es manchmal erforderlich, den PCoIP-Server-Agenten in den ausführlichen Protokollierungsmodus zu versetzen. So aktivieren Sie dies:

1. Öffnen Sie den folgenden Registrierungsschlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin_defaults`
2. Erstellen Sie im `pcoip_admin_defaults` Schlüssel das folgende 32-Bit-DWORD: `pcoip.event_filter_mode`
3. Setzen Sie den Wert für `pcoip.event_filter_mode` auf „3“ (Dez oder Hex).

Als Referenz sind dies die Protokollschwellenwerte, die in diesem DWORD definiert werden können.

- 0 – (CRITIC)
- 1 – (FEHLER)
- 2 – (INFO)
- 3 – (Debuggen)

Wenn das `pcoip_admin_default` DWORD nicht vorhanden ist, ist die Protokollebene 2 standardmäßig . Es wird empfohlen, einen Wert von 2 im DWORD wiederherzustellen, nachdem es keine ausführlichen Protokolle mehr benötigt, da sie viel größer sind und unnötig Speicherplatz belegen.

WebAccess serverseitige Protokolle

Für PCoIP und WSP (Version 1.0+) verwendet WorkSpacesder WorkSpaces Web-Access-Client den STXHD-Service. Die Protokolle für WorkSpaces Web Access werden unter gespeichert`C:\ProgramData\Amazon\Stxhd\Logs`.

Für WSP (Version 2.0+) werden WorkSpacesdie Protokolle für WorkSpaces Web Access unter gespeichert`C:\ProgramData\Amazon\WSP\`.

Clientseitige Protokolle

Diese Protokolle stammen von dem WorkSpaces Client, mit dem der Benutzer eine Verbindung herstellt, sodass sich die Protokolle auf dem Computer des Endbenutzers befinden. Die Speicherorte der Protokolldateien für Windows und Mac sind:

- Windows: `"%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\Logs"`
- macOS `~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs`:
- Linux: `~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs`

Um Probleme zu beheben, die Benutzer möglicherweise haben, aktivieren Sie die erweiterte Protokollierung, die auf jedem Amazon- WorkSpaces Client verwendet werden kann. Die erweiterte Protokollierung ist für jede nachfolgende Clientsitzung aktiviert, bis sie deaktiviert ist.

1. Bevor der Endbenutzer eine Verbindung mit dem herstellt WorkSpace, sollte er die erweiterte Protokollierung für seinen Client aktivieren. WorkSpaces
2. Der Endbenutzer sollte dann wie gewohnt eine Verbindung herstellen, seine verwenden und versuchen WorkSpace, das Problem zu reproduzieren.
3. Die erweiterte Protokollierung erstellt Protokolldateien mit Diagnoseinformationen und Details auf Debugging-Ebene, einschließlich Verbose-Leistungsdaten.

Diese Einstellung bleibt bestehen, bis sie explizit deaktiviert wird. Nachdem der Benutzer das Problem mit der ausführlichen Protokollierung erfolgreich reproduziert hat, sollte diese Einstellung deaktiviert werden, da große Protokolldateien generiert werden.

Automatisierte serverseitige Protokollpaketerfassung für Windows

Das `Get-WorkSpaceLogs.ps1` Skript ist hilfreich, um schnell ein serverseitiges Protokollpaket für zu sammeln AWS Support. Das Skript kann von angefordert werden, AWS Support indem es in einem Support-Fall angefordert wird:

1. Stellen Sie WorkSpace über den Client oder über das Remote Desktop Protocol (RDP) eine Verbindung mit dem her.
2. Starten Sie eine administrative Eingabeaufforderung (führen Sie als Administrator aus).
3. Starten Sie das Skript über die Eingabeaufforderung mit dem folgenden Befehl:

```
powershell.exe -NoLogo -ExecutionPolicy RemoteSigned -NoProfile -File "C:\Program
 Files\Amazon\WorkSpacesConfig\Scripts\Get-WorkSpaceLogs.ps1"
```

4. Das Skript erstellt ein Protokollpaket auf dem Desktop des Benutzers.

   Das Skript erstellt eine ZIP-Datei mit den folgenden Ordnern:

   - C – Enthält die Dateien aus Programmdateien, Programmdateien (x86) und Windows ProgramDataim Zusammenhang mit Bollight, EC2Config, Teradici, Event Viewer und Windows-Protokollen (Panther und andere).
   - CliXML – Enthält XML-Dateien, die in Powershell importiert werden können, indem `Import-CliXML` für die interaktive Filterung verwendet wird. Weitere Informationen finden Sie unter Import-Clixml.
   - Config – Detaillierte Protokolle für jede durchgeführte Prüfung
   - ScriptLogs – Protokolliert die Skriptausführung (nicht relevant für die Untersuchung, aber nützlich, um zu debuggen, was das Skript macht).
   - tmp – Vorübergehender Ordner (er sollte leer sein).
   - Ablaufverfolgungen – Die Paketerfassung wurde während der Protokollerfassung durchgeführt.

So überprüfen Sie die Latenz zur nächstgelegenen AWS Region

Die Website Connection Health Check prüft schnell, ob alle erforderlichen Services, die Amazon verwenden, erreicht werden WorkSpaces können. Außerdem wird für jede AWS Region, in der Amazon verfügbar WorkSpaces ist, eine Leistungsprüfung durchgeführt und die Benutzer werden darüber informiert, welche Region am schnellsten sein wird.

Schlussfolgerung

Es gibt einen strategischen Wandel beim Endbenutzer-Computing, da Organisationen versuchen, agiler zu sein, ihre Daten besser zu schützen und ihren Mitarbeitern zu helfen, produktiver zu sein. Viele der bereits mit Cloud Computing erzielten Vorteile gelten auch für Endbenutzer-Computing. Durch das Verschieben ihrer Windows- oder Linux-Desktops in die AWS Cloud mit Amazon können Organisationen schnell skalieren WorkSpaces, wenn sie Worker hinzufügen, ihren Sicherheitsstatus verbessern, indem sie Daten außerhalb von Geräten halten, und ihren Workern mithilfe des Geräts ihrer Wahl einen portablen Desktop mit Zugriff von überall aus anbieten.

Amazon WorkSpaces ist so konzipiert, dass es in bestehende IT-Systeme und -Prozesse integriert werden kann, und in diesem Whitepaper wurden die bewährten Methoden dafür beschrieben. Das Ergebnis der Einhaltung der Richtlinien in diesem Whitepaper ist eine kostengünstige Cloud-Desktop-Bereitstellung, die mit Ihrem Unternehmen in der AWS globalen -Infrastruktur sicher skaliert werden kann.

Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Bol, EUC-Lösungsarchitekt, Amazon Web Services
- Don Bol, Sr. EUC Specialized, Amazon Web Services
- Klaus Becker, Sr. EUC Architect, Amazon Web Services
- Naviero Magicee, Architektur für Prinzipallösungen, Amazon Web Services
- Bol Fountain, EUC Specialized, Amazon Web Services
- Stephen Stetler, Sr. EUC Solutions Architect, Amazon Web Services

Weitere Informationen

Weitere Informationen finden Sie unter:

- Amazon- WorkSpaces Administratorhandbuch
- Amazon- WorkSpaces Entwicklerhandbuch
- Amazon WorkSpaces -Clients
- Verwalten von Amazon Linux 2 Amazon WorkSpaces mit AWS OpsWorks für Puppet Enterprise
- Anpassen von Amazon Linux WorkSpace
- So verbessern Sie die LDAP-Sicherheit in AWS Directory Service mit clientseitigem LDAPS
- Verwenden von Amazon CloudWatch Events mit Amazon WorkSpaces und AWS Lambda für eine bessere Flottentransparenz
- So WorkSpaces verwendet Amazon AWS KMS
- AWS CLI -Befehlsreferenz – WorkSpaces
- Überwachen von Amazon- WorkSpaces Metriken
- MATE-Desktop-Umgebung
- Fehlerbehebung bei Problemen mit der AWS Directory-Service-Verwaltung
- Fehlerbehebung bei Amazon- WorkSpaces Administrationsproblemen
- Fehlerbehebung bei Amazon WorkSpaces Client-Problemen
- Automatisieren von Amazon WorkSpaces mit einem Self-Service-Portal

Dokumentversionen

Um über Aktualisierungen dieses Whitepapers benachrichtigt zu werden, abonnieren Sie den RSS-Feed.

Änderung	Beschreibung	Datum
Kleines Update	Aktualisierter Inhalt für AD Directory Services, Notfallwiederherstellung/Geschäftskontinuität und regionsübergreifende Umleitung. WorkSpaces & Audiooptimierung von Amazon Connect hinzugefügt. Kleinere Aktualisierungen der Formatierung.	26. Mai 2022
Kleines Update	Korrigiert Nicht-inklusive-Sprache.	6. April 2022
Whitepaper aktualisiert	Aktualisierter Inhalt	24. März 2022
Whitepaper aktualisiert	Aktualisierter Inhalt für AWS Network Firewall, MAD-replizierte Verzeichnisse, YubiKey Support, Container, WSLv1, Smartcard-Unterstützung, WorkSpaces Service Quota und vertrauenswürdige Geräte.	20. Dezember 2021
Whitepaper aktualisiert	Aktualisierter Inhalt für WorkSpaces Streaming Protocol, Smartcard-Authentifizierung, Diagramme, Client-Bereitstellungen, Endgeräteauswahl und Webzugriff	28. April 2021

Whitepaper aktualisiert	Aktualisierter Inhalt	1. Dezember 2020
Whitepaper aktualisiert	Inhalt seit der ersten Veröffentlichung aktualisiert und neue Diagramme hinzugefügt.	1. Mai 2020
Erste Veröffentlichung	Erst veröffentlicht.	1. Juli 2016

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und -praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) erstellt keine Verpflichtungen oder Zusicherungen von AWS und seinen Partnern, Lieferanten oder Benutzern. - AWS Produkte oder -Services werden „im Ist-Zustand“ ohne Garantien, Darstellungen oder Bedingungen irgendwelcher Art bereitgestellt, weder ausdrücklich noch implizit. Die Verantwortlichkeiten und Haftung von AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen gesteuert, und dieses Dokument ist nicht Teil einer Vereinbarung zwischen AWS und seinen Kunden und ändert sie auch nicht.

AWS Glossar

Die neueste AWS Terminologie finden Sie im -AWS Glossar in der AWS-Glossar -Referenz.

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.