AWS Livro branco

Melhores práticas para implantação WorkSpaces

Melhores práticas para implantação WorkSpaces: AWS Livro branco

Table of Contents

Melhores práticas para implantar a Amazon WorkSpaces

Data de publicação: 1 de junho de 2022 (Revisões do documento)

Resumo

Este whitepaper descreve um conjunto de melhores práticas para a implantação do. WorkSpaces O whitepaper aborda considerações de rede, serviços de diretório e autenticação de usuários, segurança, monitoramento e registro.

Esse whitepaper também permite acesso rápido a informações relevantes e é destinado a engenheiros de rede, engenheiros de diretórios ou engenheiros de segurança.

Introdução

A Amazon WorkSpaces é um serviço gerenciado de computação de desktop na nuvem. A Amazon WorkSpaces elimina a carga de adquirir ou implantar hardware ou instalar software complexo e oferece uma experiência de desktop com apenas alguns cliques AWS Management Console, usando a interface de linha de comando (CLIAWS) do Amazon Web Services () ou usando a interface de programação de aplicativos (API). Com a Amazon WorkSpaces, você pode lançar um desktop Microsoft Windows ou Amazon Linux em minutos, o que permite que você se conecte e acesse seu software de desktop de forma segura, confiável e rápida a partir do local ou de uma rede externa. É possível:

- Aproveite seu Microsoft Active Directory (AD) existente no local usando o AWS Directory Service: Active Directory Connector (AD Connector).
- Estenda seu diretório para a AWS nuvem.
- Crie um diretório gerenciado com o AWS Directory Service Microsoft AD ou Simple AD, para gerenciar seus usuários WorkSpaces e.
- Aproveite seu servidor RADIUS local ou hospedado na nuvem com o AD Connector para fornecer autenticação multifator (MFA) ao seu. WorkSpaces

Você pode automatizar o provisionamento da Amazon WorkSpaces usando a CLI ou a API, o que permite integrar a Amazon WorkSpaces aos seus fluxos de trabalho de provisionamento existentes.

Por segurança, além da criptografia de rede integrada que o WorkSpaces serviço da Amazon fornece, você também pode habilitar a criptografia em repouso para você WorkSpaces. Consulte a WorkSpaces seção Criptografada deste documento.

Você pode implantar aplicativos no seu WorkSpaces usando suas ferramentas locais existentes, como o Microsoft System Center Configuration Manager (SCCM), o Puppet Enterprise ou o Ansible.

As seções a seguir fornecem detalhes sobre a Amazon WorkSpaces, explicam como o serviço funciona, descrevem o que você precisa para iniciar o serviço e informam quais opções e recursos estão disponíveis para você usar.

WorkSpaces requisitos

O WorkSpaces serviço da Amazon requer três componentes para ser implantado com sucesso:

- WorkSpaces aplicativo cliente — Um dispositivo cliente WorkSpaces compatível com a Amazon. Consulte Introdução ao seu WorkSpace.

  Você também pode usar o Personal Computer over Internet Protocol (PCoIP) Zero Clients para se conectar. WorkSpaces Para obter uma lista dos dispositivos disponíveis, consulte PCoIP Zero Clients for Amazon. WorkSpaces
- Um serviço de diretório para autenticar usuários e fornecer acesso a eles WorkSpace — a Amazon WorkSpaces atualmente trabalha com o AWS Directory Service e o Microsoft AD. Você pode usar seu servidor AD local com o AWS Directory Service para oferecer suporte às suas credenciais de usuário corporativo existentes na Amazon. WorkSpaces
- Amazon Virtual Private Cloud (Amazon VPC) para executar sua Amazon WorkSpaces — Você precisará de no mínimo duas sub-redes para uma implantação da Amazon porque cada construção do AWS Directory Service requer duas sub-redes em uma WorkSpaces implantação Multi-AZ.

Considerações sobre a rede

Cada um WorkSpace está associado à construção específica do Amazon VPC e AWS do Directory Service que você usou para criá-lo. Todas as construções do AWS Directory Service (Simple AD, AD Connector e Microsoft AD) exigem duas sub-redes para operar, cada uma em diferentes zonas de disponibilidade (AZs). As sub-redes são permanentemente afiliadas a uma construção do Directory Service e não podem ser modificadas após sua criação. Por isso, é fundamental que você determine os tamanhos corretos de sub-rede antes de criar a construção dos Serviços de Diretório. Considere cuidadosamente o seguinte antes de criar as sub-redes:

- Quantos você WorkSpaces precisará ao longo do tempo?
- Qual é o crescimento esperado?
- Que tipos de usuários você precisará acomodar?
- Quantos domínios do AD você conectará?
- Onde residem suas contas corporativas?

A Amazon recomenda definir grupos de usuários, ou personas, com base no tipo de acesso e na autenticação de usuário que você precisa como parte do seu processo de planejamento. As respostas a essas perguntas são úteis quando você precisa limitar o acesso a determinados aplicativos ou recursos. Personas de usuário definidas podem ajudar você a segmentar e restringir o acesso usando o AWS Directory Service, listas de controle de acesso à rede, tabelas de roteamento e grupos de segurança de VPC. Cada construção AWS do Directory Service usa duas sub-redes e aplica as mesmas configurações a todas as inicializações a partir WorkSpaces dessa construção. Por exemplo, você pode usar um grupo de segurança que se aplica a todos WorkSpaces conectados a um AD Connector para especificar se o MFA é necessário ou se um usuário final pode ter acesso de administrador local em seu. WorkSpace

> **Note**
>
> Cada AD Connector se conecta ao seu Microsoft AD corporativo existente. Para aproveitar esse recurso e especificar uma Unidade Organizacional (OU), você deve criar seu Directory Service para levar em consideração suas personalidades de usuário.

Design em VPC

Esta seção descreve as melhores práticas para dimensionar sua VPC e sub-redes, fluxo de tráfego e implicações para o design de serviços de diretório.

Aqui estão algumas coisas a serem consideradas ao projetar a VPC, as sub-redes, os grupos de segurança, as políticas de roteamento e as listas de controle de acesso à rede (ACLs) para sua WorkSpaces Amazon, para que você possa criar WorkSpaces seu ambiente para escalabilidade, segurança e facilidade de gerenciamento:

- VPC — recomendamos usar uma VPC separada especificamente para sua implantação. WorkSpaces Com uma VPC separada, você pode especificar as barreiras de governança e segurança necessárias para você criando uma separação de tráfego WorkSpaces .
- Serviços de diretório — Cada AWS Directory Service construção requer um par de sub-redes que forneça um serviço de diretório altamente disponível dividido entre AZs.
- Tamanho da sub-rede — WorkSpaces as implantações estão vinculadas a uma construção de diretório e residem na mesma VPC escolhida AWS Directory Service, mas podem estar em sub-redes VPC diferentes. Algumas considerações:
  - Os tamanhos das sub-redes são permanentes e não podem ser alterados. Você deve deixar amplo espaço para crescimento futuro.
  - Você pode especificar um grupo de segurança padrão para sua escolha AWS Directory Service. O grupo de segurança se aplica a todos os WorkSpaces que estão associados à AWS Directory Service construção específica.
  - Você pode ter várias instâncias de AWS Directory Service uso da mesma sub-rede.

Considere os planos futuros ao projetar sua VPC. Por exemplo, talvez você queira adicionar componentes de gerenciamento, como um servidor antivírus, um servidor de gerenciamento de patches ou um servidor AD ou RADIUS MFA. Vale a pena planejar outros endereços IP disponíveis em seu design de VPC para acomodar esses requisitos.

Para obter orientações e considerações detalhadas sobre design de VPC e dimensionamento de sub-rede, consulte a apresentação do re:Invent Como a Amazon.com está migrando para a Amazon. WorkSpaces

Interfaces de rede

Cada uma WorkSpaces tem duas interfaces de rede elástica (ENIs), uma interface de rede de gerenciamento (`eth0`) e uma interface de rede primária (`eth1`). AWS usa a interface da rede de gerenciamento para gerenciar o WorkSpace — é a interface na qual a conexão do seu cliente termina. AWS usa um intervalo de endereços IP privado para essa interface. Para que o roteamento de rede funcione corretamente, você não pode usar esse espaço de endereço privado em nenhuma rede que possa se comunicar com sua WorkSpaces VPC.

Para obter uma lista dos intervalos de IP privados que são usados por região, consulte WorkSpaces Detalhes da Amazon.

> **Note**
>
> A Amazon WorkSpaces e suas interfaces de rede de gerenciamento associadas não residem na sua VPC, e você não pode visualizar a interface da rede de gerenciamento ou o ID da instância do Amazon Elastic Compute Cloud (Amazon EC2) na AWS Management Console sua (consulte, e). Figure 5 Figure 6 Figure 7 No entanto, você pode visualizar e modificar as configurações do grupo de segurança da sua interface de rede primária (`eth1`) no console. A interface de rede primária de cada um WorkSpace conta para suas cotas de recursos do ENI Amazon EC2. Para grandes implantações da Amazon WorkSpaces, você precisa abrir um ticket de suporte por meio do AWS Management Console para aumentar suas cotas de ENI.

Fluxo de tráfego

Você pode dividir o WorkSpaces tráfego da Amazon em dois componentes principais:

- O tráfego entre o dispositivo cliente e o WorkSpaces serviço da Amazon.
- O tráfego entre o WorkSpaces serviço da Amazon e o tráfego da rede do cliente.

A próxima seção discute esses dois componentes.

Dispositivo cliente para WorkSpace

Independentemente de sua localização (local ou remota), o dispositivo que executa o WorkSpaces cliente da Amazon usa as mesmas duas portas para conectividade com o WorkSpaces serviço da Amazon. O cliente usa a porta 443 (porta HTTPS) para todas as informações relacionadas à autenticação e à sessão, e a porta 4172 (porta PCoIP), com Protocolo de Controle de Transmissão (TCP) e Protocolo de Datagrama de Usuário (UDP), para streaming de pixels para um determinado e verificações de integridade da rede. WorkSpace O tráfego nas duas portas é criptografado. O tráfego da porta 443 é usado para informações de autenticação e sessão e usa TLS para criptografar o tráfego. O tráfego de streaming de pixels usa criptografia AES de 256 bits para comunicação entre o cliente e o do WorkSpace, por meio `eth0` do gateway de streaming. Mais informações podem ser encontradas na Segurança seção deste documento.

Publicamos intervalos de IP por região de nossos gateways de streaming PCoIP e endpoints de verificação de integridade da rede. Você pode limitar o tráfego de saída na porta 4172 da sua rede corporativa para o gateway de AWS streaming e os endpoints de verificação de integridade da rede, permitindo somente o tráfego de saída na porta 4172 para as regiões específicas AWS nas quais você está usando a Amazon. WorkSpaces Para os intervalos de IP e os endpoints de verificação de integridade da rede, consulte Intervalos de IP do Amazon WorkSpaces PCoIP Gateway.

O WorkSpaces cliente Amazon tem uma verificação de status de rede integrada. Esse utilitário mostra aos usuários se sua rede pode suportar uma conexão por meio de um indicador de status no canto inferior direito do aplicativo. A figura a seguir mostra uma visão mais detalhada do status da rede que pode ser acessada escolhendo Rede no lado superior direito do cliente.

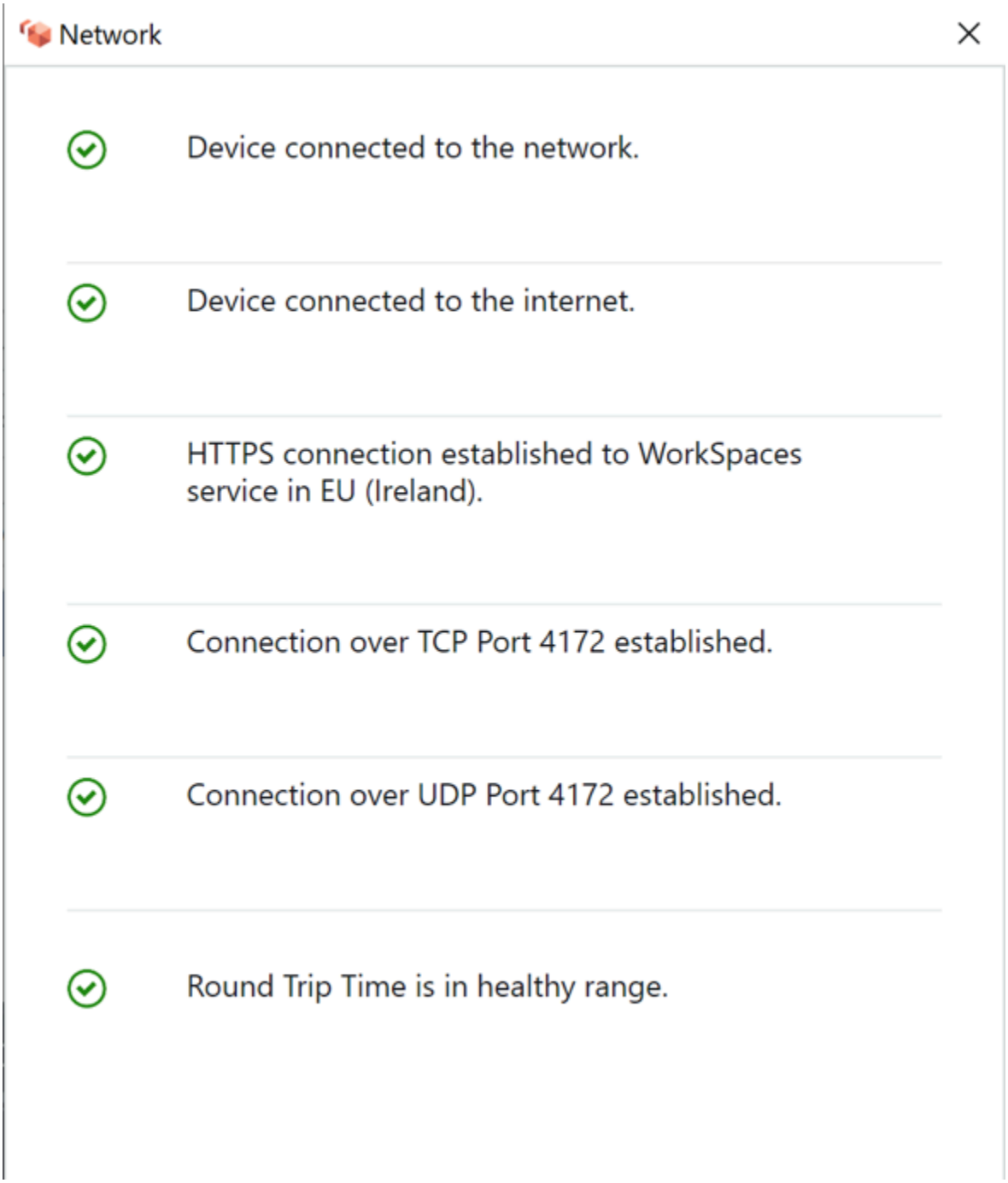

Figura 1: WorkSpaces Cliente: verificação de rede

Um usuário inicia uma conexão de seu cliente com o WorkSpaces serviço da Amazon fornecendo suas informações de login para o diretório usado pela construção do Directory Service, normalmente seu diretório corporativo. As informações de login são enviadas via HTTPS para os gateways de autenticação do WorkSpaces serviço Amazon na região em que o WorkSpace está localizado.

O gateway de autenticação do WorkSpaces serviço Amazon então encaminha o tráfego para a construção específica do AWS Directory Service associada à sua WorkSpace.

Por exemplo, ao usar o AD Connector, o AD Connector encaminha a solicitação de autenticação diretamente para seu serviço AD, que pode estar no local ou em uma AWS VPC. Para obter mais informações, consulte a seção Cenários de implantação do AD DS deste documento. O AD Connector não armazena nenhuma informação de autenticação e atua como um proxy sem estado. Como resultado, é fundamental que o AD Connector tenha conectividade com um servidor AD. O AD Connector determina a qual servidor AD se conectar usando os servidores DNS que você define ao criar o AD Connector.

Se você estiver usando um AD Connector e tiver o MFA ativado no diretório, o token de MFA será verificado antes da autenticação do serviço de diretório. Se a validação da MFA falhar, as informações de login do usuário não serão encaminhadas para o Directory Service AWS .

Depois que um usuário é autenticado, o tráfego de streaming começa usando a porta 4172 (porta PCoIP) através do AWS gateway de streaming até o. WorkSpace As informações relacionadas à sessão ainda são trocadas via HTTPS durante toda a sessão. O tráfego de streaming usa a primeira ENI no WorkSpace (`eth0`no WorkSpace) que não está conectada à sua VPC. A conexão de rede do gateway de streaming com o ENI é gerenciada por AWS. No caso de uma falha na conexão dos gateways de streaming com a ENI WorkSpaces de streaming, um CloudWatch evento é gerado. Para obter mais informações, consulte a CloudWatch seção Monitoramento ou registro usando a Amazon deste documento.

A quantidade de dados enviados entre o WorkSpaces serviço da Amazon e o cliente depende do nível de atividade do pixel. Para garantir uma experiência ideal para os usuários, recomendamos que o tempo de ida e volta (RTT) entre o WorkSpaces cliente e a AWS região em que você WorkSpaces está localizado seja inferior a 100 milissegundos (ms). Normalmente, isso significa que seu WorkSpaces cliente está localizado a menos de duas mil milhas da região em que WorkSpace está sendo hospedado. A página do Connection Health Check pode ajudar você a determinar a melhor AWS região para se conectar ao WorkSpaces serviço da Amazon.

Amazon WorkSpaces Service para VPC

Depois que uma conexão for autenticada de um cliente para um WorkSpace e o tráfego de streaming for iniciado, seu WorkSpaces cliente exibirá um desktop Windows ou Linux (sua Amazon WorkSpace) conectado à sua nuvem privada virtual (VPC), e sua rede deverá mostrar que você estabeleceu essa conexão. A interface WorkSpace de rede elástica (ENI) primária da empresa,

identificada como`eth1`, terá um endereço IP atribuído a ela pelo serviço Dynamic Host Configuration Protocol (DHCP) fornecido pela sua VPC, normalmente das mesmas sub-redes do seu Directory Service. AWS O endereço IP permanece com o WorkSpace durante toda a vida útil do WorkSpace. A ENI na sua VPC tem acesso a qualquer recurso na VPC e a qualquer rede que você tenha conectado à sua VPC (por meio de um emparelhamento de VPC, uma conexão ou uma conexão VPN). AWS Direct Connect

O acesso do ENI aos seus recursos de rede é determinado pela tabela de rotas da sub-rede e pelo grupo de segurança padrão que seu AWS Directory Service configura para cada um WorkSpace, bem como por quaisquer grupos de segurança adicionais que você atribuir ao ENI. Você pode adicionar grupos de segurança à ENI voltada para sua VPC a qualquer momento usando o AWS Management Console ou. AWS CLI (Para obter mais informações sobre grupos de segurança, consulte Grupos de segurança para você WorkSpaces.) Além dos grupos de segurança, você pode usar seu firewall baseado em host preferido em um determinado local WorkSpace para limitar o acesso à rede aos recursos dentro da VPC.

É recomendável criar suas opções de DHCP definidas com os IPs do servidor DNS e nomes de domínio totalmente qualificados que sejam autoritativos para seu Active Directory específicos para seu ambiente e, em seguida, atribuir essas opções personalizadas de DHCP definidas à Amazon VPC usada pela Amazon. WorkSpaces Por padrão, a Amazon Virtual Private Cloud (Amazon VPC) usa o AWS DNS em vez do DNS do seu serviço de diretório. O uso de um conjunto de opções de DHCP garantirá a resolução adequada de nomes DNS e a configuração consistente de seus servidores de nomes DNS internos não apenas para você WorkSpaces, mas para qualquer carga de trabalho ou instância de suporte que você possa ter planejado para sua implantação.

Quando as opções de DHCP são aplicadas, há duas diferenças importantes na forma como elas serão aplicadas WorkSpaces em comparação com a forma como são aplicadas às instâncias EC2 tradicionais:

- A primeira diferença é como os sufixos DNS da opção DHCP serão aplicados. Cada um WorkSpace tem configurações de DNS definidas para seu adaptador de rede com as opções Anexar sufixos DNS primário e específico da conexão e Acrescentar sufixos principais do sufixo DNS primário ativadas. A configuração será atualizada com o sufixo DNS configurado no AWS Directory Service que você registrou e associado ao WorkSpace por padrão. Além disso, se o sufixo DNS configurado no Conjunto de Opções DHCP usado for diferente, ele será adicionado e aplicado a qualquer associado. WorkSpaces

- A segunda diferença é que os IPs DNS da opção DHCP configurados não serão aplicados WorkSpace ao devido ao WorkSpaces serviço da Amazon priorizar os endereços IP dos controladores de domínio do diretório configurado.

Como alternativa, você pode configurar uma zona hospedada privada do Route 53 para suportar um ambiente de DNS híbrido ou dividido e obter a resolução de DNS adequada para seu ambiente Amazon WorkSpaces . Para obter mais informações, consulte Opções de DNS de nuvem híbrida para VPC AWS e DNS híbrido com Active Directory.

> **Note**
>
> Cada um WorkSpace deve atualizar a tabela IP ao aplicar uma opção DHCP nova ou diferente definida à VPC. Para atualizar, você pode executar ipconfig /renew ou reinicializar qualquer (WorkSpaces) na VPC configurada com seu conjunto de opções DHCP atualizado. Se você estiver usando o AD Connector e atualizar os endereços IP dos endereços IP/ controladores de domínio conectados, deverá então atualizar a chave de registro do Skylight `DomainJoinDNS` no seu. WorkSpaces É recomendável fazer isso por meio de um GPO. O caminho para essa chave de registro é`HKLM:\SOFTWARE\Amazon\Skylight`. O valor disso não `REG_SZ` será atualizado se as configurações de DNS do AD Connector forem modificadas, e os conjuntos de opções DHCP da VPC também não atualizarão essa chave.

A figura na seção Cenários de implantação do AD DS deste whitepaper mostra o fluxo de tráfego descrito.

Conforme explicado anteriormente, o WorkSpaces serviço da Amazon prioriza os endereços IP do controlador de domínio do diretório configurado para resolução de DNS e ignora os servidores DNS configurados em seu conjunto de opções de DHCP. Se você precisar ter um controle mais granular sobre as configurações do seu servidor DNS na Amazon WorkSpaces, você pode usar as instruções para atualizar servidores DNS para a Amazon WorkSpaces no guia Atualizar servidores DNS para a Amazon do Guia WorkSpaces de Administração da Amazon. WorkSpaces

Se você WorkSpaces precisar resolver outros serviços e estiver usando as opções de DHCP padrão definidas com sua VPC AWS, seu serviço DNS de controlador de domínio nessa VPC deve, portanto, ser configurado para usar o encaminhamento de DNS, apontando para o servidor Amazon DNS com o endereço IP na base do seu CIDR de VPC mais dois; ou seja, se seu CIDR de VPC for 10.0.0.0/24, você configure o encaminhamento de DNS para usar o resolvedor de DNS padrão do Route 53 em 10.0.0.2.

Caso você WorkSpaces precise de resolução de DNS de recursos em sua rede local, você pode usar um endpoint de saída do resolvedor do Route 53, criar uma regra de encaminhamento do Route 53 e associar essa regra às VPCs que exigem essa resolução de DNS. Se você configurou o encaminhamento no serviço DNS do seu controlador de domínio para o resolvedor de DNS padrão do Route 53 da sua VPC, conforme explicado no parágrafo anterior, o processo de resolução de DNS pode ser encontrado em Resolvendo consultas de DNS entre VPCs e no guia de rede do Amazon Route 53 Developer Guide.

Se você estiver usando o conjunto de opções DHCP padrão e precisar que outros hosts em suas VPCs que não façam parte do seu domínio do Active Directory possam resolver nomes de host em seu namespace do Active Directory, você pode usar esse Endpoint de saída do Resolvedor do Route 53 e adicionar outra regra de encaminhamento do Route 53 que encaminha consultas de DNS do seu domínio do Active Directory para seus servidores DNS do Active Directory. Essa regra de encaminhamento do Route 53 deverá estar associada ao Endpoint de saída do Resolvedor do Route 53 que é capaz de acessar seu serviço DNS do Active Directory e a todas as VPCs que você deseja habilitar para resolver registros DNS em seu domínio do Active Directory. WorkSpaces

Da mesma forma, um endpoint de entrada do Route 53 Resolver pode ser usado para permitir a resolução DNS dos registros DNS do seu domínio do WorkSpaces Active Directory a partir da sua rede local.

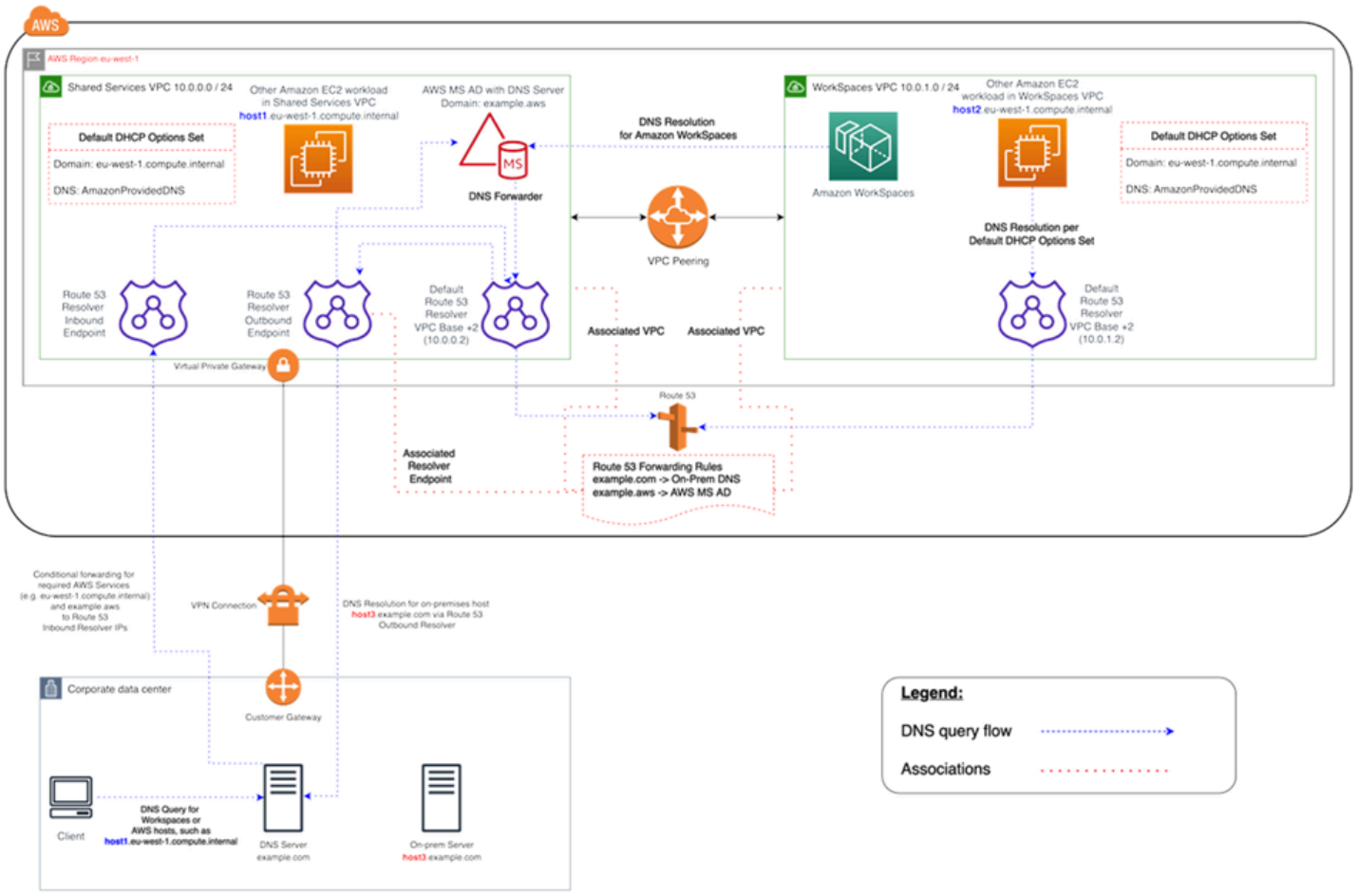

Figura 2: Exemplo de resolução de WorkSpaces DNS com endpoints do Route 53

- Sua Amazon WorkSpaces usará o serviço AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) DNS para resolução de DNS. O serviço AWS Managed Microsoft AD DNS resolve o `example.aws` domínio e encaminha todas as outras consultas de DNS para o resolvedor de DNS padrão do Route 53 no endereço IP base CIDR da VPC +2 para habilitar a resolução de DNS

  A VPC do Shared Services contém um endpoint do Route 53 Outbound Resolver, que está associado a duas regras de encaminhamento do Route 53. Uma dessas regras encaminha as consultas de DNS do `example.com` domínio para os servidores DNS locais. A segunda regra encaminha as consultas de DNS do seu AWS Managed Microsoft AD domínio `example.aws` para o serviço DNS do Active Directory na VPC do Shared Services.

  Com essa arquitetura, sua Amazon WorkSpaces poderá resolver consultas de DNS para o seguinte:

  - Seu AWS Managed Microsoft AD domínio`example.aws`.
  - Instâncias do EC2 no domínio configuradas com seu conjunto de opções DHCP padrão (por exemplo,`host1.eu-west-1.compute.internal`), bem como outros AWS serviços ou endpoints.
  - Hosts e serviços em seu domínio local, como`host3.example.com`.
- • As outras cargas de trabalho do EC2 na VPC () e na VPC (`host1.eu-west-1.compute.internal`) do Shared Services podem executar as mesmas resoluções de DNS que a sua WorkSpaces, desde que as regras de encaminhamento do Route 53 estejam associadas às duas WorkSpaces VPCs. `host2.eu-west-1.compute.internal` Nesse caso, a resolução de DNS para o `example.aws` domínio passará pelo resolvedor de DNS padrão do Route 53 no endereço IP base VPC CIDR +2, que, de acordo com as regras de encaminhamento do Route 53 configuradas e associadas, os encaminhará por meio do Route 53 Resolver Outbound Endpoint para o serviço DNS do Active Directory. WorkSpaces
- • Por fim, um cliente local também pode fazer a mesma resolução de DNS, já que o servidor DNS local é configurado com encaminhadores condicionais para os domínios `example.aws` e, encaminhando as consultas DNS desses `eu-west-1.compute.internal` domínios para os endereços IP do ponto final de entrada do resolvedor do Route 53.

Exemplo de uma configuração típica

Vamos considerar um cenário em que você tem dois tipos de usuários e seu AWS Directory Service usa um AD centralizado para autenticação de usuários:

- Trabalhadores que precisam de acesso total de qualquer lugar (por exemplo, funcionários em tempo integral) — Esses usuários terão acesso total à Internet e à rede interna e passarão por um firewall da VPC para a rede local.
- Funcionários que deveriam ter acesso restrito apenas de dentro da rede corporativa (por exemplo, prestadores de serviços e consultores) — Esses usuários restringiram o acesso à Internet por meio de um servidor proxy a sites específicos na VPC e terão acesso limitado à rede na VPC e na rede local.

Você gostaria de dar aos funcionários em tempo integral a capacidade de ter acesso de administrador local WorkSpace para instalar o software e gostaria de aplicar a autenticação de dois fatores com o MFA. Você também deseja permitir que funcionários em tempo integral acessem a Internet sem restrições. WorkSpace

Para prestadores de serviços, você deseja bloquear o acesso do administrador local para que eles possam usar somente aplicativos específicos pré-instalados. Você deseja aplicar controles restritivos de acesso à rede usando grupos de segurança para eles WorkSpaces. Você precisa abrir as portas 80 e 443 somente para sites internos específicos e deseja bloquear totalmente o acesso deles à Internet.

Nesse cenário, há dois tipos completamente diferentes de personas de usuário com requisitos diferentes de acesso à rede e ao desktop. É uma prática recomendada gerenciá-los e configurá-los de WorkSpaces forma diferente. Você precisará criar dois conectores AD, um para cada pessoa do usuário. Cada AD Connector exige duas sub-redes que tenham endereços IP suficientes disponíveis para atender às suas estimativas de crescimento WorkSpaces de uso.

> **Note**
>
> Cada sub-rede AWS VPC consome cinco endereços IP (os quatro primeiros e o último endereço IP) para fins de gerenciamento, e cada AD Connector consome um endereço IP em cada sub-rede em que persiste.

Outras considerações sobre esse cenário são as seguintes:

- AWS As sub-redes VPC devem ser sub-redes privadas, para que o tráfego, como o acesso à Internet, possa ser controlado por meio de um gateway de tradução de endereços de rede (NAT), de um servidor proxy-NAT na nuvem ou roteado de volta pelo sistema de gerenciamento de tráfego local.
- Existe um firewall para todo o tráfego de VPC vinculado à rede local.
- O servidor Microsoft AD e os servidores RADIUS do MFA estão no local (consulte o Cenário 1: Usando o AD Connector para autenticação de proxy no AD DS local neste documento) ou fazem parte da implementação da AWS nuvem (consulte o Cenário 2 e o Cenário 3, Cenários de implantação do AD DS, neste documento).

Como todos WorkSpaces recebem alguma forma de acesso à Internet e estão hospedados em uma sub-rede privada, você também deve criar sub-redes públicas que possam acessar a Internet por meio de um gateway de Internet. Você precisa de um gateway NAT para os funcionários em tempo integral, permitindo que eles acessem a Internet, e um servidor proxy-NAT para consultores e contratados, para limitar o acesso a sites internos específicos. Para planejar falhas, projetar para alta disponibilidade e limitar as cobranças de tráfego entre AZ, você deve ter dois gateways NAT e

servidores NAT ou proxy em duas sub-redes diferentes em uma implantação Multi-AZ. As duas AZs que você seleciona como sub-redes públicas corresponderão às duas AZs que você usa para suas WorkSpaces sub-redes, em regiões com mais de duas zonas. Você pode rotear todo o tráfego de cada WorkSpaces AZ para a sub-rede pública correspondente para limitar as tarifas de tráfego entre AZ e facilitar o gerenciamento. A figura a seguir mostra a configuração da VPC.

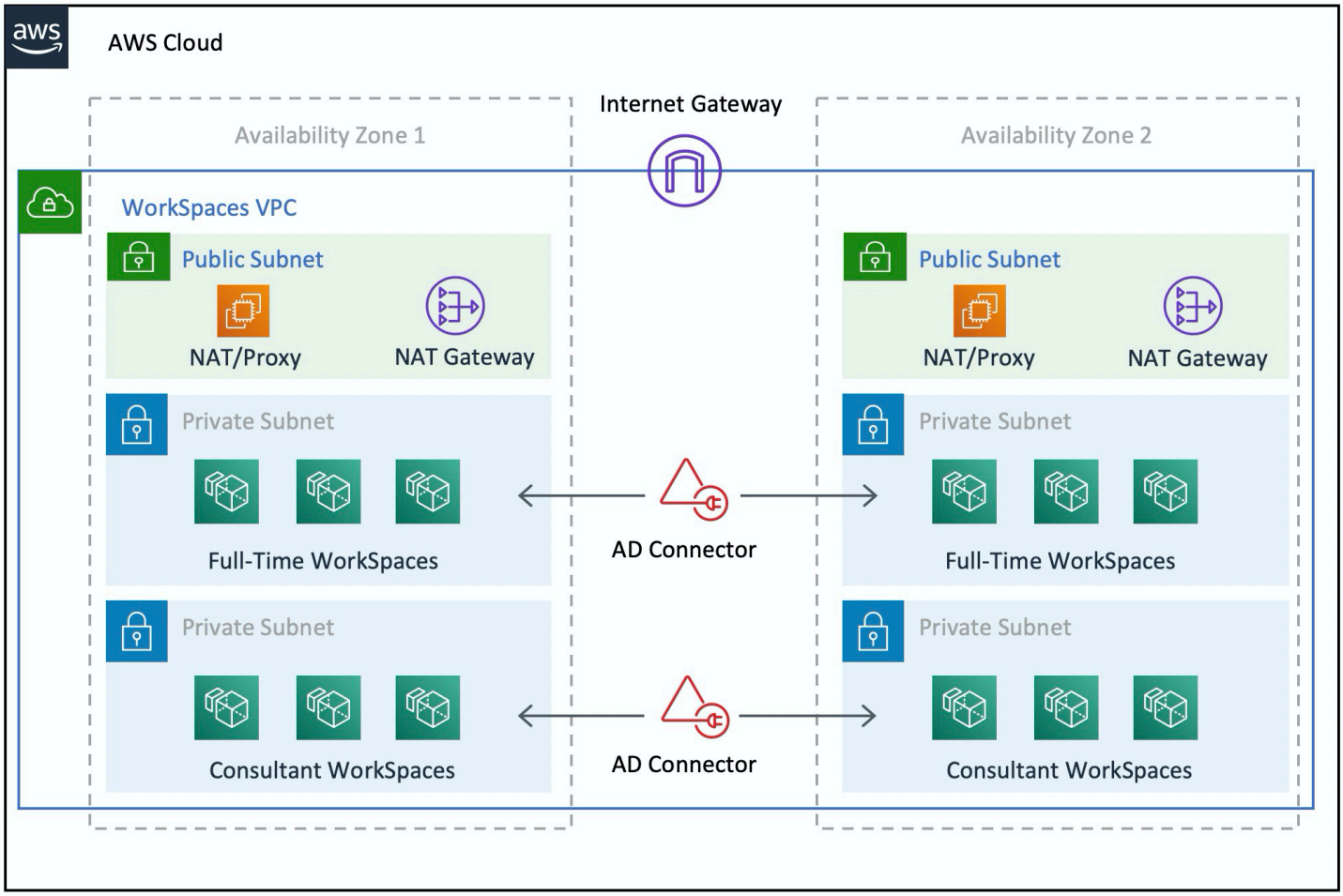

Figura 3: Design de VPC de alto nível

As informações a seguir descrevem como configurar os dois WorkSpaces tipos diferentes:

Para configurar WorkSpaces para funcionários em tempo integral:

1. No Amazon WorkSpaces Management Console, escolha a opção Diretórios na barra de menu.
2. Escolha o diretório que hospeda seus funcionários em tempo integral.
3. Escolha Configuração do administrador local.

Ao ativar essa opção, qualquer recém-criado WorkSpace terá privilégios de administrador local. Para conceder acesso à Internet, configure o NAT para acesso de saída à Internet a partir da sua VPC. Para habilitar o MFA, você precisa especificar um servidor RADIUS, IPs de servidor, portas e uma chave pré-compartilhada.

Para funcionários em tempo integral WorkSpaces, o tráfego de entrada para o WorkSpace pode ser limitado ao Remote Desktop Protocol (RDP) da sub-rede do Helpdesk, aplicando um grupo de segurança padrão por meio das configurações do AD Connector.

Para configurar WorkSpaces para prestadores de serviços e consultores:

1. No Amazon WorkSpaces Management Console, desative o acesso à Internet e a configuração do administrador local.
2. Adicione um grupo de segurança na seção Configurações do Grupo de Segurança para impor um grupo de segurança para todos os novos WorkSpaces criados nesse diretório.

Para consultores WorkSpaces, limite o tráfego de saída e entrada ao aplicando um grupo de segurança padrão WorkSpaces por meio das configurações do AD Connector a todos os WorkSpaces associados ao AD Connector. O grupo de segurança impede o acesso de saída WorkSpaces a qualquer coisa que não seja o tráfego HTTP e HTTPS e o tráfego de entrada ao RDP a partir da sub-rede do Helpdesk na rede local.

> **Note**
>
> O grupo de segurança se aplica somente à ENI que está na VPC `eth1` (no), e WorkSpace o acesso ao WorkSpace WorkSpaces do cliente não é restrito como resultado de um grupo de segurança. A figura a seguir mostra o design final da WorkSpaces VPC.

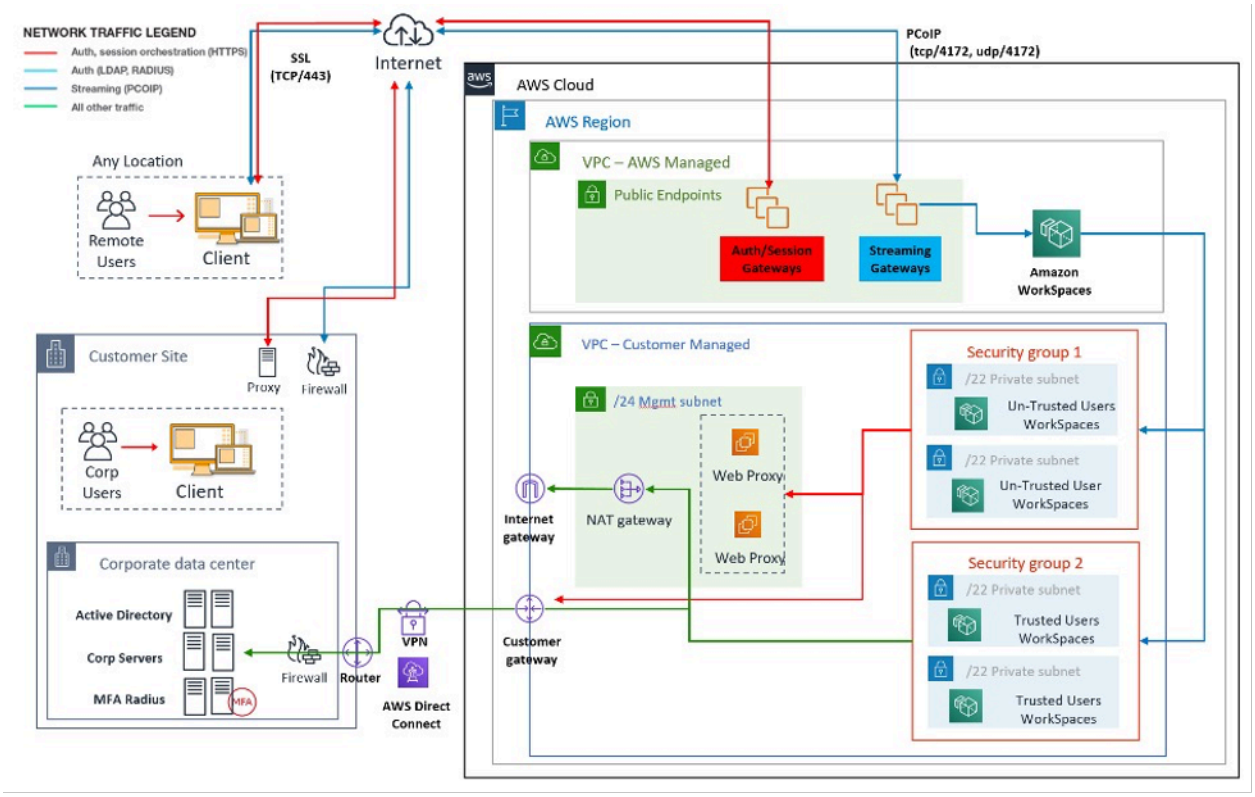

Figura 4: WorkSpaces design com personas de usuário

AWS Directory Service

Conforme mencionado na introdução, o AWS Directory Service é um componente essencial da Amazon WorkSpaces. Com o AWS Directory Service, você pode criar três tipos de diretórios com a Amazon WorkSpaces:

- AWS O Microsoft AD gerenciado é um Microsoft AD gerenciado, desenvolvido pelo Windows Server 2012 R2. AWS O Microsoft AD gerenciado está disponível nas edições Standard ou Enterprise.
- O Simple AD é um serviço de diretório gerenciado autônomo, compatível com o Microsoft AD e desenvolvido com o Samba 4.
- O AD Connector é um proxy de diretório para redirecionar solicitações de autenticação e pesquisas de usuários ou grupos para o Microsoft AD local existente.

A seção a seguir descreve os fluxos de comunicação para autenticação entre o serviço de WorkSpaces corretagem da Amazon e o AWS Directory Service, as melhores práticas para implementação WorkSpaces com o AWS Directory Service e conceitos avançados, como o MFA.

Também discute conceitos de arquitetura de infraestrutura para a Amazon WorkSpaces em grande escala, requisitos na Amazon VPC e Directory AWS Service, incluindo a integração com o Microsoft AD Domain Services (AD DS) local.

Cenários de implantação do AD DS

O apoio da Amazon WorkSpaces é o AWS Directory Service, e o design e a implantação adequados do serviço de diretório são essenciais. Os seis cenários a seguir se baseiam nos Serviços de Domínio do Active Directory no guia de Início AWS Rápido e descrevem as melhores práticas de implantação do AD DS quando usado com a Amazon WorkSpaces. A seção Considerações de design deste documento detalha os requisitos específicos e as melhores práticas de uso do AD Connector for WorkSpaces, que é parte integrante do conceito geral de WorkSpaces design.

- Cenário 1: Usando o AD Connector para a autenticação por proxy para o AD DS local — Nesse cenário, a conectividade de rede (VPN/Direct Connect) está em vigor para o cliente, com toda a autenticação enviada por proxy AWS via Directory Service (AD Connector) para o AD DS local do cliente.
- Cenário 2: Estendendo o AD DS local para AWS (réplica) — Esse cenário é semelhante ao cenário 1, mas aqui uma réplica do AD DS do cliente é implantada em combinação AWS com o AD Connector, reduzindo a latência das solicitações de autenticação/consulta para o AD DS e o catálogo global do AD DS.
- Cenário 3: implantação isolada autônoma usando o AWS Directory Service na AWS nuvem — Esse é um cenário isolado e não inclui conectividade com o cliente para autenticação. Essa abordagem usa o AWS Directory Service (Microsoft AD) e o AD Connector. Embora esse cenário não dependa da conectividade com o cliente para autenticação, ele provisiona o tráfego do aplicativo, quando necessário, via VPN ou Direct Connect.
- Cenário 4: AWS Microsoft AD e uma confiança transitiva bidirecional para o local — Esse cenário inclui o serviço gerenciado AWS do Microsoft AD (MAD) com uma confiança transitiva bidirecional para a floresta local do Microsoft AD.
- Cenário 5: AWS Microsoft AD usando uma VPC de Serviços Compartilhados — Esse cenário usa o AWS Microsoft AD gerenciado em uma VPC de Serviços Compartilhados para ser usado como um domínio de identidade para vários serviços (AWS Amazon EC2 WorkSpaces, Amazon etc.) enquanto usa o AD Connector para proxy de solicitações de autenticação de usuário do Lightweight Directory Access Protocol (LDAP) para os controladores de domínio AD.
- Cenário 6: AWS Microsoft AD, Shared Services VPC e uma confiança unidirecional no AD local — Esse cenário é semelhante ao Cenário 5, mas inclui domínios de identidade e recursos diferentes usando uma confiança unidirecional no local.

Você precisa fazer várias considerações ao selecionar seu cenário de implantação para os Serviços de Domínio do Active Directory (ADDS). Esta seção explica a função do AD Connector na Amazon WorkSpaces e aborda algumas considerações importantes ao selecionar um cenário de implantação do ADDS. Para obter mais orientações sobre design e planejamento do ADDS on AWS, consulte o Guia de AWS Design e Planejamento dos Serviços de Domínio do Active Directory.

O papel do AWS AD Connector com a Amazon WorkSpaces

O AWS AD Connector é um AWS Directory Service que atua como um serviço de proxy para um Active Directory. Ele não armazena nem armazena em cache nenhuma credencial de usuário, mas encaminha solicitações de autenticação ou pesquisa para o Active Directory, no local ou no local. AWS A menos que você esteja usando AWS Managed Microsoft AD, também é a única maneira de registrar seu Active Directory (local ou estendido para AWS) para uso com a Amazon WorkSpaces (WorkSpaces).

Um AD Connector pode apontar para seu Active Directory local, para um Active Directory estendido para AWS (controladores de domínio AD no Amazon EC2) ou para um. AWS Managed Microsoft AD

O AD Connector desempenha um papel importante na maioria dos cenários de implantação abordados nas seções a seguir. O uso do AD Connector com WorkSpaces oferece vários benefícios:

- Quando direcionado para o Active Directory corporativo, ele permite que seus usuários usem suas credenciais corporativas existentes para WorkSpaces fazer login em outros serviços, como a Amazon WorkDocs.
- Você pode aplicar consistentemente as políticas de segurança existentes (expiração de senha, bloqueios de conta etc.), independentemente de seus usuários estarem acessando recursos em sua infraestrutura local ou na Nuvem AWS, como. WorkSpaces
- O AD Connector permite uma integração simples com sua infraestrutura de MFA baseada em RADIUS existente para fornecer uma camada adicional de segurança.
- Ele permite a segregação de seus usuários. Por exemplo, ele permite a configuração de várias WorkSpaces opções por unidade de negócios ou pessoa, já que vários conectores AD podem estar apontando para os mesmos controladores de domínio (servidores DNS) do Active Directory para autenticação do usuário:
  - Domínio de destino ou unidade organizacional para aplicação direcionada de Objetos de Política de Grupo (GPOs) do Active Directory
  - Diferentes grupos de segurança para controlar o fluxo de tráfego de/para WorkSpaces

- Diferentes opções de controle de acesso (dispositivos clientes permitidos) e grupos de controle de acesso IP (limite o acesso aos intervalos de IP)
- Ativação seletiva de permissões de administrador local
- Permissões de autoatendimento diferentes
- Aplicação seletiva da Autenticação Multi-Factor (MFA)
- Posicionamento de suas interfaces de rede WorkSpaces elástica (ENI) em diferentes VPCs ou sub-redes para isolamento

Vários AD Connectors também permitem oferecer suporte a um número maior de usuários, se você estiver atingindo o limite de desempenho de um único AD Connector pequeno ou grande. Consulte a Dimensionamento de AWS Managed Microsoft AD seção para obter mais detalhes.

O uso de AD Connectors com WorkSpaces é gratuito, desde que você tenha pelo menos um WorkSpaces usuário ativo em um AD Connector pequeno e pelo menos 100 WorkSpaces usuários ativos em um AD Connector grande. Para obter mais informações, consulte a página de preços dos serviços de AWS diretório.

A importância de seu link de rede AWS com um Active Directory local

WorkSpaces depende da conectividade com seu Active Directory. Portanto, a disponibilidade do link de rede para o Active Directory é de extrema importância. Por exemplo, se seu link de rede no Cenário 1 estiver inativo, seus usuários não conseguirão se autenticar e, como resultado, não poderão usá-los WorkSpaces.

Se um Active Directory local for usado como parte do cenário, você precisará considerar a resiliência, a latência e o custo do tráfego do seu link de rede. AWS Em uma WorkSpaces implantação multirregional, isso pode envolver vários links de rede em diferentes AWS regiões ou vários AWS Transit Gateway s com emparelhamento estabelecido entre eles para rotear o tráfego do AD para a VPC com conectividade com o AD local. Essas considerações sobre links de rede se aplicam à maioria dos cenários descritos nas seções a seguir, mas são especialmente importantes para aqueles cenários em que o tráfego do AD a partir dos conectores AD WorkSpaces precisa atravessar o link de rede para chegar ao Active Directory local. O cenário 1 destaca algumas das ressalvas.

Usando a autenticação multifatorial com WorkSpaces

Se você planeja usar o Multi-Factor Authentication (MFA) WorkSpaces com, você deve usar um AD AWS Connector ou AWS Managed Microsoft AD um, pois somente esses serviços permitem o

registro do diretório para uso WorkSpaces e a configuração do RADIUS. Para o posicionamento de seus servidores RADIUS, as considerações sobre links de rede abordadas na A importância de seu link de rede AWS com um Active Directory local seção se aplicam.

Separando a conta e o domínio do recurso

Por motivos de segurança ou para melhorar a capacidade de gerenciamento, talvez seja desejável separar o domínio da conta do domínio do recurso. Por exemplo, coloque os objetos do WorkSpaces computador em um domínio de recursos separado, enquanto os usuários fazem parte do domínio da conta. Uma implementação como essa pode ser usada para permitir que uma organização parceira gerencie o WorkSpaces uso de políticas de grupo do AD no domínio de recursos, sem abrir mão do controle ou conceder acesso ao domínio da conta. Isso pode ser feito usando dois Active Directories com um Active Directory Trust configurado. As seções a seguir abordam isso com mais detalhes:

- Cenário 4: AWS Microsoft AD e uma confiança transitiva bidirecional para o local
- Cenário 6: AWS Microsoft AD, VPC de serviços compartilhados e uma confiança unidirecional no local

Grandes implantações do Active Directory

Você deve garantir que os Sites e Serviços do Active Directory estejam configurados adequadamente. Isso é especialmente importante se o Active Directory consistir em um grande número de controladores de domínio em diferentes localizações geográficas. Seu Windows WorkSpaces usa o mecanismo padrão da Microsoft para descobrir seu controlador de domínio para o site do Active Directory ao qual está atribuído. Esse processo do DC Locator depende do DNS e pode ser significativamente prolongado caso uma longa lista de controladores de domínio com prioridade e peso inespecíficos seja retornada no estágio inicial do processo do DC Locator. Mais importante ainda, se você WorkSpaces ficar “preso” a um controlador de domínio abaixo do ideal, toda comunicação subsequente com esse controlador de domínio poderá sofrer com o aumento da latência da rede e a redução da largura de banda ao atravessar links de rede de longa distância. Isso diminuirá qualquer comunicação com o controlador de domínio, incluindo o processamento de um número potencialmente grande de Objetos de Política de Grupo (GPOs) e transferências de arquivos do controlador de domínio. Dependendo da topologia da rede, isso também pode aumentar seu custo de rede, porque os dados trocados entre os controladores de domínio WorkSpaces e os controladores de domínio podem percorrer desnecessariamente um caminho de rede mais caro. Consulte as Considerações sobre design seções Design em VPC e para obter orientação sobre DHCP e DNS com seu design de VPC e sites e serviços do Active Directory.

Usando o Microsoft Azure Active Directory ou os Serviços de Domínio do Active Directory com WorkSpaces

Se você pretende usar o Microsoft Azure Active Directory com WorkSpaces, você pode usar o Azure AD Connect para sincronizar sua identidade com o Active Directory local ou com o Active Directory em AWS (controlador de domínio no Amazon AWS Managed Microsoft AD EC2 ou). No entanto, isso não permitirá que você participe WorkSpaces do Azure Active Directory. Para obter mais informações, consulte a Documentação de Identidade Híbrida da Microsoft na Documentação do Microsoft Azure.

Se quiser associá-lo ao Azure Active Directory, você precisará implantar o Microsoft Azure Active Directory Domain Services (Azure AD DS), estabelecer conectividade entre o Azure AWS e usar um AWS AD Connector apontando para seus Controladores de Domínio do Azure AD DS. WorkSpaces Para obter mais informações sobre como configurar isso, consulte a postagem do blog Adicione seu WorkSpaces ao Azure AD usando o Azure Active Directory Domain Services.

Ao usar AWS Directory Service s with WorkSpaces, você precisará considerar o tamanho de sua WorkSpaces implantação e o crescimento esperado para dimensioná-la AWS Directory Service adequadamente. Esta seção fornece orientação sobre o dimensionamento do AWS Directory Service para uso com WorkSpaces. Também recomendamos que você revise as melhores práticas para o AD Connector e as melhores práticas para AWS Managed Microsoft AD as seções do Guia de AWS Directory Service administração.

Dimensionamento do AD Connector com WorkSpaces

O conector do Active Directory (AD Connector) está disponível em dois tamanhos, pequeno e grande. Embora não haja limites forçados de usuários ou conexões, recomendamos usar um pequeno AD Connector para até 500 usuários WorkSpaces autorizados e um AD Connector grande para até 5.000 usuários WorkSpaces autorizados. Você pode distribuir cargas de aplicativos em vários AD Connector para escalar de acordo com suas necessidades de desempenho. Por exemplo, se você precisar oferecer suporte a 1500 WorkSpaces usuários, poderá distribuí-los WorkSpaces igualmente por três pequenos AD Connector, cada um suportando 500 usuários. Se todos os seus usuários residirem no mesmo domínio, o AD Connector pode apontar todos para o mesmo conjunto de servidores DNS resolvendo seu domínio do Active Directory.

Observe que, se você começou com um AD Connector pequeno e sua WorkSpaces implantação cresce com o tempo, você pode criar um ticket de suporte para que o tamanho do AD Connector

seja alterado de pequeno para grande, a fim de lidar com o maior número de usuários WorkSpaces autorizados.

Dimensionamento de AWS Managed Microsoft AD

AWS Managed Microsoft ADpermite que você execute o Microsoft Active Directory como um serviço gerenciado. Você pode escolher entre a Standard Edition e a Enterprise Edition ao iniciar o serviço. A Standard Edition é recomendada para empresas de pequeno e médio porte com até 5.000 usuários e oferece suporte a aproximadamente 30.000 objetos de diretório, como usuários, grupos e computadores. A Enterprise Edition foi projetada para suportar até 500.000 objetos de diretório e também oferece um recurso adicional, como replicação multirregional.

Se você precisar oferecer suporte a mais de 500.000 objetos de diretório, considere a implantação de controladores de domínio do Microsoft Active Directory no Amazon EC2. Para saber o tamanho desses controladores de domínio, consulte o documento Planejamento de capacidade para serviços de domínio do Active Directory da Microsoft.

Cenário 1: Usando o conector AD para autenticação de proxy no Active Directory Service local

Esse cenário é para clientes que não desejam estender seu serviço AD local ou onde uma nova implantação do AD DS não é uma opção. AWS A figura a seguir mostra, em alto nível, cada um dos componentes e o fluxo de autenticação do usuário.

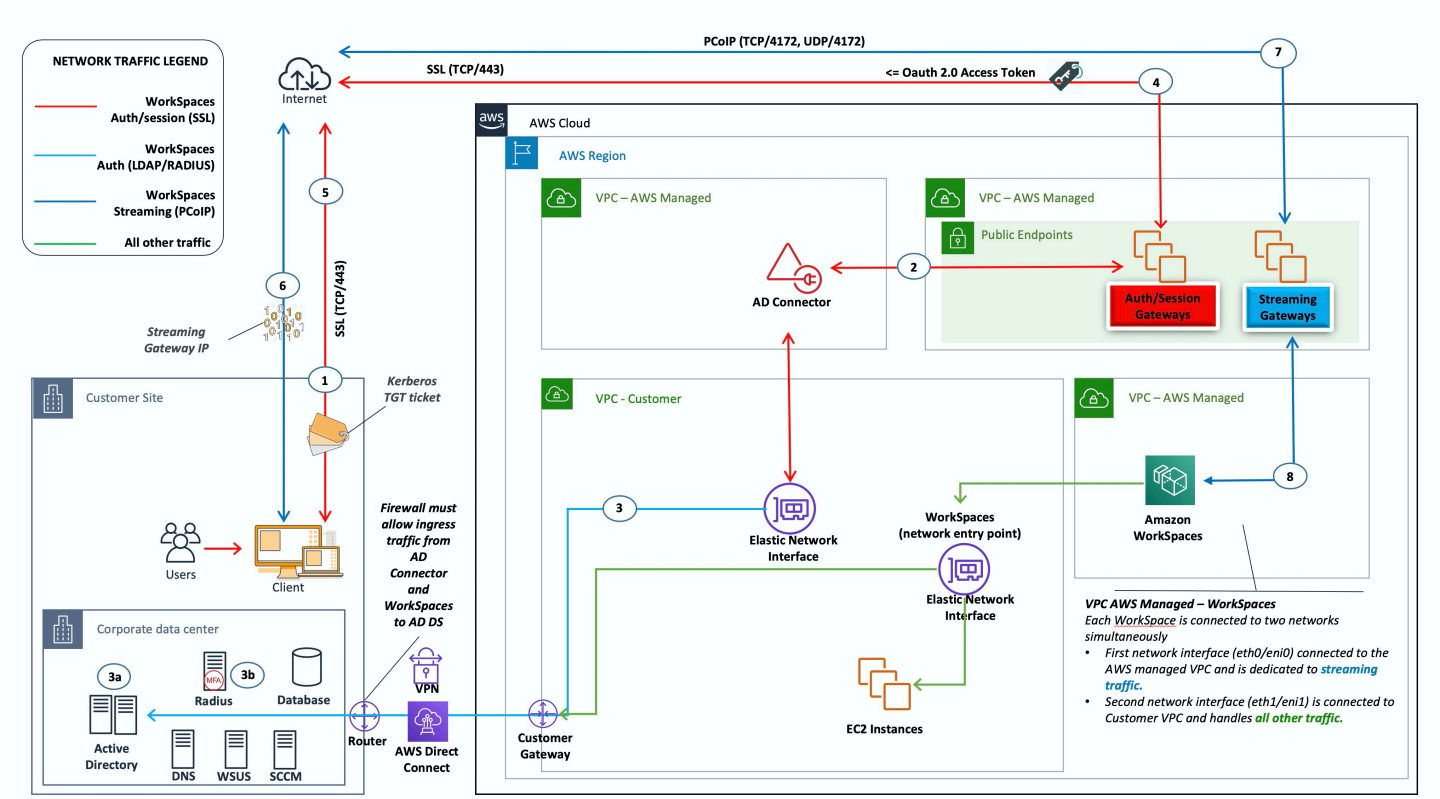

Figura 5: AD Connector para o Active Directory local

Nesse cenário, o AWS Directory Service (AD Connector) é usado para todas as autenticações de usuário ou MFA enviadas por proxy por meio do AD Connector para o AD DS local do cliente (detalhado na figura a seguir). Para obter detalhes sobre os protocolos ou a criptografia usados para o processo de autenticação, consulte a Segurança seção deste documento.

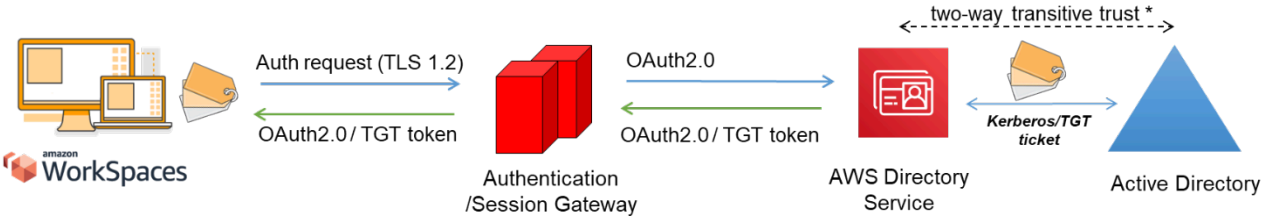

Figura 6: Autenticação do usuário por meio do Authentication Gateway

O cenário 1 mostra uma arquitetura híbrida na qual o cliente pode já ter recursos AWS, bem como recursos em um data center local que pode ser acessado via Amazon WorkSpaces. O cliente pode aproveitar seus servidores AD DS e RADIUS locais existentes para autenticação de usuário e MFA.

Essa arquitetura usa os seguintes componentes ou construções:

AWS

- Amazon VPC — Criação de uma Amazon VPC com pelo menos duas sub-redes privadas em duas AZs.
- Conjunto de opções DHCP — Criação de um conjunto de opções DHCP da Amazon VPC. Isso permite que o nome de domínio especificado pelo cliente e os servidores de nomes de domínio (DNS) (serviços locais) sejam definidos. Para obter mais informações, consulte Conjuntos de opções de DHCP.
- Amazon Virtual Private Gateway — Habilite a comunicação com sua própria rede por meio de um túnel VPN IPsec ou uma AWS Direct Connect conexão.
- AWS Directory Service — O AD Connector é implantado em um par de sub-redes privadas da Amazon VPC.
- Amazon WorkSpaces — WorkSpaces são implantados nas mesmas sub-redes privadas do AD Connector. Para obter mais informações, consulte a seção Active Directory: Sites e Serviços deste documento.

Cliente

- Conectividade de rede — VPN corporativa ou endpoints Direct Connect.
- AD DS — AD DS corporativo.
- MFA (opcional) — servidor RADIUS corporativo.
- Dispositivos de usuário final — Dispositivos de usuário final corporativos ou com licença própria (BYOL) (como Windows, Macs, iPads, tablets Android, zero clients e Chromebooks) usados para acessar o serviço da Amazon. WorkSpaces Consulte esta lista de aplicativos cliente para dispositivos e navegadores da Web compatíveis.

Embora essa solução seja excelente para clientes que não desejam implantar o AD DS na nuvem, ela vem com algumas ressalvas:

- Confiança na conectividade — Se a conectividade com o data center for perdida, os usuários não poderão fazer login em suas respectivas conexões WorkSpaces, e as conexões existentes permanecerão ativas durante toda a vida útil do Kerberos/Ticket-Granting Ticket (TGT).

- Latência — Se a latência existir por meio da conexão (esse é mais o caso da VPN do que do Direct Connect), a WorkSpaces autenticação e qualquer atividade relacionada ao AD DS, como a aplicação da Política de Grupo (GPO), levarão mais tempo.
- Custos de tráfego — Toda autenticação deve passar pelo link da VPN ou do Direct Connect e, portanto, depende do tipo de conexão. Isso é transferência de dados para fora do Amazon EC2 para a Internet ou transferência de dados para fora (Direct Connect).

> **Note**
>
> O AD Connector é um serviço de proxy. Ele não armazena nem armazena em cache as credenciais do usuário. Em vez disso, todas as solicitações de autenticação, pesquisa e gerenciamento são tratadas pelo seu AD. É necessária uma conta com privilégios de delegação em seu serviço de diretório com direitos para ler todas as informações do usuário e associar um computador ao domínio.

Em geral, a WorkSpaces experiência depende muito do processo de autenticação do Active Directory mostrado na figura anterior. Nesse cenário, a experiência de WorkSpaces autenticação é altamente dependente do link de rede entre o AD do cliente e a WorkSpaces VPC. O cliente deve garantir que o link esteja altamente disponível.

Cenário 2: Estendendo o AD DS local para AWS (réplica)

Esse cenário é semelhante ao cenário 1. No entanto, nesse cenário, uma réplica do AD DS do cliente é implantada AWS em combinação com o AD Connector. Isso reduz a latência das solicitações de autenticação ou consulta para o AD DS em execução no Amazon Elastic Compute Cloud (Amazon EC2). A figura a seguir mostra uma visão de alto nível de cada um dos componentes e do fluxo de autenticação do usuário.

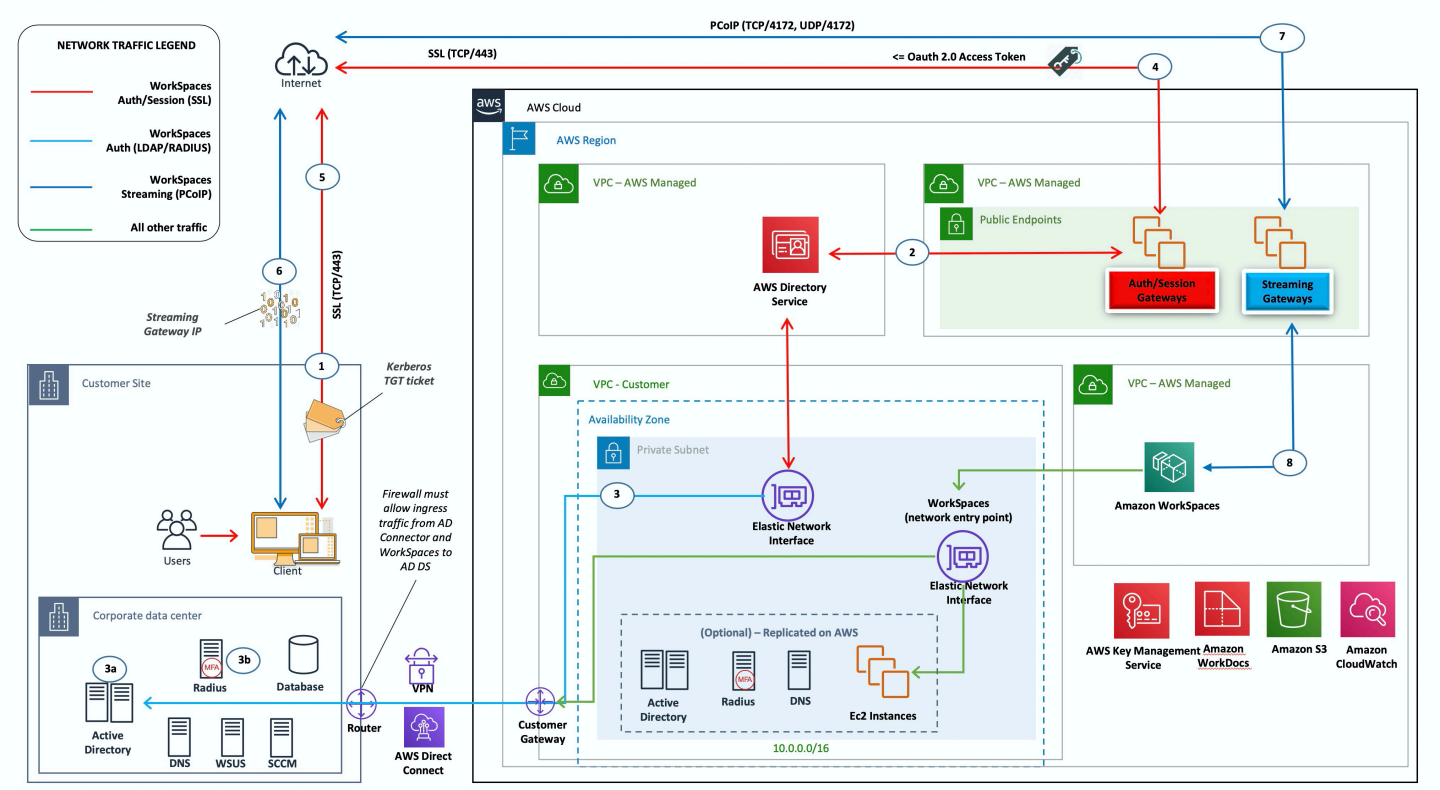

Figura 7: Estenda o domínio do Active Directory do cliente para a nuvem

Como no cenário 1, o AD Connector é usado para todas as autenticações de usuários ou MFA, que, por sua vez, são enviadas por proxy para o AD DS do cliente (consulte a figura anterior). Nesse cenário, o AD DS do cliente é implantado em AZs em instâncias do Amazon EC2 que são promovidas a controladoras de domínio na floresta AD local do cliente, em execução na nuvem. AWS Cada controlador de domínio é implantado em sub-redes privadas da VPC para tornar o AD DS altamente disponível na nuvem. AWS Para obter as melhores práticas para implantar o AD DS em AWS, consulte a seção Considerações de design deste documento.

Depois que as WorkSpaces instâncias são implantadas, elas têm acesso aos controladores de domínio baseados em nuvem para serviços de diretório e DNS seguros e de baixa latência. Todo o tráfego de rede, incluindo comunicação do AD DS, solicitações de autenticação e replicação do AD, é protegido nas sub-redes privadas ou no túnel VPN do cliente ou no Direct Connect.

Essa arquitetura usa os seguintes componentes ou construções:

AWS

- Amazon VPC — Criação de uma Amazon VPC com pelo menos quatro sub-redes privadas em duas AZs — duas para o cliente AD DS, duas para o AD Connector ou Amazon. WorkSpaces

- Conjunto de opções DHCP — Criação de um conjunto de opções DHCP da Amazon VPC. Isso permite que o cliente defina um nome de domínio e DNSs específicos (AD DS local). Para obter mais informações, consulte Conjuntos de opções de DHCP.
- Amazon Virtual Private Gateway — Habilite a comunicação com uma rede de propriedade do cliente por meio de um túnel ou conexão VPN IPsec. AWS Direct Connect
- Amazon EC2
  - Controladores de domínio AD DS corporativos do cliente implantados em instâncias do Amazon EC2 em sub-redes VPC privadas dedicadas.
  - Servidores RADIUS do cliente (opcionais) para MFA em instâncias do Amazon EC2 em sub-redes VPC privadas dedicadas.
- AWS Serviços de diretório — O AD Connector é implantado em um par de sub-redes privadas da Amazon VPC.
- Amazon WorkSpaces — WorkSpaces são implantados nas mesmas sub-redes privadas do AD Connector. Para obter mais informações, consulte a seção Active Directory: Sites e Serviços deste documento.

Cliente

- Conectividade de rede — VPN corporativa ou AWS Direct Connect endpoints.
- AD DS — AD DS corporativo (necessário para replicação).
- MFA (opcional) — servidor RADIUS corporativo.
- Dispositivos de usuário final — dispositivos de usuário final corporativos ou BYOL (como Windows, Macs, iPads, tablets Android, zero clients e Chromebooks) usados para acessar o serviço da Amazon. WorkSpaces Consulte a lista de aplicativos cliente para dispositivos e navegadores da Web compatíveis. Essa solução não tem as mesmas ressalvas do cenário 1. A Amazon WorkSpaces e o AWS Directory Service não dependem da conectividade existente.
- Confiança na conectividade — Se a conectividade com o data center do cliente for perdida, os usuários finais poderão continuar trabalhando porque a autenticação e a MFA opcional são processadas localmente.
- Latência — Com exceção do tráfego de replicação, toda autenticação é local e tem baixa latência. Consulte a seção Active Directory: Sites e Serviços deste documento.

- Custos de tráfego — Nesse cenário, a autenticação é local, com apenas a replicação do AD DS precisando atravessar o link da VPN ou do Direct Connect, reduzindo a transferência de dados.

Em geral, a WorkSpaces experiência é aprimorada e não depende muito da conectividade com os controladores de domínio locais, conforme mostrado na figura anterior. Esse também é o caso quando um cliente deseja escalar WorkSpaces para milhares de desktops, especialmente em relação às consultas do catálogo global do AD DS, pois esse tráfego permanece local para o WorkSpaces ambiente.

Cenário 3: implantação isolada autônoma usando AWS Directory Service na nuvem AWS

Esse cenário, mostrado na figura a seguir, tem o AD DS implantado na AWS nuvem em um ambiente isolado autônomo. AWS O Directory Service é usado exclusivamente nesse cenário. Em vez de gerenciar totalmente o AD DS, os clientes podem confiar no AWS Directory Service para tarefas como criar uma topologia de diretório altamente disponível, monitorar controladores de domínio e configurar backups e instantâneos.

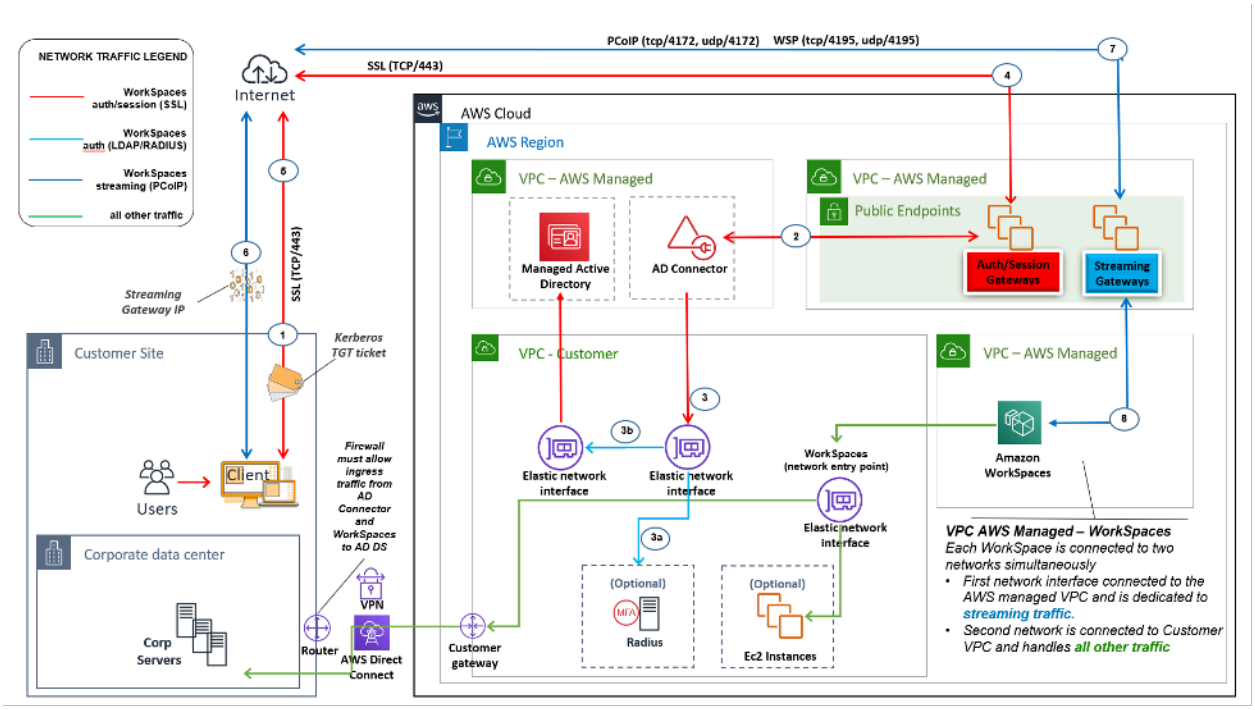

Figura 8: Somente na nuvem: Serviços de AWS diretório (Microsoft AD)

Como no cenário 2, o AD DS (Microsoft AD) é implantado em sub-redes dedicadas que abrangem duas AZs, tornando o AD DS altamente disponível na nuvem. AWS Além do Microsoft AD, o AD

Connector (em todos os três cenários) é implantado para WorkSpaces autenticação ou MFA. Isso garante a separação de papéis ou funções dentro da Amazon VPC, o que é uma prática recomendada padrão. Para obter mais informações, consulte a seção Considerações de design deste documento.

O cenário 3 é uma configuração padrão e completa que funciona bem para clientes que desejam AWS gerenciar a implantação, a aplicação de patches, a alta disponibilidade e o monitoramento do AWS Directory Service. O cenário também funciona bem para provas de conceitos, laboratórios e ambientes de produção devido ao seu modo de isolamento.

Além do posicionamento do AWS Directory Service, esta figura mostra o fluxo de tráfego de um usuário para um espaço de trabalho e como o espaço de trabalho interage com o servidor AD e o servidor MFA.

Essa arquitetura usa os seguintes componentes ou construções.

AWS

- Amazon VPC — Criação de uma Amazon VPC com pelo menos quatro sub-redes privadas em duas AZs — duas para AD DS Microsoft AD, duas para AD Connector ou. WorkSpaces
- Conjunto de opções DHCP — Criação de um conjunto de opções DHCP da Amazon VPC. Isso permite que um cliente defina um nome de domínio e DNS especificados (Microsoft AD). Para obter mais informações, consulte Conjuntos de opções de DHCP.
- Opcional: Amazon virtual private gateway — Habilite a comunicação com uma rede de propriedade do cliente por meio de um túnel VPN IPsec (VPN) ou conexão. AWS Direct Connect Use para acessar sistemas de back-end locais.
- AWS Directory Service — Microsoft AD implantado em um par dedicado de sub-redes VPC (AD DS Managed Service).
- Amazon EC2 — Servidores RADIUS “opcionais” do cliente para MFA.
- AWS Serviços de diretório — O AD Connector é implantado em um par de sub-redes privadas da Amazon VPC.
- Amazon WorkSpaces — WorkSpaces são implantados nas mesmas sub-redes privadas do AD Connector. Para obter mais informações, consulte a seção Active Directory: Sites e Serviços deste documento.

Cliente

- Opcional: Conectividade de rede — VPN corporativa ou AWS Direct Connect endpoints.
- Dispositivos de usuário final — dispositivos corporativos ou BYOL para usuários finais (como Windows, Macs, iPads, tablets Android, zero clients e Chromebooks) usados para acessar o serviço da Amazon. WorkSpaces Consulte esta lista de aplicativos cliente para dispositivos e navegadores da Web compatíveis.

Assim como no cenário 2, esse cenário não tem problemas com a dependência da conectividade com o data center local do cliente, da latência ou dos custos de transferência de dados (exceto quando o acesso à Internet está habilitado dentro WorkSpaces da VPC) porque, por definição, esse é um cenário isolado ou somente na nuvem.

Cenário 4: AWS Microsoft AD e uma confiança transitiva bidirecional para o local

Esse cenário, mostrado na figura a seguir, tem o AD AWS gerenciado implantado na AWS nuvem, que tem uma confiança transitiva bidirecional no AD local do cliente. Os usuários e WorkSpaces são criados no AD gerenciado, com a confiança do AD permitindo que os recursos sejam acessados no ambiente local.

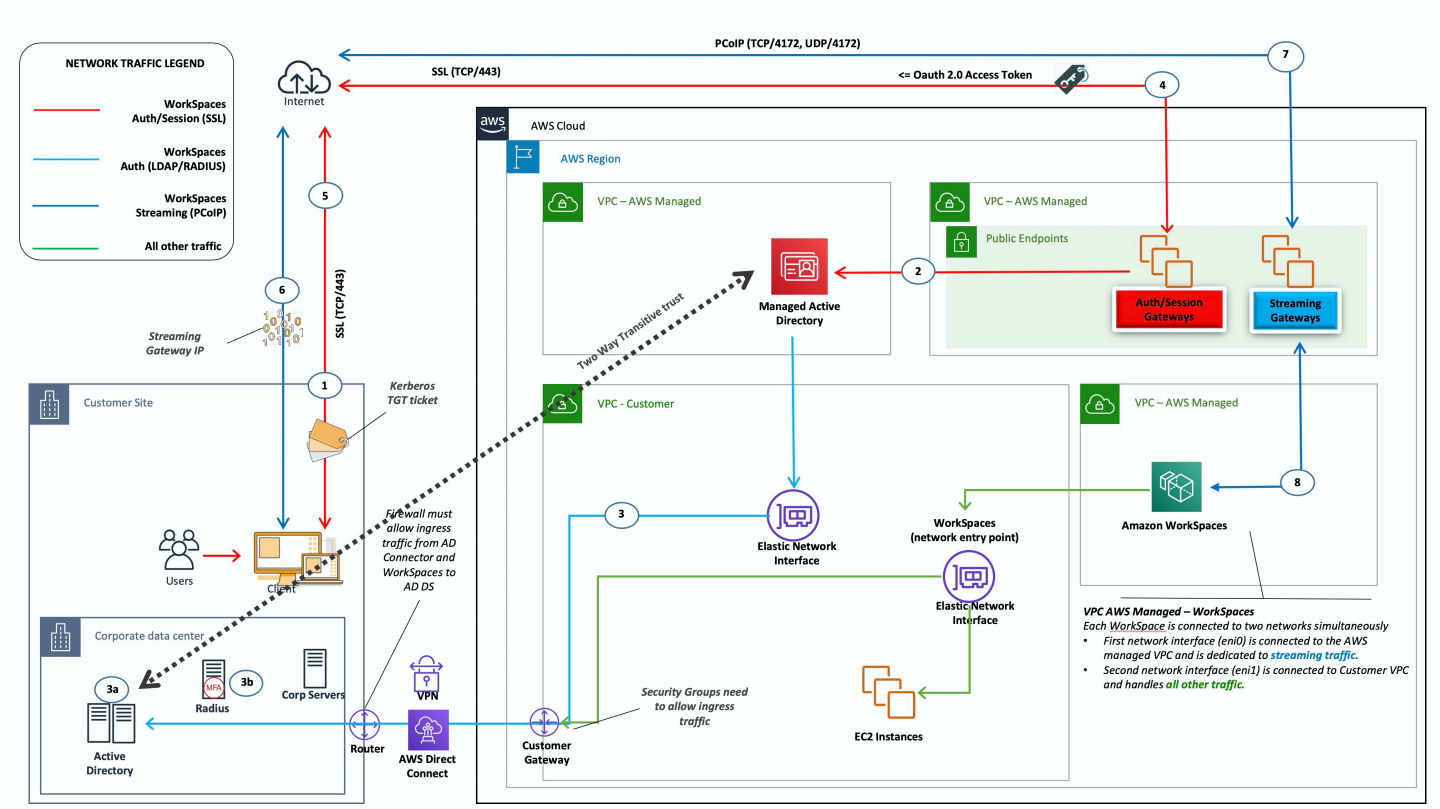

Figura 9: AWS Microsoft AD e uma confiança transitiva bidirecional para o local

Como no cenário 3, o AD DS (Microsoft AD) é implantado em sub-redes dedicadas que abrangem duas AZs, tornando o AD DS altamente disponível na nuvem. AWS

Esse cenário funciona bem para clientes que desejam ter um AWS Directory Service totalmente gerenciado, incluindo implantação, aplicação de patches, alta disponibilidade e monitoramento de sua AWS nuvem. Esse cenário também permite que WorkSpaces os usuários acessem recursos associados ao AD em suas redes existentes. Esse cenário exige a existência de uma relação de confiança de domínio. Grupos de segurança e regras de firewall precisam permitir a comunicação entre os dois diretórios ativos.

Além do posicionamento do AWS Directory Service, a figura anterior descreve o fluxo de tráfego de um usuário para um espaço de trabalho e como o espaço de trabalho interage com o servidor AD e o servidor MFA.

Essa arquitetura usa os seguintes componentes ou construções.

AWS

- Amazon VPC — Criação de uma Amazon VPC com pelo menos quatro sub-redes privadas em duas AZs — duas para AD DS Microsoft AD, duas para AD Connector ou. WorkSpaces
- Conjunto de opções DHCP — Criação de um conjunto de opções DHCP da Amazon VPC. Isso permite que o cliente defina um nome de domínio e DNS especificados (Microsoft AD). Para obter mais informações, consulte Conjuntos de opções de DHCP.
- Opcional: Amazon virtual private gateway — Habilite a comunicação com uma rede de propriedade do cliente por meio de um túnel VPN IPsec (VPN) ou conexão. AWS Direct Connect Use para acessar sistemas de back-end locais.
- AWS Directory Service — Microsoft AD implantado em um par dedicado de sub-redes VPC (AD DS Managed Service).

- Amazon EC2 — Servidores RADIUS opcionais do cliente para MFA.
- Amazon WorkSpaces — WorkSpaces são implantados nas mesmas sub-redes privadas do AD Connector. Para obter mais informações, consulte a seção Active Directory: Sites e Serviços deste documento.

Cliente

- Conectividade de rede — VPN corporativa ou AWS Direct Connect endpoints.
- Dispositivos de usuário final — dispositivos corporativos ou BYOL para usuários finais (como Windows, Macs, iPads, tablets Android, zero clients e Chromebooks) usados para acessar o serviço da Amazon. WorkSpaces Consulte a lista de aplicativos cliente para dispositivos e navegadores da Web compatíveis.

Essa solução requer conectividade com o data center local do cliente para permitir que o processo de confiança opere. Se WorkSpaces os usuários estiverem usando recursos na rede local, a latência e os custos de transferência de dados de saída precisam ser considerados.

Cenário 5: AWS Microsoft AD usando uma Virtual Private Cloud (VPC) de serviços compartilhados

Esse cenário, mostrado na figura a seguir, tem um AD AWS gerenciado implantado na AWS nuvem, fornecendo serviços de autenticação para cargas de trabalho que já estão hospedadas AWS ou planejadas para serem parte de uma migração mais ampla. A recomendação de melhores práticas é ter a Amazon WorkSpaces em uma VPC dedicada. Os clientes também devem criar um AD OU específico para organizar os objetos do WorkSpaces computador.

Para implantar WorkSpaces com uma VPC de serviços compartilhados que hospeda o AD gerenciado, implante um AD Connector (ADC) com uma conta de serviço do ADC criada no AD gerenciado. A conta de serviço exige permissões para criar objetos de computador na OU WorkSpaces designada no AD gerenciado de serviços compartilhados.

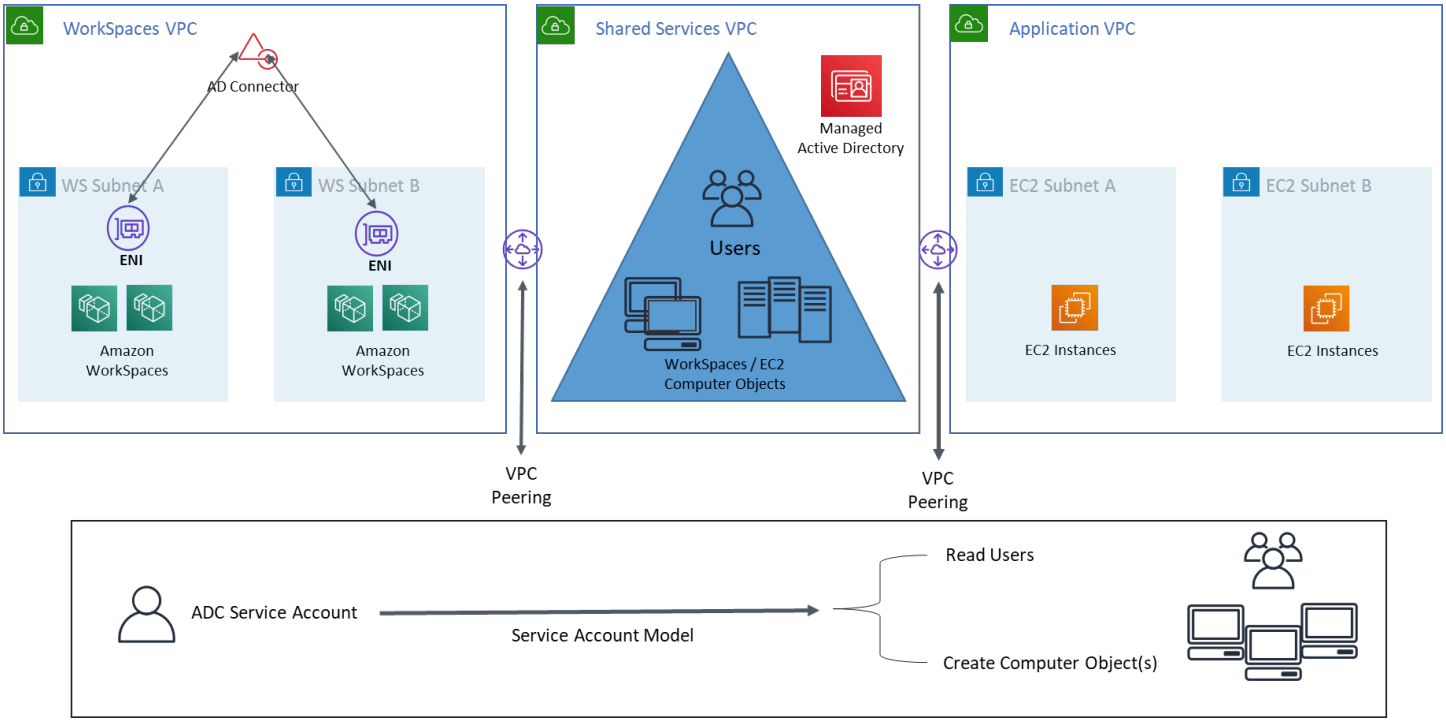

Figura 10: AWS Microsoft AD usando uma VPC de serviços compartilhados

Essa arquitetura usa os seguintes componentes ou construções.

AWS

- Amazon VPC — Criação de uma Amazon VPC com pelo menos duas sub-redes privadas em duas AZs (duas para AD Connector e). WorkSpaces

- Conjunto de opções DHCP — Criação de um conjunto de opções DHCP da Amazon VPC. Isso permite que um cliente defina um nome de domínio e DNS especificados (Microsoft AD). Para obter mais informações, consulte Conjuntos de opções de DHCP.
- Opcional: Amazon virtual private gateway — Habilite a comunicação com uma rede de propriedade do cliente por meio de um túnel VPN IPsec (VPN) ou conexão. AWS Direct Connect Use para acessar sistemas de back-end locais.
- AWS Directory Service — Microsoft AD implantado em um par dedicado de sub-redes VPC (AD DS Managed Service), AD Connector
- AWS Transit Gateway/VPC Peering — Habilite a conectividade entre o Workspaces VPC e o Shared Services VPC
- Amazon EC2 — Servidores RADIUS opcionais do cliente para MFA.
- Amazon WorkSpaces — WorkSpaces são implantados nas mesmas sub-redes privadas do AD Connector. Para obter mais informações, consulte a seção Active Directory: Sites e Serviços deste documento.

Cliente

- Conectividade de rede — VPN corporativa ou AWS Direct Connect endpoints.
- Dispositivos de usuário final — dispositivos corporativos ou BYOL para usuários finais (como Windows, Macs, iPads, tablets Android, zero clients e Chromebooks) usados para acessar o serviço da Amazon. WorkSpaces Consulte a lista de aplicativos cliente para dispositivos e navegadores da Web compatíveis.

Cenário 6: AWS Microsoft AD, VPC de serviços compartilhados e uma confiança unidirecional no local

Esse cenário, conforme mostrado na figura a seguir, usa um Active Directory local existente para usuários e introduz um Active Directory gerenciado separado na AWS nuvem para hospedar os objetos de computador associados ao. WorkSpaces Esse cenário permite que os objetos do computador e as políticas de grupo do Active Directory sejam gerenciados independentemente do Active Directory corporativo.

Esse cenário é útil quando um terceiro deseja gerenciar o Windows WorkSpaces em nome de um cliente, pois permite que o terceiro defina e controle as WorkSpaces políticas associadas a elas, sem

a necessidade de conceder acesso ao AD do cliente. Nesse cenário, uma unidade organizacional (OU) específica do Active Directory é criada para organizar os objetos do WorkSpaces computador no AD do Shared Services.

> **Note**
>
> O Amazon Linux WorkSpaces exige que exista uma relação de confiança bidirecional para que eles sejam criados.

Para implantar o Windows WorkSpaces com os objetos de computador criados na VPC do Shared Services que hospeda o Active Directory Gerenciado usando usuários do domínio de identidade do cliente, implante um Conector do Active Directory (ADC) referenciando o AD corporativo. Use uma conta de serviço do ADC criada no AD corporativo (domínio de identidade) que tenha permissões delegadas para criar objetos de computador na Unidade Organizacional (OU) que foi configurada para o Windows WorkSpaces no AD gerenciado do Shared Services e que tenha permissões de leitura no Active Directory corporativo (domínio de identidade).

Para garantir que a função Localizador de Domínio seja capaz de autenticar WorkSpaces usuários no site do AD desejado para o domínio de identidade, nomeie os dois sites AD do domínio para as WorkSpaces sub-redes da Amazon de forma idêntica, conforme a documentação da Microsoft. É uma prática recomendada ter controladores de domínio AD do domínio de identidade e do domínio de Serviços Compartilhados na mesma AWS região da Amazon WorkSpaces.

Para obter instruções detalhadas sobre como configurar esse cenário, consulte o guia de implementação para configurar uma confiança unidirecional para a Amazon WorkSpaces com o AWS Directory Services

Nesse cenário, estabelecemos uma confiança transitiva unidirecional entre a AWS Managed Microsoft AD VPC do Shared Services e o AD local. A Figura 11 mostra a direção da confiança e do acesso e como o AWS AD Connector usa a conta de serviço do AD Connector para criar objetos de computador no domínio do recurso.

Uma relação de confiança florestal é usada de acordo com a recomendação da Microsoft para garantir que a autenticação Kerberos seja usada sempre que possível. Você WorkSpaces recebe Objetos de Política de Grupo (GPOs) do seu domínio de recursos no AWS Managed Microsoft AD. Além disso, você WorkSpaces realiza a autenticação Kerberos com seu domínio de identidade. Para que isso funcione de forma confiável, é uma prática recomendada estender seu domínio de identidade para, AWS conforme já explicado acima. Sugerimos que você analise o guia de

implementação do Deploy Amazon WorkSpaces using a One-Way Trust Resource Domain com guia de AWS Directory Service implementação para obter mais detalhes.

Tanto o AD Connector quanto o seu WorkSpaces devem ser capazes de se comunicar com os controladores de domínio do seu domínio de identidade e do seu domínio de recursos. Para obter mais informações, consulte os requisitos de endereço IP e porta WorkSpaces no Guia de WorkSpaces Administração da Amazon.

Se você usa vários conectores AD, é uma prática recomendada que cada um dos conectores AD use sua própria conta de serviço do AD Connector.

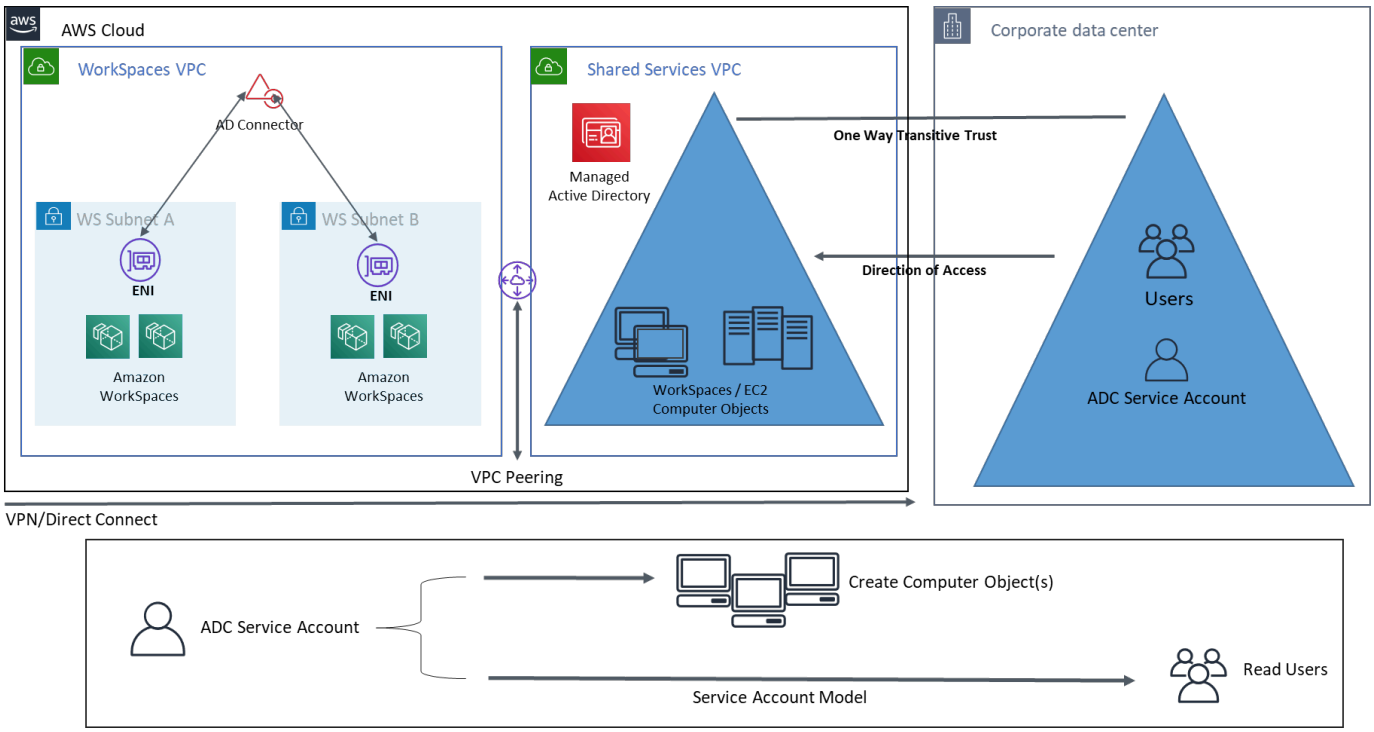

Figura 11: AWS Microsoft, VPC de serviços compartilhados e uma confiança unidirecional no AD local

Essa arquitetura usa os seguintes componentes ou construções:

AWS

- Amazon VPC — Criação de uma Amazon VPC com pelo menos duas sub-redes privadas em duas AZs — duas para AD Connector e. WorkSpaces
- Conjunto de opções DHCP — Criação de um conjunto de opções DHCP da Amazon VPC. Isso permite que um cliente defina um nome de domínio e DNS especificados (Microsoft AD). Para obter mais informações, consulte Conjuntos de opções de DHCP.

- Opcional: Amazon virtual private gateway — Habilite a comunicação com uma rede de propriedade do cliente por meio de um túnel VPN IPsec (VPN) ou conexão. AWS Direct Connect Use para acessar sistemas de back-end locais.
- AWS Directory Service — Microsoft AD implantado em um par dedicado de sub-redes VPC (AD DS Managed Service), AD Connector.
- Transit Gateway/VPC Peering — Habilite a conectividade entre o Workspaces VPC e o Shared Services VPC.
- Amazon EC2 — Servidores RADIUS “opcionais” do cliente para MFA.
- Amazon WorkSpaces — WorkSpaces são implantados nas mesmas sub-redes privadas do AD Connector. Para obter mais informações, consulte a seção Active Directory: Sites e Serviços deste documento.

Cliente

- Conectividade de rede — VPN corporativa ou AWS Direct Connect endpoints.
- Dispositivos de usuário final — dispositivos corporativos ou BYOL para usuários finais (como Windows, Macs, iPads, tablets Android, zero clients e Chromebooks) usados para acessar o serviço da Amazon. WorkSpaces Consulte esta lista de aplicativos cliente para dispositivos e navegadores da Web compatíveis.

Usando o Active Directory AWS gerenciado em várias regiões com a Amazon WorkSpaces

AWS O Directory Service for Microsoft Active Directory (MAD) é um Microsoft Active Directory (AD) totalmente gerenciado que pode ser emparelhado com a Amazon WorkSpaces. Os clientes escolhem o AWS Managed Microsoft AD porque ele tem alta disponibilidade, monitoramento e backups integrados. AWS A edição gerenciada do Microsoft AD Enterprise adiciona a capacidade de configurar a replicação multirregional. Esse recurso configura automaticamente a conectividade de rede entre regiões, implanta controladores de domínio e replica todos os dados do Active Directory em várias regiões, garantindo que as cargas de trabalho do Windows e do Linux residentes nessas regiões possam se conectar e usar o AWS MAD com baixa latência e alto desempenho. As regiões MAD replicadas não podem ser registradas diretamente WorkSpaces, mas um diretório MAD replicado pode ser registrado WorkSpaces configurando um AD Connector (ADC) para apontar para seus controladores de domínio replicados.

A melhor prática ao implantar AD Connectors com MAD é criar um AD Connector para cada unidade de negócios em seu WorkSpaces ambiente. Isso permitirá que você alinhe cada unidade de negócios com uma unidade organizacional específica no Active Directory. Em seguida, você pode atribuir Objetos de Política de Grupo do AD no nível da Unidade Organizacional que se alinhem diretamente com a unidade de negócios em questão.

Arquitetura

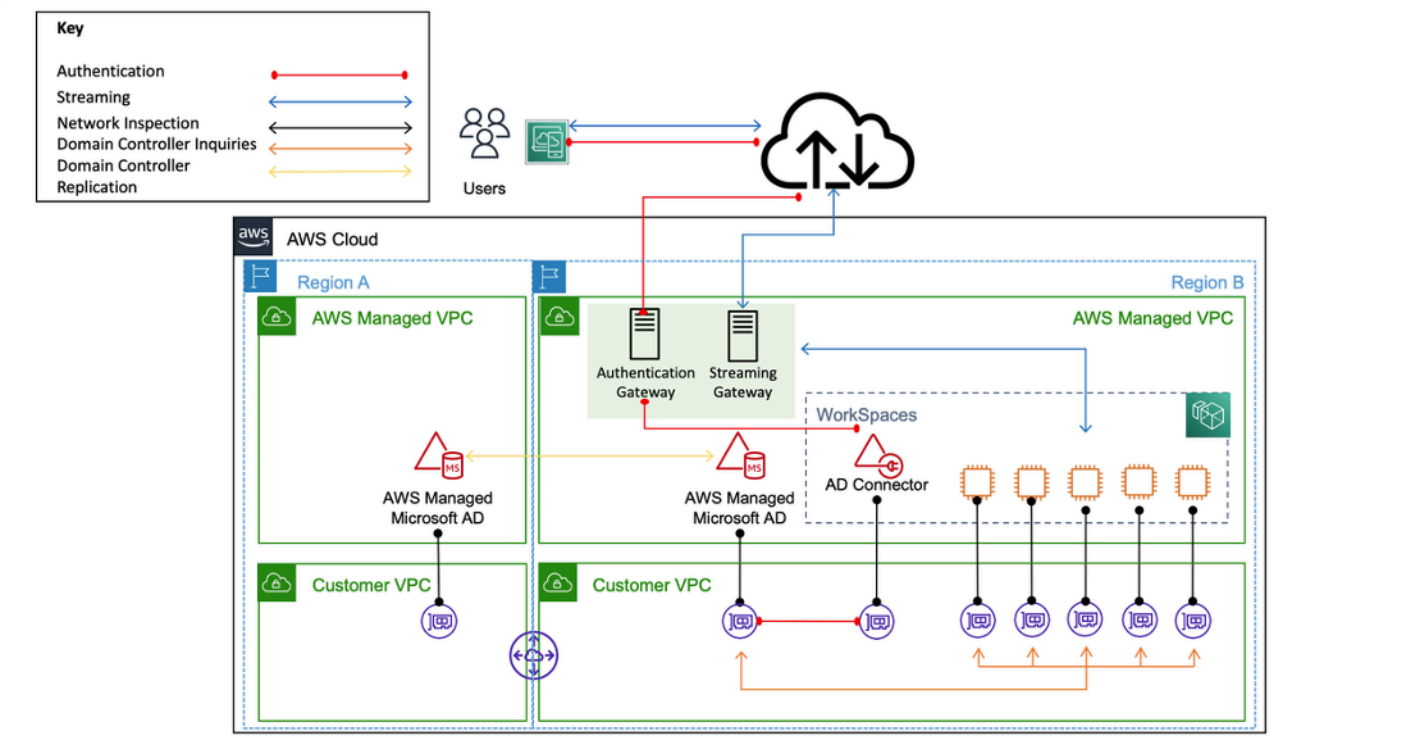

Figura 12: Exemplo de arquitetura para registrar uma região MAD replicada em um WorkSpace

Implementação

Para registrar sua região MAD replicada em WorkSpaces, você precisará criar um AD Connector apontado para seus IPs do controlador de domínio MAD. Você pode encontrar os endereços IP do controlador de domínio MAD acessando o painel de navegação do console do AWS Directory Service, selecionando Diretórios e escolhendo a ID de diretório correta. Para criar esses conectores AD, siga este guia. Depois de criados, você pode registrá-los no WorkSpaces. Antes de implantar WorkSpaces em sua nova região, certifique-se de ter atualizado o conjunto de opções DHCP de sua VPC.

Considerações sobre design

Uma implantação funcional do AD DS na AWS nuvem exige uma boa compreensão dos conceitos e AWS serviços específicos do Active Directory. Esta seção discute as principais considerações de design ao implantar o AD DS para Amazon, as melhores práticas de WorkSpaces VPC para AWS Directory Service, requisitos de DHCP e DNS, especificações do AD Connector e sites e serviços do AD.

Design em VPC

Conforme discutido anteriormente na seção Considerações de rede deste documento e documentado anteriormente para os cenários 2 e 3, os clientes devem implantar o AD DS na AWS nuvem em um par dedicado de sub-redes privadas, em duas AZs e separadas do AD Connector ou sub-redes. WorkSpaces Essa construção fornece acesso altamente disponível e de baixa latência aos serviços do AD DS WorkSpaces, mantendo as melhores práticas padrão de separação de funções ou funções na Amazon VPC.

A figura a seguir mostra a separação do AD DS e do AD Connector em sub-redes privadas dedicadas (cenário 3). Neste exemplo, todos os serviços residem na mesma Amazon VPC.

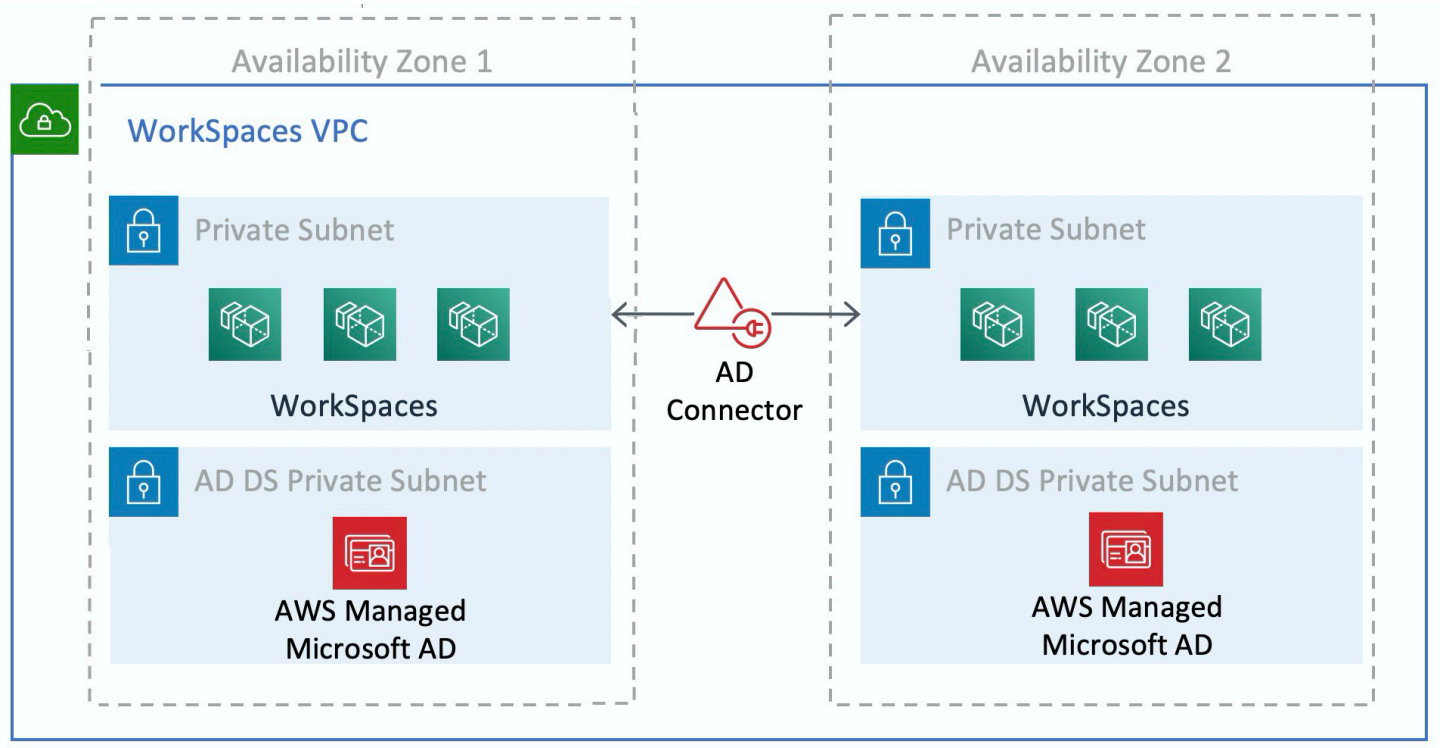

Figura 13: Separação de rede do AD DS

A figura a seguir mostra um design semelhante ao cenário 1; no entanto, nesse cenário, a parte local reside em uma Amazon VPC dedicada.

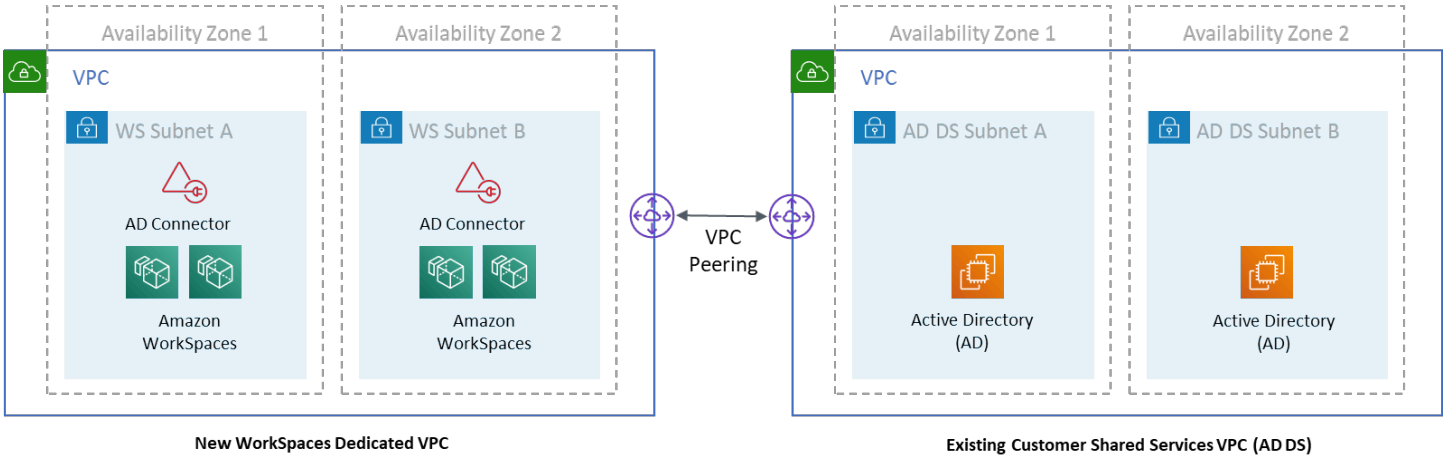

Figura 14: WorkSpaces VPC dedicada

> **Note**
>
> Para clientes que já têm uma AWS implantação em que o AD DS está sendo usado, é recomendável que eles a WorkSpaces localizem em uma VPC dedicada e usem o emparelhamento de VPC para comunicações do AD DS.

Além da criação de sub-redes privadas dedicadas para o AD DS, os controladores de domínio e os servidores membros exigem várias regras do Grupo de Segurança para permitir tráfego para serviços, como replicação do AD DS, autenticação de usuário, serviços do Windows Time e sistema de arquivos distribuído (DFS).

> **Note**
>
> A melhor prática é restringir as regras de grupo de segurança necessárias às sub-redes WorkSpaces privadas e, no caso do cenário 2, permitir comunicações bidirecionais do AD DS no local de e para a AWS nuvem, conforme mostrado na tabela a seguir.

Tabela 1 — Comunicações bidirecionais do AD DS de e para a nuvem AWS

Protocolo	Port	Use	Destino
TCP	53, 88, 135, 139, 389, 445, 464, 636	Autenticação (primária)	Active Directory (data center privado ou Amazon EC2) *
TCP	49152 — 65535	Portas altas de RPC	Active Directory (data center privado ou Amazon EC2) **
TCP	3268-3269	Confiança	Active Directory (data center privado ou Amazon EC2) *
TCP	9389	Microsoft Windows remoto PowerShell (opcional)	Active Directory (data center privado ou Amazon EC2) *
UDP	53, 88, 123, 137, 138, 389, 445, 464	Autenticação (primária)	Active Directory (data center privado ou Amazon EC2) *
UDP	1812	Autenticação (MFA) (opcional)	RADIUS (data center privado ou Amazon EC2) *

Para obter mais informações, consulte Requisitos de porta do Active Directory e dos Serviços de Domínio Active Directory e visão geral do serviço e requisitos de porta de rede para Windows

Para step-by-step obter orientação sobre a implementação de regras, consulte Adicionar regras a um grupo de segurança no Guia do usuário do Amazon Elastic Compute Cloud.

Design de VPC: DHCP e DNS

Com uma Amazon VPC, os serviços do Dynamic Host Configuration Protocol (DHCP) são fornecidos por padrão para suas instâncias. Por padrão, cada VPC fornece um servidor interno do Sistema de Nomes de Domínio (DNS) que pode ser acessado por meio do espaço de endereço Classless Inter-

Domain Routing (CIDR) +2 e é atribuído a todas as instâncias por meio de um conjunto de opções DHCP padrão.

Os conjuntos de opções de DHCP são usados em uma Amazon VPC para definir opções de escopo, como o nome de domínio ou os servidores de nomes que devem ser entregues às instâncias do cliente via DHCP. A funcionalidade correta dos serviços do Windows em uma VPC do cliente depende dessa opção de escopo de DHCP. Em cada um dos cenários definidos anteriormente, os clientes criam e atribuem seu próprio escopo que define o nome de domínio e os servidores de nomes. Isso garante que as instâncias do Windows associadas ao domínio WorkSpaces estejam configuradas para usar o AD DNS.

A tabela a seguir é um exemplo de um conjunto personalizado de opções de escopo DHCP que devem ser criadas para que a Amazon WorkSpaces e o AWS Directory Services funcionem corretamente.

Tabela 2 — Conjunto personalizado de opções de escopo DHCP

Parâmetro	Valor
Name tag	Cria uma tag com chave = nome e valor definidos para uma string específica Exemplo: example.com
Nome de domínio	exemplo.com
Servidores de nomes de domínio	Endereço do servidor DNS, separado por vírgulas Exemplo: 192.0.2.10, 192.0.2.21
Servidores NTP	Deixe esse campo em branco
Servidores de nomes NetBIOS	Insira os mesmos IPs separados por vírgula de acordo com os servidores de nomes de domínio Exemplo: 192.0.2.10, 192.0.2.21
Tipo de nó NetBIOS	2

Para obter detalhes sobre como criar um conjunto de opções DHCP personalizado e associá-lo a uma Amazon VPC, consulte Como trabalhar com conjuntos de opções de DHCP no Guia do usuário da Amazon Virtual Private Cloud.

No cenário 1, o escopo do DHCP seria o DNS local ou o AD DS. No entanto, nos cenários 2 ou 3, esse seria o serviço de diretório implantado localmente (AD DS no Amazon EC2 AWS ou Directory Services: Microsoft AD). É recomendável que cada controlador de domínio que resida na AWS nuvem seja um catálogo global e um servidor DNS integrado ao diretório.

Active Directory: sites e serviços

Para o Cenário 2, sites e serviços são componentes essenciais para o funcionamento correto do AD DS. A topologia do site controla a replicação do AD entre controladores de domínio dentro do mesmo site e entre os limites do site. No cenário 2, pelo menos dois sites estão presentes: no local e a Amazon WorkSpaces na nuvem.

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

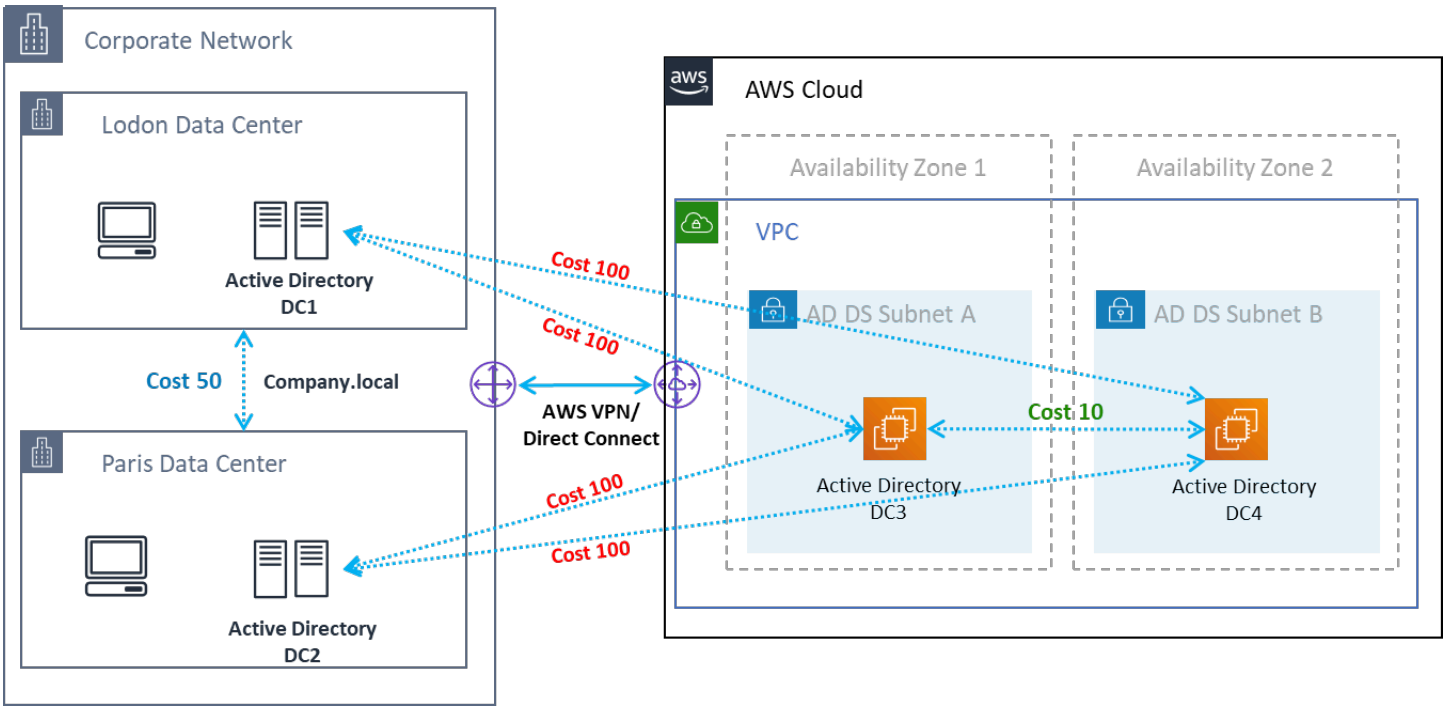

Figura 15: Sites e serviços do Active Directory: afinidade com o cliente

Prática recomendada: defina o alto custo dos links de sites entre o AD DS local e a AWS nuvem. A figura a seguir é um exemplo de quais custos atribuir aos links do site (custo 100) para garantir a afinidade com o cliente independente do site.

Essas associações ajudam a garantir que o tráfego, como a replicação do AD DS e a autenticação do cliente, use o caminho mais eficiente para um controlador de domínio. No caso dos cenários 2 e 3, isso ajuda a garantir menor latência e tráfego de links cruzados.

Protocolo

O Amazon WorkSpaces Streaming Protocol (WSP) é um protocolo de streaming nativo da nuvem que permite uma experiência de usuário consistente em distâncias globais e redes não confiáveis. O WSP separa o protocolo do WorkSpaces descarregando a análise métrica, a codificação, o uso e a seleção do codec. O WSP usa a porta TCP/UDP 4195. Ao decidir se usar ou não o protocolo WSP, há várias perguntas importantes que devem ser respondidas antes da implantação. Consulte a matriz de decisão abaixo:

Pergunta	VESPA	PCoIP
Os WorkSpaces usuários identificados precisarão de áudio/vídeo bidirecional?	•	
Zero clientes serão usados como endpoint remoto (dispositivo local)?		•
O Windows ou o macOS serão usados como endpoint remoto?	•	•
O Ubuntu 18.04 será usado para endpoint remoto?		•
Os usuários acessarão a Amazon WorkSpaces via acesso à web?		•

Pergunta	VESPA	PCoIP
É necessário suporte para cartões inteligentes (PIC/CAC) antes da sessão ou durante a sessão?	•	
WorkSpaces Será usado na região da China (Ningxia)?		•
A pré-autenticação do cartão inteligente ou o suporte durante a sessão serão necessários?	•	
Os usuários finais estão usando conexões não confiáveis, de alta latência ou baixa largura de banda?	•	

As perguntas anteriores são fundamentais para determinar o protocolo que deve ser usado. Informações adicionais sobre os casos de uso de protocolos recomendados podem ser revisadas aqui. O protocolo usado também pode ser alterado posteriormente usando o recurso Amazon WorkSpaces Migrate. Mais informações sobre o uso desse recurso podem ser revisadas aqui.

Ao implantar WorkSpaces usando o WSP, os Gateways WSP devem ser adicionados a uma lista de permissões para garantir a conectividade com o serviço. Além disso, para usuários que se conectam a um WorkSpaces usando WSP, o tempo de ida e volta (RTT) deve ser inferior a 250 ms para melhor desempenho. As conexões com um RTT entre 250 ms e 400 ms serão degradadas. Se a conexão do usuário estiver constantemente degradada, é recomendável implantar uma Amazon WorkSpaces em uma região com suporte de serviços mais próxima do usuário final, se possível.

Autenticação multifator (MFA)

A implementação do MFA exige WorkSpaces que a Amazon seja configurada com um Active Directory Connector (AD Connector) ou Managed AWS Microsoft AD (MAD) como seu Directory

Service e tenha um servidor RADIUS acessível em rede pelo Directory Service. O Simple Active Directory não oferece suporte ao MFA.

Consulte a seção anterior, abordando as considerações sobre a implantação do Active Directory e dos Serviços de Diretório para as opções de design do AD e do RADIUS em cada cenário.

MFA — Autenticação de dois fatores

Depois que a MFA for ativada, os usuários deverão fornecer seu nome de usuário, senha e código de MFA ao WorkSpaces cliente para autenticação em seus respectivos desktops. WorkSpaces

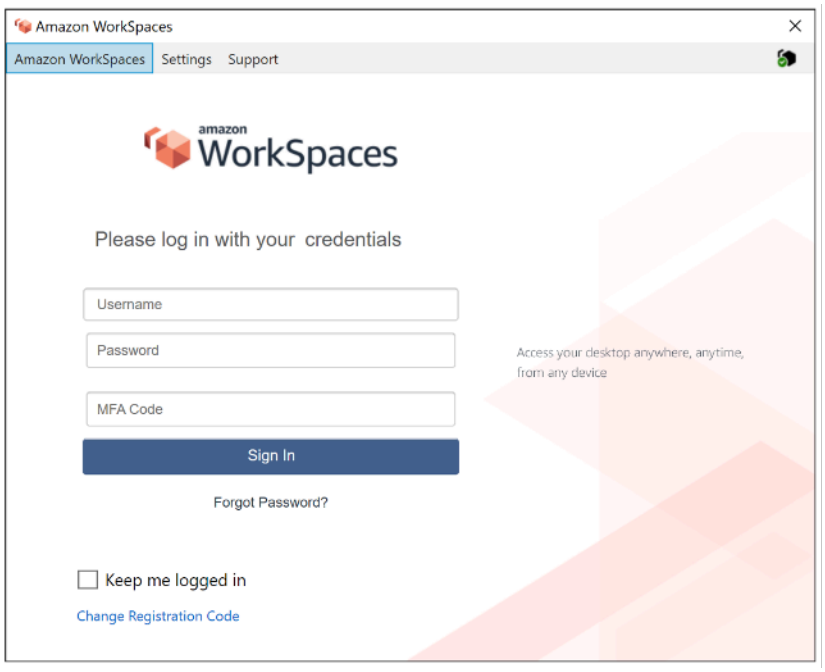

Figura 16: WorkSpaces cliente com MFA habilitado

> **Note**
>
> O AWS Directory Service não oferece suporte à MFA seletiva por usuário ou contextual: essa é uma configuração global por diretório. Se a MFA seletiva “por usuário” for necessária, os usuários deverão ser separados por um AD Connector, que pode apontar para a mesma origem do Active Directory.

WorkSpaces O MFA requer um ou mais servidores RADIUS. Normalmente, essas são soluções existentes que você já pode ter implantado, por exemplo, RSA ou Gemalto. Como alternativa, os servidores RADIUS podem ser implantados em sua VPC em instâncias EC2 (consulte a seção

Cenários de implantação do AD DS deste documento para ver as opções de arquitetura). Se você estiver implantando uma nova solução RADIUS, existem várias implementações, como o FreeRADIUS, junto com ofertas de SaaS, como Duo Security ou Okta MFA.

É uma prática recomendada utilizar vários servidores RADIUS para garantir que sua solução seja resistente a falhas. Ao configurar seu Directory Service para MFA, você pode inserir vários endereços IP separando-os com uma vírgula (por exemplo, 192.0.0.0,192.0.0.12). O recurso MFA dos Serviços de Diretório tentará o primeiro endereço IP especificado e passará para o segundo endereço IP caso a conectividade de rede não possa ser estabelecida com o primeiro. A configuração do RADIUS para uma arquitetura de alta disponibilidade é exclusiva para cada conjunto de soluções, no entanto, a recomendação geral é colocar as instâncias subjacentes do seu recurso RADIUS em diferentes zonas de disponibilidade. Um exemplo de configuração é o Duo Security e, para o Okta MFA, você pode implantar vários agentes do servidor Okta RADIUS da mesma maneira.

Para obter etapas detalhadas para habilitar seu AWS Directory Service para MFA, consulte AD Connector e Managed AWS Microsoft AD.

Recuperação de desastres/ Continuidade de negócios

WorkSpaces Redirecionamento entre regiões

A Amazon WorkSpaces é um serviço regional que fornece acesso remoto ao desktop aos clientes. Dependendo dos requisitos de continuidade de negócios e recuperação de desastres (BC/DR), alguns clientes exigem um failover contínuo para outra região em que o serviço esteja disponível. WorkSpaces Esse requisito de BC/DR pode ser cumprido usando a opção de redirecionamento WorkSpaces entre regiões. Ele permite que os clientes usem um nome de domínio totalmente qualificado (FQDN) como código de WorkSpaces registro.

Uma consideração importante é determinar em que ponto um redirecionamento para uma região de failover deve ocorrer. Os critérios para essa decisão devem ser baseados na política da sua empresa, mas devem incluir o Objetivo de Tempo de Recuperação (RTO) e o Objetivo de Ponto de Recuperação (RPO). Um projeto de WorkSpaces arquitetura Well-Architected deve incluir o potencial de falha no serviço. A tolerância de tempo para a recuperação normal das operações comerciais também influenciará a decisão.

Quando seus usuários finais fazem login WorkSpaces com um FQDN como código de registro, um WorkSpaces registro DNS TXT é resolvido contendo um identificador de conexão que determina o diretório registrado para o qual o usuário será direcionado. A página inicial de login do WorkSpaces

cliente será então apresentada com base no diretório registrado associado ao identificador de conexão retornado. Isso permite que os administradores direcionem seus usuários finais para diferentes WorkSpaces diretórios com base em suas políticas de DNS para o FQDN. Essa opção pode ser usada com zonas DNS públicas ou privadas, supondo que as zonas privadas possam ser resolvidas na máquina cliente. O redirecionamento entre regiões pode ser manual ou automatizado. Esses dois failovers podem ser obtidos alterando o registro TXT contendo o identificador de conexão a ser apontado para o diretório desejado.

Ao desenvolver sua estratégia de BC/DR, é importante considerar os dados do usuário, pois a opção de redirecionamento WorkSpaces entre regiões não sincroniza nenhum dado do usuário nem sincroniza suas imagens. WorkSpaces Suas WorkSpaces implantações em diferentes AWS regiões são entidades independentes. Portanto, você precisará tomar medidas adicionais para garantir que seus WorkSpaces usuários possam acessar seus dados quando ocorrer um redirecionamento para uma região secundária. Há muitas opções disponíveis para replicação de dados do usuário WorkSpaces, como o Windows FSx (DFS Share) ou utilitários de terceiros para sincronizar volumes de dados entre regiões. Da mesma forma, você precisará garantir que sua região secundária tenha acesso às WorkSpaces imagens necessárias, por exemplo, copiando as imagens entre regiões. Para obter mais informações, consulte Redirecionamento entre regiões da Amazon WorkSpaces no Guia de WorkSpaces Administração da Amazon e o exemplo no diagrama.

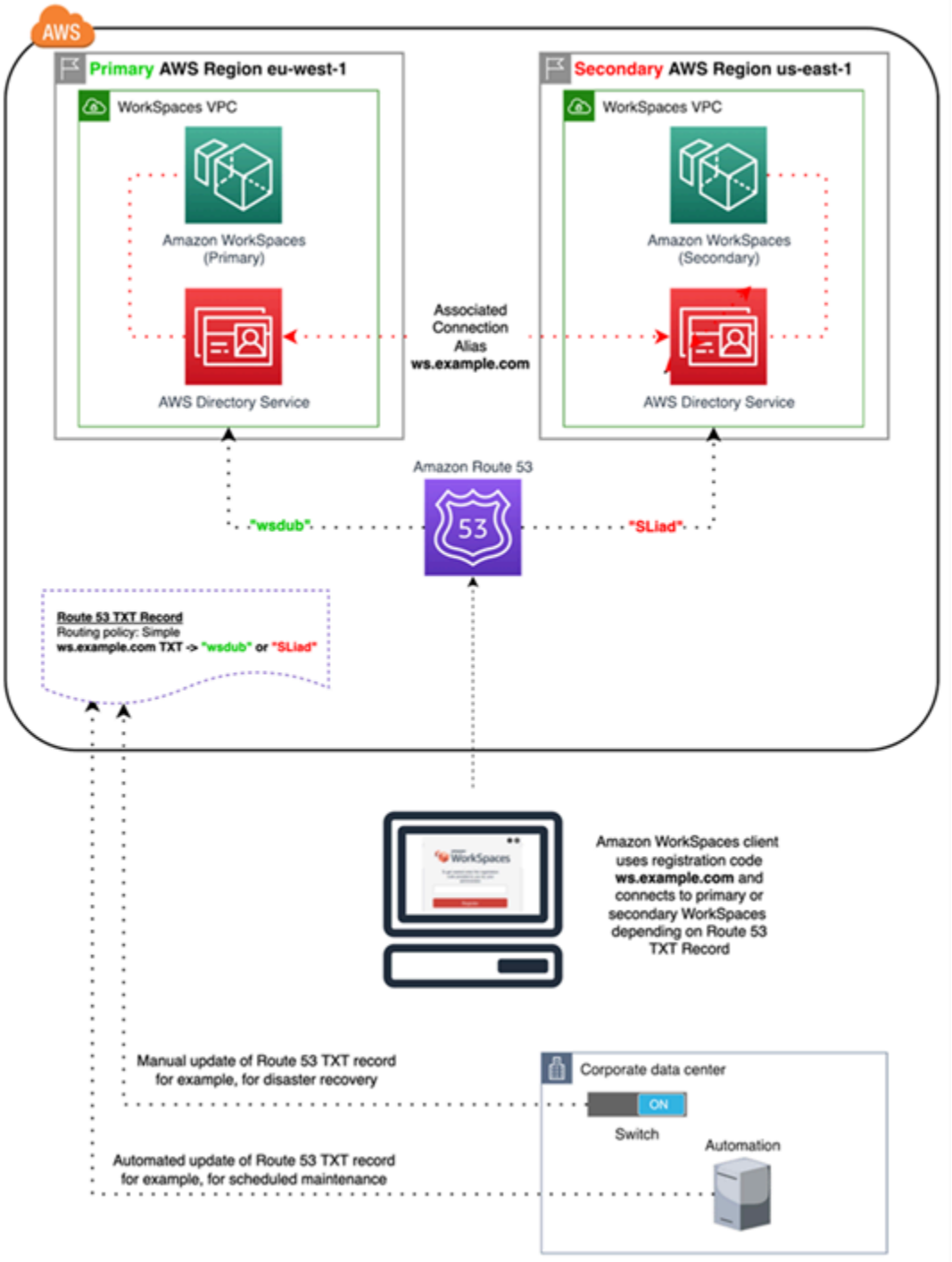

Figura 17: Exemplo de WorkSpaces redirecionamento entre regiões com o Amazon Route 53

WorkSpaces Interface VPC Endpoint (AWS PrivateLink) — Chamadas de API

As APIs WorkSpaces públicas da Amazon são suportadas no. AWS PrivateLink AWS PrivateLink aumenta a segurança dos dados compartilhados com aplicativos baseados em nuvem, reduzindo a exposição dos dados à Internet pública. WorkSpaces O tráfego de API pode ser protegido dentro de uma VPC usando um endpoint de interface, que é uma interface de rede elástica com um endereço IP privado do intervalo de endereços IP da sua sub-rede que serve como ponto de entrada para o tráfego destinado a um serviço compatível. Isso permite que você acesse de forma privada os serviços de WorkSpaces API usando endereços IP privados.

O uso PrivateLink com APIs WorkSpaces públicas também permite que você exponha com segurança as APIs REST aos recursos somente dentro da sua VPC ou àqueles conectados aos seus data centers via. AWS Direct Connect

Você pode restringir o acesso a Amazon VPCs e VPC Endpoints selecionados e habilitar o acesso entre contas usando políticas específicas de recursos.

Certifique-se de que o grupo de segurança associado à interface de rede do endpoint permita a comunicação entre a interface da rede do endpoint e os recursos em sua VPC que se comunicam com o serviço. Se o grupo de segurança restringir o tráfego HTTPS de entrada (porta 443) de recursos na VPC, talvez você não consiga enviar tráfego pela interface de rede do endpoint. Um endpoint de interface é compatível somente com tráfego TCP.

- Endpoints são compatíveis somente com tráfego de IPv4.
- Ao criar um endpoint, você pode anexar uma política de endpoint a ele para controlar o acesso ao serviço ao qual está se conectando.
- Você tem uma cota para o número de endpoints criados por você por VPC.
- Os endpoints são compatíveis somente na mesma região. Você não pode criar um endpoint entre uma VPC e um serviço em uma região diferente.

Criar notificação para receber alertas sobre eventos de endpoint de interface — Você pode criar uma notificação para receber alertas de eventos específicos que ocorrem em seu endpoint de interface. Para criar uma notificação, é preciso associar um tópico do Amazon SNS a ela. Você pode se inscrever no tópico do SNS para receber uma notificação por e-mail quando ocorrer um evento do endpoint.

Crie uma política de endpoint de VPC para a Amazon WorkSpaces — Você pode criar uma política para endpoints de VPC da Amazon para a Amazon WorkSpaces para especificar o seguinte:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

Conecte sua rede privada à sua VPC — Para chamar a WorkSpaces API da Amazon por meio de sua VPC, você precisa se conectar a partir de uma instância que esteja dentro da VPC ou conectar sua rede privada à sua VPC usando uma Amazon Virtual Private Network (VPN) ou. AWS Direct Connect Para obter informações sobre o Amazon VPN, consulte as conexões VPN no Guia do usuário da Amazon Virtual Private Cloud. Para obter informações sobre AWS Direct Connect, consulte Criar uma conexão no Guia do AWS Direct Connect usuário.

Para obter mais informações sobre o uso da WorkSpaces API da Amazon por meio de um endpoint de interface VPC, consulte Segurança de infraestrutura na Amazon. WorkSpaces

Suporte ao cartão inteligente

O suporte a cartões inteligentes está disponível para Microsoft Windows e Amazon Linux WorkSpaces. O suporte a cartões inteligentes por meio do Common Access Card (CAC) e da Verificação de Identidade Pessoal (PIV) está disponível exclusivamente na Amazon WorkSpaces usando o WorkSpaces Streaming Protocol (WSP). O suporte a cartões inteligentes no WSP WorkSpaces oferece uma postura de segurança aprimorada para autenticar usuários em terminais de conexão aprovados pela organização com hardware específico na forma de leitores de cartões inteligentes. É importante primeiro se familiarizar com o escopo de suporte disponível para cartões inteligentes e determinar como os cartões inteligentes funcionariam em WorkSpaces implantações existentes e futuras.

É uma prática recomendada determinar qual tipo de suporte de cartão inteligente é necessário, autenticação pré-sessão ou autenticação em sessão. A autenticação pré-sessão só está disponível no momento da redação deste artigo em AWS GovCloud (Oeste dos EUA), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Europa (Irlanda), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Sydney). A autenticação por cartão inteligente em sessão geralmente está disponível com algumas considerações, como:

- Sua organização possui uma infraestrutura de cartão inteligente integrada ao seu Windows Active Directory?

- Seu respondente do Online Certificate Status Protocol (OCSP) está acessível publicamente pela Internet?
- Os certificados de usuário são emitidos com o nome principal do usuário (UPN) no campo Nome alternativo do assunto (SAN)?
- Mais considerações são detalhadas para as seções em sessão e pré-sessão.

O suporte a cartões inteligentes é habilitado por meio da Política de Grupo. É uma prática recomendada adicionar o modelo administrativo da Política de WorkSpaces Grupo da Amazon para o WSP ao Armazenamento Central do seu domínio do Active Directory usado pelo Amazon WorkSpaces Directory (s). Ao aplicar essa política a uma WorkSpaces implantação existente da Amazon, todos WorkSpaces exigirão a atualização da política de grupo e uma reinicialização para que a alteração entre em vigor para todos os usuários, pois é uma política baseada em computador.

CA raiz

A natureza da portabilidade do WorkSpaces cliente e do usuário da Amazon exige a exigência de entregar remotamente um certificado de CA raiz de terceiros ao armazenamento confiável de certificados raiz de cada dispositivo que os usuários usam para se conectar à Amazon. WorkSpaces Os controladores de domínio do AD e os dispositivos de usuário com cartões inteligentes devem confiar nas CAs raiz. Consulte as diretrizes fornecidas pela Microsoft para habilitar CAs de terceiros para obter mais informações sobre os requisitos exatos.

Em ambientes associados a um domínio do AD, esses dispositivos atendem a esse requisito por meio da Política de Grupo que distribui certificados de CA raiz. Em cenários em que o Amazon WorkSpaces Client é usado a partir de non-domain-joined dispositivos, um método de entrega alternativo para as CAs raiz de terceiros deve ser determinado, como o Intune.

Em sessão

A autenticação na sessão simplifica e protege a autenticação do aplicativo após o início das sessões de WorkSpaces usuário da Amazon. Conforme mencionado anteriormente, o comportamento padrão da Amazon WorkSpaces desativa os cartões inteligentes e deve ser ativado por meio da Política de Grupo. Do ponto de vista da WorkSpaces administração da Amazon, a configuração é especificamente necessária para aplicativos que passam pela autenticação (como navegadores da web). Nenhuma alteração é necessária para os conectores e diretórios do AD.

Os aplicativos mais comuns que exigem suporte à autenticação em sessão são por meio de navegadores da Web, como o Mozilla Firefox e o Google Chrome. O Mozilla Firefox requer configuração limitada para suporte a cartões inteligentes em sessão. O Amazon Linux WSP WorkSpaces exige configuração adicional para suporte a cartões inteligentes em sessão para o Mozilla Firefox e o Google Chrome.

É uma prática recomendada garantir que as CAs raiz sejam carregadas no armazenamento de certificados pessoais do usuário antes da solução de problemas, pois o Amazon WorkSpaces Client pode não ter permissões para o computador local. Além disso, use o OpenSC para identificar dispositivos de cartão inteligente ao solucionar qualquer suspeita de problemas de autenticação na sessão com cartões inteligentes. Por fim, um Respondente do Online Certificate Status Protocol (OCSP) é recomendado para melhorar a postura de segurança da autenticação do aplicativo por meio de uma verificação de revogação de certificado.

Pré-sessão

O suporte para autenticação pré-sessão requer Windows WorkSpaces Client versão 3.1.1 e posterior, ou WorkSpaces cliente macOS versão 3.1.5 e posterior. A autenticação pré-sessão com cartões inteligentes é fundamentalmente diferente da autenticação padrão, exigindo que o usuário se autentique por meio de uma combinação da inserção do cartão inteligente e da inserção de um código PIN. Com esse tipo de autenticação, a duração das sessões do usuário é limitada pela vida útil do ticket Kerberos. Um guia de instalação completo pode ser encontrado aqui.

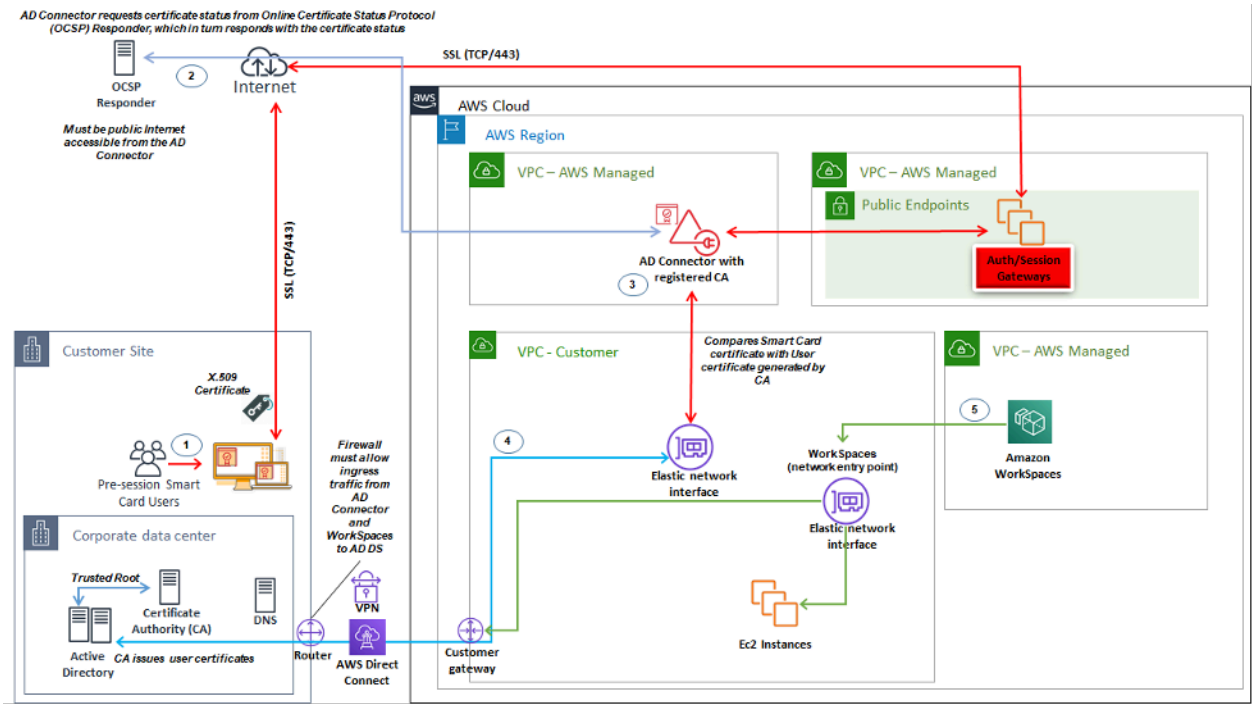

Figura 18: Visão geral da autenticação pré-sessão

1. O usuário abre o Amazon WorkSpaces Client, insere o cartão inteligente e insere seu PIN. O PIN é usado pelo Amazon WorkSpaces Client para descriptografar o certificado X.509, que é enviado por proxy para o AD Connector por meio do Authentication Gateway.
2. O AD Connector valida o Certificado X.509 em relação ao URL do Respondente OCSP acessível ao público especificado nas Configurações do Diretório para garantir que o certificado não tenha sido revogado.
3. Se o certificado for válido, o Amazon WorkSpaces Client continuará o processo de autenticação solicitando que o usuário insira seu PIN pela segunda vez para descriptografar o certificado X.509 e o proxy para o AD Connector, onde ele é então combinado com os certificados raiz e intermediário do AD Connector para validação.
4. Depois que a validação do certificado é correspondida com êxito, o Active Directory é usado pelo AD Connector para autenticar o usuário e um tíquete Kerberos é criado.
5. O tíquete Kerberos é passado para a Amazon do usuário WorkSpace para autenticar e iniciar a sessão do WSP.

O Respondente OCSP deve estar acessível publicamente, pois a conexão é realizada pela rede AWS gerenciada e não pela rede gerenciada pelo cliente, portanto, não há roteamento para redes privadas nesta etapa.

Não é necessário inserir o nome do usuário, pois os certificados de usuário apresentados ao AD Connector incluem o userPrincipalName (UPN) do usuário no campo subjectAltName (SAN) do certificado. É uma prática recomendada automatizar todos os usuários que precisam de autenticação pré-sessão com Smartcards e ter seus objetos de usuário do AD atualizados para se autenticarem com o UPN previsto no certificado usando PowerShell, em vez de realizar isso individualmente nos Consoles de Gerenciamento Microsoft.

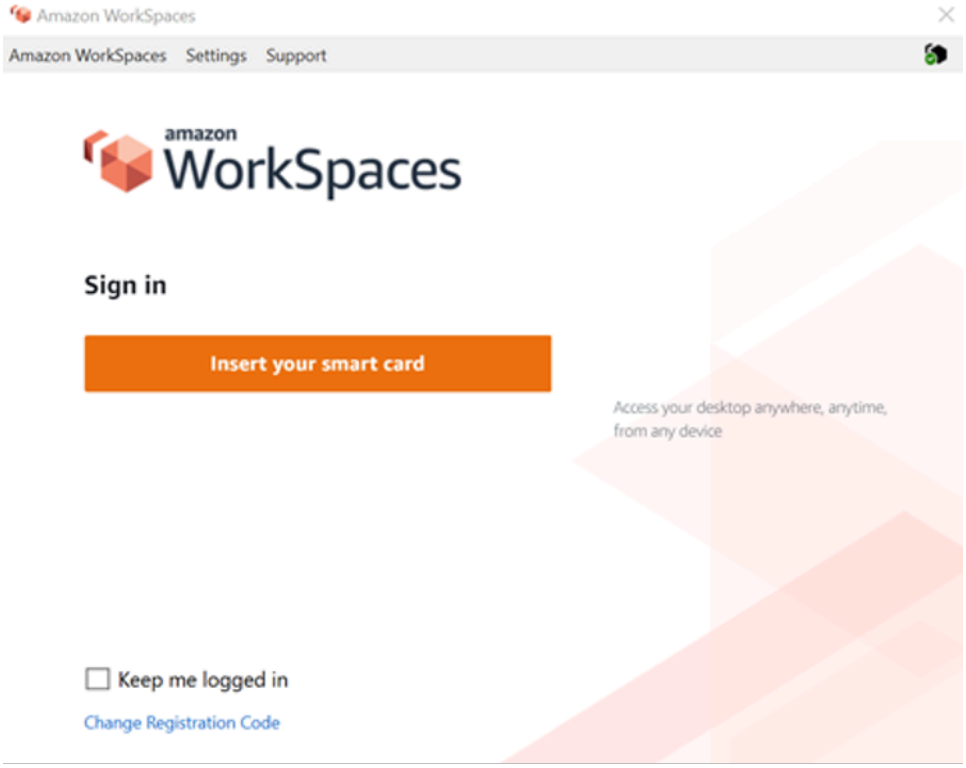

Figura 19: console de WorkSpaces login

Implantação do cliente

O Amazon WorkSpaces Client (versão 3.X+) usa arquivos de configuração padronizados que podem ser aproveitados pelos administradores para pré-configurar o cliente do usuário. WorkSpaces O caminho para os dois arquivos de configuração principais pode ser encontrado em:

SO	Caminho do arquivo de configuração
Windows	C:\Users\USERNAME\AppData\ Local\ Amazon Web Services\ Amazon WorkSpaces
macOS	/Usuários/Nome de usuário/Biblioteca/Suporte de aplicativos/Amazon Web Services/Amazon WorkSpaces
Linux (Ubuntu 18.04)	/home/ubuntu/.local/share/Amazon Web Services/Amazon/ WorkSpaces

Dentro desses caminhos, você encontrará os dois arquivos de configuração. O primeiro arquivo de configuração é UserSettings .json, que definirá coisas como registro atual, configuração de proxy, nível de registro e a capacidade de salvar a lista de registro. O segundo arquivo de configuração é RegistrationList .json. Esse arquivo conterá todas as informações do WorkSpaces diretório para o cliente usar para mapear para o WorkSpaces diretório correto. A pré-configuração do RegistrationList .json preencherá todos os códigos de registro do cliente para o usuário.

> **Note**
>
> Se seus usuários estiverem executando a versão 2.5.11 do WorkSpaces Client, o proxy.cfg será usado para as configurações de proxy do cliente e o client_settings.ini definirá o nível do log, bem como a capacidade de salvar a lista de registro. A configuração padrão do proxy usará o que está definido no sistema operacional.

Como esses arquivos são padronizados, os administradores podem baixar o WorkSpaces Cliente, definir todas as configurações aplicáveis e, em seguida, enviar os mesmos arquivos de configuração para todos os usuários finais. Para que as configurações entrem em vigor, o cliente deve ser iniciado após a definição das novas configurações. Se você alterar a configuração enquanto o cliente estiver em execução, nenhuma das alterações será definida no cliente.

A última configuração que pode ser definida para WorkSpaces os usuários é a atualização automática do Windows Client. Isso não é controlado por meio de arquivos de configuração, mas sim pelo Registro do Windows. Quando uma nova versão do cliente for lançada, você poderá criar uma chave de registro para ignorar essa versão. Isso pode ser definido criando uma string de nomes de entrada de registro SkipThisVersion com um valor do número completo da versão no caminho abaixo: Computer\ HKEY_CURRENT_USER\ Software\ Amazon Web Services. LLC\ Amazon WorkSpaces\ WinSparkle Essa opção também está disponível para macOS; no entanto, a configuração está dentro de um arquivo plist que requer software especial para edição. Se você ainda quiser realizar essa ação, isso pode ser feito adicionando uma SkippedVersion entrada SU no domínio com.amazon.workspaces localizado em: /Users/username/Library/Preferences

Seleção de WorkSpaces endpoints da Amazon

Escolhendo um endpoint para seu WorkSpaces

WorkSpaces A Amazon oferece suporte para vários dispositivos de endpoint, desde desktops Windows até iPads e Chromebooks. Você pode baixar os WorkSpaces clientes da Amazon

disponíveis no site do Amazon Workspaces. Escolher o endpoint certo para seus usuários é uma decisão importante. Se seus usuários precisarem do uso de áudio/vídeo bidirecional e estiverem utilizando o protocolo de WorkSpaces streaming, eles deverão usar o cliente Windows ou macOS. Para todos os clientes, certifique-se de que os endereços IP e portas listados nos Requisitos de Endereço IP e Porta da Amazon WorkSpaces tenham sido configurados explicitamente para garantir que o cliente possa se conectar ao serviço. Aqui estão algumas considerações adicionais para ajudá-lo a escolher um dispositivo de endpoint:

- Windows — Para utilizar o cliente Windows Amazon, o WorkSpaces cliente 4.x deve executar o desktop Microsoft Windows 8.1, Windows 10 de 64 bits necessário. Os usuários podem instalar o cliente apenas para seu perfil de usuário sem privilégios administrativos na máquina local. Os administradores do sistema podem implantar o cliente em endpoints gerenciados com a Política de Grupo, o Microsoft Endpoint Manager Configuration Manager (MEMCM) ou outras ferramentas de implantação de aplicativos usadas em um ambiente. O cliente Windows suporta no máximo quatro monitores e uma resolução máxima de 3840x2160.
- macOS — Para implantar o cliente macOS Amazon mais recente WorkSpaces , os dispositivos macOS devem executar o macOS 10.12 (Sierra) ou posterior. Você pode implantar uma versão mais antiga do WorkSpaces cliente para se conectar ao PCoIP WorkSpaces se o endpoint estiver executando o OSX 10.8.1 ou posterior. O cliente macOS suporta até dois monitores com resolução 4K ou quatro monitores com resolução WUXGA (1920 x 1200).
- Linux — O cliente Amazon WorkSpaces Linux requer o Ubuntu 18.04 (AMD64) de 64 bits para ser executado. Se seus endpoints Linux não executarem essa versão do sistema operacional, o cliente Linux não será suportado. Antes de implantar clientes Linux ou fornecer aos usuários seu código de registro, certifique-se de habilitar o acesso ao cliente Linux no nível do WorkSpaces diretório, pois isso está desabilitado por padrão e os usuários não poderão se conectar a partir de clientes Linux até que seja habilitado. O cliente Linux suporta até dois monitores com resolução 4K ou quatro monitores com resolução WUXGA (1920 x 1200).
- iPad — O aplicativo cliente Amazon WorkSpaces iPad é compatível com PCoIP WorkSpaces. Os iPads compatíveis são o iPad2 ou posterior com iOS 8.0 ou posterior, iPad Retina com iOS 8.0 e posterior, iPad Mini com iOS 8.0 e posterior e iPad Pro com iOS 9.0 e posterior. Certifique-se de que o dispositivo a partir do qual os usuários se conectarão atenda a esses critérios. O aplicativo cliente para iPad suporta muitos gestos diferentes. (Consulte uma lista completa dos gestos compatíveis.) O aplicativo cliente Amazon WorkSpaces iPad também oferece suporte aos mouses Swiftpoint GT e PadPoint . ProPoint O Swiftpoint TRACPOINT PenPoint e os GoPoint mouses não são suportados.

- Android/Chromebook — Ao implantar um dispositivo Android ou Chromebook como endpoint para seus usuários finais, há algumas considerações que devem ser levadas em consideração. Certifique-se de que WorkSpaces os usuários se conectarão sejam PCoIP WorkSpaces, pois esse cliente suporta apenas PCoIP. WorkSpaces Esse cliente suporta apenas um único monitor. Se os usuários precisarem de suporte para vários monitores, utilize um endpoint diferente. Se você quiser implantar um Chromebook, certifique-se de que o modelo implantado seja compatível com a instalação de aplicativos Android. O suporte completo a recursos é suportado somente no cliente Android, e não no cliente antigo do Chromebook. Normalmente, isso é apenas uma consideração para Chromebooks feitos antes de 2019. O suporte para Android é fornecido para tablets e telefones, desde que o Android esteja executando o OS 4.4 e posterior. No entanto, é recomendável que o dispositivo Android execute o OS 9 ou superior para utilizar o cliente WorkSpace Android mais recente. Se seus Chromebooks estiverem executando a versão 3.0.1 ou superior do WorkSpaces cliente, seus usuários agora podem aproveitar os recursos de autoatendimento. WorkSpaces Além disso, como administrador, você pode utilizar certificados de dispositivos confiáveis para restringir o WorkSpaces acesso a dispositivos confiáveis com certificados válidos.
- Acesso à Web — Os usuários podem acessar o Windows WorkSpaces de qualquer local usando um navegador da Web. Isso é ideal para usuários que precisam usar um dispositivo bloqueado ou uma rede restritiva. Em vez de usar uma solução de acesso remoto tradicional e instalar a aplicação cliente apropriada, os usuários podem visitar o site e acessar seus recursos de trabalho. Os usuários podem utilizar o WorkSpaces Web Access para se conectar ao non-graphics-based Windows PCoIP WorkSpaces executando o Windows 10 ou o Windows Server 2016 com o Desktop Experience. Os usuários devem se conectar usando o Chrome 53 ou posterior ou o Firefox 49 ou posterior. Para sistemas baseados em WSP WorkSpaces, os usuários podem utilizar o WorkSpaces Web Access para se conectar a sistemas gráficos não baseados em Windows. WorkSpaces Esses usuários devem se conectar usando o Microsoft Edge 91 ou posterior ou o Google Chrome 91 ou posterior. A resolução mínima de tela suportada é 960 x 720 com uma resolução máxima suportada de 2560 x 1600. Não há suporte para vários monitores. Para a melhor experiência do usuário, quando possível, é recomendável que os usuários usem uma versão do sistema operacional do cliente.
- PCoIP Zero Client — Você pode implantar clientes zero PCoIP para usuários finais que tenham ou terão WorkSpaces PCoIP atribuído a eles. O cliente zero Tera2 deve ter uma versão de firmware 6.0.0 ou posterior para se conectar diretamente ao. WorkSpace Para usar a autenticação multifator com a Amazon WorkSpaces, o dispositivo zero client Tera2 deve executar a versão 6.0.0 ou posterior do firmware. O suporte e a solução de problemas do hardware de cliente zero devem ser feitos com o fabricante.

- IGEL OS — Você pode utilizar o sistema operacional IGEL em dispositivos terminais para se conectar ao PCoIP, WorkSpaces desde que a versão do firmware seja 11.04.280 ou superior. Os recursos suportados correspondem aos do cliente Linux existente atualmente. Antes de implantar clientes do sistema operacional IGEL ou fornecer aos usuários seu código de registro, certifique-se de habilitar o acesso do cliente Linux no nível do WorkSpaces diretório, pois isso está desativado por padrão e os usuários não poderão se conectar a partir dos clientes do sistema operacional IGEL até que ele seja ativado. O cliente LGel OS suporta até dois monitores com resolução 4K ou quatro monitores com resolução WUXGA (1920x1200).

Cliente de acesso à Web

Projetado para dispositivos bloqueados, o cliente Web Access fornece acesso à Amazon WorkSpaces sem a necessidade de implantar software cliente. O cliente Web Access é recomendado somente em configurações em que a Amazon WorkSpaces é do sistema operacional Windows (OS) e é usado para fluxos de trabalho de usuários limitados, como um ambiente de quiosque. A maioria dos casos de uso se beneficia do conjunto de recursos disponível no WorkSpaces cliente da Amazon. O cliente do Web Access só é recomendado em casos de uso específicos em que dispositivos e restrições de rede exigem um método de conexão alternativo.

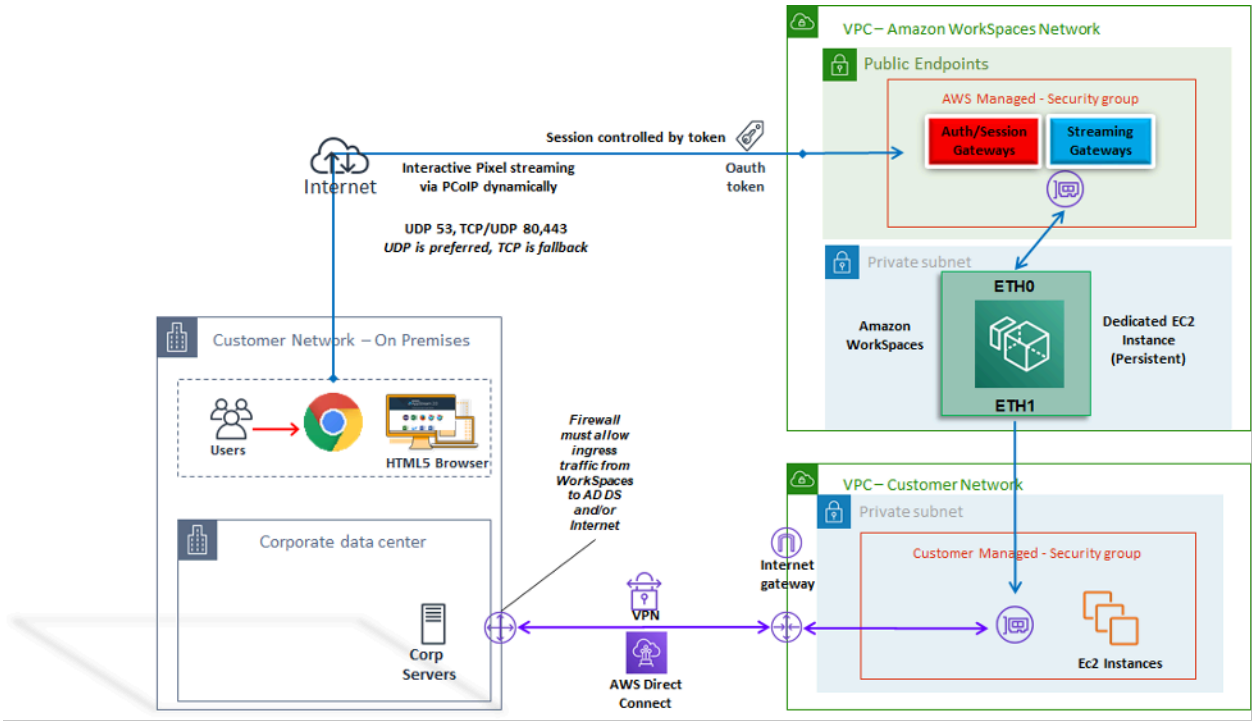

Figura 20: Arquitetura do cliente de acesso à Web

Conforme mostrado no diagrama, o cliente do Web Access tem requisitos de rede diferentes para transmitir a sessão aos usuários. O Web Access está disponível para Windows WorkSpaces usando o protocolo PCoIP ou WSP. DNS e HTTP/HTTPS são necessários para autenticação e registro nos gateways. WorkSpaces Para WorkSpaces usar o protocolo WSP, é necessário que a conexão direta do UDP/TCP 4195 seja aberta aos intervalos de endereços IP do WSP Gateway. O tráfego de streaming não é alocado para uma porta fixa, como acontece com o WorkSpaces cliente Amazon completo; em vez disso, é alocado dinamicamente. O UDP é preferível para tráfego de streaming; no entanto, o navegador retornará ao TCP quando o UDP for restrito. Em ambientes em que a porta TCP/UDP 4172 está bloqueada e não pode ser desbloqueada devido a restrições organizacionais, o cliente do Web Access fornece um método de conexão alternativo para os usuários.

Por padrão, o cliente do Web Access está desativado no nível do Diretório. Para permitir que os usuários acessem sua Amazon WorkSpaces por meio de um navegador da web, use o AWS Management Console para atualizar as configurações do diretório ou use programaticamente a WorkspaceAccessProperties API para modificar DeviceTypeWeb para Permitir. Além disso, o administrador deve garantir que as configurações da Política de Grupo não entrem em conflito com os requisitos de login.

WorkSpaces Etiquetas da Amazon

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

Tag restrictions
```

- Número máximo de tags por recurso: 50
- Comprimento máximo da chave: 127 caracteres Unicode
- Comprimento máximo de valor: 255 caracteres Unicode
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas. Os caracteres permitidos são letras, espaços e números representáveis em UTF-8, além dos seguintes caracteres especiais: + - = . _ : / @. Não use espaços no início nem no fim.
- Não use os prefixos aws: ou aws:workspaces: nos nomes ou valores de suas tags porque eles estão reservados para uso. AWS Não é possível editar nem excluir nomes ou valores de tag com esses prefixos.

Recursos que você pode marcar

- Você pode adicionar tags aos seguintes recursos ao criá-los: imagens WorkSpaces importadas e grupos de controle de acesso IP.
- Você pode adicionar tags aos recursos existentes dos seguintes tipos: diretórios registrados WorkSpaces, pacotes personalizados, imagens e grupos de controle de acesso IP.

  Usando a tag de alocação de custos

Para visualizar suas tags de WorkSpaces recursos no Cost Explorer, ative as tags que você aplicou aos seus WorkSpaces recursos seguindo as instruções em Ativando Tags de Alocação de Custos Definidas pelo Usuário no Guia do Usuário do AWS Billing and Cost Management Cost Management.

Embora as tags apareçam 24 horas após a ativação, pode levar de quatro a cinco dias para que os valores associados a essas tags apareçam no Cost Explorer, apareçam e forneçam dados de custo no Cost Explorer. Os WorkSpaces recursos que foram marcados devem ser cobrados durante esse período. O Cost Explorer mostra somente os dados de custo do momento em que as tags foram ativadas posteriormente. Não há dados de histórico disponíveis no momento.

Como gerenciar tags

Para atualizar as tags de um recurso existente usando o AWS CLI, use os comandos create-tags e delete-tags. Para atualizações em massa e para automatizar a tarefa em um grande número de WorkSpaces recursos, a Amazon WorkSpaces adiciona suporte ao Editor de AWS Resource Groups tags. AWS Resource Groups O Editor de tags permite que você adicione, edite ou exclua AWS tags do seu WorkSpaces junto com seus outros AWS recursos.

Cotas WorkSpaces de serviços da Amazon

As Cotas de Serviço facilitam a pesquisa do valor de uma cota específica, também chamada de limite. Você também pode pesquisar todas as cotas de um serviço específico.

Para ver suas cotas para WorkSpaces

1. Navegue até o console Service Quotas.
2. No painel de navegação à esquerda, escolha serviços. AWS
3. Selecione Amazon na WorkSpaces lista ou insira Amazon WorkSpaces no campo de pesquisa de digitação antecipada.

4. Para ver informações adicionais sobre uma cota, como sua descrição e Amazon Resource Name (ARN), escolha o nome da cota.

WorkSpaces A Amazon fornece diferentes recursos que você pode usar em sua conta em uma determinada região, incluindo imagens WorkSpaces, pacotes, diretórios, aliases de conexão e grupos de controle de IP. Quando você cria sua conta da Amazon Web Services, as cotas padrão são definidas (também chamadas de limites) no número de recursos que você pode criar.

Você pode usar o console de Cotas de Serviço para visualizar as Cotas de Serviço padrão ou solicitar aumentos de cotas para cotas ajustáveis.

Para obter mais informações, consulte Como visualizar cotas de serviço e Solicitar um aumento de cota no Guia do usuário de cotas de serviço.

Automatizando a implantação da Amazon WorkSpaces

Com a Amazon WorkSpaces, você pode iniciar um desktop Microsoft Windows ou Amazon Linux em minutos, conectar-se e acessar seu software de desktop no local ou em uma rede externa de forma segura, confiável e rápida. Você pode automatizar o provisionamento da Amazon WorkSpaces para permitir que você integre a Amazon aos seus fluxos de trabalho de provisionamento existentes. WorkSpaces

Métodos comuns WorkSpaces de automação

Os clientes podem usar várias ferramentas para permitir a rápida WorkSpaces implantação da Amazon. As ferramentas podem ser usadas para simplificar o gerenciamento WorkSpaces, reduzir custos e possibilitar um ambiente ágil que pode ser expandido e movido rapidamente.

AWS CLI e API

Existem operações de WorkSpaces API da Amazon que você pode usar para interagir com o serviço de forma segura e em grande escala. Todas as APIs públicas estão disponíveis com o AWS CLI SDK e o Tools for PowerShell, enquanto as APIs privadas, como a criação de imagens, estão disponíveis somente por meio do. AWS Management Console Ao considerar o gerenciamento operacional e o autoatendimento comercial para a Amazon WorkSpaces, considere que as WorkSpaces APIs exigem conhecimento técnico e permissões de segurança para serem usadas.

As chamadas de API podem ser feitas usando o AWS SDK. AWS O Tools for Windows PowerShell e o AWS Tools for PowerShell Core são PowerShell módulos criados com base na funcionalidade exposta pelo AWS SDK for .NET. Esses módulos permitem que você crie scripts de operações em AWS recursos a partir da linha de PowerShell comando e se integre às ferramentas e serviços existentes. Por exemplo, as chamadas de API podem permitir que você gerencie automaticamente o WorkSpaces ciclo de vida por meio da integração com o AD para provisionar e descomissionar com WorkSpaces base na associação de um usuário ao grupo AD.

AWS CloudFormation

AWS CloudFormation permite que você modele toda a sua infraestrutura em um arquivo de texto. Esse modelo se torna a única fonte confiável para sua infraestrutura. Isso ajuda você a padronizar os componentes de infraestrutura usados em toda a sua organização, permitindo a conformidade da configuração e a solução de problemas mais rápida.

AWS CloudFormation provisiona seus recursos de forma segura e reproduzível, permitindo que você crie e reconstrua sua infraestrutura e seus aplicativos. Você pode usar CloudFormation para comissionar e descomissionar ambientes, o que é útil quando você tem várias contas que deseja criar e descomissionar de forma repetível. Ao considerar o gerenciamento operacional e o autoatendimento comercial para a Amazon WorkSpaces, considere que isso AWS CloudFormationrequer conhecimento técnico e permissões de segurança para uso.

Portal de autoatendimento WorkSpaces

Os clientes podem usar comandos de WorkSpaces API de compilação e outros AWS serviços para criar um portal de WorkSpaces autoatendimento. Isso ajuda os clientes a simplificar o processo de implantação e recuperação em grande escala. WorkSpaces Usando um WorkSpaces portal, você pode permitir que sua força de trabalho provisione sua própria força de trabalho WorkSpaces com um fluxo de trabalho de aprovação integrado que não exija intervenção de TI para cada solicitação. Isso reduz os custos operacionais de TI, ao mesmo tempo em que ajuda os usuários finais a começar a trabalhar com WorkSpaces mais rapidez. O fluxo de trabalho adicional de aprovação integrado simplifica o processo de aprovação por desktop para empresas. Um portal dedicado pode oferecer uma ferramenta automatizada para provisionar desktops em nuvem Windows ou Linux e permitir que os usuários os reconstruam, reiniciem ou migrem WorkSpace, além de fornecer um recurso para redefinições de senha.

Há exemplos guiados de criação de WorkSpaces portais de autoatendimento mencionados na seção Leitura adicional deste documento. AWS Os parceiros fornecem portais WorkSpaces de gerenciamento pré-configurados por meio do. AWS Marketplace

Integração com o gerenciamento de serviços de TI corporativos

À medida que as empresas adotam a Amazon WorkSpaces como sua solução de desktop virtual em grande escala, é necessário implementar ou integrar sistemas de gerenciamento de serviços de TI (ITSM). A integração do ITSM permite ofertas de autoatendimento para provisionamento e operações. O Service Catalog permite que você gerencie AWS serviços comumente implantados e produtos de software provisionados de forma centralizada. Esse serviço ajuda sua organização a alcançar requisitos consistentes de governança e conformidade, ao mesmo tempo em que permite que os usuários implantem somente os AWS serviços aprovados de que precisam. O Service Catalog pode ser usado para permitir uma oferta de gerenciamento de ciclo de vida de autoatendimento para a WorkSpaces Amazon a partir de ferramentas de gerenciamento de serviços de TI, como. ServiceNow

WorkSpaces Melhores práticas de automação de implantação

Você deve considerar os princípios da Well Architected para selecionar e projetar a automação WorkSpaces de implantação.

- Design para automação — Projete para fornecer a menor intervenção manual possível no processo para permitir repetibilidade e escala.
- Design para otimização de custos — Ao criar e recuperar automaticamente WorkSpaces, você pode reduzir o esforço administrativo necessário para fornecer recursos e evitar que recursos ociosos ou não utilizados gerem custos desnecessários.
- Design para eficiência — Minimize os recursos necessários para criar e finalizar. WorkSpaces Sempre que possível, forneça recursos de autoatendimento de nível 0 para que a empresa melhore a eficiência.
- Design para flexibilidade — Crie um mecanismo de implantação consistente que possa lidar com vários cenários e escalar com o mesmo mecanismo (personalizado usando identificadores marcados de caso de uso e perfil).
- Design para produtividade — Projete suas WorkSpaces operações para permitir a autorização e a validação corretas para adicionar ou remover recursos.
- Design para escalabilidade — O modelo pay-as-you go que a Amazon WorkSpaces usa pode gerar economia de custos criando recursos conforme necessário e removendo-os quando não forem mais necessários.
- Design para segurança — Projete suas WorkSpaces operações para permitir a autorização e a validação corretas para adicionar ou remover recursos.

- Design para suporte — Projete suas WorkSpaces operações para permitir mecanismos e processos de suporte e recuperação não invasivos.

WorkSpaces Patches e atualizações locais da Amazon

Com a Amazon WorkSpaces, você pode gerenciar patches e atualizações usando ferramentas de terceiros existentes, como o Microsoft System Center Configuration Manager (SCCM), o Puppet Enterprise ou o Ansible. A implantação local de patches de segurança normalmente mantém um ciclo mensal de patches, com processos adicionais para escalonamento ou implantação rápida. No entanto, no caso de atualizações de sistema operacional ou de recursos no local, muitas vezes são necessárias considerações especiais.

WorkSpace manutenção

A Amazon WorkSpaces tem uma janela de manutenção padrão durante a qual WorkSpace instala as atualizações do WorkSpaces agente Amazon e todas as atualizações disponíveis do sistema operacional. WorkSpaces não estarão disponíveis para as conexões do usuário durante a janela de manutenção programada.

- AlwaysOn WorkSpaces a janela de manutenção padrão é das 00h00 às 04h00, no fuso horário do WorkSpace, todos os domingos de manhã.

- O redirecionamento de fuso horário é ativado por padrão e pode substituir a janela padrão para corresponder ao fuso horário local do usuário.
- Você pode desativar o redirecionamento de fuso horário para Windows WorkSpaces usando a Política de Grupo. Você pode desativar o redirecionamento de fuso horário para Linux WorkSpaces usando a configuração do PCoIP Agent.

- AutoStop WorkSpaces são iniciados automaticamente uma vez por mês para instalar atualizações importantes. A partir da terceira segunda-feira do mês e por até duas semanas, a janela de manutenção está aberta todos os dias, das 00h00 às 05h00, no fuso horário da AWS Região para o. WorkSpace Eles WorkSpace podem ser mantidos em qualquer dia na janela de manutenção.

- Embora você não possa modificar o fuso horário usado para manutenção AutoStop WorkSpaces, você pode desativar a janela de manutenção do seu AutoStop WorkSpaces.

- As janelas de manutenção manual podem ser definidas com base em sua programação preferida, definindo o estado do WorkSpace como ADMIN_MAINTENANCE.

- O AWS CLI comando modify-workspace-statepode ser usado para modificar o WorkSpace estado para ADMIN_MAINTENANCE.

Amazon Linux WorkSpaces

Para considerações, pré-requisitos e padrões sugeridos para gerenciar atualizações e patches em imagens WorkSpaces personalizadas do Amazon Linux, consulte o whitepaper Best Practices to Prepare your Amazon for Linux Images. WorkSpaces

Pré-requisitos e considerações sobre a aplicação de patches no Linux

- Os repositórios do Amazon Linux são hospedados em buckets do Amazon Simple Storage Service (Amazon S3), que podem ser acessados por meio de endpoints públicos acessíveis pela Internet ou endpoints privados. Se o seu Amazon Linux WorkSpaces não tiver acesso à Internet, consulte este processo para tornar as atualizações acessíveis: Como posso atualizar o yum ou instalar pacotes sem acesso à Internet em minhas instâncias EC2 executando o Amazon Linux 1 ou o Amazon Linux 2?
- Você não pode configurar a janela de manutenção padrão para Linux WorkSpaces. Se a personalização dessa janela for necessária, o processo de manutenção manual poderá ser utilizado.

Aplicação de patches no Amazon Windows

Por padrão, seu Windows WorkSpaces está configurado para receber atualizações do Windows Update que exigem acesso à Internet de sua WorkSpaces VPC. Para configurar seus próprios mecanismos de atualização automática para o Windows, consulte a documentação do Windows Server Update Services (WSUS) e do Configuration Manager.

Atualização local do Amazon Windows

- Se você planeja criar uma imagem a partir de um Windows 10 WorkSpace, observe que a criação de imagens não é suportada em sistemas Windows 10 que foram atualizados de uma versão anterior (uma atualização de recurso/versão do Windows). No entanto, as atualizações

cumulativas ou de segurança do Windows são suportadas pelo processo de criação e captura de WorkSpaces imagens.

- As imagens personalizadas do Windows 10 Bring Your Own License (BYOL) devem começar com a versão mais recente suportada do Windows em uma VM como fonte para o processo de importação de BYOL: consulte a documentação de importação de BYOL para obter mais detalhes.

Pré-requisitos de atualização in-loco do Windows

- Se você adiou ou pausou as atualizações do Windows 10 usando a Política de Grupo do Active Directory ou o SCCM, habilite as atualizações do sistema operacional para o Windows 10. WorkSpaces
- Se WorkSpace for um AutoStop WorkSpace, altere o AutoStop horário para pelo menos três horas para acomodar a janela de upgrade.
- O processo de atualização in-loco recria o perfil do usuário fazendo uma cópia do Usuário padrão (C:\Users\Default). Não use o perfil de usuário padrão para fazer personalizações. Em vez disso, é recomendável fazer qualquer personalização no perfil do usuário por meio de Objetos de Política de Grupo (GPOs). As personalizações feitas por meio de GPOs podem ser facilmente modificadas ou revertidas e são menos propensas a erros.
- O processo de atualização no local pode fazer backup e recriar somente um perfil de usuário. Se você tiver vários perfis de usuário na unidade D, exclua todos os perfis, exceto aquele que você precisa.

Considerações sobre a atualização in-loco do Windows

- O processo de atualização in-loco usa dois scripts de registro (enable-inplace-upgrade.ps1 e update-pvdrivers.ps1) para fazer as alterações necessárias no seu e permitir que o processo do Windows Update seja executado. WorkSpaces Essas alterações envolvem a criação de um perfil de usuário temporário na unidade C em vez da unidade D. Se um perfil de usuário já existir na unidade D, os dados desse perfil de usuário original permanecerão na unidade D.
- Depois que a atualização in-loco for implantada, você deverá restaurar os perfis de usuário na unidade D para garantir que você possa reconstruir ou migrar sua WorkSpaces e para evitar possíveis problemas com o redirecionamento da pasta shell do usuário. Você pode fazer isso usando a chave de registro PostUpgradeRestoreProfileOnD, conforme explicado na página de referência de atualização do BYOL.

Pacotes de WorkSpaces idiomas da Amazon

WorkSpaces Os pacotes da Amazon que oferecem a experiência de desktop do Windows 10 oferecem suporte para inglês (EUA), francês (canadense), coreano e japonês. No entanto, você pode incluir pacotes de idiomas adicionais para espanhol, italiano, português e muitas outras opções de idiomas. Para obter mais informações, consulte Como faço para criar uma nova WorkSpace imagem do Windows com um idioma de cliente diferente do inglês? .

Gerenciamento de WorkSpaces perfil da Amazon

A Amazon WorkSpaces separa o perfil do usuário do sistema operacional (OS) básico redirecionando todas as gravações do perfil para um volume separado do Amazon Elastic Block Store (Amazon EBS). No Microsoft Windows, o perfil do usuário é armazenado em D:\Users \username. No Amazon Linux, o perfil do usuário é armazenado em /home. O volume do EBS é capturado automaticamente a cada 12 horas. O snapshot é armazenado automaticamente em um bucket AWS gerenciado do S3, para ser usado no caso de uma Amazon ser reconstruída ou WorkSpace restaurada.

Para a maioria das organizações, ter instantâneos automáticos a cada 12 horas é superior à implantação de desktop existente, sem backups para perfis de usuário. No entanto, os clientes podem exigir um controle mais granular sobre os perfis de usuário; por exemplo, migração do desktop para WorkSpaces um novo sistema AWS operacional/região, suporte para DR e assim por diante. Existem métodos alternativos para gerenciamento de perfis disponíveis para a Amazon WorkSpaces.

Redirecionamento de pasta

Embora o redirecionamento de pastas seja uma consideração de design comum nas arquiteturas de infraestrutura de desktop virtual (VDI), não é uma prática recomendada nem mesmo um requisito comum nos projetos da Amazon. WorkSpaces A razão para isso é que a Amazon WorkSpaces é uma solução persistente de desktop como serviço (DaaS), com dados de aplicativos e usuários persistindo imediatamente.

Há cenários específicos em que o redirecionamento de pastas para pastas do shell do usuário (por exemplo, D:\Users\username\Desktop redirecionado para\\ Server\ RedirectionShare $\ username\ Desktop) é necessário, como objetivo de ponto de recuperação imediata (RPO) para dados de perfil de usuário em ambientes de recuperação de desastres (DR).

Práticas recomendadas

As práticas recomendadas a seguir estão listadas para um redirecionamento robusto de pastas:

- Hospede os servidores de arquivos do Windows na mesma AWS região e AZ em que a Amazon WorkSpaces é lançada.
- Certifique-se de que as regras de entrada do grupo de segurança do AD incluam o grupo de segurança do servidor de arquivos do Windows ou endereços IP privados; caso contrário, certifique-se de que o firewall local permita o mesmo tráfego baseado em portas TCP e UDP.
- Certifique-se de que as regras de entrada do grupo de segurança do Windows File Server incluam TCP 445 (SMB) para todos os grupos de segurança da Amazon. WorkSpaces
- Crie um grupo de segurança do AD para WorkSpaces usuários da Amazon para autorizar o acesso dos usuários ao Compartilhamento de arquivos do Windows.
- Use o Namespace DFS (DFS-N) e a Replicação DFS (DFS-R) para garantir que seu compartilhamento de arquivos do Windows seja ágil, não vinculado a nenhum servidor de arquivos específico do Windows, e que todos os dados do usuário sejam replicados automaticamente entre os servidores de arquivos do Windows.
- Anexe '$' ao final do nome do compartilhamento para ocultar o compartilhamento que hospeda os dados do usuário ao navegar pelos compartilhamentos de rede no Windows Explorer.
- Crie o compartilhamento de arquivos seguindo as orientações da Microsoft para pastas redirecionadas: Implantar redirecionamento de pastas com arquivos off-line. Siga atentamente as orientações sobre permissões de segurança e configuração de GPO.
- Se sua WorkSpaces implantação na Amazon for Bring Your Own License (BYOL), você também deverá especificar a desativação de arquivos off-line seguindo a orientação da Microsoft: Desativar arquivos off-line em pastas redirecionadas individuais.
- Instale e execute a desduplicação de dados (comumente chamada de “desduplicação”) se o Windows File Server for o Windows Server 2016 ou mais recente para reduzir o consumo de armazenamento e otimizar os custos. Consulte Instalar e ativar a desduplicação de dados e Executar a desduplicação de dados.
- Faça backup dos compartilhamentos de arquivos do Windows File Server usando as soluções de backup organizacional existentes.

Coisa a evitar

- Não use servidores de arquivos do Windows que sejam acessíveis somente por meio de uma conexão de rede de longa distância (WAN), pois o protocolo SMB não foi projetado para esse uso.
- Não use o mesmo compartilhamento de arquivos do Windows usado nos diretórios pessoais para reduzir as chances de os usuários excluírem acidentalmente suas pastas do User Shell.
- Embora a ativação do Volume Shadow Copy Service (VSS) seja recomendada para facilitar a restauração de arquivos, isso por si só não elimina a necessidade de fazer backup dos compartilhamentos de arquivos do Windows File Server.

Outras considerações

- O Amazon FSx for Windows File Server oferece um serviço gerenciado para compartilhamentos de arquivos do Windows e simplifica a sobrecarga operacional do redirecionamento de pastas, incluindo backups automáticos.
- Utilize AWS Storage Gateway o SMB File Share para fazer backup de seus compartilhamentos de arquivos se não houver uma solução de backup organizacional existente.

Configurações do perfil

Políticas de grupo

Uma prática recomendada comum em implantações corporativas do Microsoft Windows é definir as configurações do ambiente do usuário por meio das configurações de Objeto de Política de Grupo (GPO) e Preferências de Política de Grupo (GPP). Configurações como atalhos, mapeamentos de unidades, chaves do registro e impressoras são definidas por meio do Console de Gerenciamento de Política de Grupo. Os benefícios de definir o ambiente do usuário por meio de GPOs incluem, mas não estão limitados a:

- Gerenciamento centralizado de configurações
- Perfil de usuário definido pela associação ao grupo de segurança do AD ou pelo posicionamento da OU
- Proteção contra exclusão de configurações
- Automatize a criação e a personalização do perfil no primeiro login
- Facilidade de atualização futura

> **Note**
>
> Siga as melhores práticas da Microsoft para otimizar o desempenho da Política de Grupo.

As políticas de grupo de banners de login interativos não devem ser usadas, pois não são suportadas na Amazon. WorkSpaces Os banners são apresentados no Amazon WorkSpaces Client por meio de solicitações de AWS suporte. Além disso, dispositivos removíveis não devem ser bloqueados pela política de grupo, pois são necessários para a Amazon WorkSpaces.

Os GPOs podem ser usados para gerenciar o Windows WorkSpaces. Para obter mais informações, consulte Gerenciar seu Windows WorkSpaces.

WorkSpaces Volumes da Amazon

Cada WorkSpaces instância da Amazon contém dois volumes: um volume do sistema operacional e um volume do usuário.

- Amazon Windows WorkSpaces — A unidade C:\ é usada para o sistema operacional (OS) e a unidade D:\ é o volume do usuário. O perfil do usuário está localizado no volume do usuário (DocumentosAppData, Imagens, Downloads etc.).
- Amazon Linux WorkSpaces — Com um Amazon Linux WorkSpace, o volume do sistema (/dev/xvda1) é montado como a pasta raiz. O volume do usuário é para dados e aplicativos do usuário; /dev/xvdf1 é montado como /home.

Para volumes do sistema operacional, você pode selecionar um tamanho inicial para essa unidade de 80 GB ou 175 GB. Para volumes de usuários, você pode selecionar um tamanho inicial de 10 GB, 50 GB ou 100 GB. Ambos os volumes podem ser aumentados em até 2 TB conforme necessário; no entanto, para aumentar o volume do usuário além de 100 GB, o volume do sistema operacional deve ser 175 GB. As alterações de volume só podem ser realizadas uma vez a cada seis horas por volume. Para obter informações adicionais sobre como modificar o tamanho do WorkSpaces volume, consulte a WorkSpace seção Modificar a do Guia de Administração.

WorkSpaces melhores práticas de volumes

Ao planejar uma WorkSpaces implantação da Amazon, é recomendável considerar os requisitos mínimos para instalação do sistema operacional, atualizações no local e aplicativos principais

adicionais que serão adicionados à imagem no volume do sistema operacional. Para o volume do usuário, é recomendável começar com uma alocação de disco menor e aumentar gradativamente o tamanho do volume do usuário conforme necessário. Minimizar o tamanho dos volumes de disco reduz o custo de execução do WorkSpace.

> **Note**
>
> Embora o tamanho do volume possa ser aumentado, ele não pode ser diminuído.

WorkSpaces Registro na Amazon

Em um WorkSpaces ambiente Amazon, há muitas fontes de log que podem ser capturadas para solucionar problemas e monitorar o WorkSpaces desempenho geral.

Amazon WorkSpaces Client 3.x Em cada WorkSpaces cliente da Amazon, os registros do cliente estão localizados nos seguintes diretórios:

- Windows — %LOCALAPPDATA%\ Amazon Web Services\ Amazon\ logs WorkSpaces
- macOS — ~/Library/"Application Support" /"Amazon Web Services" /"Amazon "/logs WorkSpaces
- Linux (Ubuntu 18.04 ou posterior) — /opt/workspacesclient/workspacesclient

Há muitos casos em que detalhes de diagnóstico ou depuração podem ser necessários para uma WorkSpaces sessão do lado do cliente. Os registros avançados do cliente também podem ser habilitados adicionando um "-l3 "ao arquivo executável do espaço de trabalho. Por exemplo: .

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

WorkSpaces Serviço Amazon

O WorkSpaces serviço Amazon é integrado com Amazon CloudWatch Metrics, CloudWatch Events CloudTrail e. Essa integração permite que os dados de desempenho e as chamadas de API sejam registrados no AWS serviço central.

Ao gerenciar um WorkSpaces ambiente Amazon, é importante monitorar constantemente determinadas CloudWatch métricas para determinar o status geral da saúde do ambiente. Métricas

Embora existam outras CloudWatch métricas disponíveis para a Amazon WorkSpaces (consulte Monitore suas CloudWatch métricas de WorkSpaces uso), as três métricas a seguir ajudarão a manter a disponibilidade da WorkSpace instância:

- Insalubre — O número WorkSpaces que retornou um status insalubre.
- SessionLaunchTime— A quantidade de tempo necessária para iniciar uma WorkSpaces sessão.
- InSessionLatency— O tempo de ida e volta entre o WorkSpaces cliente e o. WorkSpace

Para obter mais informações sobre as opções de WorkSpaces registro, consulte Logging Amazon WorkSpaces API Calls by Using CloudTrail. Os CloudWatch eventos adicionais ajudarão a capturar o IP do lado do cliente da sessão do usuário, quando o usuário se conectou à WorkSpaces sessão e qual endpoint foi usado durante a conexão. Todos esses detalhes ajudam a isolar ou identificar problemas relatados pelo usuário durante as sessões de solução de problemas.

> **Note**
>
> Algumas CloudWatch métricas estão disponíveis somente com o AD AWS gerenciado.

Contêineres e subsistema Windows para Linux na Amazon WorkSpaces

Contêineres e Amazon WorkSpaces

A computação do usuário final geralmente é abordada por clientes que desejam atender cargas de trabalho de contêineres com a Amazon WorkSpaces. Embora possível, essa não é a solução preferida ou recomendada. Os clientes que desejam descobrir as possíveis economias operacionais e de custo dos contêineres são fortemente encorajados a avaliar o Amazon Elastic Container Service (Amazon ECS) e/ou o Amazon Elastic Kubernetes Service (Amazon EKS).

Nos casos em que os requisitos do cliente exigem a habilitação de contêineres usando a Amazon WorkSpaces, foi publicado um manual técnico que permite o uso do Docker. Os clientes devem ser informados de que isso requer outros serviços de rastreamento e que há custos e complexidade maiores quando comparados aos serviços de contêineres nativos e desacoplados.

Subsistema Windows para Linux

Com o lançamento do Windows Server 2019 como sistema operacional subjacente da Amazon WorkSpaces, os clientes estão ansiosos para implementar o Windows Subsystem for Linux (WSL), especificamente o WSL2. Como o WSL2 invoca uma máquina virtual (Hyper-V) para realizar suas funções, ele não pode ser executado na Amazon WorkSpaces, que é gerenciada por hipervisores. AWS Os clientes devem saber que somente o WSL1 estará disponível por esse motivo e compreender as diferenças entre o WSL1 e o WSL2.

Amazon WorkSpaces migra

O recurso Amazon WorkSpaces Migrate permite que você traga os dados de volume do usuário para um novo pacote. Você pode usar esse recurso para:

- Migre sua experiência WorkSpaces do Windows 7 para a experiência de desktop do Windows 10.
- Migre de um PCoIP WorkSpace para um protocolo de WorkSpaces streaming (WSP). WorkSpace
- Migre WorkSpaces de um pacote público ou personalizado para outro. Por exemplo, você pode migrar de pacotes habilitados para GPU (gráficos e GraphicsPro) para pacotes não habilitados para GPU e vice-versa.

Processo de migração

Com o WorkSpaces migrate, você pode especificar o WorkSpaces pacote de destino. O processo de migração recria o WorkSpace uso de um novo volume raiz da imagem do pacote de destino e o volume do usuário a partir do último instantâneo do volume original do usuário. Um novo perfil de usuário é gerado durante a migração para melhor compatibilidade. Os dados do seu perfil de usuário antigo que não podem ser movidos para o novo perfil são armazenados em uma pasta .NotMigrated.

Durante a migração, os dados no volume do usuário (unidade D) são preservados, mas todos os dados no volume raiz (unidade C:\) são perdidos. Isso significa que nenhum dos aplicativos instalados, configurações e alterações no registro são preservados. A pasta antiga do perfil do usuário é renomeada com o. NotMigrated sufixo e um novo perfil de usuário é criado.

O processo de migração leva até uma hora por WorkSpace. Além disso, se o fluxo de trabalho de migração falhar em concluir o processo, o serviço retornará automaticamente WorkSpace ao estado original antes da migração, minimizando qualquer risco de perda de dados.

Todas as etiquetas atribuídas ao original WorkSpace são transferidas durante a migração. O modo de execução do WorkSpace é preservado. O migrado WorkSpace tem um novo WorkSpace ID, nome do computador e endereço IP. Procedimento de migração

Você pode migrar WorkSpaces pelo WorkSpaces console da Amazon, AWS CLI usando o comando migrate-workspace ou a API da Amazon. WorkSpaces Todas as solicitações de migração ficam na fila, e o serviço reduzirá automaticamente o número total de solicitações de migração se houver muitas. Limites de migração

- Não é possível migrar para um pacote de experiência de desktop do Windows 7 público ou personalizado.
- Você não pode migrar para pacotes BYOL do Windows 7.
- Você pode migrar o BYOL WorkSpaces somente para outros pacotes BYOL.
- Você não pode migrar um pacote WorkSpace criado de pacotes públicos ou personalizados para um pacote BYOL.
- Atualmente, a migração do Linux não WorkSpaces é suportada.
- Em AWS regiões que oferecem suporte a mais de um idioma, você pode migrar WorkSpaces entre pacotes de idiomas.
- Os pacotes de origem e destino devem ser diferentes. (No entanto, em regiões que oferecem suporte a mais de um idioma, você pode migrar para o mesmo pacote do Windows 10, desde que os idiomas sejam diferentes.) Se você quiser atualizar seu WorkSpace usando o mesmo pacote, reconstrua o em vez disso. WorkSpace
- Você não pode migrar WorkSpaces entre regiões.
- WorkSpaces não podem ser migrados quando estão no modo ADMIN_MAINTENANCE.

Custos

Durante o mês em que a migração ocorre, são cobrados valores rateados tanto pelo novo quanto pelo original. WorkSpaces Por exemplo, se você migrar WorkSpace de A para WorkSpace B em 10 de maio, você será cobrado por WorkSpace A de 1º a 10 de maio e por WorkSpace B de 11 a 30 de maio.

WorkSpaces melhores práticas de migração

Antes de migrar um WorkSpace, faça o seguinte:

- Faça backup de todos os dados importantes na unidade C para outro local. Todos os dados na unidade C são apagados durante a migração.
- Certifique-se de que o que está WorkSpace sendo migrado tenha pelo menos 12 horas, para garantir que um instantâneo do volume do usuário tenha sido criado. Na WorkSpaces página Migrate no WorkSpaces console da Amazon, você pode consultar a hora do último snapshot. Todos os dados criados após o último snapshot são perdidos durante a migração.
- Para evitar possíveis perdas de dados, certifique-se de que seus usuários se desconectem e não façam login novamente até que o processo de migração seja concluído. WorkSpaces

- Certifique-se de que WorkSpaces você deseja migrar tenha o status DISPONÍVEL, PARADO ou ERRO.
- Verifique se você tem endereços IP suficientes para o WorkSpaces que você está migrando. Durante a migração, novos endereços IP serão alocados para o. WorkSpaces
- Se você estiver usando scripts para migrar WorkSpaces, migre-os em lotes de no máximo 25 por WorkSpaces vez.

Well-Architected Framework

AWS O Well-Architected ajuda os arquitetos de nuvem a criar uma infraestrutura segura, de alto desempenho, resiliente e eficiente para seus aplicativos e cargas de trabalho. Ele descreve os principais conceitos, princípios de design e melhores práticas arquitetônicas para projetar e executar cargas de trabalho na nuvem. É baseado em cinco pilares principais:

- Excelência operacional
- Segurança
- Confiabilidade
- Eficiência de desempenho
- Otimização de custo

Ao arquitetar um WorkSpaces ambiente Amazon, é importante avaliar esses pilares fundamentais para determinar o nível de maturidade de implantação e descobrir recursos adicionais que podem ser usados com a Amazon. WorkSpaces Embora haja uma orientação geral para o AWS Well-Architect Framework, o texto a seguir fornece algumas perguntas-chave que podem ser incluídas na fase de planejamento de sua WorkSpaces implantação para garantir que cada um dos cinco pilares seja considerado.

Geral

- Qual é o impulsionador de negócios desse projeto?

Excelência operacional

- Como você separa o controle de acesso entre usuários e diferentes grupos de administradores?

Segurança

1. Quais são os requisitos de segurança e conformidade a serem considerados WorkSpaces para operar?
2. Há alguma restrição no roteamento para endereços IP externos?
3. As WorkSpaces portas necessárias são permitidas pelo firewall corporativo?

4. A autenticação multifator é ou será usada com essa implantação?
5. Como você faz muitas identidades de usuário e solicitações de autorização atualmente?

Confiabilidade

1. Qual é a política de retenção de dados para desktops?
2. O que é o objetivo de ponto de recuperação (RPO) para dados do usuário final?
3. Qual é o objetivo de tempo de recuperação (RTO) para dados do usuário final?

Otimização de custo

1. Os WorkSpaces pacotes foram dimensionados corretamente para o caso de usuário e os aplicativos?
2. Os usuários consumirão WorkSpaces mais de 82 horas por mês?

Embora as perguntas acima não constituam uma lista exaustiva de itens que devem ser considerados, elas fornecem algumas orientações abrangentes para ajudá-lo com a implantação do Well-Architected Amazon. WorkSpaces

Segurança

Esta seção explica como proteger dados usando criptografia ao usar os WorkSpaces serviços da Amazon. Ele descreve a criptografia em trânsito e em repouso e o uso de grupos de segurança para proteger o acesso da rede ao WorkSpaces. Esta seção também fornece informações sobre como controlar o acesso do dispositivo final WorkSpaces usando dispositivos confiáveis e grupos de controle de acesso IP.

Informações adicionais sobre autenticação (incluindo suporte a MFA) no AWS Directory Service podem ser encontradas nesta seção.

Criptografia em trânsito

A Amazon WorkSpaces usa criptografia para proteger a confidencialidade em diferentes estágios da comunicação (em trânsito) e também para proteger dados em repouso (criptografados WorkSpaces). Os processos em cada estágio da criptografia usada pela Amazon WorkSpaces em trânsito são descritos nas seções a seguir.

Para obter informações sobre a criptografia em repouso, consulte a WorkSpaces seção Criptografada deste documento.

Registro e atualizações

O aplicativo cliente de desktop se comunica com a Amazon para atualizações e registro usando HTTPS.

Estágio de autenticação

O cliente de desktop inicia a autenticação enviando credenciais para o gateway de autenticação. A comunicação entre o cliente de desktop e o gateway de autenticação usa HTTPS. Ao final desse estágio, se a autenticação for bem-sucedida, o gateway de autenticação retornará um token OAuth 2.0 para o cliente de desktop, por meio da mesma conexão HTTPS.

> **Note**
>
> O aplicativo cliente de desktop suporta o uso de um servidor proxy para tráfego da porta 443 (HTTPS), para atualizações, registro e autenticação.

Depois de receber as credenciais do cliente, o gateway de autenticação envia uma solicitação de autenticação para o AWS Directory Service. A comunicação do gateway de autenticação com o AWS Directory Service ocorre por HTTPS, portanto, nenhuma credencial de usuário é transmitida em texto simples.

Autenticação — Conector do Active Directory (ADC)

O AD Connector usa o Kerberos para estabelecer comunicação autenticada com o AD local, para que ele possa se vincular ao LDAP e executar consultas LDAP subsequentes. O suporte LDAPS do lado do cliente no ADC também está disponível para criptografar consultas entre o Microsoft AD e o Applications. AWS Antes de implementar a funcionalidade LDAPS do lado do cliente, revise os pré-requisitos para o LDAPS do lado do cliente.

O AWS Directory Service também oferece suporte a LDAP com TLS. Nenhuma credencial de usuário é transmitida em texto simples a qualquer momento. Para aumentar a segurança, é possível conectar uma WorkSpaces VPC à rede local (onde o AD reside) usando uma conexão VPN. Ao usar uma conexão VPN de AWS hardware, os clientes podem configurar a criptografia em trânsito usando IPSEC (Internet Key Exchange (IKE) e IPSEC SAs) padrão com chaves de criptografia simétricas AES-128 ou AES-256, SHA-1 ou SHA-256 para hash de integridade e grupos DH (2,14-18, 22, 23 e 24 para a fase 1; 1,2,5, 14-18, 22, 23 e 24 para a fase 2) usando o encaminhamento perfeito rectidão (PFS).

Fase de corretora

Depois de receber o token OAuth 2.0 (do gateway de autenticação, se a autenticação for bem-sucedida), o cliente de desktop consulta os WorkSpaces serviços da Amazon (Broker Connection Manager) usando HTTPS. O cliente de desktop se autentica enviando o token OAuth 2.0 e, como resultado, o cliente recebe as informações do endpoint do gateway de streaming. WorkSpaces

Estágio de streaming

O cliente de desktop solicita a abertura de uma sessão PCoIP com o gateway de streaming (usando o token OAuth 2.0). Essa sessão é criptografada com AES-256 e usa a porta PCoIP para controle de comunicação (4172/TCP).

Usando o token OAuth2.0, o gateway de streaming solicita as WorkSpaces informações específicas do usuário do WorkSpaces serviço Amazon, via HTTPS.

O gateway de streaming também recebe o TGT do cliente (que é criptografado usando a senha do usuário do cliente) e, usando a passagem Kerberos TGT, o gateway inicia um login do Windows no WorkSpace, usando o Kerberos TGT recuperado pelo usuário.

WorkSpace Em seguida, inicia uma solicitação de autenticação para o AWS Directory Service configurado, usando a autenticação Kerberos padrão.

Depois que o login WorkSpace for feito com sucesso, o streaming do PCoIP será iniciado. A conexão é iniciada pelo cliente na porta TCP 4172 com o tráfego de retorno na porta UDP 4172. Além disso, a conexão inicial entre o gateway de streaming e um WorkSpaces desktop pela interface de gerenciamento é via UDP 55002. (Consulte a documentação para obter os requisitos de endereço IP e porta da Amazon WorkSpaces. A porta UDP de saída inicial é 55002.) A conexão de streaming, usando as portas 4172 (TCP e UDP), é criptografada usando cifras AES de 128 e 256 bits, mas o padrão é de 128 bits. Os clientes podem alterar isso ativamente para 256 bits, usando as configurações de política de grupo do AD específicas do PCoIP para Windows ou com o arquivo WorkSpaces pcoip-agent.conf para Amazon Linux. WorkSpaces Para obter mais informações sobre a administração da Política de Grupo para a Amazon WorkSpaces, consulte a documentação.

Interfaces de rede

Cada Amazon WorkSpace tem duas interfaces de rede, chamadas de interface de rede primária e interface de rede de gerenciamento.

A interface de rede primária fornece conectividade aos recursos dentro da VPC do cliente, como acesso ao AWS Directory Service, à Internet e à rede corporativa do cliente. É possível anexar grupos de segurança a essa interface de rede primária. Conceitualmente, os grupos de segurança são diferenciados anexados a essa ENI com base no escopo da implantação: grupo de segurança e grupos de WorkSpaces segurança ENI.

Interface de rede de gerenciamento

A interface da rede de gerenciamento não pode ser controlada por meio de grupos de segurança; no entanto, os clientes podem usar um firewall baseado em host WorkSpaces para bloquear portas ou controlar o acesso. Não recomendamos aplicar restrições na interface da rede de gerenciamento. Se um cliente decidir adicionar regras de firewall baseadas em host para gerenciar essa interface, algumas portas devem estar abertas para que o WorkSpaces serviço da Amazon possa gerenciar a integridade e a acessibilidade do WorkSpace. Para obter mais informações, consulte Interfaces de rede no Guia de administração do Amazon Workspaces.

WorkSpaces grupos de segurança

Um grupo de segurança padrão é criado por AWS Directory Service e é automaticamente anexado a todos os WorkSpaces que pertencem a esse diretório específico.

A Amazon WorkSpaces, como muitos outros AWS serviços, faz uso de grupos de segurança. WorkSpaces A Amazon cria dois grupos de AWS segurança quando você registra um diretório no WorkSpaces serviço. Um para controladores de diretório DirectoryID_Controllers e outro para o diretório DirectoryID_WORKSPACESMEMBERS. WorkSpaces Não exclua nenhum desses grupos de segurança, ou você WorkSpaces ficará prejudicado. Por padrão, o grupo de segurança WorkSpaces Membros tem a saída aberta para 0.0.0.0/0. Você pode adicionar um grupo WorkSpaces de segurança padrão a um diretório. Depois de associar um novo grupo de segurança a um WorkSpaces diretório, os novos WorkSpaces que você iniciar ou os existentes WorkSpaces que você reconstruir terão o novo grupo de segurança. Você também pode adicionar esse novo grupo de segurança padrão aos existentes WorkSpaces sem reconstruí-los. Ao associar vários grupos de segurança a um WorkSpaces diretório, WorkSpaces agregue as regras de cada grupo de segurança em um único conjunto de regras. Recomendamos que você condense as regras do grupo de segurança o máximo possível. Para obter mais informações sobre grupos de segurança, consulte Grupos de segurança para sua VPC no Guia do usuário da Amazon VPC.

Para obter mais informações sobre como adicionar um grupo de segurança a um WorkSpaces diretório existente ou a um diretório existente WorkSpace, consulte o Guia do WorkSpaces administrador.

Alguns clientes querem restringir portas e destinos pelos quais o WorkSpaces tráfego pode sair. Para restringir o tráfego de saída do WorkSpaces, você deve garantir que as portas específicas sejam deixadas necessárias para a comunicação do serviço; caso contrário, seus usuários não conseguirão fazer login nelas. WorkSpaces

WorkSpaces utilize a Elastic Network Interface (ENI) na VPC do cliente para comunicação com os controladores WorkSpace de domínio durante o login. Para permitir que seus usuários façam login WorkSpaces com êxito, você deve permitir que as seguintes portas acessem seus controladores de domínio ou os intervalos CIDR que incluem seus controladores de domínio no grupo de segurança _workspacesMembers.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticação de Kerberos
- TCP/UDP 389 — LDAP

- TCP/UDP 445 - SMB
- TCP 3268-3269 - catálogo global
- TCP/UDP 464 - Alteração de senha do Kerberos
- TCP 139 - Netlogon
- UDP 137-138 - Netlogon
- UDP 123 - NTP
- Portas efêmeras TCP/UDP 49152-65535 para RPC

Se WorkSpaces precisar acessar outros aplicativos, a Internet ou outros locais, você precisará permitir essas portas e destinos na notação CIDR dentro do grupo de segurança _workspacesMembers. Se você não adicionar essas portas e destinos, eles não WorkSpaces alcançarão nada além das portas listadas acima. Uma consideração final: por padrão, um novo grupo de segurança não tem regras de entrada. Portanto, nenhum tráfego de entrada originário de outro host para a instância será permitido até que você adicione regras de entrada ao security group. As etapas acima são necessárias somente se você quiser restringir a saída do WorkSpaces ou restringir as regras de entrada somente aos recursos ou intervalos de CIDR que devem ter acesso a elas.

> **Note**
>
> Um grupo de segurança recém-associado será anexado somente ao grupo WorkSpaces criado ou reconstruído após a modificação.

Grupos de segurança ENI

Como a interface de rede primária é uma ENI comum, ela pode ser gerenciada usando as diferentes ferramentas AWS de gerenciamento. Para obter mais informações, consulte Elastic Network Interfaces. Navegue até o endereço WorkSpace IP (na WorkSpaces página no WorkSpaces console da Amazon) e use esse endereço IP como filtro para encontrar a ENI correspondente (na seção Interfaces de rede do console do Amazon EC2).

Uma vez localizada, a ENI pode ser gerenciada diretamente por grupos de segurança. Ao atribuir manualmente grupos de segurança à interface de rede primária, considere os requisitos de porta da Amazon WorkSpaces. Para obter mais informações, consulte Interfaces de rede no Guia de administração do Amazon Workspaces.

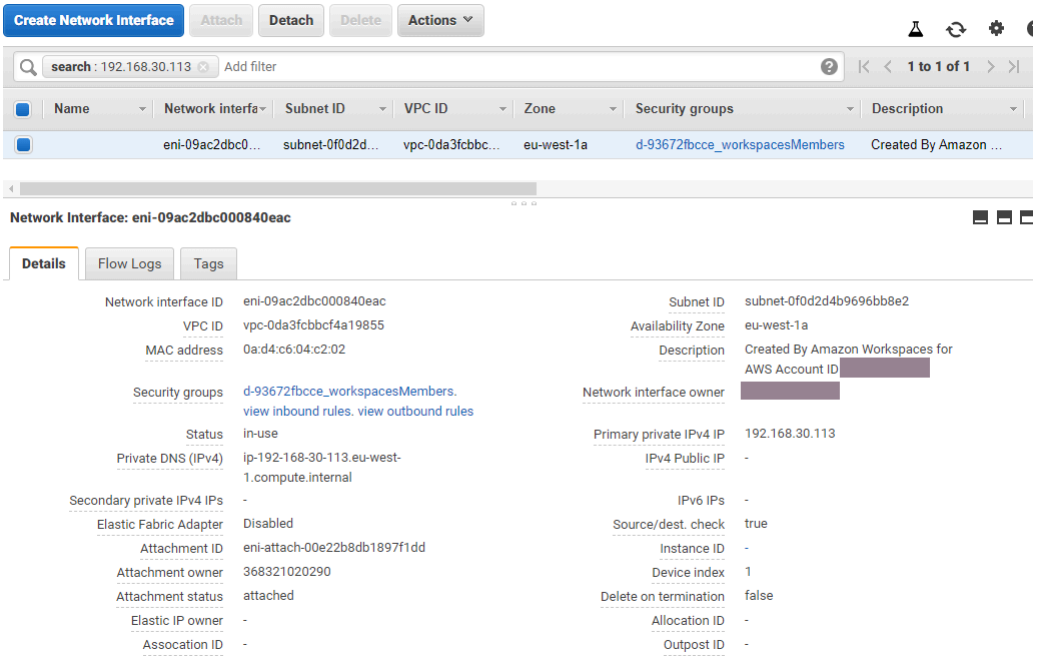

Figura 21: WorkSpaces cliente com MFA habilitado

Network Access Control Lists (ACLs)

Devido à complexidade adicional no gerenciamento de outro firewall, as ACLs de rede são comumente usadas em implantações muito complexas e geralmente não são usadas como uma prática recomendada. Como as ACLs de rede são anexadas às sub-redes na VPC, isso concentra sua função na camada 3 (rede) do modelo OSI. Como a Amazon WorkSpaces foi projetada com base nos Serviços de Diretório, duas sub-redes devem ser definidas. As ACLs de rede são gerenciadas separadamente dos Serviços de Diretório, e é bem provável que uma ACL de Rede possa ser atribuída a somente uma das sub-redes atribuídas WorkSpaces.

Quando um firewall sem estado é necessário, as ACLs de rede são a melhor prática de segurança. Certifique-se de que todas as alterações feitas nas ACLs de rede além das configurações padrão sejam validadas por sub-rede como uma prática recomendada. Se as ACLs de rede não estiverem funcionando conforme o esperado, considere usar os registros de fluxo da VPC para analisar o tráfego.

AWS Firewall de rede

AWS O Firewall de Rede oferece funcionalidades além das oferecidas pelos grupos de segurança e ACLs de rede nativos, mas com um custo. Quando os clientes ~~solicitaram~~ a capacidade de aumentar

a segurança em conexões de rede, como inspeção de nomes de servidor (SNI) para sites baseados em HTTPS, detecção e prevenção de intrusões e uma lista de permissão e recusa para nomes de domínio, eles precisaram encontrar firewalls alternativos no. AWS Marketplace A complexidade na implantação desses firewalls apresentou desafios além do que os administradores padrão de EUC são qualificados. AWS O Network Firewall oferece uma AWS experiência nativa enquanto ativa as proteções das camadas 3 a 7. Usar o Firewall de AWS Rede em conjunto com o NAT Gateway é uma prática recomendada quando as organizações não possuem nenhum outro meio (excluindo o licenciamento local existente para firewalls de terceiros que podem ser transferidos para a nuvem ou equipes separadas que gerenciam firewalls) para cobrir todas as proteções de rede EUC. O NAT Gateway também é gratuito com o AWS Network Firewall.

As implantações do AWS Network Firewall são projetadas de acordo com o design EUC existente. Projetos de VPC únicos podem obter uma arquitetura simplificada com sub-redes para endpoints de firewall e considerações separadas de roteamento de saída da Internet, enquanto projetos de várias VPC se beneficiam muito de uma VPC de inspeção consolidada com firewall e terminais Transit Gateways.

Cenários de design

Cenário 1: bloqueio básico de instâncias

O Grupo WorkSpaces de Segurança padrão não permite a entrada de tráfego, pois os Grupos de Segurança são negados por padrão e são monitorados. Isso significa que não há configurações adicionais que precisem ser configuradas para proteger ainda mais as próprias WorkSpaces instâncias. Considere as regras de saída que permitem todo o tráfego e se isso se adequa ao caso de uso. Por exemplo, talvez seja melhor negar todo o tráfego de saída da porta 443 para qualquer endereço e intervalos de IP específicos adequados aos casos de uso de portas, como 389 para LDAP, 636 para LDAPS, 445 para SMB, entre outros; embora observe que a complexidade do ambiente pode exigir várias regras e, portanto, ser melhor atendida por meio de ACLs de rede ou de um dispositivo de firewall.

Cenário 2: exceções de entrada

Embora não seja um requisito constante, pode haver momentos em que o tráfego de rede seja iniciado na entrada. WorkSpaces Por exemplo, a triagem de instâncias em que o WorkSpaces cliente não consegue se conectar exige conectividade remota alternativa. Nesses casos, é melhor habilitar temporariamente o TCP 3389 de entrada para o Grupo de Segurança da ENI do cliente do WorkSpace cliente.

Outro cenário são scripts organizacionais que executam comandos para funções de inventário ou automação, iniciados por uma instância centralizada. Proteger o tráfego nessa porta a partir dessas instâncias centralizadas específicas na entrada pode ser configurado permanentemente, no entanto, é uma prática recomendada fazer isso no Grupo de Segurança adicional anexado à configuração do Diretório, pois ele pode ser aplicado a várias implantações na conta. AWS

Por fim, há algum tráfego de rede que não é baseado em estado e exigirá que portas efêmeras sejam especificadas nas exceções de entrada. Se as consultas e os scripts falharem, é uma prática recomendada permitir portas efêmeras, pelo menos temporariamente, enquanto determina a causa raiz da falha de conectividade.

Cenário 3: inspeção única de VPC

Implantações simplificadas de WorkSpaces (como uma única VPC sem planos de escalabilidade) não exigem uma VPC separada para inspeção e, portanto, a conexão com outras VPCs pode ser simplificada com o emparelhamento de VPC. No entanto, sub-redes separadas para endpoints de firewall devem ser criadas com roteamento configurado para esses endpoints, bem como roteamento de saída do Internet Gateway (IGW), que de outra forma não precisaria ser configurado. As implantações existentes podem não ter o espaço IP disponível se todas as sub-redes utilizarem todo o bloco CIDR da VPC. Nesses casos, o Cenário 4 pode ser melhor, pois a implantação já foi escalada além do design inicial.

Cenário 4: Inspeção centralizada

Frequentemente preferido em várias implantações de EUC em uma AWS região, simplificando a administração das regras com e sem estado do Firewall de AWS Rede. Os pares de VPC existentes serão substituídos por Transit Gateways, pois esse design exige o uso de anexos do Transit Gateway, bem como do roteamento de inspeção que só pode ser configurado por meio desses anexos. Também é exercido um maior grau de controle sobre essa configuração e permite uma segurança além da WorkSpaces experiência padrão.

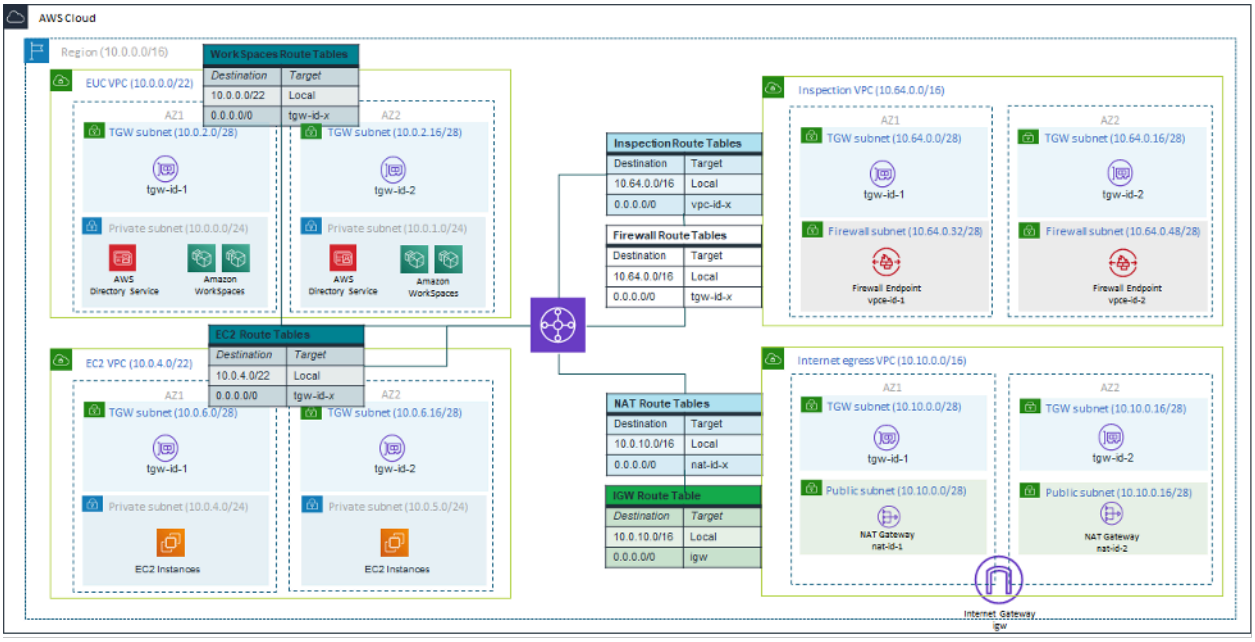

Figura 22: Exemplo de arquitetura usando anexos do Transit Gateway

Encriptado WorkSpaces

Cada Amazon WorkSpace é provisionada com um volume raiz (C: drive para Windows WorkSpaces, root para Amazon Linux WorkSpaces) e um volume de usuário (D: drive para Windows WorkSpaces, /home para Amazon Linux). WorkSpaces O WorkSpaces recurso criptografado permite que um ou ambos os volumes sejam criptografados.

O que é criptografado?

Os dados armazenados em repouso, a entrada/saída de disco (E/S) do volume e os instantâneos criados a partir de volumes criptografados são todos criptografados.

Quando a criptografia ocorre?

A criptografia para a WorkSpace deve ser especificada ao iniciar (criar) WorkSpace o. WorkSpaces os volumes só podem ser criptografados no momento da inicialização: após o lançamento, o status da criptografia do volume não pode ser alterado. A figura a seguir mostra a página do WorkSpaces console da Amazon para escolher a criptografia durante o lançamento de uma nova WorkSpace.

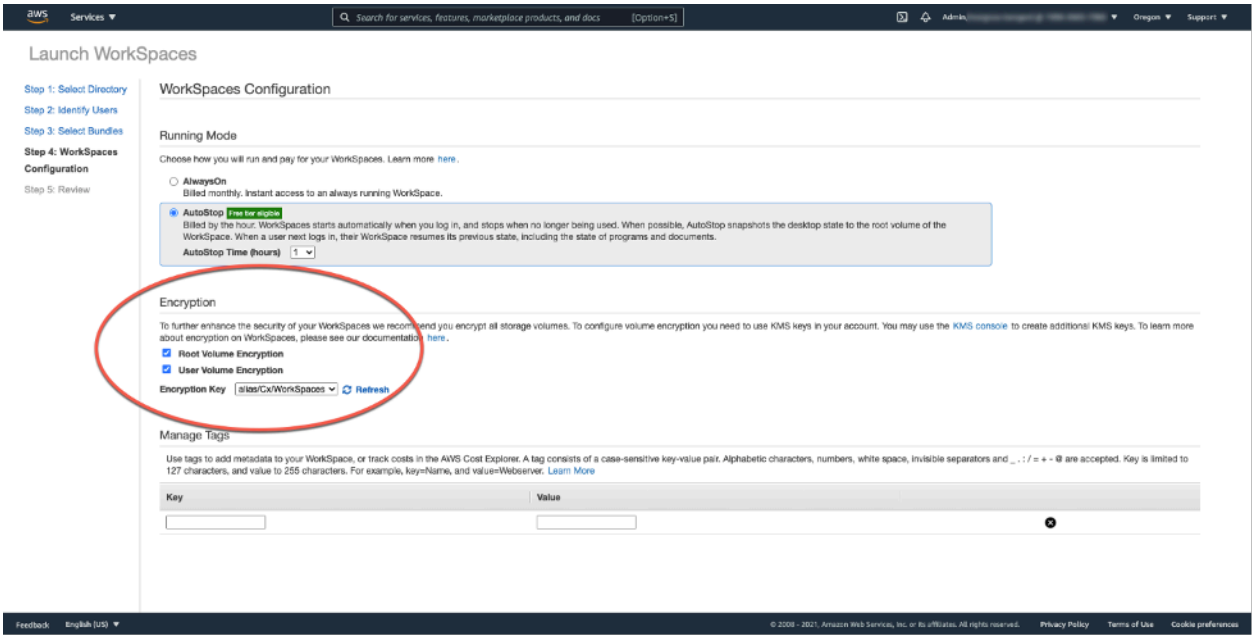

Figura 23: Criptografando volumes WorkSpace raiz

Como um novo é WorkSpace criptografado?

Um cliente pode escolher a WorkSpaces opção Criptografada no WorkSpaces console da Amazon ou usando a WorkSpaces API da Amazon quando um cliente lança uma nova WorkSpace. AWS CLI

Para criptografar os volumes, a Amazon WorkSpaces usa uma CMK de AWS Key Management Service ()AWS KMS. Uma AWS KMS CMK padrão é criada na primeira vez que a WorkSpace é iniciada em uma região. (As CMKs têm um escopo regional.)

Um cliente também pode criar uma CMK gerenciada pelo cliente para usar com criptografia. WorkSpaces A CMK é usada para criptografar as chaves de dados usadas pelo WorkSpaces serviço da Amazon para criptografar cada um dos volumes. WorkSpace (Em um sentido estrito, é o Amazon EBS que criptografará os volumes). Para ver os limites atuais da CMK, consulte Cotas de AWS KMS recursos.

> **Note**
>
> A criação de imagens personalizadas a partir de uma imagem criptografada não WorkSpace é suportada. Além disso, WorkSpaces o lançamento com a criptografia de volume raiz ativada pode levar até uma hora para ser provisionado.

Para obter uma descrição detalhada do processo de WorkSpaces criptografia, consulte Como a Amazon WorkSpaces usa AWS KMS. Considere como o uso da CMK será monitorado para garantir que uma solicitação de criptografia WorkSpace seja atendida corretamente. Para obter informações adicionais sobre AWS KMS chaves e chaves de dados, consulte a AWS KMS página.

Opções de controle de acesso e dispositivos confiáveis

WorkSpaces A Amazon oferece aos clientes opções para gerenciar quais dispositivos clientes podem acessar WorkSpaces. Os clientes podem limitar o WorkSpaces acesso somente a dispositivos confiáveis. O acesso a WorkSpaces pode ser permitido a partir de PCs macOS e Microsoft Windows usando certificados digitais. Ele também pode permitir ou bloquear o acesso para iOS, Android, Chrome OS, Linux e clientes zero, bem como para o cliente WorkSpaces Web Access. Com esses recursos, ele pode melhorar ainda mais a postura de segurança.

As opções de controle de acesso estão habilitadas para novas implantações para que os usuários acessem seus clientes a WorkSpaces partir de clientes no Windows, macOS, iOS, Android, ChromeOS e Zero Clients. O acesso usando o Web Access ou um WorkSpaces cliente Linux não está habilitado por padrão para uma nova WorkSpaces implantação e precisará ser habilitado.

Se houver limites no acesso aos dados corporativos a partir de dispositivos confiáveis (também conhecidos como dispositivos gerenciados), o WorkSpaces acesso poderá ser restrito a dispositivos confiáveis com certificados válidos. Quando esse recurso está ativado, a Amazon WorkSpaces usa autenticação baseada em certificado para determinar se um dispositivo é confiável. Se o aplicativo WorkSpaces cliente não puder verificar se um dispositivo é confiável, ele bloqueia as tentativas de login ou reconexão a partir do dispositivo.

O suporte confiável a dispositivos está disponível para os seguintes clientes:

- Aplicativo Amazon WorkSpaces Android Client no Google Play que roda em dispositivos Chrome OS compatíveis com Android e Android
- Aplicativo Amazon WorkSpaces macOS Client executado em dispositivos macOS
- Aplicativo Amazon WorkSpaces Windows Client executado em dispositivos Windows

Para obter mais informações sobre como controlar quais dispositivos podem acessar WorkSpaces, consulte Restringir WorkSpaces acesso a dispositivos confiáveis.

> **Note**
>
> Os certificados para dispositivos confiáveis se aplicam somente aos WorkSpaces clientes Amazon Windows, macOS e Android. Esse recurso não se aplica ao cliente Amazon WorkSpaces Web Access ou a quaisquer clientes terceirizados, incluindo, mas não se limitando ao software Teradici PCoIP e clientes móveis, clientes zero Teradici PCoIP, clientes RDP e aplicativos de desktop remoto.

Grupos de controle de acesso IP

Usando grupos de controle baseados em endereços IP, os clientes podem definir e gerenciar grupos de endereços IP confiáveis e permitir que os usuários os acessem WorkSpaces somente quando estiverem conectados a uma rede confiável. Esse recurso ajuda os clientes a obter maior controle sobre sua postura de segurança.

Grupos de controle de acesso IP podem ser adicionados no nível do WorkSpaces diretório. Há duas maneiras de começar a usar grupos de controle de acesso IP.

- Página de controles de acesso IP — No console WorkSpaces de gerenciamento, grupos de controle de acesso IP podem ser criados na página Controles de acesso IP. As regras podem ser adicionadas a esses grupos inserindo os endereços IP ou intervalos de IP a partir dos quais WorkSpaces podem ser acessados. Esses grupos podem então ser adicionados aos diretórios na página Detalhes da atualização.
- APIs do espaço de trabalho — as WorkSpaces APIs podem ser usadas para criar, excluir e visualizar grupos; criar ou excluir regras de acesso; ou para adicionar e remover grupos de diretórios.

Para obter uma descrição detalhada do uso de grupos de controle de acesso IP com o processo de WorkSpaces criptografia da Amazon, consulte IP Access Control Groups for Your WorkSpaces.

Monitoramento ou registro usando a Amazon CloudWatch

O monitoramento de redes, servidores e registros é parte integrante de qualquer infraestrutura. Os clientes que implantam a Amazon WorkSpaces precisam monitorar suas implantações, especificamente a saúde geral e o status de conexão do indivíduo WorkSpaces.

CloudWatch Métricas da Amazon para WorkSpaces

CloudWatch O metrics WorkSpaces for foi projetado para fornecer aos administradores uma visão adicional sobre a saúde geral e o status da conexão do indivíduo WorkSpaces. As métricas estão disponíveis por WorkSpace ou agregadas para todos WorkSpaces em uma organização em um determinado diretório.

Essas métricas, como todas as CloudWatch métricas, podem ser visualizadas na AWS Management Console (mostrada na figura a seguir), acessadas por meio das CloudWatch APIs e monitoradas por CloudWatch alarmes e ferramentas de terceiros.

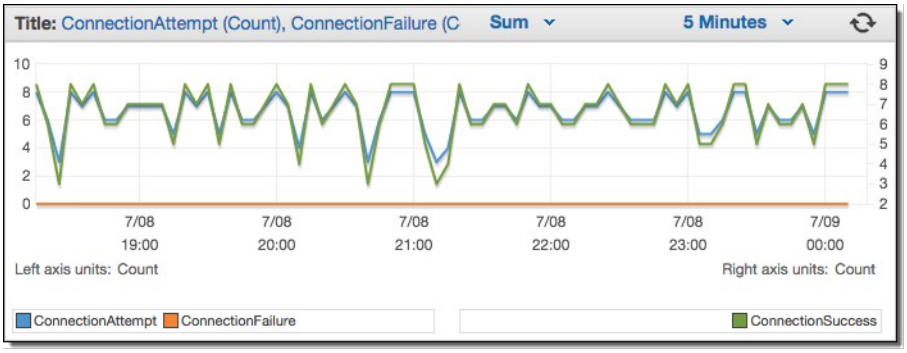

Figura 24: CloudWatch métricas: ConnectionAttempt / ConnectionFailure

Por padrão, as seguintes métricas estão habilitadas e estão disponíveis sem custo adicional:

- Disponível — aqueles WorkSpaces que respondem a uma verificação de status são contados nessa métrica.
- Insalubres — WorkSpaces aqueles que não respondem à mesma verificação de status são contabilizados nessa métrica.
- ConnectionAttempt— O número de tentativas de conexão feitas com um WorkSpace.
- ConnectionSuccess— O número de tentativas de conexão bem-sucedidas.
- ConnectionFailure— O número de tentativas de conexão malsucedidas.
- SessionLaunchTime— A quantidade de tempo necessária para iniciar uma sessão, conforme medido pelo WorkSpaces cliente.
- InSessionLatency— O tempo de ida e volta entre o WorkSpaces cliente e WorkSpaces, conforme medido e relatado pelo cliente.
- SessionDisconnect— O número de sessões iniciadas pelo usuário e fechadas automaticamente.

Além disso, os alarmes podem ser criados, conforme mostrado na figura a seguir.

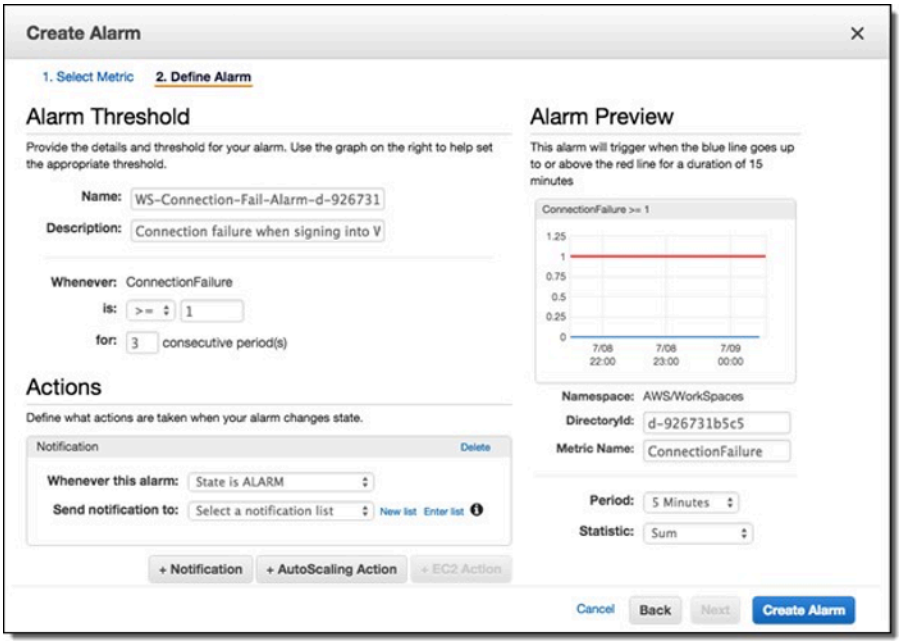

Figura 25: Criar CloudWatch alarme para erros de WorkSpaces conexão

CloudWatch Eventos da Amazon para WorkSpaces

Os eventos da Amazon CloudWatch Events podem ser usados para visualizar, pesquisar, baixar, arquivar, analisar e responder a logins bem-sucedidos no. WorkSpaces O serviço pode monitorar endereços IP da WAN do cliente, sistema operacional, WorkSpaces ID e informações de ID de diretório para os logins dos usuários. WorkSpaces Por exemplo, ele pode usar eventos para as seguintes finalidades:

- Armazene ou arquive eventos de WorkSpaces login como registros para futura referência, analise os registros para procurar padrões e tome medidas com base nesses padrões.
- Use o endereço IP da WAN para determinar de onde os usuários estão conectados e, em seguida, use políticas para permitir que os usuários acessem somente arquivos ou dados WorkSpaces que atendam aos critérios de acesso encontrados no Tipo de WorkSpaces acesso de CloudWatch evento.
- Usar controles de política para bloquear o acesso a arquivos e aplicativos de endereços IP não autorizados.

Para obter mais informações sobre como usar o CloudWatch Events, consulte o Amazon CloudWatch Events User Guide. Para saber mais sobre CloudWatch eventos para WorkSpaces, consulte Monitore seu WorkSpaces uso do Cloudwatch Events.

YubiKey suporte para Amazon WorkSpaces

Para adicionar uma camada de segurança adicional, os clientes geralmente optam por proteger ferramentas e sites com autenticação multifatorial. Alguns clientes optam por fazer isso com um Yubico YubiKey. A Amazon WorkSpaces oferece suporte a senhas de uso único (OTP) e ao protocolo de autenticação FIDO U2F com. YubiKeys

WorkSpaces Atualmente, a Amazon oferece suporte ao modo OTP, e não há nenhuma etapa adicional exigida de um administrador ou usuário final para utilizar um YubiKey com OTP. O usuário pode conectá-los YubiKey ao computador, garantir que o teclado esteja focado no WorkSpace (especificamente no campo em que o OTP precisa ser inserido) e tocar no contato dourado noYubiKey. O YubiKey inserirá automaticamente o OTP no campo selecionado.

Para utilizar o modo FIDO U2F com YubiKey e WorkSpaces, etapas adicionais são necessárias. Certifique-se de que seus usuários recebam um desses YubiKey modelos compatíveis para utilizar o redirecionamento U2F com: WorkSpaces

- YubiKey 4
- YubiKey 5 NFC
- YubiKey 5 Nano
- YubiKey 5C
- YubiKey 5C Nano
- YubiKey 5 NFC

Para habilitar o redirecionamento USB para YubiKey U2F

Por padrão, o redirecionamento USB está desativado para PCoIP WorkSpaces; para utilizar o modo U2F com YubiKeys, você deve ativá-lo.

1. Verifique se você instalou o modelo administrativo de Política de WorkSpaces Grupo mais recente para PCoIP (32 bits) ou o modelo administrativo de Política de WorkSpaces Grupo para PCoIP (64 bits).
2. Em uma administração de diretório WorkSpace ou em uma instância do Amazon EC2 associada ao seu WorkSpaces diretório, abra a ferramenta Group Policy Management (gpmc.msc) e navegue até Variáveis de sessão PCoIP.
3. Para permitir que o usuário substitua sua configuração, escolha Padrões substituíveis do administrador. Caso contrário, escolha Padrões do administrador não substituíveis.

4. Abra a configuração Habilitar/desabilitar USB na sessão PCoIP.
5. Selecione Habilitado e, em seguida, Salvar.
6. Abra a configuração Configurar regras de dispositivos USB permitidos e não permitidos no PCoIP.
7. Selecione Habilitado e, em Inserir a tabela de autorização USB (máximo de dez regras), configure as regras da lista de permissões de dispositivos USB.
   a. Regra de autorização: 110500407. Esse valor é uma combinação do ID de um fornecedor (VID) e do ID de um produto (PID). O formato para uma combinação VID/PID é`1xxxxyyyy`, onde `xxxx` está o VID no formato hexadecimal e `yyyy` o PID no formato hexadecimal. Nesse exemplo, 1050 é o VID e 0407 é o PID. Para obter mais valores YubiKey USB, consulte Valores de ID YubiKey USB.
8. Em Inserir a tabela de autorização USB (máximo de dez regras), configure as regras da lista de bloqueio de dispositivos USB.
   a. Para Regra de não autorização, defina uma string vazia. Isso significa que somente dispositivos USB na lista de autorização são permitidos.

   > **Note**
   >
   > Você pode definir no máximo dez regras de autorização de USB e no máximo dez regras de não autorização de USB. Use o caractere de barra vertical (|) para separar várias regras. Para obter informações detalhadas sobre as regras de autorização/desautorização, consulte Teradici PCoIP Standard Agent for Windows

9. Escolha OK.
10. A alteração da configuração da Política de Grupo entra em vigor após a próxima atualização da Política de Grupo WorkSpace e após a reinicialização da WorkSpace sessão. Para aplicar as alterações de política de grupo, execute um destes procedimentos:
    a. Reinicie o WorkSpace (no WorkSpaces console da Amazon, selecione o e, em seguida WorkSpace, escolha Ações, Reinicialização WorkSpaces).
    b. Em um prompt de comando administrativo, digite gpupdate /force.
11. Depois que a configuração entrar em vigor, todos os dispositivos USB compatíveis poderão ser redirecionados, a WorkSpaces menos que as restrições sejam configuradas por meio da configuração de regras do dispositivo USB.

Depois de habilitar o redirecionamento USB para YubiKey U2F, você pode utilizá-lo YubiKey com o modo Fido U2F.

Otimização de custo

Recursos de WorkSpace gerenciamento de autoatendimento

Na Amazon WorkSpaces, os recursos WorkSpace de gerenciamento de autoatendimento podem ser habilitados para que os usuários tenham mais controle sobre sua experiência. Permitir aos usuários a capacidade de autoatendimento pode reduzir a carga de trabalho da equipe de suporte de TI na Amazon. WorkSpaces Quando os recursos de autoatendimento estão habilitados, eles permitem que os usuários executem uma ou mais das seguintes tarefas diretamente do cliente Windows, macOS ou Linux da Amazon: WorkSpaces

- Armazene em cache as credenciais dos usuários no seu cliente. Isso permite que os usuários se reconectem WorkSpace sem reinserir suas credenciais.
- Reinicie seu WorkSpace.
- Aumente o tamanho dos volumes raiz e do usuário em seus WorkSpace.
- Altere o tipo de computação (pacote) para seus. WorkSpace
- Mude o modo de execução deles WorkSpace.
- Reconstrua seus. WorkSpace

Não há implicações contínuas de custo em permitir aos usuários as opções de reinicialização e reconstrução para seus WorkSpaces. Os usuários devem estar cientes de que uma reconstrução deles WorkSpace fará com que WorkSpace fiquem indisponíveis por até uma hora, enquanto o processo de reconstrução ocorre.

As opções para aumentar o tamanho dos volumes, alterar o tipo de computação e alternar o modo de execução podem gerar custos adicionais. WorkSpaces Uma prática recomendada é permitir o autoatendimento para reduzir a carga de trabalho da equipe de suporte. O autoatendimento para itens de custo adicional deve ser permitido dentro de um processo de fluxo de trabalho que garanta que a autorização para cobranças adicionais tenha sido obtida. Isso pode ser feito por meio de um portal de autoatendimento dedicado ou por meio da integração com serviços existentes de Gerenciamento de Serviços de Tecnologia da Informação (ITSM), como. WorkSpaces ServiceNow

Para obter informações mais detalhadas, consulte Habilitando recursos de WorkSpace gerenciamento de autoatendimento para seus usuários. Para obter um exemplo descrevendo a

ativação de um portal estruturado para autoatendimento do usuário, consulte Automatize a Amazon WorkSpaces com um portal de autoatendimento.

Otimizador WorkSpaces de custos da Amazon

A solução Amazon WorkSpaces Cost Optimizer analisa todos os seus dados de WorkSpaces uso da Amazon. Dependendo do seu uso, ele a converte automaticamente na opção WorkSpace de cobrança mais econômica (por hora ou mensal). Essa solução ajuda você a monitorar seu WorkSpace uso e otimizar custos, além de provisionar e configurar automaticamente os AWS serviços necessários para analisar o uso a cada 24 horas e converter indivíduos WorkSpaces. AWS CloudFormation A versão mais recente, 2.4, oferece aos clientes a flexibilidade de implantar a solução em uma VPC existente, configurar opcionalmente para região e terminação. Também melhorou a precisão dos cálculos de horas de cobrança WorkSpaces e aprimorou os metadados de relatórios. Se você já implantou uma versão anterior (v2.2.1 ou inferior) dessa solução, siga a documentação da pilha de atualização para atualizar a pilha do Amazon WorkSpaces Cost Optimizer CloudFormation e obter a versão mais recente da estrutura da solução.

O modo de execução de um WorkSpace determina sua disponibilidade e cobrança imediatas. Aqui está o modo de WorkSpaces execução atual:

AlwaysOn— Use ao pagar uma taxa mensal fixa para uso ilimitado de WorkSpaces. Esse modo é ideal para usuários que o usam WorkSpace como desktop principal e precisam de acesso instantâneo a um ambiente WorkSpace em execução o tempo todo.

AutoStop— Use ao pagar WorkSpaces por hora. Com esse modo, WorkSpaces pare após um período especificado de inatividade e o estado dos aplicativos e dos dados seja salvo. Para definir a hora de parada automática, use AutoStop Tempo (horas). Esse modo é ideal para usuários que precisam apenas de acesso em tempo parcial aos seus. WorkSpaces

Uma prática recomendada é monitorar o uso e definir o modo de execução da Amazon WorkSpaces como o mais econômico usando uma solução como o Amazon WorkSpaces Cost Optimizer. Essa solução implanta uma regra de CloudWatch eventos da Amazon que invoca uma AWS Lambdafunção a cada 24 horas.

Essa solução pode converter um modelo individual WorkSpaces de cobrança por hora em um modelo de cobrança mensal em qualquer dia após atingir o limite. Se a solução converter uma WorkSpace cobrança por hora em cobrança mensal, a solução não converterá a cobrança de WorkSpace volta em cobrança por hora até o início do próximo mês, e somente se o uso

estiver abaixo do limite. No entanto, o modelo de cobrança pode ser alterado manualmente a qualquer momento usando a WorkSpaces API AWS Management Console ou a Amazon. O AWS CloudFormation modelo da solução inclui parâmetros que executarão essas conversões e permitirão a execução da solução no modo de execução a seco para fornecer relatórios das recomendações.

Optando por não usar tags

Para evitar que a solução converta WorkSpace entre modelos de cobrança, aplique uma tag de recurso WorkSpace usando a chave de tag Skip_Convert e qualquer valor de tag. Essa solução registrará as tags WorkSpaces, mas não converterá as marcadas WorkSpaces. Remova a tag a qualquer momento para retomar a conversão automática WorkSpace. Para obter mais detalhes, consulte o Amazon WorkSpaces Cost Optimizer.

Optando por regiões

Por padrão, essa solução WorkSpaces monitorará todas as AWS regiões disponíveis examinando os diretórios registrados WorkSpaces na Amazon na mesma AWS conta. Você pode fornecer uma lista separada por vírgulas das AWS regiões que deseja monitorar no parâmetro de entrada Lista de AWS regiões para limitar as regiões a serem monitoradas.

Implantação em uma VPC existente

Essa solução requer uma VPC para executar a tarefa do ECS. Por padrão, a solução criará uma nova VPC, mas você pode implantá-la em uma VPC existente fornecendo os IDs de sub-rede e o ID do grupo de segurança como parte do parâmetro de entrada. Sua sub-rede atual tem uma rota para a Internet para a tarefa do ECS extrair a imagem do Docker hospedada em um repositório público do Amazon ECR.

Rescisão do não utilizado WorkSpaces

Essa solução permite que você encerre sem uso WorkSpaces no último dia do mês, quando todos os critérios tiverem sido atendidos. Você pode optar por esse recurso alterando o parâmetro TerminateUnusedWorkSpacesde entrada para o CloudFormation modelo. Uma prática recomendada é executar esse recurso no modo Dry Run por alguns meses e verificar os relatórios mensais para revisar os WorkSpaces marcados para rescisão.

Otimização do Amazon Connect para Amazon WorkSpaces

A experiência do usuário final para agentes de contact center precisa ser uma prioridade máxima, pois se o áudio deles for degradado, isso criará uma experiência de chamada ruim para o cliente que eles estão atendendo. Ao executar uma solução de contact center em um desktop remoto, o desempenho de áudio sempre será afetado em alguma escala mensurável quando o tráfego de voz não for priorizado na conexão de rede. Esse impacto se deve ao fato de o áudio fluir do terminal de áudio para a sessão virtual e, em seguida, ser compactado pelo protocolo de streaming para ser entregue ao usuário final. Esse roteamento adicional faz com que o áudio tenha um desempenho degradado por meio de gargalos na rede.

Uma abordagem para evitar esse comportamento é separar o áudio da sessão, o que significa que todos os recursos do agente do contact center permanecem em sessão, enquanto o fluxo de áudio permanece fora da sessão. Essa divisão permite que o áudio seja transmitido do endpoint de áudio diretamente para o usuário final, enquanto todos os outros recursos de chamada, incluindo as PII que o agente está visualizando, permaneçam em uma sessão segura. Essa otimização de áudio é considerada uma prática recomendada, pois garante que a experiência de chamada do cliente seja a melhor possível.

O Amazon Connect oferece uma API Streams que permite que os administradores personalizem seu Painel de Controle de Contato (CCP) para atender às suas necessidades comerciais. Uma das opções que um administrador tem é controlar se o CCP personalizado pode receber áudio para a chamada. Essas configurações nos permitem configurar uma CCP dividida; uma CCP somente de áudio para fora da sessão e uma CCP sem mídia para dentro da sessão. Depois que os administradores tiverem configurado esses CCPs personalizados, eles poderão aproveitar a otimização de áudio do Amazon Connect para. WorkSpaces Como os CCPs são entregues no navegador, essa configuração permite que os administradores forneçam sua URL de CCP somente de áudio para o diretório. WorkSpaces Depois de configurado, quando os agentes da central de atendimento do WorkSpaces Connect se autenticarem com sucesso WorkSpaces, o WorkSpaces cliente abrirá automaticamente a URL CCP somente de áudio fornecida no navegador padrão local do agente. Essa ação permite que o áudio flua diretamente para a máquina local do agente, enquanto o CCP sem mídia lida com todo o resto na sessão segura. WorkSpaces

Diagrama de arquitetura

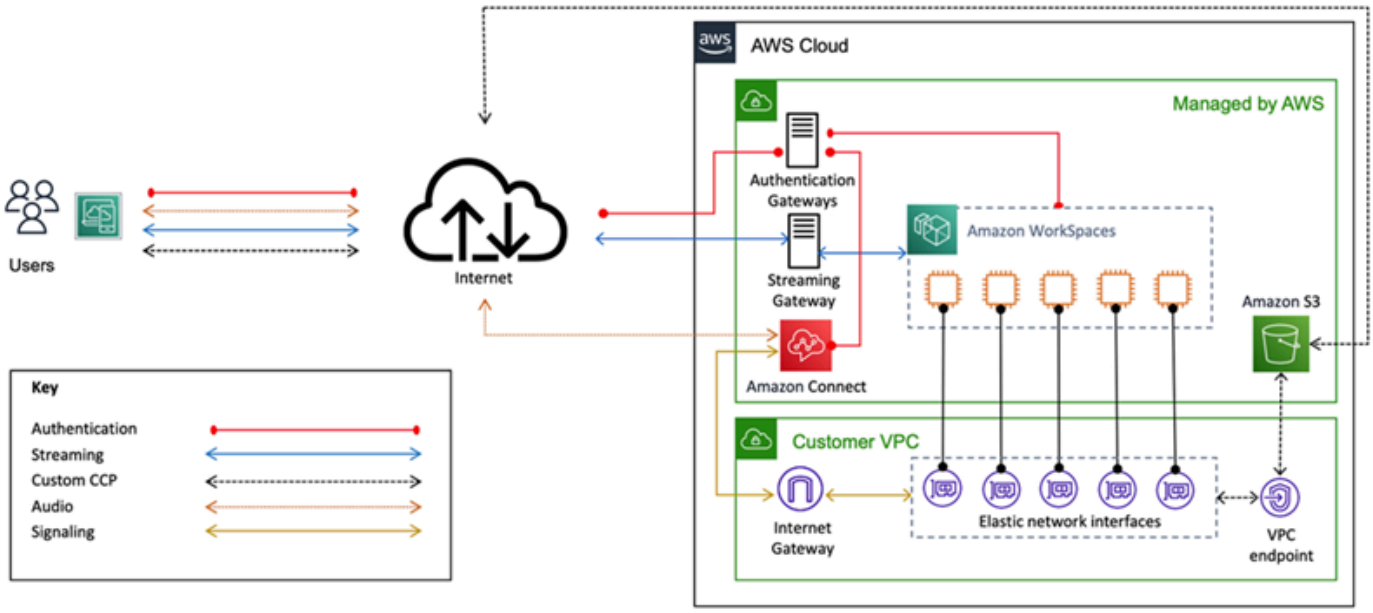

Figura 26 — Diagrama de WorkSpaces arquitetura e do Amazon Connect

Solução de problemas

Problemas comuns de administração e clientes, como mensagens de erro como “Seu dispositivo não consegue se conectar ao serviço de WorkSpaces registro” ou “Não consegue se conectar a um WorkSpace banner de login interativo”, podem ser encontrados nas páginas de solução de problemas de clientes e administradores no Guia de WorkSpaces Administração da Amazon.

Tópicos

O AD Connector não pode se conectar ao Active Directory

Para que o AD Connector se conecte ao diretório local, o firewall da rede local deve ter determinadas portas abertas para os CIDRs de ambas as sub-redes na VPC. Consulte o Cenário 1: Usando o AD Connector para autenticação de proxy no Active Directory Service local. Para testar se essas condições foram atendidas, execute as etapas a seguir.

Para testar a conexão:

1. Inicie uma instância do Windows na VPC e conecte-se a ela por RDP. As etapas restantes são executadas na instância da VPC.
2. Baixe e descompacte o aplicativo DirectoryServicePortTestde teste. O código-fonte e os arquivos de projeto do Microsoft Visual Studio estão incluídos para modificar o aplicativo de teste, se desejado.
3. Em um prompt de comando do Windows, execute o aplicativo de DirectoryServicePortTest teste com as seguintes opções:

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

<domain_name>— O nome de domínio totalmente qualificado, usado para testar os níveis funcionais da floresta e do domínio. Se o nome de domínio for excluído, os níveis funcionais não serão testados.

< Server_IP_address> — O endereço IP de um controlador de domínio no domínio local. As portas são testadas em relação a esse endereço IP. Se o endereço IP for excluído, as portas não serão testadas.

Esse teste determina se as portas necessárias estão abertas da VPC para o domínio. A aplicação de teste também verifica os níveis funcionais mínimos de floresta e domínio.

Solução de problemas Um erro de criação de imagem WorkSpace personalizada

Se um Windows ou Amazon Linux WorkSpace tiver sido lançado e personalizado, uma imagem personalizada poderá ser criada a partir dele WorkSpace. Uma imagem personalizada contém o sistema operacional, o software do aplicativo e as configurações do WorkSpace.

Analise os requisitos para criar uma imagem personalizada do Windows ou os requisitos para criar uma imagem personalizada do Amazon Linux. A criação de imagens exige que todos os pré-requisitos sejam atendidos antes que a criação da imagem possa começar.

Para confirmar se o Windows WorkSpace atende aos requisitos de criação de imagens, recomendamos executar o Verificador de Imagem. O Image Checker realiza uma série de testes sobre WorkSpace quando uma imagem é criada e fornece orientação sobre como resolver quaisquer problemas encontrados. Para obter informações detalhadas, consulte Instalação e configuração do verificador de imagens.

Depois de WorkSpace passar em todos os testes, uma mensagem “Validação bem-sucedida” é exibida. Agora você pode criar um pacote personalizado. Caso contrário, resolva quaisquer problemas que causem falhas e avisos no teste e repita o processo de execução do Image Checker até que WorkSpace ele passe em todos os testes. Todas as falhas e avisos devem ser resolvidos antes que uma imagem possa ser criada.

Para obter mais informações, siga as dicas para resolver problemas detectados pelo Image Checker.

Solução de problemas de um Windows WorkSpace marcado como não íntegro

O WorkSpaces serviço da Amazon verifica periodicamente a integridade de um WorkSpace enviando uma solicitação de status. O WorkSpace é marcado como Não íntegro se uma resposta não for recebida do WorkSpace em tempo hábil. As causas comuns para esse problema são:

- Um aplicativo no WorkSpace está bloqueando a conexão de rede entre o WorkSpaces serviço Amazon e WorkSpace o.
- Alta utilização da CPU no WorkSpace.
- O nome do computador do WorkSpace foi alterado.
- O agente ou serviço que responde ao WorkSpaces serviço da Amazon não está em estado de execução.

As etapas de solução de problemas a seguir podem WorkSpace retornar o a um estado saudável:

- Primeiro, reinicie o a WorkSpace partir do WorkSpaces console da Amazon. Se a reinicialização WorkSpace não resolver o problema, use o RDP ou conecte-se a um Amazon Linux WorkSpace usando SSH.
- Se o WorkSpace estiver inacessível por um protocolo diferente, reconstrua-o a partir do console WorkSpace da Amazon. WorkSpaces
- Se não for possível estabelecer uma WorkSpaces conexão, verifique o seguinte:

Verifique a utilização da CPU

Use o Open Task Manager para determinar se o WorkSpace está experimentando alta utilização da CPU. Se estiver, tente qualquer uma das etapas de solução de problemas a seguir para resolver o problema:

1. Pare qualquer serviço que esteja consumindo uma grande quantidade de CPU.
2. Redimensione o WorkSpace para um tipo de computação maior do que o usado atualmente.
3. Reinicie o. WorkSpace

> **Note**
>
> Para diagnosticar a alta utilização da CPU e obter orientação se as etapas acima não resolverem o problema de alta utilização da CPU, consulte Como faço para diagnosticar a alta utilização da CPU na minha instância EC2 do Windows quando minha CPU não está limitada?

Verifique o nome do computador do WorkSpace

Se o nome do computador do espaço de trabalho foi alterado, altere-o novamente para o nome original:

1. Abra o WorkSpaces console da Amazon e, em seguida, expanda a opção Insalubre WorkSpace para mostrar detalhes.
2. Copie o nome do computador.
3. Conecte-se ao WorkSpace usando RDP.
4. Abra um prompt de comando e digite hostname para ver o nome do computador atual.
   a. Se o nome corresponder ao Nome do computador da etapa 2, vá para a próxima seção de solução de problemas.
   b. Se os nomes não corresponderem, digite sysdm.cpl para abrir as propriedades do sistema e siga as etapas restantes nesta seção.
5. Escolha Alterar e cole o Nome do computador da etapa 2.
6. Insira as credenciais do usuário do domínio, se solicitado.
7. Confirme se SkyLightWorkspaceConfigServiceestá em estado de execução
   a. Em Serviços, verifique se o WorkSpace serviço SkyLightWorkspaceConfigService está em execução. Se não estiver, inicie o serviço.

Verifique as regras de firewall

Confirme se o Firewall do Windows e qualquer firewall de terceiros em execução têm regras para permitir as seguintes portas:

- TCP de entrada na porta 4172: estabeleça a conexão de streaming.
- UDP de entrada na porta 4172: transmita a entrada do usuário.

- TCP de entrada na porta 8200: gerencie e configure o. WorkSpace
- UDP de saída na porta 55002: streaming PCoIP.

Se o firewall usar filtragem sem estado, abra as portas efêmeras 49152-65535 para permitir a comunicação de retorno.

Se o firewall usar filtragem de estado, a porta efêmera 55002 já estará aberta.

Coletando um pacote de registros de WorkSpaces suporte para depuração

Ao solucionar WorkSpaces problemas, é necessário reunir o pacote de registros do host afetado WorkSpace e do host em que o WorkSpaces cliente está instalado. Há duas categorias fundamentais de registros:

- Registros do lado do servidor: WorkSpace é o servidor nesse cenário, portanto, esses são registros que residem nele mesmo. WorkSpace
- Registros do lado do cliente: Registros no dispositivo que o usuário final está usando para se conectar ao. WorkSpace

- Somente clientes Windows e macOS gravam registros localmente.
- Clientes zero e clientes iOS não se registram.
- Os registros do Android são criptografados no armazenamento local e enviados automaticamente para a equipe de engenharia WorkSpaces do cliente. Somente essa equipe pode revisar os registros dos dispositivos Android.

Registros do lado do servidor do WSP

Todos os componentes do WSP gravam seus arquivos de log em uma das duas pastas:

- Localização principal: `C:\ProgramData\Amazon\WSP\` e `C:\ProgramData\NICE\dcv\log\`
- Local de arquivamento: `C:\ProgramData\Amazon\WSP\TRANSMITTED\`

Alterando a verbosidade do arquivo de log no Windows

Você pode configurar o nível de detalhamento do arquivo de log para Windows do WSP WorkSpaces em grande escala definindo a configuração da Política de Grupo do nível de detalhamento do log.

Para alterar a verbosidade do arquivo de log para um indivíduo WorkSpaces, configure a `h_log_verbosity_options` chave usando o Editor do Registro do Windows:

1. Abra o Editor do registro do Windows como administrador.
2. Acesse `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. Se a `WSP` chave não existir, clique com o botão direito do mouse e escolha Novo > Chave e dê um nome a ela`WSP`.
4. Acesse `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP`.
5. Se o `h_log_verbosity_options` valor não existir, clique com o botão direito do mouse e escolha Novo > DWORD e dê um nome a ele. `h_log_verbosity_options`
6. Clique no novo `h_log_verbosity_options` DWORD e altere o Valor para um dos seguintes números, dependendo do nível de detalhamento necessário:
   - 0 — Erro
   - 1 — Advertência
   - 2 — Informações
   - 3 — Depurar
7. Escolha OK e feche o Editor do Registro do Windows.
8. Reinicie WorkSpace o.

Registros do lado do servidor PCoIP

Todos os componentes do PCoIP gravam seus arquivos de log em uma das duas pastas:

- Localização principal: `C:\ProgramData\Teradici\PCoIPAgent\logs`
- Local de arquivamento: `C:\ProgramData\Teradici\logs`

Às vezes, ao AWS Support trabalhar com um problema complexo, é necessário colocar o agente do servidor PCoIP no modo de registro detalhado. Para habilitar isso:

1. Abra a seguinte chave de registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin_defaults`
2. Na `pcoip_admin_defaults` chave, crie o seguinte DWORD de 32 bits: `pcoip.event_filter_mode`
3. Defina o valor `pcoip.event_filter_mode` para “3” (Dec ou Hex).

Para referência, esses são os limites de log que podem ser definidos neste DWORD.

- 0 — (CRÍTICO)
- 1 — (ERRO)
- 2 — (INFORMAÇÕES)
- 3 — (Depuração)

Se o `pcoip_admin_default` DWORD não existir, o nível do log será, 2 por padrão. É recomendável restaurar um valor de 2 para o DWORD depois que ele não precisar mais de registros detalhados, pois eles são muito maiores e consumirão espaço em disco desnecessariamente.

WebAccess registros do lado do servidor

Para PCoIP e WSP (versão 1.0+) WorkSpaces, o cliente WorkSpaces Web Access usa o serviço STXHD. Os registros do WorkSpaces Web Access são armazenados em`C:\ProgramData\Amazon\Stxhd\Logs`.

Para o WSP (versão 2.0+) WorkSpaces, os registros do WorkSpaces Web Access são armazenados em. `C:\ProgramData\Amazon\WSP\`

Registros do lado do cliente

Esses registros vêm do WorkSpaces cliente ao qual o usuário se conecta, então os registros estão no computador do usuário final. Os locais dos arquivos de log para Windows e Mac são:

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

Para ajudar a solucionar problemas que os usuários possam enfrentar, ative o registro avançado que pode ser usado em qualquer WorkSpaces cliente da Amazon. O registro avançado é ativado para cada sessão subseqüente do cliente até que seja desativado.

1. Antes de se conectar ao WorkSpace, o usuário final deve habilitar o registro avançado para seu WorkSpaces cliente.
2. O usuário final deve então se conectar normalmente, usar o deles WorkSpace e tentar reproduzir o problema.
3. O registro em log avançado gera arquivos de log que contêm informações de diagnóstico e detalhes no nível da depuração, incluindo dados de desempenho detalhados.

Essa configuração persiste até que seja explicitamente desativada. Depois que o usuário reproduzir com êxito o problema com o login detalhado, essa configuração deverá ser desativada, pois gera arquivos de log grandes.

Coleção automatizada de pacotes de registros do lado do servidor para Windows

O `Get-WorkSpaceLogs.ps1` script é útil para reunir rapidamente um pacote de registros do lado do servidor para. AWS Support O script pode ser solicitado AWS Support solicitando-o em um caso de suporte:

1. Conecte-se ao WorkSpace usando o cliente ou usando o Remote Desktop Protocol (RDP).
2. Inicie um prompt de comando administrativo (executado como administrador).
3. Inicie o script a partir do prompt de comando com o seguinte comando:

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

4. O script cria um pacote de registros na área de trabalho do usuário.

   O script cria um arquivo zip com as seguintes pastas:

   - C — Contém os arquivos de Arquivos de Programas, Arquivos de Programas (x86) e Windows relacionados ao Skylight ProgramData, EC2Config, Teradici, Visualizador de eventos e registros do Windows (Panther e outros).

- CliXML — contém arquivos XML que podem ser importados no Powershell usando `Import-CliXML` para filtragem interativa. Consulte Import-Clixml.
- Config — Registros detalhados para cada verificação que é realizada
- ScriptLogs— Registros sobre a execução do script (não relevantes para a investigação, mas úteis para depurar o que o script faz).
- tmp — Pasta temporária (deve estar vazia).
- Traços — Captura de pacotes feita durante a coleta de registros.

Como verificar a latência na região mais próxima AWS

O site Connection Health Check verifica rapidamente se todos os serviços necessários que usam a Amazon WorkSpaces podem ser acessados. Ele também verifica o desempenho de cada AWS região em que a Amazon WorkSpaces está disponível e permite que os usuários saibam qual será a mais rápida.

Conclusão

Há uma mudança estratégica na computação do usuário final, à medida que as organizações se esforçam para ser mais ágeis, proteger melhor seus dados e ajudar seus funcionários a serem mais produtivos. Muitos dos benefícios já obtidos com a computação em nuvem também se aplicam à computação do usuário final. Ao migrar seus desktops Windows ou Linux para a AWS nuvem com a Amazon WorkSpaces, as organizações podem escalar rapidamente à medida que adicionam funcionários, melhoram sua postura de segurança mantendo os dados fora dos dispositivos e oferecem aos funcionários um desktop portátil, com acesso de qualquer lugar, usando o dispositivo de sua escolha.

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

Colaboradores

Os colaboradores deste documento incluem:

- Andrew Morgan, arquiteto de soluções de EUC, Amazon Web Services
- Don Scott, consultor sênior especializado em EUC, Amazon Web Services
- Klaus Becker, arquiteto sênior de soluções especialista em EUC, Amazon Web Services
- Naviero Magee, arquiteto de soluções principal, Amazon Web Services
- Robert Fountain, consultor especializado em EUC, Amazon Web Services
- Stephen Stetler, arquiteto sênior de soluções de EUC, Amazon Web Services

Outras fontes de leitura

Para obter informações adicionais, consulte:

- Guia de WorkSpaces administração da Amazon
- Guia do WorkSpaces desenvolvedor da Amazon
- WorkSpaces Clientes da Amazon
- Gerenciando o Amazon Linux 2 Amazon WorkSpaces com o AWS OpsWorks Puppet Enterprise
- Personalização do Amazon Linux WorkSpace
- Como melhorar a segurança do LDAP no AWS Directory Service com o LDAPS do lado do cliente
- Use o Amazon CloudWatch Events com a Amazon WorkSpaces e AWS Lambda para maior visibilidade da frota
- Como a Amazon WorkSpaces usa AWS KMS
- AWS CLI Referência de comando — WorkSpaces
- Monitorando as WorkSpaces métricas da Amazon
- Ambiente de trabalho MATE
- Solução de problemas de administração do AWS Directory Service
- Solução de problemas WorkSpaces administrativos da Amazon
- Solução de problemas de WorkSpaces clientes da Amazon
- Automatize a Amazon WorkSpaces com um portal de autoatendimento

Revisões do documento

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

Alteração	Descrição	Data
Atualização secundária	Conteúdo atualizado para AD Directory Services, recuperação de desastres/continuidade de negócios e redirecionamento entre regiões. Adicionado WorkSpaces e otimização de áudio do Amazon Connect. Pequenas atualizações na formatação.	26 de maio de 2022
Atualização secundária	Corrija o idioma não inclusivo.	6 de abril de 2022
Whitepaper atualizado	Conteúdo atualizado	24 de março de 2022
Whitepaper atualizado	Conteúdo atualizado para AWS Network Firewall, diretórios replicados MAD, YubiKey Support, Containers, WSLv1, Smart Card Support, WorkSpaces Service Quota e Trusted Devices.	20 de dezembro de 2021
Whitepaper atualizado	Conteúdo atualizado para protocolo WorkSpaces de streaming, autenticação por cartão inteligente, diagramas, implantações de clientes, seleção de dispositivos finais e acesso à web	28 de abril de 2021
Whitepaper atualizado	Conteúdo atualizado	1º de dezembro de 2020

Whitepaper atualizado	Conteúdo atualizado desde a primeira publicação e adição de novos diagramas.	1º de maio de 2020
Publicação inicial	Publicado pela primeira vez.	1 de julho de 2016

Avisos

Os clientes são responsáveis por fazer a própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas atuais de AWS produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de AWS suas afiliadas, fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “como estão” sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e obrigações de AWS seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum contrato entre AWS e seus clientes.

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

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.