Bewährte Methoden zum Bereitstellen von Amazon WorkSpaces

Netzwerkzugriff, Directory Services und Sicherheit

Juli 2016

Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Praktiken von AWS zum Erstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind für ihre eigene unabhängige Einschätzung der Informationen in diesem Dokument und jedwede Nutzung der AWS-Services verantwortlich. Jeder Service wird „wie besehen“ ohne Gewähr und ohne Garantie jeglicher Art, weder ausdrücklich noch impliziert, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertragliche Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Übersicht

Dieses Whitepaper beschreibt eine Reihe von bewährten Methoden für die Bereitstellung von Amazon WorkSpaces. Behandelt werden Überlegungen zum Netzwerk, dazu die Themen Sicherheit, Verzeichnisdienste und Benutzerauthentifizierung sowie Überwachung und Protokollierung.

Für den schnellen Zugriff auf relevante Informationen ist dieses Dokument in vier Hauptabschnitte unterteilt. Es wendet sich an Experten, die für das Netzwerk, das Verzeichnis oder die Sicherheit zuständig sind.

Einführung

Amazon WorkSpaces ist ein verwalteter Service für Desktop-Computing in der Cloud. Mit Amazon WorkSpaces entfallen das Beschaffen und Bereitstellen von Hardware sowie komplexe Software-Installationen. Ein Desktop ist mit wenigen Klicks in der AWS Management Console eingerichtet. Oder verwenden Sie dazu die AWS-Befehlszeilenschnittstelle (Command Line Interface, CLI) bzw. die APIs. Mit Amazon WorkSpaces dauert es nur wenige Minuten, um einen Desktop zu starten und die Verbindung zu Ihrer Desktop-Software in einem lokalen oder externen Netzwerk sicher, zuverlässig und schnell herzustellen. Sie haben folgende Möglichkeiten:

- Weiterverwenden Ihres lokalen Microsoft Active Directory (AD) mithilfe von AWS Directory Service: AD Connector
- Erweitern Ihres Verzeichnisses in die AWS Cloud
- Erstellen eines verwalteten Verzeichnisses mithilfe von AWS Directory Service: Microsoft AD oder Simple AD zur Verwaltung Ihrer Benutzer und WorkSpaces

Mit AD Connector haben Sie zudem die Möglichkeit, Multi-Faktor-Authentifizierung (MFA) über Ihren lokalen oder in der Cloud gehosteten RADIUS-Server für Ihre WorkSpaces bereitzustellen.

Sie können die Bereitstellung von Amazon WorkSpaces automatisieren, indem Sie Amazon WorkSpaces mithilfe der CLI oder APIs in Ihren bestehenden Bereitstellungsablauf integrieren.

Zusätzlich zur integrierten Netzwerkverschlüsselung, die der WorkSpaces-Service bereitstellt, können Sie die Verschlüsselung der ruhenden Daten in Ihren WorkSpaces aktivieren (siehe Verschlüsselte WorkSpaces im Abschnitt „Sicherheit“).

Anwendungen stellen Sie in Ihren WorkSpaces entweder mithilfe vorhandener lokaler Tools wie Microsoft System Center Configuration Manager (SCCM) oder dem Amazon WorkSpaces Application Manager (Amazon WAM) bereit.

Die folgenden Abschnitte enthalten Details über Amazon WorkSpaces. Erläutert wird, wie der Service funktioniert und welche Voraussetzungen für den Start erfüllt sein müssen. Zudem erfahren Sie, welche Optionen und Funktionen zur Verfügung stehen.

Voraussetzungen für WorkSpaces

Der Amazon WorkSpaces-Service erfordert, dass drei Komponenten erfolgreich installiert werden:

- **WorkSpaces-Clientanwendung**. Ein von Amazon WorkSpaces unterstütztes Clientgerät. Eine vollständige Liste finden Sie unter Supported Platforms and Devices.

  Sie können auch Zero-Clients verwenden und über PCoIP (Personal Computer over Internet Protocol) eine Verbindung mit WorkSpaces herstellen. Eine Liste verfügbarer Geräte finden Sie unter PCoIP Zero Clients for Amazon WorkSpaces.
- **Ein Verzeichnisdienst, der einen Benutzer authentifiziert und ihm den Zugang zu seinem WorkSpace ermöglicht.** Amazon WorkSpaces unterstützt derzeit AWS Directory Service und Active Directory. Sie können Ihren lokalen Active Directory-Server zusammen mit AWS Directory Service verwenden, um vorhandene Anmeldeinformationen Ihrer Benutzer für WorkSpaces zu unterstützen.
- **Amazon Virtual Private Cloud (Amazon VPC), in der Ihre Amazon WorkSpaces ausgeführt werden**. Sie benötigen mindestens zwei Subnetze für eine WorkSpaces-Bereitstellung, weil jedes AWS Directory Service-Konstrukt in einer Multi-AZ-Bereitstellung zwei Subnetze erfordert.

Überlegungen zum Netzwerk

Jeder WorkSpace ist mit einer bestimmten Amazon VPC und dem AWS Directory Service-Konstrukt verknüpft, mit dem er erstellt wurde. Alle AWS Directory Service-Konstrukte (Simple AD, AD Connector und Microsoft AD) benötigen für ihren Betrieb zwei Subnetze, jedes in einer anderen Availability Zone. Subnetze sind einem Directory Service-Konstrukt dauerhaft zugeordnet und können nicht geändert werden, nachdem ein AWS Directory Service erstellt wurde. Es ist daher zwingend notwendig, dass Sie die richtigen Subnetzgrößen wählen, bevor Sie das Directory Services-Konstrukt erstellen. Klären Sie deshalb folgende Fragen, bevor Sie die Subnetze erstellen:

- Wie viele WorkSpaces werden im Lauf der Zeit benötigt? Welches Wachstum ist zu erwarten?
- Welche Arten von Benutzern sollen unterstützt werden?
- Wie viele Active Directory-Domänen werden angeschlossen?
- Wo sind die Benutzerkonten Ihres Unternehmens gespeichert?

Amazon empfiehlt, Benutzergruppen (Personas) einzurichten, die auf der geplanten Zugriffsart und Benutzerauthentifizierung basieren. Das ist von Vorteil, wenn Sie den Zugriff auf bestimmte Anwendungen und Ressourcen beschränken müssen. Durch definierte Benutzergruppen und mithilfe von AWS Directory Service, Netzwerk-Zugriffskontrolllisten, Routing-Tabellen und VPC-Sicherheitsgruppen können Sie Zugriffe segmentieren und beschränken. Jedes AWS Directory Service-Konstrukt verwendet zwei Subnetze und wendet die gleichen Einstellungen auf alle WorkSpaces an, die von diesem Konstrukt starten. Zum Beispiel können Sie eine Sicherheitsgruppe für alle WorkSpaces verwenden, die einem AD Connector zugeordnet sind, um festzulegen, ob MFA erforderlich ist, oder ob der Endbenutzer mit den Rechten eines lokalen Administrators auf seinen WorkSpace zugreifen darf.

> **Hinweis:** Jeder AD Connector ist mit einer Organisationseinheit (Organizational Unit, OU) im Microsoft Active Directory verknüpft. Um von den Vorteilen zu profitieren, die Benutzergruppen bieten, müssen Sie Ihren Directory Service so erstellen, dass er Ihre Benutzergruppen berücksichtigt.

In diesem Abschnitt werden bewährte Methoden zum Dimensionieren von VPC, Subnetzen und Datenverkehrsfluss beschrieben sowie Überlegungen für den Entwurf von Verzeichnisdiensten erörtert.

VPC-Entwurf

Sie sollten beim Entwerfen von VPC, Subnetzen, Sicherheitsgruppen, Routing-Richtlinien und Netzwerk-ACLs für Ihre Amazon WorkSpaces folgendes beachten, damit Ihre WorkSpaces-Umgebung skalierbar, sicher und einfach zu verwalten ist:

- **VPC**. Wir empfehlen, eine separate VPC speziell für die WorkSpaces-Bereitstellung zu verwenden. Mit einer separaten VPC können Sie die notwendigen Überwachungs- und Sicherheitsmaßnamen für Ihre WorkSpaces durch Datenverkehrstrennung ermöglichen.
- **Verzeichnisdienste**. Jedes AWS Directory Service-Konstrukt erfordert ein Subnetzpaar, um einen hochverfügbaren Verzeichnisdienst über Amazon AZs hinweg sicherzustellen.
- **Subnetzgröße**. WorkSpaces-Bereitstellungen sind an ein Verzeichniskonstrukt gebunden und befinden sich in denselben VPC-Subnetzen wie der ausgewählte AWS Directory Service. Dazu einige Anmerkungen:
  - Subnetzgrößen sind statisch und können nicht geändert werden. Berücksichtigen Sie daher auch zukünftiges Wachstum bei der Größenfestlegung.
  - Sie können eine Standardsicherheitsgruppe für den ausgewählten AWS Directory Service festlegen. Eine Sicherheitsgruppe gilt für alle WorkSpaces, die dem jeweiligen AWS Directory Service-Konstrukt zugeordnet sind.
  - Ein Subnetz kann von mehreren AWS Directory Services verwendet werden.

Ziehen Sie in Ihrem VPC-Entwurf zukünftige Erweiterungen in Betracht. Möglicherweise möchten Sie später Verwaltungskomponenten wie einen Antivirusserver, einen Server für das Patch-Management, einen Active Directory-Server oder einen RADIUS MFA-Server hinzufügen. Für derartige Komponenten sollten Sie zusätzliche IP-Adressen in Ihrem VPC-Entwurf vorsehen.

Detaillierte Anleitungen und Überlegungen zum VPC- und Subnetzentwurf finden Sie in der **re:Invent**-Präsentation How Amazon.com is Moving to Amazon WorkSpaces.

Netzwerkschnittstellen

Jeder WorkSpace verfügt über zwei Elastic Network Interfaces (ENIs), eine Verwaltungs-Netzwerkschnittstelle (eth0) und eine primäre Netzwerkschnittstelle (eth1). AWS verwendet die Verwaltungs-Netzwerkschnittstelle zur WorkSpace-Verwaltung – an dieser Schnittstelle wird Ihre Clientverbindung terminiert. AWS nutzt für diese Schnittstelle einen privaten IP-Adressbereich. Damit korrektes Netzwerk-Routing möglich ist, können Sie diesen privaten Adressraum nicht in jedem Netzwerk verwenden, das mit Ihrem WorkSpaces-VPC kommunizieren kann.

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

> **Hinweis:** Amazon WorkSpaces und die zugehörigen Verwaltungs-Netzwerkschnittstellen befinden sich nicht in Ihrer VPC, und Sie können weder die Instance-ID der Verwaltungs-Netzwerkschnittstelle noch die der Amazon Elastic Compute Cloud (Amazon EC2) in Ihrer AWS Management Console anzeigen (siehe Abbildung 4, Abbildung 5 und Abbildung 6). Sie können jedoch die Sicherheitsgruppeneinstellungen Ihrer primären Netzwerkschnittstelle (eth1) in der AWS Management Console anzeigen und ändern. Die primäre Netzwerkschnittstelle in jedem WorkSpace wird auf Ihr ENI Amazon EC2-Ressourcenlimit angerechnet. Für große Bereitstellungen von WorkSpaces müssen Sie in der AWS Management Console ein Support-Ticket öffnen, um Ihre ENI-Limits zu erhöhen.

Datenverkehrsfluss

Der Amazon WorkSpaces betreffende Datenverkehrsfluss kann in zwei Kategorien unterteilt werden:

- Datenverkehr zwischen dem Clientgerät und dem Amazon WorkSpaces-Service
- Datenverkehr zwischen dem Amazon WorkSpaces-Service und dem Kundennetzwerk

Diese beiden Kategorien werden im nächsten Abschnitt erläutert.

Datenverkehr Clientgerät zu WorkSpace

Das Gerät, auf dem der Amazon WorkSpaces-Client ausgeführt wird, verwendet unabhängig von seinem Standort (lokal oder remote) dieselben beiden Ports für die Verbindung mit dem WorkSpaces-Service. Der Client verwendet HTTPS über Port 443 für alle Informationen bezüglich Authentifizierung und Sitzung. Port 4172 (PCoIP-Port) wird sowohl mit TCP als auch UDP für das Pixel-Streaming zu einem bestimmten WorkSpace sowie zur Prüfung des Netzwerkzustands verwendet. Der Datenverkehr über beide Ports erfolgt verschlüsselt. Die über Port 443 gesendeten Authentifizierungs- und Sitzungsinformationen werden per TLS verschlüsselt. Beim Pixel-Streaming über das Streaming-Gateway zwischen dem Client und der Schnittstelle eth0 im WorkSpace werden die Daten mit AES-256 verschlüsselt. Weitere Informationen dazu finden Sie weiter unten im Abschnitt Sicherheit.

Wir veröffentlichen für jede Region die IP-Bereiche unserer PCoIP-Streaming-Gateways und Endpunkte für Netzwerkzustandsprüfungen. Sie können den aus dem Firmennetz über Port 4172 ausgehenden Datenverkehr zum AWS-Streaming-Gateway und den Endpunkten für Netzwerkzustandsprüfungen begrenzen, indem Sie auf Port 4172 nur ausgehenden Datenverkehr in die AWS-Regionen erlauben, in denen Sie Amazon WorkSpaces verwenden. Informationen über IP-Bereiche und Endpunkte für Netzwerkzustandsprüfungen finden Sie unter Amazon WorkSpaces PCoIP Gateway IP Ranges.

Der Amazon WorkSpaces-Client verfügt über eine integrierte Netzwerkzustandsprüfung. Dieses Dienstprogramm meldet dem Benutzer über eine Statusanzeige in der rechten unteren Ecke der Anwendung, ob sein Netzwerk eine Verbindung unterstützt. Eine detailliertere Ansicht des Netzwerkzustands (siehe Abbildung 1) kann durch Auswahl von **Network** rechts unten im Client aufgerufen werden.

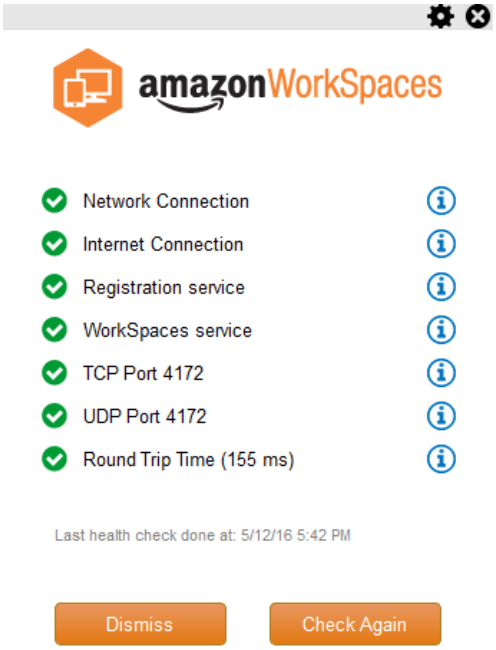

Abbildung 1: WorkSpaces-Client – Netzwerk-Check

Ein Benutzer initiiert eine Verbindung von seinem Client zum WorkSpaces-Service, indem er seine Anmeldedaten an das vom Directory Service-Konstrukt verwendete Verzeichnis (üblicherweise sein Firmenverzeichnis) übergibt. Die Anmeldeinformationen werden über HTTPS an das Authentifizierungs-Gateway des Amazon WorkSpaces-Service in der Region gesendet, zu welcher der WorkSpace gehört. Das Authentifizierungs-Gateway des Amazon WorkSpaces-Service leitet den Datenverkehr dann an das AWS Directory Service-Konstrukt weiter, das Ihrem WorkSpace zugeordnet ist. Beispielsweise übergibt ein AD Connector die Authentifizierungsanforderung direkt an Ihren lokalen oder in einer AWS VPC befindlichen Active Directory-Service (siehe AD DS-Bereitstellungsszenarien). Der AD Connector speichert keine Authentifizierungsinformationen und fungiert als zustandsloser Proxy. Deshalb benötigt der AD Connector eine aktive Verbindung mit einem Active Directory-Server. Der AD Connector bestimmt den Active Directory-Server, mit dem er eine Verbindung herstellt, mithilfe der DNS-Server, die Sie bei der AD Connector-Erstellung definiert haben.

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

Sobald ein Benutzer authentifiziert ist, werden die Streaming-Daten über Port 4172 (PCoIP-Port) und das AWS Streaming-Gateway zum WorkSpace übertragen. Sitzungsbezogene Informationen werden während einer Sitzung weiterhin über HTTPS ausgetauscht. Der Streaming-Datenverkehr verwendet die erste WorkSpace-ENI (eth0 im WorkSpace), die nicht mit Ihrer VPC verbunden ist. Die Netzwerkverbindung zwischen Streaming-Gateway und ENI wird von AWS verwaltet. Sollte zwischen einem Streaming-Gateway und einer WorkSpaces-Streaming-ENI ein Verbindungsfehler auftreten, wird ein CloudWatch-Ereignis erzeugt (siehe dazu den Abschnitt Überwachen und Protokollieren mit Amazon CloudWatch in diesem Whitepaper).

Die zwischen Amazon WorkSpaces-Service und Client übertragene Datenmenge ist abhängig von der Pixelaktivität. Um eine optimale Benutzererfahrung zu gewährleisten, empfehlen wir, dass die Umlaufzeit (Round Trip Time, RTT) zwischen dem WorkSpaces-Client und der AWS-Region, zu der Ihre WorkSpaces gehören, weniger als 100 ms beträgt. Normalerweise bedeutet dies, dass Ihr WorkSpaces-Client höchstens 3200 km von der Region entfernt sein darf, in der Ihr WorkSpace gehostet wird. Auf der Webseite Connection Health Check können Sie die optimale AWS-Region für eine Verbindung mit dem Amazon WorkSpaces-Service ermitteln.

Datenverkehr Amazon WorkSpaces-Service zu VPC

Nachdem eine Verbindung von einem Client zu einem WorkSpace authentifiziert und der Streaming-Datenverkehr initiiert ist, zeigt der WorkSpaces-Client einen Windows-Desktop (Ihren WorkSpace) an, der mit Ihrer VPC verbunden ist, und Ihr Netzwerk sollte signalisieren, dass Sie die Verbindung hergestellt haben. Der primären, als eth1 identifizierten ENI für den WorkSpace wird vom Dynamic Host Configuration Protocol (DHCP)-Service eine IP-Adresse zugewiesen, die von Ihrer VPC bereitgestellt wird und in der Regel zum gleichen Subnetz gehört wie Ihr AWS Directory Service. Diese IP-Adresse bleibt für die WorkSpace-Lebensdauer unverändert. Die zu Ihrer VPC gehörende ENI 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 Netzwerkressourcen wird durch die Standardsicherheitsgruppe bestimmt (mehr zu Sicherheitsgruppen finden Sie hier>), die Ihr AWS Directory Service für jeden WorkSpace konfiguriert, und durch alle zusätzlichen Sicherheitsgruppen, die Sie der ENI zugeordnet haben. Sie können Sicherheitsgruppen für die ENI Ihrer VPC nach Bedarf über die AWS Management Console oder die CLI hinzufügen. Neben Sicherheitsgruppen können Sie Ihre bevorzugte hostbasierte Firewall auf einem bestimmten WorkSpace verwenden, um den Netzwerkzugriff auf die Ressourcen innerhalb der VPC zu begrenzen.

Abbildung 4 in AD DS-Bereitstellungsszenarien weiter unten in diesem Whitepaper zeigt den zuvor beschriebenen Datenfluss.

Beispiel für eine typische Konfiguration

Betrachten wir ein Szenario mit zwei Arten von Benutzern und einem AWS Directory Service, der ein zentrales Active Directory zur Benutzerauthentifizierung verwendet:

- **Mitarbeiter, die überall vollen Zugriff benötigen** (beispielsweise Vollzeitmitarbeiter). Diese Benutzer haben vollen Zugriff auf das Internet und das interne Netzwerk. Sie passieren eine Firewall zwischen der VPC und dem lokalen Netzwerk.
- **Mitarbeiter, die nur über eingeschränkten Zugriff aus dem Unternehmensnetzwerk heraus verfügen** (beispielsweise Auftragnehmer und Berater). Diese Benutzer haben eingeschränkten Zugriff auf das Internet (auf bestimmte Websites) über einen Proxy-Server in der VPC sowie eingeschränkten Zugriff in der VPC und im lokalen Netzwerk.

Sie möchten den Vollzeitmitarbeitern die Möglichkeit geben, mit den Rechten eines lokalen Administrators auf ihren WorkSpace zuzugreifen, damit sie Software installieren können, und Sie möchten Zwei-Faktor-Authentifizierung mit MFA erzwingen. Zudem sollen Vollzeitmitarbeiter über ihren WorkSpace uneingeschränkten Zugriff auf das Internet erhalten.

Für Auftragnehmer soll der Zugriff mit lokalen Administratorrechten blockiert sein, sodass sie nur bestimmte vorinstallierte Anwendungen verwenden können. Für diese WorkSpaces möchten Sie sehr restriktive Netzzugangskontrollen über Sicherheitsgruppen anwenden. Die Ports 80 und 443 müssen nur bestimmten internen Websites offenstehen und sollen nicht für den Internetzugang geöffnet sein.

Dieses Szenario umfasst zwei völlig verschiedene Benutzergruppen mit unterschiedlichen Anforderungen für den Netzwerk- und Desktop-Zugriff. Es hat sich bewährt, auch ihre WorkSpaces auf unterschiedliche Weise zu verwalten und zu konfigurieren. Dazu müssen Sie zwei AD Connectors erstellen, einen für jede Benutzergruppe. Jeder AD Connector benötigt zwei Subnetze mit genügend IP-Adressen, um das voraussichtliche Wachstum Ihrer WorkSpaces abzudecken.

> **Hinweis:** Jedes AWS VPC-Subnetz belegt fünf IP-Adressen (die ersten vier und die letzte) für Verwaltungszwecke, und jeder AD Connector belegt eine IP-Adresse in jedem Subnetz, in dem er enthalten ist.

Für dieses Szenario gilt zudem:

- AWS VPC-Subnetze sollten private Subnetze sein, so dass Datenverkehr wie z. B. Internetaktivitäten entweder mit einem NAT-Gateway (bzw. Proxy-NAT-Server in der Cloud) kontrolliert oder durch Ihr lokales Verkehrsverwaltungssystem zurückgeleitet werden kann.
- Für den VPC-Datenverkehr durch das lokale Netzwerk ist eine Firewall eingerichtet.
- Microsoft Active Directory-Server und die MFA-RADIUS-Server sind entweder lokale Server (siehe Szenario 1: Verwendung von AD Connector zum Weiterleiten der Authentifizierung an ein **lokales AD DS**) oder Teil der AWS Cloud-Implementierung (siehe Szenarien 2 und 3 in AD DS-Bereitstellungsszenarien).

Wenn in allen WorkSpaces in irgendeiner Weise der Zugriff auf das Internet möglich sein soll und sie in einem privaten Subnetz gehostet werden, müssen Sie öffentliche Subnetze erstellen, die über ein Internet-Gateway Zugriff auf das Internet haben. Sie benötigen ein NAT-Gateway für die Vollzeitmitarbeiter, damit diese auf das Internet zugreifen können, und einen Proxy-NAT-Server für die Berater und Auftragnehmer, um deren Zugriff auf bestimmte interne Websites zu beschränken. Um hohe Verfügbarkeit sicherzustellen, Ausfälle abzufangen und die Kosten für AZ-übergreifenden Verkehr zu minimieren, sollten Sie in einer Multi-AZ-Bereitstellung zwei NAT-Gateways und NAT- oder Proxy-Server in zwei verschiedenen Subnetzen installieren. Die beiden AZs, die Sie als öffentliche Subnetze auswählen, werden den beiden AZs entsprechen, die Sie für Ihre WorkSpaces-Subnetze in Regionen verwenden, die mehr als zwei AZs umfassen. Sie können den gesamten Datenverkehr von jeder WorkSpaces-AZ in das entsprechende öffentliche Subnetz routen, um so Gebühren für AZ-übergreifenden Datenverkehr zu sparen und eine einfachere Verwaltung zu ermöglichen. In Abbildung 2 ist die VPC-Konfiguration dargestellt.

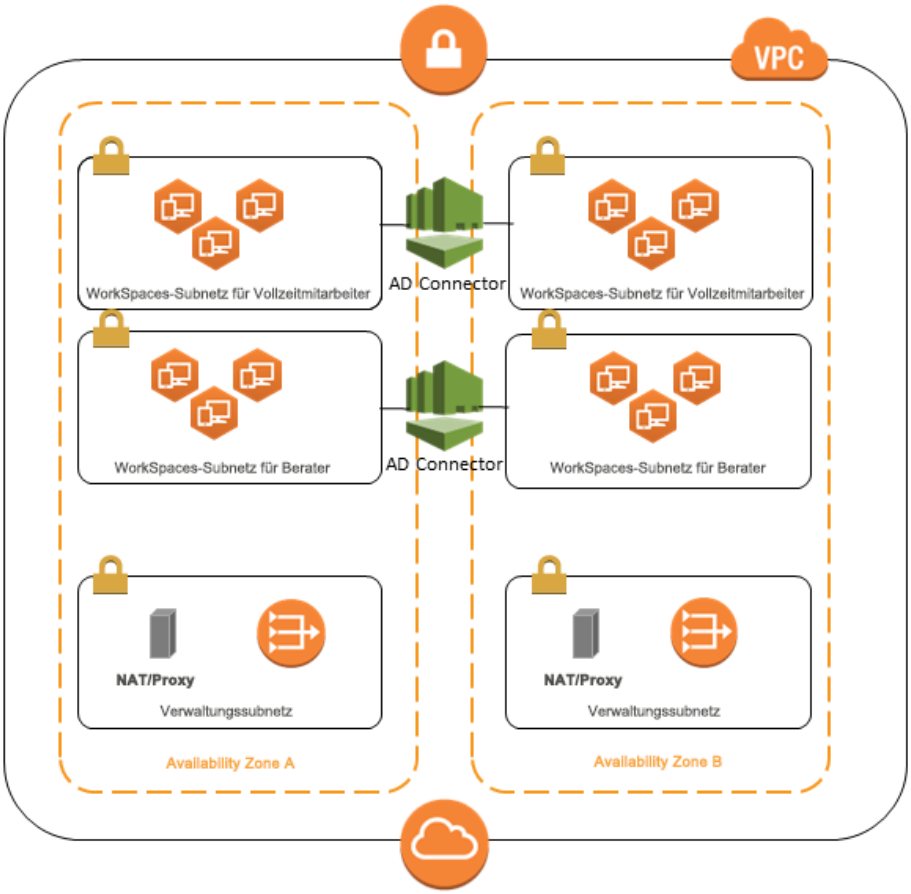

Abbildung 2: Effizienter VPC-Entwurf

Im Folgenden wird erläutert, wie die beiden unterschiedlichen, weiter oben im Dokument vorgestellten WorkSpaces-Typen konfiguriert werden.

- **Vollzeitmitarbeiter:** Wählen Sie in der Amazon WorkSpaces Management Console in der Menüleiste die Option **Directories**, wählen Sie das Verzeichnis, in dem Ihre Vollzeitmitarbeiter gehostet werden, und wählen Sie dann **Local Administrator Setting**. Nachdem Sie diese Option aktiviert haben, werden alle neu erstellten WorkSpaces mit lokalen Administratorberechtigungen ausgestattet. Um Internetzugang zu gewähren, müssen Sie die Network Address Translation (NAT) für Internetzugriffe konfigurieren, die von Ihrer VPC ausgehen. Zur Aktivierung von MFA müssen Sie einen RADIUS-Server, Server-IPs, Ports und ein Kennwort angeben.

Für die WorkSpaces der Vollzeitmitarbeiter können Sie den eingehenden Datenverkehr aus dem Helpdesk-Subnetz auf das Remote Desktop Protocol (RDP) beschränken, indem Sie über die AD Connector-Einstellungen eine Standardsicherheitsgruppe anwenden.

- **Auftragnehmer und Berater:** Deaktivieren Sie in der Amazon WorkSpaces Management Console die Optionen **Internet Access** und **Local Administrator Setting**. Dann fügen Sie im Abschnitt **Security Group** eine Sicherheitsgruppe hinzu. Sie erzwingen damit eine Sicherheitsgruppe für alle neuen WorkSpaces, die in diesem Verzeichnis erstellt werden.

  Für Berater-WorkSpaces beschränken Sie den ein- und ausgehenden Datenverkehr auf diese WorkSpaces, indem Sie über die AD Connector-Einstellungen eine Standardsicherheitsgruppe auf alle WorkSpaces anwenden, die dem AD Connector zugeordnet sind. Die Sicherheitsgruppe lässt auf den WorkSpaces nur ausgehenden HTTP- und HTTPS-Datenverkehr zu und nur eingehenden RDP-Datenverkehr aus dem Helpdesk-Subnetz im lokalen Netz.

> **Hinweis:** Die Sicherheitsgruppe gilt nur für die ENI in der VPC (eth1 im WorkSpace). Der Zugriff auf den WorkSpace über den WorkSpaces-Client wird nicht durch eine Sicherheitsgruppe beschränkt. Abbildung 3 zeigt den endgültigen WorkSpaces-VPC-Entwurf, der weiter oben im Dokument beschrieben wurde.

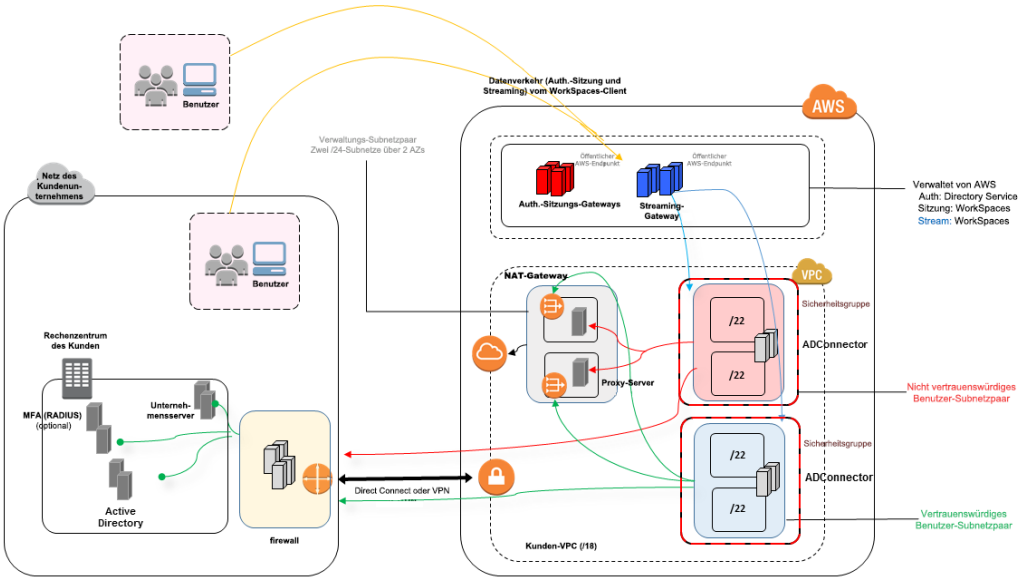

Abbildung 3: WorkSpaces-Entwurf mit Benutzergruppen

AWS Directory Service

Wie in der Einleitung erwähnt, wird Amazon WorkSpaces von AWS Directory Service unterstützt. Mit AWS Directory Service können Sie drei Arten von Verzeichnissen erstellen. Die beiden ersten sind in der AWS Cloud angesiedelt:

- AWS Directory Service für Microsoft Active Directory (Enterprise Edition) oder kurz **Microsoft AD** ist ein verwalteter Verzeichnisdienst von Microsoft in Windows Server 2012 R2.
- **Simple AD** ist ein eigenständiger, verwalteter und zu Microsoft Active Directory kompatibler Verzeichnisdienst unter Samba 4.

Das dritte, **AD Connector,** ist ein Verzeichnis-Gateway, mit dem Sie Authentifizierungsanfragen und Benutzer- oder Gruppen-Lookups an Ihr vorhandenes lokales Microsoft Active Directory weiterleiten können.

Im folgenden Abschnitt werden die zur Authentifizierung erforderlichen Kommunikationsströme zwischen Amazon WorkSpaces Brokerage-Service und AWS Directory Service beschrieben, bewährte Methoden zur Implementierung von WorkSpaces mit AWS Directory Service vorgestellt und anspruchsvolle Konzepte wie MFA erläutert. Wir stellen zudem Konzepte für die Infrastrukturarchitektur skalierender Amazon WorkSpaces vor und erläutern die Voraussetzungen für Amazon VPC, AWS Directory Service und die Integration eines lokalen Microsoft AD DS (Active Directory Domain Services).

AD DS-Bereitstellungsszenarien

Amazon WorkSpaces basieren auf AWS Directory Service. Daher sind der korrekte Entwurf und die richtige Bereitstellung des Verzeichnisdiensts von entscheidender Bedeutung. Die folgenden drei Szenarien beziehen sich auf die Kurzanleitung für *Microsoft Active Directory Domain Services*. Vorgestellt werden bewährte Bereitstellungsoptionen für AD DS im Zusammenhang mit WorkSpaces. Der Abschnitt *Überlegungen zum* Entwurf dieses Kapitels befasst sich mit den spezifischen Anforderungen und bewährten Methoden bezüglich der Verwendung von AD Connector für WorkSpaces, die ein wesentlicher Bestandteil des gesamten WorkSpaces-Entwurfskonzepts ist.

- **Szenario 1: Verwendung von AD Connector zum Weiterleiten der Authentifizierung an ein lokales AD DS** In diesem Szenario befinden sich alle Netzwerkverbindungen (VPN/Direct Connect (DX)) beim Kunden. Die Authentifizierung wird über AWS Directory Service (AD Connector) an das lokale AD DS des Kunden weitergeleitet.
- **Szenario 2: Erweiterung eines lokalen AD DS in die AWS Cloud (Replikat)** Dieses Szenario ähnelt Szenario 1, jedoch wird in Szenario 2 ein AD DS-Replikat des Kunden in Verbindung mit AD Connector in AWS bereitgestellt, wodurch sich die Latenz bei Authentifizierungs- und Abfrageanforderungen an AD DS und den globalen AD DS-Katalog reduziert.
- **Szenario 3: Eigenständige, isolierte Bereitstellung mit AWS Directory Service in der AWS Cloud.** Dies ist ein isoliertes Szenario, das keine Rückverbindungen zur Authentifizierung beim Kunden umfasst. Dieser Ansatz verwendet AWS Directory Service (Microsoft AD) und AD Connector. Obwohl in diesem Szenario keine Rückverbindung zur Authentifizierung beim Kunden besteht, ist Anwendungsdatenverkehr bei Bedarf über VPN oder DX möglich.

Szenario 1: Verwendung von AD Connector zum Weiterleiten der Authentifizierung an ein lokales AD DS

Dieses Szenario richtet sich an Kunden, die ihr lokales AD DS nicht in die AWS Cloud erweitern bzw. nicht neu bereitstellen möchten. Abbildung 4: AD Connector für lokales Active Directory zeigt detailliert jede der Komponenten sowie den Authentifizierungsfluss des Benutzers.

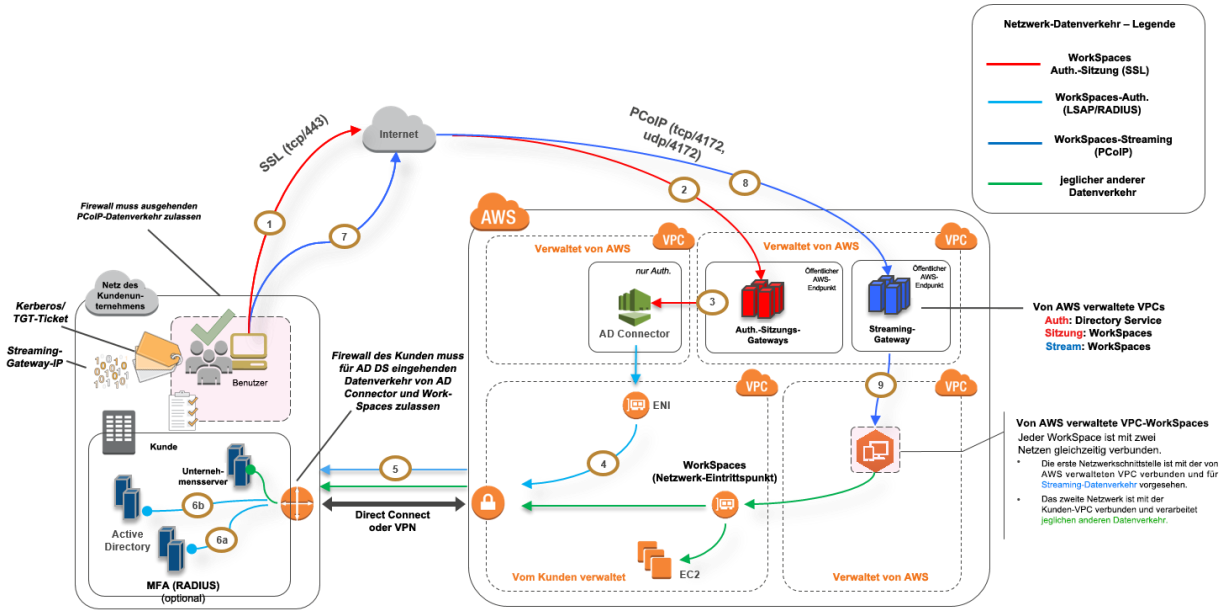

Abbildung 4: AD Connector für lokales Active Directory

In diesem Szenario wird AWS Directory Service (AD Connector) für jede Benutzerauthentifizierung bzw. MFA verwendet, die über den AD Connector in das AD DS (Abbildung 5) des Kunden weitergeleitet wird. Details zu Protokollen und Verschlüsselung für alle Authentifizierungsprozesse finden Sie im Abschnitt Sicherheit in diesem Whitepaper.

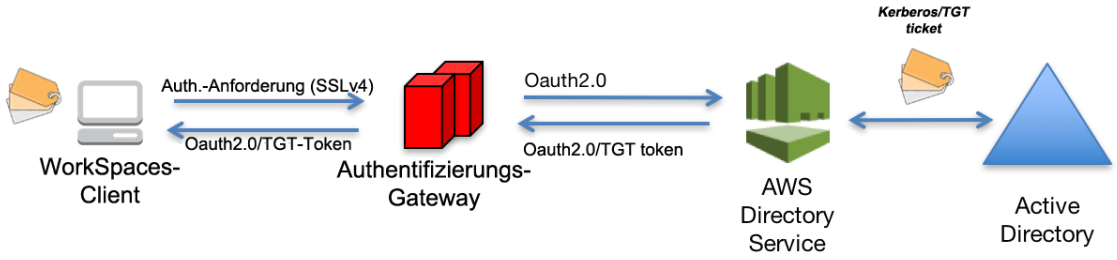

Abbildung 5: Benutzerauthentifizierung über das Authentifizierungs-Gateway

Szenario 1 verwendet eine Hybridarchitektur – der Kunde besitzt Ressourcen sowohl in AWS als auch in einem lokalen Rechenzentrum, auf die über WorkSpaces zugegriffen werden kann. Der Kunde kann vorhandene lokale AD DS- und RADIUS-Server zur Benutzerauthentifizierung bzw. MFA verwenden.

In dieser Architektur werden die folgenden Komponenten und Konstrukte verwendet.

Amazon Web Services:

- **Amazon VPC:** Erstellung einer Amazon VPC mit mindestens zwei privaten Subnetzen über zwei Availability Zones.
- **DHCP-Optionsliste:** Erstellung einer DHCP-Optionsliste für Amazon VPC. In dieser Liste können kundenspezifische Domänennamen und Domain Name Server (DNS) (lokale Services) definiert werden. (Weitere Informationen finden Sie unter DHCP Options Sets.)
- **Virtuelles privates Gateway von Amazon:** Ermöglicht die Kommunikation mit Ihrem eigenen Netzwerk über einen IPSec-VPN-Tunnel oder eine AWS Direct Connect-Verbindung.
- **AWS Directory Service**: AD Connector wird in zwei privaten Subnetzen in Amazon VPC bereitgestellt.
- **Amazon WorkSpaces:** WorkSpaces werden in den gleichen privaten Subnetzen wie AD Connector bereitgestellt (siehe Überlegungen zum Entwurf, AD Connector).

Kunde:

- **Netzwerkkonnektivität:** VPN des Unternehmens oder Direct Connect-Endpunkte
- **AD DS:** AD DS des Unternehmens
- **MFA (optional):** RADIUS-Server des Unternehmens
- **Endbenutzergeräte:** Unternehmens- oder BYOL-Endbenutzergeräte (z. B. Windows-, Mac-, iPad- oder Android-Tablets, Zero-Clients, Chromebook), mit denen auf den Amazon WorkSpaces-Service zugegriffen wird (siehe Unterstützte Plattformen und Geräte).

Diese Lösung ist für Kunden, die ihr AD DS nicht in der Cloud bereitstellen möchten, bestens geeignet, hat aber auch ihre Tücken.

- **Abhängigkeit von Konnektivität:** Geht die Konnektivität zum Rechenzentrum verloren, ist kein Benutzer mehr in der Lage, sich bei seinem WorkSpace anzumelden, und bestehende Verbindungen bleiben für die Kerberos/TGT-Lebensdauer aktiv.

- **Latenz:** Wenn auf der Verbindung Latenz vorhanden ist (was bei VPN öfter der Fall ist als bei DX), dauern die WorkSpaces-Authentifizierung und alle AD DS-bezogenen Aktivitäten (wie die Erzwingung von Gruppenrichtlinien) länger.
- **Datenverkehrskosten:** Jegliche Authentifizierung erfolgt über die VPN- oder DX-Verbindung, sodass die Kosten von der Verbindungsart abhängen. Dabei handelt es sich entweder um „Data Transfer OUT From Amazon EC2 To Internet“ oder um „Data Transfer Out (DX)“.

> **Hinweis:** AD Connector ist ein Proxy-Service. Die Anmeldeinformationen des Benutzers werden weder dauerhaft noch in einem Cache gespeichert. Stattdessen werden alle Authentifizierungs-, Lookup- und Verwaltungsanforderungen von Ihrem Active Directory behandelt. Dieses muss ein Konto mit Delegationsberechtigungen enthalten, das alle Benutzerinformationen lesen und der Domäne einen Computer hinzufügen darf.

Details dazu, wie ein Benutzer in Ihrem Verzeichnis für AD Connector zu konfigurieren ist, finden Sie unter Delegating Connect Privileges.

Im Allgemeinen ist die WorkSpaces-Erfahrung stark abhängig von Element 5 aus Abbildung 4.

Szenario 2: Erweiterung eines lokalen AD DS in die AWS Cloud (Replikat)

Dieses Szenario ähnelt Szenario 1, jedoch wird in Szenario 2 ein AD DS-Replikat des Kunden in Verbindung mit AD Connector in AWS bereitgestellt. Dadurch wird die Latenz bei Abfrageanforderungen an AD DS reduziert. Abbildung 6 zeigt detailliert jede der Komponenten sowie den Authentifizierungsfluss des Benutzers.

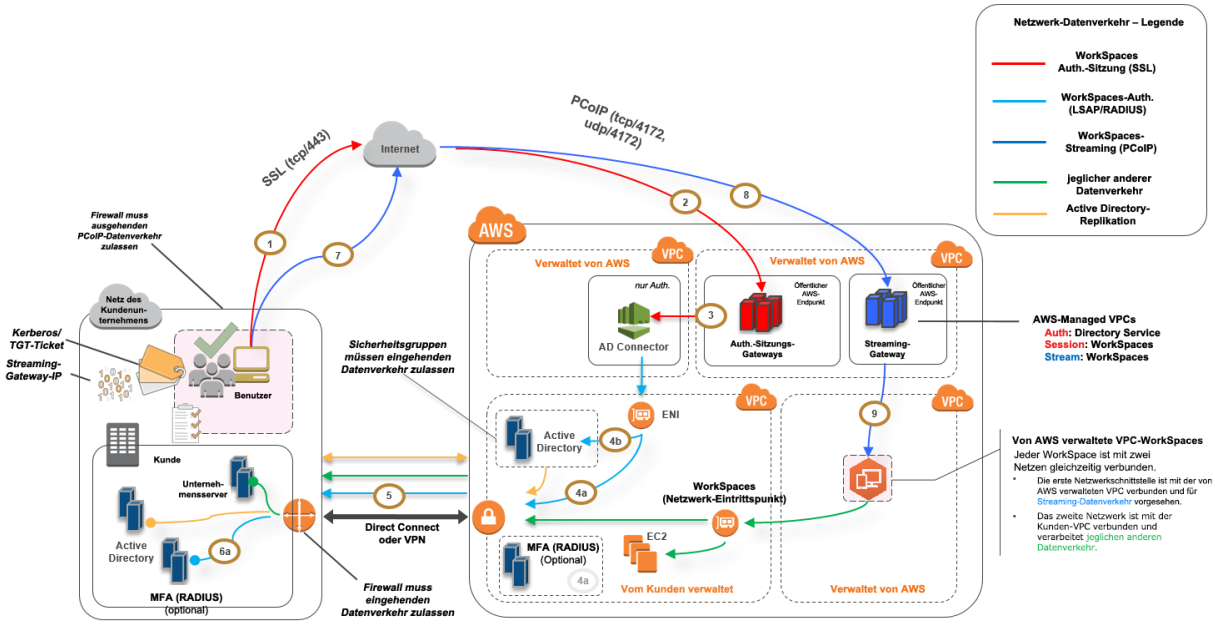

Abbildung 6: Erweitern der Active Directory Domain des Kunden in die Cloud

Wie in Szenario 1 wird AD Connector für jede Benutzerauthentifizierung bzw. MFA verwendet, die wiederum in das AD DS (Abbildung 5) des Kunden weitergeleitet wird. In Szenario 2 wird das AD DS des Kunden über Availability Zones hinweg auf Amazon EC2 Instances bereitgestellt, die als Domänencontroller in der Active Directory-Gesamtstruktur des Kunden dienen und in der AWS Cloud ausgeführt werden. Jeder Domänencontroller wird in privaten VPC-Subnetzen bereitgestellt, um sicherzustellen, dass AD DS in der AWS Cloud hochverfügbar ist. Bewährte Methoden zur Bereitstellung von AD DS in der AWS Cloud finden Sie im Abschnitt „Überlegungen zum Entwurf“ weiter unten in diesem Whitepaper.

Sobald WorkSpaces-Instances bereitgestellt sind, haben diese Zugriff auf die Domänencontroller in der Cloud und ermöglichen einen sichere Betrieb der Verzeichnisdienste und des DNS mit geringer Latenz. Der gesamte Netzwerkverkehr, einschließlich der AD DS-Kommunikation, der Authentifizierungsanforderungen und der Active Directory-Replikation, ist abgesichert, entweder innerhalb der privaten Subnetze oder im VPN-Tunnel des Kunden oder durch DX.

In dieser Architektur werden die folgenden Komponenten und Konstrukte verwendet.

Amazon Web Services:

- **Amazon VPC:** Erstellung einer Amazon VPC mit mindestens vier privaten Subnetzen (zwei für kundeneigene AD DS, zwei für AD Connector oder WorkSpaces) über zwei Availability Zones.
- **DHCP-Optionsliste:** Erstellung einer DHCP-Optionsliste für Amazon VPC. Darin können ein kundenspezifischer Domänenname und DNS (AD DS lokal) definiert werden. Weitere Informationen finden Sie unter DHCP Options Sets.
- **Virtuelles privates Gateway von Amazon:** Ermöglicht die Kommunikation mit Ihrem eigenen Netzwerk über einen IPSec-VPN-Tunnel oder eine AWS Direct Connect-Verbindung.
- **Amazon EC2:**
  - Kundeneigene AD DS-Domänencontroller, bereitgestellt auf Amazon EC2 Instances in dedizierten privaten VPC Subnetzen.
  - Optionale kundeneigene RADIUS-Server für MFA.
- **AWS Directory Services**: AD Connector wird in zwei privaten Subnetzen in Amazon VPC bereitgestellt.
- **Amazon WorkSpaces:** WorkSpaces werden in den gleichen privaten Subnetzen wie AD Connector bereitgestellt (siehe Überlegungen zum Entwurf, AD Connector).

Kunde:

- **Netzwerkkonnektivität:** VPN des Unternehmens oder AWS Direct Connect-Endpunkte
- **AD DS:** Firmeneigenes AD DS (für Replikation erforderlich).
- **MFA (optional):** RADIUS-Server des Unternehmens
- **Endbenutzergeräte:** Unternehmens- oder BYOL-Endbenutzergeräte (z. B. Windows-, Mac-, iPad- oder Android-Tablets, Zero-Clients, Chromebook), mit denen auf den Amazon WorkSpaces-Service zugegriffen wird (siehe Unterstützte Plattformen und Geräte).

Die in Szenario 1 angesprochenen Tücken sind in diesem Szenario nicht vorhanden. Deshalb sind WorkSpaces und AWS Directory Service von einem eventuellen Konnektivitätsverlust nicht betroffen.

- **Abhängigkeit von Konnektivität:** Sollte die Konnektivität zum Rechenzentrum des Kunden verloren gehen, können Endbenutzer weiterarbeiten, da Authentifizierung und optionale MFA lokal verarbeitet werden.
- **Latenz:** Mit Ausnahme des Datenverkehrs bei der Replikation (siehe *Überlegungen zum* Entwurf*:* Active Directory: Standorte und Services) erfolgt jede Authentifizierung lokal und mit geringer Latenz.
- **Datenverkehrskosten:** In diesem Szenario erfolgt die Authentifizierung lokal. Da somit nur die AD DS-Replikation die VPN- oder DX-Verbindung verwendet, ergibt sich eine Reduzierung der übertragenen Datenmenge.

Im Allgemeinen wird die WorkSpaces-Erfahrung verbessert und ist nicht wesentlich abhängig von Element 5 , wie in Abbildung 6 dargestellt. Dies ist umso mehr der Fall, wenn Sie WorkSpaces auf Tausende von Desktops skalieren möchten, vor allem in Bezug auf Abfragen im globalen AD DS-Katalog, da dieser Datenverkehr auf die lokale WorkSpaces-Umgebung beschränkt bleibt.

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

In diesem Szenario, dargestellt in Abbildung 7, wird AD DS in der AWS Cloud in einer eigenständigen, isolierten Umgebung bereitgestellt. AWS Directory Service wird in diesem Szenario exklusiv verwendet. Statt dass Sie AD DS selbst vollständig verwalten, nutzen Sie AWS Directory Service für Aufgaben wie den Aufbau einer hochverfügbaren Verzeichnistopologie, die Überwachung der Domänencontroller sowie die Konfiguration von Backups und Snapshots.

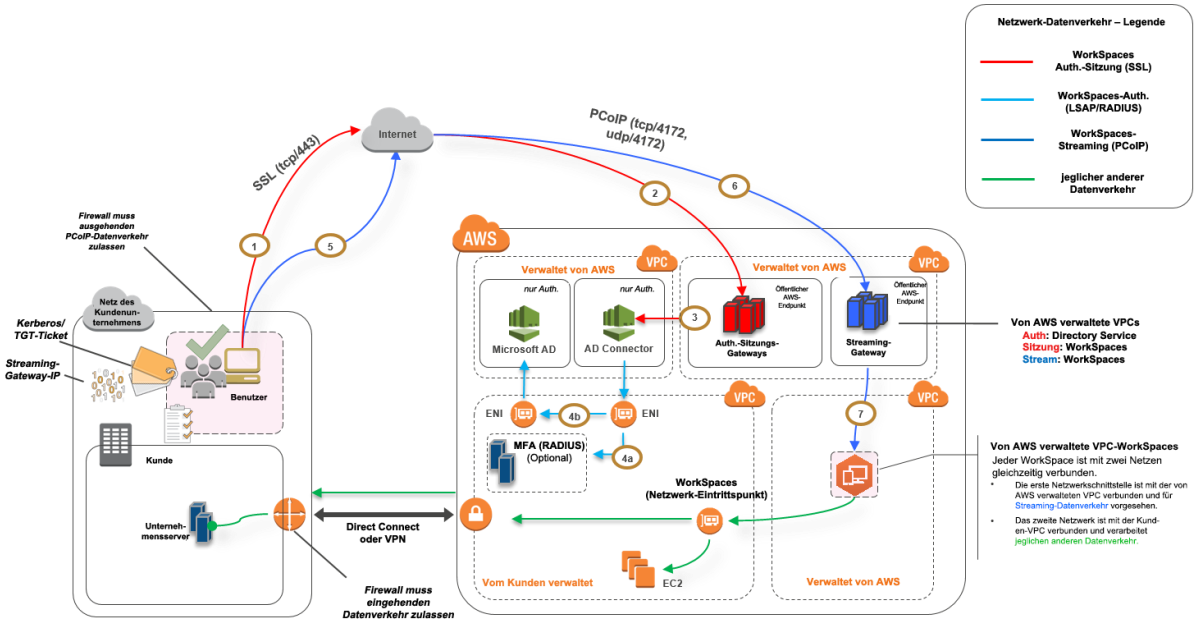

Abbildung 7: Nur in der Cloud – AWS Directory Services (Microsoft AD)

Wie in Szenario 2 wird AD DS in dedizierten Subnetzen bereitgestellt, die sich über zwei Availability Zones erstrecken, sodass AD DS in der AWS Cloud hochverfügbar ist. Zusätzlich zu Microsoft AD wird AD Connector (in allen drei Szenarien) für MFA oder WorkSpaces-Authentifizierung bereitgestellt. Damit ist in der Amazon VPC die Trennung von Rollen oder Funktionen sichergestellt, was eine bewährte Standardmethode ist (siehe Abschnitt *Überlegungen zum* Entwurf: Partitioned Network).

Szenario 3 ist eine vollständig in AWS integrierte Standardkonfiguration für Kunden, die wünschen, dass AWS die Bereitstellung verwaltet, das Patching übernimmt, für hohe Verfügbarkeit sorgt und den AWS Directory Service überwacht. Dank der Isolation ist dieses Szenario nicht nur für die Produktion geeignet, sondern auch für Machbarkeitsnachweise und Testumgebungen.

Neben der Platzierung von AWS Directory Service zeigt Abbildung 7 auch den Datenverkehrsfluss von einem Benutzer zu einem WorkSpace und wie der WorkSpace mit dem AD-Server und dem MFA-Server interagiert.

In dieser Architektur werden die folgenden Komponenten und Konstrukte verwendet.

Amazon Web Services:

- **Amazon VPC:** Erstellung einer Amazon VPC mit mindestens vier privaten Subnetzen (zwei für AD DS *Microsoft AD* zwei für AD Connector oder WorkSpaces) über zwei Availability Zones. „*Rollentrennung*."
- **DHCP-Optionsliste:** Erstellung einer DHCP-Optionsliste für Amazon VPC. In dieser Liste können kundenspezifische Domänennamen und DNS (Microsoft AD) definiert werden. (Weitere Informationen finden Sie unter DHCP Options Sets.)
- **(Optional) Virtuelles privates Gateway von Amazon:** Ermöglicht die Kommunikation mit Ihrem eigenen Netzwerk über einen IPSec-VPN-Tunnel (VPN) oder eine AWS Direct Connect-Verbindung. Wird für den Zugriff auf lokale Back-End-Systeme verwendet.
- **AWS Directory Service:** Microsoft AD wird in zwei dedizierten Subnetzen in Amazon VPC bereitgestellt (AD DS Managed Service).
- **Amazon EC2:** Kundeneigener optionaler RADIUS-Server für MFA.
- **AWS Directory Services**: AD Connector wird in zwei privaten Subnetzen in Amazon VPC bereitgestellt.
- **Amazon WorkSpaces:** WorkSpaces werden in den gleichen privaten Subnetzen wie AD Connector bereitgestellt (siehe Überlegungen zum Entwurf, AD Connector).

Kunde:

- **(Optional) Netzwerkkonnektivität:** VPN des Unternehmens oder AWS Direct Connect-Endpunkte.
- **Endbenutzergeräte:** Unternehmens- oder BYOL-Endbenutzergeräte (z. B. Windows-, Mac-, iPad- oder Android-Tablets, Zero-Clients, Chromebook), mit denen auf den Amazon WorkSpaces-Service zugegriffen wird (siehe Unterstützte Plattformen und Geräte).

Wie in Szenario 2 gibt es bei dieser Lösung keine Probleme mit der Konnektivität zum lokalen Rechenzentrum des Kunden, mit Latenz oder Kosten für ausgehenden Datentransfer (es sei denn, WorkSpaces innerhalb der VPC hätten Zugriff auf das Internet), weil dies entwurfsbedingt ein isoliertes (nur in der Cloud realisiertes) Szenario ist.

Überlegungen zum Entwurf

Eine funktionelle AD DS-Bereitstellung in der AWS Cloud erfordert ein gutes Verständnis sowohl für Active Directory-Konzepte als auch für bestimmte AWS-Services. In diesem Abschnitt behandeln wir grundlegende Überlegungen zum Entwurf eines Konzepts zur Bereitstellung von AD DS in WorkSpaces, bewährte Methoden für VPC und AWS Directory Service, DHCP- und DNS-Anforderungen, Besonderheiten bezüglich AD Connector sowie Active Directory-Standorte und -Services.

VPC-Entwurf

Wie wir bereits im Abschnitt Überlegungen zum Netzwerk dieses Dokuments und zuvor in den Szenarien 2 und 3 empfohlen haben, sollten Sie AD DS in der AWS Cloud in zwei dedizierten privaten Subnetzen bereitstellen, die sich über zwei Availability Zones erstrecken und von AD Connector- oder WorkSpaces-Subnetzen getrennt sind. Dieses Konstrukt garantiert in WorkSpaces hochverfügbaren Zugriff mit geringer Latenz auf AD DS-Services und entspricht den bewährten Methoden zur Trennung von Rollen oder Funktionen innerhalb der Amazon VPC.

Abbildung 8 zeigt die Aufteilung von AD DS und AD Connector in dedizierte private Subnetze (Szenario 3). In diesem Beispiel befinden sich alle Services in derselben Amazon VPC.

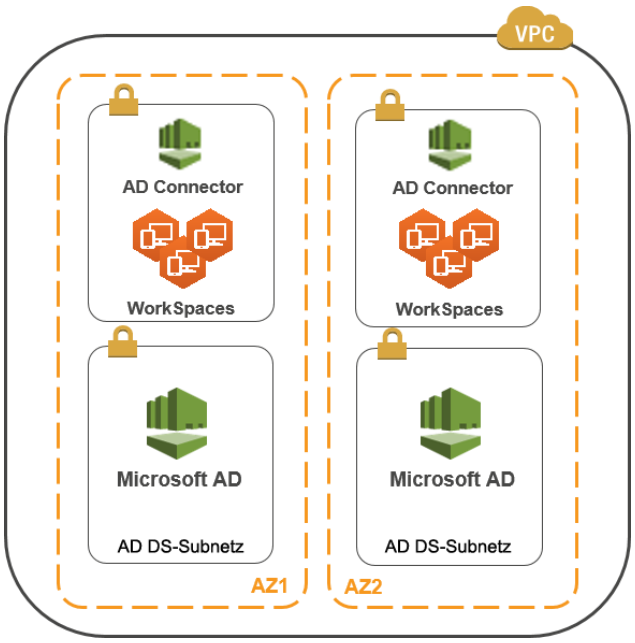

Abbildung 8: AD DS-Netzwerktrennung

Abbildung 9 zeigt einen ähnlichen Entwurf wie Szenario 1, jedoch befindet sich der lokale Teil jetzt in einer dedizierten Amazon VPC.

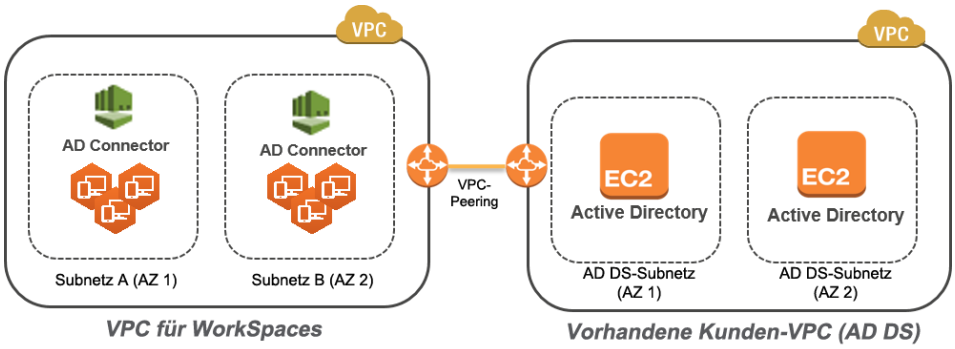

Abbildung 9: VPC mit dedizierten WorkSpaces

Hinweis: Für Kunden, die AD DS bereits in AWS ausführen, empfehlen wir, dass sie ihre WorkSpaces in einer dedizierten VPC zusammenfassen und VPC-Peering für die AD DS-Kommunikation verwenden.

Zusätzlich zur Erstellung dedizierter privater Subnetze für AD DS ist es erforderlich, für Domänencontroller und Mitgliedsserver Sicherheitsgruppenregeln zu implementieren, die Datenverkehr für Services wie AD DS-Replikation, Benutzerauthentifizierung, Windows-Zeitdienste und DFS (Distributed File System) zulassen.

> **Hinweis:** Eine bewährte Methode ist, die erforderlichen Sicherheitsgruppenregeln auf private WorkSpaces-Subnetze zu beschränken und – im Fall von Szenario 2 – lokale bidirektionale AD DS-Kommunikation mit der AWS Cloud zuzulassen, wie in der folgenden Tabelle dargestellt.

Protokoll	Port	Verwendung	Ziel
TCP	53, 88, 135, 139, 389, 445, 464, 636	Auth. (primär)	Active Directory (privates Rechenzentrum oder EC2)*
TCP	49152 – 65535	RPC-High-Ports	Active Directory (privates Rechenzentrum oder EC2)**
TCP	3268-3269	Vertrauensstellungen	Active Directory (privates Rechenzentrum oder EC2)*
TCP	9389	Remote-Zugriff auf Microsoft Windows PowerShell (optional)	Active Directory (privates Rechenzentrum oder EC2)*
UDP	53, 88, 123, 137, 138, 389, 445, 464	Auth. (primär)	Active Directory (privates Rechenzentrum oder EC2)*
UDP	1812	Auth. (MFA) (optional)	RADIUS (privates Rechenzentrum oder EC2)*

* Siehe Active Directory and Active Directory Domain Services Port Requirements

**Siehe Service overview and network port requirements for Windows

Eine schrittweise Anleitung zur Implementierung von Regeln finden Sie unter Adding Rules to a Security Group im *Amazon Elastic Compute Cloud User Guide*.

VPC-Entwurf: DHCP and DNS

Mit einem Amazon VPC werden standardmäßig auch DHCP-Services für Ihre Instances bereitgestellt. Standardmäßig gehört zu jeder VPC ein interner DNS-Server, der im Adressraum Classless Inter Routing (CIDR) +2 liegt und allen Instances über eine Standard-DHCP-Optionsliste zugeordnet ist.

DHCP-Optionslisten werden in einer Amazon VPC verwendet, um Bereichsoptionen zu definieren, wie beispielsweise die Domänennamen oder die Namenserver, die auf Ihren Instances per DHCP verwaltet werden sollten. Die korrekte Funktionalität der Windows-Services innerhalb Ihrer VPC ist von diesen DHCP-Bereichsoptionen abhängig, die deshalb sorgfältig gewählt sein müssen. In jedem der zuvor genannten Szenarien müssen Sie Ihren eigenen Bereich, der Ihren Domänennamen und die Namenserver definiert, erstellen und zuweisen. Dadurch stellen Sie sicher, dass die zu einer Domäne gehörenden Windows-Instances oder WorkSpaces so konfiguriert werden, dass sie das Active Directory-DNS verwenden. Die folgende Tabelle ist ein Beispiel für eine Liste benutzerdefinierter DHCP-Bereichsoptionen, die für WorkSpaces und AWS Directory Services erstellt werden müssen, damit diese korrekt funktionieren.

Parameter	Wert
Namensbezeichner	Ein Bezeichner, der aus den Elementen **Name** und **Wert** besteht, die bestimmte Zeichenfolgen darstellen. Beispiel: exampleco.com
Domänenname	exampleco.com
Domänennamenserver	Durch Kommata getrennte DNS-Serveradressen Beispiel: 10.0.0.10, 10.0.1.10
NTP-Server	Dieses Feld bleibt leer.
NetBIOS-Namenserver	Wiederholen Sie hier die durch Kommata getrennten IPs der Domänennamenserver. Beispiel: 10.0.0.10, 10.0.1.10
NetBIOS-Knotentyp	2

Details zur Erstellung einer benutzerdefinierten DHCP-Optionsliste für Ihre Amazon VPC finden Sie unter Working with DHCP Options Sets im *Amazon Virtual Private Cloud User Guide*.

In Szenario 1 wäre der DHCP-Bereich das lokale DNS oder AD DS. In Szenario 2 oder 3 wäre er jedoch der lokal bereitgestellte Verzeichnisdienst (AD DS auf Amazon EC2 oder AWS Directory Services: Microsoft AD). Wir empfehlen, dass Sie jeden Domänencontroller in der AWS Cloud zu einem GC- und Active Directory-integrated DNS-Server machen.

Active Directory: Standorte und Services

In Szenario 2 sind Standorte und Services kritische Komponenten für die korrekte Funktion von AD DS. Die Active Directory-Replikation zwischen Domänencontrollern am Standort und über Standortgrenzen hinweg wird von der Standorttopologie bestimmt. In Szenario 2 sind mindestens zwei Standorte vorhanden, der lokale und die AWS WorksSpaces in der Cloud. Die Wahl der richtige Standorttopologie stellt Clientaffinität sicher, was bedeutet, dass Clients (in diesem Fall die WorkSpaces) ihre bevorzugten lokalen Domänencontroller verwenden.

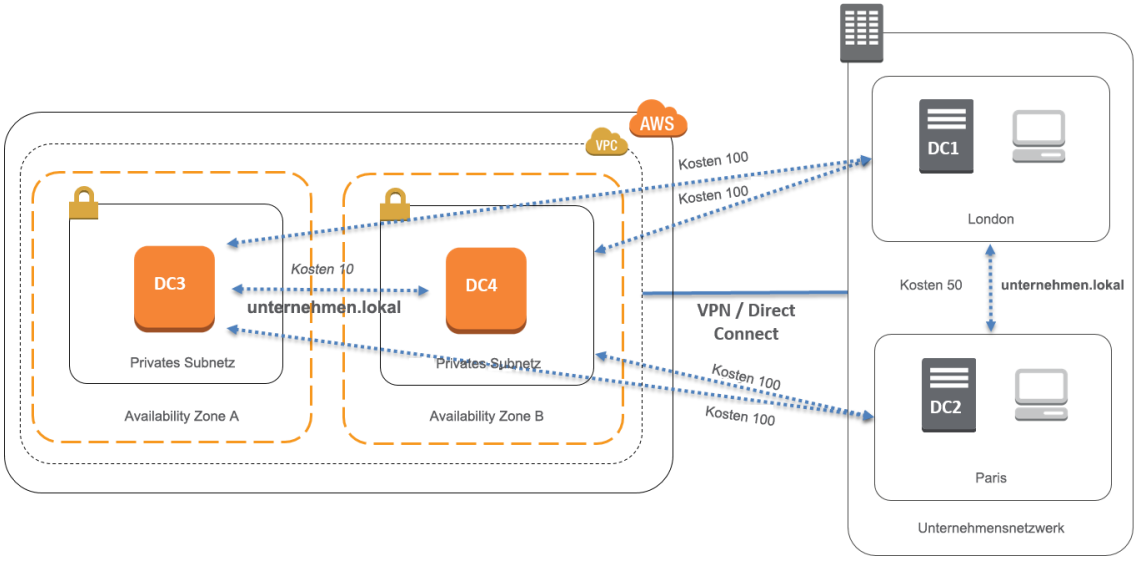

Abbildung 10: Active Directory – Standorte und Services: Clientaffinität

> **Bewährte Methode:** Definieren Sie hohe Kosten für Standortverbindungen zwischen dem lokalen AD DS und der AWS Cloud. Abbildung 10 zeigt beispielhaft, welche Kosten den Standortverbindungen (Kosten 100) zuzuweisen sind, um standortunabhängige Clientaffinität zu gewährleisten.

Diese Zuordnungen tragen dazu bei, dass Datenverkehr wie AD DS-Replikation und Client-Authentifizierung den effizientesten Pfad zu einem Domänencontroller verwendet. Das stellt in den Szenarien 2 und 3 geringe Latenz und wenig verbindungsübergreifenden Datenverkehr sicher.

Multi-Faktor-Authentifizierung (MFA)

Voraussetzung für die Implementierung von MFA ist, dass die WorkSpaces-Infrastruktur AD Connector als AWS Directory Service sowie einen RADIUS-Server verwendet. Obwohl in diesem Dokument die Bereitstellung eines RADIUS-Servers nicht behandelt wird, ist im vorherigen Abschnitt AD DS-Bereitstellungsszenarien in jedem Szenario die Verwendung von RADIUS detailliert beschrieben.

MFA – Zwei-Faktor-Authentifizierung

Amazon WorkSpaces unterstützt MFA, wenn AWS Directory Service: AD Connector und ein *kundeneigener* RADIUS-Server vorhanden sind. Nach der Aktivierung müssen die Benutzer im WorkSpaces-Client für den Zugriff auf ihre jeweiligen WorkSpaces-Desktops die Felder **Username**, **Password** und **MFA-Code** ausfüllen.

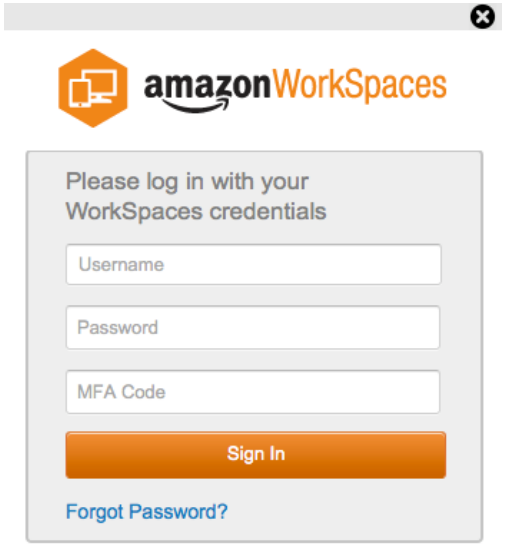

Abbildung 11: WorkSpaces-Client mit aktivierter MFA

> **Grundregel:** MFA-Implementierung erfordert die Verwendung von AD Connector. AD Connector unterstützt keine selektive MFA pro Benutzer (dies ist ein globale Einstellung für jeden AD Connector). Wenn Sie selektive MFA pro Benutzer benötigen, müssen Sie die Benutzer nach AD Connector separieren.

Für WorkSpaces-MFA ist mindestens ein RADIUS-Server erforderlich. Üblicherweise handelt es sich dabei um bestehende Lösungen, zum Beispiel RSA, oder die Server können in Ihrer VPC bereitgestellt werden (siehe AD DS-Bereitstellungsszenarien). Für den Fall, dass Sie eine neue RADIUS-Lösung bereitstellen möchten, bietet der Markt etliche Implementierungen, beispielsweise FreeRADIUS oder Cloud-Anwendungen wie Duo Security.

Eine Liste der Voraussetzungen für die Implementierung von MFA für Amazon WorkSpaces finden Sie im *Amazon WorkSpaces Administration Guide* unter Preparing Your Network for an AD Connector Directory. Der Prozess zu Konfiguration von AD Connector für MFA ist im *Amazon WorkSpaces Administration Guide* beschrieben unter „Managing an AD Connector Directory: Multi-factor Authentication“.

Sicherheit

In diesem Abschnitt wird erläutert, wie Daten bei Verwendung der Amazon WorkSpaces-Services durch Verschlüsselung gesichert werden. Beschrieben wird ie Verschlüsselung ruhender Daten, die Verschlüsselung während der Übertragung sowie die Verwendung von Sicherheitsgruppen zum Schutz des Netzwerkzugriffs auf die WorkSpaces. Weitere Informationen zur Authentifizierung (einschließlich MFA-Unterstützung) finden Sie im Abschnitt „AWS Directory Service“.

Verschlüsselung während der Übertragung

Amazon WorkSpaces verwendet Kryptographie zum Schutz der Vertraulichkeit in den verschiedenen Phasen der Kommunikation (Datenübertragung) und zum Schutz ruhender Daten (verschlüsselte WorkSpaces). Die Prozesse in jeder Phase der von Amazon WorkSpaces verwendeten Verschlüsselung für Daten während der Übertragung werden in den folgenden Abschnitten beschrieben. Informationen über die Verschlüsselung ruhender Daten finden Sie im Abschnitt Verschlüsselte WorkSpaces weiter unten in diesem Whitepaper.

Registrierung und Updates

Die Desktop-Clientanwendung kommuniziert mit Amazon bezüglich Updates und Registrierung über HTTPS.

Authentifizierungsphase

Der Desktop-Client initiiert die Authentifizierung durch Senden der Anmeldeinformationen an das Authentifizierung-Gateway. Der Desktop-Client kommuniziert mit dem Authentifizierung-Gateway über HTTPS. Am Ende dieser Phase gibt das Authentifizierung-Gateway über dieselbe HTTPS-Verbindung ein OAuth 2.0-Token an den Desktop-Client zurück, sofern die Authentifizierung erfolgreich war.

> **Hinweis:** Die Desktop-Clientanwendung unterstützt die Verwendung eines Proxy-Servers für Updates, Registrierung und Authentifizierung über Port 443 (HTTPS).

Nachdem das Authentifizierung-Gateway die Anmeldeinformationen vom Client empfangen hat, sendet es eine Authentifizierungsanforderung an AWS Directory Service. Die Kommunikation zwischen Authentifizierungs-Gateway und AWS Directory Service erfolgt über HTTPS, sodass keine Anmeldeinformationen des Benutzers im Klartext übertragen werden.

Authentifizierung – AD Connector

AD Connector verwendet Kerberos für die Authentifizierungskommunikation mit dem lokalen AD, sodass LDAP eingebunden und nachfolgende LDAP-Abfragen ausgeführt werden können. Momentan wird LDAP mit TLS (LDAPs) von AWS Directory Service noch nicht unterstützt. Anmeldeinformationen des Benutzers werden jedoch zu keiner Zeit im Klartext übertragen. Zur Erhöhung der Sicherheit können Sie Ihre WorkSpaces-VPC über eine VPN-Verbindung mit dem lokalen Netzwerk (das Ihr AD enthält) verbinden. Beim Einsatz einer hardwarebasierten AWS VPN-Verbindung verwenden Sie zur Verschlüsselung der Übertragung standardmäßiges IPSEC (IKE und IPSEC SAs) mit symmetrischen Schlüsseln (AES-128 oder AES-256), SHA-1 oder SHA-256 für den Integritäts-Hash und DH-Gruppen (2, 14-18, 22, 23 und 24 für Phase 1 sowie 1, 2, 5, 14-18, 22, 23 und 24 für Phase 2) unter Verwendung von PFS.

Broker-Phase

Nach Empfang des OAuth 2.0-Tokens vom Authentifizierung-Gateway (sofern die Authentifizierung erfolgreich war) sendet der Desktop-Client über HTTPS eine Abfrage an den Amazon WorkSpaces-Service (Broker Connection Manager). Der Desktop-Client authentifiziert sich selbst durch Übersendung des OAuth 2.0-Tokens und erhält daraufhin die Endpunktinformation für das WorkSpaces-Streaming-Gateway.

Streaming-Phase

Der Desktop-Client fordert das Öffnen einer PCoIP-Sitzung mit dem Streaming-Gateway an (unter Verwendung des OAuth-2.0-Tokens). Diese Sitzung ist mit AES-256 verschlüsselt und verwendet den PCoIP-Port für die Kommunikationssteuerung (d. h. 4172/TCP).

Mit dem OAuth-2.0-Token fordert das Streaming-Gateway über HTTPS die benutzerspezifischen WorkSpaces-Informationen vom WorkSpaces-Service an.

Das Streaming-Gateway erhält auch das TGT vom Client (das mit dem Passwort des Clientbenutzers verschlüsselt ist) und initiiert durch Kerberos-TGT-Weiterleitung eine Windows-Anmeldung im WorkSpace, wobei das abgerufene Kerberos-TGT des Benutzers verwendet wird.

Der WorkSpace initiiert dann unter Verwendung der standardmäßigen Kerberos-Authentifizierung eine Authentifizierungsanforderung an den konfigurierten AWS Directory Service.

Nachdem der WorkSpace erfolgreich angemeldet wurde, beginnt das PCoIP-Streaming. Die Verbindung wird vom Client auf TCP-Port 4172 initiiert, der Rückverkehr läuft über den UDP-Port 4172. Die erstmalige Verbindung über die Verwaltungsschnittstelle zwischen dem Streaming-Gateway und Ihrem WorkSpaces-Desktop erfolgt über UDP 55002. (Informationen dazu finden Sie in der Amazon WorkSpaces-Dokumentation unter Amazon WorkSpaces Details. Der anfängliche ausgehende UDP-Port ist 55002). Die Streaming-Verbindung verwendet Port 4172 (TCP und UDP) und wird mit AES-128 oder AES-256 verschlüsselt. Voreingestellt sind 128 Bit. Sie können 256 Bit mit dem PCoIP-spezifischen Active Directory-Gruppenrichtlinienobjekt (pcoip.adm) einstellen.

Netzwerkschnittstellen

Jeder Amazon WorkSpace verfügt über zwei Netzwerkschnittstellen, die primäre Netzwerkschnittstelle und die Verwaltungs-Netzwerkschnittstelle.

Die primäre Netzwerkschnittstelle ermöglicht die Verbindung zu Ressourcen innerhalb Ihrer VPC, beispielsweise den Zugriff auf AWS Directory Service, das nternet und Ihr Unternehmensnetzwerk. Es ist möglich, dieser primären Netzwerkschnittstelle wie jeder anderen ENI Sicherheitsgruppen zuzuordnen. Konzeptionell unterscheiden wir die dieser ENI zugeordneten Sicherheitsgruppen anhand ihres Bereitstellungsbereichs: WorkSpaces-Sicherheitsgruppen und ENI Sicherheitsgruppen.

Verwaltungs-Netzwerkschnittstelle

Sie können die Verwaltungs-Netzwerkschnittstelle nicht über Sicherheitsgruppen steuern, aber eine hostbasierte Firewall in Ihrem WorkSpace verwenden, um Ports zu blockieren oder den Zugriff zu steuern. Wir empfehlen, keine Beschränkungen für die Verwaltungs-Netzwerkschnittstelle anzuwenden. Wenn Sie sich entscheiden, hostbasierte Firewall-Regeln hinzuzufügen, um diese Schnittstelle zu verwalten, müssen Sie einige Ports offenhalten, damit der WorkSpaces-Service Zustand und Zugänglichkeit des WorkSpace verwalten kann. Einzelheiten dazu finden Sie im Amazon WorkSpaces Administration Guide.

WorkSpaces-Sicherheitsgruppe

Pro AWS Directory Service wird eine Standardsicherheitsgruppe erstellt und automatisch allen WorkSpaces zugeordnet, die zu diesem bestimmten Verzeichnis gehören.

Wie bei jeder anderen Sicherheitsgruppe ist es auch bei einer WorkSpaces-Sicherheitsgruppe möglich, die Regeln zu ändern. Vorgenommene Änderungen wirken sich sofort aus.

Es ist auch möglich, die standardmäßig zu einem AWS Directory Service gehörende WorkSpaces-Sicherheitsgruppe durch Änderung der Zuordnung durch eine andere WorkSpaces-Sicherheitsgruppe zu ersetzen.

> **Hinweis:** Eine neu zugeordnete Sicherheitsgruppe wird nur mit WorkSpaces verknüpft, die nach der Änderung neu oder erneut erstellt worden sind.

ENI-Sicherheitsgruppen

Da die primäre Netzwerkschnittstelle eine reguläre ENI ist, kann sie mithilfe der erschiedenen AWS-Verwaltungstools konfiguriert werden (siehe Elastic Network Interfaces (ENI)). Dazu suchen Sie die IP-Adresse für den WorkSpace (auf der Seite „WorkSpaces“ in der Amazon WorkSpaces-Konsole) und verwenden diese IP-Adresse dann als Filter, um die entsprechende ENI zu finden (im Abschnitt „Network Interfaces“ der Amazon EC2-Konsole).

Nachdem Sie die ENI gefunden haben, können Sie dafür sofort Sicherheitsgruppen verwalten. Bei der manuellen Zuweisung von Sicherheitsgruppen an die primäre Netzwerkschnittstelle müssen Sie die in [Amazon WorkSpaces Details] *beschriebenen Anforderungen für Ports berücksichtigen.*

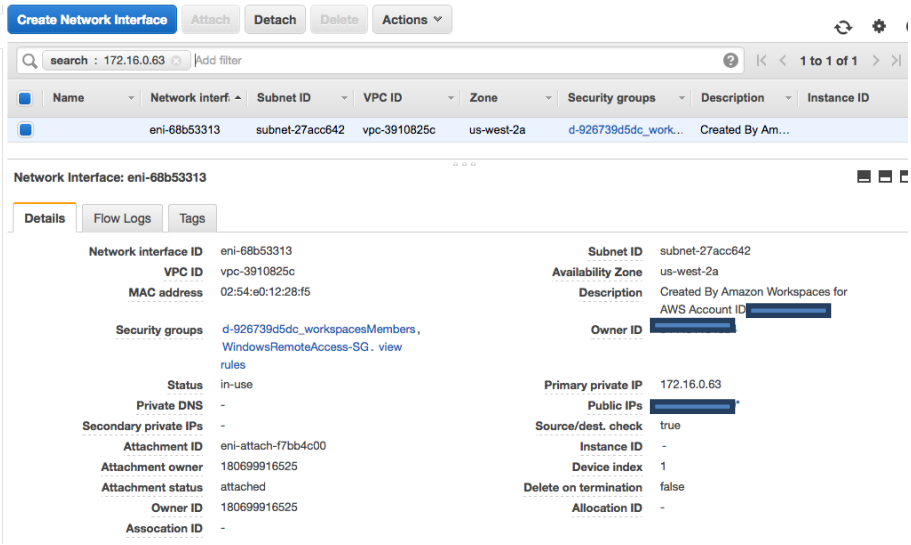

Abbildung 12: Verwalten von Sicherheitsgruppen-Zuordnungen

Verschlüsselte WorkSpaces

Jeder Amazon WorkSpace verfügt über ein Stamm-Volume (C: Laufwerk) und ein Benutzer-Volume (D: Laufwerk) Sie können ein Volume oder beide verschlüsseln lassen.

Was wird verschlüsselt?

Verschlüsselt werden die Daten im Ruhezustand, Festplatten-Ein/Ausgaben und Snapshots von verschlüsselten Volumes.

Wann erfolgt die Verschlüsselung?

Sie sollten festlegen, dass die Verschlüsselung für einen WorkSpace schon bei dessen Erstellung bzw. Start erfolgt. WorkSpaces-Volumes können nur beim Start verschlüsselt werden – nach dem Start ist eine Änderung ihres Verschlüsselungsstatus nicht mehr möglich. Abbildung 13 zeigt die Seite der Amazon WorkSpaces-Konsole, auf der eingestellt werden kann, dass ein neuer WorkSpace beim Start verschlüsselt wird.

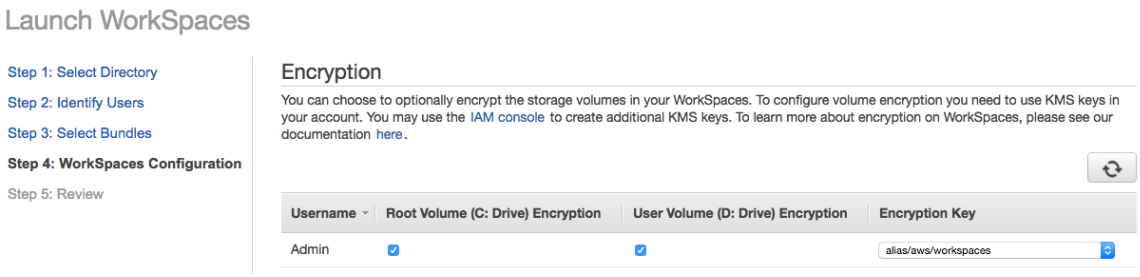

Abbildung 13: Verschlüsseln von WorkSpaces-Volumes

Wie wird ein neuer WorkSpace verschlüsselt?

Sie können die Option „Encrypted WorkSpaces“ sowohl in der Amazon WorkSpaces-Konsole als auch in der AWS CLI einstellen oder mithilfe der Amazon WorkSpaces-API festlegen, dass ein neuer WorkSpace beim Start verschlüsselt wird.

Um die Volumes zu verschlüsseln, verwendet Amazon WorkSpaces einen Kundenhauptschlüssel (Customer Master Key, CMK) des AWS Key Management Service (KMS). AWS KMS erstellt einen Standard-CMK, wenn der WorkSpace erstmalig in einer Region gestartet wird (CMKs gelten regionsweit). Sie können für verschlüsselte WorkSpaces auch selbst einen CMK verwalten. Der CMK wird verwendet, um die Datenschlüssel zu verschlüsseln, mit denen der Amazon WorkSpaces-Service die Volumes verschlüsselt (genaugenommen ist es der Amazon Elastic Block Store (Amazon EBS)-Service, der die Volumes verschlüsselt). Jeder CMK kann verwendet werden, um Schlüssel für bis zu 30 WorkSpaces zu verschlüsseln.

> **Hinweis:** Von einem verschlüsselten WorkSpace kann derzeit kein benutzereigenes Image erstellt werden. Die Bereitstellung von WorkSpaces, die mit verschlüsselten Stamm-Volumes aktiviert wurden, kann bis zu eine Stunde dauern.

Eine detaillierte Beschreibung des Verschlüsselungsprozesses für WorkSpaces finden Sie unter Overview of Amazon WorkSpaces Encryption Using AWS KMS. Weitere Informationen über AWS KMS-Kundenhauptschlüssel und Datenschlüssel finden Sie unter AWS Key Management Service Concepts.

Überwachen und Protokollieren mit Amazon CloudWatch

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

Amazon CloudWatch-Metriken für WorkSpaces

CloudWatch-Metriken für WorkSpaces dienen dazu, Administratoren zusätzliche Informationen über den allgemeinen Zustand und den Verbindungsstatus einzelnen WorkSpaces zu liefern. Metriken stehen pro WorkSpace zur Verfügung oder in zusammengefasster Form für alle WorkSpaces einer Organisation in einem bestimmten Verzeichnis (*AD Connector, siehe Identity*).

Diese Metriken können wie alle CloudWatch-Metriken in der AWS Management Console angezeigt (Abbildung 13), über CloudWatch-APIs aufgerufen und mithilfe von CloudWatch-Alarmen oder Drittanbietertools überwacht werden.

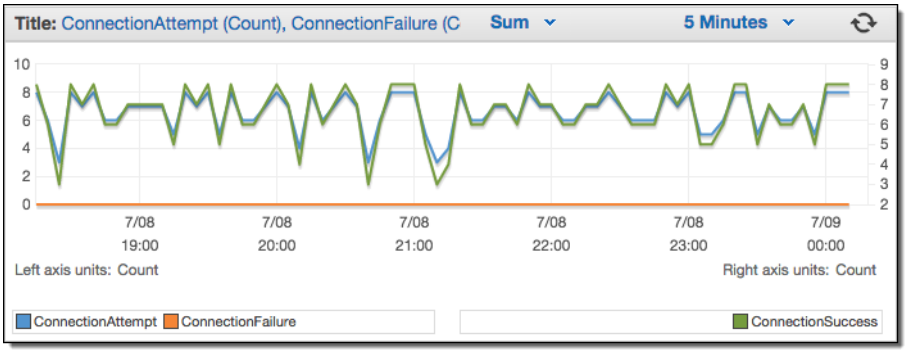

Abbildung 14: CloudWatch-Metriken – ConnectionAttempt/ConnectionFailure

Standardmäßig sind die folgenden Metriken aktiviert und ohne Aufpreis verfügbar:

- **Available**: Diese Metrik zählt WorkSpaces, die auf eine Statusprüfung antworten.

- **Unhealthy**: Diese Metrik zählt WorkSpaces, die auf die o. g. Statusprüfung nicht antworten.
- **ConnectionAttempt**: Die Anzahl der Versuche, eine Verbindung mit einem WorkSpace herzustellen.
- **ConnectionSuccess**: Die Anzahl der erfolgreichen Verbindungsversuche.
- **ConnectionFailure**: Die Anzahl der fehlgeschlagenen Verbindungsversuche.
- **SessionLaunchTime**: Der vom WorkSpaces-Client ermittelte Zeitbedarf für die Initialisierung einer Sitzung.
- **InSessionLatency**: Die vom Client ermittelte und angegebene Umlaufzeit zwischen dem WorkSpaces-Client und WorkSpaces.
- **SessionDisconnect**: Die Anzahl der vom Benutzer initiierten und automatisch beendeten Sitzungen.

Zusätzlich können Alarme erstellt werden (siehe Abbildung 15).

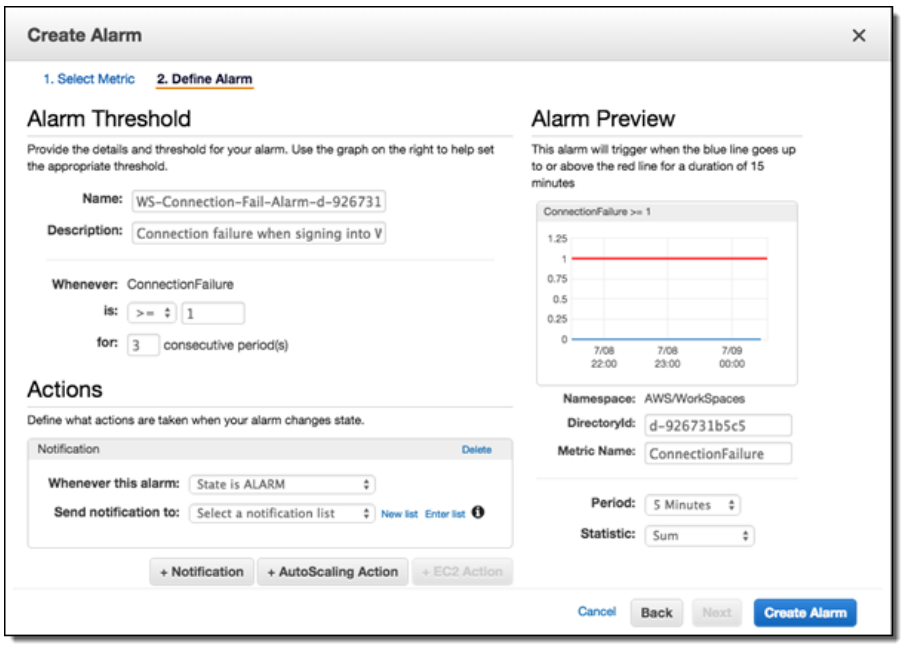

Abbildung 15: Erstellung von CloudWatch-Alarmen für WorkSpaces-Verbindungsfehler

Fehlersuche

Informationen zu häufigen Verwaltungs- und Clientproblemen wie „Ich sehe die folgende Fehlermeldung: Ihr Gerät ist nicht in der Lage, eine Verbindung zum WorkSpaces Registration-Service herzustellen“ oder „Es kann keine Verbindung zu einem WorkSpace mit einem interaktiven Anmeldungs-Banner hergestellt werden“ finden Sie auf den Fehlerbehebungsseiten Client und Admin im *Amazon WorkSpaces Administration Guide*.

AD Connector kann keine Verbindung zum Active Directory herstellen

Damit AD Connector eine Verbindung zu Ihrem lokalen Verzeichnis herstellen kann, muss die Firewall für Ihr lokales Netzwerk bestimmte Ports für das CIDR in beide Subnetze in der VPC geöffnet haben (siehe AD Connector). Um zu Prüfen, ob das der Fall ist, führen Sie die folgenden Schritt aus.

Prüfen der 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 Testanwendung DirectoryServicePortTest herunter und extrahieren Sie den Inhalt der ZIP-Datei. Der Quellcode und die Visual Studio-Projektdateien sind enthalten, sodass Sie die Testanwendung bei Bedarf ändern können.
3. Führen Sie die Testanwendung DirectoryServicePortTest in einer Windows-Eingabeaufforderung mit den folgenden Optionen aus:

```
DirectoryServicePortTest.exe -d <Domänenname> -ip <Server_IP_Adresse> -tcp
"53,88,135,139,389,445,464,636,49152" -udp "53,88,123,137,138,389,445,464"
<Domänenname>
```

<*Domänenname*>

Der vollständig qualifizierte Domänenname zum Testen der Gesamtstruktur und der Funktionsebenen der Domäne. Wenn Sie den Domänennamen nicht angeben, werden die Funktionsebenen nicht getestet.

<*Server_IP_Adresse*>

Die IP-Adresse eines Domänencontrollers in Ihrer lokalen Domäne. Die Ports werden mit dieser IP-Adresse getestet. Wenn Sie die IP-Adresse nicht angeben, werden die Ports nicht getestet.

Damit wird bestimmt, ob die erforderlichen Ports für Übertragungen aus der VPC in Ihre Domäne geöffnet sind. Die Testanwendung prüft zudem die mindestens erforderlichen Gesamtstruktur- und Funktionsebenen der Domäne.

Suchen der nächstliegenden AWS-Region mit der geringsten Latenz

Im Oktober 2015 hat Amazon WorkSpaces die Website Connection Health Check gestartet. Die Website prüft schnell, ob Sie alle für die Verwendung von WorkSpaces erforderlichen Services erhalten können. Sie führt zudem eine Leistungsprüfung für jede AWS-Region aus, in der WorkSpaces ausgeführt werden, und teilt dem Benutzer mit, welche die schnellste Region für ihn ist.

Zusammenfassung

Organisationen streben heute danach, agiler zu sein, ihre Daten besser zu schützen und ihren Mitarbeitern eine höhere Produktivität zu ermöglichen. All das führt zu einer strategischen Verschiebung im Endbenutzer-Computing. Viele der bereits mit Cloud Computing realisierten Vorteile gelten auch das Endbenutzer-Computing. Durch die Übertragung ihrer Desktops in die AWS Cloud mit Amazon WorkSpaces können Organisationen schnell skalieren, sobald neue Mitarbeiter hinzukommen, ihre Sicherheitslage verbessen, da Daten nicht in Geräten vorgehalten werden, und ihren Mitarbeitern einen mobilen Desktop bieten, auf den sie von überall und mit den Geräten ihrer Wahl zugreifen können.

Amazon WorkSpaces ist dafür konzipiert, in bestehende IT-Systeme und Prozesse integriert zu werden, und dieses Whitepaper beschreibt bewährte Methoden für diese Integration. Das Ergebnis der Anwendung dieser Methoden ist eine kosteneffiziente Cloud-Desktop-Bereitstellung, die im Gleichklang mit Ihrem Unternehmen in der globalen AWS-Infrastruktur wächst.

Mitwirkende

Dieses Dokument ist unter der Mitarbeit folgender Personen entstanden:

- Justin Bradley, Solutions Architect, Amazon Web Services
- Mahdi Sajjadpour, Senior Consultant, AWS Professional Services
- Mauricio Munoz, Solutions Architect, Amazon Web Services

Weitere Informationen

Zusätzliche Informationen finden Sie in den folgenden Ressourcen:

- Troubleshooting AWS Directory Service Administration Issues
- Troubleshooting Amazon WorkSpaces Administration Issues
- Troubleshooting Amazon WorkSpaces Client Issues
- Amazon WorkSpaces Administration Guide
- Amazon WorkSpaces Developer Guide
- Unterstützte Plattformen und Geräte
- How Amazon WorkSpaces Uses AWS KMS
- AWS CLI Command Reference – workspaces
- Monitoring Amazon WorkSpaces Metrics