Melhores práticas para implantar aplicativos da Amazon WorkSpaces

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Melhores práticas para implantar aplicativos da Amazon WorkSpaces:

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

Resumo i
Resumo 1
Introdução 1
Principais conceitos 2
Design em VPC 3
Diretrizes para projeto 3
Zonas de disponibilidade 3
Dimensionamento de sub-rede 4
Roteamento de sub-rede 6
Intra-Region conectividade 6
Tráfego de saída da Internet 7
On-premises 7
Endpoints da VPC 7
Endpoint da VPC para o Amazon S3 7
Interface de API da Amazon WorkSpaces Applications VPC endpoint 8
Endpoint VPC da interface de streaming de WorkSpaces aplicativos da Amazon 8
Criação e gerenciamento de imagens 10
Criando uma imagem WorkSpaces de aplicativos 10
Sistema operacional 10
Aplicativos 12
Bloco de aplicativos 13
Personalização de perfil do usuário 14
Segurança 14
desempenho 15
WorkSpaces Seleção da versão do agente de aplicativos 15
Interface de linha de comandos (CLI) do Image Assistant 16
Como gerenciar a experiência de streaming dos usuários 17
Personalização usando scripts de sessão 17
Como usar a Política de grupo do Active Directory 17
Atualizações de imagem 17
Personalização da frota 19
Tipo de frota 19
Dimensionamento da frota 25
Capacidade mínima e ajuste da escala programado 25
Capacidade máxima e cotas de serviço 25

Como escolher a exibição da área de trabalho ou do aplicativo 27
Exibição da área de trabalho 27
Exibição somente de aplicativos 27
AWS Identity and Access Management configuração de função 28
Uso de credenciais estáticas 28
Protegendo seus WorkSpaces aplicativos S3 Bucket 29
Estratégias de ajuste de escala automático da frota 30
Compreendendo WorkSpaces as instâncias de aplicativos 30
Políticas de ajuste de escala 30
Ajuste de escala em etapas 30
Monitoramento do objetivo 30
Scheduled-based escalonamento 31
Políticas de ajuste de escala na produção 31
Práticas recomendadas para ajuste de escala das políticas de design 33
Combinar políticas de ajuste de escala 33
Evitar a rotatividade do ajuste de escala 33
Entender a taxa máxima de provisionamento 34
Utilizar várias zonas de disponibilidade 34
Monitorar métricas de erro de capacidade insuficiente 35
Métodos de conexão 36
Resumo do suporte a atributos e dispositivos 36
Acesso pelo navegador da web 37
WorkSpaces Cliente de aplicativos para Windows 37
WorkSpaces Modos de conexão do cliente de aplicativos 38
Implantação e gerenciamento do cliente 39
Domínios personalizados 40
Autenticação 41
Como determinar o método otimizado 41
Configuração do provedor de identidade 43
SAML 2.0 43
Grupo de usuários 44
URL de streaming 44
Direito à inscrição 45
Integração com o Microsoft Active Directory 47
Opções de serviço 47
Cenários de implantação 47
Cenário 1: Serviços de Domínio do Active Directory (ADDS) implantados no local 48

Cenário 2: Estenda os Serviços de Domínio Ativo (ADDS) à AWS VPC do cliente 49
Cenário 3: Microsoft Active Directory AWS gerenciado 50
Topologia do site do serviço do Active Directory 51
Unidades organizacionais do Active Directory 53
Limpeza de objetos no computador do Active Directory 53
Segurança 54
Como proteger dados persistentes 54
Estado e dados do usuário 54
Segurança de endpoints e antivírus 56
Como remover identificadores exclusivos 56
Otimização de desempenho 56
Exclusões de verificação 57
Pastas 58
Limpeza do console de segurança de endpoints 59
Exclusões de rede 59
Protegendo uma sessão de WorkSpaces aplicativos 60
Como limitar os controles de aplicativos e sistemas operacionais 60
Firewalls e roteamento 61
Prevenção de perda de dados 61
Controles de transferência de dados de instâncias de cliente para WorkSpaces aplicativos 61
Controle do tráfego de saída da Instância de WorkSpaces Aplicativos 62
Usando AWS serviços 63
AWS Identity and Access Management 63
Endpoints da VPC 63
Recuperação de desastres 66
Roteamento de identidade 66
Método 1: como alterar o estado de retransmissão do aplicativo 66
Método 2: Configurando dois WorkSpaces aplicativos em seu IdP 67
Persistência de armazenamento 68
Monitoramento 69
Usar painéis 69
Como antecipar o crescimento 69
Monitoramento do uso pelos usuários 70
Logs persistentes de aplicativos e eventos do Windows 70
Auditoria da atividade de rede e administrativa 70
Otimização de custos 72

Projetando implantações WorkSpaces de aplicativos econômicas 72
Como otimizar custos com a escolha do tipo de instância 73
Como otimizar custos com a escolha do tipo de frota 73
Políticas de ajuste de escala 75
Taxas de usuário 75
Uso do Image Builder 76
Conclusão 77
Colaboradores 78
Outras fontes de leitura 79
Revisões do documento 80
Avisos 81
..... lxxxii

Melhores práticas para implantar aplicativos da Amazon WorkSpaces

Data de publicação: 19 de janeiro de 2022 (Revisões do documento)

Resumo

Este whitepaper descreve um conjunto de melhores práticas para a implantação de aplicativos da Amazon. WorkSpaces O documento aborda o design da Amazon Virtual Private Cloud (Amazon VPC), a geração e o gerenciamento de imagens, a personalização da frota e as estratégias de ajuste de escala automático da frota. Inclui métodos de conexão do usuário, autenticação e integração com o Microsoft Active Directory. Este paper também inclui recomendações para projetar a segurança, o monitoramento e a otimização de custos de WorkSpaces aplicativos.

Este whitepaper foi escrito com o objetivo de permitir o acesso rápido às informações relevantes. É um documento para engenheiros de rede, especialistas em entrega de aplicativos, engenheiros de diretórios ou engenheiros de segurança.

Introdução

O Amazon WorkSpaces Applications é um serviço de streaming de aplicativos totalmente gerenciado que fornece aos usuários acesso instantâneo aos seus aplicativos de desktop de qualquer lugar. WorkSpaces Os aplicativos gerenciam os AWS recursos necessários para hospedar e executar seus aplicativos. Ele é dimensionado automaticamente e fornece acesso aos seus usuários sob demanda. WorkSpaces Os aplicativos fornecem aos usuários finais acesso aos aplicativos de que precisam no dispositivo de sua escolha, com uma experiência de usuário responsiva, indistinguível dos aplicativos instalados nativamente.

As seções a seguir fornecem detalhes sobre os WorkSpaces aplicativos da Amazon, explicam como o serviço funciona, descrevem o que você precisa para iniciar o serviço e informam quais opções e recursos estão disponíveis para você usar. Ao implantar WorkSpaces aplicativos para usuários finais, é importante implementar as melhores práticas para proporcionar uma excelente experiência ao usuário. Além disso, empresas de todos os portes se beneficiam da otimização de custos que reduz os custos operacionais mensais.

Principais conceitos

Para aproveitar ao máximo os WorkSpaces aplicativos, familiarize-se com os seguintes conceitos:

- Imagem: uma imagem é um modelo de instância pré-configurado. Uma imagem contém aplicativos que você pode transmitir para seus usuários e as configurações padrão do Windows e do aplicativo para permitir que os usuários comecem a usar seus aplicativos rapidamente. AWS fornece imagens básicas que você pode usar para criar imagens que incluem seus próprios aplicativos. Depois que criar uma imagem, você não poderá alterá-la. Para adicionar outros aplicativos, atualizar os aplicativos existentes ou alterar as configurações de imagem, você deve criar uma nova imagem. Você pode copiar suas imagens para outras Regiões da AWSpessoas ou compartilhá-las com outras Conta da AWS pessoas na mesma região.
- Construtor de imagem: um construtor de imagens é uma máquina virtual que você usa para criar uma imagem. Você pode iniciar e se conectar a um construtor de imagens usando o console de WorkSpaces aplicativos. Depois que você se conectar a um criador de imagens, você pode instalar, adicionar e testar seus aplicativos e usá-lo para criar uma imagem. Você pode iniciar novos criadores de imagem usando imagens privadas que você tem.
- Frota: uma frota consiste em instâncias (também conhecidas como instâncias de streaming) que executam a imagem especificada. Você pode definir o número desejado de instâncias de streaming para sua frota e configurar políticas para dimensionar sua frota automaticamente com base na demanda. Observe que cada usuário requer uma instância.
- Pilha: uma pilha consiste em uma frota associada, políticas de acesso de usuário e configurações de armazenamento. Você configura uma pilha para iniciar o streaming de aplicativos para os usuários.
- Instância de streaming: uma instância de streaming (também conhecida como instância de frota) é uma instância do Amazon Elastic Compute Cloud (Amazon EC2), que é disponibilizada para um único usuário com objetivo de fazer streaming de aplicativos. Depois que a sessão do usuário é concluída, a instância é encerrada pelo Amazon EC2.

Design em VPC

Diretrizes para projeto

Implante WorkSpaces aplicativos em uma VPC dedicada. Ao projetar a VPC de WorkSpaces aplicativos, dimensione o crescimento previsto. Reserve a capacidade do endereço IP para novos casos de uso e zonas de disponibilidade (AZs) adicionais que podem ser adicionadas posteriormente. Um ponto fundamental do design de WorkSpaces aplicativos é que somente um usuário pode consumir uma instância de WorkSpaces aplicativos. Ao alocar espaço IP, pense em um usuário como um endereço IP por instância de WorkSpaces aplicativos. Com WorkSpaces os aplicativos, é possível que um usuário consuma várias instâncias de WorkSpaces aplicativos. Portanto, o planejamento do espaço IP também deve levar em conta os casos de uso que exigem instâncias adicionais de WorkSpaces aplicativos.

Embora o tamanho máximo de um VPC Classless Inter-Domain Routing (CIDR) seja /16, é recomendável não superalocar endereços IP privados AWS . É possível estender o tamanho do VPC por meio de CIDRs adicionais, mas há um limite para isso; portanto, aloque o que é necessário desde o início.

Se a implantação de WorkSpaces aplicativos for associada a um domínio do Active Directory, as opções de DHCP definidas para a VPC devem ter o domínio DNS configurado. O servidor de nomes de domínio deve especificar os endereços IP do DNS que são autoritativos para o domínio do Active Directory, ou o DNS deve encaminhar solicitações de DNS para as instâncias de DNS autoritativas do domínio do Active Directory. Além disso, é necessário configurar `enableDnsHostnames` e `EnableDnsSupport` da VPC.

Zonas de disponibilidade

Uma Zona de disponibilidade (AZ) é um ou mais datacenters discretos com energia, redes e conectividade redundantes em uma Região da AWS. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

O Amazon WorkSpaces Applications requer apenas uma sub-rede para o lançamento de uma frota. A prática recomendada é configurar no mínimo duas zonas de disponibilidade, uma sub-rede por zona de disponibilidade exclusiva. Para otimizar o ajuste de escala automático da frota, use mais de duas zonas de disponibilidade. O ajuste de escala tem o benefício adicional de adicionar espaço

IP em sub-redes para crescimento, o que é abordado na seção de dimensionamento de sub-rede a seguir neste documento. O Console de Gerenciamento da AWS fornece que apenas duas sub-redes sejam especificadas durante a criação de uma frota. Use a AWS Command Line Interface(AWS CLI) ou AWS CloudFormation para permitir mais de duas IDs de sub-rede.

Dimensionamento de sub-rede

Dedique sub-redes às frotas de WorkSpaces aplicativos para permitir flexibilidade nas políticas de roteamento e na Lista de Controle de Acesso à Rede. As pilhas provavelmente terão requisitos de recursos separados. Por exemplo, as pilhas de WorkSpaces aplicativos podem ter requisitos de isolamento dando lugar a conjuntos de regras separados. Quando várias frotas de WorkSpaces aplicativos da Amazon usam as mesmas sub-redes, certifique-se de que a soma da capacidade máxima de todas as frotas não exceda o número total de endereços IP disponíveis.

Se a capacidade máxima de todas as frotas na mesma sub-rede puder ou tiver excedido o total de endereços IP disponíveis, migre as frotas para sub-redes dedicadas. Isso evita que eventos de escalabilidade automática esgotem o espaço IP alocado. Se a capacidade total de uma frota exceder o espaço IP alocado das sub-redes atribuídas, use a API ou a “frota de atualização” da AWS CLI para atribuir mais sub-redes. Para obter mais informações, consulte as cotas da Amazon VPC e como aumentá-las.

A prática recomendada é aumentar a escala horizontalmente das sub-redes, dimensionando-as adequadamente e reservando a capacidade de crescimento na VPC. Além disso, garanta que os limites máximos da frota de WorkSpaces aplicativos não excedam o espaço IP total alocado pelas sub-redes. Para cada entrada de sub-rede AWS, cinco endereços IP são reservados ao calcular a quantidade total de espaço IP. Há vários benefícios de usar mais de duas sub-redes e dimensionar horizontalmente, como:

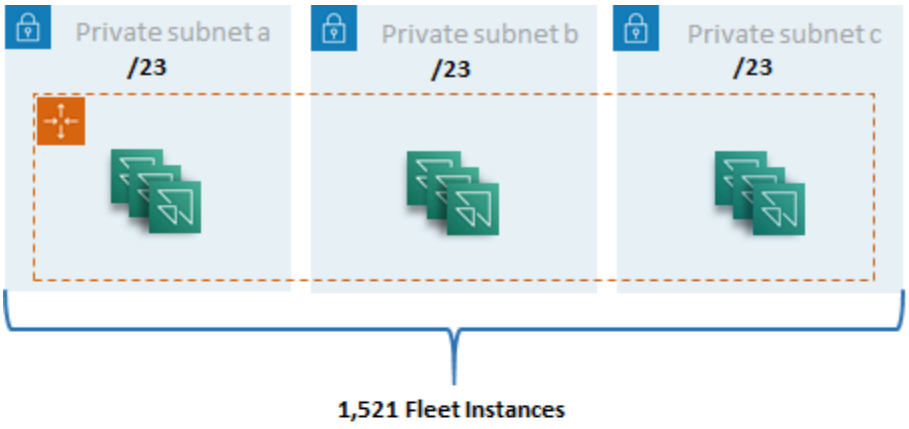
- Mais resiliência em caso de falha na zona de disponibilidade
- Aumento de throughput ao escalar automaticamente as instâncias da frota
- Uso mais eficiente de endereços IP privados, evitando a codificação permanente do IP

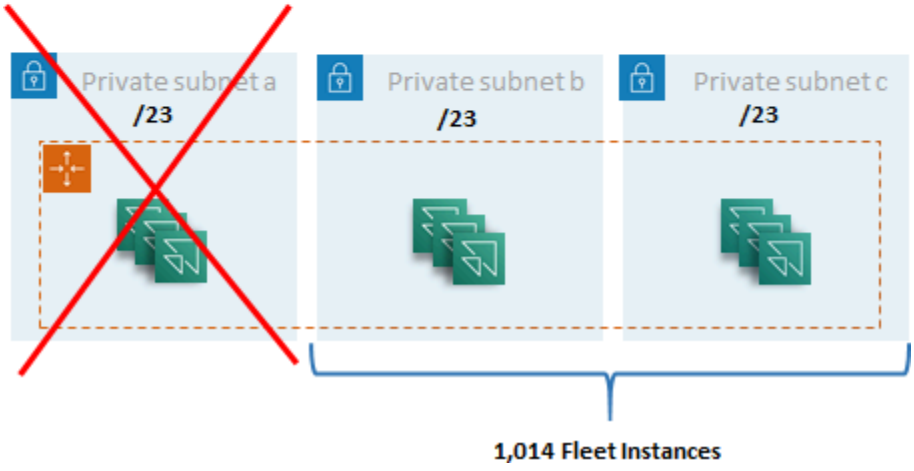
Ao dimensionar sub-redes para WorkSpaces aplicativos da Amazon, considere o número total de sub-redes e o pico esperado de simultaneidade durante o pico de utilização. Isso pode ser monitorado usando (`InUseCapacity`) mais a capacidade reservada (`AvailableCapacity`) para uma frota. Na Amazon WorkSpaces Applications, a soma das instâncias da frota de aplicativos consumidas e disponíveis para consumo é rotulada WorkSpaces . `ActualCapacity` Para

dimensionar adequadamente o espaço IP total, preveja o `ActualCapacity` necessário e divida pelo número de sub-redes, menos uma sub-rede para resiliência atribuída à frota.

Por exemplo, se o número máximo previsto de instâncias de frota no pico for 1000 e o requisito comercial for resiliente em uma falha de zona de disponibilidade, três x/23 sub-redes atenderão aos requisitos técnicos e comerciais.

- /23 = 512 hosts — 5 reservados = 507 instâncias de frota por sub-rede
- 3 sub-redes — 1 sub-rede = 2 sub-redes
- 2 sub-redes x 507 instâncias de frota por sub-rede = 1.014 instâncias de frota no pico





Exemplo de dimensionamento da sub-rede

Embora 2 x /22 sub-redes também satisfaçam a resiliência, considere o seguinte:

- Em vez de reservar 1.536 endereços IP, o uso de duas AZs resulta na reserva de 2.048 endereços IP, desperdiçando endereços IP que poderiam ser usados em outras funções.
- Se uma AZ ficar inacessível, a capacidade de aumentar a escala horizontalmente das instâncias da frota é limitada pela throughput de uma AZ. Isso pode estender a duração do `PendingCapacity`.

Roteamento de sub-rede

É uma prática recomendada criar sub-redes privadas para instâncias de WorkSpaces aplicativos, roteando para a Internet pública por meio de uma VPC centralizada para tráfego de saída. O tráfego de entrada para o streaming da sessão de WorkSpaces aplicativos é tratado pelo serviço Amazon WorkSpaces Applications por meio de gateways de streaming: você não precisa configurar sub-redes públicas para isso.

Intra-Region conectividade

Para instâncias da frota de WorkSpaces aplicativos unidas a um domínio do Active Directory, configure os controladores de domínio do Active Directory em uma VPC de serviços compartilhados em cada uma. Região da AWS As fontes do Active Directory podem ser controladores de domínio que usam como base o Amazon EC2 ou Microsoft AD gerenciado pela AWS . O roteamento entre os serviços compartilhados e as VPCs de WorkSpaces aplicativos pode ser feito por meio de uma conexão de emparelhamento de VPC ou de um gateway de trânsito. Embora os gateways de trânsito resolvam a complexidade do roteamento em grande escala, há vários motivos pelos quais o emparelhamento da VPC é preferível na maioria das configurações:

- O emparelhamento da VPC é uma conexão direta entre as duas VPCs (sem salto extra).
- Não há cobrança por hora, apenas a taxa padrão de transferência de dados entre as zonas de disponibilidade.
- Não há limite de largura de banda.
- Suporte para acessar grupos de segurança entre VPCs.

Isso é especialmente verdadeiro se as instâncias de WorkSpaces aplicativos se conectarem a servidores de and/or arquivos de infraestrutura de aplicativos com grandes conjuntos de dados em uma VPC de serviço compartilhado. Ao otimizar o caminho para esses recursos comumente acessados, a conexão de emparelhamento da VPC é ideal, mesmo nos projetos em que todos os outros roteamentos da VPC e Internet são executados por meio de um gateway de trânsito.

Tráfego de saída da Internet

Embora o roteamento direto para serviços compartilhados seja otimizado principalmente por meio de uma conexão de peering, o tráfego de saída para WorkSpaces aplicativos pode ser projetado criando um único ponto de saída da Internet a partir de várias VPCs usando o Transit Gateway. AWS Em um design de várias VPCs, é uma prática padrão ter uma VPC dedicada que controle todo o tráfego de saída da Internet. Com essa configuração, os gateways de trânsito têm maior flexibilidade e controle do roteamento em relação às tabelas de rotas padrão conectadas às sub-redes. Esse design também oferece suporte ao roteamento transitivo sem complexidade adicional e elimina a necessidade de gateways redundantes de conversão de endereços de rede (NAT) ou instâncias NAT em cada VPC.

Quando todo o tráfego de saída da Internet é centralizado em uma única VPCos , gateways NAT ou as instâncias NAT são uma opção comum de design. Para determinar o que é melhor para sua organização, consulte o guia de administração para comparar gateways NAT e instâncias NAT. O AWS Firewall de rede pode estender a proteção além dos níveis de grupo de segurança e controle de acesso à rede, protegendo no nível da rota e oferecendo regras com e sem estado das camadas 3 a 7 no modelo de OSI. Para obter mais informações, consulte Modelos de implantação do AWS Network Firewall. Caso a sua organização escolha um produto de terceiros que executa recursos avançados, como filtragem de URL, implante o serviço em sua VPC de saída da Internet. Isso pode substituir gateways NAT ou instâncias NAT. Siga as diretrizes fornecidas pelo fornecedor terceirizado.

On-premises

Quando for necessária conectividade com recursos locais, especialmente para instâncias de WorkSpaces aplicativos associadas ao Active Directory, estabeleça uma conexão altamente resiliente por meio de. AWS Direct Connect

Endpoints da VPC

Endpoint da VPC para o Amazon S3

Muitas implantações da Amazon WorkSpaces Applications exigem a persistência do estado do usuário por meio de pastas iniciais e configurações do aplicativo. Habilite a comunicação privada com esses locais do Amazon Simple Storage Service (Amazon S3), pois isso evita o uso da Internet pública. Você pode conseguir isso por meio de um gateway de endpoint da VPC. Um gateway de endpoint da VPC é preferível ao AWS PrivateLink para Amazon S3 porque:

- É otimizado em termos de custo para os requisitos de acesso à rede de WorkSpaces aplicativos
- O acesso ao bucket do Amazon S3 não é necessário a partir de recursos locais
- Um documento de política personalizado pode ser usado para restringir o acesso somente a partir das instâncias de WorkSpaces Aplicativos.

Depois de criar o gateway de endpoint da VPC, é uma prática recomendada proteger a conexão privatizada criando uma política personalizada. A política personalizada começa com o Amazon Resource Name (ARN) da função Identity and Access Management do serviço de WorkSpaces aplicativos. Especifique explicitamente as ações do S3 necessárias para a persistência do estado do usuário.

> **Note**
>
> O exemplo a seguir na seção `Resources` especifica primeiro o caminho da pasta inicial do estado e depois o caminho das configurações do aplicativo.

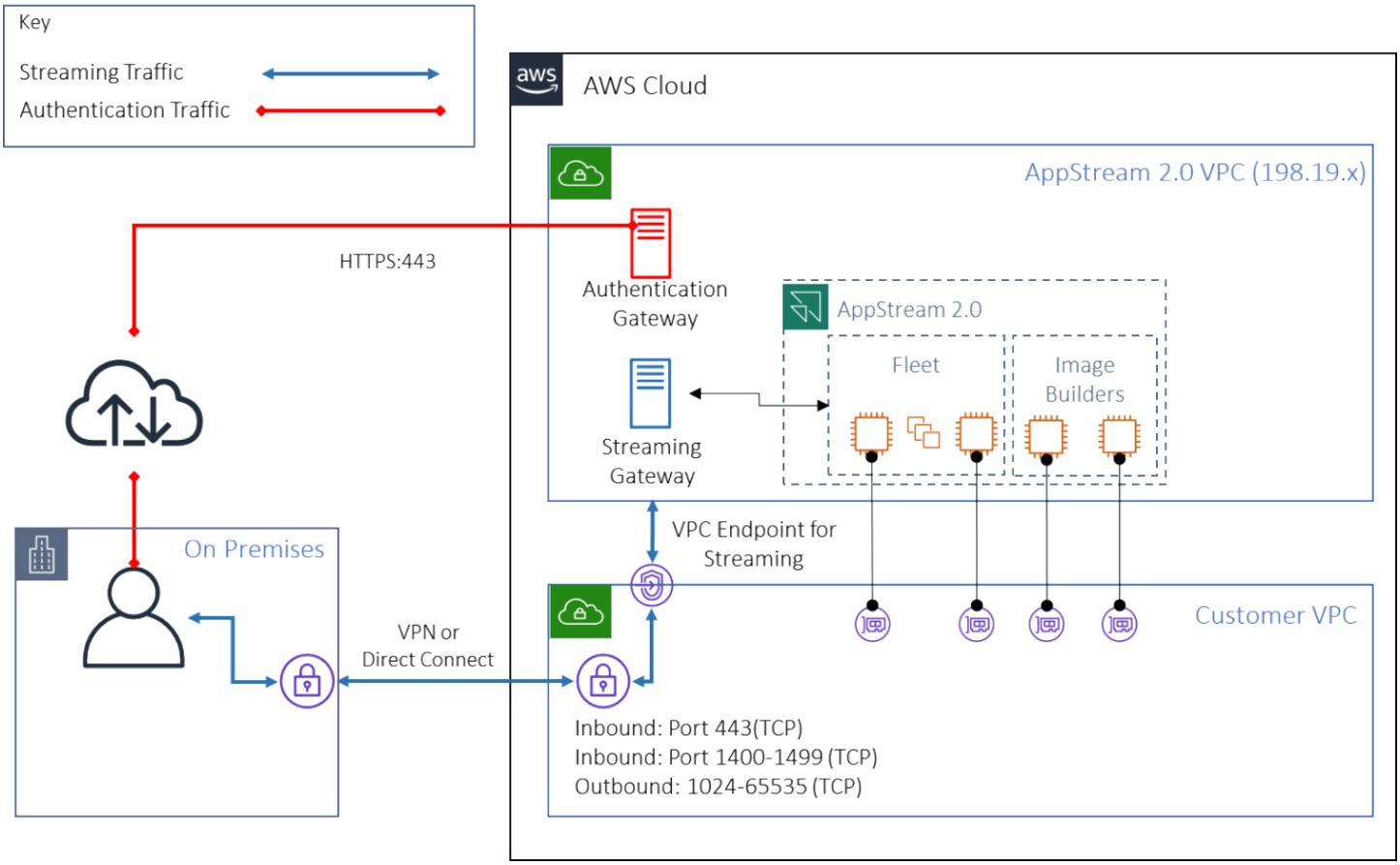
Example

Interface de API da Amazon WorkSpaces Applications VPC endpoint

Em cenários de design em que os comandos de API e CLI para WorkSpaces aplicativos da Amazon se originam em sua VPC, privatize essas chamadas programáticas por meio de uma interface VPC endpoint.

Endpoint VPC da interface de streaming de WorkSpaces aplicativos da Amazon

Embora seja possível rotear o tráfego de streaming do Amazon WorkSpaces Applications por meio de uma interface VPC endpoint, use essa configuração com cuidado. O comportamento padrão de streaming pela Internet pública é o método de entrega mais eficiente e eficiente para o tráfego de streaming da Amazon WorkSpaces Applications.



Endpoint VPC da interface de streaming de WorkSpaces aplicativos da Amazon

Conforme mostrado na figura anterior, a Internet pública é o caminho mais eficiente para os Amazon WorkSpaces Applications Streaming Gateways. O roteamento por meio da VPC e da rede gerenciadas pelo cliente aumenta a complexidade e a latência. Ele também adiciona taxas de transferência de dados da Direct Connect.

> **Note**
>
> Somente o streaming é compatível com o endpoint da VPC, e a autenticação ainda deve ocorrer na Internet pública. O acesso pré-requisito, como o SAML Single Sign-On (SSO) Identity Provider (IdP), continua sendo um requisito acessível somente pela Internet pública.

Criação e gerenciamento de imagens

Ao iniciar uma frota ou um construtor de imagens em WorkSpaces Aplicativos, você deve selecionar uma das imagens base dos WorkSpaces Aplicativos. Em seguida, os administradores podem criar a imagem base para adicionar seus próprios aplicativos e configurações.

Há considerações importantes ao criar uma imagem para garantir que os aplicativos funcionem corretamente e com segurança. Além disso, há considerações de design sobre como a imagem será mantida.

Criando uma imagem WorkSpaces de aplicativos

Ao criar uma nova imagem, é importante considerar:

- Sistema operacional
- Aplicativos
- Perfis de usuário
- Segurança
- desempenho
- Versão do agente
- CLI do Image Assistant

Criando uma imagem WorkSpaces de aplicativos

Em novembro de 2021, a WorkSpaces Applications lançou suporte para o Amazon Linux 2. Com esse anúncio, os WorkSpaces aplicativos agora oferecem suporte a quatro tipos de plataforma:

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

É possível que você precise escolher uma plataforma específica com base no que é exigido pelo seu aplicativo (por exemplo, se o aplicativo exigir o Windows, o Amazon Linux 2 não será uma opção).

Além dos requisitos do aplicativo, consulte a seguinte matriz de comparação para ajudar você a escolher qual tipo de plataforma melhor se adapta ao seu caso de uso e ambiente:

Tabela 1: tipos de plataformas, quando usá-las e preços

Tipos de plataforma	Quando usar	Preços da frota*
Windows Server (2012 R2, 2016 ou 2019)	O aplicativo pode ser executado somente no Windows (e não é compatível com o Amazon Linux 2). Você quer ingressar no domínio de suas instâncias de streaming. Você deseja usar a Política de Grupo existente nas instâncias de streaming de seus WorkSpaces aplicativos (o Linux não adere à Política de Grupo, mas você pode usar scripts de sessão para automatizar a configuração quando uma sessão é iniciada). Você usará a Visualização de área de trabalho e seus usuários vão preferir a experiência de área de trabalho do Windows. Você prefere usar o aplicativo Image Assistant, que fornece um assistente passo a passo, para criar o catálogo e a imagem do aplicativo. No momento, você deve criar sua imagem do Amazon Linux 2 usando comandos de terminal (consulte este tutorial para obter mais informações). Você	Taxa RDS SAL (Microsoft Remote Desktop Services Subscriber Access License) de 4,19 USD por mês para cada usuário exclusivo** mais o seguinte: 1. $0,10 por hora para frotas Always-On On-Demand 2. 0,15 USD por hora para frotas elásticas

Tipos de plataforma	Quando usar	Preços da frota*
	deseja usar a persistência das configurações do aplicativo. Atualmente, não há suporte para a ativação da persistência das configurações do aplicativo em Linux-based pilhas.	
Amazon Linux 2	Você quer aproveitar as instâncias de streaming de menor custo e evitar taxas de licença de RDS SAL. Os aplicativos são compatíveis com o Amazon Linux 2	As instâncias Linux têm um custo mais baixo em comparação com as instâncias do Windows. Com o Linux, você não paga taxas de RDS SAL e as seguintes taxas por hora: 1. $0,084 por hora para frotas Always-On On-Demand 2. 0,112 USD por hora para frotas elásticas

* Com base em stream.standard.medium na região norte da Virgínia

** Clientes qualificados podem trazer sua própria licença para eliminar as taxas de SAL RDS da AWS. Consulte a página de preços dos WorkSpaces aplicativos para obter mais detalhes. Os clientes da área de educação também podem receber um preço especial. Escolas, universidades e determinadas instituições públicas podem ter uma taxa de usuário reduzida do Microsoft RDS SAL.

Aplicativos

Antes de instalar os aplicativos, é importante analisar os requisitos, como dependências e requisitos de hardware. Depois de instalar com sucesso os aplicativos nas instâncias do construtor de imagens, troque de usuário e teste os aplicativos no contexto do usuário de teste.

Ao planejar a implantação do aplicativo, esteja ciente de endpoints e cotas do serviço. Além disso, limpe os arquivos do instalador e do auxiliar para otimizar o espaço total da unidade C antes de

criar uma imagem. Como lembrete, as instâncias do WorkSpaces Applications têm um volume de tamanho fixo de 200 GB. A otimização do espaço em disco após as instalações é uma prática recomendada para garantir que o volume de tamanho fixo nunca seja excedido.

Se você quiser modificar o catálogo de aplicativos que os usuários podem acessar em tempo real, a estrutura dinâmica de aplicativos fornece operações de API. Os aplicativos gerenciados pelos provedores de aplicativos dinâmicos podem estar dentro da imagem ou podem estar fora da instância, como em um compartilhamento de arquivos do Windows ou uma tecnologias de virtualização de aplicativos. Esse recurso requer uma frota de WorkSpaces aplicativos associada a um domínio do Microsoft Active Directory. Para obter mais informações, consulte Usando o Active Directory com WorkSpaces aplicativos.

Blocos de aplicativos

Os blocos de aplicativos representam o script de configuração e os arquivos necessários para iniciar os aplicativos que seus usuários usarão. O disco rígido virtual (VHD) pode ser qualquer objeto do Amazon S3. É recomendado que esse objeto tenha menos de 1,5 GB, pois ele precisa ser totalmente baixado antes que o usuário possa acessar o aplicativo.

Como otimizar os blocos de aplicativos

Para Windows-based frotas, é recomendável criar um arquivo VHDX para conter seu aplicativo. Para Linux-based frotas, é recomendável criar uma imagem (IMG). Esses discos virtuais devem ser criados com o menor tamanho possível para hospedar os arquivos do aplicativo. Os discos virtuais podem ser compactados para diminuir ainda mais o tamanho. No script de configuração, você precisará descompactar o disco antes de montar. O exemplo de script PowerShell de configuração do Windows tem a funcionalidade de descompactação incluída. Há uma compensação entre a expansão de um arquivo (zip) e a velocidade de download. Alguns testes podem ser necessários para encontrar um equilíbrio que ofereça o tempo de inicialização mais rápido do aplicativo.

Atualizar aplicativos

Os aplicativos podem ter alterações menores e maiores. Para pequenas atualizações, use habilitar versionamento no bucket do Amazon S3 que hospeda os arquivos de blocos de aplicações. Essa configuração permite que os administradores retornem às versões anteriores de um aplicativo específico alterando a versão do objeto VHD do aplicativo em questão sem alterar a configuração do bloco de aplicações. Com as principais atualizações, crie um novo bloco de aplicações para o VHD atualizado. Dessa forma, os administradores poderão separar as principais alterações do aplicativo

no nível do bloco de aplicações em oposição ao nível do controle de versão, o que fornece uma abordagem mais organizada para o gerenciamento administrativo de aplicativos.

Personalização de perfil do usuário

O Amazon WorkSpaces Applications é, por definição, uma solução não persistente de aplicativos e desktops. Quando uma sessão de usuário é encerrada, as alterações do sistema e do usuário também são encerradas. Ative a persistência das configurações do aplicativo somente quando necessário. Isso pode adicionar sobrecarga ao processo de login e considerações de custo para o armazenamento do S3 necessário.

Em situações em que a persistência das configurações do aplicativo é necessária, AWS recomenda proteger essa conexão por meio de uma política personalizada e do endpoint do gateway S3 VPC. Avalie o tamanho geral das configurações do aplicativo e minimize as configurações salvas na persistência das configurações do aplicativo para otimizar o custo e o desempenho.

A personalização do perfil do usuário pode ser configurada em uma instância do WorkSpaces Applications Image Builder. Isso inclui adicionar e modificar chaves de registro, adicionar arquivos e outras configurações específicas do usuário. No WorkSpaces Applications Image Assistant, há uma opção para criar um perfil de usuário. Assim, é possível copiar o perfil de usuário do modelo para o perfil de usuário padrão. Depois que a imagem for implantada em uma frota, os usuários finais que transmitem sessões dela terão seu perfil de usuário criado a partir do perfil de usuário padrão. É importante considerar a minimização do tamanho do perfil do usuário, principalmente quando a persistência das configurações do aplicativo está ativada. Por padrão, o tamanho máximo do VHDx para o perfil do usuário é de 1 GB. Sempre que uma sessão de streaming é iniciada, um arquivo VHDx de perfil de usuário é baixado de um bucket do S3. Isso aumenta o tempo de preparação da sessão de streaming e apresenta o risco de exceder o limite, o que causará uma falha na montagem do perfil do usuário usando o arquivo VHDx.

Para casos de uso que exigem um perfil de usuário com mais de 1 GB, a AWS recomenda o uso de métodos alternativos para armazenar perfis. Por exemplo, usando perfis de roaming ou contêineres de perfil FSLogix em armazenamento compartilhado, como Amazon FSx para Windows File Server. Para obter mais informações, consulte Usar o Amazon FSx for Windows File Server e o FSLogix para otimizar a persistência das configurações do aplicativo nos aplicativos da Amazon. WorkSpaces

Segurança

Há diferentes medidas de segurança que os desenvolvedores precisam considerar. WorkSpaces Os administradores de aplicativos são responsáveis por instalar e manter as atualizações para

o sistema operacional Windows, seus aplicativos e suas dependências. Para obter orientação adicional sobre como manter as imagens básicas atualizadas, consulte Mantenha a imagem do seu WorkSpaces aplicativo Up-to-Date para obter orientações adicionais sobre como manter as imagens base atualizadas.

Por padrão, os WorkSpaces aplicativos permitem que usuários ou aplicativos iniciem qualquer programa na instância, além do especificado no catálogo de aplicativos de imagem. Isso é útil quando o aplicativo depende de outro como parte de um fluxo de trabalho, mas você não quer que o usuário possa iniciar esse aplicativo dependente de modo direto. Por exemplo, o aplicativo inicia o navegador para fornecer instruções de ajuda no site do fornecedor do aplicativo, mas você não quer que o usuário inicie o navegador diretamente. Em algumas situações, talvez você queira controlar quais aplicativos podem ser executados nas instâncias de streaming. A Microsoft AppLocker é um software de controle de aplicativos que usa políticas de controle explícitas para habilitar ou desabilitar quais aplicativos um usuário pode executar.

O software antivírus pode afetar adversamente as sessões de streaming e as instâncias do criador de imagens. AWS recomenda que você não habilite as atualizações automáticas para o software antivírus. Para obter mais informações sobre o Windows Defender, consulte Software antivírus.

desempenho

Antes de criar uma nova imagem, é importante testar os aplicativos como usuário de teste. Com o teste, é possível garantir que os aplicativos possam ser executados em um contexto de usuário não administrador. Além disso, verifique o desempenho do aplicativo e a experiência do usuário usando ferramentas integradas, como o Gerenciador de Tarefas e o Monitor de Desempenho. É uma prática recomendada monitorar a utilização de recursos, como CPU, memória e memória da GPU. Em caso de restrição dos recursos da memória de CPU, memória ou GPU, considere atualizar o tipo de instância. Para melhorar o desempenho:

- Desative janelas pop-up do navegador
- Desative a segurança aprimorada do IE

WorkSpaces Seleção da versão do agente de aplicativos

Ao criar uma nova imagem, você pode optar por usar o software agente de WorkSpaces aplicativos mais recente ou não atualizá-lo. Cada versão do software do agente WorkSpaces Applications inclui correções de erros e aprimoramentos de recursos. Mantenha a imagem com o software mais atualizado. Analise os mecanismos para isso na seção Atualizações de imagem deste documento.

Você pode escolher a opção Usar o agente mais recente. Essa opção garante que, na inicialização, o agente de WorkSpaces aplicativos mais recente esteja sempre instalado. No entanto, mudanças inesperadas podem afetar as experiências do usuário, e uma atualização do agente pode aumentar o tempo de inicialização de uma instância. A atualização de uma imagem base exige a recriação da imagem. Também é importante que você realize testes antes de distribuir a imagem atualizada para produção a fim de minimizar o tempo de inicialização.

Interface de linha de comandos (CLI) do Image Assistant

Para desenvolvedores que desejam automatizar ou criar programaticamente imagens de WorkSpaces aplicativos, use a CLI do Image Assistant. Isso está disponível em criadores de imagens com o software WorkSpaces Applications Agent lançado em ou após 26 de julho de 2019. A visão geral de alto nível a seguir descreve o processo de criação programática de uma WorkSpaces imagem de aplicativos:

1. Use sua automação de instalação de aplicativos para instalar os aplicativos necessários em seu construtor de imagens. Essa instalação pode incluir os aplicativos que seus usuários iniciarão, quaisquer dependências e aplicativos em segundo plano.
2. Determine os arquivos e as pastas a serem otimizados.
3. Se aplicável, use a operação `add-application` CLI do Image Assistant para especificar os metadados do aplicativo e o manifesto de otimização para a imagem do WorkSpaces Applications.
4. Para especificar aplicativos adicionais para a imagem de WorkSpaces Aplicativos, repita as etapas de 1 a 3 para cada aplicativo, conforme necessário.
5. Se aplicável, use a operação `update-default-profile` da CLI do Image Assistant para substituir o perfil padrão do Windows e criar configurações padrão de aplicativo e do Windows para seus usuários.
6. Use a operação `create-image` da CLI do Image Assistant para criar a imagem.

Para obter mais informações, consulte Criar a imagem do seu WorkSpaces aplicativo de forma programática usando as operações da CLI do Image Assistant.

Como gerenciar a experiência de streaming dos usuários

Personalização usando scripts de sessão

WorkSpaces Os aplicativos fornecem scripts de sessão na instância. Você pode usar esses scripts para executar seus próprios scripts personalizados quando eventos específicos ocorrerem em sessões de streaming dos usuários. Por exemplo, você pode usar scripts personalizados para preparar seu ambiente de WorkSpaces aplicativos antes do início das sessões de streaming dos usuários. Você também pode usar scripts personalizados para limpar instâncias de streaming depois que os usuários concluem as sessões de streaming.

Especifique scripts de sessão em uma imagem de WorkSpaces aplicativos. Para obter mais informações sobre como configurar scripts de sessão, consulte a seção do guia de administração sobre o uso de scripts de sessão para gerenciar a experiência do usuário. Usado com um compartilhamento de rede ou perfil AWS Identity and Access Management (IAM), você pode usar scripts de sessão para recuperar scripts adicionais de um local de armazenamento. Com esse script adicional, você pode otimizar mais a experiência do usuário. Isso pode minimizar o número de imagens e frotas necessárias para fornecer ambientes de aplicativos aos usuários.

Como usar a Política de grupo do Active Directory

Se você planeja usar frotas de WorkSpaces aplicativos em um domínio do Active Directory, você pode usar objetos de políticas de grupo (GPOs) para gerenciar a experiência do usuário. Os GPOs podem ser atribuídos à Unidade Organizacional (OU) na qual as instâncias de WorkSpaces aplicativos são criadas. Para simplificar a criação de imagens, inicie a imagem básica dos WorkSpaces aplicativos em uma OU que bloqueia a herança. Isso evita que outras políticas de domínio afetem as experiências do usuário dos WorkSpaces aplicativos. Implante cada frota em sua OU dedicada, com GPOs exclusivos, estabelecendo o ambiente, permitindo o benefício consolidado de um para muitos do gerenciamento de imagens de WorkSpaces aplicativos.

Um exemplo de uso da Política de Grupo é especificar o conjunto de imagens de diferentes páginas iniciais do Internet Explorer para cada frota de WorkSpaces aplicativos.

Atualizações de imagem

A aplicação de patches de software é essencial para a segurança e o desempenho dos recursos computacionais. A aplicação frequente de patches está listada como uma prática recomendada no Pilar de Segurança da Well-Architected Estrutura.

Quando sua imagem é criada e implantada, há quatro categorias de software que exigem patches na imagem de seus WorkSpaces aplicativos:

- Aplicativos e dependências: você é responsável por corrigir os aplicativos e dependências em suas imagens.
- Sistema operacional Microsoft Windows: você é responsável por instalar e manter as atualizações do Windows.
- Componentes de software — São drivers, agentes e outros softwares necessários para a operação de WorkSpaces aplicativos (por exemplo, o CloudWatch agente da Amazon). WorkSpaces Os aplicativos lançam periodicamente novas imagens básicas que contêm novos agentes e drivers. Você pode reconstruir sua imagem usando a base mais recente para levar os componentes de software em suas imagens à linha de base mais recente. O processo para recriar uma imagem usando a base mais recente pode ser demorado e complicado quando há muitos aplicativos, ou com instalações complexas de aplicativos.
- WorkSpaces Agente de aplicativos — Você pode escolher Sempre usar a versão mais recente do agente no Image Assistant. Com essa opção, as instâncias de streaming executadas a partir da imagem usam automaticamente a versão mais recente do agente.

Você pode manter a imagem de seus WorkSpaces aplicativos atualizada fazendo o seguinte:

- Atualizar uma imagem usando atualizações de imagem de WorkSpaces aplicativos gerenciados — Esse método de atualização fornece as atualizações mais recentes do sistema operacional e do driver do Windows e o software mais recente do agente de WorkSpaces aplicativos. Esse método gerenciado atualiza os componentes do serviço e do sistema operacional da Microsoft, mas não permite que você atualize os componentes do aplicativo. É uma prática recomendada usar esse método quando as instalações do aplicativo são complexas ou exigem configuração manual.
- Atualize o software do WorkSpaces Applications Agent usando versões de imagem de WorkSpaces aplicativos gerenciados — Esse método de atualização fornece o software mais recente do agente de WorkSpaces aplicativos. Esse método permite que você atualize os componentes do aplicativo.

Personalização da frota

Tipo de frota

Ao criar uma frota, os clientes devem escolher um tipo. Cada tipo de frota oferece benefícios diferentes para a experiência do usuário, custos e despesas gerais de manutenção. Independentemente do tipo de frota escolhido, cada opção é compatível com os tipos de plataforma Windows e Linux, bem como o Desktop View ou o Application View.

Os clientes já podem escolher entre os seguintes tipos de frota:

- Always-On— Esse tipo de frota fornece aos usuários acesso instantâneo aos seus aplicativos. Você será cobrado por todas as instâncias em execução na frota, mesmo se nenhum usuário estiver fazendo streaming de aplicativos.
- On-Demand— Selecione esse tipo de frota para otimizar seus custos de streaming. Com uma frota sob demanda, os usuários terão um horário de início de aproximadamente um a dois minutos para a sessão. No entanto, você só pagará as taxas da instância de streaming quando os usuários estiverem conectados e uma pequena taxa horária para cada instância da frota que não seja um aplicativo de streaming.
- Elástica: as frotas elásticas podem ser usadas para aplicativos que não exigem instalação e podem ser executados a partir de um disco rígido virtual (VHD). As frotas elásticas não oferecem suporte a imagens de WorkSpaces aplicativos, nem exigem políticas de escalabilidade. Você será cobrado apenas pela duração de uma sessão de streaming.

Tabela 2 — Tipos de frota de WorkSpaces aplicativos da Amazon

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
Always-On	Os usuários precisam de acesso instantâneo aos aplicativos quando	Acesso instantâneo aos aplicativos	Você paga o preço total por cada instância disponível na frota (independ	Oferece suporte a políticas personalizadas de imagem e de ajuste de escala.

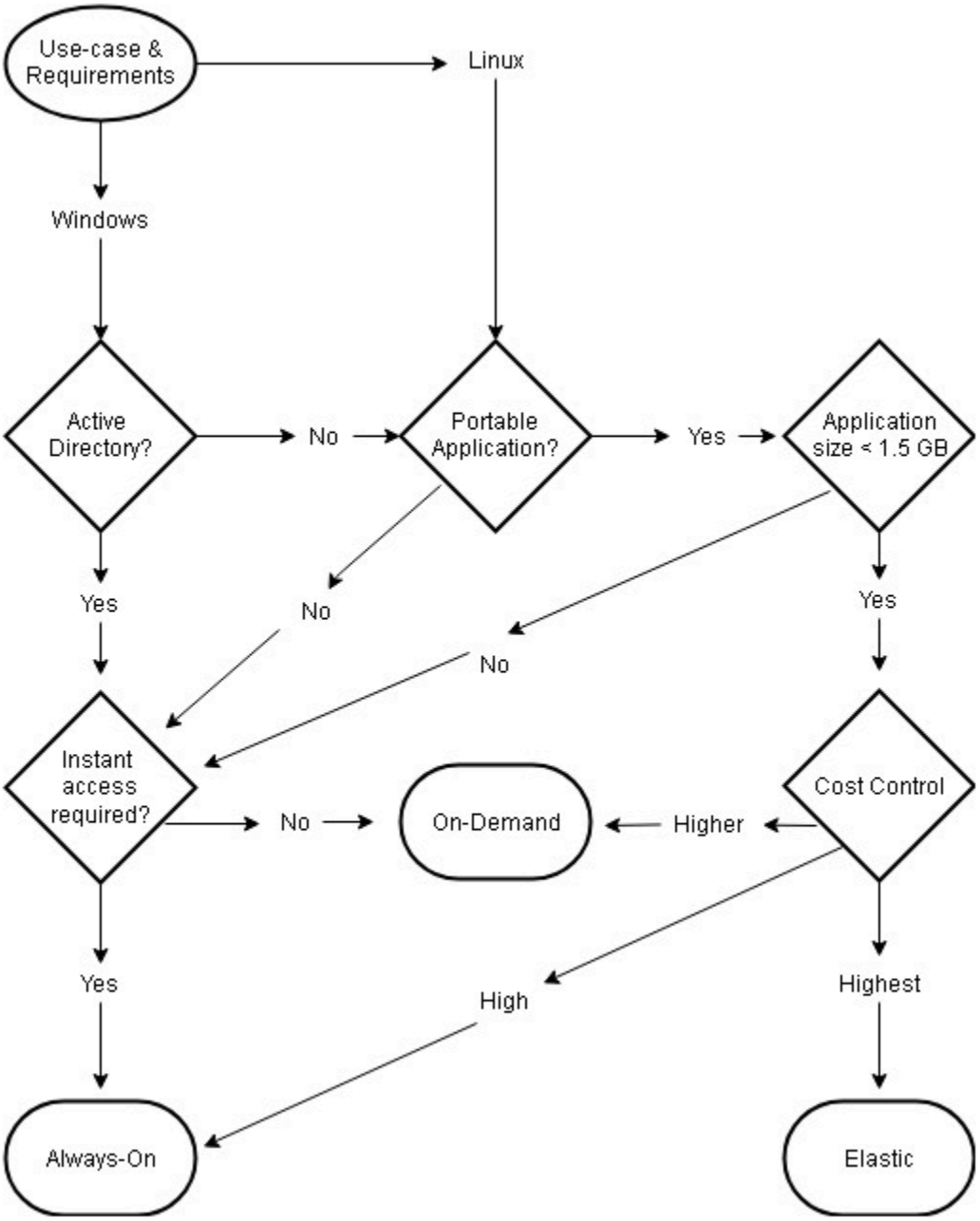
Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
	iniciam uma sessão. Você não terá excesso significativo de capacidad e em sua frota, talvez porque os padrões de uso sejam previsíve is e seja possível controlar os custos de modo confiável com políticas de ajuste de escala.		entemente de ser usada para uma sessão).	

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
On-Demand	Você deve manter um excesso significativo de capacidade em suas frotas. Você quer o ambiente mais econômico e não quer pagar o preço total pela capacidade não utilizada. Os usuários podem esperar de um a dois minutos para acessar os aplicativos depois de iniciar uma sessão. Você está usando tipos de instância maiores. O custo por hora de uma instância em execução é muito mais caro do que a taxa de instância interrompida.	Os usuários esperam de um a dois minutos para acessar os aplicativos depois de iniciar uma sessão.	Você paga o preço total somente pelas instâncias de streaming com uma sessão ativa e, em seguida, um pequeno custo por hora pelas instâncias ociosas.	Oferece suporte a políticas personalizadas de imagem e escalabilidade.

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
Elástica	O aplicativo e suas dependências têm menos de ~1,5 GB. Sempre que um usuário inicia uma sessão em uma frota elástica, seu arquivo de disco rígido virtual (VHD) deve ser baixado do Amazon S3 para a sessão. Como resultado, arquivos de VHD maiores (ou seja, com mais de 1,5 GB) resultarão em uma experiência inadequada para o usuário final. O aplicativo é portátil. Ou seja, seu aplicativo e todas as suas dependências podem ser colocados em um VHD e lançados a partir	O usuário espera de 45 segundos a três minutos para acessar os aplicativos após iniciar a sessão (o tempo de espera depende do tamanho do disco rígido virtual).	Você será cobrado apenas pela duração de uma sessão de streaming. Como não existe o conceito de instâncias ociosas com frotas elásticas, você não incorre em cobranças por instâncias não utilizadas.	Não há suporte a imagens personalizadas (o cliente fornece aplicativos ao VHD) nem a políticas de ajuste de escala. Atualmente, dá suporte para instâncias de `stream.standard.small` e `stream.standard.medium`. Se seu caso de uso exigir um tipo de instância diferente, entre em contato com a equipe da sua AWS conta.

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
	de instâncias de streaming VHD.You não obrigatórias associadas ao domínio (atualmente, a união de domínios não está disponíve l com frotas da Elastic). Você deseja pagar somente pelas sessões ativas (ou seja, você não paga pela capacidade não utilizada em sua frota) .Seus usuários podem esperar 45 segundos ou mais para acessar seus aplicativos após iniciar uma sessão.Vo cê quer que a AWS gerencie a escalabilidade para você (sem escalabilidade)			

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
	políticas para gerenciar).			



Dimensionamento da frota

Capacidade mínima e ajuste da escala programado

Ao dimensionar sua frota de WorkSpaces aplicativos, há várias considerações que se traduzem diretamente na experiência e no custo do usuário. O valor inserido para Capacidade mínima garante que o número de instâncias de WorkSpaces aplicativos raramente seja menor que esse valor. Após o término de uma sessão de WorkSpaces aplicativos, se o total de instâncias de WorkSpaces aplicativos for menor que o valor mínimo da capacidade, uma nova instância de frota será iniciada. Como sempre, é importante lembrar que uma instância de WorkSpaces aplicativos é mapeada diretamente para uma sessão de usuário, influenciando diretamente o valor da capacidade mínima.

Inserir um valor para a capacidade mínima que esteja além da simultaneidade prevista resulta em aumento de custo, embora a experiência do usuário não seja afetada. Um valor muito baixo resulta em custos reduzidos, mas afeta a experiência do usuário quando o total de solicitações excede a capacidade disponível. Os administradores observarão erros de “Capacidade insuficiente” nesse tipo de situação. Por exemplo, esperar `PendingCapacity` se tornar `AvailableCapacity` é um uso ineficiente do tempo do usuário quando o número de conexões previstas no início do dia é um valor previsivelmente consistente.

Comece com uma capacidade mínima que acomode os horários típicos fora de pico e, em seguida, use a política de ajuste de escala programada para redefinir efetivamente a capacidade mínima antes do início do dia de trabalho. Não se esqueça de criar outra política de ajuste de escala programada para reverter a capacidade mínima para os horários fora do pico. Para obter mais informações sobre políticas de ajuste de escala e como implementá-las, consulte a seção Estratégias de ajuste de escala automático de frotas neste documento.

Capacidade máxima e cotas de serviço

A definição da capacidade máxima pode parecer um valor arbitrário, mas quando previsto e definido adequadamente, otimiza o consumo e o custo total dos recursos. Um valor inserido que seja maior do que a cota de serviço da frota de WorkSpaces aplicativos em sua Conta da AWS pode parecer válido, mas, quando eventos de auto scaling tentam escalar recursos até a capacidade máxima, eles não são iniciados, pois o valor da capacidade máxima excede a cota de serviço disponível. Garanta que uma solicitação de cota de serviço exista para a capacidade máxima desejada, garantindo as funções de ajuste de escala automático conforme previsto pela sua organização.

Outra consideração importante ao definir um valor máximo de capacidade é o custo. Para obter mais informações, consulte a seção Como otimizar custos com a escolha do tipo de frota deste documento.

Como escolher a exibição da área de trabalho ou do aplicativo

A determinação de escolher uma exibição de aplicativo ou de desktop não tem impacto no desempenho ou no custo. Somente uma visualização está acessível a qualquer momento por frota de WorkSpaces aplicativos. Você pode alterar a opção de Exibição do stream. Planeje essa mudança fora do horário comercial de pico, pois a mudança da exibição do stream exige a reinicialização da frota.

Não há uma única prática recomendada para a exibição de streams. O impacto das opções de exibição do stream é resumido da seguinte forma:

- Relatórios detalhados sobre o uso do aplicativo por meio do atributo Relatórios de uso para administradores
- Experiência geral e fluxo de trabalho para usuários finais (por exemplo, um desktop completo atende às necessidades do caso de uso ou somente a visualização dos aplicativos é suficiente?).

Exibição da área de trabalho

Para casos de uso em que todo o fluxo de trabalho do usuário é executado em sessão, a Exibição da área de trabalho simplifica a experiência do usuário, mantendo todos os aplicativos focados em um único ambiente. A Exibição da área de trabalho pode oferecer uma experiência de usuário mais consistente para implantações de mais de três a cinco aplicativos que exigem integração com o sistema operacional (SO). Ela é eficaz ao manter dois ambientes separados e distintos. Por exemplo, um usuário pode ter acesso simultâneo a um ambiente de área de trabalho de produção e pré-produção para validar alterações no layout, na configuração e no acesso ao aplicativo.

WorkSpaces Os Relatórios de Uso de Aplicativos criam um relatório diário de aplicativos para o Desktop View. A saída resultante para o aplicativo é simplesmente “desktop”, mapeada diretamente para a sessão de WorkSpaces aplicativos. Para obter mais informações, consulte a seção Monitoramento do uso pelo usuário deste documento.

Exibição somente de aplicativos

A visualização Somente aplicativos também é eficaz quando a pilha de WorkSpaces aplicativos se destina a fornecer alguns aplicativos que são necessários de forma intermitente. Em ambientes de

quiosque, uma entrega segura de aplicativos é fornecida por meio da Exibição de aplicativos. Com o Application View, os WorkSpaces aplicativos substituem o shell padrão do Windows por um shell personalizado. Esse shell personalizado apresenta apenas aplicativos em execução, minimizando a superfície de ataque do sistema operacional.

Para casos de uso em que os WorkSpaces aplicativos são usados para aumentar o ambiente de desktop de uma organização existente, a visualização Somente aplicativos é preferida. Implante os WorkSpaces aplicativos Windows Client no modo de aplicativo nativo para minimizar a confusão do usuário, permitindo o uso total dos atalhos do teclado.

O Amazon WorkSpaces Applications Usage Reports cria um relatório diário do aplicativo para visualização do aplicativo. Para obter relatórios mais detalhados sobre o uso de aplicativos e execuções, considere uma solução de terceiros para gerar relatórios no nível do sistema operacional. Você pode usar a Microsoft AppLocker no modo de relatório ou considerar soluções que estão disponíveis no AWS Marketplace, como o Stratusphere UX da Liquidware.

AWS Identity and Access Management configuração de função

Se uma carga de trabalho exigir que os usuários finais dos WorkSpaces aplicativos acessem outros AWS serviços de dentro da sessão, é uma prática recomendada delegar o acesso por meio do uso de funções AWS Identity and Access Management (IAM). Os perfis do IAM podem ser vinculados diretamente à sessão do seu usuário final por meio da atribuição no nível da frota. Para obter mais práticas recomendadas ao usar funções do IAM com WorkSpaces aplicativos, consulte esta seção do guia do administrador.

Uso de credenciais estáticas

Algumas cargas de trabalho podem exigir entradas estáticas para as chaves de acesso do IAM, em vez de herdá-las da função anexada. Há dois métodos para receber essas credenciais. O primeiro método envolve armazenar as chaves de acesso em um AWS serviço e, em seguida, dar aos usuários finais acesso explícito ao IAM para extrair esse valor específico do serviço. Dois exemplos de mecanismos de armazenamento de chaves de acesso estão usando o AWS Secrets Manager ou a AWS SSM Parameter Store. O segundo método é usar o provedor de credenciais de WorkSpaces aplicativos para acessar as chaves de acesso da função anexada. Isso pode ser feito invocando o provedor de credenciais e analisando a saída da chave de acesso e da chave secreta. Veja a PowerShell seguir um exemplo de como realizar essa ação.

```
$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
```

Protegendo seu WorkSpaces bucket S3 de aplicativos

Se a carga de trabalho de seus WorkSpaces aplicativos estiver configurada com a Home Folder and/or Application Persistence, é uma prática recomendada proteger o bucket do Amazon S3 no qual os dados persistentes estão sendo armazenados contra acesso não autorizado ou exclusão acidental. A primeira camada de proteção é adicionar uma política de bucket do Amazon S3 para evitar a exclusão acidental do bucket. A segunda camada de proteção é adicionar uma política de bucket que se alinhe ao princípio privilégio mínimo. O alinhamento ao princípio pode ser feito permitindo que apenas partes necessárias acessem o bucket.

Estratégias de ajuste de escala automático da frota

Compreendendo WorkSpaces as instâncias de aplicativos

WorkSpaces As instâncias da frota de aplicativos têm uma proporção de 1:1 de usuário/instância da frota. Isso significa que cada usuário tem sua própria instância de streaming. O número de usuários conectados simultaneamente determinará o tamanho da frota.

Políticas de ajuste de escala

WorkSpaces As frotas de aplicativos são lançadas em um grupo de Application Auto Scaling. Isso permite que a frota seja dimensionada com base no uso para atender à demanda. À medida que o uso aumenta, a frota aumenta a escala automaticamente e, à medida que os usuários se desconectam, a frota reduz. Isso é controlado pela definição de políticas de ajuste de escala. Você pode definir políticas de ajuste de escala com base em agendamento, em etapas e acompanhamento de meta. Para obter mais informações sobre essas políticas de escalabilidade, consulte Fleet Auto Scaling for Amazon WorkSpaces Applications.

Ajuste de escala em etapas

Essas políticas aumentam ou diminuem a capacidade da frota em uma porcentagem do tamanho atual dela ou em um número específico de instâncias. As políticas de escalabilidade de etapas são acionadas pelas CloudWatch métricas de WorkSpaces aplicativos de`Capacity Utilization`,`Available Capacity`, ou`Insufficient Capacity Errors`.

Ao usar políticas de escalabilidade por etapas, AWS recomenda que você adicione uma porcentagem da capacidade e não um número fixo de instâncias. Dessa forma, as ações de ajuste de escala são proporcionais ao tamanho da frota. Isso evitará situações em que você aumenta a escala horizontalmente muito devagar (porque adicionou um pequeno número de instâncias em relação ao tamanho da frota) ou muitas instâncias quando a frota é pequena.

Monitoramento do objetivo

Com essa política, especifica um nível de utilização da capacidade para a frota. O escalonamento automático de aplicativos cria e gerencia CloudWatch alarmes que acionam a política de escalabilidade. Isso adiciona ou remove a capacidade de manter a frota no valor de destino

especificado ou próximo a ele. Para garantir a disponibilidade do aplicativo, a frota é expandida proporcionalmente à métrica o mais rápido possível, mas é reduzida gradualmente. Ao configurar o acompanhamento de metas, considere o tempo de espera da escala para garantir que o aumento e a redução ocorram nos intervalos desejados.

O acompanhamento de metas é eficaz para situações de alta rotatividade. A rotatividade ocorre quando um grande número de usuários inicia ou encerra sessões em um curto período de tempo. Você pode identificar a rotatividade examinando CloudWatch as métricas da sua frota. Períodos de tempo em que sua frota tem capacidade pendente diferente de zero sem alteração (ou com muito pouca alteração) na capacidade desejada indicam que é provável ocorrer uma alta rotatividade. Em situações de alta rotatividade, configure políticas de acompanhamento de metas em que (100 — porcentagem de utilização alvo) seja maior do que a taxa de rotatividade em um período de 15 minutos. Por exemplo, se 10% da frota for encerrada em 15 minutos devido à rotatividade de usuários, defina uma meta de utilização da capacidade de 90% ou menos para compensar a alta rotatividade.

Scheduled-based escalonamento

Com essas políticas, é possível definir a capacidade desejada da frota usando como base um cronograma de tempo. Essa política é efetiva quando você entende o comportamento conexão e pode prever mudanças na demanda.

Por exemplo, no início de um dia útil, você pode esperar que 100 usuários solicitem conexões de streaming às 9h. É possível configurar uma política de ajuste de escala com base em agendamento para definir o tamanho mínimo da frota como 100 às 8h40. Dessa forma, as instâncias da frota podem ser criadas e estar disponíveis no início do dia de trabalho, além de permitir que 100 usuários se conectem ao mesmo tempo. Em seguida, você pode definir outra política programada a fim de ajustar a escala da frota para um mínimo de dez às 17h. Isso permite que você economize custos, pois a demanda por sessões após o expediente é menor do que durante o dia de trabalho.

Políticas de ajuste de escala na produção

Você pode escolher combinar diferentes tipos de políticas de ajuste de escala em uma única frota, definindo políticas de ajuste de escala precisas para o comportamento do usuário. No exemplo anterior, você pode combinar a política de ajuste de escala programada com as políticas de acompanhamento de metas ou ajuste de escapa por etapa para manter um nível específico de utilização. A combinação da escalabilidade programada e da escalabilidade de rastreamento de destino pode ajudar a reduzir o impacto de um aumento acentuado nos níveis de utilização, quando a capacidade é necessária imediatamente.

Os usuários conectados às sessões de streaming quando uma política de escalabilidade altera o número desejado de instâncias não são afetados pela redução ou pelo aumento da escala horizontalmente. As políticas de ajuste de escala não encerrarão as sessões de streaming existentes. As sessões existentes continuarão ininterruptas até que a sessão seja encerrada pelo usuário ou por uma política de tempo limite da frota.

O monitoramento do uso de WorkSpaces aplicativos com CloudWatch métricas pode ajudar você a otimizar suas políticas de escalabilidade ao longo do tempo. Por exemplo, é comum provisionar recursos em excesso durante a configuração inicial e você pode perceber longos períodos de baixa utilização. Como alternativa, se a frota estiver subprovisionada, você poderá ver erros de utilização de alta capacidade e “Capacidade insuficiente”. A revisão CloudWatch das métricas pode ajudar a promover ajustes em suas políticas de escalabilidade para ajudar a mitigar esses erros. Para obter mais informações e exemplos de políticas de escalabilidade de WorkSpaces aplicativos que você pode usar, consulte Dimensione suas frotas de WorkSpaces aplicativos da Amazon.

Práticas recomendadas para ajuste de escala das políticas de design

Combinar políticas de ajuste de escala

Muitos clientes optam por combinar diferentes tipos de políticas de escalabilidade em uma única frota para aumentar a potência e a flexibilidade do Auto Scaling WorkSpaces em aplicativos. Por exemplo, você pode configurar uma política de ajuste de escala programada para aumentar o mínimo da frota às 6h, antes que os usuários comecem a trabalhar, e para diminuir o mínimo da frota às 16h, antes que os usuários parem de trabalhar. É possível combinar essa política de ajuste de escala programada com políticas de rastreamento de metas ou de ajuste de escala por etapas para manter um nível específico de utilização e aumentar, ou reduzir, a escala horizontalmente durante o dia para lidar com picos de uso. A combinação da escalabilidade programada e da escalabilidade de rastreamento de destino pode ajudar a reduzir o impacto de um aumento acentuado nos níveis de utilização, quando a capacidade é necessária imediatamente.

Evitar a rotatividade do ajuste de escala

Considere se a sua frota pode sofrer um alto grau de rotatividade devido ao seu caso de uso. A rotatividade ocorre quando um grande número de usuários inicia e encerra sessões em um curto período de tempo. Isso pode ocorrer quando muitos usuários acessam simultaneamente um aplicativo em sua frota por apenas alguns minutos antes da assinatura.

Nessas situações, o tamanho da frota pode ficar muito abaixo da capacidade desejada, pois as instâncias são encerradas quando os usuários encerram as sessões. As políticas de ajuste da escala por etapas podem não adicionar instâncias com rapidez suficiente para compensar a rotatividade e, como resultado, sua frota fica presa a um determinado tamanho.

Você pode identificar a rotatividade examinando CloudWatch as métricas da sua frota. Períodos de tempo em que sua frota tem capacidade pendente diferente de zero sem alteração (ou com muito pouca alteração) na capacidade desejada indicam que é provável ocorrer uma alta rotatividade. Com o objetivo de considerar situações de alta rotatividade, use políticas de ajuste de escala para acompanhamento de metas e escolha uma meta de utilização para que (100 - porcentagem de utilização alvo) seja maior do que a taxa de rotatividade em um período de 15 minutos. Por exemplo, se 10% da sua frota for encerrada em um período de 15 minutos devido à rotatividade de usuários, defina uma meta de utilização da capacidade de 90% ou menos para compensar a alta rotatividade.

Entender a taxa máxima de provisionamento

Clientes que gerenciam frotas de WorkSpaces aplicativos para um grande número de usuários devem considerar limites de taxa de provisionamento. Esse limite afetará a rapidez com que as instâncias podem ser adicionadas a uma frota ou a todas de uma Conta da AWS.

Há dois limites a serem considerados:

- Para uma única frota, o WorkSpaces Applications provisiona a uma taxa máxima de 20 instâncias por minuto.
- Por exemplo Conta da AWS, o WorkSpaces Applications provisiona a uma taxa de 60 instâncias por minuto (com um pico de 100 instâncias por minuto).

Se mais de três frotas forem ampliadas em paralelo, o limite da taxa de provisionamento da conta será compartilhado entre elas (por exemplo, seis frotas com ajuste de escala paralelo poderiam provisionar até 10 instâncias por minuto). Além disso, considere o tempo necessário para que uma determinada instância de streaming conclua o provisionamento em resposta a um evento de ajuste da escala. Para frotas não associadas a um domínio do Active Directory, isso normalmente demora 15 minutos. Para frotas unidas a um domínio do Active Directory, isso pode demorar até 25 minutos.

Por exemplo, considere estes cenários:

- Se você quiser escalar uma única frota de 0 a 1.000 instâncias, serão necessários 50 minutos (1.000 instances/20 instâncias por minuto) para que o provisionamento seja concluído e, em seguida, mais 15 a 25 minutos para que todas as instâncias estejam disponíveis para os usuários finais, totalizando 65 a 75 minutos.
- Se você quiser escalar simultaneamente três frotas de 0 a 333 instâncias (para um total de 999 instâncias no Conta da AWS), serão necessários aproximadamente 17 minutos (999/60instâncias por minuto) para que todas as frotas concluam o provisionamento e, em seguida, mais 15 minutos para que essas instâncias fiquem disponíveis para os usuários finais, totalizando 32 a 42 minutos.

Utilizar várias zonas de disponibilidade

Escolha várias AZs na região para a implantação da sua frota. Ao selecionar várias AZs para a frota, você aumenta a probabilidade dela ser capaz de adicionar instâncias em resposta a um evento de ajuste de escala. A CloudWatch métrica PendingCapacity é um ponto de partida para avaliar o quão otimizado é o projeto AZ da frota em grandes implantações de frotas. Um valor alto e sustentado de

PendingCapacity pode indicar a necessidade de estender a escala horizontal (entre AZs). Para obter mais informações, consulte Monitoramento de recursos de WorkSpaces aplicativos da Amazon.

Por exemplo, se o ajuste de escala automático tentar provisionar instâncias para aumentar o tamanho da frota e a AZ selecionada não tiver capacidade suficiente, o ajuste de escala automático adicionará instâncias nas outras AZs especificadas para sua frota. Para obter mais informações sobre zonas de disponibilidade e design de WorkSpaces aplicativos, consulte Zonas de disponibilidade neste documento.

Monitorar métricas de erro de capacidade insuficiente

“Erro de capacidade insuficiente” é uma CloudWatch métrica para frotas de WorkSpaces aplicativos. Esta métrica especifica o número de solicitações de sessão rejeitadas por falta de capacidade.

Ao fazer alterações em suas políticas de escalabilidade, é útil criar um CloudWatch alarme para notificá-lo quando ocorrerem erros de capacidade insuficiente. Assim, é possível ajustar rapidamente as políticas de ajuste de escala e otimizar a disponibilidade para os usuários. O guia de administração fornece etapas detalhadas para monitorar os recursos de seus WorkSpaces aplicativos.

Métodos de conexão

Ao transmitir sessões em WorkSpaces aplicativos, os usuários têm dois métodos de conexão disponíveis:

- Acesso ao navegador da Web — Qualquer HTML5-capable navegador é compatível. Não são necessários plug-ins ou downloads.
- WorkSpaces Aplicativos Windows Client

Como prática recomendada, considere os requisitos de atributos e dispositivos para o caso de uso do usuário a fim de alinhar qual navegador ou dispositivo atende melhor aos requisitos deles.

> **Note**
>
> WorkSpaces Não há suporte para aplicativos em dispositivos com resoluções de tela menores que 1024 x 768 pixels.

Resumo do suporte a atributos e dispositivos

Tabela 3: resumo do suporte a atributos e dispositivos

	Acesso pelo navegador da web	WorkSpaces Aplicativos Windows Client
Vários monitores (resolução de até 2K)	Compatível	Compatível
Vários monitores (resolução de até 4K)	N/A	Compatível
Suporte para tablets de desenho	Compatível*	Compatível
Suporte a dispositivos com tela sensível ao toque	Compatível	N/A

	Acesso pelo navegador da web	WorkSpaces Aplicativos Windows Client
Suporte para dispositivos com passagem de USB	N/A	Compatível
Atalhos de teclado	Compatível	Compatível
Deslocamento relativo do mouse	Compatível	Compatível
Transferência de arquivos	Compatível	Compatível
Redirecionamento de impressora local	N/A	Compatível
Redirecionamento de unidade local	N/A	Compatível
Web-cam apoio	Compatível	Compatível

*Somente Google Chrome e Mozilla Firefox

Acesso pelo navegador da web

WorkSpaces O acesso ao navegador da Web de aplicativos permite o acesso aos aplicativos sem a necessidade de instalar um cliente dedicado. Os usuários podem se conectar usando um HTML5-capable navegador compatível. Não requer nenhum plug-in ou extensão do navegador.

O acesso ao navegador da Web fornece uma ampla variedade de sistemas operacionais e tipos de dispositivos finais.

WorkSpaces Cliente de aplicativos para Windows

O cliente de WorkSpaces aplicativos para Windows é um aplicativo que você instala em seu PC com Windows. Esse aplicativo fornece recursos adicionais que não estão disponíveis quando você acessa os WorkSpaces aplicativos usando um navegador da web. Por exemplo, o cliente WorkSpaces Applications permite que você faça o seguinte:

- Use mais de dois monitores ou resolução 4K
- Use seus dispositivos USB com aplicativos transmitidos por meio WorkSpaces de Aplicativos
- Acesse as unidades e pastas locais durante sessões de streaming
- Redirecione trabalhos de impressão do aplicativo de streaming para uma impressora conectada ao computador local
- Use uma webcam local para conferências de áudio e vídeo nas sessões de streaming
- Use atalhos de teclado nos aplicativos acessados durante as sessões de streaming
- Interaja com seus aplicativos de streaming remotos da mesma forma que interage com os instalados localmente

WorkSpaces Modos de conexão do cliente de aplicativos

O cliente WorkSpaces Applications fornece dois modos de conexão: modo de aplicativo nativo e modo clássico. O modo de conexão escolhido determina as opções que estão disponíveis durante o streaming de aplicativos e como seus aplicativos de streaming funcionam e são exibidos. Os administradores podem controlar a capacidade dos usuários de alternar entre o modo de aplicativo nativo e o clássico.

- O modo clássico transmite aplicativos na janela de sessão de WorkSpaces aplicativos. Isso é semelhante à forma como os usuários finais transmitem aplicativos em um navegador da web. Use o modo clássico se os usuários finais preferirem transmitir aplicativos da mesma forma que os navegadores, ao mesmo tempo em que usam atributos adicionais, como conexão para redirecionamento local de arquivos e impressoras. O modo clássico é o método de conexão padrão recomendado. É o único compatível com a exibição da área de trabalho.
- Com o modo de aplicativo nativo, os usuários finais podem trabalhar com aplicativos de streaming remoto de forma semelhante a outros aplicativos instalados localmente. Se os usuários finais estiverem acostumados a trabalhar com aplicativos instalados localmente, o modo de aplicativo nativo oferece uma experiência perfeita. O aplicativo de streaming remoto funciona da mesma forma que um aplicativo instalado localmente. O ícone do aplicativo é exibido na barra de tarefas do seu computador local, assim como os ícones de seus aplicativos locais. Diferentemente dos ícones dos aplicativos locais, os ícones dos aplicativos de streaming no modo de aplicativo nativo incluem o logotipo dos WorkSpaces aplicativos. O nativo é o modo de conexão recomendado quando os usuários desejam usar atalhos de teclado para alternar facilmente entre aplicativos locais individuais e remotos individuais.

Implantação e gerenciamento do cliente

Os usuários podem instalar o cliente de WorkSpaces aplicativos sozinhos, ou os administradores podem instalar o cliente de WorkSpaces aplicativos para eles executando PowerShell scripts remotamente ou reempacotando o cliente de WorkSpaces aplicativos com configurações personalizadas.

É necessário qualificar os dispositivos USB que você deseja habilitar para que seus usuários usem com a sessão de streaming. Se o dispositivo USB não estiver qualificado, ele não será detectado pelos WorkSpaces aplicativos e não poderá ser compartilhado com a sessão. Depois que seus dispositivos forem qualificados, seus usuários deverão compartilhá-los com os WorkSpaces aplicativos sempre que iniciarem uma nova sessão de streaming.

Ao implantar o cliente de WorkSpaces aplicativos em grande escala, AWS recomenda o uso da Enterprise Deployment Tool. A Enterprise Deployment Tool inclui os arquivos de instalação do cliente WorkSpaces Applications e um modelo administrativo de Política de Grupo.

Domínios personalizados

Ao implantar WorkSpaces aplicativos de forma programática, é possível criar um domínio personalizado que pode fornecer aos usuários uma experiência familiar para sessões de streaming. Nas implantações de aplicativos WorkSpaces do SAML 2.0 IdP, é importante destacar que o acesso do usuário começa no IdP, não nos aplicativos. WorkSpaces Os usuários não precisam de URLs de WorkSpaces aplicativos, pois são fornecidos pelo IdP após a autenticação. Portanto, nomes de domínio personalizados não são necessários para implantações de IdP do SAML 2.0.

Autenticação

Com WorkSpaces os aplicativos, a autenticação pode ocorrer fora dos WorkSpaces aplicativos da Amazon ou como parte do serviço de WorkSpaces aplicativos. Selecionar como a autenticação ocorrerá para a implantação de seus WorkSpaces aplicativos é uma consideração fundamental do seu design. Não é incomum que uma organização tenha várias implantações de WorkSpaces aplicativos para diferentes casos de uso. Cada caso de uso pode ter um método de autenticação diferente.

Há três tipos de métodos de autenticação para WorkSpaces aplicativos:

- SAML 2.0
- Grupo de usuários
- Programático

Como determinar o método otimizado

O Amazon WorkSpaces Applications foi projetado para ser flexível para ser aplicado à maioria dos requisitos de design organizacional. Ao determinar o método otimizado para autenticação, é uma prática recomendada considerar os objetivos e propósitos das pessoas que consomem o serviço, bem como as políticas e os procedimentos organizacionais.

Veja alguns exemplos da combinação de casos de uso com objetivos organizacionais.

Tabela 4: casos de uso com objetivos organizacionais

Exemplo	Descrição	Autenticação
São necessárias instâncias de frota unidas ao domínio	Os aplicativos instalados na imagem WorkSpaces Applications só podem ser acessados por recursos associados ao domínio.	SAML 2.0
Forte integração com os serviços da Microsoft	Dependência organizacional no desenvolvimento de políticas de grupo e	SAML 2.0

Exemplo	Descrição	Autenticação
	infraestrutura de back-end da Microsoft	
Empresa única existente Sign-on (SSO)	Todos os novos serviços devem usar uma solução corporativa de SSO que tenha vários processos de geração de relatórios e segurança estabelecidos.	SAML 2.0
Suporte de cartão inteligente para aplicativos	Cartões inteligentes (como verificação de identidade privada e cartões de acesso comuns) para autenticação na sessão em aplicativos transmitidos por meio de um leitor de cartão inteligente.	SAML 2.0
Força de trabalho sazonal com equipe temporária	Alguns meses por ano, os trabalhadores temporári os recebem um pequeno conjunto de aplicativos que não incluem recursos internos para concluir as atividades.	Grupo de usuários
Suporte limitado da TI	Organizações de menor porte com menos de 50 usuários e equipe de TI limitada, que buscam eliminar a sobrecarg a de manutenção de um provedor de identidades (IdP)	Grupo de usuários

Exemplo	Descrição	Autenticação
Provedor de software independente (ISV)	Solução proprietária criada por sua organização que inclui autorização e autenticação do usuário, estendendo os WorkSpaces aplicativos como parte de sua solução. *	Programático
Demonstração de tecnologia	Ambiente completamente efêmero que apresenta uma tecnologia proprietária como parte de uma visita guiada da solução, sem a necessidade de armazenar informações do usuário.	Programático
Experiência interativa no site	Torne o site interativo com aplicativos de streaming do Windows.**	Programático

*Consulte Fornecedores de software: fornecimento de aplicativos para qualquer dispositivo de usuário e obtenha mais informações.

**Consulte Sessões de streaming de WorkSpaces aplicativos incorporados para obter mais informações.

Se sua organização tiver um caso de uso ou política que não esteja listado nos exemplos fornecidos anteriormente, é uma prática recomendada prever o estado final desejado do consumo do fluxo de trabalho de WorkSpaces aplicativos para garantir que a solução de autenticação não entre em conflito com ele.

Configuração do provedor de identidade

SAML 2.0

O Security Assertion Markup Language (SAML) 2.0 é uma opção comum de implantação para permitir que os usuários usem recursos. AWS Vários provedores de identidade SAML 2.0

terceirizados oferecem suporte aos WorkSpaces aplicativos. Independentemente de seus recursos de WorkSpaces aplicativos serem associados a um domínio ou não, o SAML 2.0 IdP exige que você use o IAM.

Como a maioria IdPs gera um metadata.xml exclusivo com atributos SAML específicos para cada aplicativo SAML, cada pilha de WorkSpaces aplicativos exige uma função que tenha uma relação confiável com o IdP do SAML e uma política que tenha uma única permissão para o AppStream:stream com condições que correspondam aos requisitos do IdP do SAML e do ARN da pilha de aplicativos. WorkSpaces

O guia de administração de WorkSpaces aplicativos fornece um exemplo de configuração para o design de uma única pilha de WorkSpaces aplicativos. Para implantações de várias pilhas, consulte as etapas opcionais para usar o catálogo de aplicativos de várias pilhas do SAML 2.0.

Grupo de usuários

A guia Grupo de usuários em WorkSpaces Aplicativos é uma opção válida para pequenas provas de conceito. Como prática recomendada, é melhor evitar grupos de usuários para qualquer caso de uso e organização que use WorkSpaces aplicativos para fornecer aplicativos de produção.

Um detalhe importante sobre grupos de usuários é que os endereços de e-mail dos usuários diferenciam maiúsculas de minúsculas; portanto, é uma prática recomendada garantir que os usuários sejam instruídos sobre como inserir corretamente as credenciais do usuário.

URL de streaming

Para implantações que chamam recursos de WorkSpaces aplicativos de um serviço centralizado (normalmente ISVs), a autenticação programática depende de um aplicativo para o qual fazer chamadas programáticas para transmitir informações dinamicamente e criar uma sessão de aplicativos AWS para seus usuários. WorkSpaces Use o método de autenticação da API (comumente chamado de “programático”) ao criar URLs de streaming usando a operação de CreateStreamingURL. O usuário que faz a chamada `CreateStreamingURL` deve usar um usuário ou uma função válida com permissão para `appstream:CreateStreamingURL`.

Ao criar a política para acesso programático, é uma prática recomendada proteger o acesso especificando o ARN exato da pilha de WorkSpaces aplicativos na seção Recursos em vez do padrão '*'. Por exemplo:

Example

JSON

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

> **Note**
>
> Você pode recuperar rapidamente os ARNs de suas pilhas de WorkSpaces aplicativos usando a API de descrição das pilhas ou a AWS CLI.

WorkSpaces As instâncias de aplicativos devem começar como instâncias genéricas. Por meio das informações passadas do aplicativo, a instância WorkSpaces Applications estabelece o ambiente usando o contexto da sessão para tornar as coisas dinâmicas para o usuário.

Embora os GPOs locais possam ser usados para especificar configurações no logon do usuário, o contexto da sessão é uma prática recomendada ao usar e transmitir atributos-chave`CreateStreamingURL`, como ID do cliente ou configurações de conexão do banco de dados, para serem usados na sessão de WorkSpaces aplicativos.

Direito à inscrição

WorkSpaces Os aplicativos podem criar dinamicamente o catálogo de aplicativos que é apresentado aos usuários. Os direitos do aplicativo são baseados nos atributos do SAML 2.0 ou no uso do WorkSpaces Applications Dynamic Application Framework.

Attribute-based direitos de aplicativos usando SAML 2.0 são recomendados na maioria dos cenários. Para gerenciar a entrega de pacotes de aplicativos, é recomendado usar o Dynamic Application Framework.

Integração com o Microsoft Active Directory

Os Amazon WorkSpaces Applications Image Builders e frotas podem ser integrados ao Microsoft Active Directory. Isso permite que você forneça um método centralizado para autenticação e autorização de usuários e aplique políticas de grupo do Active Directory a instâncias de WorkSpaces aplicativos associadas ao domínio. O uso de frotas de WorkSpaces aplicativos unidas a um domínio oferece os mesmos benefícios administrativos de um ambiente local. Isso inclui gerenciamento centralizado de compartilhamentos de arquivos de rede, direitos de aplicativos de usuário, perfis de roaming, acesso à impressora e outras configurações com base em políticas.

Ao integrar um ambiente de WorkSpaces aplicativos com o Active Directory, é importante observar que a autenticação inicial na pilha de WorkSpaces aplicativos ainda é gerenciada por um SAML2.0 IdP. Depois que o usuário for autenticado com êxito no IdP, ao iniciar uma sessão, ele deverá inserir a senha do domínio ou uma autenticação por cartão inteligente para o domínio do Active Directory.

Ao projetar o ambiente dos Serviços de Domínio do Active Directory (ADDS) que será usado com WorkSpaces aplicativos, há duas opções de serviço e muitos cenários de implantação disponíveis. Além disso, certifique-se de que a rede de WorkSpaces aplicativos seja analisada com o proprietário da topologia do site do Active Directory.

Opções de serviço

O Active Directory também pode ser implantado usando o Microsoft Active Directory (AD)AWS gerenciado. AWS O Microsoft AD gerenciado é um serviço totalmente gerenciado que permite executar o Microsoft Active Directory. Ele também pode ser usado em um ambiente com hospedagem automática, executado no EC2 ou no local.

Cenários de implantação

Os cenários de implantação a seguir listados são opções de integração comumente usadas e recomendadas para WorkSpaces aplicativos com o Microsoft Managed AD ou o Active Directory autogerenciado de um cliente. Todos os diagramas de arquitetura listados abaixo usam as principais estruturas da Amazon.

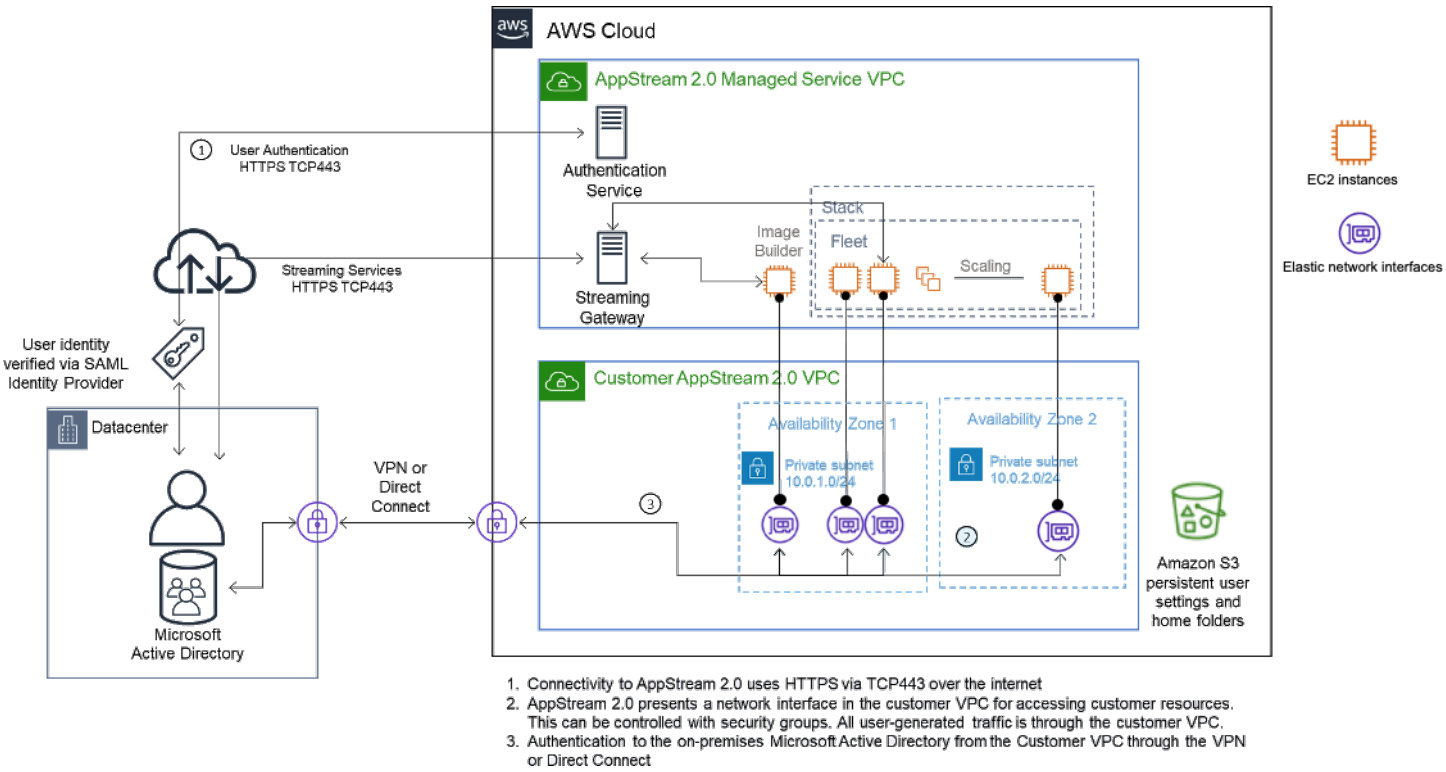
- Amazon Virtual Private Cloud (VPC) — Criação de uma Amazon VPC dedicada a serviços de WorkSpaces aplicativos com pelo menos quatro sub-redes privadas espalhadas por quatro AZs. Duas das sub-redes privadas são usadas para frotas de WorkSpaces aplicativos e construtores de

imagens. As duas sub-redes restantes são usadas para os controladores de domínio no EC2 ou no Microsoft Managed AD.

- Conjunto de opções do Dynamic Host Configuration Protocol (DHCP) — Fornece um padrão para transmitir informações de configuração para a frota de WorkSpaces aplicativos e os criadores de imagens que serão provisionados na VPC. O conjunto de opções do DHCP é definido no nível da VPC. Ele permite que os clientes definam um nome de domínio e configurações de DNS específicos que serão usados com os WorkSpaces aplicativos instanciados ao serem provisionados.
- AWS Serviços de diretório — O Amazon Microsoft Managed AD pode ser implantado em duas sub-redes privadas que serão usadas em conjunto com cargas de trabalho de aplicativos. WorkSpaces
- WorkSpaces Frotas de aplicativos — As frotas de WorkSpaces aplicativos ou construtores de imagens são hospedadas na VPC gerenciada AWS . Cada instância de WorkSpaces aplicativos tem duas interfaces de rede elásticas (ENI). A interface primária (`eth0`) é usada para fins de gerenciamento e intermediação da conexão do usuário final com a instância por meio do gateway de streaming. A interface secundária (`eth1`) é injetada na VPC do cliente e pode ser usada para acessar outros recursos na VPC personalizada ou no local.

Cenário 1: Serviços de Domínio do Active Directory (ADDS) implantados no local

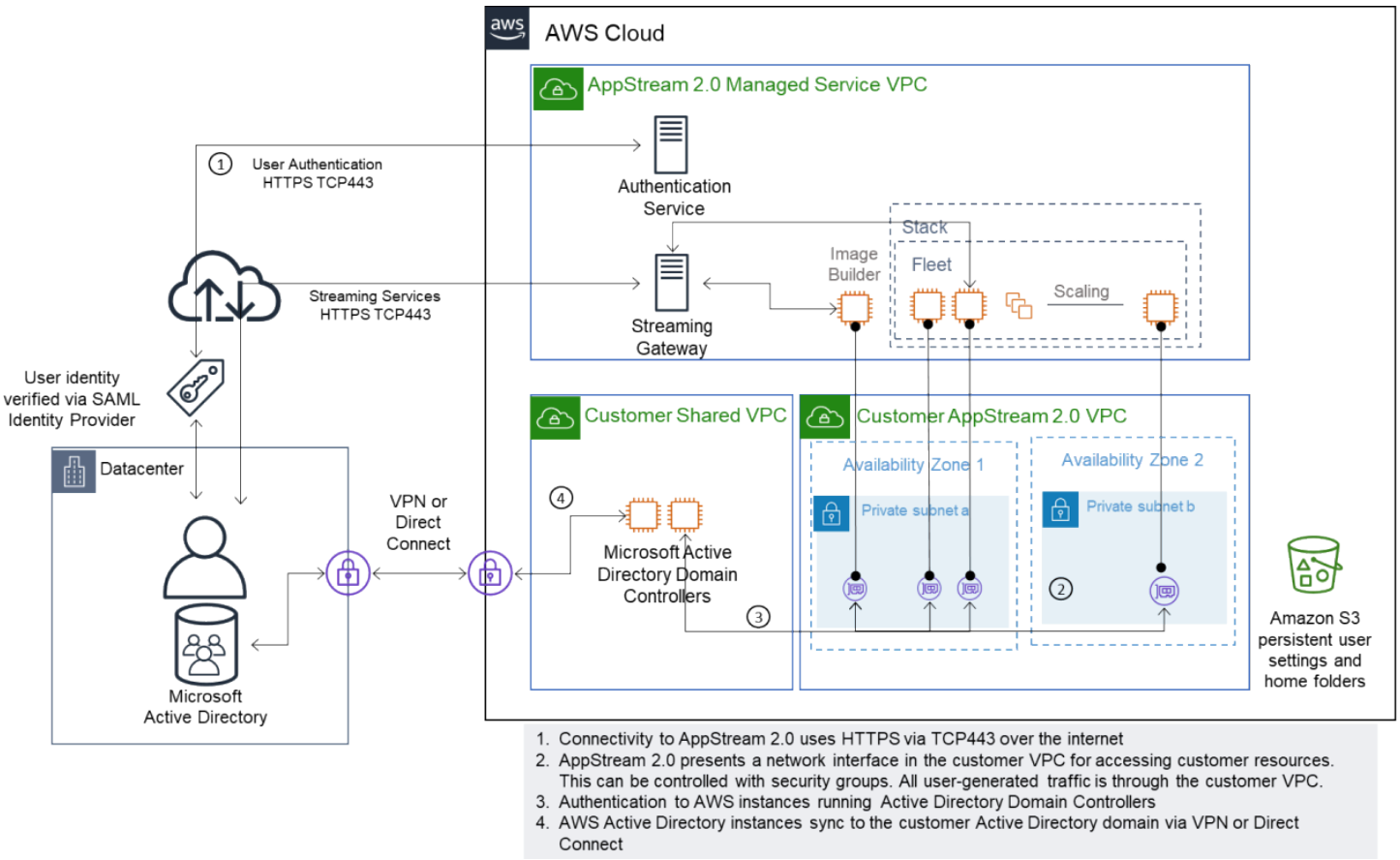
Todo o tráfego de autenticação atravessa a conexão VPN ou Direct Connect da VPC do cliente até o gateway do cliente. A vantagem desse cenário é usar um ambiente do AD possivelmente já implantado sem precisar provisionar controladores de domínio adicionais na VPC do cliente. A desvantagem é a dependência exclusiva da VPN ou do Direct Connect para autenticar e autorizar usuários para a frota de aplicativos. WorkSpaces Se houver algum problema de conectividade de rede, a frota de WorkSpaces aplicativos ou os Image Builders serão diretamente afetados. Os túneis de VPN duplos ou conexões Direct Connect com caminhos diferentes reduzem esse risco potencial.



Cenário 1: Serviços de Domínio do Active Directory (ADDS) implantados no local

Cenário 2: Estender os Serviços de Domínio Ativo (ADDS) para AWS VPC do cliente

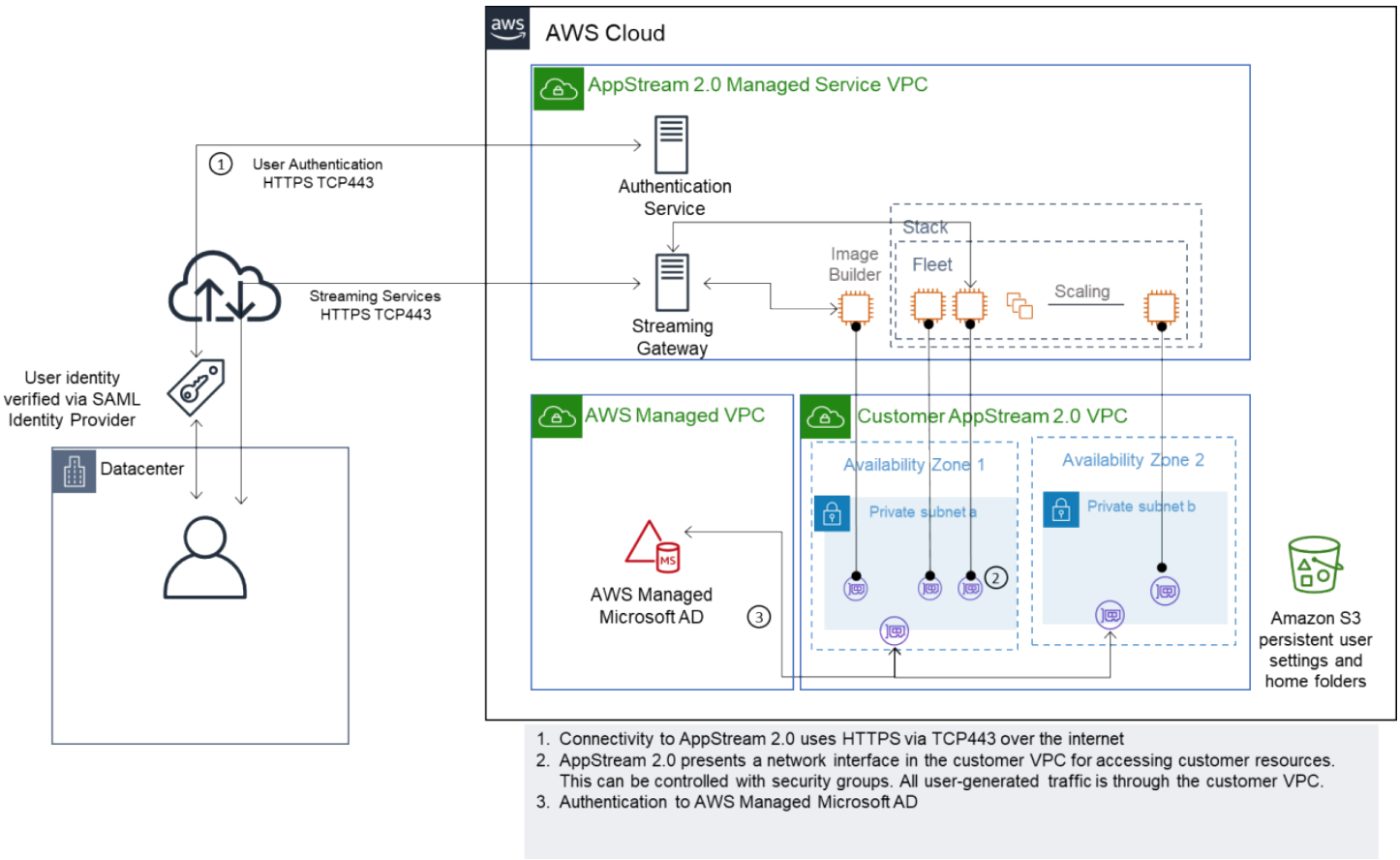
O Active Directory é estendido à VPC do cliente. Um site do Active Directory deve ser criado para os novos controladores de domínio na VPC do cliente. O tráfego de autenticação é roteado para os controladores de domínio na AWS VPC do cliente em vez de atravessar a conexão VPN ou Direct Connect.



Cenário 2 — Estenda os serviços do Active Domain à nuvem privada virtual AWS do cliente

Cenário 3: AWS Microsoft Active Directory gerenciado

AWS O Microsoft AD gerenciado é implantado no Nuvem AWS e é usado como domínio de identidade e recurso para as frotas de WorkSpaces aplicativos e os Image Builders.



Cenário 3 — Active Directory AWS gerenciado

Topologia do site do serviço do Active Directory

A topologia do site de serviços do Active Directory é uma representação lógica da sua rede física.

A topologia do site ajuda você a rotear com eficiência as consultas do cliente e o tráfego de replicação do Active Directory. Com uma topologia do site bem projetada e mantida, a organização pode obter os seguintes benefícios:

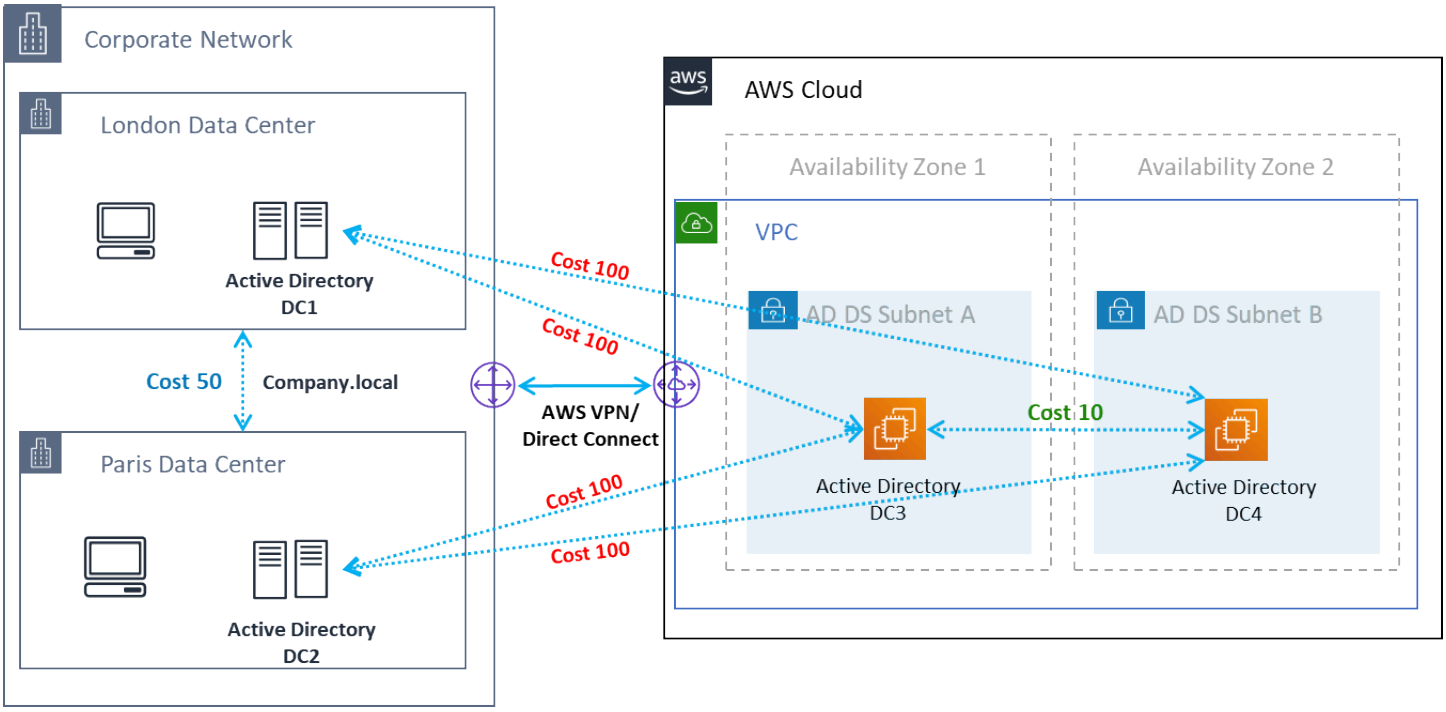
- Minimize o custo da replicação de dados do Active Directory ao sincronizar entre locais e. Nuvem AWS
- Otimize a capacidade dos computadores clientes de localizar os recursos mais próximos, como controladores de domínio. Isso ajuda a reduzir o tráfego de rede em links lentos de rede de longa distância (WAN), melhorar os processos de logon e logoff, além de acelerar as operações de acesso a recursos.

Ao introduzir os serviços de WorkSpaces aplicativos, certifique-se de que os intervalos de endereços usados nas sub-redes das instâncias de WorkSpaces aplicativos estejam atribuídos ao site correto para seu ambiente.

Para os cenários 1 e 2, sites e serviços são componentes essenciais para a melhor experiência do usuário em termos de horários de logon e tempo de acesso aos recursos do Active Directory.

A topologia do site controla a replicação do Active Directory entre os controladores de domínio dentro do mesmo site e entre limites do site.

Definir a topologia correta do site garante a afinidade com o cliente, o que significa que os clientes (nesse caso, instâncias de streaming de WorkSpaces aplicativos) usam seu controlador de domínio local preferido.



Sites e serviços do Active Directory: afinidade com o cliente

> **Tip**
>
> Como prática recomendada, defina o alto custo dos links de sites entre o AD DS local e a Nuvem AWS. A figura anterior é um exemplo de quais custos você deve atribuir aos links do site (custo 100) para garantir a afinidade com o cliente de modo independente do site.

Para obter mais informações sobre a topologia do site, consulte Como projetar a topologia do site.

Unidades organizacionais do Active Directory

A AWS recomenda armazenar as unidades organizacionais (OUs) configuradas em um único objeto do WorkSpaces Applications Directory Config. É uma prática recomendada que cada pilha de WorkSpaces aplicativos tenha sua própria OU. Isso permite a flexibilidade de ter GPOs específicos por pilha. Certifique-se de que as OUs sejam dedicadas aos objetos de computador de WorkSpaces aplicativos para evitar misturar WorkSpaces Applications-specific políticas com desktops locais. Considere o uso de Sub-OUs para cada WorkSpaces aplicativo em Região da AWS que você implanta.

Limpeza de objetos no computador do Active Directory

WorkSpaces As instâncias dos aplicativos são efêmeras. Uma frota cria e reutiliza objetos de computador do Active Directory à medida que as frotas aumentam e reduzem a escala horizontalmente.

AWS recomenda criar um processo de limpeza do AD para excluir objetos de computador obsoletos do Active Directory que possam existir após a remoção de uma frota de WorkSpaces aplicativos.

Segurança

A segurança da nuvem na Amazon Web Services (AWS) é a nossa maior prioridade. Segurança e conformidade são responsabilidades compartilhadas entre o cliente AWS e o cliente. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada. Como cliente da AWS Land WorkSpaces Applications, é importante implementar medidas de segurança em diferentes camadas, como pilha, frota, imagem e rede.

Devido à sua natureza efêmera, os WorkSpaces aplicativos geralmente são preferidos como uma solução segura para a entrega de aplicativos e desktops. Considere se as soluções antivírus comuns nas implantações do Windows são relevantes em seus casos de uso para um ambiente predefinido e eliminado no final de uma sessão de usuário. O antivírus adiciona sobrecarga às instâncias virtualizadas. Dessa forma, a prática recomendada é reduzir atividades desnecessárias. Por exemplo, escanear o volume do sistema (que é efêmero) na inicialização, por exemplo, não aumenta a segurança geral dos aplicativos. WorkSpaces

As duas questões-chave para WorkSpaces aplicativos de segurança estão centradas em:

- A persistência do estado do usuário além da sessão é um requisito?
- Quanto acesso um usuário deve ter em uma sessão?

Como proteger dados persistentes

As implantações de WorkSpaces aplicativos podem exigir que o estado do usuário persista de alguma forma. Pode ser para manter os dados de usuários individuais ou para manter os dados para colaboração usando uma pasta compartilhada. WorkSpaces O armazenamento de instâncias de aplicativos é efêmero e não tem opção de criptografia.

WorkSpaces Os aplicativos fornecem persistência do estado do usuário por meio de pastas iniciais e configurações do aplicativo no Amazon S3. Alguns casos de uso exigem maior controle sobre a persistência do estado do usuário. Para esses casos de uso, a AWS recomenda usar um compartilhamento de arquivos do protocolo de Server Message Block (SMB).

Estado e dados do usuário

Como a maioria dos aplicativos do Windows tem um desempenho melhor e mais seguro quando colocados em conjunto com os dados do aplicativo criados pelo usuário, é uma prática recomendada

manter esses dados da mesma forma Região da AWS que as frotas de aplicativos. WorkSpaces A prática recomendada é criptografar os dados. O comportamento padrão da pasta inicial do usuário é criptografar arquivos e pastas em repouso usando as chaves de S3-managed criptografia da Amazon dos serviços de gerenciamento de AWS chaves (AWS KMS). É importante observar que os usuários AWS administrativos com acesso ao AWS console ou ao bucket do Amazon S3 poderão acessar esses arquivos diretamente.

Em designs que exigem um destino de SMB (Server Message Block) de um compartilhamento de arquivos do Windows para armazenar arquivos e pastas do usuário, o processo é automático ou requer configuração.

Tabela 5: opções para proteger os dados do usuário

Meta do SMB	Encryption-at-rest	Encryption-in-transit	Antivírus (AV)
FSx para Windows File Server	Automático por meio do AWS KMS	Automático por meio de criptografia de SMB	O AV instalado em uma instância remota executa a varredura na unidade mapeada
Gateway de arquivos, AWS Storage Gateway	Por padrão, todos os dados armazenados os AWS Storage Gateway no S3 são criptografados no lado do servidor com as S3-Managed Amazon Encryption Keys (). SSE-S3 Opcionalmente, você pode configurar diferentes tipos de gateway para criptografar dados armazenados com AWS Key Management Service (KMS)	Todos os dados transferidos entre qualquer tipo de dispositivo de gateway e AWS armazenamento são criptografados usando SSL.	O AV instalado em uma instância remota executa a varredura na unidade mapeada

Meta do SMB	Encryption-at-rest	Encryption-in-transit	Antivírus (AV)
EC2-based Servidores de arquivos Windows	Habilitar criptografia do EBS	PowerShell; `Set-SmbServerConfiguration - EncryptData $True`	O AV instalado no servidor executa a varredura em unidades locais

Segurança de endpoints e antivírus

A breve natureza efêmera das instâncias do Amazon WorkSpaces Applications e a falta de persistência de dados significam que uma abordagem diferente é necessária para garantir que a experiência e o desempenho do usuário não sejam comprometidos por atividades que seriam necessárias em um desktop persistente. Os agentes do Endpoint Security são instalados em imagens de WorkSpaces aplicativos quando há uma política organizacional ou quando usados com entrada de dados externos, por exemplo, e-mail, entrada de arquivos, navegação externa na web.

Como remover identificadores exclusivos

Os agentes de segurança do endpoint podem ter um identificador global exclusivo (GUID) que deve ser redefinido durante o processo de criação da instância da frota. Os fornecedores têm instruções sobre como instalar seus produtos em imagens, garantindo que um novo GUID seja gerado para cada instância gerada a partir de uma imagem.

Para garantir que o GUID não seja gerado, instale o agente do Endpoint Security como última ação antes de executar o Assistente de WorkSpaces Aplicativos para gerar a imagem.

Otimização do desempenho

Os fornecedores de segurança de terminais fornecem switches e configurações que otimizam o desempenho dos WorkSpaces aplicativos. As configurações variam entre os fornecedores e podem ser encontradas em sua documentação, normalmente em uma seção sobre VDI. Algumas configurações comuns incluem:

- Desativar as verificações de inicialização para garantir que os tempos de criação, inicialização e login da instância sejam minimizados
- Desativar as varreduras agendadas para evitar varreduras desnecessárias
- Desativar os caches de assinatura para evitar a enumeração de arquivos

- Ativar configurações de E/S otimizadas para VDI
- Exclusões exigidas pelos aplicativos para garantir o desempenho

Os fornecedores de segurança de endepoints fornecem instruções para uso com ambientes de área de trabalho virtual que otimizam o desempenho.

- Suporte do Trend Micro Office Scan para infraestrutura de desktop virtual - Apex One/OfficeScan (trendmicro.com)
- CrowdStrike e como instalar o CrowdStrike Falcon no data center
- Sophos e Sophos Central Endpoint: como instalar em uma imagem gold para evitar identidades duplicadas e Sophos Central: práticas recomendadas ao instalar endpoints do Windows em ambientes de área de trabalho virtual
- McAfee e provisionamento e implantação de McAfee agentes em sistemas de infraestrutura de desktop virtual
- Microsoft Endpoint Security e Configuração do Microsoft Defender Antivirus para máquinas VDI não persistentes: Microsoft Tech Community

Exclusões de verificação

Se o software de segurança estiver instalado em instâncias de WorkSpaces Aplicativos, o software de segurança não deverá interferir nos processos a seguir.

Tabela 6 — O software de segurança de processos de WorkSpaces aplicativos não deve interferir nos processos a seguir.

Serviço	Processos
AmazonCloudWatchAgent	“C:\Program Files\ Amazon\AmazonCloud WatchAgent\ start-amazon- cloudwatch-agent.exe”
AmazonSSMAgent	"C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"
NICE DCV	"C:\Program Files\NICE\DCV\Server\bin\dcvserver.exe" "C:\Program Files\NICE\DCV\Server\bin\dcvagent.exe"

Serviço	Processos
WorkSpaces Aplicativos	“C:\ProgramFiles\ Amazon\ AppStream 2\StorageConnector\StorageConnector.exe” Na pasta "C:\Program Files\Amazon\Photon\" “. \ Agente\PhotonAgent.exe” ".\Agent\s5cmd.exe" ".\WebServer\PhotonAgentWebServer.exe" ".\CustomShell\PhotonWindowsAppSwitcher.exe" ".\CustomShell\PhotonWindowsCustomShell.exe" ".\CustomShell\PhotonWindowsCustomShellBackground.exe"

Pastas

Se o software de segurança estiver instalado em instâncias de WorkSpaces Aplicativos, o software não deverá interferir nas seguintes pastas:

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\
```

Limpeza do console de segurança de endpoints

WorkSpaces Os aplicativos da Amazon criarão novas instâncias exclusivas sempre que um usuário se conectar além dos tempos limite de inatividade e desconexão. As instâncias terão um nome exclusivo e se acumularão em consoles de gerenciamento de segurança de endpoints. Configurar máquinas antigas não utilizadas com mais de 4 dias (ou menos, dependendo do tempo limite da sessão de WorkSpaces aplicativos) para serem excluídas minimizará o número de instâncias expiradas no console.

Exclusões de rede

O intervalo da rede de gerenciamento de WorkSpaces aplicativos (`198.19.0.0/16`) e as seguintes portas e endereços não devem ser bloqueados por nenhuma solução de segurança/firewall ou antivírus nas instâncias de WorkSpaces aplicativos.

Tabela 7 — Portas em WorkSpaces aplicativos, instâncias de streaming, software de segurança não deve interferir com

Porta	Uso
8300, 3128	Usado para estabelecer a conexão de streaming
8000	Isso é usado para gerenciar a instância de streaming por WorkSpaces aplicativos
8443	Isso é usado para gerenciar a instância de streaming por WorkSpaces aplicativos
53	DNS

Tabela 8 — O software de segurança de endereços de serviços gerenciados de WorkSpaces aplicativos não deve interferir com

Porta	Uso
169.254.169.123	NTP
169.254.169.249	Serviço de licença NVIDIA GRID
169.254.169.250	KMS
169.254.169.251	KMS
169.254.169.253	DNS
169.254.169.254	Metadados

Protegendo uma sessão de WorkSpaces aplicativos

Como limitar os controles de aplicativos e sistemas operacionais

WorkSpaces Os aplicativos permitem que o administrador especifique exatamente quais aplicativos podem ser iniciados a partir da página da Web no modo de streaming de aplicativos. No entanto, isso não garante que somente os aplicativos especificados possam ser executados.

Os utilitários e aplicativos do Windows podem ser iniciados por meio do sistema operacional por meios adicionais. AWS recomenda usar AppLocker a Microsoft para garantir que somente os aplicativos que sua organização exige possam ser executados. É necessário modificar as regras padrão, pois concedem a todos acesso por caminhos aos diretórios essenciais do sistema.

> **Note**
>
> O Windows Server 2016 e 2019 exigem que o serviço Windows Application Identity esteja em execução para impor AppLocker as regras. O acesso a WorkSpaces aplicativos a partir de aplicativos usando AppLocker a Microsoft está detalhado no Guia do administrador de WorkSpaces aplicativos.

Para instâncias de frota unidas a um domínio do Active Directory, use Objetos de política de grupo (GPOs) para fornecer configurações de usuário e sistema, protegendo o acesso dos usuários aos aplicativos e recursos.

Firewalls e roteamento

Ao criar uma frota de WorkSpaces aplicativos, sub-redes e um grupo de segurança devem ser atribuídos. As sub-redes têm atribuições existentes de listas de controle de acesso à rede (NACLs) e tabelas de rotas. Você pode associar até cinco grupos de segurança ao iniciar um novo criador de imagens ou ao criar uma nova frota. Os grupos de segurança podem ter até cinco atribuições dos grupos de segurança existentes. Para cada grupo de segurança, adicione regras que controlam o tráfego de saída e entrada da rede de e para instâncias

A NACL é uma camada de segurança opcional para a VPC que atua como um firewall sem estado para controlar o tráfego de entrada e saída em sub-redes. Você pode configurar Network ACLs com regras semelhantes às dos grupos de segurança a fim de adicionar uma camada extra de segurança à sua VPC. Para obter mais informações sobre as diferenças entre grupos de segurança e ACLs de rede, consulte a página de comparação entre grupos de segurança e NACLs.

Ao projetar e aplicar as regras do Security Group e da NACL, considere as Well-Architected melhores práticas da AWS para obter o menor privilégio. O privilégio mínimo é o princípio de conceder somente as permissões necessárias para concluir uma tarefa.

Para clientes que têm uma rede privada de alta velocidade conectando seu ambiente local à AWS (por meio de um AWS Direct Connect), considere usar os VPC Endpoints for WorkSpaces Applications, o que significa que o tráfego de streaming será roteado por meio de sua conectividade de rede privada, em vez de passar pela Internet pública. Para obter mais informações sobre esse tópico, consulte a seção VPC endpoint da interface de streaming de WorkSpaces aplicativos deste documento.

Prevenção de perda de dados

Vamos analisar dois tipos de prevenção de perda de dados.

Controles de transferência de dados de instâncias de cliente para WorkSpaces aplicativos

Tabela 9: orientação para controlar a entrada e saída de dados

Configuração	Opções	Orientação
Área de transferência	• Copiar e colar somente na sessão remota	Desabilitar essa configuração não desabilita copiar e colar

Configuração	Opções	Orientação
	• Copiar somente para o dispositivo local • Desabilitado	na sessão. Se for necessário copiar dados para a sessão, escolha Colar somente na sessão remota para minimizar o potencial do vazamento de dados.
Transferência de arquivos	• Fazer upload e baixar • Somente upload • Somente baixar • Desabilitado	Evite ativar essa configuração para impedir o vazamento de dados.
Imprimir no dispositivo local	• Habilitado • Desabilitado	Se a impressão for necessári a, use impressoras mapeadas em rede que sejam controlad as e monitoradas pela organização.

Considere as vantagens da solução de transferência de dados organizacional existente em relação às configurações da pilha. Essas configurações não foram projetadas para substituir uma solução abrangente de transferência segura de dados.

Controle do tráfego de saída da instância do WorkSpaces Applications

Quando a perda de dados é uma preocupação, é importante cobrir o que um usuário pode acessar quando estiver dentro da instância do WorkSpaces Applications. Qual é a aparência do caminho de saída (ou regressão) da rede? É um requisito comum ter acesso público à Internet disponível para o usuário final em sua instância de WorkSpaces aplicativos, portanto, é necessário considerar a colocação de uma solução de filtragem de conteúdo WebProxy ou uma solução de filtragem de conteúdo no caminho da rede. Outras considerações incluem um aplicativo antivírus local e outras medidas de segurança de terminais dentro da instância de WorkSpaces aplicativos (consulte a seção “Segurança e antivírus de terminais” para obter mais informações).

Utilizar AWS serviços

AWS Identity and Access Management

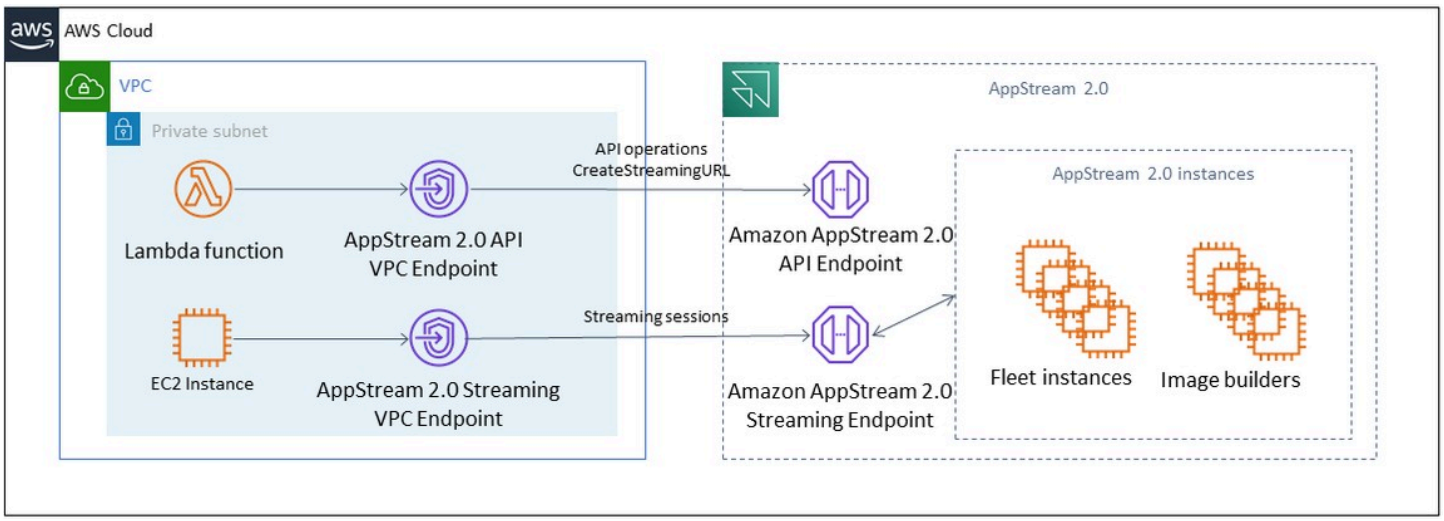
Usar uma função do IAM para acessar AWS serviços e ser específico na política do IAM anexada a ela é uma prática recomendada que permite que somente os usuários nas sessões de WorkSpaces aplicativos tenham acesso sem gerenciar credenciais adicionais. Siga as melhores práticas para usar funções do IAM com WorkSpaces aplicativos.

Crie políticas do IAM para proteger os buckets do Amazon S3 que são criados para manter os dados do usuário nas pastas iniciais e na persistência das configurações do aplicativo. Isso impede o acesso de usuários que não são administradores de WorkSpaces aplicativos.

Endpoints da VPC

Um VPC endpoint permite conexões privadas entre sua VPC e os serviços compatíveis AWS e os serviços de VPC endpoint desenvolvidos por. AWS PrivateLink AWS PrivateLink é uma tecnologia que permite acessar serviços de forma privada usando endereços IP privados. O tráfego entre a sua VPC e os outros serviços não deixa a rede da Amazon. Se o acesso público à Internet for necessário somente para AWS serviços, os VPC endpoints eliminarão completamente a exigência de gateways NAT e gateways de Internet.

Em ambientes em que as rotinas de automação ou os desenvolvedores exijam chamadas de API para WorkSpaces aplicativos, crie uma interface VPC endpoint WorkSpaces para operações de API de aplicativos. Por exemplo, se houver instâncias do EC2 em sub-redes privadas sem acesso público à Internet, um VPC endpoint para API de WorkSpaces aplicativos pode ser usado para chamar operações de API de WorkSpaces aplicativos, como URL. CreateStreaming O diagrama a seguir mostra um exemplo de configuração em que a API de WorkSpaces aplicativos e os endpoints de VPC de streaming são consumidos pelas funções Lambda e pelas instâncias do EC2.



Endpoint da VPC

O endpoint da VPC de streaming permite que você transmita sessões por meio de um endpoint da VPC. O endpoint de interface de streaming mantém o tráfego de streaming em sua VPC. O tráfego de streaming inclui pixels, USB, entrada do usuário, áudio, área de transferência, upload e download de arquivos e tráfego de impressora. Para usar o VPC endpoint, a configuração do VPC endpoint deve estar habilitada na pilha de aplicativos. WorkSpaces Isso serve como uma alternativa ao streaming de sessões de usuários pela Internet pública a partir de locais com acesso limitado à Internet e que se beneficiariam do acesso por meio de uma instância do Direct Connect. O streaming de sessões de usuário por meio de um endpoint da VPC exige o seguinte:

- Os Grupos de segurança associados ao endpoint de interface devem permitir acesso de entrada à porta `443` (TCP) e às portas `1400-1499` (TCP) do intervalo de endereços IP do qual os usuários se conectam.
- A lista de controle de acesso à rede para as sub-redes deve permitir tráfego de saída das portas de rede efêmeras `1024-65535` (TCP) para o intervalo de endereços IP do qual os usuários se conectam.
- A conectividade com a Internet é necessária para autenticar os usuários e fornecer os ativos da web que os WorkSpaces Aplicativos exigem para funcionar.

Para saber mais sobre como restringir o tráfego para AWS serviços com WorkSpaces aplicativos, consulte o guia de administração para criar e transmitir a partir de VPC endpoints.

Quando o acesso público total à Internet é necessário, a prática recomendada é desativar a Configuração de Segurança Reforçada (ESC) do Internet Explorer no Image Builder. Para obter

mais informações, consulte o guia de administração de WorkSpaces aplicativos para desabilitar a configuração de segurança aprimorada do Internet Explorer.

Recuperação de desastres

A Amazon AppStream 2.0 tem redundância integrada em até três zonas de disponibilidade. Ou seja, se um usuário tiver uma sessão ativa em uma zona de disponibilidade que se torna degradada, é possível se desconectar e reconectar, o que reservará uma sessão em uma zona de disponibilidade saudável, supondo que você tenha capacidade. Embora isso forneça alta disponibilidade na região, não fornece uma solução de recuperação de desastres se o serviço tiver problemas em nível regional.

Para fornecer um plano de recuperação de desastres para seus usuários de WorkSpaces aplicativos, primeiro você precisará criar um ambiente de WorkSpaces aplicativos em sua região secundária. Do ponto de vista do design, esse ambiente deve ter conexões redundantes com o ambiente local, se aplicável, e não deve depender da região primária. Por exemplo, se sua frota de WorkSpaces aplicativos estiver associada a um domínio, você deverá ter controladores de domínio adicionais na região secundária com sites e serviços configurados. Do ponto de vista dos WorkSpaces aplicativos, esse ambiente deve consistir nas mesmas configurações de frota e pilha que você tem na sua região principal. A frota em si deve executar a mesma imagem base, que pode ser copiada para a região secundária por meio do console ou programaticamente. Se os aplicativos executados em suas sessões de WorkSpaces aplicativos tiverem uma dependência de back-end vinculada à sua região principal, ela também deverá ter redundância regional para garantir que os usuários ainda possam acessar o back-end do aplicativo se a região principal ficar inativa. Os limites de nível de serviço na região de destino devem corresponder à região principal.

Roteamento de identidade

Há dois métodos distintos para fornecer acesso a aplicativos em um cenário de DR. Em um alto nível, os dois métodos diferem na forma como os usuários são direcionados para a região de failover. O primeiro método é executado com uma única configuração de aplicativo de WorkSpaces aplicativos em seu IdP e o segundo método é ter duas configurações de aplicativo separadas.

Método 1: como alterar o estado de retransmissão do aplicativo

Quando os usuários fazem login nos WorkSpaces aplicativos a partir de um provedor de identidade (IdP), após a autenticação, eles são retransmitidos para uma URL específica que se alinha à região e à pilha à qual eles deveriam ter acesso. Para obter mais informações sobre a URL do estado de retransmissão, consulte o Amazon WorkSpaces Applications Administration Guide. O administrador

pode configurar uma pilha entre regiões baseada na mesma imagem de WorkSpaces aplicativos da região primária para a qual os usuários podem fazer o failover. O administrador pode controlar esse failover ao atualizar o URL do estado de retransmissão a fim de apontar para a pilha de failover. Para que esse método funcione adequadamente, as políticas associadas do IAM precisarão refletir o acesso às duas pilhas: primária e de failover. Para obter mais detalhes sobre como essas políticas do IAM devem ser configuradas, consulte o exemplo de política a seguir.

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}"
                }
            }
        }
    ]
}
```

Método 2: Configurando dois WorkSpaces aplicativos em seu IdP

Esse método exige que o administrador crie dois aplicativos separados para WorkSpaces aplicativos dentro do IdP. Em seguida, eles podem apresentar os dois aplicativos e permitir que o usuário escolha para onde ir, ou usar lock/hide um aplicativo até a hora do failover. Esse método está melhor alinhado ao caso de uso de usuários globais que se movimentam com frequência. Esses usuários devem estar transmitindo do endpoint mais próximo. Portanto, ter os dois aplicativos atribuídos dá a eles a opção de escolher o aplicativo que está configurado para a região mais próxima. Isso também pode ser automatizado. Para obter mais informações, consulte esta publicação do blog.

Persistência de armazenamento

Ao aproveitar os recursos de persistência de dados incluídos nos WorkSpaces aplicativos, como persistência de aplicativos e sincronização de pastas pessoais, você precisará replicar esses dados para sua região de failover. Esses recursos armazenam os dados persistentes em um bucket do Amazon S3 na região de WorkSpaces aplicativos específica. Para que os dados persistam entre regiões, você precisará replicar todas as alterações no bucket de origem para o bucket de aplicativos da região WorkSpaces de failover. Isso pode ser feito com recursos nativos do Amazon S3, como a replicação entre regiões do Amazon S3. Os dados persistentes de cada usuário residirão em uma pasta com seu nome de usuário com hash. Como o nome de usuário será codificado na mesma região cruzada, a simples replicação dos dados fornecerá persistência de dados na região secundária. Para obter mais informações sobre os buckets do Amazon S3 usados pelos WorkSpaces aplicativos, consulte este guia.

Monitoramento

Usar painéis

O monitoramento da utilização da frota é uma atividade regular que pode ser realizada por meio de CloudWatch métricas e da criação de um painel. Como alternativa, no console de WorkSpaces aplicativos, use a guia Uso da frota. Monitore regularmente o uso da frota, pois o comportamento do usuário nem sempre é previsível e a demanda pode exceder até mesmo o planejamento inicial de primeira linha. Uma lista completa das métricas e dimensões de WorkSpaces aplicativos CloudWatch pode ser encontrada no guia de administração de WorkSpaces aplicativos em Recursos de monitoramento.

Como antecipar o crescimento

Sempre que há um grande salto em `PendingCapacity`, ocorre um evento de ajuste de escala automático. É importante confirmar isso `AvailableCapacity` e `PendingCapacity` ter uma relação inversa enquanto novas instâncias da frota de WorkSpaces aplicativos se tornam disponíveis para hospedar sessões de usuários. Crie um CloudWatch alarme para cada frota de WorkSpaces aplicativos `InsufficientCapacityError` para notificar os administradores e garantir que o escalonamento automático não fique aquém da demanda.

Se a demanda exceder a capacidade e os valores métricos de `InsufficientCapacityError` forem comuns, considere aumentar a capacidade mínima por meio de uma política de ajuste de escala programada para o início do dia de trabalho. Além disso, tenha uma segunda política de escalabilidade programada para reduzir a capacidade mínima depois que a demanda for atendida. Lembre-se de que reduzir o valor da capacidade mínima não afeta as sessões existentes. A redução da capacidade mínima antes do final do dia de trabalho permite efetivamente que a balança funcione conforme o esperado, reduzindo o valor de `ActualCapacity`. Isso otimiza o custo.

Se a demanda for consistentemente imprevisível, use a política de escalabilidade do Target Tracking para garantir que haja uma quantidade adequada `AvailableCapacity` na frota de WorkSpaces aplicativos para atender à demanda e, ao mesmo tempo, determinar os padrões de uso. Continue monitorando, pois o Rastreamento de destino usa uma porcentagem do consumo da frota. Conforme o número total de instâncias de frota cresce, o total de instâncias de frota não utilizadas se multiplica. Isso pode se tornar um desperdício, a menos que a capacidade máxima seja definida como um valor conservador. Use vários tipos de políticas de ajuste de escala (por exemplo, acompanhamento programado e de metas) para equilibrar a confiabilidade com a otimização de custos.

Monitoramento do uso pelos usuários

Monitoramento de usuários únicos, pois há um custo associado na forma de taxas de usuário. Esse custo de taxa de usuário é devido às licenças de acesso de assinantes (SAL) do Image Assistant (RDS). A avaliação de usuários exclusivos pode ser realizada por meio de relatórios do IdP em que a autenticação é realizada ou por meio de relatórios de uso.

Os relatórios de uso são armazenados como arquivos `.csv` separados em seu bucket do S3, que você pode baixar e analisar usando ferramentas de business intelligence (BI) de terceiros. Você pode analisar seus dados de uso AWS sem baixar seus relatórios ou criar relatórios em intervalos de datas personalizados sem concatenar vários arquivos. `.csv` Por exemplo, você pode usar o Amazon Athena e o Amazon Quick para criar relatórios e visualizações personalizados dos dados de uso de seus WorkSpaces aplicativos.

Logs persistentes de aplicativos e eventos do Windows

Quando uma sessão de instância de WorkSpaces aplicativos é concluída, a instância é encerrada. Isso significa que todos os registros de eventos de aplicativos e do Windows usados na sessão são perdidos. Se houver a necessidade de manter esses registros de eventos do aplicativo e do Windows, um método é usar o Amazon Data Firehose para entregá-los em tempo real ao S3 e pesquisar com o OpenSearch Amazon Service (ServiceOpenSearch). Se não houver previsão de que as consultas sejam frequentes, para otimizar o custo, use o Amazon Athena para pesquisar em vez de executar o Amazon Service. OpenSearch

Auditoria da atividade de rede e administrativa

Se ainda não estiver configurado, é uma prática recomendada configurá-lo Conta da AWS com AWS CloudTrailos WorkSpaces aplicativos da Amazon. Para auditar especificamente as chamadas da API de WorkSpaces aplicativos, use a fonte de eventos de filtro com um valor `deappstream.amazonaws.com`.

Habilite os registros de fluxo da VPC para auditar o acesso aos recursos gerenciados pelo cliente. Os registros de fluxo da VPC podem ser publicados no CloudWatch Logs para realizar consultas quando a auditoria é necessária.

O monitoramento da alocação de IP da sub-rede é importante à medida que as frotas de WorkSpaces aplicativos crescem. Relate a atribuição de IP executando a CLI describe-sub-nets para relatar os endereços IP disponíveis em cada sub-rede atribuída às frotas. Garanta que sua

organização tenha capacidade de endereço IP suficiente para atender à demanda de todas as frotas operando na capacidade máxima.

Otimização de custos

O foco da otimização de custos é evitar custos desnecessários. Os principais tópicos incluem entender e controlar onde o dinheiro é gasto e escolher o número mais adequado e correto dos tipos de recursos. Analise os gastos ao longo do tempo e ajuste a escala para atender às necessidades da empresa. Os seguintes recursos de WorkSpaces aplicativos incorrem em taxas pré-pagas:

- Always-On instâncias de frota
- On-Demand instâncias de frota
- On-Demand taxa de instância interrompida
- Instâncias do criador de imagens
- Taxas de usuário

Para obter informações atuais sobre preços, consulte o AWS site para ver os preços dos WorkSpaces aplicativos da Amazon.

Projetando implantações WorkSpaces de aplicativos econômicas

A primeira etapa no planejamento e design da implantação de WorkSpaces aplicativos é usar uma ferramenta de preços simples para estimar a linha de base de suas AWS taxas relacionadas ao seu uso. Forneça o número total de usuários, o uso simultâneo real por hora, o tipo de instância e a utilização da frota. Dessa forma, a ferramenta de preços estima seu preço por usuário. Também mostra a economia de preço estimada quando você usa uma On-Demand frota em vez de uma Always-On frota.

Os clientes gostam do modelo de preços de WorkSpaces aplicativos de pagar somente pelas instâncias que eles provisionam para atender às necessidades de streaming de seus usuários. Esse modelo é diferente dos ambientes de streaming nos aplicativos existentes. Normalmente, eles usam como base o provisionamento para capacidade máxima, mesmo durante noites, fins de semana e feriados, quando a carga é menor. A ferramenta de preços da Amazon AppStream 2.0 fornece apenas uma estimativa das taxas da AWS relacionadas ao uso dos WorkSpaces aplicativos e não inclui nenhum imposto que possa ser aplicado. As taxas reais dependem de vários fatores, incluindo a utilização real dos serviços da AWS.

A Ferramenta de Preços de WorkSpaces Aplicativos é fornecida como uma planilha do Microsoft Excel ou OpenOffice Calc que permite que você insira informações básicas sobre sua frota e, em seguida, fornece uma estimativa de custo para o ambiente de WorkSpaces aplicativos para frotas

sob demanda e sempre ativas com base em seu padrão de uso. Você pode simular custos com base em tendências de uso históricas ou previstas. Com as frotas elásticas, o administrador não precisa prever o uso, nem criar e manter imagens e políticas de ajuste de escala, ao ter esses recursos integrados. As frotas e instâncias elásticas que executam o Amazon Linux 2 (todos os tipos de frota) são cobradas pela duração da sessão de streaming, em segundos, com um mínimo de 15 minutos.

Como otimizar custos com a escolha do tipo de instância

Para instâncias de frotas e construtores de imagens, há uma variedade de famílias e tipos de instâncias diferentes disponíveis que você escolhe para o aplicativo.

Teste de usuário final — A próxima etapa é distribuir a frota de WorkSpaces aplicativos para um grupo de usuários piloto para testes para validar nossa escolha de tipo de instância. É importante solicitar que os usuários piloto testem todos os fluxos de trabalho regulares e pesados a fim de capturar métricas relacionadas à memória, CPU e gráficos, para que você possa capturar métricas básicas de desempenho. O grupo piloto deve conter as várias funções de usuário que usam o aplicativo para garantir que você o teste a partir de várias experiências de usuário. O teste de aceitação do usuário permite que você obtenha feedback sobre a experiência da sessão de streaming. Ao criar ou atualizar uma pilha, há a opção de usar um URL de feedback personalizado. Os usuários são redirecionados para esse URL depois de selecionarem o link Enviar comentários para enviar comentários sobre suas experiências de streaming no aplicativo. Se houver um gargalo de desempenho, use as métricas de desempenho do Windows para analisar as restrições de recursos. Por exemplo, se o tipo de instância de frota atual stream.standard.medium mostrar restrição de recursos, atualize o tipo de instância para stream.standard.large. Por outro lado, se as métricas de desempenho mostrarem altos níveis de subutilização de recursos, considere fazer o downgrade do tipo de instância.

Como otimizar custos com a escolha do tipo de frota

Ao criar uma nova frota de WorkSpaces aplicativos, os desenvolvedores devem escolher o tipo Always- On ou o tipo de On-Demand frota. Ao escolher o tipo de instância do ponto de vista dos preços, é importante entender como o WorkSpaces Applications gerencia as instâncias da frota. Para Always-On frotas, as instâncias da frota permanecem no estado de execução. Portanto, quando os usuários tentam transmitir sessões, as instâncias de frota estão sempre prontas para iniciar as sessões de streaming.

Para On-Demand frotas, depois que as instâncias da frota são lançadas, elas são mantidas no estado parado. A taxa da instância interrompida é menor do que a taxa da instância em execução,

o que pode ajudar a reduzir custos. As instâncias On-Demand da frota devem ser iniciadas a partir de um estado parado. O usuário deve esperar aproximadamente dois minutos para que a sessão de streaming esteja disponível.

As frotas elásticas são boas candidatas para aplicativos independentes e que podem ser instalados em discos rígidos virtuais salvos em um bucket do Amazon Simple Storage Service (Amazon S3). As frotas elásticas podem reduzir ainda mais os custos em alguns casos de uso devido ao faturamento por segundo cobrado somente pela duração do streaming. A taxa é uma função do tipo e tamanho da instância e do sistema operacional escolhido ao criar a frota.

Se os usuários finais precisarem de instâncias da frota durante o horário comercial, é recomendado manter as mesmas sessões de streaming. Isso ocorre porque as instâncias da frota são cobradas por hora e, sempre que uma nova sessão de streaming é iniciada, há outra taxa de instância da frota.

Tabela 10 — Comparação do tipo de frota de WorkSpaces aplicativos

Tipo de frota	Vantagens	Considerações
Always-On	Menos tempo de espera para sessões de streaming	Os usuários pagam pela taxa de instância por hora, pois não há opção de manter as instâncias paradas.
On-Demand	Redução de custos à medida que as instâncias permanece m paradas	Mais tempo de espera para sessões de streaming
Elástica	Per-second o faturamento pode ser útil para casos de uso que têm padrões de uso esporádicos para aplicativos que podem ser instalados no disco rígido virtual	À medida que o tamanho do disco rígido virtual do aplicativ o aumenta, o tempo necessári o para montá-lo em uma instância de streaming pode maior

WorkSpaces O Applications monitora a utilização da sua frota e realiza ajustes automáticos na capacidade da frota para atender à demanda do usuário com o menor custo possível. Os ajustes de capacidade são feitos com base nas políticas de ajuste da escala que você define, com base na

utilização atual ou em um cronograma. Analise regularmente as métricas de uso da frota para validar se as políticas de ajuste da escala não têm altos níveis de capacidade não utilizada.

Políticas de ajuste de escala

Com o Ajuste de escala automático, você pode otimizar os recursos da frota sem precisar comprometer demais os recursos esperando que os usuários façam login. Os administradores podem ajustar o tamanho da frota com base em várias utilizações para atender à demanda do usuário. Use métricas de frota de CloudWatch WorkSpaces aplicativos ou ferramentas de monitoramento de terceiros para aprender sobre a atividade do usuário e configurar políticas de escalabilidade para expandir ou reduzir frotas de WorkSpaces aplicativos com base no uso esperado. Os logs do usuário são um mecanismo essencial para entender o uso real. Esse insight pode ser usado para alterar dinamicamente o tamanho da frota com base no ajuste de escala automático.

Em muitos casos, as frotas de WorkSpaces aplicativos são criadas com base no número máximo de usuários e não são ajustadas para diferentes horários do dia e da semana, como noites e fins de semana. Muitas vezes, a contagem simultânea de usuários de aplicativos transmitidos é menor do que o número total de usuários, principalmente quando os usuários têm a flexibilidade de trabalhar remotamente. É importante considerar esses fatores ao projetar os padrões de uso. A superestimação leva ao provisionamento excessivo de instâncias de WorkSpaces aplicativos, resultando em custos adicionais. Para obter uma configuração ideal, talvez seja necessário combinar uma ou mais políticas de ajuste de escala programadas com políticas de aumento de escala horizontalmente.

Para saber mais sobre a implementação de políticas de escalabilidade, consulte Como escalar suas frotas da Amazon AppStream 2.0.

Taxas de usuário

As taxas de usuário são cobradas por usuário, por mês, em cada Região da AWS caso em que os usuários transmitem aplicativos a partir de instâncias da frota de WorkSpaces aplicativos. Em vez de gerar IDs de usuário diferentes, tenha IDs de usuário consistentes para usuários de WorkSpaces aplicativos. As taxas de usuário não são cobradas ao se conectar aos criadores de imagens.

Escolas, universidades e determinadas instituições públicas podem ter uma taxa de usuário reduzida do Microsoft RDS SAL de 0,44 USD por usuário mensalmente. Para obter os requisitos de qualificação, consulte os Termos e documentos de licenciamento da Microsoft.

Se você tiver o Microsoft License Mobility, poderá se qualificar para trazer suas próprias licenças de acesso para clientes (CALs) do Microsoft RDS e usá-las com os aplicativos da Amazon. WorkSpaces Caso esteja coberto por sua própria licença, não incorrerá em taxas mensais de usuário. Para obter mais informações sobre se você pode usar suas licenças Microsoft RDS CAL existentes com a Amazon WorkSpaces Applications, consulte a orientação de Mobilidade de AWS Licenças ou consulte seu representante de licenciamento da Microsoft.

Uso do Image Builder

WorkSpaces As instâncias do Applications Image Builder são cobradas por hora. A cobrança da instância do Image Builder inclui computação, armazenamento e qualquer tráfego de rede usado pelo protocolo de streaming. Todas as instâncias do Image Builder em execução pagam a taxa de instância em execução aplicável. Essa taxa usa como base o tipo e o tamanho da instância, mesmo quando nenhum administrador está conectado.

Como prática recomendada para otimizar o custo, encerre uma instância do Image Builder quando ela não estiver sendo usada. CloudWatch As regras de eventos podem ser usadas para agendar um trabalho diário, como invocar uma função Lambda para interromper as instâncias do construtor de imagens.

Você pode manter sua imagem de WorkSpaces aplicativos atualizada usando atualizações gerenciadas de imagens de WorkSpaces aplicativos. Esse método de atualização fornece as atualizações mais recentes do sistema operacional e do driver do Windows e o software mais recente do agente de WorkSpaces aplicativos. Ao usar esse método para atualizar imagens, um Image Builder é iniciado automaticamente e interrompido como parte do processo de serviço gerenciado.

Conclusão

Com WorkSpaces os Aplicativos, você pode adicionar facilmente seus aplicativos de desktop existentes AWS e permitir que seus usuários os transmitam instantaneamente. Os usuários do Windows podem usar o cliente de WorkSpaces aplicativos ou um navegador HTML5-capable da Web para streaming de aplicativos. Você pode manter uma única versão de cada um de seus aplicativos, o que facilita o gerenciamento dos aplicativos. Os usuários sempre acessam as versões mais recentes dos aplicativos. Seus aplicativos são executados em recursos AWS computacionais e os dados nunca são armazenados nos dispositivos dos usuários, o que significa que eles sempre têm uma experiência segura e de alto desempenho.

Diferentemente das soluções locais tradicionais para streaming de WorkSpaces aplicativos de desktop, o Applications oferece preços com pagamento conforme o uso, sem investimento inicial e sem infraestrutura para manter. Você pode alterar a escala de forma instantânea e global, garantindo que os usuários sempre tenham a melhor experiência possível.

O Amazon WorkSpaces Applications foi projetado para ser integrado aos sistemas e processos de TI existentes, e este whitepaper descreveu as melhores práticas para fazer isso. O resultado de seguir as diretrizes deste whitepaper é uma implantação econômica de desktop na nuvem que pode ser escalada com segurança com sua empresa na infraestrutura global. AWS

Colaboradores

Os colaboradores deste documento incluem:

- Andrew Wood, arquiteto de soluções sênior, Amazon Web Services
- Andrew Morgan, arquiteto de soluções especializado em EUC, Amazon Web Services
- Arun PC, arquiteto de soluções sênior especializado em EUC, Amazon Web Services
- Asriel Agronin, arquiteto de soluções sênior, Amazon Web Services
- Dustin Shelton, arquiteto de soluções sênior especializado em EUC, Amazon Web Services
- Jeremy Schiefer, arquiteto de soluções sênior, Amazon Web Services
- Navi Magee, arquiteta de soluções principal, Amazon Web Services
- Pete Fergus, engenheiro de suporte de nuvem sênior, Amazon Web Services
- Phil Persson, principal arquiteto de soluções especializado em EUC, Amazon Web Services
- Richard Spaven, arquiteto de soluções sênior especializado em EUC, Amazon Web Services
- Spencer DeBrosse, arquiteto de soluções sênior, Amazon Web Services
- Stephen Stetler, arquiteto de soluções sênior, Amazon Web Services
- Taka Matsumoto, engenheira sênior de suporte de nuvem, Amazon Web Services
- Vasant Sirsat, arquiteto de soluções sênior especializado em EUC, Amazon Web Services

Outras fontes de leitura

Para obter informações adicionais, consulte:

- Guia de administração WorkSpaces de aplicativos da Amazon
- Referência da API WorkSpaces de aplicativos da Amazon
- Use o Amazon FSx for Windows File Server e o FSLogix para otimizar a persistência das configurações do aplicativo nos aplicativos da Amazon WorkSpaces
- Monitorando WorkSpaces aplicativos da Amazon com Amazon ElasticSearch e Amazon Firehose
- Analise seus relatórios de uso de WorkSpaces aplicativos da Amazon usando o Amazon Athena e o Amazon Quick
- Dimensione suas frotas de WorkSpaces aplicativos da Amazon
- Usando AppLocker a Microsoft para gerenciar a experiência de aplicativos na Amazon WorkSpaces Applications
- Usando o domínio personalizado com os WorkSpaces aplicativos da Amazon
- Como faço para usar minhas próprias CALs do Microsoft RDS com WorkSpaces aplicativos?
- Ferramenta de preços de WorkSpaces aplicativos da Amazon
- Crie um teste de software on-line com WorkSpaces aplicativos
- Crie um portal SaaS com aplicativos da Amazon WorkSpaces

Revisões do documento

Para ser notificado sobre atualizações desse whitepaper, inscreva-se no feed RSS.

Alteração	Descrição	Data
Documento atualizado	Atualizações para incluir frotas elásticas, com direitos de aplicativos que usam como base tributos, catálogo de aplicativos de várias pilhas, frotas com base em Linux, entrada e saída de dados, recuperação de desastres e outras atualizações.	14 de junho de 2022
Documento atualizado	Versão HTML publicada.	19 de janeiro de 2022
Publicação inicial	Publicação do whitepaper.	8 de junho de 2021

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não criam nenhum compromisso ou garantia da AWS e de suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos da AWS, e este documento não é parte, nem modifica, qualquer contrato entre a AWS e seus clientes.

© 2023 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.