

Melhores práticas para implantar o Amazon 2.0 AppStream



Melhores práticas para implantar o Amazon 2.0 AppStream :

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais 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 desprestigue 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
Uma VPC com zonas de disponibilidade e uma zona Wavelength.	3
Dimensionamento de sub-rede	4
Roteamento de sub-rede	6
Conectividade intrarregional	6
Tráfego de saída da Internet	6
Infraestrutura	7
Endpoints da VPC	7
Endpoint da VPC para o Amazon S3	7
Endpoint da VPC para interface de API do Amazon AppStream 2.0	9
Endpoint da VPC para interface de streaming do Amazon AppStream 2.0	9
Criação e gerenciamento de imagens	11
Como criar uma imagem do AppStream 2.0	11
Sistema operacional	11
Aplicativos	13
Bloco de aplicativos	14
Personalização de perfil do usuário	15
Segurança	15
Desempenho	16
Seleção da versão do agente do AppStream 2.0	16
Interface de linha de comandos (CLI) do Image Assistant	17
Como gerenciar a experiência de streaming dos usuários	18
Personalização usando scripts de sessão	18
Como usar a Política de grupo do Active Directory	18
Atualizações de imagem	18
Personalização da frota	20
Tipo de frota	20
Dimensionamento da frota	25
Capacidade mínima e ajuste da escala programado	25
Capacidade máxima e cotas de serviço	26

Como escolher a exibição da área de trabalho ou do aplicativo	27
Exibição da área de trabalho	27
Exibição somente de aplicativos	27
Configuração da função do AWS Identity and Access Management	28
Uso de credenciais estáticas	28
Como proteger o bucket do S3 para AppStream 2.0	29
Estratégias de ajuste de escala automático da frota	30
Como entender as instâncias do AppStream 2.0	30
Políticas de dimensionamento	30
Ajuste de escala em etapas	30
Monitoramento do objetivo	30
Ajuste de escala programado	31
Políticas de ajuste de escala na produção	31
Práticas recomendadas para ajuste de escala das políticas de design	33
Combinar políticas do 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
Cliente do AppStream 2.0 para Windows	37
Modos de conexão do cliente do AppStream 2.0	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	46
Opções de serviço	46
Cenários de implantação	46
Cenário 1: Serviços de Domínio do Active Directory (ADDS) implantados no local	47

Cenário 2: estender os serviços de domínio ativo (ADDS) à VPC do cliente da AWS	48
Cenário 3: Microsoft Active Directory gerenciado pela AWS	49
Topologia do site do serviço do Active Directory	50
Unidades organizacionais do Active Directory	52
Limpeza de objetos no computador do Active Directory	52
Segurança	53
Como proteger dados persistentes	53
Estado e dados do usuário	53
Segurança de endpoints e antivírus	55
Como remover identificadores exclusivos	55
Otimização de desempenho	55
Exclusões de verificação	56
Pastas	57
Limpeza do console de segurança de endpoints	58
Exclusões de rede	58
Protegendo uma sessão AppStream	59
Como limitar os controles de aplicativos e sistemas operacionais	59
Firewalls e roteamento	60
Prevenção de perda de dados	60
Controles de transferência de dados de cliente para instância AppStream 2.0	60
Controle do tráfego de saída da instância AppStream 2.0	61
Usando AWS serviços	62
AWS Identity and Access Management	62
VPCendpoints	62
Recuperação de desastres	65
Roteamento de identidade	65
Método 1: como alterar o estado de retransmissão do aplicativo	65
Método 2: como configurar dois aplicativos do AppStream 2.0 no IdP	66
Persistência de armazenamento	66
Monitoramento	68
Usar painéis	68
Como antecipar o crescimento	68
Monitoramento do uso pelos usuários	69
Logs persistentes de aplicativos e eventos do Windows	69
Auditoria da atividade de rede e administrativa	69
Otimização de custo	70
Como projetar implantações econômicas do AppStream 2.0	70

Como otimizar custos com a escolha do tipo de instância	71
Como otimizar custos com a escolha do tipo de frota	71
Políticas de ajuste de escala	73
Taxas de usuário	73
Uso do Image Builder	74
Conclusão	75
Colaboradores	76
Outras fontes de leitura	77
Revisões do documento	78
Avisos	79
.....	lxxx

Práticas recomendadas para implantação do Amazon AppStream 2.0

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

Resumo

Este whitepaper descreve um conjunto de práticas recomendadas para a implantação do [Amazon AppStream 2.0](#). 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. Ele inclui métodos de conexão do usuário, autenticação e integração com o Microsoft Active Directory. Também inclui recomendações para projetar a segurança, o monitoramento e a otimização de custos do AppStream 2.0.

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

Introdução

O [Amazon AppStream 2.0](#) é um serviço de streaming de aplicações totalmente gerenciado que fornece aos usuários acesso instantâneo às aplicações da área de trabalho em qualquer lugar. O AppStream 2.0 gerencia os recursos da AWS necessários para hospedar e executar seus aplicativos. Ele é dimensionado automaticamente e fornece acesso aos seus usuários sob demanda. O AppStream 2.0 fornece aos usuários finais acesso às aplicações de que precisam no dispositivo de sua escolha, com uma experiência de usuário responsiva e indistinguível dos aplicativos instalados nativamente.

As seções a seguir fornecem detalhes sobre o Amazon AppStream 2.0, explicam como o serviço funciona, descrevem o que é necessário para iniciar o serviço e informam quais opções e recursos estão disponíveis para você usar. Ao implantar o AppStream 2.0 para usuários finais, é importante implementar as práticas recomendadas para proporcionar uma experiência de usuário excepcional. Além disso, empresas de todos os portes se beneficiam da otimização de custos que reduz os custos operacionais mensais.

Principais conceitos

Para tirar máximo proveito do AppStream 2.0, familiarize-se com os seguintes conceitos:

- Imagem: uma imagem é um modelo de instância pré-configurado. Uma imagem contém aplicativos que você pode transmitir por streaming para os usuários e configurações padrão do Windows e de aplicativos para permitir que os usuários comecem a usar as aplicações rapidamente. A AWS fornece imagens base 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 AWS](#) ou compartilhá-las com outras contas da Conta da AWS na mesma região.
- Construtor de imagem: um construtor de imagens é uma máquina virtual que você usa para criar uma imagem. Você pode inicializar e se conectar a um construtor de imagens usando o console do AppStream 2.0. 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 o AppStream 2.0 em uma VPC dedicada. Ao projetar o AppStream 2.0 VPC, dimensione de acordo com 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 projeto do AppStream 2.0 é que somente um usuário pode consumir uma instância do AppStream 2.0. Ao alocar o espaço IP, pense em um usuário como um endereço IP por instância do AppStream 2.0. Com o AppStream 2.0, é possível que um usuário consuma várias instâncias do AppStream 2.0. Portanto, o planejamento do espaço IP também deve considerar os casos de uso que exigem instâncias adicionais do AppStream 2.0.

Embora o tamanho máximo de um Encaminhamento Entre Domínios Sem Classificação (CIDR) do VPC seja /16, a AWS é recomendável não alocar em excesso os endereços IP privados. 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 do AppStream 2.0 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.

Uma VPC com zonas de disponibilidade e uma zona Wavelength.

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 mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

O Amazon AppStream 2.0 exige apenas uma sub-rede para execução em 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. A escalabilidade 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 dois IDs de [sub-rede](#).

Dimensionamento de sub-rede

Dedique sub-redes às frotas do AppStream 2.0 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 do AppStream 2.0 podem ter requisitos de isolamento dando lugar a conjuntos de regras separados. Quando várias frotas do Amazon AppStream 2.0 usam as mesmas sub-redes, verifique se a soma da capacidade máxima de todas as frotas não excede 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 “[atualização de frota](#)” da CLI da AWS para atribuir mais sub-redes. Para obter mais informações, consulte as [cotas da Amazon VPC e como aumentá-las](#).

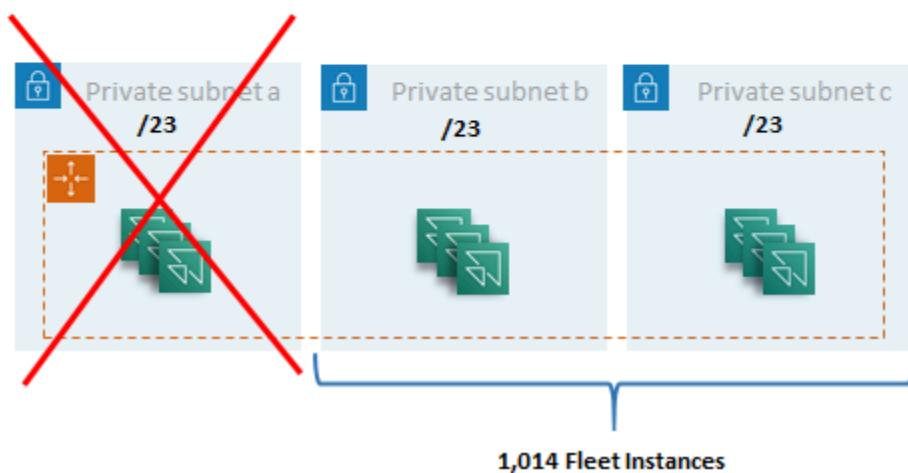
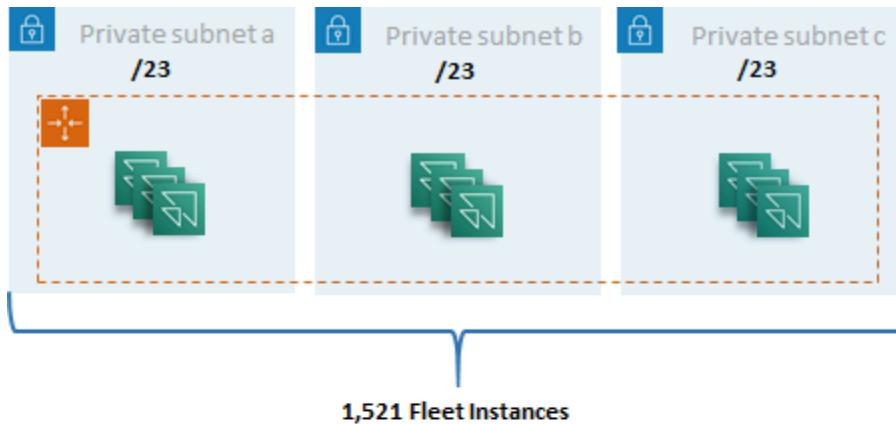
A prática recomendada é aumentar a escala horizontalmente das sub-redes, dimensionando-as adequadamente e reservando a capacidade de crescimento na VPC. Além disso, garanta que os limites máximos da frota do AppStream 2.0 não excedam o espaço IP total alocado pelas sub-redes. Para cada entrada de sub-rede na 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 produtividade ao dimensionar automaticamente as instâncias da frota
- Uso mais eficiente de endereços IP privados, evitando a codificação permanente do IP

Ao dimensionar sub-redes para o Amazon AppStream 2.0, 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. No Amazon AppStream 2.0, a soma das instâncias da frota do AppStream 2.0 consumidas e disponíveis para consumo é rotulada como `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, 3 x/23 sub-redes satisfazem os 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 expandir as instâncias da frota é limitada pela taxa de transferência de uma AZ. Isso pode estender a duração do PendingCapacity.

Roteamento de sub-rede

É uma prática recomendada criar sub-redes privadas para instâncias do AppStream 2.0, roteando para a Internet pública por meio de uma VPC centralizada para tráfego de saída. O tráfego de entrada para o streaming da sessão do AppStream 2.0 é tratado pelo serviço Amazon AppStream 2.0 por meio de gateways de streaming: você não precisa configurar sub-redes públicas para isso.

Conectividade intrarregional

Para instâncias de frota do AppStream 2.0 unidas a um domínio do Active Directory, configure os controladores de domínio do Active Directory em uma VPC de serviços compartilhados em cada 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 do AppStream 2.0 pode ser feito por meio de uma [conexão de emparelhamento da 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 verdadeiro se as instâncias do AppStream 2.0 se conectarem à infraestrutura de aplicativos e/ou servidores de arquivos 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 emparelhamento, o tráfego de saída para o AppStream 2.0 pode ser projetado [criando um único ponto de saída de Internet a partir de várias VPCs usando o AWS Transit Gateway](#). 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 VPC, gateways NAT ou as instâncias NAT são uma opção comum de design. Para determinar o que é melhor para a organização, consulte o guia de administração para [comparar gateways e instâncias NAT](#). [AWS O 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 firewall de rede da AWS](#). 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.

Infraestrutura

Quando for necessária conectividade com recursos locais, principalmente para instâncias do AppStream 2.0 associadas ao Active Directory, estabeleça uma conexão altamente [resiliente por meio da AWS Direct Connect](#).

Endpoints da VPC

Endpoint da VPC para o Amazon S3

Muitas implantações do Amazon AppStream 2.0 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 custos para os requisitos de acesso à rede do AppStream 2.0
- 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 das instâncias do AppStream 2.0

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 nome

do recurso da Amazon (ARN) da função de gerenciamento de identidade e acesso do serviço AppStream 2.0. 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

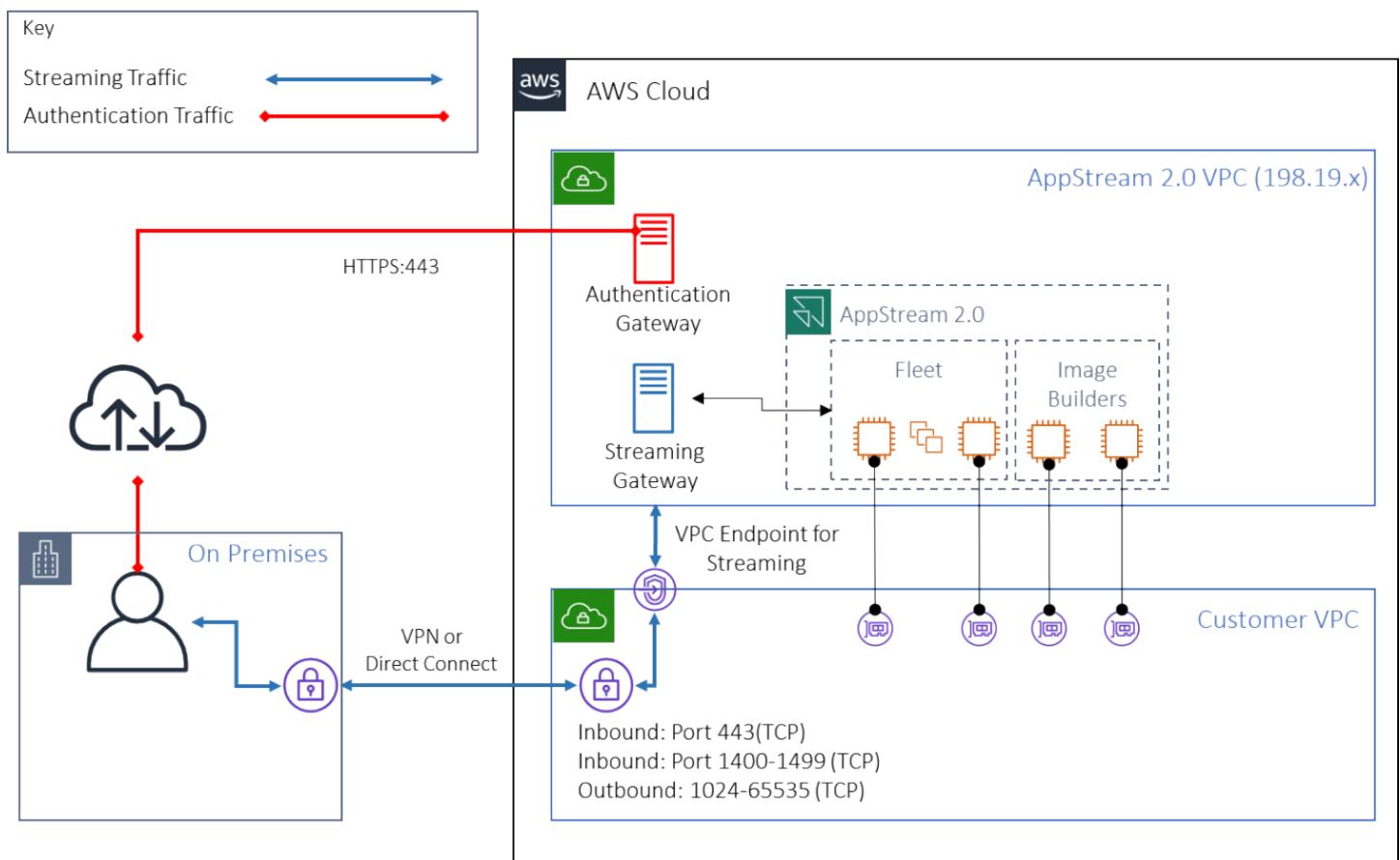
```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Allow-AppStream-to-access-home-folder-and-  
application-settings",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:sts::account-id-without-hyphens:assumed-  
role/AmazonAppStreamServiceAccess/AppStream2.0"  
            },  
            "Action": [  
                "s3>ListBucket",  
                "s3GetObject",  
                "s3PutObject",  
                "s3DeleteObject",  
                "s3GetObjectVersion",  
                "s3DeleteObjectVersion"  
            ],  
            "Resource": [  
                "arn:aws:s3:::appstream2-36fb080bb8-*",  
                "arn:aws:s3:::appstream-app-settings-*"  
            ]  
        }  
    ]  
}
```

Endpoint da VPC para interface de API do Amazon AppStream 2.0

Em cenários de design em que os comandos de API e CLI para o Amazon AppStream 2.0 se originam na sua VPC, privatize essas chamadas programáticas por meio de uma [interface de endpoint da VPC](#).

Endpoint da VPC para interface de streaming do Amazon AppStream 2.0

Embora seja possível [rotear o tráfego de streaming do Amazon AppStream 2.0 por meio de um endpoint da VPC para interface](#), 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 do Amazon AppStream 2.0.



Endpoint da VPC para interface de streaming do Amazon AppStream 2.0

Conforme mostrado na figura anterior, a Internet pública é o caminho mais eficiente para os gateways de streaming do Amazon AppStream 2.0. 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 pré-requisito de acesso, como o provedor de identidades (IdP) para autenticação única (SSO) de SAML, continua sendo um requisito acessível somente pela Internet pública.

Criação e gerenciamento de imagens

Ao iniciar uma frota ou um construtor de imagens no AppStream 2.0, você deve selecionar uma das imagens base do AppStream 2.0. 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.

Como criar uma imagem do AppStream 2.0

Ao criar uma nova imagem, é importante considerar:

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

Como criar uma imagem do AppStream 2.0

Em novembro de 2021, o AppStream 2.0 lançou suporte para o Amazon Linux 2. Com esse anúncio, o AppStream 2.0 agora oferece 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)	<p>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.</p> <p>Você quer usar a Política de Grupo existente em suas instâncias de streaming do AppStream 2.0 (o Linux não adere à Política de Grupo, mas você pode usar scripts de sessão para automatizar a configuração quando uma sessão é iniciada).</p> <p>Você usará a Visualização de área de trabalho e seus usuários vão preferir a experiência de área de trabalho do Windows.</p> <p>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).</p> <p>Você deseja usar a persistência das</p>	<p>Taxa RDS SAL (Microsoft Remote Desktop Services Subscriber Access License) de 4,19 USD por mês para cada usuário exclusivo** mais o seguinte:</p> <ol style="list-style-type: none"> 1. 0,10 USD por hora para frotas sempre ativas e sob demanda 2. 0,15 USD por hora para frotas elásticas

Tipos de plataforma	Quando usar	Preços da frota*
	<p><u>configurações do aplicativo.</u></p> <p>No momento, não há suporte à ativação da persistência das configurações de aplicações em pilhas baseadas em Linux.</p>	
Amazon Linux 2	<p>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</p>	<p>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:</p> <ol style="list-style-type: none"> 1. 0,084 USD por hora para frotas sempre ativas e sob demanda 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 do AppStream 2.0](#) 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 AppStream 2.0 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 do AppStream 2.0 associada a um domínio do Microsoft Active Directory. Para obter mais informações, consulte [Como usar o Active Directory com o AppStream 2.0](#).

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 frotas com base em Windows, é recomendado criar um arquivo VHDX para conter seu aplicativo. Para frotas com base em Linux, é recomendado 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 para configuração do Windows PowerShell](#) 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 AppStream 2.0 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 nas quais a persistência das configurações do aplicativo é necessária, a AWS recomenda proteger essa conexão por meio de uma política personalizada e do endpoint do gateway de VPC do S3. 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 Image Builder do AppStream 2.0. Isso inclui adicionar e modificar chaves de registro, adicionar arquivos e outras configurações específicas do usuário. No Image Assistant do AppStream 2.0, 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 para Windows File Server e o FSLogix para otimizar a persistência das configurações do aplicativo no Amazon AppStream 2.0](#).

Segurança

Os desenvolvedores precisam considerar diferentes medidas de segurança. Os administradores do AppStream 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 [Manter a imagem do AppStream 2.0 atualizada](#) a fim de obter orientações adicionais sobre como manter as imagens básicas atualizadas.

Por padrão, o AppStream 2.0 permite 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. O Microsoft AppLocker é um software de controle de aplicativos que usa políticas de controle explícitas para ativar ou desativar quais aplicativos um usuário pode executar.

O software antivírus pode afetar adversamente as sessões de streaming e as instâncias do construtor de imagens. A 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

Seleção da versão do agente do AppStream 2.0

Ao criar uma nova imagem, você pode optar por usar o software de agente do AppStream 2.0 mais recente ou não atualizar. Cada versão do software do agente do AppStream 2.0 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 do AppStream 2.0 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 do AppStream 2.0, use a CLI do Image Assistant. Isso está disponível em construtores de imagens com o software de agente do AppStream 2.0 lançado em ou após 26 de julho de 2019. A visão geral de alto nível a seguir descreve o processo para criar uma imagem do AppStream 2.0 de forma programática.

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` da CLI do Assistente de Imagens para especificar o manifesto de otimização e metadados da aplicação para a imagem do AppStream 2.0.
4. Para especificar aplicações adicionais para a imagem do AppStream 2.0, repita as etapas de 1 a 3 para cada aplicação, 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 sua imagem do AppStream 2.0 de forma programática usando as operações da CLI do Image Assistant](#).

Como gerenciar a experiência de streaming dos usuários

Personalização usando scripts de sessão

O AppStream 2.0 fornece 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 do AppStream 2.0 antes de iniciar as 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 do AppStream 2.0. 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 do AppStream 2.0 em um domínio do Active Directory, é possível usar Objetos de políticas de grupo (GPOs) para gerenciar a experiência do usuário. Os GPOs podem ser atribuídos à Unidade organizacional (OU) em que as instâncias do AppStream 2.0 são criadas. Para simplificar a criação de imagens, inicie a imagem básica do AppStream 2.0 em uma OU que bloqueia a herança. Isso evita que outras políticas de domínio afetem as experiências de usuário do AppStream 2.0. A implantação de cada frota em sua OU dedicada, com GPOs exclusivos e estabelecendo o ambiente, permitindo o benefício consolidado de um para muitos do gerenciamento de imagens do AppStream 2.0.

Um exemplo de uso da Política de Grupo é especificar o conjunto de imagens de [diferentes páginas iniciais do Internet Explorer para cada frota do AppStream 2.0](#).

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](#) do [Well-Architected Framework](#).

Quando sua imagem é criada e implantada, há quatro categorias de software que exigem patches na imagem do AppStream 2.0:

- 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 do AppStream 2.0 (por exemplo, o agente do [Amazon CloudWatch](#)). O AppStream 2.0 lança periodicamente novas imagens básicas com 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.
- Agente do AppStream 2.0: 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 sua imagem do AppStream 2.0 atualizada executando uma das seguintes ações:

- [Atualizar uma imagem usando atualizações de imagem gerenciadas do AppStream 2.0](#): esse método de atualização oferece as atualizações do sistema operacional Windows e as atualizações de drivers mais recentes, além do software de agente do AppStream 2.0 mais recente. 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.
- [Atualizar o software do agente do AppStream 2.0 usando versões de imagem gerenciadas do AppStream 2.0](#): esse método de atualização fornece o software mais recente do agente do AppStream 2.0. 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:

- Sempre ativa: esse tipo de frota fornece os usuários acesso instantâneo aos aplicativos. Você será cobrado por todas as instâncias em execução na frota, mesmo se nenhum usuário estiver fazendo streaming de aplicativos.
- Sob demanda: selecione esse tipo de frota para otimizar os 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 dão suporte a imagens do AppStream 2.0, nem exigem políticas de escalabilidade. Você será cobrado apenas pela duração de uma sessão de streaming.

Tabela 2: tipos de frota do Amazon AppStream 2.0

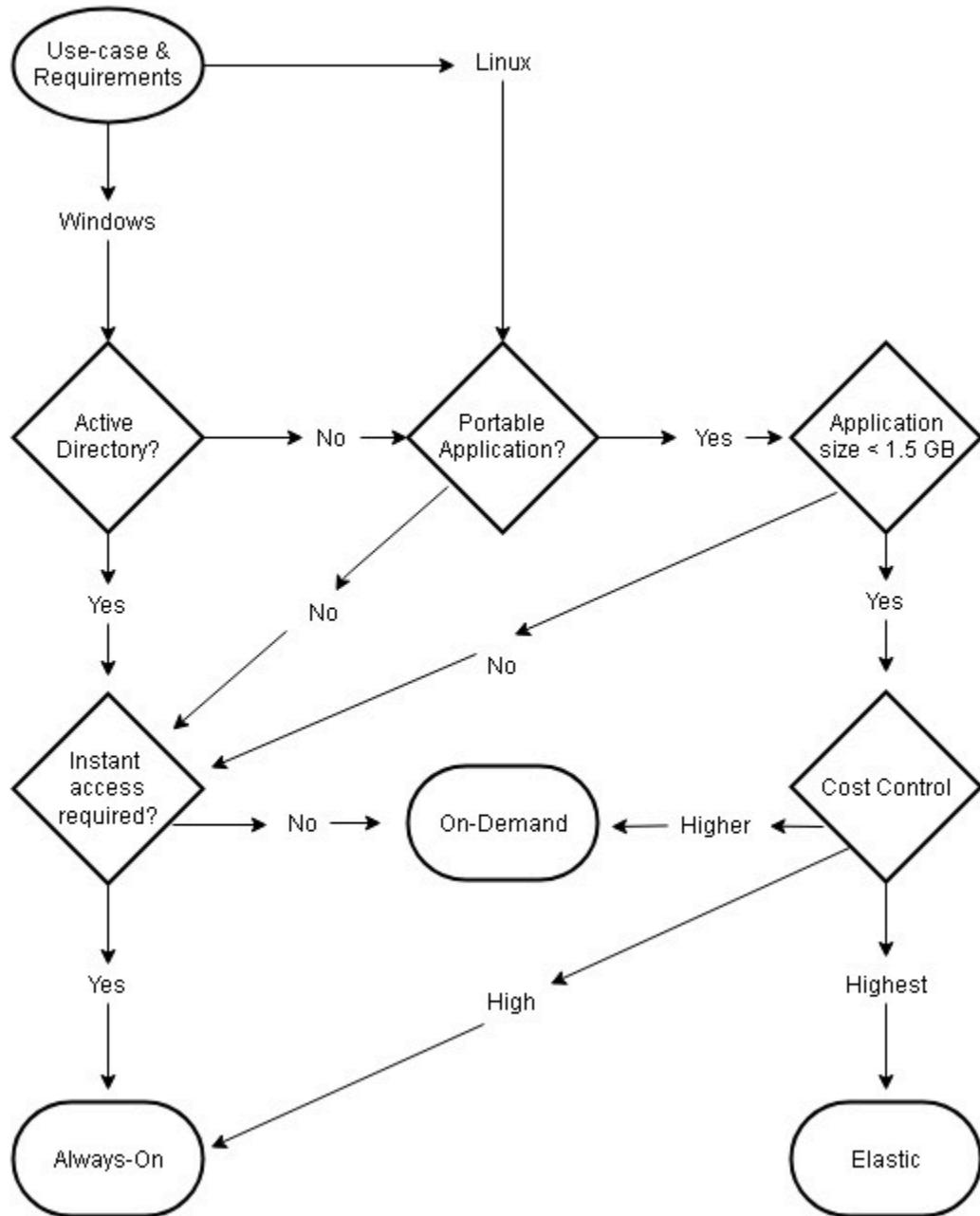
Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
Sempre ativo	Os usuários precisam de acesso instantâneo aos aplicativos quando	Acesso instantâneo aos aplicativos	Você paga o preço total por cada instância disponível na frota (independ	Oferece suporte a políticas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

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
	<p>iniciam uma sessão. Você não terá excesso significativo de capacidade e em sua frota, talvez porque os padrões de uso sejam previsíveis e seja possível controlar os custos de modo confiável com políticas de escalabilidade.</p>		<p>entemente de ser usada para uma sessão).</p>	

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
Sob demanda	<p>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.</p> <p>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.</p>	<p>Os usuários esperam de um a dois minutos para acessar os aplicativos depois de iniciar uma sessão.</p>	<p>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.</p>	<p>Oferece suporte a políticas personalizadas de imagem e escalabilidade.</p>

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
Elástica	<p>O aplicativo e suas dependências têm menos de ~1,5 GB.</p> <p>Sempre 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.</p> <p>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, o aplicativo e todas as suas dependências podem ser colocados em um VHD e iniciados a partir</p>	<p>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).</p>	<p>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.</p>	<p>Não há suporte a imagens personalizadas (o cliente fornece aplicativos ao VHD) nem a políticas de escalabilidade. Atualmente, dá suporte para instâncias de stream.standard.small e stream.standard.medium. Caso seu caso de uso exija um tipo de instância diferente, entre em contato com a equipe da sua conta da AWS.</p>

Tipo de frota	Quando usar	Experiência do usuário	Modelo de definição de preços	Observações
	<p>do VHD. Não são necessári as instâncias de streaming unidas ao domínio (atualmente, a associação de domínios não está disponíveis com frotas elásticas). Você quer pagar somente pelas sessões ativas (ou seja, não pagar pela capacidade não utilizada em sua frota).</p> <p>Os usuários podem esperar 45 segundos ou mais para acessar os aplicativos depois de iniciar uma sessão.</p> <p>Você deseja que a AWS gerencie a escalabilidade (sem políticas de escalabilidade para gerenciar).</p>			



Casos de uso e requisitos do tipo de frota

Dimensionamento da frota

Capacidade mínima e ajuste da escala programado

Ao dimensionar sua frota do AppStream 2.0, há várias considerações que se traduzem diretamente na experiência do usuário e no custo. O valor inserido para Capacidade mínima garante que o

número de instâncias do AppStream 2.0 raramente seja menor do que esse valor. Após o término de uma sessão do AppStream 2.0, se o total de instâncias for menor que o valor mínimo da capacidade, uma nova instância de frota será iniciada. Como sempre, é importante lembrar que uma instância do AppStream 2.0 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 inefficiente 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 maior do que a [cota de serviço da frota do AppStream 2.0](#) na Conta da AWS pode parecer válido, mas, quando eventos de ajuste de escala automático tentam escalar recursos até a capacidade máxima, eles não são iniciados, pois o valor máximo da capacidade 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. Apenas uma exibição pode ser acessada por vez por frota do AppStream 2.0. 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.

Os relatórios de uso do AppStream 2.0 criam um relatório diário de aplicativos para a Exibição da área de trabalho. A saída resultante para o aplicativo é simplesmente “área de trabalho”, mapeada diretamente para a sessão do AppStream 2.0. Para obter mais informações, consulte a seção [Monitoramento do uso pelo usuário](#) deste documento.

Exibição somente de aplicativos

A exibição Somente de aplicativos também é eficaz quando a pilha do AppStream 2.0 deve 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 a Exibição de

aplicativos, o AppStream 2.0 substitui o shell padrão do Windows por um personalizado. Esse shell personalizado apresenta apenas aplicativos em execução, minimizando a superfície de ataque do sistema operacional.

Para casos de uso em que o AppStream 2.0 é usado para ampliar o ambiente de desktop de uma organização existente, a visualização Somente aplicativos é preferida. Implante o Cliente Windows do AppStream 2.0 no [modo de aplicativo nativo](#) para minimizar a confusão do usuário, permitindo o uso total dos atalhos do teclado.

Os relatórios de uso do Amazon 2.0 criam um relatório diário do aplicativo para visualização. 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 o Microsoft AppLocker no modo de relatório ou considerar soluções que estão disponíveis no AWS Marketplace, como o [Stratusphere UX](#) da Liquidware.

Configuração da função do AWS Identity and Access Management

Se uma workload exigir que os usuários finais do AppStream 2.0 acessem outros serviços da AWS na sessão, é uma prática recomendada delegar o acesso por meio do uso de [perfis do 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 ver outras práticas recomendadas ao usar perfis do IAM com o AppStream 2.0, [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 serviço AWS 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 do AppStream 2.0 para acessar as chaves de acesso da função associada. Isso pode ser feito invocando o provedor de credenciais e analisando a saída da chave de acesso e da chave secreta. Confira um exemplo de como realizar essa ação no PowerShell.

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

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

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

Como proteger o bucket do S3 para AppStream 2.0

Caso a workload do AppStream 2.0 esteja configurada com pasta inicial e/ou persistência de aplicativos, é uma prática recomendada proteger o bucket do Amazon S3 no qual os dados persistentes são 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

Como entender as instâncias do AppStream 2.0

As instâncias de frota do AppStream 2.0 têm uma proporção de 1:1 de usuário para instância de 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 dimensionamento

As frotas do AppStream 2.0 são lançadas em um Grupo de ajuste de escala automático do aplicativo. Isso permite que a frota seja dimensionada com base no uso para atender à demanda. À medida que o uso aumenta, a frota aumenta 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 [Ajuste de escala automático da frota para Amazon AppStream 2.0](#).

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 por etapas são acionadas pelas [métricas do CloudWatch no AppStream 2.0](#) de Capacity Utilization, Available Capacity ou Insufficient Capacity Errors.

Ao usar políticas de escalabilidade por etapas, a 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 evitaria situações em que você expande muito lentamente (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 Ajuste de escala automático de aplicativos cria e gerencia os alarmes do CloudWatch que acionam a política de ajuste de escala. 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 as métricas do CloudWatch da 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.

Ajuste de escala programado

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 bi AppStream 2.0 com métricas do CloudWatch pode ajudar você a otimizar as políticas de ajuste de escala 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 análise das métricas do CloudWatch pode promover ajustes nas políticas de ajuste de escala para ajudar a reduzir esses erros. Para obter mais informações e exemplos de políticas de ajuste de escala do AppStream 2.0 que você pode usar, consulte [Dimensionar as frotas do Amazon AppStream 2.0](#).

Práticas recomendadas para ajuste de escala das políticas de design

Combinar políticas do ajuste de escala

Muitos clientes optam por combinar diferentes tipos de políticas de ajuste de escala em uma única frota para aumentar a potência e a flexibilidade do Ajuste de escala automático no AppStream 2.0. 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 escalabilidade por etapas para manter um nível específico de utilização e aumentar, ou reduzir, a escala 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 as métricas do CloudWatch para a 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

Os clientes que gerenciam frotas do AppStream 2.0 para um grande número de usuários devem considerar os 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 AppStream 2.0 provisiona a uma taxa máxima de 20 instâncias por minuto.
- Para uma única Conta da AWS, o AppStream 2.0 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 escalabilidade paralela 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 quiser ajustar a escala de uma única frota de 0 a 1.000 instâncias, serão necessários 50 minutos ($1.000 \text{ instâncias} / 20 \text{ instâncias por minuto}$) 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, um total de 65 a 75 minutos.
- Se quiser ajustar a escala simultaneamente de três frotas de 0 a 333 instâncias (um total de 999 instâncias na Conta da AWS), serão necessários aproximadamente 17 minutos ($999 / 60 \text{ instâncias por minuto}$) para que todas as frotas concluam o provisionamento e, em seguida, mais 15 minutos para que elas 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 escalabilidade. A métrica PendingCapacity do CloudWatch é um ponto de partida para avaliar a otimização do design na AZ da frota em grandes implantações. Um valor alto e sustentado de

PendingCapacity pode indicar a necessidade de ampliar a escala horizontal (entre AZs). Para obter mais informações, consulte [Monitoramento dos recursos do Amazon AppStream 2.0](#).

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 as zonas de disponibilidade e o projeto do AppStream 2.0, consulte [Zonas de disponibilidade](#) neste documento.

Monitorar métricas de erro de capacidade insuficiente

“Erro de capacidade insuficiente” é uma métrica do CloudWatch para frotas do AppStream 2.0. Esta métrica especifica o número de solicitações de sessão rejeitadas por falta de capacidade.

Ao fazer alterações em suas políticas de ajuste da escala, é útil criar um alerta do CloudWatch para notificar você quando ocorrerem erros de capacidade insuficiente. Assim, é possível ajustar rapidamente as políticas de escalabilidade e otimizar a disponibilidade para os usuários. O guia de administração fornece etapas detalhadas para [monitorar seus recursos do AppStream 2.0](#).

Métodos de conexão

Ao fazer streaming de sessões no AppStream 2.0, os usuários têm dois métodos de conexão disponíveis:

- Acesso ao navegador da Web: há suporte para qualquer navegador compatível com HTML5. Não são necessários plug-ins ou downloads.
- Cliente do AppStream 2.0 para Windows

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

O AppStream 2.0 não é compatível com 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	Cliente do AppStream 2.0 para Windows
Vários monitores (resolução de até 2K)	Compatível	Compatível
Vários monitores (resolução de até 4K)	N/D	Compatível
Suporte para tablets de desenho	Compatível*	Compatível
Suporte a dispositivos com tela sensível ao toque	Compatível	N/D

	Acesso pelo navegador da web	Cliente do AppStream 2.0 para Windows
Suporte para dispositivos com passagem de USB	N/D	Compatível
Atalhos de teclado	Compatível	Compatível
Deslocamento relativo do mouse	Compatível	Compatível
Transferência de arquivos	Compatível	Compatível
Redirecionamento de impressora local	N/D	Compatível
Redirecionamento de unidade local	N/D	Compatível
Suporte para webcam	Compatível	Compatível

*Somente Google Chrome e Mozilla Firefox

Acesso pelo navegador da web

O acesso ao [navegador da Web](#) do AppStream 2.0 permite o acesso aos aplicativos sem precisar instalar um cliente dedicado. Os usuários podem se conectar usando um navegador compatível com HTML5. 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.

Cliente do AppStream 2.0 para Windows

O cliente do AppStream 2.0 [para Windows](#) é um aplicativo que deve ser instalado no computador com Windows. Ele fornece atributos adicionais que não estão disponíveis ao acessar o AppStream 2.0 usando um navegador da web. Por exemplo, o cliente do AppStream permite que você:

- Use mais de dois monitores ou resolução 4K

- Use dispositivos USB com aplicativos transmitidos por streaming do AppStream 2.0
- 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

Modos de conexão do cliente do AppStream 2.0

O cliente AppStream 2.0 fornece dois modos de conexão: modo de aplicativo nativo e 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 do AppStream 2.0. 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. Ao contrário dos ícones dos aplicativos locais, os ícones dos aplicativos de streaming no modo nativo incluem o logotipo do AppStream 2.0. 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 AppStream 2.0 sozinhos, ou os administradores podem instalar o cliente AppStream 2.0 para eles executando scripts PowerShell remotamente, ou reempacotando o cliente AppStream 2.0 usando 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 pelo AppStream 2.0 e não poderá ser compartilhado com a sessão. Depois que os dispositivos estiverem qualificados, os usuários deverão compartilhar os dispositivos com o AppStream 2.0 sempre que iniciarem uma nova sessão de streaming.

Ao implantar o cliente AppStream 2.0 em grande escala, a AWS recomenda o uso da [Enterprise Deployment Tool](#). A Enterprise Deployment Tool inclui os arquivos de instalação do cliente do AppStream e um modelo administrativo da Política de Grupo.

Domínios personalizados

Ao implantar o AppStream 2.0 programaticamente, é possível criar um [domínio personalizado](#) que pode fornecer aos usuários uma experiência familiar para sessões de streaming. Nas implantações de IdP do SAML 2.0 no AppStream 2.0, é importante destacar que o acesso do usuário começa no IdP, não no AppStream 2.0. Os usuários não precisam de URLs do AppStream 2.0, 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 a AppStream versão 2.0, a autenticação pode ocorrer fora da Amazon AppStream 2.0 ou como parte do serviço AppStream 2.0. Selecionar como a autenticação ocorrerá para sua implantação AppStream 2.0 é uma consideração fundamental do seu design. Não é incomum que uma organização tenha várias implantações do AppStream 2.0 para diferentes casos de uso. Cada caso de uso pode ter um método de autenticação diferente.

Há três tipos de métodos de autenticação para AppStream 2.0:

- [SAML 2.0](#)
- [Grupo de usuários](#)
- Programático

Como determinar o método otimizado

O Amazon AppStream 2.0 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 AppStream imagem 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 infraestrutura de back-end da Microsoft	SAML 2.0

Exemplo	Descrição	Autenticação
Autenticação única (SSO) empresarial existente	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 temporários 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 sobrecarga de manutenção de um provedor de identidades (IdP)	Grupo de usuários
Provedor de software independente (ISV)	Solução proprietária criada por sua organização que inclui autorização e autenticação do usuário, estendendo a AppStream versão 2.0 como parte de sua solução. *	Programático

Exemplo	Descrição	Autenticação
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 do Embed AppStream 2.0](#) 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 AppStream 2.0 para garantir que a solução de autenticação não entre em conflito com ele.

Configuração do provedor de identidade

SAML 2.0

A Security Assertion Markup Language (SAML) 2.0 é uma opção comum de implantação para [permitir que os usuários usem recursos da AWS](#). Vários [provedores de identidade SAML 2.0 terceirizados](#) oferecem suporte ao AppStream 2.0. [Independentemente de seus recursos AppStream 2.0 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 AppStream 2.0 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 2.0. AppStream

O guia de administração AppStream 2.0 fornece um exemplo de configuração para o design de uma única pilha AppStream 2.0. 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 na AppStream versão 2.0 é uma opção válida para pequenas provas de conceito. Como prática recomendada, é melhor evitar grupos de usuários em qualquer caso de uso e organização que use AppStream 2.0 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 AppStream 2.0 de um serviço centralizado (normalmente ISVs), a autenticação programática depende de um aplicativo para fazer chamadas programáticas para transmitir informações dinamicamente e criar uma sessão 2.0 AWS para seus usuários. AppStream 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 AppStream 2.0 exato da pilha na seção Recursos em vez do padrão '*'. Por exemplo: .

Example

```
{  
    "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 AppStream 2.0 usando a API describe stacks ou a AWS CLI.](#)

AppStream As instâncias 2.0 devem começar como instâncias genéricas. Por meio das informações passadas do aplicativo, a instância AppStream 2.0 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-chaveCreateStreamingURL, como ID do cliente ou configurações de conexão do banco de dados, para serem usados na AppStream sessão.

Direito à inscrição

AppStream 2.0 pode 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 AppStream 2.0 Dynamic Application Framework.

Os direitos de aplicação com base em atributos usando SAML 2.0 são recomendados para a maioria dos cenários. Para gerenciar a entrega de pacotes de aplicativos, é recomendado usar o Dynamic Application Framework.

Integração com o Microsoft Active Directory

As frotas e os construtores de imagens do Amazon AppStream 2.0 podem ser integrados ao Microsoft Active Directory. Dessa forma, você fornece um método centralizado para autenticação e autorização de usuários, além de aplicar políticas de grupo do Active Directory às instâncias do AppStream 2.0 associadas ao domínio. Use as frotas do AppStream unidas a um domínio para ter 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 AppStream 2.0 com o Active Directory, é importante observar que a autenticação inicial na pilha do AppStream 2.0 ainda é gerenciada por um IdP SAML2.0. 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 o AppStream 2.0, há duas opções de serviço e muitos cenários de implantação disponíveis. Além disso, a rede do AppStream 2.0 deve ser 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 \(AD\) gerenciado pela AWS](#). AWS O Microsoft AD 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 seguintes cenários de implantação listados são opções de integração usadas e recomendadas para o AppStream 2.0 com o Microsoft Managed AD ou o Active Directory autogerenciado do cliente. Todos os diagramas de arquitetura listados abaixo usam as principais estruturas da Amazon.

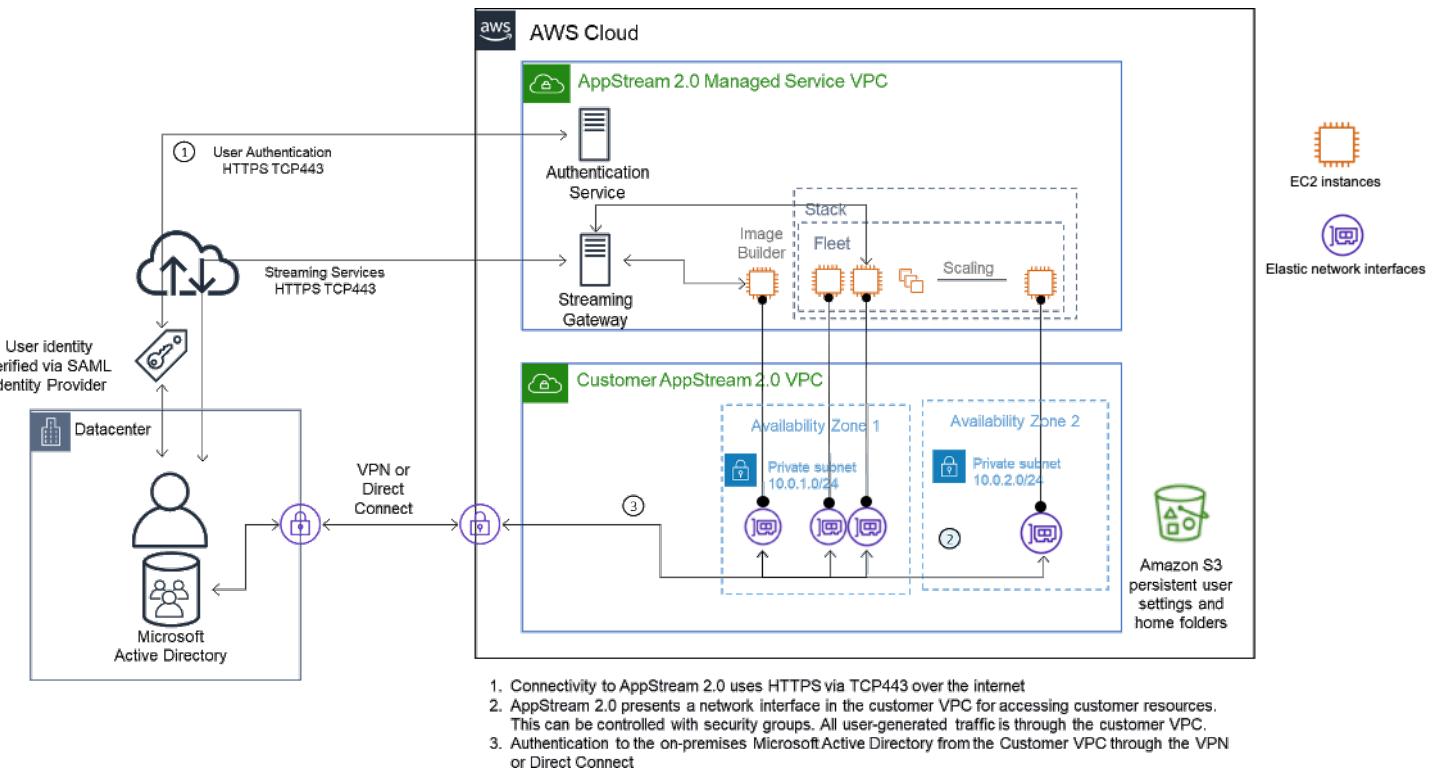
- Amazon Virtual Private Cloud (VPC): criação de uma Amazon VPC dedicada aos serviços AppStream 2.0 com pelo menos quatro sub-redes privadas espalhadas por quatro AZs. Duas das sub-redes privadas são usadas para frotas do AppStream e construtores de imagem. As duas sub-

redes restantes são usadas para os controladores de domínio no EC2 ou no Microsoft Managed AD.

- Conjunto de opções do Protocolo de Configuração Dinâmica de Host (DHCP): fornece um padrão para transmitir informações de configuração para a frota do AppStream 2.0 e os construtores de imagem que serão provisionados na VPC. O conjunto de opções do DHCP é definido no nível da VPC. Dessa forma, permite que os clientes definam um nome de domínio e configurações de DNS específicas que serão usadas com a instância do AppStream 2.0 após o provisionamento.
- AWS Serviços de diretório: o Amazon Microsoft Managed AD pode ser implantado em duas sub-redes privadas que serão usadas em conjunto com as cargas de trabalho do AppStream 2.0.
- Frotas do AppStream 2.0: as frotas do AppStream 2.0 ou os construtores de imagem são hospedados na VPC gerenciada da AWS. Cada instância do AppStream 2.0 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

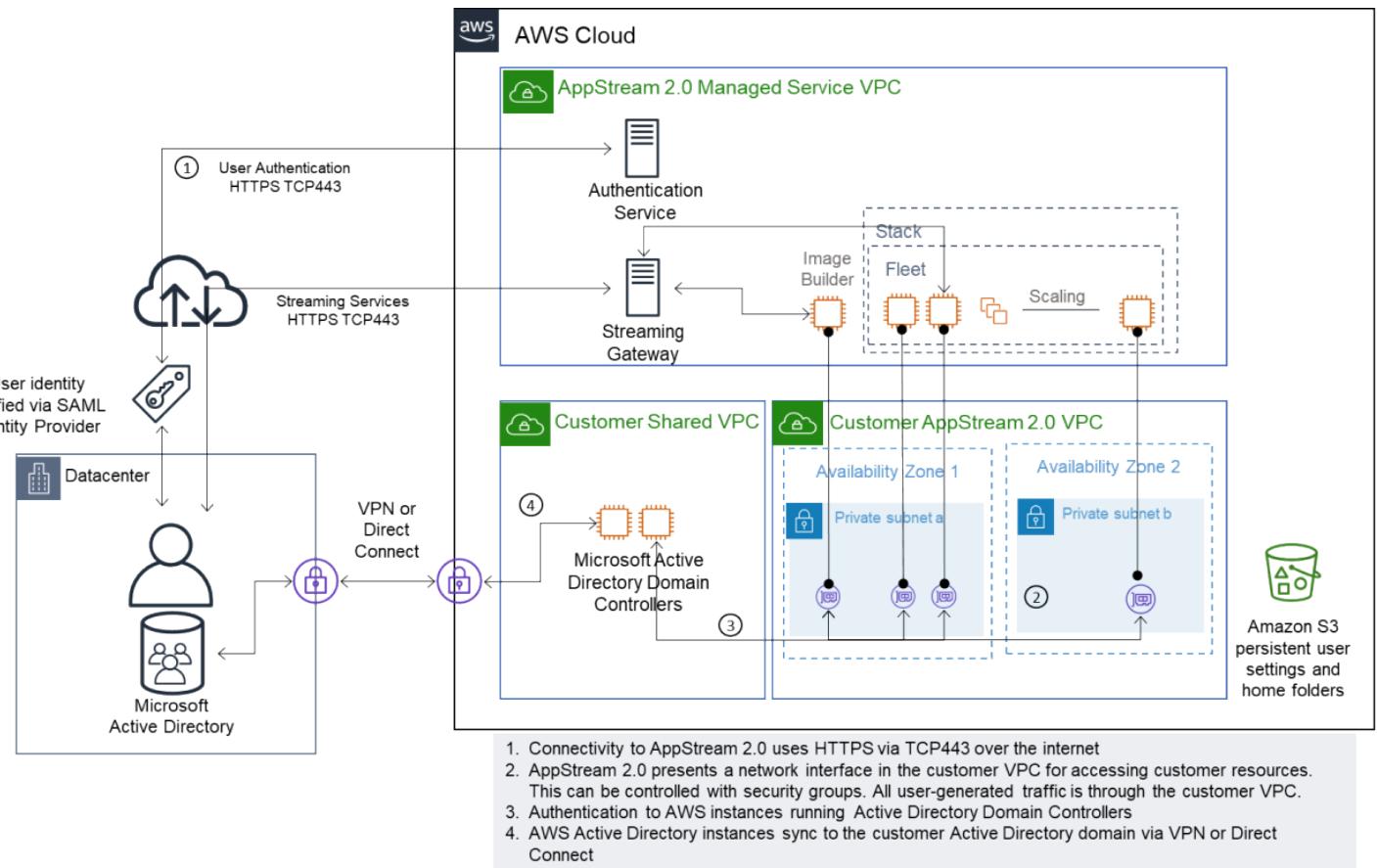
Todo o tráfego de autenticação atravessa a conexão VPN ou Direct Connect da VPC do cliente até o gateway do cliente. A vantagem desse cenário é usar um ambiente do AD possivelmente já implantado sem precisar provisionar controladores de domínio adicionais na VPC do cliente. A desvantagem é a dependência exclusiva da VPN ou do Direct Connect com o objetivo de autenticar e autorizar usuários para a frota do AppStream 2.0. Se houver algum problema de conectividade de rede, a frota do AppStream 2.0 ou os construtores de imagem seriam 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) à VPC do cliente da AWS

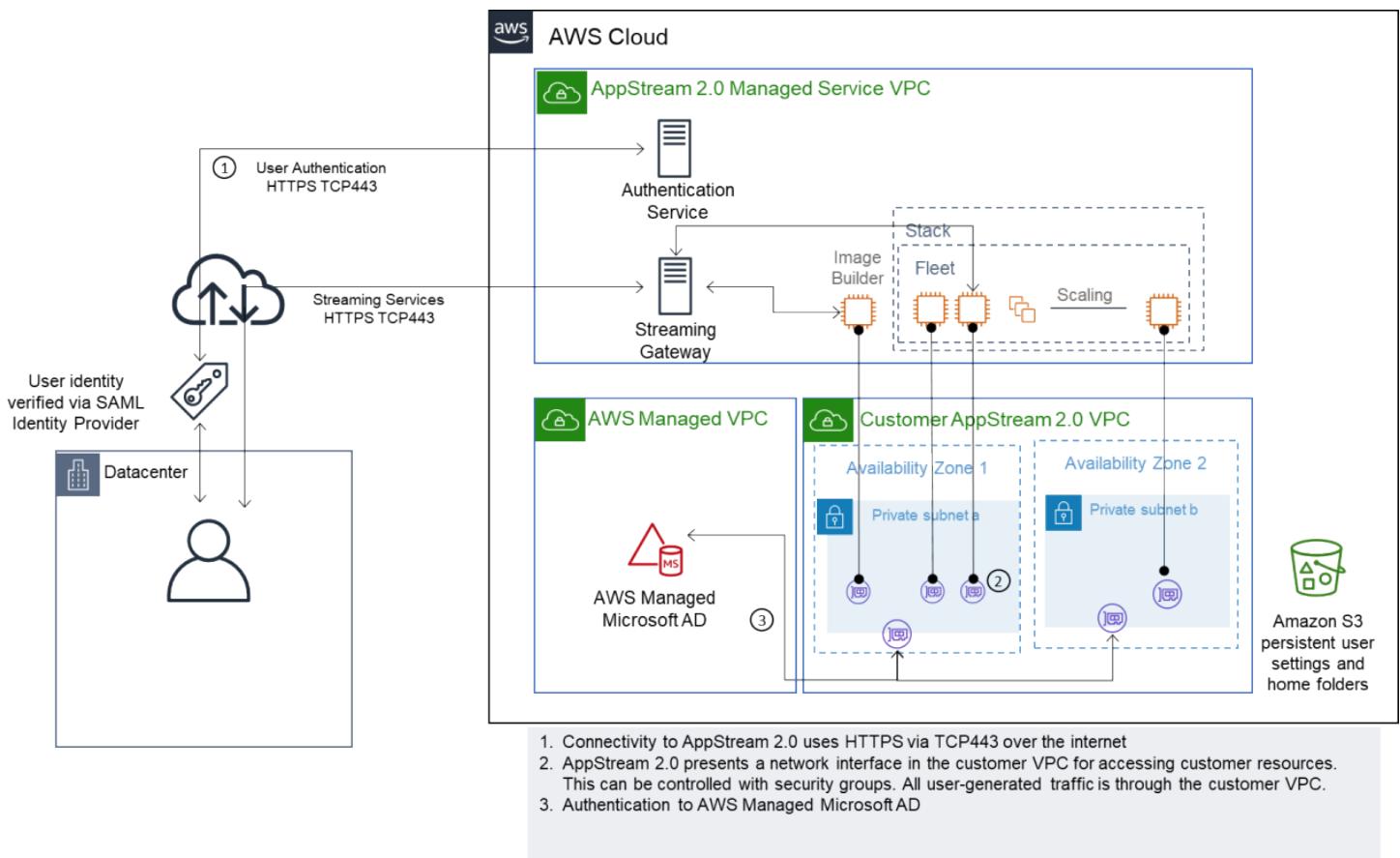
O Active Directory é estendido à VPC do cliente. Um site do Active Directory deve ser criado para os novos controladores de domínio na VPC do cliente. O tráfego de autenticação é roteado para os controladores de domínio na VPC do cliente da AWS em vez de atravessar a conexão VPN ou do Direct Connect.



Cenário 2: extensão dos serviços de domínio ativo na nuvem privada virtual do cliente da AWS

Cenário 3: Microsoft Active Directory gerenciado pela AWS

O Microsoft AD gerenciado pela AWS é implantado no Nuvem AWS e usado como domínio de identidade e recurso para as frotas do AppStream 2.0 e os construtores de imagens.



Cenário 3: Active Directory gerenciado pela AWS

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:

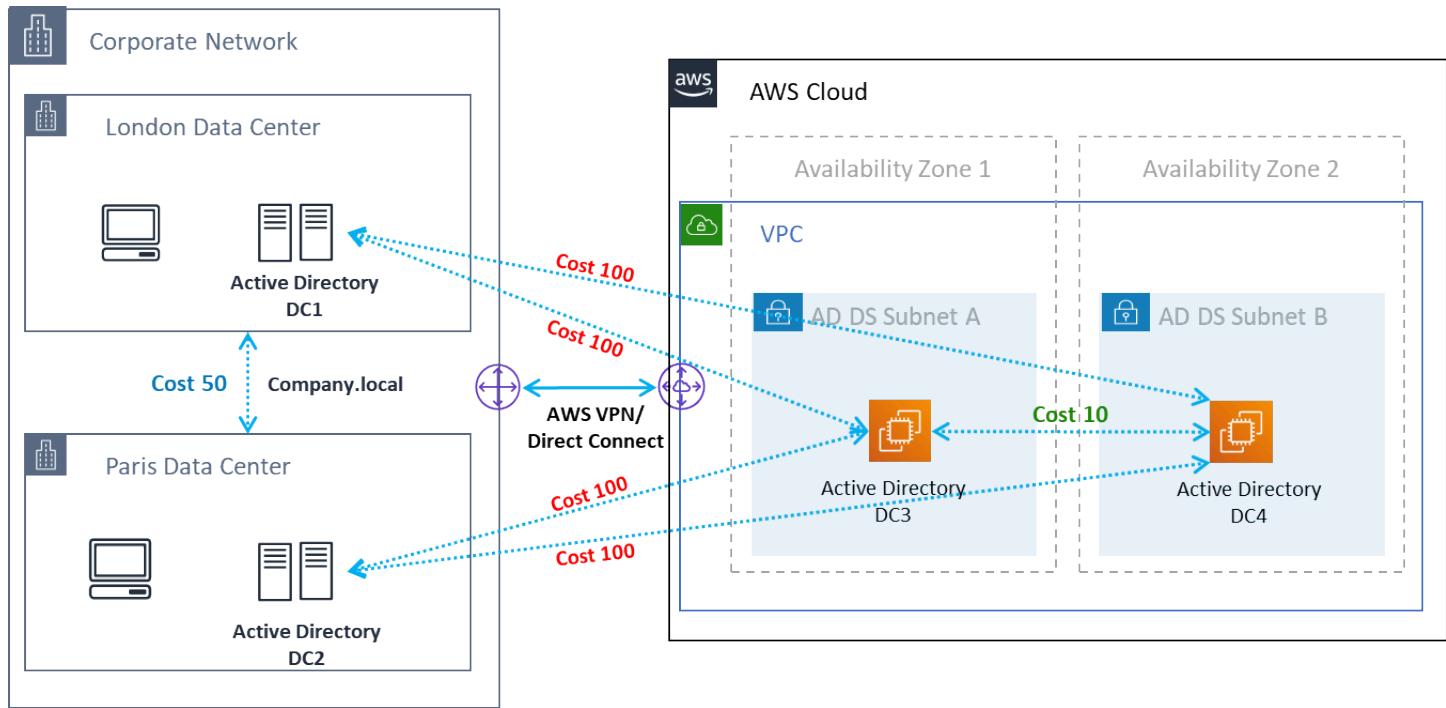
- Minimize o custo da replicação de dados do Active Directory ao sincronizar entre locais e Nuvem AWS.
- Otimize a capacidade dos computadores clientes de localizar os recursos mais próximos, como controladores de domínio. Isso ajuda a reduzir o tráfego de rede em links lentos de rede de longa distância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

Ao introduzir os serviços do AppStream 2.0, os intervalos de endereços usados para as sub-redes das instâncias do AppStream 2.0 devem ser atribuídos ao site correto para o 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.

A definição da topologia correta do site garante a afinidade com o cliente, o que significa que os clientes (nesse caso, instâncias de streaming do AppStream 2.0) 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 de configuração de diretório do AppStream 2.0. Como prática recomendada, cada pilha do AppStream 2.0 deve ter sua própria OU. Isso permite a flexibilidade de ter GPOs específicos por pilha. As OUs devem ser dedicadas aos objetos de computador do AppStream 2.0 para evitar misturar políticas específicas do AppStream 2.0 com desktops locais. Considere usar sub-OUs para cada Região da AWS em que você implanta o AppStream 2.0.

Limpeza de objetos no computador do Active Directory

As instâncias do AppStream 2.0 são efêmeras. Uma frota cria e reutiliza objetos de computador do Active Directory à medida que as frotas aumentam e reduzem a escala horizontalmente.

A 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 do AppStream.

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 AppStream versão 2.0, é importante implementar medidas de segurança em diferentes camadas, como pilha, frota, imagem e rede. AWS

Devido à sua natureza efêmera, o AppStream 2.0 geralmente é preferido 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 do 2.0. AppStream

As duas questões-chave da segurança AppStream 2.0 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 do AppStream 2.0 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. AppStreamO armazenamento de instâncias 2.0 é efêmero e não tem opção de criptografia.

AppStream 2.0 fornece persistência do estado do usuário por meio de pastas iniciais e configurações de aplicativos no Amazon S3. Alguns casos de uso exigem maior controle sobre a persistência do estado do usuário. Para esses casos de uso, AWS recomenda o uso de um compartilhamento de arquivos 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 que as frotas 2.0 Região da AWS . AppStream A prática recomendada é criptografar os dados. O comportamento padrão da pasta inicial do usuário é criptografar arquivos e pastas em repouso usando chaves de criptografia gerenciadas pelo Amazon S3 dos AWS serviços de gerenciamento de 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 Bloco de Mensagens do Servidor (SMB) 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

SMBalvo	E ncryption-at-rest	E ncryption-in-transit	Antivírus (AV)
FSxpara Windows File Server	Passagem automática AWS KMS	Automático por meio SMB de criptografia	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 AWS Storage Gateway no S3 são criptografados no lado do servidor com as chaves de criptografia gerenciadas pelo Amazon S3 (-S3). SSE 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 usandoSSL.	O AV instalado em uma instância remota executa a varredura na unidade mapeada

SMBalvo	Encryption-at-rest	Encryption-in-transit	Antivírus (AV)
EC2servidores de arquivos Windows baseados em Windows	Ativar EBS criptografia	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 AppStream 2.0 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 AppStream 2.0 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 do Endpoint Security 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, o que garantirá que um novo GUID seja gerado para cada instância gerada a partir de uma imagem.

Para garantir que o não GUID seja gerado, instale o agente do Endpoint Security como a última ação antes de executar o AppStream 2.0 Assistant para gerar a imagem.

Otimização do desempenho

Os fornecedores de segurança de terminais fornecem switches e configurações que otimizam o desempenho do AppStream 2.0. 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 VDI otimizadas
- Exclusões exigidas pelos aplicativos para garantir o desempenho

Os fornecedores de segurança de endpoints 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 não persistentes VDI - Microsoft Tech Community](#)

Exclusões de verificação

Se o software de segurança for instalado em instâncias AppStream 2.0, o software de segurança não deverá interferir nos processos a seguir.

Tabela 6 — O software de segurança de processos AppStream 2.0 não deve interferir nos processos a seguir.

Serviço	Processos
AmazonCloudWatchAgent	"C:\Program Files\ Amazon\AmazonCloud WatchAgent\ start-amazon- cloudwatch-agent.exe"
A mazonSSMAgent	"C:\Program Files\ Amazon\SSM\ amazon-ssm-agent .exe"
NICE DCV	"C:\Program FilesNICE\DCV\ Server\ bin\ dcvserver.exe" "C:\Program Arquivos\NICE \DCV\ Servidor\ bin\ dcvagent.exe"

Serviço	Processos
AppStream 2.0	<p>“C:\ProgramFiles\ Amazon\ AppStream 2\StorageConnector\ StorageConnector .exe”</p> <p>Na pasta “C:\Program Files\Amazon\Photon\”</p> <p>“. \ Agente\ PhotonAgent .exe”</p> <p>“. \ Agente\ s5cmd.exe”</p> <p>“. \WebServer\ PhotonAgentWebServer .exe”</p> <p>“. \CustomShell\ PhotonWindowsAppSw itcher .exe”</p> <p>“. \CustomShell\ PhotonWindowsCusto mShell .exe”</p> <p>“. \CustomShell\ PhotonWindowsCusto mShellBackground .exe”</p>

Pastas

Se o software de segurança for instalado em instâncias AppStream 2.0, 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

A Amazon AppStream 2.0 criará 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 AppStream 2.0) para serem excluídas minimizará o número de instâncias expiradas no console.

Exclusões de rede

O alcance da rede de gerenciamento AppStream 2.0 (198.19.0.0/16) e as seguintes portas e endereços não devem ser bloqueados por nenhuma solução de segurança/firewall ou antivírus em instâncias AppStream 2.0.

Tabela 7 — O software de segurança de portas em instâncias de streaming AppStream 2.0 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 até AppStream 2.0
8443	Isso é usado para gerenciar a instância de streaming até AppStream 2.0
53	DNS

Tabela 8 — O software de segurança de endereços de serviços gerenciados AppStream 2.0 não deve interferir com

Porta	Uso
169.254.169.123	NTP

Porta	Uso
169.254.169.249	NVIDIAGRIDServiço de licenças
169.254.169.250	KMS
169.254.169.251	KMS
169.254.169.253	DNS
169.254.169.254	Metadados

Protegendo uma sessão AppStream

Como limitar os controles de aplicativos e sistemas operacionais

AppStream 2.0 dá ao administrador a capacidade de especificar 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 ao aplicativo a partir da AppStream versão 2.0 usando a Microsoft AppLocker está detalhado no [Guia do AppStream administrador](#).

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 para proteger o acesso dos usuários aos aplicativos e recursos.

Firewalls e roteamento

Ao criar uma frota AppStream 2.0, 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

NACLA é uma camada opcional de segurança para você VPC que atua como um firewall sem estado para controlar o tráfego de entrada e saída de uma ou mais sub-redes. Você pode configurar uma rede ACLs com regras semelhantes aos seus grupos de segurança para adicionar uma camada adicional de segurança ao seuVPC. Para obter mais informações sobre as diferenças entre grupos de segurança e redeACLs, consulte [a NACLs página comparar grupos de segurança e.](#)

Ao projetar e aplicar NACL regras e grupos de segurança, considere as melhores práticas do AWS Well-Architected 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 AWS (por meio de um AWS Direct Connect), considere usar os VPC Endpoints para AppStream, o que significa que o tráfego de streaming será roteado por meio da conectividade de sua rede privada, em vez de passar pela Internet pública. Para obter mais informações sobre esse tópico, consulte a seção de VPC endpoint da interface de streaming AppStream 2.0 deste documento.

Prevenção de perda de dados

Vamos analisar dois tipos de prevenção de perda de dados.

Controles de transferência de dados de cliente para instância AppStream 2.0

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

Configuração	Opções	Orientação
Área de transferência	<ul style="list-style-type: none"> • Copiar e colar somente na sessão remota 	Desabilitar essa configuração não desabilita copiar e colar

Configuração	Opções	Orientação
	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Fazer upload e baixar • Somente upload • Somente baixar • Desabilitado 	Evite ativar essa configuração para impedir o vazamento de dados.
Imprimir no dispositivo local	<ul style="list-style-type: none"> • Habilitado • Desabilitado 	Se a impressão for necessária, use impressoras mapeadas em rede que sejam controladas 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 AppStream 2.0

Quando a perda de dados é uma preocupação, é importante cobrir o que um usuário pode acessar quando estiver dentro da instância AppStream 2.0. 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 AppStream 2.0, 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 endpoint dentro da AppStream instância (consulte a seção “Segurança e antivírus de endpoints” para obter mais informações).

Usando AWS serviços

AWS Identity and Access Management

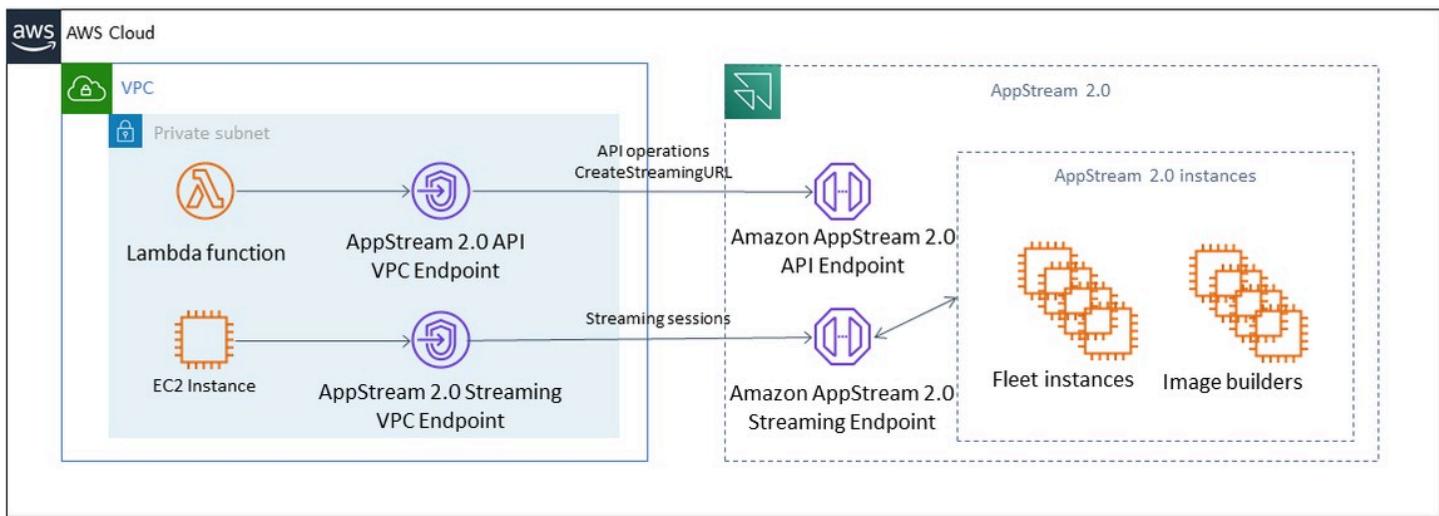
Usar uma IAM função para acessar AWS serviços e ser específico na IAM política anexada a ela é uma prática recomendada que fornece acesso somente aos usuários nas sessões AppStream 2.0 sem gerenciar credenciais adicionais. Siga as [melhores práticas para usar o IAM Roles with AppStream 2.0](#).

Crie [IAMpolíticas 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 administradores não AppStream 2.0](#).

VPCendpoints

Um VPC endpoint permite conexões privadas entre você VPC e os AWS serviços suportados e os serviços de VPC endpoint fornecidos por. AWS PrivateLink AWS PrivateLink é uma tecnologia que permite acessar serviços de forma privada usando endereços IP privados. O tráfego entre o seu VPC e o outro serviço não sai da rede Amazon. Se o acesso público à Internet for necessário apenas para AWS serviços, os VPC endpoints eliminarão completamente a necessidade de NAT gateways e gateways de Internet.

Em ambientes em que as rotinas de automação ou os desenvolvedores exijam fazer API chamadas para AppStream 2.0, [crie um VPC endpoint de interface para operações AppStream 2.0 API](#). Por exemplo, se houver EC2 instâncias em sub-redes privadas sem acesso público à Internet, um VPC endpoint para AppStream 2.0 API pode ser usado para chamar API operações AppStream 2.0, como. [CreateStreamingURL](#) O diagrama a seguir mostra um exemplo de configuração em que os VPC endpoints AppStream 2.0 API e de streaming são consumidos pelas funções EC2 e instâncias do Lambda.



VPC ponto final

O VPC endpoint de streaming permite que você transmita sessões por meio de um VPC endpoint. O endpoint da interface de streaming mantém o tráfego de streaming dentro do seu VPC. O tráfego de streaming inclui pixelsUSB, entrada do usuário, áudio, área de transferência, upload e download de arquivos e tráfego de impressoras. Para usar o VPC endpoint, a configuração do VPC endpoint deve estar habilitada na pilha AppStream 2.0. 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 VPC endpoint exige o seguinte:

- Os grupos de segurança associados ao endpoint da interface devem permitir acesso de entrada à porta 443 (TCP) e às portas 1400–1499 (TCP) do intervalo de endereços IP ao qual seus usuários se conectam.
- A Lista de Controle de Acesso à Rede das sub-redes deve permitir o tráfego de saída de portas de rede efêmeras 1024–65535 (TCP) para o intervalo de endereços IP a partir do qual seus usuários se conectam.
- A conectividade com a Internet é necessária para autenticar os usuários e fornecer os ativos da web que o AppStream 2.0 requer para funcionar.

Para saber mais sobre como restringir o tráfego aos AWS serviços com AppStream 2.0, consulte o guia de administração para [criar e transmitir a partir de VPC endpoints](#).

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

informações, consulte o guia de administração AppStream 2.0 para [desabilitar a configuração de segurança aprimorada do Internet Explorer.](#)

Recuperação de desastres

O 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 aos usuários do AppStream 2.0, primeiro será necessário criar um ambiente do AppStream 2.0 na 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 a frota do AppStream 2.0 estiver associada a um domínio, você deverá ter controladores de domínio adicionais na região secundária com sites e serviços configurados. Do ponto de vista do AppStream 2.0, esse ambiente deve consistir nas mesmas configurações de frota e pilha da 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 do AppStream 2.0 tiverem uma dependência de back-end vinculada à região principal, ela também deverá ter redundância regional, garantindo 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 do aplicativo do AppStream 2.0 no 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 entram no AppStream 2.0 a partir de um provedor de identidades (IdP), após a autenticação, eles são retransmitidos para um URL específico que se alinha à região e à pilha que devem acessar. Para obter mais informações sobre o URL do estado de retransmissão, consulte o Guia de administração do [Amazon AppStream 2.0](#). O administrador pode configurar uma pilha entre regiões criada na mesma imagem do AppStream 2.0 da região principal 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.

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

Método 2: como configurar dois aplicativos do AppStream 2.0 no IdP

Esse método exige que o administrador crie dois aplicativos separados para o AppStream 2.0 dentro do IdP. Em seguida, eles podem apresentar os dois aplicativos e permitir que o usuário escolha para onde ir, ou bloquear/ocultar um aplicativo até o momento 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 no AppStream 2.0, [como persistência de aplicativos](#) e [sincronização de pastas base](#), você precisará replicar esses dados para sua região de failover. Esses recursos armazenam os dados persistentes em um bucket do Amazon S3 na

região específica do AppStream 2.0. Para que os dados persistam entre regiões, você precisará replicar todas as alterações no bucket de origem para o bucket do AppStream 2.0 da região 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 pelo AppStream 2.0, [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 AppStream 2.0, 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 AppStream 2.0 para CloudWatch pode ser encontrada no guia de administração AppStream 2.0 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 de frota AppStream 2.0 se tornam disponíveis para hospedar sessões de usuários. Crie um CloudWatch alarme para cada frota AppStream 2.0 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 escalabilidade 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 a frota AppStream 2.0 seja adequada AvailableCapacity 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 escalabilidade (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 QuickSight para criar relatórios e visualizações personalizados dos seus dados de uso AppStream 2.0](#).

Logs persistentes de aplicativos e eventos do Windows

Quando uma sessão de instância AppStream 2.0 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 configurar [AWS CloudTrail](#) para o Conta da AWS com o Amazon AppStream 2.0. Para auditar especificamente as chamadas da API AppStream 2.0, use a fonte de eventos de filtro com um valor de `appstream.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 AppStream 2.0 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 custo

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 do AppStream 2.0 incorrem em taxas de pagamento conforme o uso:

- Instâncias de frota sempre ativas
- Instâncias de frota sob demanda
- Taxa de instância interrompida sob demanda
- Instâncias do criador de imagens
- Taxas de usuário

Para obter informações atuais sobre preços, consulte o site da AWS para ver os preços do [Amazon AppStream 2.0](#).

Como projetar implantações econômicas do AppStream 2.0

A primeira etapa no planejamento e design da implantação do AppStream 2.0 é [usar uma ferramenta de especificação simples](#) para estimar a linha de base das taxas da AWS 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 frota sob demanda em vez de uma frota sempre ativa.

Os clientes gostam do modelo de preços do AppStream 2.0 de pagar somente pelas instâncias provisionadas para atender às necessidades de streaming dos 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 do Amazon AppStream 2.0 fornece somente uma estimativa das taxas da AWS relacionadas ao uso do AppStream 2.0 e não inclui impostos que possam incidir. As taxas reais dependem de vários fatores, incluindo a utilização real dos serviços da AWS.

A ferramenta de preços do AppStream 2.0 é fornecida como uma planilha do Microsoft Excel ou do OpenOffice Calc, permitindo que você insira informações básicas sobre a frota e, em

seguida, fornece uma estimativa de custo do ambiente AppStream 2.0 para frotas sob demanda e sempre ativas com base no 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, criar e manter políticas, além de imagens de escalabilidade 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 com o usuário final: a próxima etapa é implantar a frota do AppStream 2.0 para um grupo de usuários piloto com o objetivo de fazer testes e 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 do AppStream 2.0, os desenvolvedores devem escolher o tipo de frota Sempre ativa ou Sob demanda. Ao escolher o tipo de instância do ponto de vista dos preços, é importante entender como o AppStream 2.0 gerencia as instâncias da frota. Para frotas sempre ativas, as instâncias dela permanecem em funcionamento. Portanto, quando os usuários tentam transmitir sessões, as instâncias de frota estão sempre prontas para iniciar as sessões de streaming.

Para frotas sob demanda, depois que as instâncias dela 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 da frota sob demanda 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 do AppStream 2.0

Tipo de frota	Vantagens	Considerações
Sempre ativa	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.
Sob demanda	Redução de custos à medida que as instâncias permanecem paradas	Mais tempo de espera para sessões de streaming
Elástica	O faturamento por segundo pode ser útil nos casos de uso que têm padrões de uso esporádicos para aplicativos que podem ser instalados em um disco rígido virtual	À medida que o tamanho do disco rígido virtual do aplicativo aumenta, o tempo necessário para montá-lo em uma instância de streaming pode maior

O AppStream 2.0 monitora a utilização da sua frota e realiza ajustes automáticos na capacidade dela 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 escalonamento não têm altos níveis de capacidade ociosa.

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 o CloudWatch AppStream 2.0 Fleet Metrics ou as ferramentas de monitoramento de terceiros para aprender sobre a atividade do usuário e configurar políticas de ajuste de escala para expandir ou reduzir as frotas do AppStream 2.0 usando como base o 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 do AppStream 2.0 são criadas usando como base o 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 resulta no provisionamento excessivo das instâncias do AppStream 2.0, resultando em mais custos. 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 ajuste de escala, consulte [Como ajustar a escala das frotas do Amazon AppStream 2.0](#).

Taxas de usuário

As taxas de usuário são cobradas por usuário, todo mês, em cada Região da AWS, nas quais os usuários transmitem aplicativos a partir de instâncias de frota do AppStream 2.0. Em vez de gerar IDs de usuário diferentes, crie IDs de usuário consistentes para usuários do AppStream 2.0. 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 tiver o Microsoft License Mobility, você poderá usar suas próprias licenças de acesso para clientes (CALs) do Microsoft RDS e usá-las com o Amazon AppStream 2.0. Caso esteja coberto por

sua própria licença, não incorrerá em taxas mensais de usuário. Para obter mais informações sobre o uso de suas licenças CAL do Microsoft RDS existentes com o Amazon AppStream 2.0, consulte a [orientação de mobilidade de licenças da AWS](#) ou consulte seu representante de licenciamento da Microsoft.

Uso do Image Builder

As instâncias do Image Builder do AppStream 2.0 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 em uso. As regras de eventos do CloudWatch podem ser usadas para agendar um trabalho diário, como invocar uma função do Lambda para interromper as instâncias do construtor de imagens.

Você pode manter sua imagem do AppStream 2.0 atualizada usando atualizações de imagem gerenciadas do AppStream 2.0. Esse método de atualização oferece as atualizações do sistema operacional Windows e as atualizações de drivers mais recentes, além do software de agente do AppStream 2.0 mais recente. Ao usar esse método para atualizar imagens, um Image Builder é iniciado automaticamente e interrompido como parte do processo de serviço gerenciado.

Conclusão

Com o AppStream 2.0, você pode adicionar facilmente aplicações de área de trabalho existentes à AWS e permitir que os usuários façam streaming instantâneo delas. Os usuários do Windows podem usar o cliente do AppStream 2.0 ou um navegador da web compatível com HTML5 para fazer streaming de aplicações. 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. As aplicações são executadas nos recursos de computação da AWS e os dados nunca são armazenados nos dispositivos dos usuários, o que significa que a experiência é sempre segura e de alta performance.

Ao contrário das tradicionais soluções locais para streaming de aplicativos de desktop, o AppStream oferece definição de preços conforme o uso, sem investimento inicial e a necessidade de manter infraestrutura. Você pode alterar a escala de forma instantânea e global, garantindo que os usuários sempre tenham a melhor experiência possível.

O Amazon AppStream 2.0 foi projetado para ser integrado aos sistemas e processos de TI existentes, e este whitepaper descreveu as práticas recomendadas para fazer isso. O resultado de seguir as diretrizes deste whitepaper é uma implantação econômica de desktop na nuvem que pode ser dimensionada com segurança com sua empresa na infraestrutura global da 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 da Amazon AppStream 2.0](#)
- [Referência de AppStream API da Amazon](#)
- [Use o Amazon FSx for Windows File Server e o FSLogix para otimizar a persistência das configurações do aplicativo no Amazon 2.0 AppStream](#)
- [Monitorando o Amazon AppStream 2.0 com Amazon ElasticSearch e Amazon Firehose](#)
- [Analise seus relatórios de uso do Amazon AppStream 2.0 usando o Amazon Athena e o Amazon QuickSight](#)
- [Escale suas frotas da Amazon AppStream 2.0](#)
- [Usando AppLocker a Microsoft para gerenciar a experiência de aplicativos na Amazon AppStream 2.0](#)
- [Usando domínio personalizado com o Amazon AppStream 2.0](#)
- [Como faço para usar minhas próprias CALs do Microsoft RDS com AppStream 2.0?](#)
- [Ferramenta de preços da Amazon AppStream 2.0](#)
- [Crie um teste de software on-line com AppStream 2.0](#)
- [Crie um portal SaaS com o Amazon 2.0 AppStream](#)

Revisões do documento

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

Alteração	Descrição	Data
<u>Documento atualizado</u>	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
<u>Documento atualizado</u>	Versão HTML publicada.	19 de janeiro de 2022
<u>Publicação inicial</u>	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.