Bewährte Methoden für die Bereitstellung von WorkSpaces Amazon-Anwendungen

Bewährte Methoden für die Bereitstellung von WorkSpaces Amazon-Anwendungen:

Table of Contents

Bewährte Methoden für die Bereitstellung von WorkSpaces Amazon-Anwendungen

Datum der Veröffentlichung: 19. Januar 2022 (Dokumentversionen)

Überblick

Dieses Whitepaper beschreibt eine Reihe von Best Practices für die Bereitstellung von WorkSpaces Amazon-Anwendungen. Der paper behandelt das Design von Amazon Virtual Private Cloud (VPC), die Erstellung und Verwaltung von Images, die Anpassung von Flotten und Strategien zur auto Flottenskalierung. Es umfasst Benutzerverbindungsmethoden, Authentifizierung und Integration mit Microsoft Active Directory. Dieses paper enthält auch Empfehlungen für die Gestaltung von WorkSpaces Anwendungssicherheit, Überwachung und Kostenoptimierung.

Dieses Whitepaper wurde verfasst, um einen schnellen Zugriff auf relevante Informationen zu ermöglichen. Es richtet sich an Netzwerktechniker, Spezialisten für Anwendungsbereitstellung, Verzeichnisingenieure oder Sicherheitsingenieure.

Einführung

Amazon WorkSpaces Applications ist ein vollständig verwalteter Anwendungs-Streaming-Service, der Benutzern von überall aus sofortigen Zugriff auf ihre Desktop-Anwendungen bietet. WorkSpaces Applications verwaltet die AWS Ressourcen, die zum Hosten und Ausführen Ihrer Anwendungen erforderlich sind. Es skaliert automatisch und bietet Ihren Benutzern bei Bedarf Zugriff. WorkSpaces Applications bietet Endbenutzern Zugriff auf die benötigten Anwendungen auf dem Gerät ihrer Wahl und bietet eine reaktionsschnelle Benutzererfahrung, die sich nicht von nativ installierten Anwendungen unterscheidet.

In den folgenden Abschnitten finden Sie Einzelheiten zu Amazon WorkSpaces Applications, erklären, wie der Service funktioniert, beschreiben, was Sie benötigen, um den Service zu starten, und erfahren, welche Optionen und Funktionen Ihnen zur Verfügung stehen. Bei der Bereitstellung von WorkSpaces Anwendungen für Endbenutzer ist es wichtig, bewährte Verfahren zu implementieren, um ein hervorragendes Benutzererlebnis zu bieten. Darüber hinaus profitieren Unternehmen jeder Größe von einer Kostenoptimierung, die die monatlichen Betriebskosten senkt.

Die wichtigsten Konzepte

Um das Beste aus WorkSpaces Anwendungen herauszuholen, sollten Sie sich mit den folgenden Konzepten vertraut machen:

- Image — Ein Image ist eine vorkonfigurierte Instanzvorlage. Ein Image enthält Anwendungen, die Sie an Ihre Benutzer streamen können, sowie Standard-Windows- und Anwendungseinstellungen, damit Ihre Benutzer schnell mit ihren Anwendungen beginnen können. AWS stellt Basisimages bereit, mit denen Sie Images erstellen können, die Ihre eigenen Anwendungen enthalten. Ein einmal erstelltes Abbild kann nicht mehr geändert werden. Um andere Anwendungen hinzufügen, vorhandene Anwendungen aktualisieren oder Abbildeinstellungen ändern zu können, müssen Sie ein neues Abbild erstellen. Sie können Ihre Bilder auf andere kopieren AWS-Regionenoder sie mit anderen AWS-Konto in derselben Region teilen.
- Image Builder — Ein Image Builder ist eine virtuelle Maschine, mit der Sie ein Image erstellen. Sie können einen Image Builder über die WorkSpaces Anwendungskonsole starten und eine Verbindung zu ihm herstellen. Nachdem Sie eine Verbindung zu einem Image Builder hergestellt haben, können Sie Ihre Anwendungen installieren, hinzufügen und testen und anschließend mithilfe des Image Builders ein Abbild erstellen. Sie können neue Image Builder über private Abbilder starten, deren Eigentümer Sie sind.
- Flotte — Eine Flotte besteht aus Flotteninstanzen (auch Streaming-Instances genannt), die das von Ihnen angegebene Image ausführen. Sie können die gewünschte Anzahl von Streaming-Instances für Ihre Flotte festlegen und Richtlinien konfigurieren, um Ihre Flotte automatisch je nach Bedarf zu skalieren. Beachten Sie, dass jeder Benutzer eine Instanz benötigt.
- Stack — Ein Stack besteht aus einer zugehörigen Flotte, Benutzerzugriffsrichtlinien und Speicherkonfigurationen. Sie richten einen Stack ein, um mit dem Streamen von Anwendungen an Benutzer zu beginnen.
- Streaming-Instance — Eine Streaming-Instance (auch bekannt als Fleet-Instance) ist eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die einem einzelnen Benutzer für das Anwendungsstreaming zur Verfügung gestellt wird. Nach Abschluss der Benutzersitzung wird die Instance von Amazon EC2 beendet.

VPC-Design

Richtlinien für das Design

Stellen Sie WorkSpaces Anwendungen in einer dedizierten VPC bereit. Bei der Entwicklung der WorkSpaces Anwendungs-VPC VPC die Größe dem prognostizierten Wachstum entsprechen. Reservieren Sie IP-Adresskapazität für neue Anwendungsfälle und zusätzliche Availability Zones (AZs), die zu einem späteren Zeitpunkt hinzugefügt werden können. Ein grundlegendes Konzept von WorkSpaces Applications besteht darin, dass nur ein Benutzer eine WorkSpaces Anwendungsinstanz nutzen kann. Denken Sie bei der Zuweisung von IP-Speicherplatz an einen Benutzer als eine IP-Adresse pro WorkSpaces Anwendungsinstanz. Mit WorkSpaces Applications ist es einem Benutzer möglich, mehrere WorkSpaces Anwendungsinstanzen zu nutzen. Daher müssen bei der Planung des IP-Raums auch Anwendungsfälle berücksichtigt werden, für die zusätzliche WorkSpaces Anwendungsinstanzen erforderlich sind.

Obwohl die maximale Größe einer VPC Classless Inter-Domain Routing (CIDR) /16 beträgt, wird AWS empfohlen, private IP-Adressen nicht zu stark zuzuweisen. Es ist möglich, die Größe der VPC durch zusätzliche CIDRs zu erweitern, dies ist jedoch begrenzt. Weisen Sie daher von Anfang an zu, was benötigt wird.

Wenn die WorkSpaces Anwendungsbereitstellung mit einer Active Directory-Domäne verbunden ist, muss für die für die VPC festgelegten DHCP-Optionen das Domänen-DNS konfiguriert sein. Der Domänennamenserver sollte die DNS-IP-Adressen angeben, die entweder für die Active Directory-Domäne autorisierend sind, oder der DNS sollte DNS-Anfragen an die autorisierenden DNS-Instanzen für die Active Directory-Domäne weiterleiten. Außerdem muss die VPC installiert `enableDnsHostnames` und `EnableDnsSupport` konfiguriert sein.

Verfügbarkeitszonen

Eine Availability Zone (AZ) besteht aus einem oder mehreren diskreten Rechenzentren mit redundanter Stromversorgung, Vernetzung und Konnektivität in einem AWS-Region. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Amazon WorkSpaces Applications benötigt nur ein Subnetz, in dem eine Flotte starten kann. Es hat sich bewährt, mindestens zwei Availability Zones zu konfigurieren, also ein Subnetz pro eindeutiger

Availability Zone. Verwenden Sie mehr als zwei Availability Zones, um die auto Skalierung von Flotten zu optimieren. Die horizontale Skalierung hat den zusätzlichen Vorteil, dass der IP-Speicherplatz in Subnetzen für das Wachstum hinzugefügt wird. Dieser Aspekt wird im folgenden Abschnitt zur Subnetzgröße in diesem Dokument behandelt. Die AWS-Managementkonsole sieht vor, dass bei der Erstellung einer Flotte nur zwei Subnetze angegeben werden müssen. Verwenden Sie die AWS Command Line Interface(AWS CLI) oder AWS CloudFormation , um mehr als zwei Subnetz-IDs zuzulassen.

Subnetzdimensionierung

Dedizieren Sie Subnetze für WorkSpaces Anwendungsflotten, um Flexibilität bei den Routing-Richtlinien und der Network Access Control List zu gewährleisten. Für Stacks gelten wahrscheinlich separate Ressourcenanforderungen. Beispielsweise können für WorkSpaces Anwendungsstapel Isolationsanforderungen gelten, die separaten Regelsätzen weichen. Wenn mehrere Amazon WorkSpaces Applications-Flotten dieselben Subnetze verwenden, stellen Sie sicher, dass die Summe der maximalen Kapazität aller Flotten die Gesamtzahl der verfügbaren IP-Adressen nicht überschreitet.

Wenn die maximale Kapazität für alle Flotten im selben Subnetz die Gesamtzahl der verfügbaren IP-Adressen überschreiten könnte oder hat, migrieren Sie Flotten in dedizierte Subnetze. Dadurch wird verhindert, dass automatische Skalierungsereignisse den zugewiesenen IP-Speicherplatz erschöpfen. Wenn die Gesamtkapazität einer Flotte den zugewiesenen IP-Bereich der zugewiesenen Subnetze übersteigt, verwenden Sie die API oder AWS CLI „Flotte aktualisieren“, um weitere Subnetze zuzuweisen. Weitere Informationen finden Sie unter Amazon VPC-Kontingente und wie Sie sie erhöhen können.

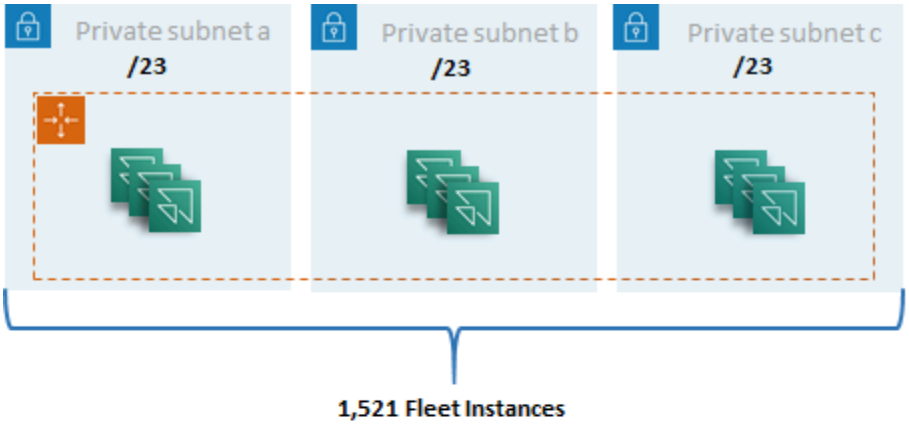
Es hat sich bewährt, die Anzahl der Subnetze zu skalieren, die Subnetze entsprechend zu dimensionieren und gleichzeitig Kapazität für das Wachstum in Ihrer VPC zu reservieren. Stellen Sie außerdem sicher, dass die Höchstwerte für die WorkSpaces Anwendungsflotte den gesamten IP-Speicherplatz, der den Subnetzen zugewiesen wurde, nicht überschreiten. Bei der Berechnung des gesamten IP-Speicherplatzes werden für jedes eingehende Subnetz fünf IP-Adressen reserviert. AWS Die Verwendung von mehr als zwei Subnetzen und die horizontale Skalierung bieten mehrere Vorteile, wie z. B.:

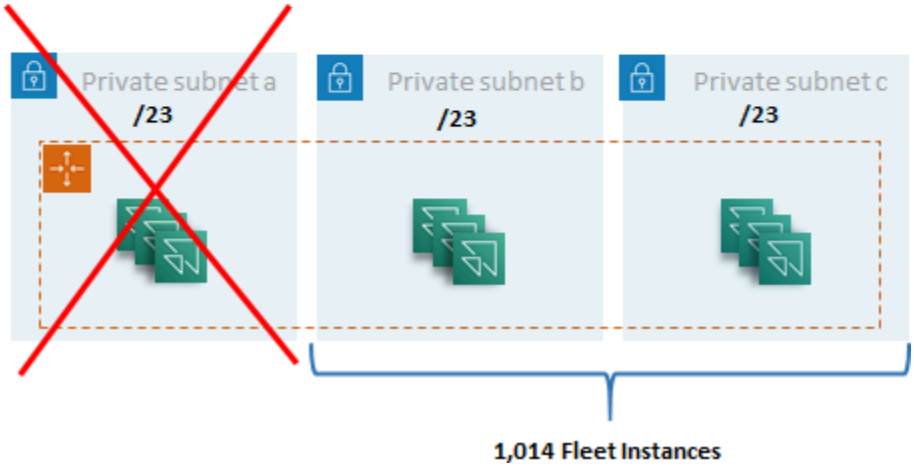
- Höhere Widerstandsfähigkeit bei einem Ausfall der Availability Zone
- Höherer Durchsatz bei automatischer Skalierung von Flotteninstanzen
- Effizientere Nutzung privater IP-Adressen, wodurch IP-Burn vermieden wird

Bei der Dimensionierung von Subnetzen für Amazon WorkSpaces Applications sollten Sie die Gesamtzahl der Subnetze und die erwartete Parallelität bei Spitzenauslastung berücksichtigen. Dies kann mithilfe von (`InUseCapacity`) plus reservierter Kapazität (`AvailableCapacity`) für eine Flotte überwacht werden. In Amazon WorkSpaces Applications ist die Summe der verbrauchten und der verfügbaren WorkSpaces Applications-Flotteninstanzen gekennzeichnet. `ActualCapacity` Um den gesamten IP-Speicherplatz richtig zu dimensionieren, prognostizieren Sie den Bedarf und dividieren Sie ihn durch die Anzahl der Subnetze`ActualCapacity`, abzüglich eines Subnetzes aus Gründen der Resilienz, die der Flotte zugewiesen sind.

Wenn die erwartete maximale Anzahl von Flotteninstanzen zu Spitzenzeiten beispielsweise 1000 beträgt und die Geschäftsanforderung darin besteht, bei einem Ausfall einer Availability Zone widerstandsfähig zu sein, erfüllen 3 x/23 Subnetze die technischen und geschäftlichen Anforderungen.

- /23 = 512 Hosts — 5 reserviert = 507 Flotteninstanzen pro Subnetz
- 3 Subnetze — 1 Subnetz = 2 Subnetze
- 2 Subnetze x 507 Flotteninstanzen pro Subnetz = 1.014 Flotteninstanzen zu Spitzenzeiten





Beispiel für die Größe eines Subnetzes

2 x /22-Subnetze würden zwar auch die Ausfallsicherheit gewährleisten, aber bedenken Sie Folgendes:

- Anstatt 1.536 IP-Adressen zu reservieren, führt die Verwendung von zwei AZs dazu, dass 2.048 IP-Adressen reserviert werden, wodurch IP-Adressen verschwendet werden, die für andere Funktionen verwendet werden könnten.
- Wenn auf eine AZ nicht mehr zugegriffen werden kann, ist die Möglichkeit, Flotteninstanzen zu skalieren, durch den Durchsatz einer AZ begrenzt. Dies kann die Dauer von `PendingCapacity` verlängern.

Subnetz-Routing

Es hat sich bewährt, private Subnetze für WorkSpaces Anwendungsinstanzen zu erstellen, die über eine zentrale VPC für ausgehenden Datenverkehr an das öffentliche Internet weitergeleitet werden.

Eingehender Datenverkehr für das Streaming der WorkSpaces Anwendungssitzung wird über den Amazon WorkSpaces Applications Service über Streaming Gateways abgewickelt: Sie müssen dafür keine öffentlichen Subnetze konfigurieren.

Intra-Region Konnektivität

Für WorkSpaces Anwendungsflotteninstanzen, die mit einer Active Directory-Domäne verbunden sind, konfigurieren Sie Active Directory-Domänencontroller in jeder AWS-Region Shared Services-VPC. Quellen für Active Directory können entweder Amazon EC2 EC2-basierte Domain-Controller oder AWS Microsoft Managed AD sein. Das Routing zwischen den VPCs für gemeinsame Dienste und WorkSpaces Anwendungen kann entweder über eine VPC-Peering-Verbindung oder über ein Transit-Gateway erfolgen. Obwohl Transit-Gateways die Komplexität des Routings in großem Umfang lösen, gibt es eine Reihe von Gründen, warum VPC-Peering in den meisten Umgebungen vorzuziehen ist:

- VPC-Peering ist eine direkte Verbindung zwischen den beiden VPCs (kein zusätzlicher Hop).
- Es fallen keine Gebühren pro Stunde an, sondern nur die standardmäßige Datenübertragungsrate zwischen Availability Zones.
- Es gibt keine Bandbreitenbeschränkung.
- Support für den Zugriff auf Sicherheitsgruppen zwischen VPCs.

Dies gilt insbesondere dann, wenn WorkSpaces Anwendungsinstanzen eine Verbindung zu and/or Dateiservern der Anwendungsinfrastruktur mit großen Datensätzen in einer Shared Service-VPC herstellen. Durch die Optimierung des Pfads zu diesen Ressourcen, auf die häufig zugegriffen wird, wird eine VPC-Peering-Verbindung bevorzugt, selbst bei Designs, bei denen alle anderen VPC- und Internet-Routings über ein Transit-Gateway ausgeführt werden.

Ausgehender Internetverkehr

Während das direkte Routing zu Shared Services größtenteils über eine Peering-Verbindung optimiert wird, kann ausgehender Datenverkehr für WorkSpaces Anwendungen entworfen werden, indem mithilfe AWS von Transit Gateway ein einziger Internetausgangspunkt aus mehreren VPCs erstellt wird. In einem Multi-VPC-Design ist es üblich, über eine dedizierte VPC zu verfügen, die den gesamten ausgehenden Internetverkehr steuert. Mit dieser Konfiguration verfügen Transit Gateways über eine größere Flexibilität und können das Routing über Standard-Routingtabellen steuern, die an Subnetze angeschlossen sind. Dieses Design unterstützt auch transitives Routing ohne zusätzliche

Komplexität und macht redundante Network Address Translation (NAT) -Gateways oder NAT-Instances in jeder VPC überflüssig.

Sobald der gesamte ausgehende Internetverkehr in einer einzigen VPC zentralisiert ist, sind NAT-Gateways oder NAT-Instances eine gängige Designwahl. Um herauszufinden, welches für Ihr Unternehmen am besten geeignet ist, schauen Sie sich das Administratorhandbuch zum Vergleich von NAT-Gateways und NAT-Instances an.AWS Die Network Firewall kann den Schutz über Sicherheitsgruppen- und Netzwerkzugriffskontrollen hinaus erweitern, indem sie auf Routenebene schützt und statusfreie und statusbehaftete Regeln auf den Ebenen 3 bis 7 im OSI-Modell anbietet. Weitere Informationen finden Sie unter Bereitstellungsmodelle für die AWS Network Firewall. Wenn sich Ihr Unternehmen für ein Drittanbieterprodukt entschieden hat, das erweiterte Funktionen wie URL-Filterung bietet, stellen Sie den Service in Ihrer ausgehenden Internet-VPC bereit. Dies kann NAT-Gateways oder NAT-Instances ersetzen. Folgen Sie den Richtlinien des Drittanbieters.

On-premises

Wenn Konnektivität zu lokalen Ressourcen erforderlich ist, insbesondere für WorkSpaces Anwendungsinstanzen, die mit Active Directory verknüpft sind, stellen Sie eine äußerst stabile Verbindung her. AWS Direct Connect

VPC-Endpunkte

Amazon S3 VPC-Endpunkt

Viele Bereitstellungen von Amazon WorkSpaces Applications erfordern die Persistenz des Benutzerstatus über Basisordner und Anwendungseinstellungen. Ermöglichen Sie die private Kommunikation mit diesen Amazon Simple Storage Service (Amazon S3) -Standorten, da dadurch die Nutzung des öffentlichen Internets vermieden wird. Sie können dies über ein VPC-Endpunkt-Gateway erreichen. Ein VPC-Endpunkt-Gateway wird dem AWS PrivateLink für Amazon S3 vorgezogen, weil:

- Es ist kostenoptimiert für die Netzwerkzugriffsanforderungen von WorkSpaces Anwendungen
- Für lokale Ressourcen ist kein Zugriff auf Amazon S3 S3-Buckets erforderlich
- Ein benutzerdefiniertes Richtliniendokument kann verwendet werden, um den Zugriff nur von den WorkSpaces Applications-Instances aus einzuschränken

Sobald Sie das VPC-Endpunkt-Gateway erstellt haben, empfiehlt es sich, die privatisierte Verbindung durch die Erstellung einer benutzerdefinierten Richtlinie zu sichern. Die benutzerdefinierte Richtlinie

beginnt mit dem Amazon-Ressourcennamen (ARN) der Identity and Access Management-Rolle des WorkSpaces Anwendungsdienstes. Geben Sie explizit die S3-Aktionen an, die für die Persistenz des Benutzerstatus erforderlich sind.

> **Note**
>
> Das folgende Beispiel in `Resources` diesem Abschnitt gibt zuerst den Pfad des State-Home-Ordners und dann den Pfad der Anwendungseinstellungen an zweiter Stelle an.

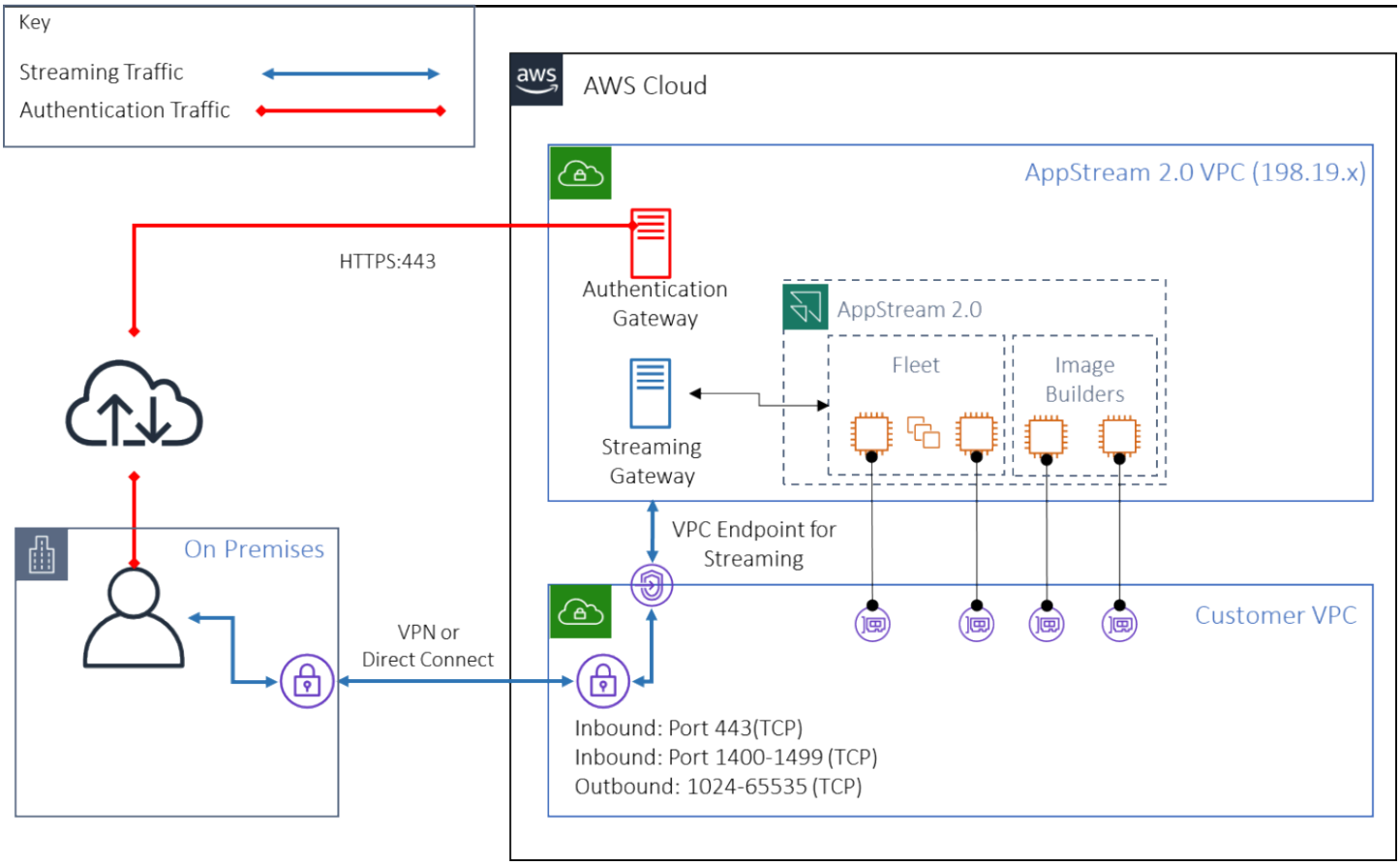
Example

VPC-Endpunkt der API-Schnittstelle von Amazon WorkSpaces Applications

Privatisieren Sie in Entwurfsszenarien, in denen API- und CLI-Befehle für WorkSpaces Amazon-Anwendungen ihren Ursprung in Ihrer VPC haben, diese programmatischen Aufrufe über einen VPC-Schnittstellen-Endpunkt.

VPC-Endpunkt der Streaming-Schnittstelle von Amazon WorkSpaces Applications

Es ist zwar möglich, den Streaming-Verkehr von Amazon WorkSpaces Applications über einen VPC-Endpunkt mit Schnittstelle zu leiten, verwenden Sie diese Konfiguration jedoch mit Vorsicht. Das standardmäßige Streaming-Verhalten über das öffentliche Internet ist die effizienteste und leistungsstärkste Übertragungsmethode für den Streaming-Verkehr von Amazon WorkSpaces Applications.



VPC-Endpunkt der Streaming-Schnittstelle von Amazon WorkSpaces Applications

Wie in der vorherigen Abbildung dargestellt, ist das öffentliche Internet der effizienteste Weg zu Amazon WorkSpaces Applications Streaming Gateways. Das Routing über die vom Kunden verwaltete VPC und das Netzwerk erhöht die Komplexität und Latenz. Außerdem fallen zusätzliche Gebühren für die Datenübertragung an. Direct Connect

> **Note**
>
> Nur Streaming wird vom VPC-Endpunkt unterstützt, und die Authentifizierung muss weiterhin über das öffentliche Internet erfolgen. Zugangsvoraussetzungen wie SAML Single Sign-On (SSO) Identity Provider (IdP) bleiben eine Voraussetzung, auf die nur über das öffentliche Internet zugegriffen werden kann.

Image-Erstellung und -Verwaltung

Wenn Sie eine Flotte oder einen Image Builder in WorkSpaces Applications starten, müssen Sie eines der Basis-Images der WorkSpaces Anwendung auswählen. Administratoren können dann auf dem Basis-Image aufbauen, um ihre eigenen Anwendungen und Konfigurationseinstellungen hinzuzufügen.

Beim Erstellen eines Images sind wichtige Überlegungen zu beachten, um sicherzustellen, dass Anwendungen ordnungsgemäß und sicher funktionieren. Darüber hinaus gibt es Überlegungen zum Design, wie dieses Image verwaltet werden soll.

Ein WorkSpaces Anwendungs-Image erstellen

Beim Erstellen eines neuen Images ist es wichtig, Folgendes zu berücksichtigen:

- Betriebssystem
- Anwendungen
- Benutzerprofil
- Sicherheit
- Leistung
- Agent-Version
- Image Assistant CLI

Erstellen eines WorkSpaces Anwendungs-Images

Im November 2021 hat WorkSpaces Applications die Unterstützung für Amazon Linux 2 eingeführt. Mit dieser Ankündigung unterstützt WorkSpaces Applications nun vier Plattformtypen:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Amazon Linux 2

Es ist möglich, dass Sie je nach den Anforderungen Ihrer Anwendung eine bestimmte Plattform auswählen müssen (wenn Ihre Anwendung beispielsweise Windows benötigt, ist Amazon Linux

2 keine Option). Neben den Anwendungsanforderungen können Sie anhand der folgenden Vergleichsmatrix herausfinden, welcher Plattformtyp am besten zu Ihrem Anwendungsfall und Ihrer Umgebung passt:

Tabelle 1 — Plattformtypen, wann sie verwendet werden sollten und Preise

Plattformtype	Wann sollte dies verwendet werden?	Preisgestaltung für Flotten*
Windows Server (2012 R2, 2016 oder 2019)	Ihre Anwendung kann nur unter Windows ausgeführt werden (und Amazon Linux 2 wird nicht unterstützt). Sie möchten Ihren Streaming-Instances einer Domain beitreten. Sie möchten die vorhandenen Gruppenrichtlinien für Ihre WorkSpaces Anwendungs-Streaming-Instances verwenden (Linux hält sich nicht an Gruppenrichtlinien, aber Sie können Sitzungsskripts verwenden, um die Konfiguration zu automatisieren, wenn eine Sitzung gestartet wird). Sie werden Desktop View verwenden und Ihre Benutzer bevorzugen das Windows-Desktop-Erlebnis. Sie bevorzugen es, die Image Assistant-Anwendung zu verwenden, die einen schrittweisen Assistenten bereitstellt, um Ihren Anwendungskatalog und Ihr Image zu erstellen. Derzeit	RDS SAL-Gebühr (Microsoft Remote Desktop Services Subscriber Access License) in Höhe von 4,19$ pro Monat für jeden einzelnen Benutzer** zuzüglich folgender Leistungen: 1. 0,10$ pro Stunde für Flotten Always-On On-Demand 2. 0,15$ pro Stunde für Elastic-Flotten

Plattformtype	Wann sollte dies verwendet werden?	Preisgestaltung für Flotten*
	müssen Sie Ihr Amazon Linux 2-Image mithilfe von Terminalbefehlen erstellen (weitere Informationen finden Sie in diesem Tutorial). Sie möchten Persistence für Anwendungseinstellungen verwenden. Das Aktivieren der Persistenz von Anwendung seinstellungen wird derzeit für Linux-based Stacks nicht unterstützt.	
Amazon Linux 2	Sie möchten kostengünstigere Streaming-Instances nutzen und RDS SAL-Lizenzgebühren vermeiden. Ihre Anwendung en sind mit Amazon Linux 2 kompatibel	Linux-Instances sind im Vergleich zu Windows-I nstances kostengünstiger. Bei Linux zahlen Sie keine RDS SAL-Gebühren und die folgenden Stundengebühren: 1. 0,084$ pro Stunde für Always-On Flotten On-Demand 2. 0,112$ pro Stunde für Elastic-Flotten

* Basierend auf stream.standard.medium in der Region Nord-Virginia

** Berechtigte Kunden können ihre eigene Lizenz mitbringen, um die Gebühren für AWS RDS SAL zu vermeiden. Weitere Informationen finden Sie auf der Seite mit den Preisen für WorkSpaces Anwendungen. Kunden aus dem Bildungswesen haben möglicherweise auch Anspruch auf ein Sonderangebot. Schulen, Universitäten und bestimmte öffentliche Einrichtungen können sich für eine reduzierte Microsoft RDS SAL-Benutzergebühr qualifizieren.

Anwendungen

Vor der Installation von Anwendungen ist es wichtig, die Anwendungsanforderungen wie Anwendungsabhängigkeiten und Hardwareanforderungen zu überprüfen. Stellen Sie nach der erfolgreichen Installation von Anwendungen auf Image Builder-Instanzen sicher, dass Sie zwischen den Benutzern wechseln und die Anwendungen im Testbenutzerkontext testen.

Beachten Sie bei der Planung Ihrer Anwendungsbereitstellung die Dienstendpunkte und Kontingente. Bereinigen Sie außerdem die Installations- und Hilfsdateien, um den gesamten Speicherplatz auf Laufwerk C zu optimieren, bevor Sie ein Image erstellen. Zur Erinnerung: Die WorkSpaces Anwendungsinstanzen verfügen über ein 200 GB-Volume mit fester Größe. Die Optimierung des Festplattenspeichers nach der Installation ist eine bewährte Methode, um sicherzustellen, dass das Volumen mit fester Größe niemals überschritten wird.

Wenn Sie den Katalog der Anwendungen ändern möchten, auf die Ihre Benutzer in Echtzeit zugreifen können, stellt das dynamische Anwendungsframework API-Operationen bereit. Die von den Anbietern dynamischer Apps verwalteten Anwendungen können im Abbild enthalten sein oder sich außerhalb der Instance befinden, etwa auf einer Windows-Dateifreigabe oder in einer Anwendungsvirtualisierungstechnologie. Für dieses Feature ist eine WorkSpaces Anwendungsflotte erforderlich, die mit einer Microsoft Active Directory-Domäne verknüpft ist. Weitere Informationen finden Sie unter Active Directory mit WorkSpaces Anwendungen verwenden.

App-Blöcke

App-Blöcke stellen das Setup-Skript und die Anwendungsdateien dar, die zum Starten der Anwendungen erforderlich sind, die Ihre Benutzer verwenden werden. Bei der virtuellen Festplatte (VHD) kann es sich um ein beliebiges Objekt aus Amazon S3 handeln. Es wird empfohlen, dass dieses Objekt weniger als 1,5 GB groß ist, da es vollständig heruntergeladen werden muss, bevor der Benutzer auf die Anwendung zugreifen kann.

Optimierung von App-Blöcken

Für Windows-based Flotten wird empfohlen, eine VHDX-Datei zu erstellen, die Ihre Anwendung enthält. Für Linux-based Flotten wird empfohlen, ein Image (IMG) zu erstellen. Diese virtuellen Festplatten sollten so klein wie möglich erstellt werden, um die Anwendungsdateien zu hosten. Virtuelle Festplatten können komprimiert werden, um ihre Größe weiter zu verringern. Im Setup-Skript müssen Sie die Festplatte vor dem Mounten entpacken. Das PowerShell Beispiel-Setupskript für Windows enthält die Entpackungsfunktion. Es gibt einen Kompromiss zwischen der Erweiterung

eines Archivs (Zip) und der Download-Geschwindigkeit. Möglicherweise sind einige Tests erforderlich, um ein Gleichgewicht zu finden, das die schnellste Startzeit der Anwendung bietet.

Anwendungen werden aktualisiert

Anwendungen können sowohl geringfügige als auch größere Änderungen aufweisen. Verwenden Sie für kleinere Updates die Option Versionsverwaltung auf dem Amazon S3 S3-Bucket aktivieren, der Ihre App-Blockdateien hostet. Mit dieser Einstellung können Administratoren zu früheren Versionen einer bestimmten Anwendung zurückkehren, indem sie die Version des betreffenden Anwendungs-VHD-Objekts ändern, ohne die App-Block-Konfiguration zu ändern. Erstellen Sie bei größeren Updates einen neuen App-Block für die aktualisierte virtuelle Festplatte. Auf diese Weise können Administratoren größere Anwendungsänderungen auf App-Blockebene und nicht auf Versionsebene trennen, wodurch ein besser organisierter Ansatz für die administrative Anwendungsverwaltung ermöglicht wird.

Anpassung des Benutzerprofils

Amazon WorkSpaces Applications ist von Natur aus eine nicht persistente Anwendungs- und Desktop-Lösung. Wenn eine Benutzersitzung beendet wird, werden sowohl System- als auch Benutzeränderungen beendet. Aktivieren Sie die Persistenz der Anwendungseinstellungen nur bei Bedarf. Dies kann den Anmeldevorgang zusätzlich belasten und die Kosten für den erforderlichen S3-Speicher mit sich bringen.

In Situationen, in denen die Persistenz der Anwendungseinstellungen erforderlich ist, AWS empfiehlt es sich, diese Verbindung über eine benutzerdefinierte Richtlinie und einen S3 VPC-Gateway-Endpunkt zu sichern. Bewerten Sie die Gesamtgröße der Anwendungseinstellungen und minimieren Sie die in der Persistenz der Anwendungseinstellungen gespeicherten Einstellungen, um Kosten und Leistung zu optimieren.

Die Anpassung des Benutzerprofils kann auf einer WorkSpaces Applications Image Builder Builder-Instanz konfiguriert werden. Dazu gehören das Hinzufügen und Ändern von Registrierungsschlüsseln, das Hinzufügen von Dateien und andere benutzerspezifische Konfigurationen. Im WorkSpaces Applications Image Assistant besteht die Möglichkeit, ein Benutzerprofil zu erstellen. Dadurch wird das Vorlagenbenutzerprofil in das Standardbenutzerprofil kopiert. Nachdem das Image für eine Flotte bereitgestellt wurde, wird das Benutzerprofil von Endbenutzern, die Sitzungen aus der Flotte streamen, anhand des Standardbenutzerprofils erstellt. Es ist wichtig, die Größe des Benutzerprofils zu minimieren, insbesondere wenn die Persistenz der Anwendungseinstellungen aktiviert ist. Standardmäßig beträgt die maximale VHDx-Größe für das Benutzerprofil 1 GB. Bei jedem Start einer Streaming-Sitzung wird eine VHDx-Benutzerprofildatei

aus einem S3-Bucket heruntergeladen. Dies erhöht die Vorbereitungszeit für die Streamingsitzung und birgt das Risiko einer Überschreitung des Grenzwerts, was zu einem Fehler beim Mounten des Benutzerprofils mithilfe der VHDx-Datei führen kann.

Für Anwendungsfälle, die ein Benutzerprofil mit mehr als 1 GB erfordern, empfiehlt AWS, alternative Methoden zum Speichern von Profilen zu verwenden. Zum Beispiel die Verwendung von Roaming-Profilen oder FSLogix-Profilcontainern auf gemeinsam genutztem Speicher wie Amazon FSx for Windows File Server. Weitere Informationen finden Sie unter Verwenden von Amazon FSx for Windows File Server und FSLogix zur Optimierung der Persistenz von Anwendungseinstellungen auf Amazon-Anwendungen. WorkSpaces

Sicherheit

Es gibt verschiedene Sicherheitsmaßnahmen, die Entwickler berücksichtigen müssen. WorkSpaces Anwendungsadministratoren sind für die Installation und Wartung der Updates für das Windows-Betriebssystem, Ihre Anwendungen und deren Abhängigkeiten verantwortlich. Weitere Hinweise zur Aktualisierung der Basis-Images finden Sie unter Keep Your WorkSpaces Applications Image. Dort finden Sie Up-to-Date weitere Hinweise dazu, wie Sie die Basis-Images auf dem neuesten Stand halten.

Standardmäßig ermöglichen WorkSpaces Applications Benutzern oder Anwendungen, jedes Programm auf der Instanz zu starten, das über die im Image-Anwendungskatalog angegebenen hinausgeht. Dies ist nützlich, wenn Ihre Anwendung im Rahmen eines Workflows auf eine andere Anwendung angewiesen ist, Sie aber nicht möchten, dass der Benutzer diese abhängige Anwendung direkt starten kann. Ihre Anwendung startet beispielsweise den Browser, um Hilfeanweisungen von der Website des Anwendungsherstellers bereitzustellen, Sie möchten jedoch nicht, dass der Benutzer den Browser direkt startet. In einigen Situationen möchten Sie möglicherweise steuern, welche Anwendungen auf den Streaming-Instances gestartet werden können. Microsoft AppLocker ist eine Anwendungssteuerungssoftware, die explizite Kontrollrichtlinien verwendet, um zu aktivieren oder zu deaktivieren, welche Anwendungen ein Benutzer ausführen kann.

Antivirensoftware kann sich nachteilig auf Streaming-Sitzungen und Image Builder-Instanzen auswirken. AWS empfiehlt, automatische Updates für die Antivirensoftware nicht zu aktivieren. Weitere Informationen zu Windows Defender finden Sie unter Antivirensoftware.

Leistung

Bevor Sie ein neues Image erstellen, ist es wichtig, die Anwendungen als Testbenutzer zu testen. Wenn Sie als Testbenutzer testen, können Sie sicherstellen, dass Anwendungen in einem

Benutzerkontext ohne Administratorrechte ausgeführt werden können. Überprüfen Sie außerdem die Anwendungsleistung und die Benutzererfahrung mithilfe integrierter Tools wie dem Task-Manager und dem Systemmonitor. Es hat sich bewährt, die Ressourcennutzung wie CPU-, Arbeitsspeicher- und GPU-Speicher zu überwachen. Wenn die CPU-, Arbeitsspeicher- oder GPU-Speicherressourcen eingeschränkt sind, sollten Sie ein Upgrade des Instance-Typs in Betracht ziehen. Um die Leistung zu verbessern:

- Deaktivieren Sie Browser-Popupfenster
- Deaktivieren Sie die erweiterte IE-Sicherheit

WorkSpaces Auswahl der Version des Anwendungsagenten

Wenn Sie ein neues Image erstellen, können Sie wählen, ob Sie die neueste WorkSpaces Applicationsagent-Software verwenden oder nicht aktualisieren möchten. Jede Version der WorkSpaces Applications Agent-Software enthält Fehlerkorrekturen und Funktionserweiterungen. Behalten Sie Ihr Image mit der aktuellsten Software bei. Die diesbezüglichen Mechanismen finden Sie im Abschnitt Image-Updates dieses Dokuments.

Sie können die Option Aktuellen Agenten verwenden wählen. Diese Option stellt sicher, dass beim Start immer der neueste WorkSpaces Anwendungsagent installiert ist. Unerwartete Änderungen können sich jedoch auf die Benutzererfahrung auswirken, und ein Agent-Update kann die Zeit bis zum Starten einer Instanz verlängern. Um ein Basis-Image zu aktualisieren, muss das Image neu erstellt werden. Es ist auch wichtig, dass Sie Tests durchführen, bevor Sie das aktualisierte Image in der Produktionsumgebung einsetzen, um die Startzeit zu minimieren.

Image Assistant-Befehlszeilenschnittstelle (CLI)

Entwickler, die WorkSpaces Anwendungs-Images automatisieren oder programmgesteuert erstellen möchten, sollten die Image Assistant CLI verwenden. Dies ist auf Image Buildern mit der WorkSpaces Applications Agent-Software verfügbar, die am oder nach dem 26. Juli 2019 veröffentlicht wurde. In der folgenden allgemeinen Übersicht wird der Prozess zur programmgesteuerten Erstellung eines WorkSpaces Anwendungs-Images beschrieben:

1. Verwenden Sie die Installationsautomatisierung Ihrer Anwendung, um die erforderlichen Anwendungen auf Ihrem Image Builder zu installieren. Diese Installation kann Anwendungen enthalten, die Ihre Benutzer starten werden, sowie mögliche Abhängigkeiten und Hintergrundanwendungen.

2. Bestimmen Sie die zu optimierenden Dateien und Ordner.
3. Verwenden Sie gegebenenfalls den `add-application` CLI-Vorgang Image Assistant, um die Anwendungsmetadaten und das Optimierungsmanifest für das WorkSpaces Anwendungs-Image anzugeben.
4. Um weitere Anwendungen für das WorkSpaces Anwendungs-Image anzugeben, wiederholen Sie die Schritte 1 bis 3 für jede Anwendung nach Bedarf.
5. Verwenden Sie gegebenenfalls den Image Assistant `update-default-profile` CLI-Vorgang, um das Standard-Windows-Profil zu überschreiben und die Standardanwendung und die Windows-Einstellungen für Ihre Benutzer zu erstellen.
6. Verwenden Sie die CLI-Operation `create-image` des Image Assistant, um das Abbild zu erstellen.

Weitere Informationen finden Sie unter Programmgesteuertes Erstellen Ihres WorkSpaces Anwendungs-Images mithilfe der Image Assistant-CLI-Operationen.

Verwaltung des Streaming-Erlebnisses von Benutzern

Anpassung mithilfe von Sitzungsskripten

WorkSpaces Applications stellt Instanz-Sitzungsskripte bereit. Sie können diese Skripte verwenden, um benutzerdefinierte Skripte auszuführen, wenn in den Streaming-Sitzungen der Benutzer bestimmte Ereignisse auftreten. Sie können beispielsweise benutzerdefinierte Skripts verwenden, um Ihre WorkSpaces Anwendungsumgebung vorzubereiten, bevor die Streaming-Sitzungen Ihrer Benutzer beginnen. Sie können benutzerdefinierte Skripte auch einsetzen, um Streaming-Instances zu bereinigen, nachdem die Benutzer ihre Streaming-Sitzungen beendet haben.

Geben Sie Sitzungsskripts in einem WorkSpaces Anwendungs-Image an. Weitere Informationen zur Konfiguration von Sitzungsskripten finden Sie im Abschnitt zur Verwaltung der Benutzererfahrung mithilfe von Sitzungsskripten im Administratorhandbuch. In Verbindung mit einer Netzwerkfreigabe oder einem AWS Identity and Access Management(IAM-) Profil können Sie Sitzungsskripts verwenden, um zusätzliches Scripting von einem Speicherort abzurufen. Mit diesem zusätzlichen Scripting können Sie die Benutzererfahrung weiter optimieren. Dadurch kann die Anzahl der Images und Flotten minimiert werden, die für die Bereitstellung von Anwendungsumgebungen für Ihre Benutzer erforderlich sind.

Verwenden der Active Directory-Gruppenrichtlinie

Wenn Sie planen, WorkSpaces Anwendungsflotten in einer Active Directory-Domäne zu verwenden, können Sie Gruppenrichtlinienobjekte (GPOs) verwenden, um die Benutzererfahrung zu verwalten. GPOs können der Organisationseinheit (OU) zugewiesen werden, in der die WorkSpaces Anwendungsinstanzen erstellt werden. Um die Image-Erstellung zu vereinfachen, starten Sie das WorkSpaces Basis-Anwendungs-Image in einer Organisationseinheit, die die Vererbung blockiert. Dadurch wird verhindert, dass sich andere Domänenrichtlinien auf die Benutzererfahrung der WorkSpaces Anwendungen auswirken. Stellen Sie jede Flotte in einer eigenen Organisationseinheit bereit, wobei die Umgebung durch einzigartige GPOs geschaffen wird. So können Sie die Vorteile des WorkSpaces Application-Image-Managements nutzen.

Ein Beispiel für die Verwendung von Gruppenrichtlinien besteht darin, für jede Anwendungsflotte verschiedene Internet Explorer-Homepages für einen Image-Satz anzugeben. WorkSpaces

Image-Updates

Software-Patches sind für die Sicherheit und Leistung von Rechenressourcen von entscheidender Bedeutung. Häufiges Patchen wird in der Sicherheitssäule des Frameworks als bewährte Methode aufgeführt. Well-Architected

Wenn Ihr Image erstellt und bereitgestellt wird, gibt es vier Kategorien von Software, für die Patches in Ihrem WorkSpaces Anwendungs-Image erforderlich sind:

- Anwendungen und Abhängigkeiten — Sie sind dafür verantwortlich, die Anwendungen und Abhängigkeiten in Ihren Images zu patchen.
- Microsoft Windows-Betriebssystem — Sie sind für die Installation und Wartung von Updates für Windows verantwortlich.
- Softwarekomponenten — Dies sind Treiber, Agenten und andere Software, die für den Betrieb von WorkSpaces Anwendungen erforderlich ist (z. B. der CloudWatchAmazon-Agent). WorkSpaces Applications veröffentlicht regelmäßig neue Basis-Images, die neue Agenten und Treiber enthalten. Sie können Ihr Image mit der neuesten Basisversion neu erstellen, um die Softwarekomponenten auf ihren Images auf den neuesten Stand zu bringen. Das Neuerstellen eines Images auf der neuesten Basis kann zeitaufwändig und umständlich sein, wenn es viele Anwendungen oder komplexe Anwendungsinstallationen gibt.
- WorkSpaces Anwendungsagent — Sie können in Image Assistant die Option Immer die neueste Agentenversion verwenden wählen. Mit dieser Option verwenden Streaming-Instances, die vom Image aus gestartet werden, automatisch die neueste Version des Agenten.

Sie können Ihr WorkSpaces Anwendungs-Image auf dem neuesten Stand halten, indem Sie einen der folgenden Schritte ausführen:

- Ein Image mithilfe von Image-Updates für verwaltete WorkSpaces Anwendungen aktualisieren — Diese Aktualisierungsmethode bietet die neuesten Windows-Betriebssystemupdates und Treiberupdates sowie die neueste WorkSpaces Applications Agent-Software. Diese verwaltete Methode aktualisiert Dienste und Microsoft-Betriebssystemkomponenten, ermöglicht Ihnen jedoch nicht, Ihre Anwendungskomponenten zu aktualisieren. Es hat sich bewährt, diese Methode zu verwenden, wenn Anwendungsinstallationen komplex sind oder eine manuelle Konfiguration erfordern.
- Aktualisieren Sie die WorkSpaces Applications Agent-Software mithilfe von Image-Versionen für verwaltete WorkSpaces Anwendungen — Diese Aktualisierungsmethode stellt die neueste WorkSpaces Applications Agent-Software bereit. Mit dieser Methode können Sie Ihre Anwendungskomponenten aktualisieren.

Anpassung der Flotte

Flottentyp

Bei der Erstellung einer Flotte müssen Kunden einen Flottentyp wählen. Jeder Flottentyp bietet unterschiedliche Vorteile in Bezug auf Benutzererfahrung, Kosten und Wartungsaufwand. Unabhängig vom gewählten Flottentyp unterstützt jede Option sowohl die Windows- als auch die Linux-Plattformtypen sowie Desktop View oder Application View.

Kunden können jetzt aus den folgenden Flottenarten wählen:

- Always-On— Dieser Flottentyp bietet Benutzern sofortigen Zugriff auf ihre Apps. Ihnen werden alle laufenden Instances in Ihrer Flotte in Rechnung gestellt, auch wenn keine Benutzer Apps streamen.
- On-Demand— Wählen Sie diesen Flottentyp aus, um Ihre Streaming-Kosten zu optimieren. Bei einer On-Demand-Flotte haben Benutzer eine Startzeit von etwa ein bis zwei Minuten für ihre Sitzung. Die Gebühren für Streaming-Instances werden Ihnen jedoch nur berechnet, wenn Benutzer verbunden sind, und eine geringe Stundengebühr für jede Instanz in der Flotte, bei der es sich nicht um Streaming-Apps handelt.
- Elastisch — Elastic Fleets können für Anwendungen verwendet werden, die keine Installation erfordern und von einer virtuellen Festplatte (VHD) ausgeführt werden können. Elastic Fleets unterstützen keine WorkSpaces Anwendungs-Images und erfordern auch keine Skalierungsrichtlinien. Ihnen wird nur die Dauer einer Streaming-Sitzung in Rechnung gestellt.

Tabelle 2 — Flottenarten von Amazon WorkSpaces Applications

Flottentyp	Wann sollte dies verwendet werden?	Benutzererfahrung	Preismodell	Hinweise
Always-On	Ihre Benutzer benötigen sofortigen Zugriff auf Anwendungen, wenn sie	Sofortiger Zugriff auf Anwendungen	Sie zahlen den vollen Preis für jede Instanz, die in Ihrer Flotte verfügbar ist	Unterstützt benutzerdefinierte Image- und Skalierungsrichtlinien.

Flottentyp	Wann sollte dies verwendet werden?	Benutzererfahrung	Preismodell	Hinweise
	eine Sitzung starten. Sie werden keine nennenswerten Kapazitätsüberschüsse in Ihrer Flotte haben, vielleicht weil Ihre Nutzungsmuster vorhersehbar sind und Sie die Kosten mit Skalierungsrichtlinien zuverlässig kontrollieren können.		(unabhängig davon, ob sie für eine Sitzung verwendet wird).	

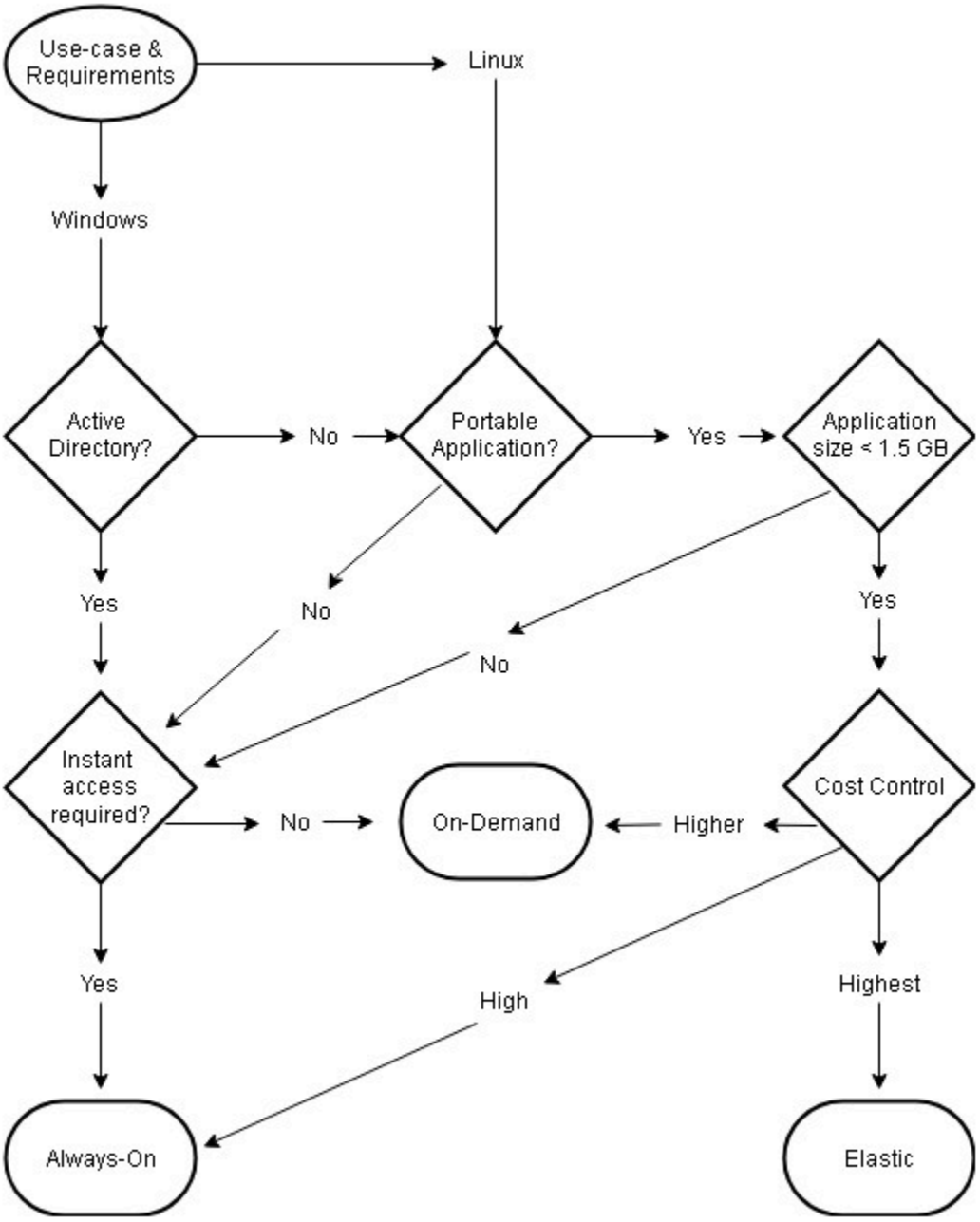
Flottentyp	Wann sollte dies verwendet werden?	Benutzererfahrung	Preismodell	Hinweise
On-Demand	Sie müssen erhebliche Überkapazitäten in Ihren Flotten aufrechterhalten. Sie möchten eine möglichst kostenoptimierte Umgebung und möchten nicht den vollen Preis für ungenutzte Kapazität zahlen. Ihre Benutzer können nach dem Starten einer Sitzung ein bis zwei Minuten warten, bis sie auf ihre Anwendungen zugreifen .Sie verwenden größere Instance-Typen. Die stündlichen Kosten für eine laufende Instance sind viel teurer als die Gebühr für	Benutzer warten nach dem Start einer Sitzung ein bis zwei Minuten, bis sie auf ihre Anwendungen zugreifen können.	Sie zahlen den vollen Preis nur für Streaming-Instances mit einer aktiven Sitzung und dann eine geringe Stundengebühr für inaktive Instances.	Unterstützt benutzerdefinierte Image- und Skalierungsrichtlinien.

Flottentyp	Wann sollte dies verwendet werden?	Benutzererfahrung	Preismodell	Hinweise
	die angehaltene Instanz.			

Flottentyp	Wann sollte dies verwendet werden?	Benutzererfahrung	Preismodell	Hinweise
Elastic	Ihre Anwendung und ihre Abhängigkeiten sind kleiner als ~1,5 GB. Jedes Mal, wenn ein Benutzer eine Sitzung in einer Elastic Fleet startet, muss Ihre virtuelle Festplattendatei (VHD) von Amazon S3 in die Sitzung heruntergeladen werden. Größere VHD-Dateien (d. h. Dateien mit einer Größe von mehr als 1,5 GB) führen daher zu einer schlechten Benutzererfahrung. Ihre Anwendung ist portabel. Das heißt, Ihre Anwendung und all ihre Abhängigkeiten können auf einer virtuelle	Der Benutzer wartet nach dem Start der Sitzung 45 Sekunden bis 3 Minuten, um auf Anwendungen zuzugreifen (die Wartezeit hängt von der Größe der virtuellen Festplatte ab).	Ihnen wird nur die Dauer einer Streaming-Sitzung in Rechnung gestellt. Da es bei Elastic-Flotten kein Konzept für inaktive Instances gibt, fallen für ungenutzte Instances keine Gebühren an.	Unterstützt keine benutzerdefinierten Images (der Kunde stellt VHD mit Anwendungen zur Verfügung) oder Skalierungsrichtlinien. Unterstützt derzeit alle `stream.standard.small` `stream.standard.medium` Instanzen. Wenn Ihr Anwendungsfall einen anderen Instanztyp erfordert, wenden Sie sich bitte an Ihr AWS Account-Team.

Flottentyp	Wann sollte dies verwendet werden?	Benutzererfahrung	Preismodell	Hinweise
	n Festplatte platziert und von den Streaming-Instances aus gestartet werden, für die VHD.You keine Domänenverbindung erforderlich ist (Domänenbeitritt ist derzeit bei Elastic-Flotten nicht verfügbar). Sie möchten nur für aktive Sitzungen zahlen (d. h. Sie zahlen nicht für ungenutzte Kapazität in Ihrer Flotte). Ihre Benutzer können nach dem Start einer Sitzung 45 Sekunden oder länger warten, bis sie auf ihre Anwendungen zugreifen. Sie möchten, dass AWS die Skalierung für			

Flottentyp	Wann sollte dies verwendet werden?	Benutzererfahrung	Preismodell	Hinweise
	Sie verwaltet (keine Skalierungsrichtlinien zur Verwaltung).			



Anwendungsfälle und Anforderungen für Flotten

Dimensionierung der Flotte

Mindestkapazität und geplante Skalierung

Bei der Dimensionierung Ihrer WorkSpaces Anwendungsflotte gibt es mehrere Überlegungen, die sich direkt auf die Benutzererfahrung und die Kosten auswirken. Der für Mindestkapazität

eingegebene Wert stellt sicher, dass die Anzahl der WorkSpaces Anwendungsinstanzen selten unter diesem Wert liegt. Wenn nach dem Beenden einer WorkSpaces Applications-Sitzung die Gesamtzahl der WorkSpaces Applications-Instances den Wert für die Mindestkapazität unterschreitet, wird eine neue Flotteninstanz gestartet. Wie immer ist es wichtig, sich daran zu erinnern, dass eine WorkSpaces Anwendungsinstanz direkt einer Benutzersitzung zugeordnet ist, was sich direkt auf den Wert für Mindestkapazität auswirkt.

Die Eingabe eines Werts für Mindestkapazität, der über der erwarteten Parallelität liegt, führt zu höheren Kosten, obwohl die Benutzererfahrung dadurch nicht beeinträchtigt wird. Ein zu niedriger Wert führt zu niedrigen Kosten, beeinträchtigt jedoch die Benutzererfahrung, wenn die Gesamtzahl der Anfragen die verfügbare Kapazität übersteigt. Administratoren werden in einer solchen Situation die Fehlermeldung „Ungenügende Kapazität“ feststellen. Beispielsweise `AvailableCapacity` ist das Warten auf `PendingCapacity` Werden eine ineffiziente Nutzung der Zeit des Benutzers, wenn die Anzahl der zu erwartenden Verbindungen zu Beginn des Tages ein vorhersehbarer konsistenter Wert ist.

Beginnen Sie mit einer Mindestkapazität, die den typischen Randzeiten gerecht wird, und setzen Sie dann mithilfe der Richtlinie für die geplante Skalierung die Mindestkapazität vor Beginn des Arbeitstages effektiv zurück. Vergessen Sie nicht, eine weitere geplante Skalierungsrichtlinie zu erstellen, um die Mindestkapazität auf die Nebenzeiten zurückzusetzen. Weitere Informationen zu Skalierungsrichtlinien und deren Implementierung finden Sie im Abschnitt Strategien zur auto-scaling von Flotten in diesem Dokument.

Maximale Kapazität und Servicekontingenten

Die Festlegung der maximalen Kapazität mag wie ein willkürlicher Wert erscheinen, aber wenn sie richtig prognostiziert und festgelegt wird, werden dadurch der gesamte Ressourcenverbrauch und die Kosten optimiert. Ein eingegebener Wert, der höher ist als das Dienstkontingent für die WorkSpaces Anwendungsflotte in Ihrem, AWS-Konto kann als gültig erscheinen, aber wenn Auto Scaling-Ereignisse versuchen, Ressourcen auf die maximale Kapazität zu skalieren, können sie nicht gestartet werden, da der maximale Kapazitätswert das verfügbare Dienstkontingent überschreitet. Stellen Sie sicher, dass eine Service-Kontingentanfrage für die gewünschte maximale Kapazität gestellt wird, um sicherzustellen, dass die automatische Skalierung wie von Ihrem Unternehmen erwartet funktioniert.

Ein weiterer wichtiger Aspekt bei der Festlegung eines maximalen Kapazitätswerts sind die Kosten. Weitere Informationen finden Sie im Abschnitt Kostenoptimierung durch die Wahl des Flottentyps in diesem Dokument.

Desktopansicht oder Anwendungsansicht wählen

Die Entscheidung, sich für eine Anwendungs- oder Desktop-Ansicht zu entscheiden, hat keine Auswirkungen auf die Leistung oder die Kosten. Pro WorkSpaces Anwendungsflotte ist jeweils nur eine Ansicht verfügbar. Sie können die Option Stream-Ansicht ändern. Planen Sie diese Änderung außerhalb der Hauptverkehrszeiten ein, da für die Änderung der Stream-Ansicht ein Neustart der Flotte erforderlich ist.

Es gibt kein einheitliches bewährtes Verfahren für die Stream-Ansicht. Die Auswirkungen der Stream-View-Optionen lassen sich wie folgt zusammenfassen:

- Detaillierte Berichte zur Anwendungsnutzung mithilfe der Funktion „Nutzungsberichte“ für Administratoren
- Gesamterfahrung und Arbeitsablauf für Endbenutzer (entspricht beispielsweise ein vollwertiger Desktop den Anforderungen des Anwendungsfalls oder reicht es aus, nur die Anwendungen anzusehen?).

Desktop-Ansicht

In Anwendungsfällen, in denen der gesamte Arbeitsablauf des Benutzers in einer Sitzung ausgeführt wird, vereinfacht Desktop View die Benutzererfahrung, da sich alle Anwendungen in einer Umgebung konzentrieren. Desktop View kann bei Bereitstellungen von mehr als 3 bis 5 Anwendungen, die eine Integration in das Betriebssystem (OS) erfordern, eine konsistentere Benutzererfahrung bieten. Desktop View ist effektiv, wenn zwei separate und unterschiedliche Umgebungen verwaltet werden. Ein Benutzer kann beispielsweise gleichzeitig auf eine Produktions- und eine Vorproduktions-Desktop-Umgebung zugreifen, um Änderungen an Layout, Konfiguration und Anwendungszugriff zu überprüfen.

WorkSpaces Applications Usage Reports erstellt täglich einen Anwendungsbericht für Desktop View. Die resultierende Ausgabe für die Anwendung ist einfach „Desktop“ und wird direkt der WorkSpaces Anwendungssitzung zugeordnet. Weitere Informationen finden Sie im Abschnitt Überwachung der Benutzernutzung in diesem Dokument.

Nur Anwendungen anzeigen

Die Ansicht „Nur Anwendungen“ ist auch dann wirksam, wenn der WorkSpaces Anwendungsstapel einige Anwendungen bereitstellen soll, die zeitweise benötigt werden. In Kioskumgebungen erfolgt

eine sichere Bereitstellung von Anwendungen über Application View. Mit Application View ersetzt WorkSpaces Applications die standardmäßige Windows-Shell durch eine benutzerdefinierte Shell. Diese benutzerdefinierte Shell präsentiert nur laufende Anwendungen, wodurch die Angriffsfläche des Betriebssystems minimiert wird.

Für Anwendungsfälle, in denen WorkSpaces Anwendungen verwendet werden, um die Desktop-Umgebung eines bestehenden Unternehmens zu erweitern, wird die Ansicht Nur Anwendungen bevorzugt. Stellen Sie den Windows-Client für WorkSpaces Anwendungen im systemeigenen Anwendungsmodus bereit, um Verwirrung bei den Benutzern zu vermeiden, indem Sie die vollständige Verwendung von Tastenkombinationen ermöglichen.

Amazon WorkSpaces Applications Usage Reports erstellt täglich einen Anwendungsbericht für die Anwendungsansicht. Für detailliertere Berichte über die Nutzung von Anwendungen und Laufwerken sollten Sie eine Drittanbieterlösung für Berichte auf Betriebssystemebene in Betracht ziehen. Sie können Microsoft AppLocker im Berichtsmodus verwenden oder Lösungen in Betracht ziehen, die in der verfügbar sind AWS Marketplace, wie z. B. Stratusphere UX von Liquidware.

AWS Identity and Access Management Rollenkonfiguration

Wenn die Endbenutzer der WorkSpaces Anwendungen aufgrund eines Workloads innerhalb ihrer Sitzung auf andere AWS Dienste zugreifen müssen, empfiehlt es sich, den Zugriff mithilfe von AWS Identity and Access Management (IAM-) Rollen zu delegieren. Durch die Zuweisung auf Flottenebene können IAM-Rollen direkt mit der Sitzung Ihres Endbenutzers verknüpft werden. Weitere bewährte Methoden für die Verwendung von IAM-Rollen mit WorkSpaces Anwendungen finden Sie in diesem Abschnitt des Administratorhandbuchs.

Verwendung statischer Anmeldeinformationen

Bei einigen Workloads sind möglicherweise statische Eingaben für die IAM-Zugriffsschlüssel erforderlich, anstatt sie von der zugehörigen Rolle zu erben. Es gibt zwei Methoden, um diese Anmeldeinformationen zu erhalten. Die erste Methode besteht darin, die Zugriffsschlüssel innerhalb eines AWS Dienstes zu speichern und Ihren Endbenutzern dann expliziten IAM-Zugriff zu gewähren, um diesen bestimmten Wert aus dem Dienst abzurufen. Zwei Beispiele für Speichermechanismen, die für die Speicherung von Zugriffsschlüsseln verwendet werden AWS Secrets Manager, sind AWS SSM Parameter Store. Die zweite Methode besteht darin, den Anmeldeinformationsanbieter WorkSpaces für Anwendungen zu verwenden, um auf die Zugriffsschlüssel der angehängten Rolle zuzugreifen. Dazu rufen Sie den Credential Provider auf und analysieren die Ausgabe nach Ihrem Zugriffsschlüssel und Ihrem geheimen Schlüssel. Im Folgenden finden Sie ein Beispiel dafür, wie Sie diese Aktion ausführen können. PowerShell

```
$CMD = 'C:\Program Files\Amazon\Photon\PhotonRoleCredentialProvider
\PhotonRoleCredentialProvider.exe'
$role = 'Machine'

$output = & $CMD --role=$role
$parsed = $output | ConvertFrom-Json

$access_key = $parsed.AccessKeyId
$secret_key = $parsed.SecretAccessKey
$session_token = $parsed.SessionToken
```

Schützen Sie Ihren S3-Bucket für WorkSpaces Anwendungen

Wenn Ihr WorkSpaces Anwendungs-Workload mit Home Folder and/or Application Persistence konfiguriert ist, empfiehlt es sich, den Amazon S3 S3-Bucket, in dem die persistenten Daten gespeichert werden, vor unberechtigtem Zugriff oder versehentlichem Löschen zu schützen. Die erste Schutzebene besteht darin, eine Amazon S3 S3-Bucket-Richtlinie hinzuzufügen, um ein versehentliches Löschen des Buckets zu verhindern. Die zweite Schutzebene besteht darin, eine Bucket-Richtlinie hinzuzufügen, die dem Prinzip der geringsten Rechte entspricht. Die Einhaltung dieses Prinzips kann erreicht werden, indem nur den erforderlichen Parteien Zugriff auf den Bucket gewährt wird.

Strategien zur auto Skalierung von Flotten

WorkSpaces Anwendungsinstanzen verstehen

WorkSpaces Flotteninstanzen für Anwendungen haben ein Verhältnis von Benutzern zu Flotteninstanzen im Verhältnis 1:1. Das bedeutet, dass jeder Benutzer seine eigene Streaming-Instanz hat. Die Anzahl der Benutzer, die Sie gleichzeitig verbinden, bestimmt die Größe der Flotte.

Skalierungsrichtlinien

WorkSpaces Anwendungsflotten werden in einer Application Auto Scaling Group gestartet. Auf diese Weise kann die Flotte je nach Nutzung skaliert werden, um der Nachfrage gerecht zu werden. Wenn die Nutzung zunimmt, wird die Flotte skaliert, und wenn die Benutzer die Verbindung trennen, wird die Flotte wieder skaliert. Dies wird durch die Festlegung von Skalierungsrichtlinien gesteuert. Sie können Richtlinien für die zeitgesteuerte Skalierung, die schrittweise Skalierung und die Skalierung mit Zielverfolgung festlegen. Weitere Informationen zu diesen Skalierungsrichtlinien finden Sie unter Fleet Auto Scaling for Amazon WorkSpaces Applications.

Schrittweise Skalierung

Diese Richtlinien erhöhen oder verringern die Flottenkapazität um einen Prozentsatz der aktuellen Flottengröße oder um eine bestimmte Anzahl von Instances. Richtlinien zur schrittweisen Skalierung werden durch WorkSpaces CloudWatch Anwendungsmetriken von `Capacity UtilizationAvailable Capacity`, oder ausgelöst`Insufficient Capacity Errors`.

AWS Empfiehlt bei der Verwendung von Richtlinien für die schrittweise Skalierung, dass Sie einen Prozentsatz der Kapazität und nicht eine feste Anzahl von Instanzen hinzufügen. Dadurch wird sichergestellt, dass Ihre Skalierungsaktionen proportional zur Größe Ihrer Flotte sind. Auf diese Weise können Sie Situationen vermeiden, in denen Sie zu langsam skalieren (weil Sie im Verhältnis zu Ihrer Flottengröße eine geringe Anzahl von Instances hinzugefügt haben) oder zu viele Instances, wenn Ihre Flotte klein ist.

Zielverfolgung

Mit dieser Richtlinie wird ein Kapazitätsauslastungsgrad für die Flotte festgelegt. Application Autoscaling erstellt und verwaltet CloudWatch Alarme, die die Skalierungsrichtlinie auslösen.

Dadurch wird Kapazität hinzugefügt oder entfernt, um die Flotte auf oder nahe dem angegebenen Zielwert zu halten. Um die Anwendungsverfügbarkeit sicherzustellen, skaliert Ihre Flotte so schnell wie möglich proportional zur Metrik, skaliert aber schrittweise. Berücksichtigen Sie bei der Konfiguration der Zielverfolgung die Abklingzeit für die Skalierung, um sicherzustellen, dass Scale-Out und Scale-In in den gewünschten Intervallen erfolgen.

Die Zielverfolgung ist in Situationen mit hoher Kundenabwanderung effektiv. Von Kundenabwanderung spricht man, wenn eine große Anzahl von Benutzern innerhalb kurzer Zeit Sitzungen startet oder beendet. Sie können die Abwanderung erkennen, indem Sie die CloudWatch Kennzahlen für Ihre Flotte untersuchen. Zeiträume, in denen Ihre Flotte noch ausstehende Kapazität aufweist, ohne dass sich die gewünschte Kapazität (oder nur sehr geringfügig) ändert, deuten darauf hin, dass es wahrscheinlich zu einer hohen Abwanderung kommt. In Situationen mit hoher Abwanderung sollten Sie Richtlinien zur Zielverfolgung konfigurieren, bei denen (100 — Zielauslastung in Prozent) höher ist als die Abwanderungsrate in einem Zeitraum von 15 Minuten. Wenn beispielsweise 10% Ihrer Flotte aufgrund von Benutzerwechseln innerhalb von 15 Minuten eingestellt werden, legen Sie ein Kapazitätsauslastungsziel von 90% oder weniger fest, um die hohe Abwanderung auszugleichen.

Scheduled-based Skalierung

Diese Richtlinien ermöglichen es Ihnen, die gewünschte Flottenkapazität auf der Grundlage eines zeitbasierten Zeitplans festzulegen. Diese Richtlinie ist wirksam, wenn Sie das Anmeldeverhalten verstehen und Änderungen der Nachfrage vorhersagen können.

Zu Beginn des Arbeitstages könnten Sie beispielsweise erwarten, dass 100 Benutzer um 9:00 Uhr Streaming-Verbindungen anfordern. Sie können eine zeitgesteuerte Skalierungsrichtlinie so konfigurieren, dass die Mindestgröße der Flotte um 8:40 Uhr auf 100 festgelegt wird. Auf diese Weise können die Flotteninstanzen zu Beginn des Arbeitstages erstellt und verfügbar gemacht werden, und 100 Benutzer können gleichzeitig eine Verbindung herstellen. Sie können dann eine weitere geplante Richtlinie festlegen, um die Flotte um 17:00 Uhr auf mindestens zehn zu skalieren. Auf diese Weise können Sie Kosten sparen, da die Nachfrage nach Sitzungen außerhalb der Geschäftszeiten geringer ist als während des Arbeitstages.

Skalierung der Richtlinien in der Produktion

Sie können verschiedene Arten von Skalierungsrichtlinien in einer einzigen Flotte kombinieren, um präzise Skalierungsrichtlinien für Ihr Benutzerverhalten zu definieren. Im vorherigen Beispiel können Sie die geplante Skalierungsrichtlinie mit Richtlinien zur Zielverfolgung oder schrittweisen Skalierung kombinieren, um ein bestimmtes Auslastungsniveau aufrechtzuerhalten. Die Kombination

aus planmäßiger Skalierung und zielgerichteter Skalierung kann dazu beitragen, die Auswirkungen eines starken Anstiegs der Auslastung zu verringern, wenn Kapazität sofort benötigt wird.

Benutzer, die mit Streaming-Sitzungen verbunden sind, wenn eine Skalierungsrichtlinie die gewünschte Anzahl von Instanzen ändert, sind von einem Scale-In oder Scale-Out nicht betroffen. Durch Skalierungsrichtlinien werden bestehende Streaming-Sitzungen nicht beendet. Bestehende Sitzungen werden ohne Unterbrechung fortgesetzt, bis die Sitzung durch den Benutzer oder durch eine Flotten-Timeout-Richtlinie beendet wird.

Durch die Überwachung der WorkSpaces Anwendungsnutzung anhand von CloudWatch Messwerten können Sie Ihre Skalierungsrichtlinien im Laufe der Zeit optimieren. Beispielsweise kommt es häufig vor, dass bei der Ersteinrichtung zu viele Ressourcen bereitgestellt werden, und es kann zu langen Zeiträumen mit geringer Auslastung kommen. Wenn die Flotte nicht ausreichend ausgestattet ist, können Ihnen auch die Fehler „Hohe Kapazitätsauslastung“ und „Ungenügende Kapazität“ angezeigt werden. Die Überprüfung der CloudWatch Kennzahlen kann Ihnen dabei helfen, Anpassungen an Ihren Skalierungsrichtlinien vorzunehmen, um diese Fehler zu minimieren. Weitere Informationen und Beispiele für Richtlinien zur WorkSpaces Anwendungsskalierung, die Sie verwenden können, finden Sie unter Skalieren Sie Ihre Amazon WorkSpaces Applications-Flotten.

Bewährte Methoden für die Skalierung der Richtliniengestaltung

Kombinieren Sie Skalierungsrichtlinien

Viele Kunden entscheiden sich dafür, verschiedene Arten von Skalierungsrichtlinien in einer einzigen Flotte zu kombinieren, um die Leistung und Flexibilität von Auto Scaling in WorkSpaces Applications zu erhöhen. Sie könnten beispielsweise eine geplante Skalierungsrichtlinie so konfigurieren, dass Ihr Flottenminimum um 6:00 Uhr erhöht wird, damit die Benutzer ihren Arbeitstag beginnen, und das Flottenminimum um 16:00 Uhr verringert wird, bevor die Benutzer ihre Arbeit einstellen. Sie können diese geplante Skalierungsrichtlinie mit Richtlinien zur Zielverfolgung oder schrittweisen Skalierung kombinieren, um ein bestimmtes Auslastungsniveau aufrechtzuerhalten und während des Tages ein- oder auszuschalten, um die hohe Auslastung zu bewältigen. Die Kombination aus planmäßiger Skalierung und zielgerichteter Skalierung kann dazu beitragen, die Auswirkungen eines starken Anstiegs der Auslastung zu verringern, wenn Kapazität sofort benötigt wird.

Vermeiden Sie eine Abwanderung bei der Skalierung

Überlegen Sie, ob es in Ihrer Flotte aufgrund Ihres Anwendungsfalls zu einer hohen Fluktuation kommen könnte. Abwanderung tritt auf, wenn eine große Anzahl von Benutzern Sitzungen innerhalb eines kurzen Zeitraums startet und dann beendet. Dies kann der Fall sein, wenn viele Benutzer nur wenige Minuten lang gleichzeitig auf eine Anwendung in Ihrer Flotte zugreifen, bevor sie sich abmelden.

In solchen Situationen kann Ihre Flottengröße weit unter die gewünschte Kapazität fallen, da Instanzen beendet werden, wenn Benutzer ihre Sitzungen beenden. Durch Richtlinien zur schrittweisen Skalierung werden Instances möglicherweise nicht schnell genug hinzugefügt, um die Fluktuation auszugleichen. Infolgedessen bleibt Ihre Flotte bei einer bestimmten Größe hängen.

Sie können die Fluktuation erkennen, indem Sie die CloudWatch Kennzahlen für Ihre Flotte untersuchen. Zeiträume, in denen die ausstehende Kapazität Ihrer Flotte ungleich Null ist, ohne dass sich die gewünschte Kapazität (oder nur sehr geringfügig) ändert, deuten darauf hin, dass es wahrscheinlich zu einer hohen Abwanderung kommt. Um Situationen mit hoher Kundenabwanderung Rechnung zu tragen, verwenden Sie Skalierungsrichtlinien zur Zielverfolgung und wählen Sie eine Zielauslastung so aus, dass (100 — Zielauslastung in Prozent) höher ist als die Abwanderungsrate

in einem Zeitraum von 15 Minuten. Wenn beispielsweise 10% Ihrer Flotte innerhalb von 15 Minuten aufgrund von Benutzerfluktuation eingestellt werden, legen Sie ein Kapazitätsauslastungsziel von 90% oder weniger fest, um eine hohe Abwanderung auszugleichen.

Machen Sie sich mit der maximalen Bereitstellungsrate vertraut

Kunden, die WorkSpaces Anwendungsflotten für eine große Anzahl von Benutzern verwalten, sollten Beschränkungen der Bereitstellungsrate in Betracht ziehen. Dieses Limit wirkt sich darauf aus, wie schnell Instances zu einer Flotte oder zu allen Flotten innerhalb einer Flotte hinzugefügt werden können. AWS-Konto

Es gibt zwei Grenzwerte, die berücksichtigt werden müssen:

- Für eine einzelne Flotte bietet WorkSpaces Applications eine maximale Rate von 20 Instanzen pro Minute.
- Für eine einzelne AWS-Konto Instanz WorkSpaces stellt Applications eine Geschwindigkeit von 60 Instanzen pro Minute bereit (mit einem Burst von 100 Instanzen pro Minute).

Wenn mehr als drei Flotten parallel hochskaliert werden, wird das Ratenlimit für die Kontobereitstellung von allen Flotten gemeinsam genutzt (z. B. könnten sechs Flotten, die parallel skalieren, jeweils bis zu 10 Instanzen pro Minute bereitstellen). Berücksichtigen Sie außerdem, wie viel Zeit eine bestimmte Streaming-Instanz benötigt, um die Bereitstellung als Reaktion auf ein Skalierungsereignis abzuschließen. Bei Flotten, die keiner Active Directory-Domäne angehören, sind dies in der Regel 15 Minuten. Bei Flotten, die einer Active Directory-Domäne angehören, kann dies bis zu 25 Minuten dauern.

Betrachten Sie angesichts dieser Einschränkungen die folgenden Beispiele:

- Wenn Sie eine einzelne Flotte von 0 auf 1000 Instances skalieren möchten, dauert es 50 Minuten (1000 instances/20 Instanzen pro Minute), bis die Bereitstellung abgeschlossen ist, und dann weitere 15-25 Minuten, bis alle Instances für Endbenutzer verfügbar sind, was insgesamt 65 bis 75 Minuten entspricht.
- Wenn Sie drei Flotten gleichzeitig von 0 auf 333 Instances skalieren möchten (für insgesamt 999 Instances in der AWS-Konto), dauert es etwa 17 Minuten (999/60Instanzen pro Minute), bis alle Flotten die Bereitstellung abgeschlossen haben, und dann weitere 15 Minuten, bis diese Instances für Endbenutzer verfügbar sind, also insgesamt 32-42 Minuten.

Nutzen Sie mehrere Availability Zones

Wählen Sie mehrere AZs in der Region für Ihren Flotteneinsatz. Wenn Sie mehrere AZs für Ihre Flotte auswählen, erhöhen Sie die Wahrscheinlichkeit, dass Ihre Flotte als Reaktion auf ein Skalierungsereignis Instances hinzufügen kann. Die CloudWatch Metrik PendingCapacity ist ein Ausgangspunkt, um zu beurteilen, wie optimiert das Flotten-AZ-Design bei großen Flotteneinsätzen ist. Ein hoher, anhaltender Wert für PendingCapacity kann darauf hindeuten, dass die horizontale Skalierung (über AZs hinweg) ausgeweitet werden muss. Weitere Informationen finden Sie unter Monitoring Amazon WorkSpaces Applications Resources.

Wenn Auto Scaling beispielsweise versucht, Instances bereitzustellen, um die Größe Ihrer Flotte zu erhöhen, und die ausgewählte AZ nicht über ausreichende Kapazität verfügt, fügt Auto Scaling stattdessen Instances in den anderen AZs hinzu, die Sie für Ihre Flotte angegeben haben. Weitere Informationen zu Availability Zones und WorkSpaces Anwendungsdesign finden Sie unter Availability Zones in diesem Dokument.

Überwachen Sie Metriken zu Fehlern bei unzureichender

„Fehler bei unzureichender Kapazität“ ist eine CloudWatch Kennzahl für WorkSpaces Anwendungsflotten. Diese Metrik gibt die Anzahl der Sitzungsanfragen an, die aufgrund mangelnder Kapazität abgelehnt wurden.

Wenn Sie Änderungen an Ihren Skalierungsrichtlinien vornehmen, ist es hilfreich, einen CloudWatch Alarm einzurichten, der Sie benachrichtigt, wenn Fehler mit unzureichender Kapazität auftreten. Auf diese Weise können Sie Ihre Skalierungsrichtlinien schnell anpassen, um die Verfügbarkeit für Benutzer zu optimieren. Das Administratorhandbuch enthält detaillierte Schritte zur Überwachung Ihrer WorkSpaces Anwendungsressourcen.

Verbindungsmethoden

Beim Streamen von Sitzungen in WorkSpaces Anwendungen stehen Benutzern zwei Verbindungsmethoden zur Verfügung:

- Webbrowser-Zugriff — Jeder HTML5-capable Browser wird unterstützt. Es sind keine Plug-ins oder Downloads erforderlich.
- WorkSpaces Anwendungen: Windows-Client

Als bewährte Methode sollten Sie die Funktionen und Geräteanforderungen für den Anwendungsfall Ihres Benutzers berücksichtigen, um herauszufinden, welcher Browser oder welches Gerät seine Anforderungen am besten unterstützt.

> **Note**
>
> WorkSpaces Anwendungen werden auf Geräten mit Bildschirmauflösungen von weniger als 1024 x 768 Pixeln nicht unterstützt.

Zusammenfassung, Funktion und Geräteunterstützung

Tabelle 3 — Zusammenfassung der Funktionen und der Geräteunterstützung

	Zugriff über einen Webbrowser	WorkSpaces Anwendungen Windows Client
Mehrere Monitore (bis zu 2.000 Auflösung)	Unterstützt	Unterstützt
Mehrere Monitore (Auflösung bis zu 4K)	N/A	Unterstützt
Unterstützung für Zeichentablets	Unterstützt*	Unterstützt
Unterstützung für Touchscreen-Geräte	Unterstützt	N/A

	Zugriff über einen Webbrowser	WorkSpaces Anwendungen Windows Client
Unterstützung für USB-Passthrough-Geräte	N/A	Unterstützt
Tastenkombination	Unterstützt	Unterstützt
Relativer Maus-Offset	Unterstützt	Unterstützt
Übertragung von Dateien	Unterstützt	Unterstützt
Umleitung des lokalen Druckers	N/A	Unterstützt
Lokale Laufwerksumleitung	N/A	Unterstützt
Web-cam Unterstützung	Unterstützt	Unterstützt

*Nur Google Chrome und Mozilla Firefox

Zugriff über einen Webbrowser

WorkSpaces Der Zugriff auf Anwendungen über den Webbrowser ermöglicht den Zugriff auf Anwendungen, ohne dass ein spezieller Client installiert werden muss. Benutzer können mit einem unterstützten HTML5-capable Browser eine Verbindung herstellen. Es ist kein Browser-Plugin oder eine Browsererweiterung erforderlich.

Der Webbrowser-Zugriff bietet eine große Auswahl an Betriebssystemen und Typen für Endgeräte.

WorkSpaces Anwendungsclient für Windows

Der WorkSpaces Anwendungsclient für Windows ist eine Anwendung, die Sie auf Ihrem Windows-PC installieren. Diese Anwendung bietet zusätzliche Funktionen, die nicht verfügbar sind, wenn Sie über einen Webbrowser auf WorkSpaces Anwendungen zugreifen. Mit dem WorkSpaces Applications Client können Sie beispielsweise Folgendes tun:

- Verwenden Sie mehr als zwei Monitore oder eine Auflösung von 4K

- Verwenden Sie Ihre USB-Geräte mit Anwendungen, die über Anwendungen gestreamt werden WorkSpaces
- Greifen Sie während Ihrer Streaming-Sitzungen auf Ihre lokalen Laufwerke und Ordner zu
- Leiten Sie Druckaufträge von Ihrer Streaming-Anwendung an einen Drucker weiter, der an Ihren lokalen Computer angeschlossen ist
- Verwenden Sie Ihre lokale Webcam für Video- und Audiokonferenzen innerhalb Ihrer Streaming-Sitzungen
- Verwenden Sie Tastenkombinationen in den Anwendungen, auf die Sie während Ihrer Streaming-Sitzungen zugreifen
- Interagieren Sie mit Ihren Remote-Streaming-Anwendungen auf die gleiche Weise wie mit lokal installierten Anwendungen

WorkSpaces Verbindungsmodi für Anwendungen und Clients

Der WorkSpaces Anwendungsclient bietet zwei Verbindungsmodi: den systemeigenen Anwendungsmodus und den klassischen Modus. Der gewählte Verbindungsmodus bestimmt die Optionen, die Ihnen während des Anwendungs-Streamings zur Verfügung stehen sowie dessen Funktionsweise und Anzeige. Administratoren können die Fähigkeit der Benutzer steuern, zwischen dem systemeigenen Anwendungsmodus und dem klassischen Modus zu wechseln.

- Im klassischen Modus werden Anwendungen im Fenster der WorkSpaces Anwendungssitzung gestreamt. Dies ähnelt der Art und Weise, wie Endbenutzer Anwendungen in einem Webbrowser streamen. Verwenden Sie den klassischen Modus, wenn Endbenutzer es vorziehen, Anwendungen auf die gleiche Weise wie Browser zu streamen und dabei zusätzliche Funktionen wie die Verbindung zur lokalen Datei- und Druckerumleitung zu nutzen. Der klassische Modus ist der empfohlene Standardverbindungsmodus. Der klassische Modus ist der einzige Modus, der für Desktop View unterstützt wird.
- Der native Anwendungsmodus ermöglicht es Endbenutzern, mit Remote-Streaming-Anwendungen auf ähnliche Weise zu arbeiten wie mit anderen lokal installierten Anwendungen. Wenn Endbenutzer es gewohnt sind, mit lokal installierten Anwendungen zu arbeiten, bietet der native Anwendungsmodus ein nahtloses Benutzererlebnis. Die Remote-Streaming-Anwendung funktioniert fast genauso wie eine lokal installierte Anwendung. Das Anwendungssymbol wird in der Taskleiste Ihres lokalen PCs angezeigt, genau wie die Symbole für Ihre lokalen Anwendungen. Im Gegensatz zu den Symbolen für Ihre lokalen Anwendungen enthalten die Symbole für Ihre Streaming-Anwendungen im nativen Anwendungsmodus das WorkSpaces Anwendungslogo. Der native Anwendungsmodus ist der empfohlene Verbindungsmodus, wenn Benutzer

Tastenkombinationen für Anwendungen verwenden und mithilfe von Tastenkombinationen problemlos zwischen einzelnen lokalen und einzelnen Remoteanwendungen wechseln möchten.

Bereitstellung und Verwaltung von Clients

Benutzer können den WorkSpaces Applications Client selbst installieren, oder Administratoren können den WorkSpaces Applications Client für sie installieren, indem sie PowerShell Skripts remote ausführen oder den WorkSpaces Applications Client mit benutzerdefinierten Einstellungen neu verpacken.

Sie müssen USB-Geräte qualifizieren, die Ihre Benutzer für ihre Streaming-Sitzung verwenden können sollen. Wenn ihr USB-Gerät nicht qualifiziert ist, wird es von WorkSpaces Anwendungen nicht erkannt und kann nicht für die Sitzung freigegeben werden. Nachdem ihre Geräte qualifiziert wurden, müssen Ihre Benutzer die Geräte jedes Mal, wenn sie eine neue Streaming-Sitzung starten, für WorkSpaces Anwendungen freigeben.

AWS Empfiehlt die Verwendung des Enterprise Deployment Tools, wenn der WorkSpaces Applications Client in großem Umfang bereitgestellt wird. Das Enterprise Deployment Tool umfasst die Installationsdateien WorkSpaces für den Applicationsclient und eine administrative Gruppenrichtlinienvorlage.

Benutzerdefinierte Domänen

Bei der programmgesteuerten Bereitstellung von WorkSpaces Anwendungen ist es möglich, eine benutzerdefinierte Domäne zu erstellen, die Benutzern eine vertraute Erfahrung bei Streaming-Sitzungen bietet. Bei SAML 2.0-IdP-Bereitstellungen von WorkSpaces Anwendungen ist es wichtig zu betonen, dass der Benutzerzugriff beim IdP beginnt, nicht bei Anwendungen. WorkSpaces Benutzer benötigen keine WorkSpaces Anwendungs-URLs, da diese nach der Authentifizierung vom IdP bereitgestellt werden. Daher sind benutzerdefinierte Domainnamen für SAML 2.0-IdP-Bereitstellungen nicht erforderlich.

Authentifizierung

Bei WorkSpaces Applications kann die Authentifizierung entweder außerhalb von Amazon WorkSpaces Applications oder als Teil des WorkSpaces Applications-Service erfolgen. Die Entscheidung, wie die Authentifizierung für Ihre WorkSpaces Anwendungsbereitstellung erfolgen soll, ist eine grundlegende Überlegung Ihres Entwurfs. Es ist nicht ungewöhnlich, dass ein Unternehmen mehrere WorkSpaces Anwendungen für unterschiedliche Anwendungsfälle bereitstellt. Jeder Anwendungsfall kann eine andere Authentifizierungsmethode haben.

Es gibt drei Arten von Authentifizierungsmethoden für WorkSpaces Anwendungen:

- SAML 2.0
- Benutzerpool
- Programmatisch

Bestimmung der optimierten Methode

Amazon WorkSpaces Applications ist so konzipiert, dass es flexibel ist und die meisten organisatorischen Designanforderungen erfüllt. Bei der Festlegung der optimierten Authentifizierungsmethode empfiehlt es sich, die Ziele und Zwecke der Nutzer des Services sowie die Unternehmensrichtlinien und -verfahren zu berücksichtigen.

Im Folgenden finden Sie einige Beispiele für die Kombination von Anwendungsfällen mit organisatorischen Zielen.

Tabelle 4 — Anwendungsfälle mit organisatorischen Zielen

Beispiel	Beschreibung	Authentifizierung
In eine Domäne eingebundene Flotteninstanzen sind erforderlich	Auf Anwendungen, die auf dem WorkSpaces Anwendungs-Image installiert sind, können nur Ressourcen zugreifen, die einer Domäne angehören.	SAML 2.0
Starke Integration mit Microsoft-Diensten	Organisatorische Abhängigkeit von der Entwicklung Microsoft	SAML 2.0

Beispiel	Beschreibung	Authentifizierung
	Microsoft-Gruppenrichtlinien und der Backend-Infrastruktur	
Bestehendes Single Sign-on (SSO) für Unternehmen	Alle neuen Dienste müssen eine SSO-Lösung für Unternehmen nutzen, für die mehrere Berichts- und Sicherheitsprozesse eingerich tet wurden.	SAML 2.0
Smartcard-Unterstützung für Anwendungen	Smartcards (wie Private Identity Verification und Common Access Cards) für die Sitzungsauthentifizierung bei gestreamten Anwendung en über ein Smartcard-Lesegerät.	SAML 2.0
Saisonarbeitskräfte mit Zeitarbeitskräften	Wenige Monate im Jahr erhalten Zeitarbeitskräfte eine kleine Anzahl von Bewerbungen, die keine internen Ressourcen für die Durchführung der Aktivitäten enthalten.	Benutzerpool
Eingeschränkter IT-Support	Kleinere Unternehmen mit weniger als 50 Benutzern und begrenztem IT-Personal, die den Aufwand für die Wartung eines Identity Providers (IdP) verringern möchten	Benutzerpool

Beispiel	Beschreibung	Authentifizierung
Unabhängiger Softwarea nbieter (ISV)	Proprietäre Lösung, die von Ihrem Unternehmen entwickelt wurde und Benutzerberechtigu ngen und Authentifizierung umfasst und WorkSpaces Anwendungen als Teil Ihrer Lösung erweitert. *	Programmatisch
Technologisches Schaufenster	Vollständig kurzlebige Umgebung, in der eine proprietäre Technologie im Rahmen einer Führung durch Ihre Lösung vorgestellt wird, ohne dass Benutzerinformatio nen gespeichert werden müssen.	Programmatisch
Interaktives Website-Erlebnis	Machen Sie Ihre Website interaktiv mit Streaming-Windows-Anwendungen. **	Programmatisch

*Weitere Informationen erhalten Sie bei den Softwareanbietern: Stellen Sie Ihre Anwendungen auf jedem beliebigen Benutzergerät bereit.

**Weitere Informationen finden Sie unter Streaming-Sitzungen für WorkSpaces Anwendungen einbetten.

Wenn Ihr Unternehmen über einen Anwendungsfall oder eine Richtlinie verfügt, die in den zuvor genannten Beispielen nicht aufgeführt sind, empfiehlt es sich, den gewünschten Endstatus der Workflow-Nutzung von WorkSpaces Anwendungen vorherzusagen, um sicherzustellen, dass die Authentifizierungslösung nicht damit in Konflikt gerät.

Konfiguration Ihres Identitätsanbieters

SAML 2.0

Security Assertion Markup Language (SAML) 2.0 ist eine gängige Bereitstellungsoption, mit der Benutzer Ressourcen nutzen können. AWS Verschiedene SAML 2.0-Identitätsanbieter von Drittanbietern unterstützen Anwendungen. WorkSpaces Unabhängig davon, ob Ihre WorkSpaces Anwendungsressourcen domänengebunden sind oder nicht, erfordert SAML 2.0 IdP, dass Sie IAM verwenden.

Da die meisten eine eindeutige metadata.xml mit spezifischen SAML-Attributen für jede SAML-Anwendung IdPs generieren, benötigt jeder WorkSpaces Anwendungsstapel eine Rolle, die eine vertrauenswürdige Beziehung zum SAML-IdP hat, und eine Richtlinie, die über eine einzige Berechtigung für AppStream:Stream mit Bedingungen verfügt, die den Anforderungen des SAML-IdP und des ARN des Anwendungsstapels entsprechen. WorkSpaces

Das Handbuch zur WorkSpaces Anwendungsadministration enthält eine Beispielkonfiguration für das Design eines einzelnen Anwendungsstapels. WorkSpaces Informationen zu Bereitstellungen mit mehreren Stacks finden Sie in den optionalen Schritten zur Verwendung des SAML 2.0-Multi-Stack-Anwendungskatalogs.

Benutzerpool

Die Registerkarte „Benutzerpool“ in WorkSpaces Anwendungen ist eine gültige Option für kleine Machbarkeitsnachweise. Es hat sich bewährt, Benutzerpools für jeden Anwendungsfall und jede Organisation zu vermeiden, die WorkSpaces Anwendungen zur Bereitstellung von Produktionsanwendungen verwendet.

Ein wichtiger Punkt bei Benutzerpools ist, dass bei den E-Mail-Adressen von Benutzern Groß- und Kleinschreibung unterschieden wird. Daher ist es eine bewährte Methode, sicherzustellen, dass Benutzer in der korrekten Eingabe von Benutzeranmeldeinformationen geschult werden.

Streaming-URL

Bei Bereitstellungen, die WorkSpaces Anwendungsressourcen von einem zentralen Dienst (in der Regel ISVs) aufrufen, basiert die programmatische Authentifizierung darauf, dass eine Anwendung programmatische Aufrufe tätigt, AWS um Informationen dynamisch weiterzuleiten und eine WorkSpaces Anwendungssitzung für ihre Benutzer zu erstellen. Verwenden Sie die API-Authentifizierungsmethode (allgemein als „programmatisch“ bezeichnet), wenn Sie

Streaming-URLs mithilfe der URL-Operation erstellen. CreateStreaming Der Benutzer, der den `CreateStreamingURL` Anruf tätigt, muss einen gültigen Benutzer oder eine gültige Rolle mit der entsprechenden Berechtigung verwenden. `appstream:CreateStreamingURL`

Bei der Erstellung der Richtlinie für den programmatischen Zugriff hat es sich bewährt, den Zugriff zu sichern, indem im Abschnitt Ressourcen anstelle des Standardwerts '*' der genaue ARN für den WorkSpaces Anwendungsstapel angegeben wird. Beispiel:

Example

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appstream:createStreamingURL"
            ],
            "Resource": "arn:aws:appstream:us-east-1:031421429609:stack/
BestPracticesStack"
        }
    ]
}
```

> **Note**
>
> Sie können die ARNs Ihrer WorkSpaces Applications Stacks schnell abrufen, indem Sie die Describe Stacks API oder die AWS-CLI verwenden.

WorkSpaces Anwendungsinstanzen sollten als generische Instanzen beginnen. Mithilfe von Informationen, die ihr von der Anwendung übermittelt werden, richtet die WorkSpaces Anwendungsinstanz die Umgebung mithilfe des Sitzungskontextes ein, um die Dinge für den Benutzer dynamisch zu gestalten.

Lokale GPOs können zwar verwendet werden, um Einstellungen bei der Benutzeranmeldung festzulegen, aber der Sitzungskontext ist eine bewährte Methode`CreateStreamingURL`, wenn

wichtige Attribute wie Kunden-ID oder Datenbankverbindungseinstellungen verwendet und übergeben werden, die in der WorkSpaces Anwendungssitzung verwendet werden sollen.

Anspruch auf Anwendungen

WorkSpaces Anwendungen können den Anwendungskatalog, der Benutzern präsentiert wird, dynamisch erstellen. Anwendungsberechtigungen basieren auf SAML 2.0-Attributen oder mithilfe des WorkSpaces Applications Dynamic Application Framework.

Attribute-based Anwendungsberechtigungen mit SAML 2.0 werden in den meisten Szenarien empfohlen. Für die Verwaltung der Bereitstellung von Anwendungspaketen wird Dynamic Application Framework empfohlen.

Integration mit Microsoft Active Directory

Amazon WorkSpaces Applications Image Builders und Fleets können in Microsoft Active Directory integriert werden. Auf diese Weise können Sie eine zentralisierte Methode für die Benutzerauthentifizierung und -autorisierung bereitstellen und Active Directory-Gruppenrichtlinien auf domänengebundene WorkSpaces Applications-Instances anwenden. Die Verwendung von WorkSpaces Anwendungsflotten, die zu einer Domäne gehören, bietet dieselben administrativen Vorteile wie eine lokale Umgebung. Dazu gehört die zentrale Verwaltung von Netzwerkdateifreigaben, Benutzeranwendungsberechtigungen, Roaming-Profilen, Druckerzugriffen und anderen richtlinienbasierten Einstellungen.

Bei der Integration einer WorkSpaces Anwendungsumgebung mit Active Directory ist zu beachten, dass die anfängliche Authentifizierung für den WorkSpaces Anwendungsstapel weiterhin von einem SAML2.0 IdP verwaltet wird. Nachdem der Benutzer erfolgreich beim IdP authentifiziert wurde und eine Sitzung startet, muss er sein Domänenkennwort oder eine Smartcard-Authentifizierung für die Active Directory-Domäne eingeben.

Beim Entwerfen der Active Directory Domain Services (ADDS) -Umgebung, die mit WorkSpaces Anwendungen verwendet werden soll, stehen zwei Dienstoptionen und viele Bereitstellungsszenarien zur Verfügung. Stellen Sie außerdem sicher, dass das WorkSpaces Anwendungsnetzwerk mit Ihrem Besitzer der Active Directory-Standorttopologie besprochen wurde.

Dienstoptionen

Active Directory kann auch mithilfe von AWS Managed Microsoft Active Directory (AD) bereitgestellt werden. AWS Managed Microsoft AD ist ein vollständig verwalteter Dienst, mit dem Sie Microsoft Active Directory ausführen können. Microsoft Active Directory kann auch in einer selbst gehosteten Umgebung verwendet werden, die auf EC2 oder lokal ausgeführt wird.

Bereitstellungsszenarien

Die folgenden Bereitstellungsszenarien sind häufig verwendete und empfohlene Integrationsoptionen für WorkSpaces Anwendungen mit Microsoft Managed AD oder dem selbstverwalteten Active Directory eines Kunden. Alle unten aufgeführten Architekturdiagramme verwenden Kernkonstrukte von Amazon.

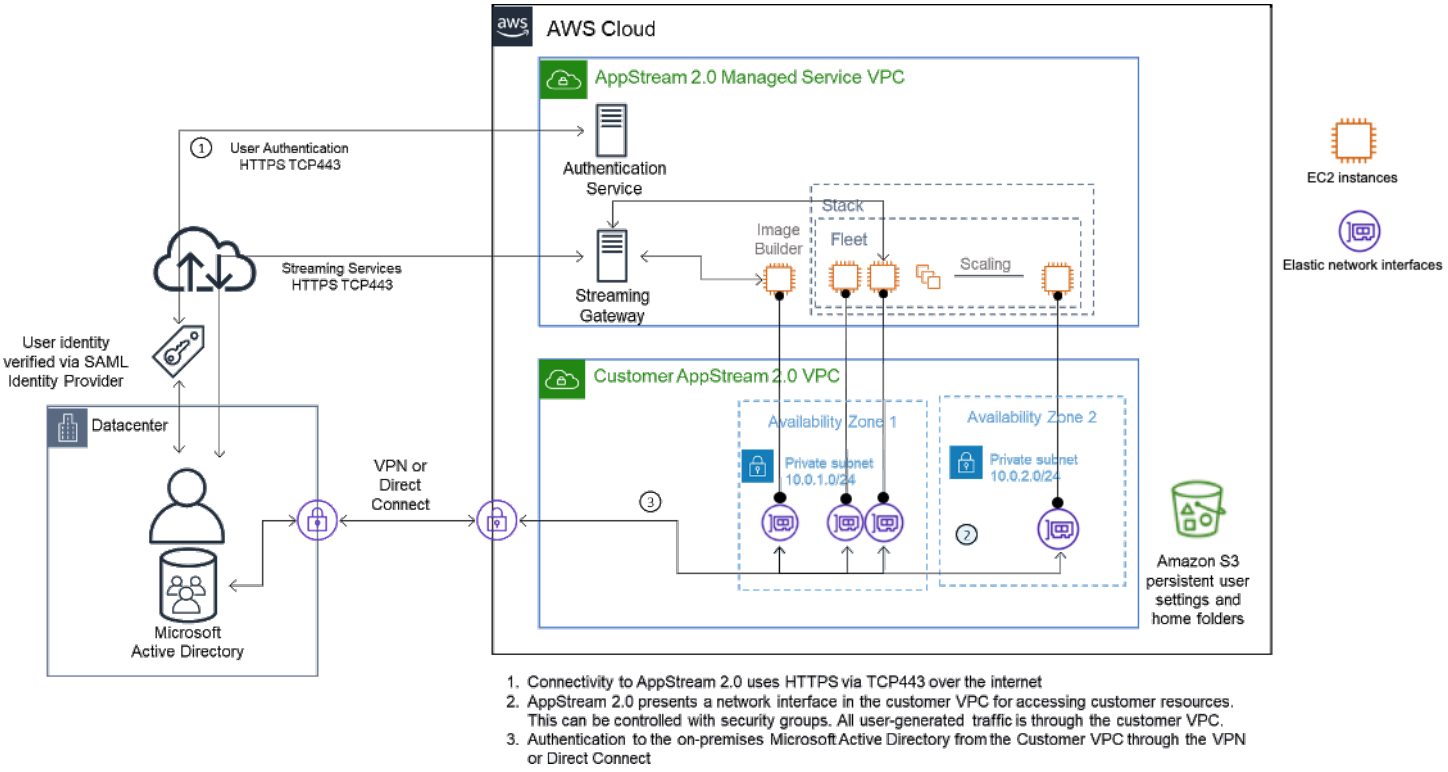
- Amazon Virtual Private Cloud (VPC) — Schaffung einer Amazon VPC für WorkSpaces Anwendungsdienste mit mindestens vier privaten Subnetzen, die auf vier AZs verteilt sind. Zwei der

privaten Subnetze werden für WorkSpaces Anwendungsflotten und Image Builders verwendet. Die verbleibenden zwei Subnetze werden für die Domänencontroller auf EC2 (oder Microsoft Managed AD) verwendet.

- DHCP-Optionssatz (Dynamic Host Configuration Protocol) — Stellt einen Standard für die Weitergabe von Konfigurationsinformationen an die WorkSpaces Anwendungsflotte und die Image Builder bereit, die in der VPC bereitgestellt werden. Der DHCP-Optionssatz wird auf VPC-Ebene definiert. Es ermöglicht Kunden, einen bestimmten Domainnamen und DNS-Einstellungen zu definieren, die bei der Bereitstellung mit den instanzierten WorkSpaces Anwendungen verwendet werden.
- AWS Verzeichnisdienste — Amazon Microsoft Managed AD kann in zwei privaten Subnetzen bereitgestellt werden, die in Verbindung mit WorkSpaces Anwendungs-Workloads verwendet werden.
- WorkSpaces Anwendungsflotten — Die WorkSpaces Anwendungsflotten oder Image Builders werden in der AWS verwalteten VPC gehostet. Jede WorkSpaces Anwendungsinstanz verfügt über zwei Elastic Network Interfaces (ENI). Die primäre Schnittstelle (`eth0`) wird für Verwaltungszwecke und für die Vermittlung der Endbenutzerverbindung zur Instance über das Streaming-Gateway verwendet. Die sekundäre Schnittstelle (`eth1`) wird in die Kunden-VPC eingefügt und kann für den Zugriff auf andere Ressourcen in der maßgeschneiderten VPC oder vor Ort verwendet werden.

Szenario 1: Active Directory-Domänendienste (ADDS) werden lokal bereitgestellt

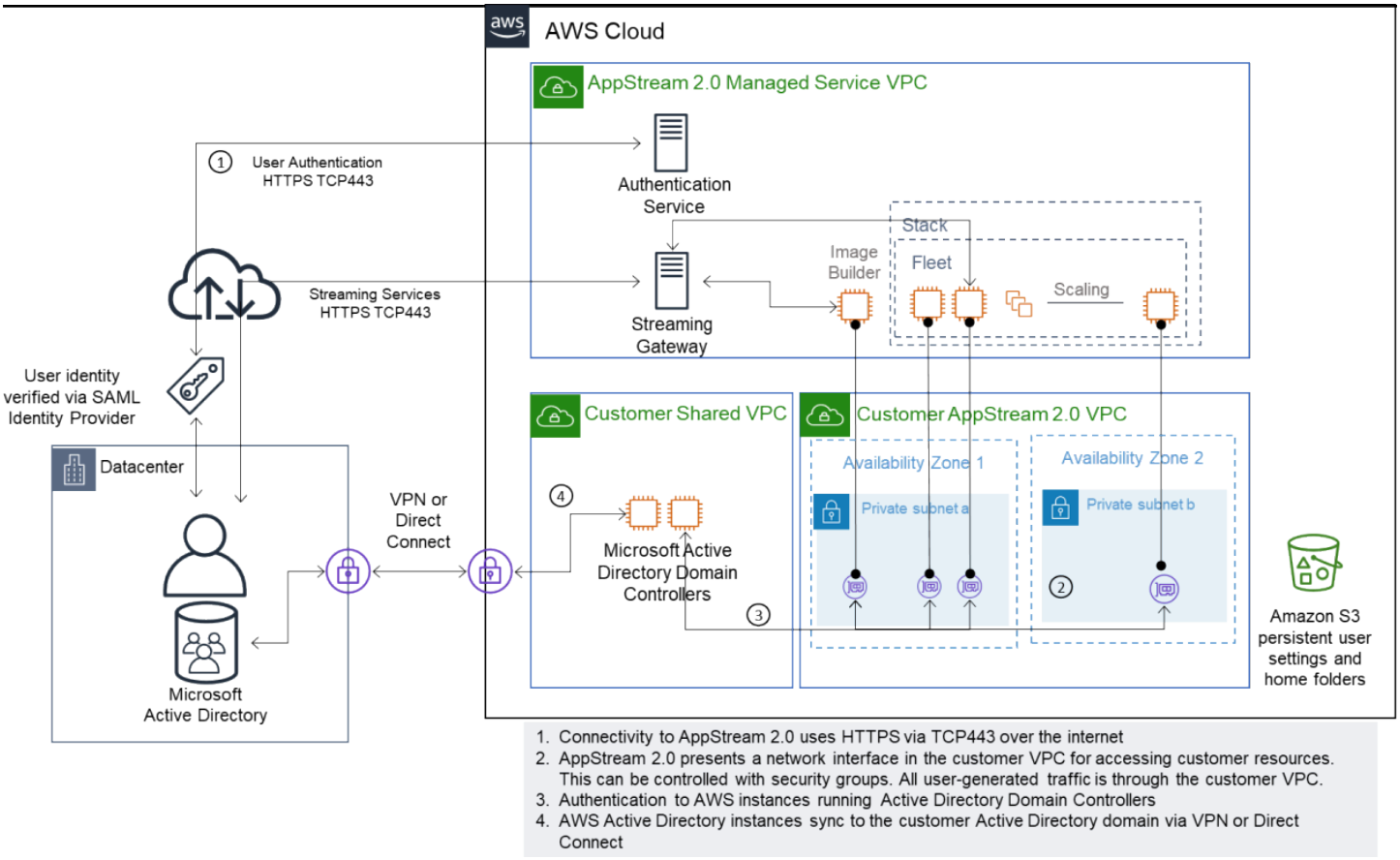
Der gesamte Authentifizierungsverkehr durchläuft die VPN- oder Direct Connect-Verbindung von der Kunden-VPC zum Kunden-Gateway. Der Vorteil dieses Szenarios besteht darin, dass eine möglicherweise bereits bereitgestellte AD-Umgebung verwendet wird, ohne dass zusätzliche Domänencontroller in der Kunden-VPC bereitgestellt werden müssen. Der Nachteil ist die alleinige Abhängigkeit von VPN oder Direct Connect, um Benutzer für die WorkSpaces Anwendungsflotte zu authentifizieren und zu autorisieren. Wenn es ein Problem mit der Netzwerkverbindung gibt, wären die WorkSpaces Applications Fleet oder Image Builders direkt betroffen. Die Bereitstellung von dualen VPN-Tunneln oder Direct Connect-Verbindungen mit unterschiedlichen Pfaden mindert dieses potenzielle Risiko.



Szenario 1 — Active Directory-Domänendienste (ADDS) werden lokal bereitgestellt

Szenario 2: Erweitern Sie Active Domain Services (ADDS) auf AWS Kunden-VPC

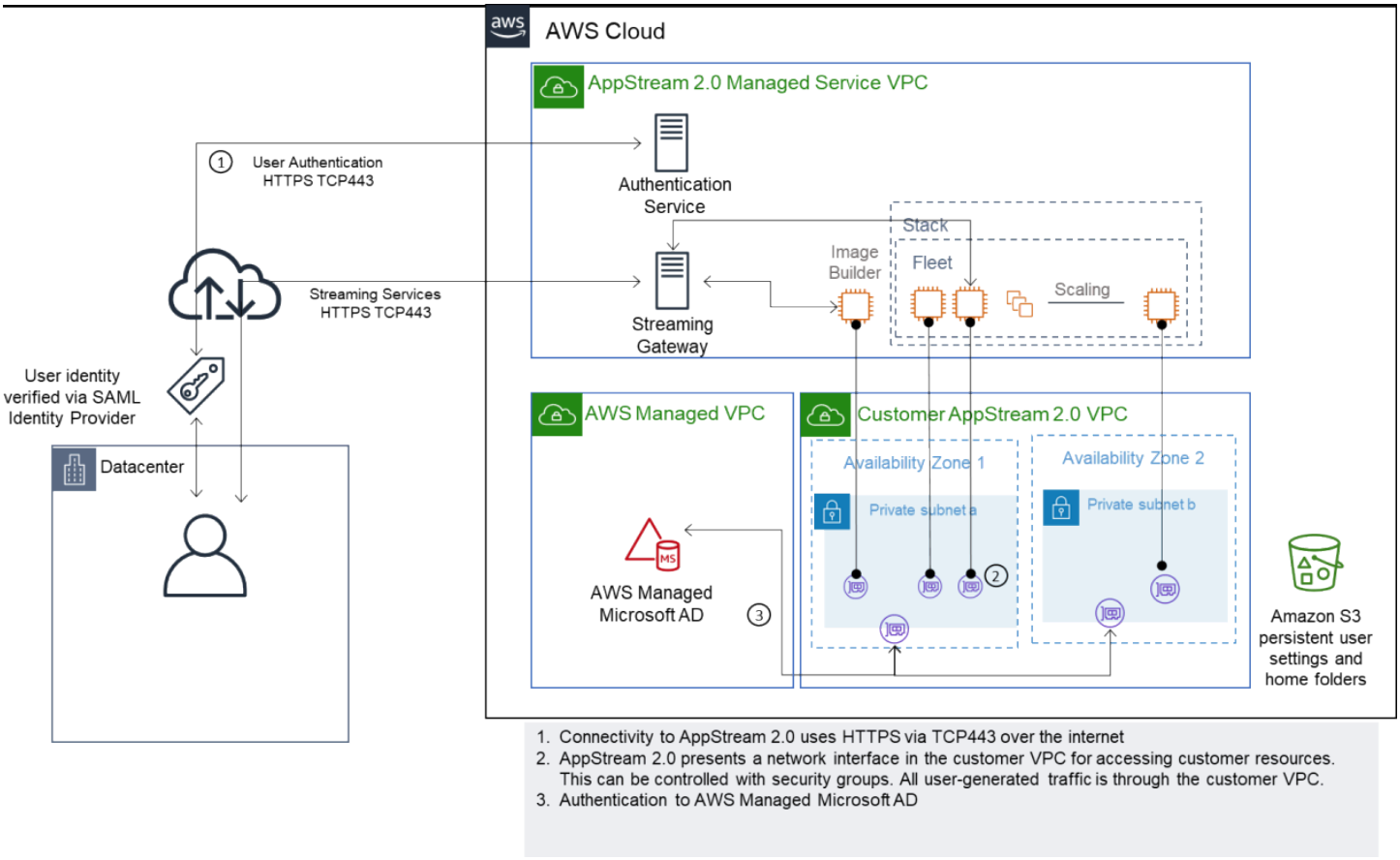
Das Active Directory wird auf Ihre Kunden-VPC erweitert. Ein Active Directory-Standort sollte für die neuen Domänencontroller in der Kunden-VPC erstellt werden. Der Authentifizierungsverkehr wird an die Domänencontroller in der AWS Kunden-VPC weitergeleitet, anstatt die VPN- oder Direct Connect-Verbindung zu durchqueren.



Szenario 2 — Erweitern Sie Active Domain Services auf die Virtual Private Cloud des AWS Kunden

Szenario 3: AWS Verwaltetes Microsoft Active Directory

AWS Managed Microsoft AD wird in der bereitgestellt AWS Cloud und als Identitäts- und Ressourcendomäne für die WorkSpaces Anwendungsflotten und Image Builders verwendet.



Szenario 3 — AWS Verwaltetes Active Directory

Standorttopologie Directory Service

Eine Standorttopologie des Active Directory-Dienstes ist eine logische Darstellung Ihres physischen Netzwerks.

Eine Standorttopologie hilft Ihnen dabei, Clientabfragen und Active Directory-Replikationsverkehr effizient weiterzuleiten. Eine gut konzipierte und gepflegte Standorttopologie hilft Ihrem Unternehmen, die folgenden Vorteile zu erzielen:

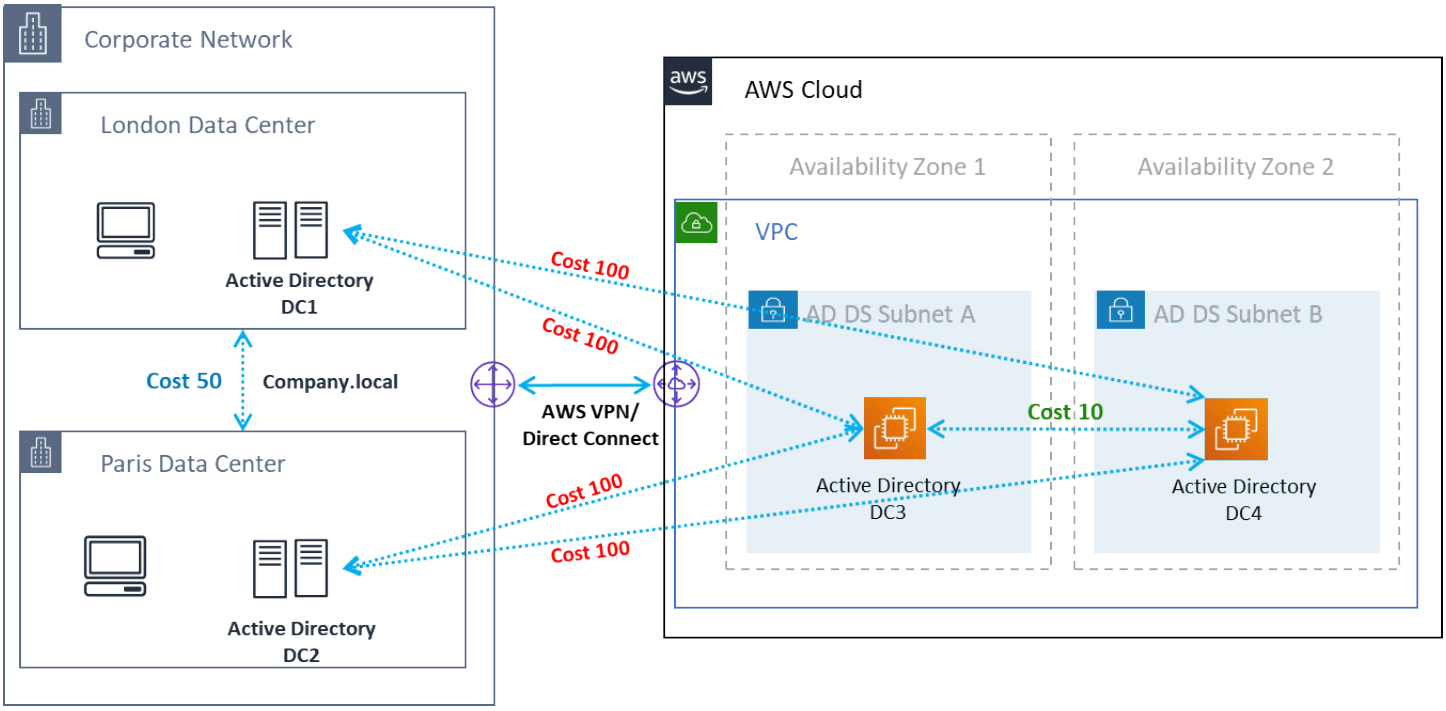
- Minimiert die Kosten für die Replikation von Active Directory-Daten bei der Synchronisation zwischen lokalen und. AWS Cloud
- Optimieren Sie die Fähigkeit von Client-Computern, die nächstgelegenen Ressourcen wie Domänencontroller zu finden. Dies trägt dazu bei, den Netzwerkverkehr über langsame WAN-Verbindungen (Wide Area Network) zu reduzieren, Anmelde- und Abmeldeprozesse zu verbessern und den Ressourcenzugriff zu beschleunigen.

Stellen Sie bei der Einführung von WorkSpaces Anwendungsdiensten sicher, dass die Adressbereiche, die für die Subnetze der WorkSpaces Anwendungsinstanzen verwendet werden, dem richtigen Standort für Ihre Umgebung zugewiesen sind.

In Szenario 1 und Szenario 2 sind Standorte und Dienste wichtige Komponenten für ein optimales Benutzererlebnis, was die Anmeldezeiten und die Zeit für den Zugriff auf Active Directory-Ressourcen angeht.

Die Active Directory-Replikation zwischen Domänencontrollern am Standort und über Standortgrenzen hinweg wird von der Standorttopologie bestimmt.

Durch die Definition der richtigen Standorttopologie wird die Clientaffinität gewährleistet, was bedeutet, dass Clients (in diesem Fall WorkSpaces Anwendungsstreaming-Instances) ihren bevorzugten lokalen Domänencontroller verwenden.



Active Directory-Standorte und -Dienste — Kundenaffinität

> **Tip**
>
> Es hat sich bewährt, hohe Kosten für Standortverknüpfungen zwischen lokalem AD DS und der AWS-Cloud zu definieren. Die obige Abbildung ist ein Beispiel dafür, welche Kosten Sie den Site-Links zuordnen sollten (Kosten 100), um eine standortunabhängige Kundenaffinität sicherzustellen.

Weitere Informationen zur Standorttopologie finden Sie unter Entwerfen der Standorttopologie.

Active Directory-Organisationseinheiten

AWS empfiehlt, die konfigurierten Organisationseinheiten (OUs) in einem einzigen WorkSpaces Applications Directory Config-Objekt zu speichern. Es hat sich bewährt, dass jeder WorkSpaces Anwendungsstapel über eine eigene Organisationseinheit verfügt. Dies bietet Ihnen die Flexibilität, spezifische GPOs pro Stack zu haben. Stellen Sie sicher, dass die Organisationseinheiten den Computerobjekten der WorkSpaces Anwendungen zugewiesen sind, um zu vermeiden, dass WorkSpaces Applications-specific Richtlinien mit lokalen Desktops vermischt werden. Erwägen Sie die Verwendung von Unter-OUs für jede Anwendung, in der AWS-Region Sie WorkSpaces Anwendungen bereitstellen.

Säuberung von Active Directory-Computerobjekten

WorkSpaces Anwendungsinstanzen sind kurzlebig. Eine Flotte erstellt Active Directory-Computerobjekte und verwendet sie wieder, während Flotten nach oben und unten skalieren.

AWS empfiehlt, einen AD-Bereinigungsprozess zu erstellen, um veraltete Active Directory-Computerobjekte zu löschen, die nach dem Entfernen einer WorkSpaces Anwendungsflotte noch vorhanden sein können.

Sicherheit

Cloud-Sicherheit genießt bei Amazon Web Services (AWS) höchste Priorität. Sicherheit und Compliance liegen in der gemeinsamen AWS Verantwortung des Kunden. Weitere Informationen finden Sie im Modell der geteilten Verantwortung. Als Kunde von AWS and WorkSpaces Applications ist es wichtig, Sicherheitsmaßnahmen auf verschiedenen Ebenen wie Stack, Flotte, Image und Netzwerk zu implementieren.

Da Applications kurzlebig ist, wird WorkSpaces Applications häufig als sichere Lösung für die Bereitstellung von Anwendungen und Desktops bevorzugt. Überlegen Sie, ob Antivirenlösungen, die in Windows-Bereitstellungen üblich sind, in Ihren Anwendungsfällen für eine Umgebung relevant sind, die vordefiniert ist und am Ende einer Benutzersitzung gelöscht wird. Virenschutz erhöht den Mehraufwand für virtualisierte Instanzen und ist daher eine bewährte Methode, um unnötige Aktivitäten zu vermeiden. Beispielsweise trägt das Scannen des Systemvolumes (das kurzlebig ist) beim Systemstart nicht zur allgemeinen Sicherheit von Anwendungen bei. WorkSpaces

Im Mittelpunkt der beiden wichtigsten Fragen für WorkSpaces Sicherheitsanwendungen stehen:

- Ist es erforderlich, den Benutzerstatus über die Sitzung hinaus beizubehalten?
- Wie viel Zugriff sollte ein Benutzer innerhalb einer Sitzung haben?

Sicherung persistenter Daten

Bei der Bereitstellung von WorkSpaces Anwendungen kann es erforderlich sein, dass der Benutzerstatus in irgendeiner Form beibehalten wird. Dabei kann es sich um die persistente Speicherung von Daten für einzelne Benutzer oder um die Beibehaltung von Daten für die Zusammenarbeit mithilfe eines gemeinsam genutzten Ordners handeln. WorkSpaces Der Instanzspeicher von Anwendungen ist kurzlebig und bietet keine Verschlüsselungsoption.

WorkSpaces Applications ermöglicht die Persistenz des Benutzerstatus über Basisordner und Anwendungseinstellungen in Amazon S3. In einigen Anwendungsfällen ist eine bessere Kontrolle über die Persistenz des Benutzerstatus erforderlich. AWS Empfiehlt für diese Anwendungsfälle die Verwendung einer SMB-Dateifreigabe (Server Message Block).

Benutzerstatus und Daten

Da die meisten Windows-Anwendungen am besten und sichersten funktionieren, wenn sie zusammen mit vom Benutzer erstellten Anwendungsdaten gespeichert werden, ist es eine

bewährte Methode, diese Daten in den WorkSpaces Anwendungsflotten zu speichern. AWS-Region Die Verschlüsselung dieser Daten ist eine bewährte Methode. Das Standardverhalten des Benutzer-Basisordners besteht darin, Dateien und Ordner im Ruhezustand mit S3-managed Amazon-Verschlüsselungsschlüsseln aus den AWS Schlüsselverwaltungsdiensten (AWS KMS) zu verschlüsseln. Es ist wichtig zu beachten, dass AWS Administratorbenutzer mit Zugriff auf die AWS Konsole oder den Amazon S3 S3-Bucket direkt auf diese Dateien zugreifen können.

Bei Designs, die ein SMB-Ziel (Server Message Block) von einer Windows-Dateifreigabe zum Speichern von Benutzerdateien und -ordnern erfordern, erfolgt der Vorgang entweder automatisch oder erfordert eine Konfiguration.

Tabelle 5 — Optionen für die Sicherung von Benutzerdaten

Ziel für kleine und mittlere Unternehmen	Encryption-at-rest	Encryption-in-transit	Virenschutz (AV)
FSx for Windows File Server	Automatisch über KMS AWS	Automatisch durch SMB-Verschlüsselung	AV, das auf einer Remote-Instanz installiert ist, führt einen Scan auf dem zugewiesenen Laufwerk durch
Datei-Gateway, AWS Storage Gateway	Standardmäßig werden alle AWS Storage Gateway in S3 gespeicherten Daten serverseitig mit Amazon S3-Manage d Encryption Keys (SSE-S3) verschlüs selt. Sie können optional verschied ene Gateway-T ypen konfigurieren, um gespeicherte Daten mit AWS Key Management Service	Alle Daten, die zwischen einer beliebigen Art von Gateway-Appliance und AWS Speicher übertragen werden, werden mit SSL verschlüsselt.	AV, das auf einer Remote-Instanz installiert ist, führt einen Scan auf dem zugewiesenen Laufwerk durch

Ziel für kleine und mittlere Unternehmen	Encryption-at-rest	Encryption-in-transit	Virenschutz (AV)
	(KMS) zu verschlüs seln		
EC2-based Windows-Dateiserver	Aktivieren Sie die EBS-Verschlüsselung	PowerShell; `Set-SmbServer Configuration - EncryptData $True`	Auf dem Server installiertes AV führt einen Scan auf lokalen Laufwerken durch

Endpunktsicherheit und Virenschutz

Die kurzlebige Natur von Amazon WorkSpaces Applications-Instances und die mangelnde Persistenz der Daten bedeuten, dass ein anderer Ansatz erforderlich ist, um sicherzustellen, dass das Benutzererlebnis und die Leistung nicht durch Aktivitäten beeinträchtigt werden, die auf einem persistenten Desktop erforderlich wären. Endpoint Security Agents werden in WorkSpaces Anwendungs-Images installiert, wenn es eine Unternehmensrichtlinie gibt oder wenn sie für den externen Datenzugriff verwendet werden, z. B. E-Mail, Dateizugriff, externes Surfen im Internet.

Entfernen eindeutiger Kennungen

Endpoint Security Agents verfügen möglicherweise über eine GUID (Global Unique Identifier), die bei der Erstellung der Flotteninstanz zurückgesetzt werden muss. Anbieter haben Anweisungen zur Installation ihrer Produkte in Images, die sicherstellen, dass für jede aus einem Image generierte Instanz eine neue GUID generiert wird.

Um sicherzustellen, dass die GUID nicht generiert wird, installieren Sie den Endpoint Security Agent als letzte Aktion, bevor Sie den WorkSpaces Anwendungsassistenten ausführen, um das Image zu generieren.

Leistungsoptimierung

Anbieter von Endpoint Security bieten Switches und Einstellungen an, mit denen die Leistung von WorkSpaces Anwendungen optimiert wird. Die Einstellungen variieren je nach Anbieter und sind in deren Dokumentation zu finden, in der Regel in einem Abschnitt über VDI. Zu den gängigen Einstellungen gehören, ohne darauf beschränkt zu sein, die folgenden:

- Schalten Sie die Startscans aus, um sicherzustellen, dass die Zeiten für die Erstellung, den Start und die Anmeldung von Instanzen minimiert werden
- Schalten Sie geplante Scans aus, um unnötige Scans zu verhindern
- Deaktivieren Sie Signatur-Caches, um die Dateiaufzählung zu verhindern
- Aktivieren Sie die für VDI optimierten I/O-Einstellungen
- Ausnahmen, die von Anwendungen zur Sicherstellung der Leistung erforderlich sind

Anbieter von Endpunktsicherheit stellen Anleitungen zur Verwendung mit virtuellen Desktop-Umgebungen zur Verfügung, die die Leistung optimieren.

- Trend Micro Office Scan-Unterstützung für die virtuelle Desktop-Infrastruktur — Apex One/ OfficeScan (trendmicro.com)
- CrowdStrike und wie installiert man den CrowdStrike Falcon im Rechenzentrum
- Sophos und Sophos Central Endpoint: So installieren Sie auf einem Gold-Image, um doppelte Identitäten zu vermeiden, und Sophos Central: Bewährte Methoden bei der Installation von Windows-Endpunkten in virtuellen Desktop-Umgebungen
- McAfee und Bereitstellung und Bereitstellung von McAfee Agenten auf Virtual Desktop Infrastructure-Systemen
- Microsoft Endpoint Security und Konfiguration von Microsoft Defender Antivirus für nicht persistente VDI-Maschinen - Microsoft Tech Community

Ausnahmen beim Scannen

Wenn Sicherheitssoftware in WorkSpaces Anwendungsinstanzen installiert ist, darf die Sicherheitssoftware die folgenden Prozesse nicht beeinträchtigen.

Tabelle 6 — WorkSpaces Anwendungsprozesse Sicherheitssoftware darf die folgenden Prozesse nicht beeinträchtigen.

Service	Prozesse
AmazonCloudWatchAgent	„C:\Program Dateien\ Amazon\AmazonCloud WatchAgent\ start-amazon- cloudwatch-agent.exe“

Service	Prozesse
AmazonSSMAgent	„C:\Program Dateien\ Amazon\ SSM\ amazon-ssm-agent.exe“
NICE DCV	„C:\Program Dateien\ NICE\ DCV\ Server\ bin \ dcvserver.exe“ "C:\Program Dateien\ NICE\ DCV\ Server\ bin\ dcvagent.exe“
WorkSpaces Anwendungen	„C:\ProgramFiles\ Amazon\ AppStream 2\StorageConnector\StorageConnector.exe“ Im Ordner "C:\Program Files\ Amazon\ Photon\“ “. \ Agent\PhotonAgent.exe“ “. \ Agent\ s5cmd.exe“ ".\WebServer\PhotonAgentWebServer.exe" ".\CustomShell\PhotonWindowsAppSwitcher.exe" ".\CustomShell\PhotonWindowsCustomShell.exe" ".\CustomShell\PhotonWindowsCustomShellBackground.exe"

Ordner

Wenn Sicherheitssoftware in WorkSpaces Anwendungsinstanzen installiert ist, darf die Software die folgenden Ordner nicht beeinträchtigen:

Example

```
C:\Program Files\Amazon\*
C:\ProgramData\Amazon\*
C:\Program Files (x86)\AWS Tools\*
```

```
C:\Program Files (x86)\AWS SDK for .NET\*
C:\Program Files\NICE\*
C:\ProgramData\NICE\*
C:\AppStream\*
C:\Program Files\Internet Explorer\*
C:\Program Files\nodejs\
```

Hygiene der Endpunktsicherheitskonsole

Amazon WorkSpaces Applications erstellt jedes Mal, wenn ein Benutzer nach Ablauf der Leerlauf- und Verbindungszeiten eine Verbindung herstellt, neue eindeutige Instances. Die Instances erhalten einen eindeutigen Namen und werden in Kondolen für das Endpoint Security Management gespeichert. Wenn Sie festlegen, dass ungenutzte, veraltete Maschinen gelöscht werden, die älter als 4 Tage oder mehr sind (oder weniger, je nach Zeitlimit für WorkSpaces Anwendungssitzungen), wird die Anzahl der abgelaufenen Instanzen in der Konsole minimiert.

Netzwerkausschlüsse

Der Netzwerkbereich für die WorkSpaces Anwendungsverwaltung (`198.19.0.0/16`) und die folgenden Ports und Adressen sollten nicht durch Sicherheits-/Firewall- oder Antivirenlösungen innerhalb von WorkSpaces Anwendungsinstanzen blockiert werden.

Tabelle 7 — Ports in WorkSpaces Anwendungs-Streaming-Instanzen darf Sicherheitssoftware nicht stören

Port	Usage
8300, 3128	Dies wird für den Aufbau der Streaming-Verbindung verwendet
8000	Dies wird für die Verwaltung der Streaming -Instanz von WorkSpaces Applications verwendet
8443	Dies wird für die Verwaltung der Streaming -Instanz von WorkSpaces Applications verwendet

Port	Usage
53	DNS

Tabelle 8 — WorkSpaces Anwendungen, verwaltete Serviceadressen, mit denen Sicherheitssoftware nicht interferieren darf

Port	Usage
169.254.169.123	NTP
169,254,169,249	NVIDIA GRID-Lizenzservice
169.254.169.250	KMS
169,254,169,251	KMS
169,254,169,253	DNS
169,254,169,254	Metadaten

Sicherung einer Anwendungssitzung WorkSpaces

Einschränkung der Anwendungs- und Betriebssystemkontrollen

WorkSpaces Mithilfe von Anwendungen kann der Administrator genau angeben, welche Anwendungen im Anwendungsstreaming-Modus von der Webseite aus gestartet werden können. Dies garantiert jedoch nicht, dass nur die angegebenen Anwendungen ausgeführt werden können.

Windows-Dienstprogramme und -Anwendungen können auf zusätzliche Weise über das Betriebssystem gestartet werden. AWS empfiehlt die Verwendung von Microsoft, AppLocker um sicherzustellen, dass nur die Anwendungen ausgeführt werden können, die Ihr Unternehmen benötigt. Die Standardregeln müssen geändert werden, da sie jedem Benutzer Pfadzugriff auf wichtige Systemverzeichnisse gewähren.

> **Note**
>
> Für Windows Server 2016 und 2019 muss der Windows Application Identity-Dienst ausgeführt werden, um AppLocker Regeln durchzusetzen. Der Anwendungszugriff über WorkSpaces Anwendungen, die Microsoft verwenden, AppLocker ist im WorkSpaces Applications Admin Guide detailliert beschrieben.

Verwenden Sie für Flotteninstanzen, die zu einer Active Directory-Domäne gehören, Gruppenrichtlinienobjekte (GPOs), um Benutzer- und Systemeinstellungen bereitzustellen, um den Anwendungs- und Ressourcenzugriff der Benutzer zu sichern.

Firewalls und Routing

Bei der Erstellung einer WorkSpaces Anwendungsflotte müssen Subnetze und eine Sicherheitsgruppe zugewiesen werden. Subnetzen sind bereits Netzwerkzugriffskontrolllisten (Network Access Control Lists, NACLs) und Routing-Tabellen zugewiesen. Sie können beim Starten eines neuen Image Builders oder beim Erstellen einer neuen Flotte bis zu fünf Sicherheitsgruppen zuordnen. Sicherheitsgruppen können bis zu fünf Zuweisungen aus den vorhandenen Sicherheitsgruppen erhalten. Für jede Sicherheitsgruppe fügen Sie Regeln hinzu, die den ausgehenden und eingehenden Netzwerkverkehr von und zu Ihren Instances steuern

Eine NACL ist eine optionale Sicherheitsebene für Ihre VPC, die als statuslose Firewall zur Steuerung des Datenverkehrs in und aus einem oder mehreren Subnetzen fungiert. Sie können Netzwerk-ACLs mit ähnlichen Regeln wie die für Sicherheitsgruppen einrichten, um Ihre VPC noch sicherer zu machen. Weitere Informationen zu den Unterschieden zwischen Sicherheitsgruppen und Netzwerk-ACLs finden Sie auf der Seite Sicherheitsgruppen und NACLs vergleichen.

Beachten Sie bei der Entwicklung und Anwendung von Sicherheitsgruppen- und NACL-Regeln die Well-Architected bewährten AWS-Methoden für geringste Rechte. Bei den geringsten Rechten handelt es sich um ein Prinzip, bei dem nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewährt werden.

Für Kunden, die über ein privates Hochgeschwindigkeitsnetzwerk verfügen, das ihre lokale Umgebung mit AWS (über AWS Direct Connect) verbindet, können Sie die Verwendung der VPC-Endpunkte für WorkSpaces Anwendungen in Betracht ziehen, was bedeutet, dass der Streaming-Verkehr über Ihre private Netzwerkverbindung geleitet wird und nicht über das öffentliche Internet. Weitere Informationen zu diesem Thema finden Sie im Abschnitt VPC-Endpunkt der WorkSpaces Anwendungsstreaming-Schnittstelle in diesem Dokument.

Verhinderung von Datenverlust

Wir werden uns zwei Arten der Verhinderung von Datenverlust ansehen.

Steuerelemente für die Datenübertragung zwischen Client und WorkSpaces Anwendungsinstanz

Tabelle 9 — Leitlinien für die Steuerung des Dateneingangs und -ausgangs

Einstellung	Optionen	Empfehlung
Zwischenablage	• Nur in die Remotesitzung kopieren und einfügen • Nur auf ein lokales Gerät kopieren • Disabled	Wenn Sie diese Einstellung deaktivieren, wird das Kopieren und Einfügen innerhalb der Sitzung nicht deaktiviert. Wenn das Kopieren von Daten in die Sitzung erforderlich ist, wählen Sie Nur in Remotesitzung einfügen, um das Risiko eines Datenverlusts zu minimieren.
Übertragung von Dateien	• Upload und Download • Nur hochladen • Nur herunterladen • Disabled	Vermeiden Sie es, diese Einstellung zu aktivieren, um Datenlecks zu verhindern.
Auf lokales Gerät drucken	• Enabled • Disabled	Wenn Drucken erforderlich ist, verwenden Sie Netzwerkdrucker, die von Ihrem Unternehmen gesteuert und überwacht werden.

Berücksichtigen Sie die Vorteile der bestehenden Datenübertragungslösung für Unternehmen gegenüber den Stack-Einstellungen. Diese Konfigurationen sind nicht als Ersatz für eine umfassende sichere Datenübertragungslösung konzipiert.

Steuern des ausgehenden Datenverkehrs von der WorkSpaces Anwendungsinstanz

Wenn Datenverlust ein Problem darstellt, ist es wichtig, zu vertuschen, worauf ein Benutzer zugreifen kann, sobald er sich in seiner WorkSpaces Anwendungsinstanz befindet. Wie sieht der Netzwerkausgangspfad (oder Ausgangspfad) aus? Es ist eine allgemeine Anforderung, dass dem Endbenutzer innerhalb seiner WorkSpaces Anwendungsinstanz ein öffentlicher Internetzugang zur Verfügung steht. Daher muss die Platzierung einer WebProxy oder einer Content-Filtering-Lösung im Netzwerkpfad in Betracht gezogen werden. Zu den weiteren Überlegungen gehören eine lokale Antiviren-Anwendung und andere Sicherheitsmaßnahmen für Endgeräte innerhalb der WorkSpaces Anwendungsinstanz (weitere Informationen finden Sie im Abschnitt „Endpunktsicherheit und Virenschutz“).

Verwenden AWS service

AWS Identity and Access Management

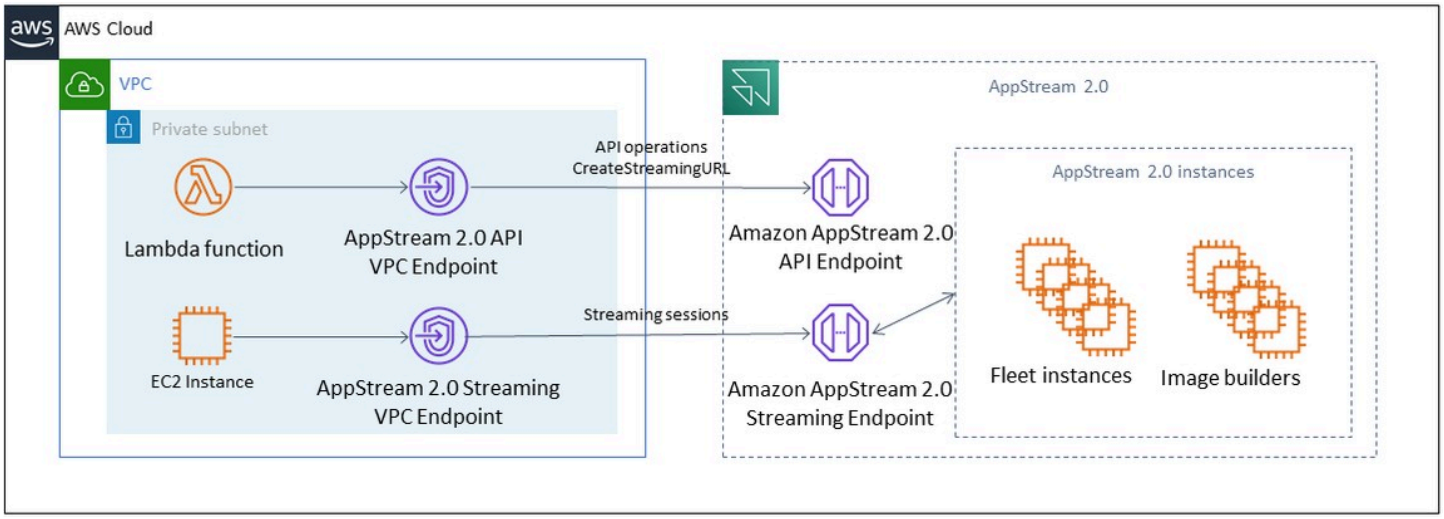
Es hat sich bewährt, eine IAM-Rolle für den Zugriff auf AWS Dienste zu verwenden und die damit verbundene IAM-Richtlinie genau festzulegen, sodass nur Benutzer in WorkSpaces Anwendungssitzungen Zugriff haben, ohne dass zusätzliche Anmeldeinformationen verwaltet werden müssen. Folgen Sie den bewährten Methoden für die Verwendung von IAM-Rollen mit Anwendungen. WorkSpaces

Erstellen Sie IAM-Richtlinien zum Schutz von Amazon S3 S3-Buckets, die erstellt wurden, um Benutzerdaten sowohl in Basisordnern als auch in Anwendungseinstellungen dauerhaft zu speichern. Dadurch wird der Zugriff durch Administratoren, die keine WorkSpaces Anwendungen sind, verhindert.

VPC-Endpunkte

Ein VPC-Endpunkt ermöglicht private Verbindungen zwischen Ihrer VPC und unterstützten AWS Diensten und VPC-Endpunktdiensten, die von bereitgestellt werden. AWS PrivateLink AWS PrivateLink ist eine Technologie, mit der Sie privat auf Dienste zugreifen können, indem Sie private IP-Adressen verwenden. Der Datenverkehr zwischen Ihrer VPC und dem anderen Service verlässt das Amazon-Netzwerk nicht. Wenn der öffentliche Internetzugang nur für AWS Dienste erforderlich ist, entfernen VPC-Endpunkte die Anforderung für NAT-Gateways und Internet-Gateways vollständig.

In Umgebungen, in denen Automatisierungsroutinen oder Entwickler API-Aufrufe für WorkSpaces Anwendungen benötigen, erstellen Sie einen VPC-Schnittstellen-Endpunkt für WorkSpaces Anwendungs-API-Operationen. Wenn es beispielsweise EC2-Instances in privaten Subnetzen ohne öffentlichen Internetzugang gibt, kann ein VPC-Endpunkt für WorkSpaces Applications API verwendet werden, um Anwendungs-API-Operationen wie WorkSpaces URL aufzurufen. CreateStreaming Das folgende Diagramm zeigt ein Beispiel-Setup, bei dem WorkSpaces Anwendungs-API und Streaming-VPC-Endpunkte von Lambda-Funktionen und EC2-Instances genutzt werden.



VPC-Endpunkt

Mit dem Streaming-VPC-Endpunkt können Sie Sitzungen über einen VPC-Endpunkt streamen. Der Streaming-Schnittstellenendpunkt verwaltet den Streaming-Datenverkehr innerhalb Ihrer VPC. Der Streaming-Datenverkehr umfasst Pixel, USB, Benutzereingaben, Audio, Zwischenablage, Datei-Upload und -Download sowie Druckerdatenverkehr. Um den VPC-Endpunkt zu verwenden, muss die VPC-Endpunkteinstellung im WorkSpaces Anwendungsstapel aktiviert sein. Dies dient als Alternative zum Streamen von Benutzersitzungen über das öffentliche Internet von Standorten aus, die nur eingeschränkten Internetzugang haben und von einem Zugriff über eine Direct Connect-Instanz profitieren würden. Für das Streaming von Benutzersitzungen über einen VPC-Endpunkt ist Folgendes erforderlich:

- Die Sicherheitsgruppen, die dem Schnittstellenendpunkt zugeordnet sind, müssen eingehenden Zugriff auf Port `443` (TCP) und Ports `1400-1499` (TCP) aus dem IP-Adressbereich ermöglichen, von dem aus Ihre Benutzer eine Verbindung herstellen.
- Die Network Access Control List für die Subnetze muss ausgehenden Datenverkehr von kurzlebigen Netzwerkports `1024-65535` (TCP) in den IP-Adressbereich zulassen, von dem aus Ihre Benutzer eine Verbindung herstellen.

- Eine Internetverbindung ist erforderlich, um Benutzer zu authentifizieren und die Webressourcen bereitzustellen, die Applications zum Funktionieren benötigen. WorkSpaces

Weitere Informationen zur Beschränkung des Datenverkehrs auf AWS Dienste mit WorkSpaces Anwendungen finden Sie im Administratorhandbuch für das Erstellen und Streamen von VPC-Endpunkten.

Wenn ein vollständiger öffentlicher Internetzugang erforderlich ist, empfiehlt es sich, die verstärkte Sicherheitskonfiguration (ESC) von Internet Explorer im Image Builder zu deaktivieren. Weitere Informationen finden Sie im Administratorhandbuch für WorkSpaces Anwendungen zur Deaktivierung der erweiterten Sicherheitskonfiguration von Internet Explorer.

Notfallwiederherstellung

Amazon AppStream 2.0 verfügt über integrierte Redundanz in bis zu drei Availability Zones. Das heißt, wenn ein Benutzer eine aktive Sitzung in einer Availability Zone hat, die heruntergefahren ist, kann er einfach die Verbindung trennen und erneut verbinden, wodurch ihm eine Sitzung in einer fehlerfreien Availability Zone reserviert wird, vorausgesetzt, Sie haben Kapazität. Dadurch wird zwar eine hohe Verfügbarkeit innerhalb der Region gewährleistet, es ist jedoch keine Notfallwiederherstellungslösung, wenn der Service auf regionaler Ebene Probleme hat.

Um einen Notfallwiederherstellungsplan für Ihre WorkSpaces Anwendungsbenutzer bereitzustellen, müssen Sie zunächst eine WorkSpaces Anwendungsumgebung in Ihrer sekundären Region aufbauen. Aus Sicht des Designs sollte diese Umgebung gegebenenfalls redundante Verbindungen zu Ihrer lokalen Umgebung haben und nicht von der primären Region abhängig sein. Wenn Ihre WorkSpaces Anwendungsflotte beispielsweise zu einer Domäne gehört, sollten Sie zusätzliche Domänencontroller in der sekundären Region haben, für die Standorte und Dienste konfiguriert sind. Aus Sicht der WorkSpaces Anwendungen sollte diese Umgebung aus denselben Flotten- und Stack-Einstellungen bestehen wie in Ihrer primären Region. Auf der Flotte selbst sollte dasselbe Basis-Image ausgeführt werden, das über die Konsole oder programmgesteuert in Ihre sekundäre Region kopiert werden kann. Wenn die Anwendungen, die in Ihren WorkSpaces Anwendungssitzungen ausgeführt werden, eine Backend-Abhängigkeit haben, die an Ihre primäre Region gebunden ist, sollte auch diese über regionale Redundanz verfügen, um sicherzustellen, dass die Benutzer auch dann auf das Backend der Anwendung zugreifen können, wenn die primäre Region ausfällt. Ihre Service-Level-Grenzwerte in Ihrer Zielregion sollten mit Ihrer Hauptregion übereinstimmen.

Routing von Identitäten

Es gibt zwei unterschiedliche Methoden, um den Zugriff auf Anwendungen in einem DR-Szenario bereitzustellen. Im Großen und Ganzen unterscheiden sich die beiden Methoden darin, wie die Benutzer in die Failover-Region geleitet werden. Die erste Methode wird mit einer einzigen WorkSpaces Anwendungskonfiguration in Ihrem IdP ausgeführt, und die zweite Methode besteht aus zwei separaten Anwendungskonfigurationen.

Methode 1: Ändern des Relay-Status Ihrer Anwendung

Wenn sich Benutzer über einen Identitätsanbieter (IdP) bei WorkSpaces Anwendungen anmelden, werden sie nach ihrer Authentifizierung an eine bestimmte URL weitergeleitet, die der Region und dem Stack entspricht, auf die sie Zugriff haben sollen. Weitere Informationen zur Relay State-URL

finden Sie im Amazon WorkSpaces Applications Administration Guide. Der Administrator kann einen regionsübergreifenden Stack konfigurieren, der auf demselben WorkSpaces Anwendungs-Image wie die primäre Region basiert und zu dem Benutzer ein Failover durchführen können. Der Administrator kann dieses Failover steuern, indem er einfach die Relay-State-URL so aktualisiert, dass sie auf den Failover-Stack verweist. Damit diese Methode ordnungsgemäß funktioniert, müssen die zugehörigen IAM-Richtlinien den Zugriff auf beide Stacks (primär und Failover) widerspiegeln. Weitere Informationen zur Konfiguration dieser IAM-Richtlinien finden Sie in der folgenden Beispielrichtlinie.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "appstream:Stream",
            "Resource": [
                "arn:aws:appstream:us-east-1:190836837966:stack/StackName",
                "arn:aws:appstream:us-east-1:190836837966:stack/StackName"
            ],
            "Condition": {
                "StringEquals": {
                    "appstream:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

Methode 2: Konfiguration von zwei WorkSpaces Anwendungsanwendungen in Ihrem IdP

Bei dieser Methode muss der Administrator zwei separate Anwendungen für WorkSpaces Anwendungen innerhalb des IdP erstellen. Sie können dann entweder beide Anwendungen präsentieren und dem Benutzer die Wahl lassen, wohin er gehen soll, oder sie können lock/hide eine Anwendung erstellen, bis ein Failover erforderlich ist. Diese Methode eignet sich besser für den Anwendungsfall globaler Benutzer, die sich häufig bewegen. Diese Benutzer sollten vom

nächstgelegenen Endpunkt aus streamen. Wenn ihnen also beide Anwendungen zugewiesen sind, haben sie die Möglichkeit, die Anwendung auszuwählen, die für ihre nächstgelegene Region konfiguriert ist. Dies kann auch automatisiert werden. Weitere Informationen finden Sie in diesem Blogbeitrag.

Persistenz des Speichers

Wenn Sie die in WorkSpaces Anwendungen enthaltenen Datenpersistenzfunktionen wie Anwendungspersistenz und Home-Folder-Synchronisierung nutzen möchten, müssen Sie diese Daten in Ihre Failover-Region replizieren. Diese Funktionen speichern die persistenten Daten in einem Amazon S3 S3-Bucket in der angegebenen WorkSpaces Anwendungsregion. Damit die Daten regionsübergreifend bestehen bleiben, müssen Sie alle Änderungen im Quell-Bucket in den Anwendungs-Bucket der Failover-Region WorkSpaces replizieren. Dies kann mit systemeigenen Amazon S3 S3-Funktionen wie der regionsübergreifenden Amazon S3-Replikation geschehen. Die persistenten Daten jedes Benutzers werden in einem Ordner mit seinem Hash-Benutzernamen gespeichert. Da der Benutzername regionsübergreifend gleich gehasht wird, sorgt eine einfache Replikation der Daten für Datenpersistenz in Ihrer sekundären Region. Weitere Informationen zu den Amazon S3 S3-Buckets, die von WorkSpaces Applications verwendet werden, finden Sie in diesem Handbuch.

Überwachen

Verwenden von Dashboards

Die Überwachung der Flottenauslastung ist eine regelmäßige Aktivität, die anhand von CloudWatch Kennzahlen und der Erstellung eines Dashboards durchgeführt werden kann. Alternativ können Sie in der WorkSpaces Anwendungskonsole die Registerkarte Flottennutzung verwenden. Überwachen Sie regelmäßig Ihre Flottennutzung, da das Nutzerverhalten nicht immer vorhersehbar ist und die Nachfrage selbst die erste Planung im Voraus übersteigen kann. Eine vollständige Liste der WorkSpaces Anwendungsmetriken und -dimensionen für CloudWatch finden Sie im Leitfaden zur WorkSpaces Anwendungsadministration unter Ressourcen überwachen.

Wir erwarten Wachstum

Immer wenn es einen großen Sprung gibt`PendingCapacity`, ist ein Auto Scaling-Ereignis eingetreten. Es ist wichtig, dies zu bestätigen `AvailableCapacity` und `PendingCapacity` eine umgekehrte Beziehung herzustellen, solange neue WorkSpaces Anwendungsflotteninstanzen für Benutzersitzungen verfügbar werden. Erstellen Sie `InsufficientCapacityError` für jede WorkSpaces Anwendungsflotte einen CloudWatch Alarm, um Administratoren zu benachrichtigen und sicherzustellen, dass die automatische Skalierung nicht hinter dem Bedarf zurückbleibt.

Wenn der Bedarf die Kapazität übersteigt und `InsufficientCapacityError` Metrikwerte üblich sind, sollten Sie erwägen, die Mindestkapazität zu Beginn des Arbeitstages mithilfe einer Richtlinie zur geplanten Skalierung anzuheben. Führen Sie außerdem eine zweite Richtlinie zur geplanten Skalierung ein, um die Mindestkapazität zu senken, sobald der Bedarf gedeckt ist. Beachten Sie, dass eine Senkung des Werts für die Mindestkapazität keine Auswirkungen auf bestehende Sitzungen hat. Wenn Sie die Mindestkapazität vor dem Ende des Arbeitstages verringern, kann die Waage effektiv wie vorgesehen funktionieren, indem der Wert für gesenkt wird`ActualCapacity`. Dadurch werden die Kosten optimiert.

Wenn die Nachfrage ständig unvorhersehbar ist, verwenden Sie die Skalierungsrichtlinie von Target Tracking, um sicherzustellen, dass die WorkSpaces Anwendungsflotte ausreichend `AvailableCapacity` ist, um die Nachfrage zu decken, und gleichzeitig die Nutzungsmuster zu bestimmen. Setzen Sie die Überwachung fort, da Target Tracking einen Prozentsatz des Flottenverbrauchs verwendet. Wenn die Gesamtzahl der Flotteninstanzen zunimmt, vervielfacht sich die Gesamtzahl der ungenutzten Flotteninstanzen. Dies kann verschwenderisch werden, es sei

denn, die maximale Kapazität wird auf einen konservativen Wert festgelegt. Verwenden Sie mehrere Arten von Skalierungsrichtlinien (z. B. Scheduled und Target Tracking), um Zuverlässigkeit und Kostenoptimierung in Einklang zu bringen.

Überwachung der Benutzernutzung

Überwachung einzelner Benutzer, da damit Kosten in Form von Benutzergebühren verbunden sind. Diese Benutzergebühr ist auf die Abonnentenzugriffslizenzen (SAL) von Image Assistant (RDS) zurückzuführen. Die Bewertung einzelner Benutzer kann entweder durch Berichte des IdP, bei dem die Authentifizierung durchgeführt wird, oder durch Nutzungsberichte erfolgen.

Nutzungsberichte werden als separate `.csv` Dateien in Ihrem S3-Bucket gespeichert, die Sie mithilfe von Business Intelligence-Tools (BI) von Drittanbietern herunterladen und analysieren können. Sie können Ihre Nutzungsdaten analysieren, AWS ohne Ihre Berichte herunterzuladen, oder Berichte für benutzerdefinierte Datumsbereiche erstellen, ohne mehrere Dateien zu verketten. `.csv` Sie können beispielsweise Amazon Athena und Amazon Quick verwenden, um benutzerdefinierte Berichte und Visualisierungen Ihrer WorkSpaces Anwendungsnutzungsdaten zu erstellen.

Dauerhafte Anwendungs- und Windows-Ereignisprotokolle

Wenn eine WorkSpaces Anwendungsinstanzsitzung abgeschlossen ist, wird die Instanz beendet. Das bedeutet, dass alle in der Sitzung verwendeten Anwendungs- und Windows-Ereignisprotokolle verloren gehen. Wenn diese Anwendungs- und Windows-Ereignisprotokolle dauerhaft gespeichert werden müssen, besteht eine Methode darin, sie mithilfe von Amazon Data Firehose in Echtzeit an S3 zu übermitteln und mit Amazon OpenSearch Service (OpenSearch Service) zu suchen. Wenn nicht zu erwarten ist, dass Anfragen häufig auftreten, verwenden Sie zur Kostenoptimierung Amazon Athena für die Suche, anstatt Amazon OpenSearch Service auszuführen.

Prüfung von Netzwerk- und Verwaltungsaktivitäten

Falls noch nicht eingerichtet, empfiehlt es sich, die Konfiguration AWS CloudTrail AWS-Konto mit Amazon WorkSpaces Applications vorzunehmen. Um WorkSpaces Applications API-Aufrufe speziell zu prüfen, verwenden Sie die Filterereignisquelle mit dem Wert`appstream.amazonaws.com`.

Aktivieren Sie VPC-Flussprotokolle, um den Zugriff auf vom Kunden verwaltete Ressourcen zu überprüfen. VPC-Flussprotokolle können in Logs veröffentlicht werden, CloudWatch um Abfragen durchzuführen, wenn eine Überwachung erforderlich ist.

Die Überwachung der Subnetz-IP-Zuweisung ist wichtig, da die WorkSpaces Anwendungsflotten immer größer werden. Melden Sie die IP-Zuweisung, indem Sie die Describe-subnets-CLI ausführen, um die verfügbaren IP-Adressen in jedem Subnetz zu melden, das Flotten zugewiesen ist. Stellen Sie sicher, dass Ihr Unternehmen über ausreichende IP-Adresskapazitäten verfügt, um den Bedarf aller Flotten mit maximaler Kapazität zu decken.

Kostenoptimierung

Die Kostenoptimierung konzentriert sich auf die Vermeidung unnötiger Kosten. Zu den wichtigsten Themen gehören das Verständnis und die Kontrolle darüber, wofür Geld ausgegeben wird, sowie die Auswahl der am besten geeigneten und korrekten Anzahl von Ressourcentypen. Analysieren Sie die Ausgaben im Zeitverlauf und skalieren Sie sie, um den Geschäftsanforderungen gerecht zu werden. Für die folgenden WorkSpaces Anwendungsressourcen fallen nutzungsabhängige Gebühren an:

- Always-On Flotteninstanzen
- On-Demand Flotteninstanzen
- On-Demand Gebühr für gestoppte Instanzen
- Image Builder-Instances
- Gebühren für Nutzer

Aktuelle Preisinformationen finden Sie auf der AWS Website mit den Preisen für Amazon WorkSpaces Applications.

Entwerfen kosteneffizienter WorkSpaces Anwendungsbereitstellungen

Der erste Schritt bei der Planung und Gestaltung der WorkSpaces Anwendungsbereitstellung besteht darin, mithilfe eines einfachen Tools zur Preisgestaltung die Höhe Ihrer AWS Gebühren im Zusammenhang mit Ihrer Nutzung abzuschätzen. Geben Sie Ihre Gesamtzahl der Benutzer, die tatsächliche gleichzeitige Nutzung pro Stunde, den Instance-Typ und die Flottenauslastung an, und das Preisfindungstool berechnet Ihren Preis pro Benutzer. Es zeigt auch die geschätzten Preiseinsparungen, wenn Sie eine On-Demand Flotte anstelle einer Always-On Flotte verwenden.

Kunden schätzen das Preismodell für WorkSpaces Anwendungen, bei dem nur für die Instances bezahlt wird, die sie zur Erfüllung der Streaming-Anforderungen ihrer Benutzer bereitstellen. Dieses Modell unterscheidet sich von ihren bestehenden Anwendungs-Streaming-Umgebungen. Diese basieren in der Regel auf der Bereitstellung von Spitzenkapazitäten, auch nachts, am Wochenende und an Feiertagen, wenn die Auslastung geringer ist. Das Amazon AppStream 2.0 Pricing Tool bietet nur eine Schätzung Ihrer AWS-Gebühren im Zusammenhang mit Ihrer Nutzung von WorkSpaces Anwendungen und beinhaltet keine Steuern, die möglicherweise anfallen könnten. Ihre tatsächlichen Gebühren hängen von einer Vielzahl von Faktoren ab, einschließlich Ihrer tatsächlichen Nutzung der AWS-Services.

Das WorkSpaces Applications Pricing Tool wird als Microsoft Excel- oder OpenOffice Calc-Tabelle bereitgestellt, mit der Sie grundlegende Informationen zu Ihrer Flotte eingeben können. Anschließend erhalten Sie auf der Grundlage Ihres Nutzungsmusters einen Kostenvoranschlag für die WorkSpaces Anwendungsumgebung für On-Demand- und Always-On-Flotten. Sie könnten Kosten auf der Grundlage historischer oder erwarteter Nutzungstrends simulieren. Elastic Fleets machen es dem Administrator überflüssig, die Nutzung vorherzusagen und Skalierungsrichtlinien und Images zu erstellen und zu verwalten, da diese Funktionen integriert sind. Elastic-Flotten und Instances, auf denen Amazon Linux 2 ausgeführt wird (alle Flottenarten), werden für die Dauer der Streaming-Sitzung in Sekunden mit einem Minimum von 15 Minuten in Rechnung gestellt.

Optimierung der Kosten durch Wahl des Instance-Typs

Für Fleet- und Image Builder-Instances stehen eine Reihe verschiedener Instance-Familien und Typen zur Verfügung, die Sie für Ihre Anwendung auswählen können.

Tests durch Endbenutzer — Der nächste Schritt besteht darin, die WorkSpaces Anwendungsflotte einer Gruppe von Pilotbenutzern zum Testen zur Validierung unseres ausgewählten Instance-Typs zur Verfügung zu stellen. Es ist wichtig, dass Sie die Pilotbenutzer auffordern, all ihre regulären und umfangreichen Workflows zu testen, um Metriken rund um Speicher, CPU und Grafik zu erfassen, damit Sie grundlegende Leistungskennzahlen erfassen können. Die Pilotgruppe sollte die verschiedenen Benutzerrollen enthalten, die die Anwendung verwenden, um sicherzustellen, dass Sie sie anhand mehrerer Benutzererfahrungen testen. Der Benutzerakzeptanztest ermöglicht es Ihnen, Feedback zur Erfahrung mit Streaming-Sitzungen zu sammeln. Beim Erstellen oder Aktualisieren eines Stacks besteht die Möglichkeit, eine benutzerdefinierte Feedback-URL zu verwenden. Benutzer werden zu dieser URL weitergeleitet, nachdem sie auf den Link „Feedback senden“ geklickt haben, um Feedback zum Streaming-Erlebnis ihrer Anwendung einzureichen. Wenn es einen Leistungsengpass gibt, verwenden Sie Windows-Leistungsmetriken, um Ressourcenbeschränkungen zu analysieren. Wenn für den aktuellen Flotteninstance-Typ stream.standard.medium beispielsweise eine Ressourcenbeschränkung angezeigt wird, aktualisieren Sie den Instance-Typ auf stream.standard.large. Umgekehrt sollten Sie eine Herabstufung des Instance-Typs in Betracht ziehen, wenn Leistungskennzahlen ein hohes Maß an unzureichender Nutzung von Ressourcen zeigen.

Optimierung der Kosten durch die Wahl des Flottentyps

Bei der Erstellung einer neuen WorkSpaces Anwendungsflotte müssen Entwickler entweder einen Always-On- oder einen On-Demand Flotten-Typ wählen. Bei der Auswahl des Instance-Typs aus

Preissicht ist es wichtig zu verstehen, wie WorkSpaces Applications Flotteninstanzen verwaltet. Bei Always-On Flotten bleiben Flotteninstanzen im laufenden Zustand. Wenn Benutzer versuchen, Sitzungen zu streamen, sind Flotteninstanzen daher immer bereit, Streaming-Sitzungen zu starten.

Bei On-Demand Flotten werden Flotteninstanzen nach dem Start im Status „Gestoppt“ belassen. Die Gebühr für gestoppte Instances ist niedriger als die Gebühr für laufende Instances, was zur Kostensenkung beitragen kann. Die On-Demand Flotteninstanzen müssen aus einem angehaltenen Zustand gestartet werden. Ein Benutzer muss ungefähr zwei Minuten warten, bis seine Streaming-Sitzung verfügbar ist.

Elastic Fleets eignen sich gut für eigenständige Anwendungen, die auf virtuellen Festplatten installiert werden können, die in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert sind. Elastic Fleets kann die Kosten in einigen Anwendungsfällen weiter senken, da die Abrechnung pro Sekunde nur für die Dauer des Streamings erfolgt. Die Rate hängt vom Instance-Typ und der Größe sowie vom Betriebssystem ab, das Sie bei der Erstellung der Flotte auswählen.

Wenn Endbenutzer während der Geschäftszeiten Flotteninstanzen benötigen, ist es besser, dieselben Streaming-Sitzungen beizubehalten. Das liegt daran, dass Flotteninstanzen pro Stunde berechnet werden und jedes Mal, wenn eine neue Streaming-Sitzung beginnt, eine weitere Flotteninstanzgebühr anfällt.

Tabelle 10 — Vergleich der Flottenarten der WorkSpaces Anwendungen

Art der Flotte	Vorteile	Überlegungen
Always-On	Weniger Wartezeit für Streaming-Sitzungen	Benutzer zahlen für die stündliche Instanzgebühr, da es keine Möglichkeit gibt, Instances im gestoppten Zustand zu belassen.
On-Demand	Kosteneinsparung, da die Instances im gestoppten Zustand bleiben	Längere Wartezeit für Streaming-Sitzungen
Elastic	Per-second Die Abrechnun g ist möglicherweise nützlich für Anwendungsfälle mit sporadischen Nutzungsm	Je größer die virtuelle Festplatte einer Anwendung wird, desto länger kann

Art der Flotte	Vorteile	Überlegungen
	ustern für Anwendungen, die auf einer virtuellen Festplatte installiert werden können	es dauern, sie auf einer Streaming-Instanz zu mounten

WorkSpaces Applications überwacht Ihre Flottenauslastung und nimmt automatische Anpassungen der Flottenkapazität vor, um Ihren Benutzeranforderungen zu möglichst niedrigen Kosten gerecht zu werden. Die Kapazitätsanpassungen werden auf der Grundlage von Skalierungsrichtlinien vorgenommen, die Sie entweder auf der aktuellen Auslastung oder auf der Grundlage eines Zeitplans definieren. Überprüfen Sie regelmäßig die Kennzahlen zur Flottennutzung, um sicherzustellen, dass die Richtlinien zur Flottenskalierung keine hohen Kapazitätsreserven vorsehen.

Skalierungsrichtlinien

Fleet Auto Scaling ermöglicht es Ihnen, die Flottenressourcen zu optimieren, indem Sie nicht zu viele Ressourcen beanspruchen müssen, bis sich Benutzer anmelden. Administratoren können die Größe der Flotte auf der Grundlage verschiedener Nutzungsarten an die Benutzeranforderungen anpassen. Verwenden Sie CloudWatch WorkSpaces Applications Fleet Metrics oder Überwachungstools von Drittanbietern, um mehr über Benutzeraktivitäten zu erfahren und Skalierungsrichtlinien zu konfigurieren, um WorkSpaces Anwendungsflotten je nach erwarteter Nutzung zu erweitern oder zu verkleinern. Benutzerprotokolle sind ein wichtiger Mechanismus, um sich ein Bild von der tatsächlichen Nutzung zu machen. Diese Erkenntnisse können genutzt werden, um die Flottengröße mithilfe von Auto Scaling dynamisch zu ändern.

In vielen Fällen werden WorkSpaces Anwendungsflotten auf der Grundlage der maximalen Benutzerzahl erstellt und nicht an unterschiedliche Tages- und Wochentage wie Nächte und Wochenenden angepasst. Oft ist die Anzahl der gleichzeitigen Benutzer von gestreamten Anwendungen geringer als die Gesamtzahl der Benutzer, insbesondere wenn Benutzer die Flexibilität haben, remote zu arbeiten. Es ist wichtig, diese Faktoren bei der Prognose von Nutzungsmustern zu berücksichtigen. Eine Überschätzung führt zu einer übermäßigen Bereitstellung von WorkSpaces Anwendungsinstanzen, was zu zusätzlichen Kosten führt. Um eine optimale Konfiguration zu erreichen, müssen Sie möglicherweise eine oder mehrere geplante Skalierungsrichtlinien mit Scale-Out-Richtlinien kombinieren.

Weitere Informationen zur Implementierung von Skalierungsrichtlinien finden Sie unter Skalierung Ihrer Amazon AppStream 2.0-Flotten.

Gebühren für Nutzer

Benutzergebühren werden pro Benutzer und Monat in allen Fällen erhoben, in AWS-Region denen Benutzer WorkSpaces Anwendungen von Applications Fleet-Instances streamen. Anstatt unterschiedliche Benutzer-IDs zu generieren, sollten Sie einheitliche Benutzer-IDs für WorkSpaces Anwendungsbenutzer verwenden. Benutzergebühren werden nicht erhoben, wenn eine Verbindung zu Image Builders hergestellt wird.

Schulen, Universitäten und bestimmte öffentliche Einrichtungen können sich für eine reduzierte Microsoft RDS SAL-Benutzergebühr von 0,44 USD pro Benutzer und Monat qualifizieren. Informationen zu den Qualifikationsanforderungen finden Sie in den Microsoft-Lizenzbedingungen und -dokumenten.

Wenn Sie über Microsoft License Mobility verfügen, sind Sie möglicherweise berechtigt, Ihre eigenen Microsoft RDS-Clientzugriffslizenzen (CALs) mitzubringen und diese mit WorkSpaces Amazon-Anwendungen zu verwenden. Wenn Sie durch Ihre eigene Lizenz abgedeckt sind, fallen keine monatlichen Benutzergebühren an. Weitere Informationen darüber, ob Sie Ihre vorhandenen Microsoft RDS CAL-Lizenzen mit Amazon WorkSpaces Applications verwenden können, finden Sie in den AWS License Mobility-Richtlinien oder wenden Sie sich an Ihren Microsoft-Lizenzvertreter.

Verwendung von Image Builder

WorkSpaces Applications Image Builder Builder-Instanzen werden stündlich berechnet. Die Gebühr für die Image Builder Builder-Instanz umfasst Rechenleistung, Speicherplatz und jeglichen Netzwerkverkehr, der vom Streaming-Protokoll verwendet wird. Für alle laufenden Image Builder Builder-Instanzen wird die entsprechende Gebühr für laufende Instanzen berechnet. Diese Gebühr richtet sich nach dem Instanztyp und der Größe der Instanz, auch wenn keine Administratoren verbunden sind.

Als bewährte Methode zur Kostenoptimierung sollten Sie eine Image Builder Builder-Instanz herunterfahren, wenn sie nicht verwendet wird. CloudWatch Ereignisregeln können verwendet werden, um einen täglichen Job zu planen, z. B. das Aufrufen einer Lambda-Funktion zum Stoppen von Image Builder-Instances.

Sie können Ihr WorkSpaces Anwendungs-Image auf dem neuesten Stand halten, indem Sie verwaltete WorkSpaces Anwendungs-Image-Updates verwenden. Diese Aktualisierungsmethode bietet die neuesten Windows-Betriebssystemupdates und Treiberupdates sowie die neueste WorkSpaces Applications Agent-Software. Wenn Sie diese Methode zum Aktualisieren von Images

verwenden, wird ein Image Builder als Teil des Managed Service-Prozesses automatisch gestartet und gestoppt.

Schlussfolgerung

Mit WorkSpaces Applications können Sie ganz einfach Ihre vorhandenen Desktop-Anwendungen hinzufügen AWS und es Ihren Benutzern ermöglichen, sie sofort zu streamen. Windows-Benutzer können entweder den WorkSpaces Anwendungsclient oder einen HTML5-capable Webbrowser für das Anwendungsstreaming verwenden. Da Sie nur jeweils eine Anwendungsversion unterhalten müssen, vereinfacht sich das Anwendungsmanagement beträchtlich. Ihre Benutzer arbeiten stets mit der aktuellen Anwendungsversion. Ihre Anwendungen werden auf AWS Rechenressourcen ausgeführt, und Daten werden niemals auf den Geräten der Benutzer gespeichert, was bedeutet, dass sie immer ein leistungsstarkes und sicheres Erlebnis haben.

Im Gegensatz zu herkömmlichen lokalen Lösungen für das Streaming von WorkSpaces Desktop-Anwendungen bietet Applications nutzungsabhängige Preise, ohne Vorabinvestitionen und ohne Wartung der Infrastruktur. Sie können sofort und global skalieren und so sicherstellen, dass Ihre Benutzer stets ein hervorragendes Erlebnis haben.

Amazon WorkSpaces Applications ist so konzipiert, dass es in bestehende IT-Systeme und -Prozesse integriert werden kann. In diesem Whitepaper wurden die dafür bewährten Methoden beschrieben. Das Ergebnis der Einhaltung der Richtlinien in diesem Whitepaper ist eine kostengünstige Cloud-Desktop-Implementierung, die sich sicher an die Anforderungen Ihres Unternehmens in der AWS globalen Infrastruktur anpassen lässt.

Beitragende Faktoren

Zu den Mitwirkenden an diesem Dokument gehören:

- Andrew Wood, leitender Lösungsarchitekt, Amazon Web Services
- Andrew Morgan, EUC Specialist SA, Amazon Web Services
- Arun PC, Senior EUC Specialist SA, Amazon Web Services
- Asriel Agronin, leitender Lösungsarchitekt, Amazon Web Services
- Dustin Shelton, Senior EUC Specialist SA, Amazon Web Services
- Jeremy Schiefer, leitender Lösungsarchitekt, Amazon Web Services
- Navi Magee, Hauptarchitektin für Lösungen, Amazon Web Services
- Pete Fergus, leitender Cloud-Supportingenieur, Amazon Web Services
- Phil Persson, Principal EUC Specialist SA, Amazon Web Services
- Richard Spaven, Senior EUC Specialist SA, Amazon Web Services
- Spencer DeBrosse, Senior Solutions Architect, Amazon Web Services
- Stephen Stetler, leitender Lösungsarchitekt, Amazon Web Services
- Taka Matsumoto, leitender Cloud-Supportingenieur, Amazon Web Services
- Vasant Sirsat, Senior EUC Specialist SA, Amazon Web Services

Weitere Informationen

Weitere Informationen finden Sie unter:

- Administratorhandbuch WorkSpaces für Amazon-Anwendungen
- API-Referenz WorkSpaces für Amazon-Anwendungen
- Verwenden Sie Amazon FSx for Windows File Server und FSLogix, um die Persistenz von Anwendungseinstellungen in Amazon-Anwendungen zu optimieren WorkSpaces
- Überwachung von WorkSpaces Amazon-Anwendungen mit Amazon ElasticSearch und Amazon Firehose
- Analysieren Sie Ihre WorkSpaces Amazon-Anwendungsnutzungsberichte mit Amazon Athena und Amazon Quick
- Skalieren Sie Ihre Amazon WorkSpaces Applications-Flotten
- Verwendung von Microsoft AppLocker zur Verwaltung der Anwendungserfahrung auf Amazon WorkSpaces Applications
- Verwenden einer benutzerdefinierten Domain mit Amazon WorkSpaces Applications
- Wie verwende ich meine eigenen Microsoft RDS-CALs mit WorkSpaces Anwendungen?
- Preisgestaltungstool für WorkSpaces Amazon-Anwendungen
- Erstellen Sie eine Online-Softwaretestversion mit WorkSpaces Anwendungen
- Erstellen Sie ein SaaS-Portal mit WorkSpaces Amazon-Anwendungen

Dokumentversionen

Abonnieren Sie den RSS-Feed, um über Aktualisierungen dieses Whitepapers informiert zu werden.

Änderung	Beschreibung	Datum
Dokument wurde aktualisiert	Die Aktualisierungen umfassen Elastic-Flotten, attributebasierte Anwendung sberechtigungen, einen Multi-Stack-Anwendungskatal og, Linux-basierte Flotten, Datenein- und -ausgang, Disaster Recovery und weitere Updates.	14. Juni 2022
Dokument aktualisiert	HTML-Version veröffentlicht.	19. Januar 2022
Erste Veröffentlichung	Whitepaper veröffentlicht.	8. Juni 2021

Hinweise

Die Kunden sind dafür verantwortlich, die Informationen in diesem Dokument selbst unabhängig zu beurteilen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWSProdukte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

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.