Práticas recomendadas para implantação do Amazon WorkSpaces

Acesso à rede, serviços de diretório e segurança

Julho de 2016

Avisos

Este documento é fornecido apenas para fins informativos. Ele relaciona as atuais ofertas de produtos e práticas da AWS a contar da data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis por fazer sua própria avaliação independente das informações deste documento e de qualquer uso dos produtos ou serviços da AWS, cada um dos quais é fornecido “no estado em que se encontra”, sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria quaisquer garantias, representações, compromissos contratuais ou condições da AWS, suas afiliadas, seus fornecedores ou licenciadores. As responsabilidades e obrigações da AWS para com seus clientes são controladas pelos acordos com a AWS. Este documento não é parte de nenhum acordo entre a AWS e seus clientes nem o modifica de forma alguma.

Sumário

Resumo

Este whitepaper apresenta uma série de práticas recomendadas para implantação do Amazon WorkSpaces. O documento abrange considerações sobre rede, serviços de diretório e autenticação do usuário, segurança, monitoramento e registro.

Para permitir acesso mais rápido às informações pertinentes, as informações foram separadas em quatro categorias. Este documento é destinado a engenheiros de rede, engenheiros de diretório ou engenheiros de segurança.

Introdução

O Amazon WorkSpaces é um serviço de computação de desktop gerenciado na nuvem. O Amazon WorkSpaces elimina o ônus da compra e implantação de hardware e da instalação de softwares complexos, além de proporcionar uma experiência de desktop com poucos cliques no Console de Gerenciamento da AWS, usando a interface de linha de comando (CLI) da AWS ou as APIs. Com o Amazon WorkSpaces, você pode iniciar um desktop em poucos minutos, conectar-se ao software do seu desktop e acessá-lo a partir de uma rede local ou externa com segurança, confiabilidade e rapidez. Você pode:

- Aproveitar o seu Microsoft Active Directory (AD) local existente ao usar AWS Directory Service: AD Connector.
- Estender seu diretório para a Nuvem AWS.
- Construir um diretório gerenciado com o AWS Directory Service: Microsoft AD ou Simple AD, de forma a gerenciar seus usuários e WorkSpaces.

Além disso, você pode aproveitar o servidor RADIUS local ou hospedado na nuvem com o AD Connector para oferecer Multi-Factor Authentication (MFA) aos seus WorkSpaces.

É possível automatizar o provisionamento do Amazon WorkSpaces usando CLI ou API, que permite a integração do Amazon WorkSpaces aos fluxos de provisionamento existentes.

Por segurança, além da criptografia de rede integrada que o serviço WorkSpaces fornece, você também pode habilitar criptografia de dados em repouso para seus WorkSpaces (veja WorkSpaces criptografados, na seção sobre segurança).

Você pode implantar aplicações nos seus WorkSpaces usando as ferramentas locais existentes, como Microsoft System Center Configuration Manager (SCCM), ou aproveitando o Amazon WorkSpaces Application Manager (Amazon WAM).

As seções a seguir dão mais detalhes sobre o Amazon WorkSpaces, explicam como o serviço funciona, descrevem o que é necessário para iniciar o serviço e o informam quais opções e recursos estão disponíveis para seu uso.

Requisitos do WorkSpaces

O serviço Amazon WorkSpaces exige três componentes para ser implantado com êxito:

- **Aplicação WorkSpaces para o cliente**. Um dispositivo cliente compatível com o Amazon WorkSpaces. Encontre uma lista completa aqui: Supported Platforms and Devices (Dispositivos e plataformas compatíveis).

  Você também pode usar zero clients PCoIP (Personal Computer over Internet Protocol) para se conectar ao WorkSpaces. Para uma lista de dispositivos disponíveis, veja PCoIP Zero Clients for Amazon WorkSpaces (Zero clients PCoIP para Amazon WorkSpaces).

- **Um serviço de diretório para autenticar usuários e prover acesso ao WorkSpace deles**. O Amazon WorkSpaces funciona atualmente com o AWS Directory Service e com o Active Directory. Você pode usar o servidor do Active Directory local com o AWS Directory Service para embasar as credenciais existentes de usuário corporativo com WorkSpaces.

- **Um Amazon Virtual Private Cloud (Amazon VPC) no qual executar o Amazon WorkSpaces**. Você precisará de no mínimo duas sub-redes para a implantação do WorkSpaces, pois cada construção do AWS Directory Service exige duas sub-redes em uma implantação Multi-AZ.

Considerações sobre a rede

Cada WorkSpace está associado a um Amazon VPC específico e à construção do AWS 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 funcionarem, cada uma em uma zona de disponibilidade diferente. As sub-redes são permanentemente afiliadas a uma construção do Directory Service e não podem ser modificadas depois da criação do AWS Directory Service. Assim, é essencial dimensionar corretamente a sub-rede antes de criar a construção do Directory Services. Leve as seguintes questões em consideração antes de criar as sub-redes:

- De quantos WorkSpaces você precisará ao longo do tempo? Qual é o crescimento esperado?
- Que tipos de usuário você precisará acomodar?
- Quantos domínios do Active Directory você conectará?
- Onde residem suas contas de usuários corporativos?

A Amazon recomenda a definição de grupos de usuários, ou personas, com base no tipo de acesso e autenticação de usuário que você exigir como parte do processo de planejamento. Essas respostas serão úteis quando você precisar limitar o acesso a determinadas aplicações ou recursos. As personas de usuários definidas podem ajudá-lo a segmentar e restringir o acesso usando o AWS Directory Service, as listas de controle de acesso à rede, as tabelas de roteamento e os grupos de segurança do VPC. Cada construção do AWS Directory Service usa duas sub-redes e aplica as mesmas configurações a todos os WorkSpaces iniciados dessa construção. Por exemplo: você pode usar um grupo de segurança que se aplique a todos os WorkSpaces conectados a um AD Connector para especificar se a autenticação MFA é necessária ou se o usuário final pode ter acesso de administrador local ao seu WorkSpace.

> **Nota** Cada AD Connector conecta-se a uma unidade organizacional (OU) do Microsoft Active Directory. Você precisa construir seu Directory Service levando as personas de usuário em consideração, de forma que possa aproveitar esse recurso.

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

Design do VPC

Aqui estão algumas coisas a serem levadas em consideração ao projetar o VPC, as sub-redes, os grupos de segurança, as políticas de roteamento e as ACLs de rede para seu Amazon WorkSpaces, de forma que possa construir o ambiente do WorkSpaces para dimensionamento, segurança e facilidade de gerenciamento:

- **VPC**. Recomendamos usar um VPC separado específico para a implantação do WorkSpaces. Com um VPC separado, você pode especificar a governança e as proteções de segurança necessárias para o WorkSpaces, criando separação de tráfego.
- **Directory Services**. Cada construção do AWS Directory Service exige um par de sub-redes preparadas para a divisão de um serviço de diretório altamente disponível entre as zonas de disponibilidade da Amazon.
- **Tamanho da sub-rede**. As implantações do WorkSpaces são vinculadas a uma construção de diretório e residem nas mesmas sub-redes de VPC que o AWS Directory Service escolhido. Algumas considerações:
  - Os tamanhos da sub-rede são permanentes e não podem ser alterados; deixe bastante espaço para futuro crescimento.
  - Você pode especificar um grupo de segurança padrão para o AWS Directory Service escolhido; o grupo de segurança se aplica a todos os WorkSpaces associados à construção específica do AWS Directory Service.
  - Vários AWS Directory Services podem usar a mesma sub-rede.

Leve em consideração os planos futuros ao projetar seu VPC. Por exemplo: pode ser que você queira adicionar componentes de gerenciamento, como servidor antivírus, servidor de gerenciamento de patches ou servidor do Active Directory ou RADIUS com MFA. Vale a pena planejar endereços IP disponíveis adicionais no design do seu VPC para acomodar tais necessidades.

Para orientação e considerações aprofundadas de design do VPC e dimensionamento de sub-rede, veja a apresentação no evento **re:Invent** chamada How Amazon.com is Moving to Amazon WorkSpaces (Como o Amazon.com está sendo transferido para o Amazon WorkSpaces).

Interfaces de rede

Cada WorkSpace tem duas interfaces de rede elásticas (ENIs, elastic network interfaces), uma interface de rede de gerenciamento (eth0) e uma interface de rede primária (eth1). A AWS usa a interface de rede de gerenciamento para gerenciar o WorkSpace; é a interface na qual a conexão do seu cliente termina. A AWS usa um intervalo de endereços IP privados para essa interface. Para o roteamento de rede funcionar corretamente, você não pode usar esse espaço de endereços privativos em nenhuma rede que possa se comunicar com o VPC do WorkSpaces.

Para uma lista dos intervalos de IP privados que usamos em cada região, veja Amazon WorkSpaces Details (Detalhes do Amazon WorkSpaces).

> **Nota** O Amazon WorkSpaces e suas interfaces de rede de gerenciamento associadas não residem no seu VPC, e você não pode ver a interface de rede de gerenciamento nem a ID da instância do Amazon Elastic Compute Cloud (EC2) no Console de Gerenciamento da AWS (veja Figura 4, Figura 5 e Figura 6). No entanto, você pode ver e modificar as configurações do grupo de segurança da interface de rede primária (eth1) no Console de Gerenciamento da AWS. Além disso, a interface de rede primária de cada WorkSpace entra na conta dos limites de recurso do Amazon EC2 da ENI. Para grandes implantações do WorkSpaces, você precisa abrir um bilhete de suporte pelo Console de Gerenciamento da AWS para aumentar os limites da sua ENI.

Fluxo do tráfego

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

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

Na próxima seção, falaremos sobre esses dois componentes.

Dispositivo cliente para WorkSpace

O dispositivo que executa o cliente Amazon WorkSpaces, independente da localização (local ou remota), usará as mesmas duas portas para conectividade ao serviço do WorkSpaces. O cliente usa https na porta 443 para todas as informações relacionadas à autenticação e à sessão, e usa a porta 4172 (porta PCoIP) com TCP e UDP para pixel streaming a determinado WorkSpace e para verificações de integridade de rede. O tráfego nas duas portas é criptografado. O tráfego na porta 443 é usado para informações de autenticação e sessão e usa TLS para criptografar o tráfego. O tráfego de pixel streaming usa a criptografia AES de 256 bits para comunicação entre o cliente e eth0 do WorkSpace pelo gateway de streaming. Mais informações podem ser encontradas na seção Segurança, adiante neste documento.

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

O cliente Amazon WorkSpaces tem uma verificação incorporada do status de rede. Esse utilitário mostra aos usuários se a rede deles suportará uma conexão, por meio de um indicador de status na parte inferior direita da aplicação. Uma visão mais detalhada do status de rede pode ser acessada ao selecionar **Rede** no lado direito inferior do cliente, cujo resultado está exibido na Figura 1.

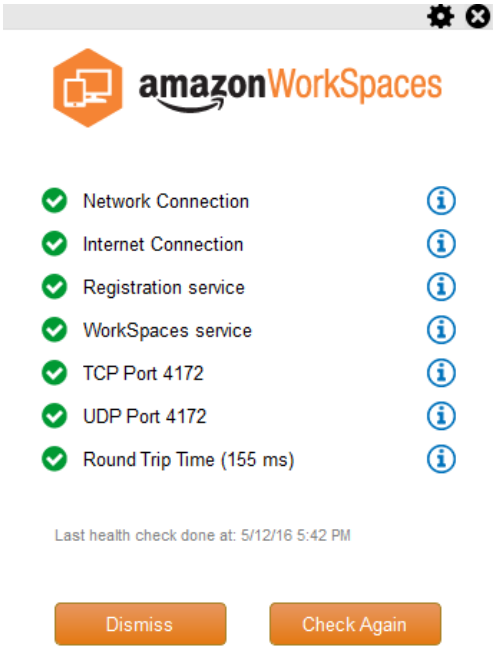

Figura 1: Cliente WorkSpaces – verificação de rede

Um usuário inicia em seu cliente uma conexão ao serviço WorkSpaces ao fornecer as informações de login para o diretório usado pela construção do Directory Service, que costuma ser o diretório corporativo. As informações de login são enviadas via https para gateways de autenticação do serviço Amazon WorkSpaces na região em que o WorkSpace está localizado. O gateway de autenticação do serviço Amazon WorkSpaces, então, encaminha o tráfego à construção do serviço específico do AWS Directory Service associada ao seu WorkSpace. Por exemplo, ao usar o AD Connector, este encaminha a solicitação de autenticação diretamente ao seu serviço do Active Directory, que poderia ser local ou em um AWS VPC (veja Cenários de implantação do AD DS). O AD Connector não armazena informações de autenticação, agindo como proxy stateless. Como resultado, é essencial que o AD Connector tenha conectividade com um servidor do Active Directory. O AD Connector determina o servidor do Active Directory ao qual está se conectando usando os servidores DNS que você pode definir ao criar o AD Connector.

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

Quando o usuário estiver autenticado, o tráfego de streaming será iniciado na porta 4172 (porta PCoIP) pelo gateway de streaming da AWS para o WorkSpace. As informações relacionadas à sessão ainda são trocadas via https durante toda a sessão. O tráfego de streaming aproveita a primeira ENI do WorkSpace (eth0 no WorkSpace) que não está conectada ao seu VPC. A conexão de rede do gateway de streaming à ENI é gerenciada pela AWS. No caso de falha de conexão dos gateways de streaming para a ENI de streaming do WorkSpaces, um evento de CloudWatch é gerado (veja a seção Monitoramento ou registro usando Amazon CloudWatch deste whitepaper).

A quantidade de dados enviada entre o serviço Amazon WorkSpaces e o cliente depende do nível de atividade de pixels. Para garantir a experiência ideal para usuários, recomendamos que o round trip time (RTT) entre o cliente WorkSpaces e a Região AWS onde seus WorkSpaces estão localizados seja inferior a 100 ms. Isso costuma significa que o cliente WorkSpaces está localizado a menos de 2000 milhas (3200 km) da Região em que o WorkSpace está hospedado. Nós fornecemos a página Connection Health Check, que você pode consultar para determinar a Região AWS ideal a que se conectar para o serviço Amazon WorkSpaces.

Serviço do Amazon WorkSpaces para VPC

Depois de a conexão ser autenticada por um cliente a um WorkSpace e o tráfego de streaming ser iniciado, o cliente WorkSpaces exibirá uma área de trabalho do Windows (seu WorkSpace) que estará conectada ao seu VPC, e sua rede deve mostrar que você estabeleceu essa conexão. A ENI principal do WorkSpace, identificada como eth1, terá um endereço IP atribuído a ela pelo serviço DHCP (Dynamic Host Configuration Protocol) que é fornecido pelo seu VPC, normalmente das mesmas sub-redes que o AWS Directory Service. O endereço IP permanece com o WorkSpace durante toda a vida do WorkSpace. A ENI que está no seu VPC tem acesso a qualquer recurso do VPC e a qualquer rede à qual você tenha conectado seu VPC (via VPC peering, conexão com AWS Direct Connect ou conexão com VPN).

O acesso da ENI aos recursos da sua rede é determinado pelo grupo de segurança padrão (veja mais sobre grupos de segurança aqui) que seu AWS Directory Service configura para cada WorkSpace e todos os grupos de segurança adicionais atribuídos à ENI. Você pode adicionar grupos de segurança à ENI voltados paro seu VPC à vontade, aproveitando a CLI ou o Console de Gerenciamento da AWS. Além dos grupos de segurança, você pode usar o firewall preferido baseado em host em determinado WorkSpace para limitar o acesso de rede aos recursos dentro do VPC.

A Figura 4, em Cenários de implantação do AD DS, mais adiante neste whitepaper, mostra o fluxo de tráfego descrito anteriormente.

Exemplo de uma configuração típica

Vamos considerar um cenário no qual você tenha dois tipos de usuários e que o AWS Directory Service usa um Active Directory centralizado para autenticação do usuário:

- **Trabalhadores que precisam de acesso total e de qualquer lugar** (por exemplo, funcionários em tempo integral). Esses usuários terão acesso total à Internet e à rede interna, e atravessarão um firewall pelo VPC na rede local.
- **Trabalhadores que devem ter somente acesso restrito de dentro da rede corporativa** (por exemplo, prestadores de serviços e consultores). Esses usuários restringiram o acesso à Internet por um servidor de proxy (a sites específicos) no VPC e terão acesso de rede limitado no VPC e à rede local.

Você gostaria de dar aos funcionários em tempo integral a possibilidade de acesso de administrador local no WorkSpace para instalar software, e gostaria de impor autenticação bifatorial com MFA. Você também quer permitir que funcionários em tempo integral acessem a Internet sem interrupções pelo WorkSpace.

Para prestadores de serviço, você quer bloquear acesso admin local, para que eles possam usar somente as aplicações específicas pré-instaladas. Você quer aplicar controles de acesso muito restritos à rede via grupos de segurança para esses WorkSpaces. Você precisa abrir as portas 80 e 443 somente para sites internos específicos e gostaria de bloquear o acesso à Internet.

Nesse cenário, existem dois tipos completamente diferentes de personas de usuário, com diferentes requisitos para acesso à rede e ao desktop. A prática recomendada é gerenciar e configurar os WorkSpaces de um jeito diferente. Para isso, você precisará criar dois AD Connectors, um para a persona de cada usuário. Cada AD Connector exige duas sub-redes que precisam de endereços IP suficientes para atender às estimativas de crescimento de uso do WorkSpaces.

> **Nota** Cada sub-rede do 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 persistir.

As outras considerações para esse cenário são as seguintes:

- As sub-redes do AWS VPC devem ser privadas, de forma que o tráfego, como acesso à Internet, possa ser controlado por gateway NAT, servidor Proxy-NAT na nuvem ou roteadas de volta para o sistema de gerenciamento de tráfego local.
- O firewall está posicionado para todo o tráfego de VPC destinado à rede local.
- O servidor do Microsoft Active Directory e os servidores RADIUS com MFA são locais (veja Cenário 1: Usar o AD Connector para enviar por proxy a autenticação ao AD DS local) ou parte da implementação da Nuvem AWS (veja os Cenários 2 e 3, Cenários de implantação do AD DS).

Como todos os WorkSpaces receberão alguma forma de acesso à Internet, e como eles estarão hospedados em uma sub-rede privada, você também precisará criar sub-redes públicas que possam acessar a Internet por meio de um gateway de Internet. Você precisará de um gateway NAT para os funcionários em tempo integral, permitindo que eles acessem a internet, e um servidor Proxy-NAT para os consultores e prestadores de serviço, para limitar o acesso por eles a sites internos específicos. Para planejar-se para falhas, projetar para alta disponibilidade ou limitar cobranças de tráfego entre zonas de disponibilidade, você precisa ter dois gateways NAT e servidores NAT ou proxy em duas sub-redes diferentes em uma implantação Multi-AZ. As duas AZs que você selecionar como

sub-redes públicas corresponderão às duas AZs que você usar para as sub-redes do WorkSpaces nas regiões com mais de duas AZs. Você pode encaminhar todo o tráfego de cada AZ do WorkSpaces para a sub-rede pública correspondente para limitar as cobranças de tráfego entre zonas de disponibilidade e facilitar o gerenciamento. A Figura 2 mostra a configuração do VPC.

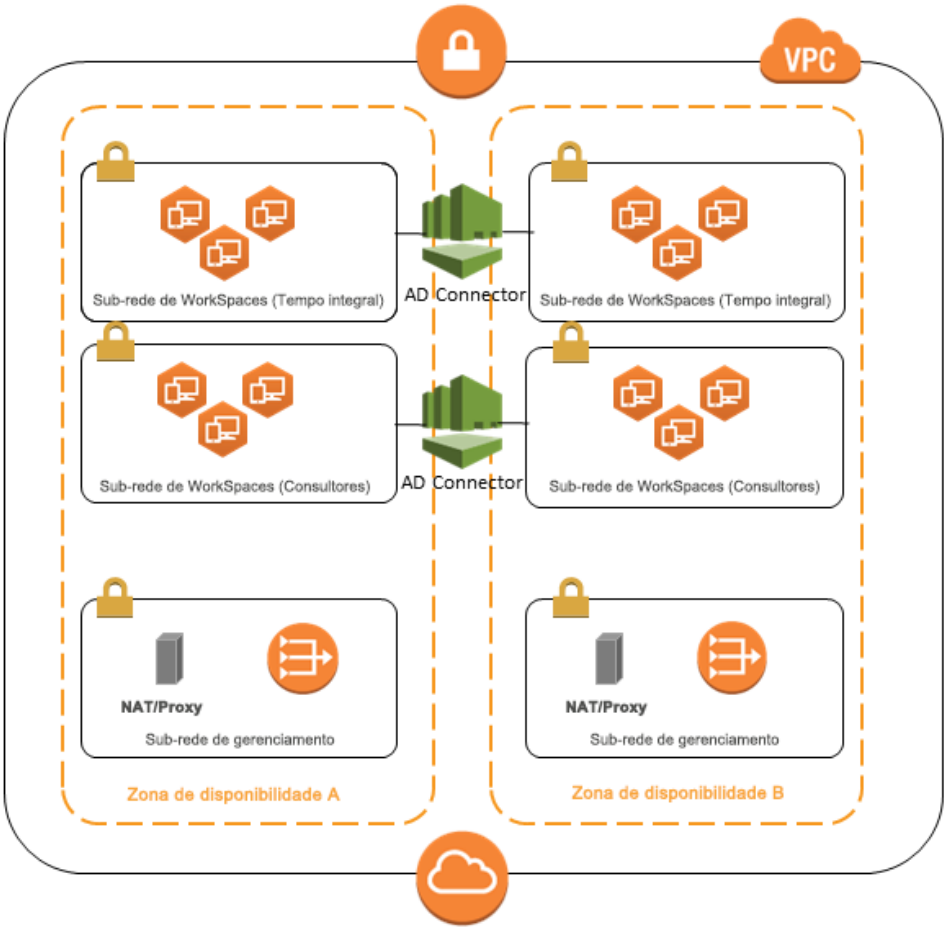

Figura 2: Design de VPC de alto nível

As informações a seguir descrevem como configurar os dois tipos diferentes de WorkSpaces descritos anteriormente.

- **Funcionários em tempo integral:** No Console de Gerenciamento do Amazon WorkSpaces, selecione a opção **Diretórios** na barra de menus, selecione o diretório onde estão os funcionários de tempo integral e selecione **Configuração do administrador local**. Ao habilitar essa opção, todos os WorkSpaces recém-criados terão privilégios do administrador local. Para conceder acesso à Internet, configure a Network Address Translation (NAT) para acesso à Internet de saída a partir do seu VPC. Para habilitar MFA, você precisa especificar um servidor RADIUS, IPs do servidor, portas e chave pré-compartilhada.

  Para WorkSpaces de funcionários em tempo real, o tráfego de entrada ao WorkSpace seria limitado ao Remote Desktop Protocol (RDP) da sub-rede do Helpdesk ao aplicar um grupo de segurança padrão via configurações do AD Connector.

- **Prestadores de serviço e consultores:** No Console de Gerenciamento do Amazon WorkSpaces, desabilite o **Acesso à Internet** e a **Configuração admin local**. Em seguida, adicione um grupo de segurança sob a configuração **Grupo de segurança** para forçar um grupo de segurança para todos os novos WorkSpaces criados sob esse diretório.

  Para os WorkSpaces dos consultores, limite o tráfego de saída e de entrada aos WorkSpaces aplicando um grupo de segurança padrão via configurações do AD Connector a todos os WorkSpaces associados a tal AD Connector. O grupo de segurança evitaria acesso de saída dos WorkSpaces a qualquer coisa além do tráfego HTTP e HTTPS e tráfego de entrada a RDP pela sub-rede do Helpdesk na rede local.

> **Nota** O grupo de segurança se aplica somente à ENI que está no VPC (eth1 no WorkSpace) e acesso ao WorkSpace pelo cliente WorkSpaces não é restrito como resultado de um grupo de segurança. A Figura 3 mostra o design do VPC do WorkSpaces descrito anteriormente.

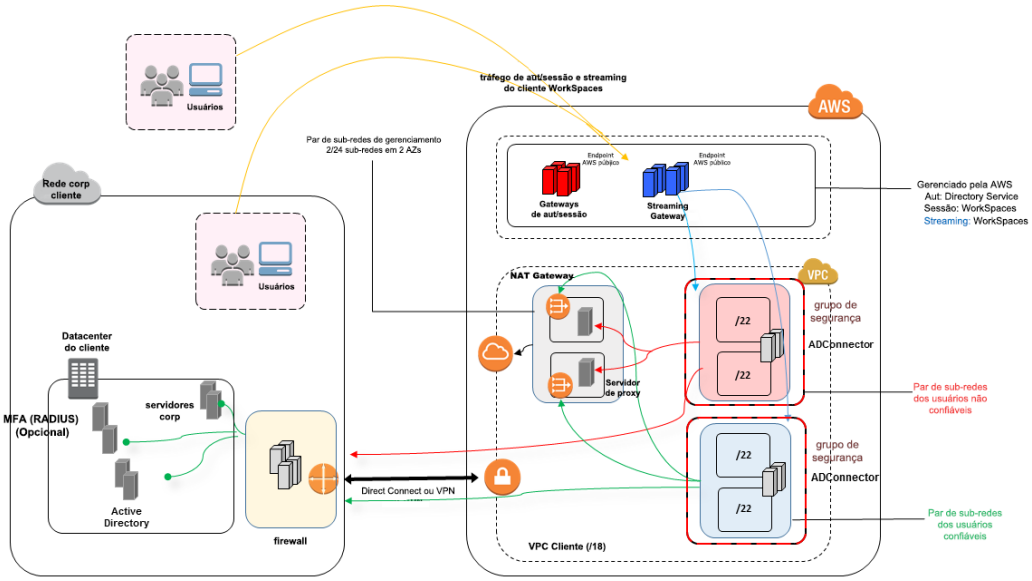

Figura 3: Design do WorkSpaces com personas de usuários

AWS Directory Service

Conforme mencionado na Introdução, o Amazon WorkSpaces tem como base o AWS Directory Service. Com o AWS Directory Service, você pode criar três tipos de diretório. Os dois primeiros moram na Nuvem AWS:

- AWS Directory Service para Microsoft Active Directory (Enterprise Edition), ou **Microsoft AD**, que é gerenciado pelo Microsoft Active Directory, alimentado pelo Windows Server 2012 R2.
- **Simple AD**, um Directory Service gerenciado, independente e compatível com Microsoft Active Directory alimentado por Samba 4.

O terceiro, **AD Connector,** é um gateway de diretório que lhe permite agir como proxy das solicitações de autenticação e buscas de usuário ou grupo no Microsoft Active Directory local existente.

A seção a seguir descreve os fluxos de comunicação para autenticação entre o serviço de corretagem do Amazon WorkSpaces e o AWS Directory Service, práticas recomendadas para implementar o WorkSpaces com o AWS Directory Service e conceitos avançados, como MFA. Nós também debatemos conceitos de arquitetura de infraestrutura para Amazon WorkSpaces em escala, requisitos do Amazon VPC, e AWS Directory Service, inclusive integração com o Microsoft Active Directory Domain Services (AD DS) local.

Cenários de implantação do AD DS

Na base do Amazon WorkSpaces está o AWS Directory Service, e o design e a implantação corretos do serviço de diretório são essenciais. Os três cenários a seguir se baseiam no guia de início rápido do *Microsoft Active Directory Domain Services*, detalhando as opções de implantação de práticas recomendadas para AD DS, especificamente para integração com WorkSpaces. A seção *Considerações sobre design* deste capítulo versa sobre requisitos específicos e práticas recomendadas do uso do AD Connector para WorkSpaces, que é parte integral do conceito do design do WorkSpaces como um todo.

- **Cenário 1: Usar o AD Connector para enviar por proxy a autenticação ao AD DS local.** Neste cenário, a conectividade de rede (VPN/Direct Connect (DX)) está no lugar para o cliente, com toda a autenticação passando via AWS Directory Service (AD Connector) ao AD DS local do cliente.
- **Cenário 2: Estender o AD DS local ao AWS (réplica).** Este cenário é semelhante ao cenário 1, mas aqui uma réplica do AD DS do cliente é implantada no AWS em combinação com o AD Connector, reduzindo a latência das requisições de autenticação/consulta ao AD DS e ao catálogo global de AD DS.
- **Cenário 3: Implantação isolada independente usando AWS Directory Service na Nuvem AWS.** Este é um cenário isolado e não inclui conectividade de volta ao cliente para autenticação. Essa abordagem usa o AWS Directory Service (Microsoft AD) e o AD Connector. Embora esse cenário não dependa da conectividade ao cliente para autenticação, não faz provisionamento para tráfego de aplicações quando necessário sobre VPN ou DX.

Cenário 1: Usar o AD Connector para enviar por proxy a autenticação ao AD DS local

Esse cenário é para clientes que não querem ampliar o AD DS local para AWS ou quando uma nova implantação de AD DS não for uma opção. A Figura 4: AD Connector ao Active Directory local descreve em alto nível cada um dos componentes e mostra o fluxo de autenticação de usuários.

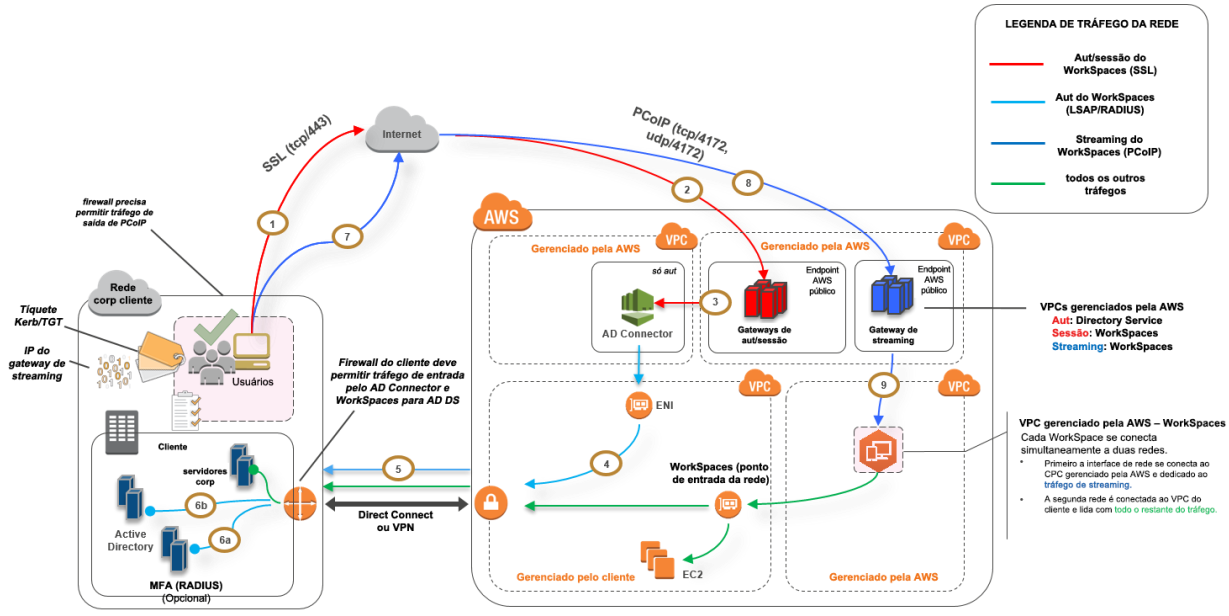

Figura 4: AD Connector ao Active Directory local

Neste cenário, o AWS Directory Service (AD Connector) é usado por todos os usuários ou autenticação via MFA que passa por proxy AD Connector ao AD DS local do cliente (Figura 5). Para detalhes sobre os protocolos ou criptografia usadas para processo de autenticação, veja a seção Segurança deste whitepaper.

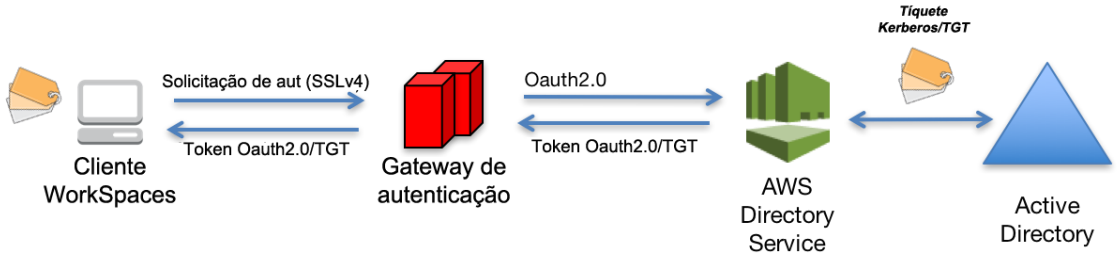

Figura 5: Autenticação do usuário via gateway de autenticação

O Cenário 1 mostra uma arquitetura híbrida na qual o cliente já pode ter recursos no AWS, além de recursos em um datacenter local que possa ser acessado via WorkSpaces. O cliente pode aproveitar o AD DS local existente e os servidores RADIUS para autenticação de usuário e MFA.

Esta arquitetura usa os componentes ou construções a seguir.

Amazon Web Services:

- **Amazon VPC:** Criação de um Amazon VPC com pelo menos duas sub-redes privadas entre duas zonas de disponibilidade.
- **Conjunto de opções de DHCP:** Criação de um conjunto de opções de DHCP do Amazon VPC. Isso permite que o nome de domínio especificado pelo cliente e Domain Name Servers (DNS) (serviços locais) seja definido. (Para obter mais informações veja DHCP Options Sets [Conjunto de opções de DHCP].)
- **Gateway privado virtual da Amazon:** Habilita comunicação com sua própria rede sobre um túnel VPN IPsec ou uma conexão com AWS Direct Connect.
- **AWS Directory Service**: O AD Connector é implantado em um par de sub-redes privadas do Amazon VPC.
- **Amazon WorkSpaces:** Os WorkSpaces são implantados nas mesmas sub-redes privadas que o AD Connector (veja Considerações sobre design, AD Connector).

Cliente:

- **Conectividade de rede:** endpoints do Direct Connect ou VPN corporativa.
- **AD DS:** AD DS corporativo.
- **MFA (opcional):** servidor RADIUS corporativo.
- **Dispositivos do usuário final:** dispositivos de usuário final corporativos ou BYOL (como Windows, Mac, iPad ou tablets Android, zero clients, Chromebook), usados para acessar o serviço Amazon WorkSpaces (veja Supported Platforms and Devices [Dispositivos e plataformas compatíveis]).

Embora essa solução seja ótima para clientes que não queiram implantar AD DS na nuvem, ela reserva algumas ciladas.

- **Dependência da conectividade:** Se a conectividade com o datacenter for perdida, nenhum usuário poderá fazer login nos respectivos WorkSpaces e as conexões existentes continuarão ativas durante toda a vida do Kerberos/TGT.

- **Latência:** Se existir latência via conexão (esse é mais o caso com VPN que com DX), a autenticação do WorkSpaces e alguma atividade relacionada a AD DS, como aplicação de Group Policy (GPO), levarão mais tempo.
- **Custos do tráfego:** Toda a autenticação deve atravessar o link de VPN ou DX, por isso depende do tipo de conexão. Tal conexão é transferência de dados para fora do Amazon EC2 para internet ou transferência de dados para fora (DX).

> **Nota** O AD Connector é um serviço de proxy. Ele não armazena nem coloca em cache as credenciais do usuário. O que ele faz é manusear todos os requisitos de autenticação, busca e gerenciamentos pelo seu Active Directory. Seu serviço de diretório precisa ter uma conta com privilégios de delegação com direito de ler todas as informações do usuário e integrar um computador ao domínio.

Para obter detalhes sobre como configurar um usuário no seu diretório para o AD Connector, veja Delegating Connect Privileges (Como delegar privilégios de conexão).

No geral, a experiência com o WorkSpaces é altamente dependente do item 5 exibido na Figura 4.

Cenário 2: Estender o AD DS local ao AWS (réplica).

Este cenário é semelhante ao cenário 1, mas no cenário 2 uma réplica do AD DS do cliente é implantada no AWS em combinação com o AD Connector. Isso reduz a latência da autenticação ou os requisitos de consulta ao AD DS. A Figura 6 mostra uma visão de alto nível de cada um dos componentes e do fluxo de autenticação do usuário.

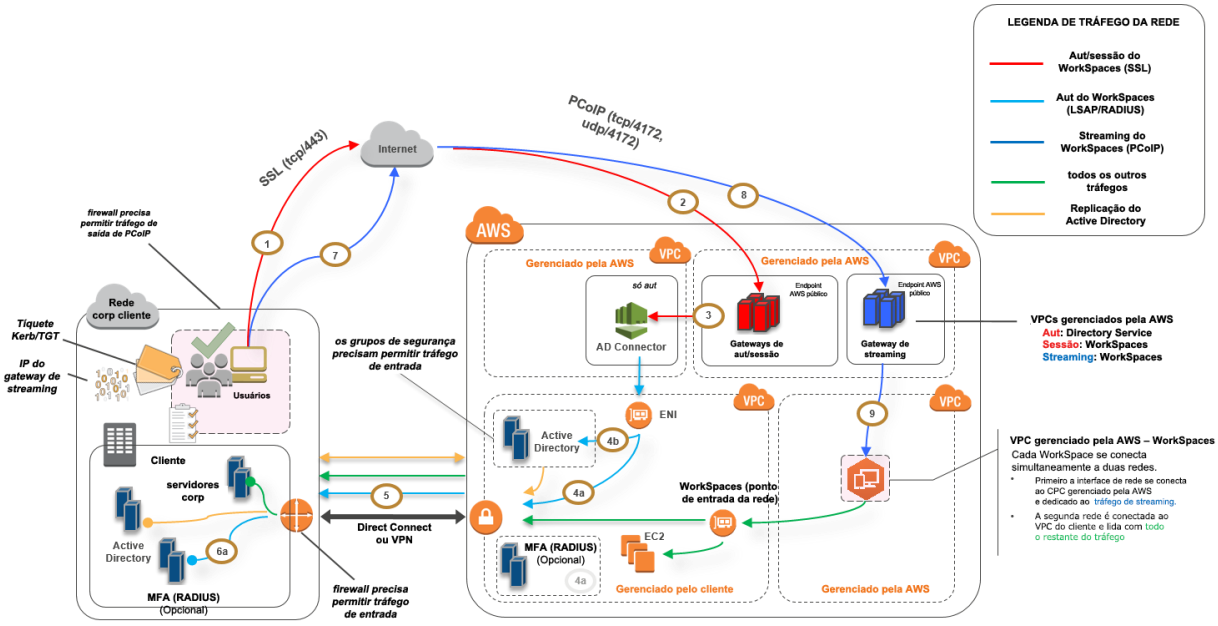

Figura 6: Estenda o domínio do Active Directory para a nuvem

Como no cenário 1, o AD Connector é usado para todos os usuários ou autenticação via MFA, o que é enviado por proxy para o AD DS do cliente (Figura 5). No cenário 2, o AD DS do cliente é implantando nas zonas de disponibilidade das instâncias do Amazon EC2 que são promovidas para serem controladores de domínio na floresta Active Directory local do cliente, executando na Nuvem AWS. Cada controlador de domínio é implantado nas sub-redes privadas do VPC para deixar o AD DS altamente disponível na Nuvem AWS. Para práticas recomendadas para implantar AD DS na Nuvem AWS, veja Considerações sobre o design, ainda neste whitepaper.

Quando as instâncias do WorkSpaces forem implantadas, elas precisarão acessar os controladores do domínio baseados na nuvem para serviços de diretório seguros, de baixa latência e DNS. Todo o tráfego de rede, inclusive comunicação AD DS, solicitações de autenticação e replicação do Active Directory são garantidos dentro das sub-redes privadas ou entre o túnel de VPN do cliente ou DX.

Essa arquitetura usa os componentes ou construções a seguir.

Amazon Web Services:

- **Amazon VPC:** Criação de um Amazon VPC com pelo menos quatro sub-redes privadas em duas zonas de disponibilidade (duas para o AD DS do cliente, duas para o AD Connector ou para os WorkSpaces).
- **Conjunto de opções de DHCP:** Criação de um conjunto de opções de DHCP do Amazon VPC. Assim, você pode definir um nome de domínio especificado pelo cliente e pelos DNSs (AD DS local). Para obter mais informações veja DHCP Options Sets (Conjuntos de opções de DHCP).
- **Gateway privado virtual da Amazon:** Habilita comunicação com sua própria rede sobre um túnel VPN IPsec ou uma conexão com 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 "opcionais" do cliente para MFA.
- **AWS Directory Service**: O AD Connector é implantado em um par de sub-redes privadas do Amazon VPC.
- **Amazon WorkSpaces:** Os WorkSpaces são implantados nas mesmas sub-redes privadas que o AD Connector (veja Considerações sobre design, AD Connector).

Cliente:

- **Conectividade de rede:** VPN corporativa ou endpoints do AWS Direct Connect.
- **AD DS:** AD DS corporativo (exigido para replicação).
- **MFA "opcional":** servidor RADIUS corporativo.
- **Dispositivos do usuário final:** dispositivos de usuário final corporativos ou BYOL (como Windows, Mac, iPad ou tablets Android, zero clients, Chromebook), usados para acessar o serviço Amazon WorkSpaces (veja Supported Platforms and Devices [Dispositivos e plataformas compatíveis]).

Ao contrário do cenário 1, esta solução não traz as mesmas ciladas. Portanto, os WorkSpaces e o AWS Directory Service não dependem da existência de conectividade.

- **Dependência da conectividade:** Se a conectividade com o datacenter do cliente for perdida, os usuários finais poderão continuar a trabalhar, pois a autenticação e a MFA "opcional" são processadas localmente.
- **Latência:** Com exceção do tráfego de replicação (veja *Considerações sobre design:* Sites e serviços de AD DS), toda autenticação é local e de baixa latência.
- **Custos de tráfego:** Neste cenário, a autenticação é local, com apenas replicação AD DS tendo que cruzar a ligação via VPN ou DX, o que reduz a transferência de dados.

No geral, a experiência com o WorkSpaces é melhor e não é altamente dependente do item 5, exibido na Figura 6. Esse é ainda mais o caso quando você quer escalar o WorkSpaces para milhares de desktops, especialmente em relação às consultas do catálogo global de AD DS, pois esse tráfego continua sendo local ao ambiente do WorkSpaces.

Cenário 3: Implantação isolada independente usando AWS Directory Service na Nuvem AWS

Esse cenário, exibido na Figura 7, tem AD DS implantado na Nuvem AWS em um ambiente isolado independente. O AWS Directory Service é usado exclusivamente neste cenário. Em vez de gerenciar totalmente o AD DS sozinho, você usa o AWS Directory Service para tarefas como construir uma topologia de diretório altamente disponível, monitorar controladores de domínio e configurar backups e snapshots.

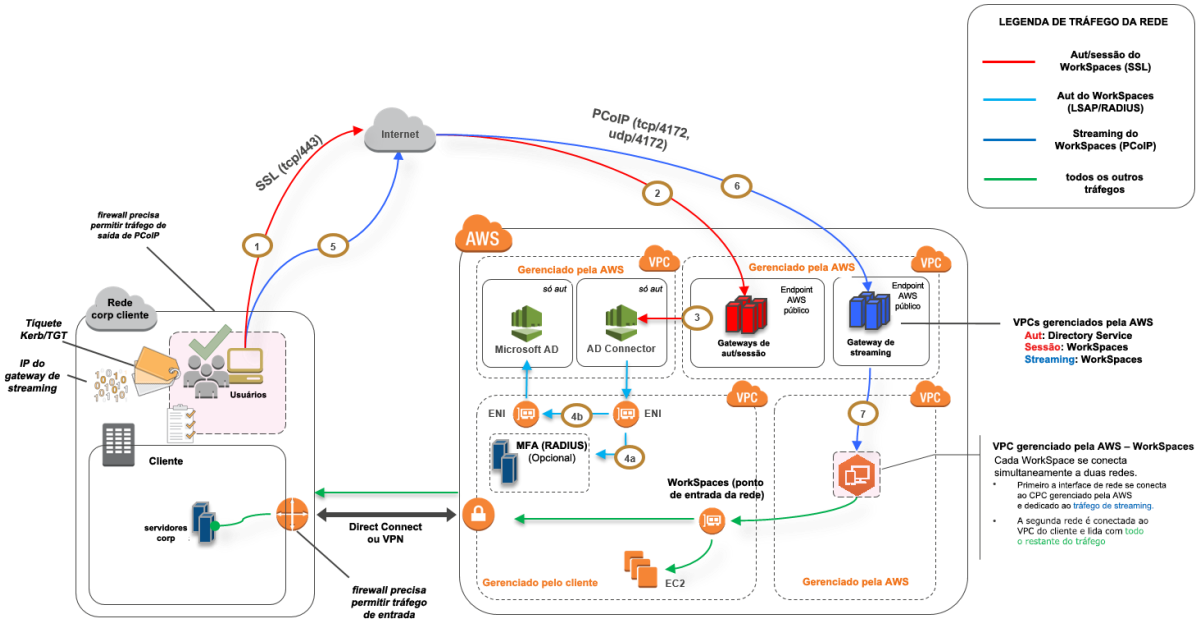

Figura 7: Somente nuvem – AWS Directory Services (Microsoft AD)

Como no cenário 2, o AD DS (Microsoft AD) é implantado em sub-redes dedicadas que cobrem duas zonas de disponibilidade, tornando o AD DS altamente disponível na Nuvem AWS. Além do Microsoft AD, o AD Connector (em todos os três cenários) é implantado para autenticação do WorkSpaces ou via MFA. Isso garante separação das funções ou da função dentro do Amazon VPC, que é uma prática recomendada padrão (veja a seção *Considerações sobre design*: Rede particionada).

O cenário 3 é uma configuração "all-in" padrão que funciona bem para clientes que querem que o AWS gerencie implantação, patches, alta disponibilidade e monitoramento do AWS Directory Service. Por conta do modo de isolamento, além de produção, o cenário também funciona bem para provas de conceito e ambientes laboratoriais.

Além do posicionamento do AWS Directory Service, a Figura 7 mostra o fluxo do tráfego de um usuário para um WorkSpace e como este interage com o servidor AD e o servidor MFA.

Esta arquitetura usa os componentes ou construções a seguir.

Amazon Web Services:

- **Amazon VPC:** Criação de um Amazon VPC com pelo menos quatro sub-redes privadas em duas zonas de disponibilidade (duas para o AD DS do *Microsoft AD*, duas para o AD Connector ou para os WorkSpaces). "*Separação de funções*."
- **Conjunto de opções de DHCP:** Criação de um conjunto de opções de DHCP do Amazon VPC. Assim, você pode definir um nome de domínio especificado pelo cliente e DNSs (Microsoft AD). Para obter mais informações veja DHCP Options Sets (Conjuntos de opções de DHCP).
- **Opcional: gateway privado virtual da Amazon:** Habilita comunicação com sua própria rede sobre um túnel VPN IPsec (VPN) ou uma conexão com AWS Direct Connect. Use para acessar sistemas de back-end locais.
- **AWS Directory Service:** Microsoft AD implantado em um par dedicado de sub-redes de VPC (Serviço gerenciado de AD DS).
- **Amazon EC2:** Servidores RADIUS "opcionais" do cliente para MFA.
- **AWS Directory Service**: O AD Connector é implantado em um par de sub-redes privadas do Amazon VPC.
- **Amazon WorkSpaces:** Os WorkSpaces são implantados nas mesmas sub-redes privadas que o AD Connector (veja Considerações sobre design, AD Connector).

Cliente:

- **Opcional: conectividade de rede:** endpoints do AWS Direct Connect ou VPN corporativa.
- **Dispositivos do usuário final:** dispositivos de usuário final corporativos ou BYOL (como Windows, Mac, iPad ou tablets Android, zero clients, Chromebook), usados para acessar o serviço Amazon WorkSpaces (veja Supported Platforms and Devices [Dispositivos e plataformas compatíveis]).

Assim como no cenário 2, esta solução não tem problemas com dependência de conectividade em relação ao datacenter local do cliente, latência ou custos de transferência externa de dados (exceto quando o acesso à Internet for habilitado para o WorkSpaces de dentro do VPC), pois, por design, este é um cenário isolado ou somente de nuvem.

Considerações sobre design

Uma implantação de AD DS funcional na Nuvem AWS exige uma boa compreensão dos conceitos de Active Directory e dos serviços específicos da AWS. Nesta seção, veremos as principais considerações de design ao implantar o AD DS para WorkSpaces, práticas recomendadas de VPC para AWS Directory Service, requisitos de DHCP e DNS, especificidades do AD Connector e sites e serviços do Active Directory.

Design do VPC

Conforme falamos na seção Considerações de rede deste documento e documentado anteriormente para os cenários 2 e 3, você deve implantar o AD DS na Nuvem AWS em um par dedicado de sub-redes privadas, entre duas zonas de disponibilidade, e separados das sub-redes AD Connector ou WorkSpaces. Essa construção oferece acesso altamente disponível e de baixa latência a serviços de AD DS para WorkSpaces, ao mesmo tempo mantendo as práticas recomendadas padrão de separação de funções ou papéis dentro do Amazon VPC.

A Figura 8 mostra a separação de AD DS e AD Connector em sub-redes privadas dedicadas (cenário 3). Neste exemplo, todos os serviços residem no mesmo Amazon VPC.

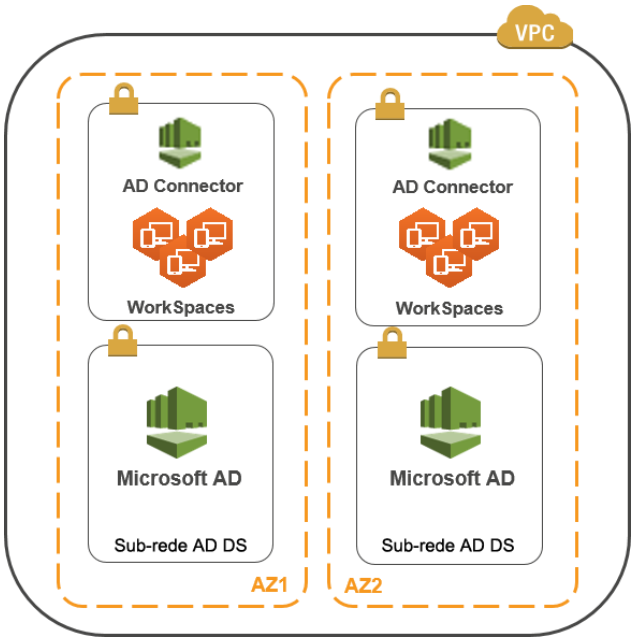

Figura 8: Segregação da rede AD DS

A Figura 9 mostra um design parecido com o cenário 1, mas nesse cenário, a parte local reside em um Amazon VPC dedicado.

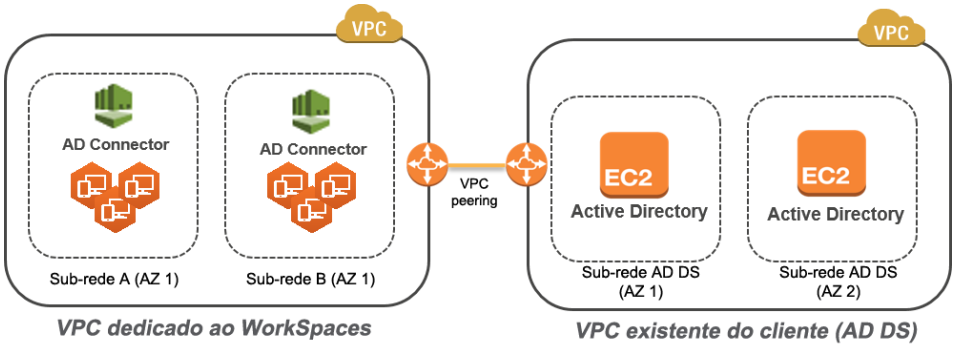

Figura 9: VPC dedicado do WorkSpaces

> **Nota** Para clientes com uma implantação existente do AWS na qual está sendo usado AD DS, recomendamos localizar seus WorkSpaces em um VPC dedicado e que você use VPC peering para comunicações AD DS.

Além da criação de sub-redes privadas dedicadas para AD DS, controladores de domínio e servidores de membros exigem várias regras de grupo de segurança para permitir tráfego para serviços, como replicação AD DS, autenticação do usuário, serviços Windows Time e Distributed File System (DFS).

> **Nota** A prática recomendada é restringir as regras do grupo de segurança necessárias às sub-redes privadas dos WorkSpaces e, no caso do cenário 2, levar em conta comunicações AD DS bidirecionais locais de/para a Nuvem AWS, conforme exibido na tabela a seguir.

Protocolo	Porta	Uso	Destino
tcp	53, 88, 135, 139, 389, 445, 464, 636	Aut (primário)	Active Directory (datacenter privado ou EC2)*
tcp	49152 – 65535	Portas altas RPC	Active Directory (datacenter privado ou EC2)*
tcp	3268-3269	Confiança	Active Directory (datacenter privado ou EC2)*
tcp	9389	Remote Microsoft Windows PowerShell (opcional)	Active Directory (datacenter privado ou EC2)*
udp	53, 88, 123, 137, 138, 389, 445, 464	Aut (primário)	Active Directory (datacenter privado ou EC2)*
udp	1812	Aut (MFA) (opcional)	RADIUS (datacenter privado ou EC2)*

* Veja Requisitos da porta do Active Directory e dos serviços de domínio do Active Directory

**Veja Visão geral do serviço e requisitos de porta de rede para o Windows

Para orientações passo a passo para implementar as regras, veja Adding Rules to a Security Group (Como adicionar regras a um grupo de segurança) no *Amazon Elastic Compute Cloud User Guide* (Guia do usuário do Amazon Elastic Compute Cloud).

Design do VPC: DHCP e DNS

Com um Amazon VPC, os serviços DHCP são fornecidos por padrão para suas instâncias. Por padrão, todo VPC fornece um servidor DNS interno acessível via espaço do endereço Classless Inter-Domain Routing (CIDR) +2 e é atribuído a todas as instâncias por um conjunto de opções de DHCP padrão.

Os conjuntos de opção do DHCP são usados dentro de um Amazon VPC para definir opções de escopo, como nome do domínio ou servidores de nome que deveriam ser enviados às suas instâncias via DHCP. A funcionalidade correta dos serviços Windows dentro do seu VPC depende dessa opção do escopo de DHCP, então você precisa defini-la corretamente. Em cada um dos cenários definidos anteriormente, você criaria e atribuiria seu próprio escopo que define o nome de domínio e os servidores de nome. Isso garante que instâncias do Windows integradas por domínio ou WorkSpaces sejam configurados para usar o DNS do Active Directory. A tabela a seguir é um exemplo de um conjunto personalizado de opções de escopo do DHCP que devem ser criadas para WorkSpaces e AWS Directory Services funcionarem corretamente.

Parâmetro	Valor
Tag de nome	Cria um tag com chave = **nome** e **valor** definido a uma string específica Exemplo: exampleco.com
Nome do domínio	exampleco.com
Domain Name Servers	Endereço do servidor DNS, separado por vírgulas Exemplo: 10.0.0.10, 10.0.1.10
Servidores NTP	Deixe este campo em branco
NetBIOS Name Servers	Insira os mesmos IPs separados por vírgula segundo os Domain Name Servers Exemplo: 10.0.0.10, 10.0.1.10
Tipo de nó NetBIOS	2

Para obter detalhes sobre a criação de um conjunto de opções de DHCP personalizado e associá-lo ao Amazon VPC, veja Working with DHCP Options Sets (Como trabalhar com conjuntos de opções de DHCP) no *Amazon Virtual Private Cloud User Guide* (Guia do usuário do Amazon Virtual Private Cloud).

No cenário 1, o escopo do DHCP seria DNS ou AD DS local. No entanto, no cenário 2 ou 3, isso seria o serviço de diretório implantado localmente (AD DS no Amazon EC2 ou AWS Directory Services: Microsoft AD). Recomendamos que você torne cada controlador de domínio que reside na Nuvem AWS um catálogo global e servidor DNS Directory Integrated.

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 Active Directory entre os controladores de domínio dentro do mesmo site e entre limites do site. No cenário 2, pelo menos dois sites estão presentes, local e AWS WorkSpaces na nuvem. Definir a topologia correta do site garante afinidade do cliente, o que significa que os clientes (neste caso, WorkSpaces) usem o controlador de domínio local preferido.

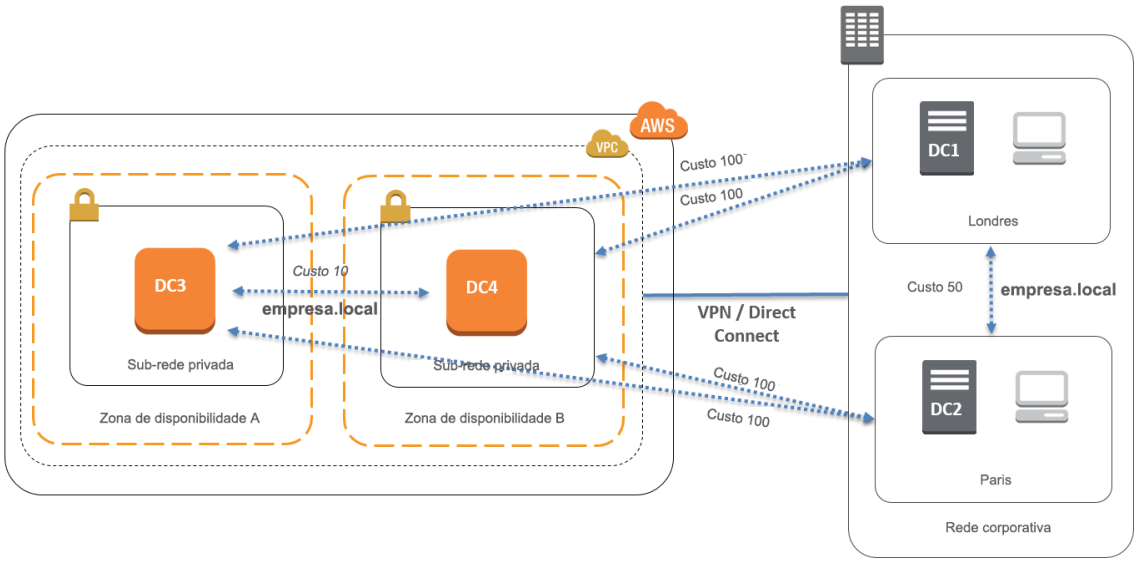

Figura 10: Sites e serviços do Active Directory: afinidade de cliente

Prática recomendada Defina o alto custo para links do site entre seu AD DS local e a Nuvem AWS. A Figura 10 é um exemplo do que custa atribuir os links do site (custo 100) para garantir afinidade de cliente independente de site.

Essas associações ajudam a garantir que o tráfego – como replicação AD DS e autenticação de cliente – usam o caminho mais eficiente para um controlador de domínio. No caso dos cenários 2 e 3, ajuda a garantir latência mais baixa e tráfego entre links.

Multi-Factor Authentication (MFA)

A implementação de MFA exige que a infraestrutura do WorkSpaces use o AD Connector como AWS Directory Service e tenha servidor RADIUS. Embora este documento não discuta a implantação de um servidor RADIUS, a seção anterior, Cenários de implantação do AD DS, detalha o posicionamento do RADIUS dentro de cada cenário.

MFA – Two-Factor Authentication

O Amazon WorkSpaces é compatível com MFA pelo AWS Directory Service: AD Connector e um servidor RADIUS *de propriedade do cliente*. Uma vez habilitado, os usuários precisam fornecer **Nome de usuário**, **Senha** e **Código MFA** ao cliente WorkSpaces para autenticação a seus respectivos desktops do WorkSpaces.

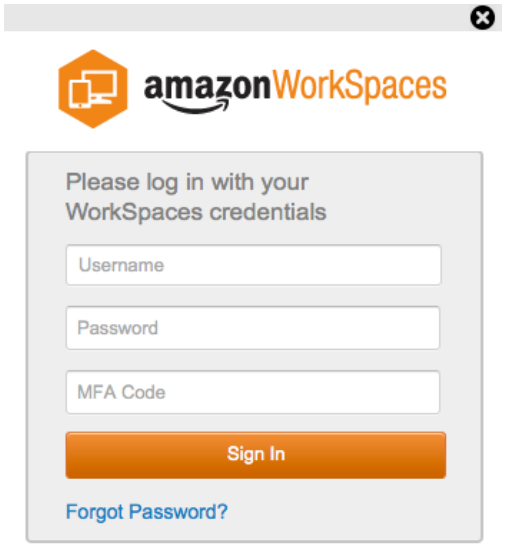

Figura 11: Cliente WorkSpaces com MFA habilitado

> **Regra rígida** A implementação de autenticação via MFA exige o uso do AD Connector. O AD Connector não é compatível com MFA "por usuário" seletiva, pois é uma configuração global por AD Connector. Se você exigir uma MFA seletiva "por usuário", é preciso separar usuários por AD Connector.

O MFA do WorkSpaces exige um ou mais servidores RADIUS. Normalmente, estas são as soluções existentes – como por exemplo RSA ou os servidores podem ser implantados dentro do seu VPC (veja Cenários de implantação do AD DS). Se você estiver implementando uma nova solução RADIUS, existem várias implementações na indústria atualmente, como FreeRADIUS e serviços de nuvem como Duo Security.

Para obter uma lista de pré-requisitos para implementar MFA com Amazon WorkSpaces, veja o *Amazon WorkSpaces Administration Guide* (Guia de administração do Amazon WorkSpaces), Preparing Your Network for an AD Connector Directory (Preparação da sua rede para o AD Connector Directory). O processo para configurar seu AD Connector para MFA está descrito em Gerenciamento de um AD Connector Directory: Multi-factor Authentication, no *Amazon WorkSpaces Administration Guide* (Guia de Administração do Amazon WorkSpaces).

Segurança

Esta seção explica como proteger os dados usando criptografia quando você estiver usando os serviços do Amazon WorkSpaces. Descrevemos a criptografia em trânsito e em repouso, além da utilização de grupos de segurança para proteger o acesso de rede aos WorkSpaces. Você pode encontrar informações adicionais sobre autenticação (inclusive suporte a MFA) na seção AWS Directory Service.

Criptografia em trânsito

O Amazon WorkSpaces usa criptografia para proteger a confidencialidade em diferentes estágios de comunicação (em trânsito) e também para proteger dados em repouso (WorkSpaces criptografados). Os processos em cada estágio da criptografia usada pelo Amazon WorkSpaces em trânsito são descritos nas seções a seguir. Para obter informações sobre a criptografia em repouso, veja a seção WorkSpaces criptografados ainda neste whitepaper.

Registro e atualizações

A aplicação do cliente desktop se comunica com o Amazon para atualizações e registro usando https.

Estágio de autenticação

O cliente desktop inicia a autenticação enviando credenciais ao gateway de autenticação. A comunicação entre o cliente desktop e o gateway de autenticação usa https. Ao final deste estágio, se a autenticação der certo, o gateway de autenticação retornará o token OAuth 2.0 ao cliente desktop atrabés da mesma conexão https.

> **Nota** A aplicação do cliente desktop é compatível com o uso de um servidor de proxy para tráfego da porta 443 (HTTPS), atualizações, registro e autenticação.

Depois de receber as credenciais do cliente, o gateway de autenticação envia uma solicitação de autenticação ao AWS Directory Service. A comunicação do gateway de autenticação para o AWS Directory Service ocorre sobre HTTPS, então nenhuma credencial do usuário é transmitida em texto claro.

Autenticação – AD Connector

O AD Connector usa Kerberos para estabelecer comunicação autenticada com AD local, de forma que possa unir ao LDAP e executar consultas LDAP subsequentes. Neste momento, o AWS Directory Service não é compatível de LDAP com TLS (LDAPs). No entanto, nenhuma credencial de usuário é transmitida em texto claro em momento algum. Para maior segurança, é possível conectar seu WorkSpaces VPC à rede local (no qual o AD reside) usando uma conexão VPN. Ao usar uma conexão VPN de hardware AWS, você configurará a criptografia em trânsito usando IPSEC padrão (SAs IKE e IPSEC) 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 fase 1; 1,2,5, 14-18, 22, 23 e 24 para fase 2) usando PFS.

Estágio Broker

Depois de receber o token OAuth 2.0 (do gateway de autenticação, se a autenticação der certo), o cliente desktop enviará uma consulta aos serviços do Amazon WorkSpaces (Broker Connection Manager) usando HTTPS. O cliente desktop se autentica ao enviar o token OAuth 2.0 e, como resultado, o cliente receberá as informações do endpoint do gateway de streaming do WorkSpaces.

Estágio de streaming

O cliente desktop solicita abrir 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 (ou seja, 4172/tcp).

Usando o token OAuth2.0, o gateway de streaming solicita informações dos WorkSpaces específicos do usuário do serviço WorkSpaces, sobre https.

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

O WorkSpace então inicia uma solicitação de autenticação ao AWS Directory Service configurado usando a autenticação Kerberos padrão.

Depois de o WorkSpace fazer login com sucesso, será iniciado o streaming de PCoIP. 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 seu desktop do WorkSpaces sobre a interface de gerenciamento é via UDP 55002. (Veja a documentação do Amazon Workspaces, Amazon WorkSpaces Details [Detalhes do Amazon WorkSpaces]. A porta UDP de saída inicial é 55002.) A conexão de streaming, usando as portas 4172 (tcp e udp), é criptografada usando chave AES de 128 e 256 bits, mas o padrão é 128 bits. Você pode alterar ativamente isso para 256 bits via GPO do Active Directory específico de PCoIP (pcoip.adm).

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 do seu VPC, como acesso ao AWS Directory Service, à Internet e à rede corporativa. É possível anexar grupos de segurança a esta interface de rede primária (como você faria com qualquer ENI). Conceitualmente, diferenciamos os grupos de segurança ligados a esta ENI com base no escopo da implantação: grupo de segurança do WorkSpaces e grupos de segurança da ENI.

Interface da rede de gerenciamento

Você não consegue controlar a interface de rede de gerenciamento via grupos de segurança, mas pode aproveitar um firewall baseado em host no WorkSpace para bloquear portas ou acesso de controle. Não recomendamos aplicar restrições na interface de rede de gerenciamento. Se você decidir adicionar regras de firewall baseadas em host para gerenciar essa interface, é preciso manter algumas portas abertas para que o serviço WorkSpaces possa gerenciar a integridade e a acessibilidade ao WorkSpace, conforme definido no Amazon WorkSpaces Administration Guide (Guia de Administração do Amazon WorkSpaces).

Grupo de segurança do WorkSpaces

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

Assim como qualquer outro grupo de segurança, é possível modificar as regras de um grupo de segurança dos WorkSpaces. Os resultados entram em vigor imediatamente após as mudanças serem aplicadas.

É possível também alterar o grupo de segurança padrão dos WorkSpaces ligados a um AWS Directory Service ao alterar a associação do grupo de segurança do WorkSpaces.

> **Nota** Um grupo de segurança recém-associado será conectado somente aos WorkSpaces criados ou reconstruídos após a modificação.

Grupo de segurança de ENI

Como a interface de rede primária é uma ENI regular, você pode gerenciar a configuração usando diferentes ferramentas de gerenciamento da AWS (veja Elastic Network Interfaces [ENI]). Mais particularmente, procure pelo IP do WorkSpace (na página WorkSpaces do console do Amazon WorkSpaces) e, em seguida use esse endereço IP como filtro para encontrar a ENI correspondente (na seção Interfaces de Rede do console do Amazon EC2).

Assim que encontrar a ENI, você pode gerenciar diretamente os grupos de segurança daí. Ao atribuir manualmente os grupos de segurança à interface de rede primária, leve em consideração os requisitos de porta do Amazon WorkSpaces, conforme explicado em Amazon WorkSpaces Details (Detalhes do Amazon WorkSpaces).

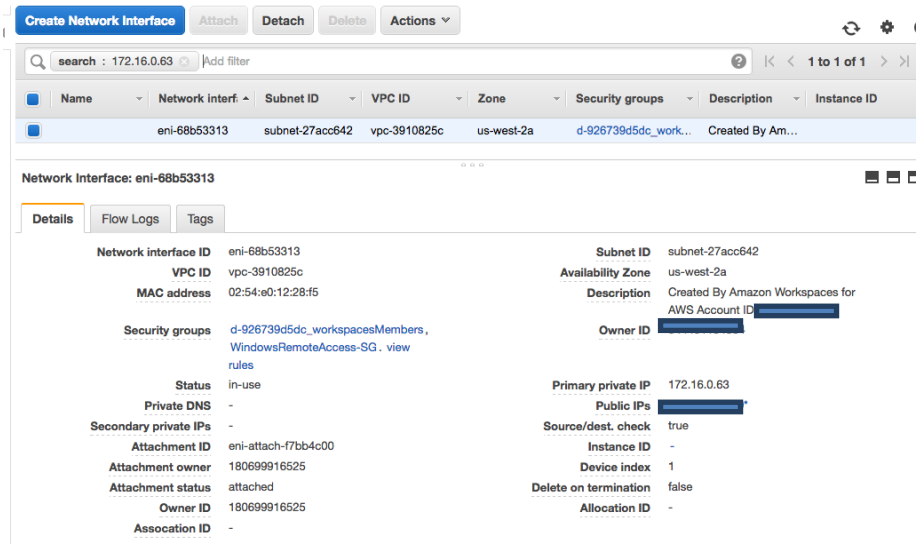

Figura 12: Gerenciamento das associações do grupo de segurança

WorkSpaces criptografados

Cada Amazon WorkSpace é provisionado com um volume raiz (unidade C:) e um volume de usuário (unidade D:). O recurso criptografado do WorkSpaces lhe permite criptografar um dos volumes ou os dois volumes.

O que é criptografado?

Os dados armazenados em repouso, a E/S do disco para o volume e os instantâneos criados com base nos volumes criptografados estão todos criptografados.

Quando a criptografia ocorre?

Você precisa especificar uma criptografia para um WorkSpace ao lançar (criar) o WorkSpace. Os volumes dos WorkSpaces só podem ser criptografados no momento do lançamento: depois do lançamento, não é possível alterar o status de criptografia de um volume. A Figura 13 mostra a página do console do Amazon WorkSpaces para escolher a criptografia durante o lançamento de um novo WorkSpace.

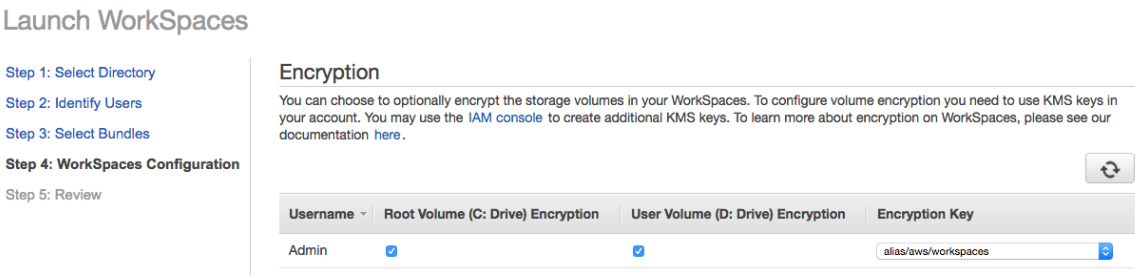

Figura 13: Criptografia dos volumes do WorkSpaces

Como o novo WorkSpace é criptografado?

Você pode escolher a opção WorkSpaces Criptografados no console do Amazon WorkSpaces ou do AWS CLI, ou usar a API do Amazon WorkSpaces no momento que lança um novo WorkSpace.

Para criptografar os volumes, o Amazon WorkSpaces usa uma customer master key (CMK) do AWS Key Management Service (KMS). A CMK padrão do AWS KMS é criada na primeira vez que o WorkSpace é lançado em uma região (as CMKs têm escopo de região). Você também pode criar uma CMK gerenciada pelo cliente para usar com WorkSpaces criptografados. O CMK é usado para criptografar as chaves de dados usadas pelo serviço Amazon WorkSpaces para criptografar os volumes (estritamente, será o serviço Amazon Elastic Block Store (Amazon EBS) que criptografará os volumes). Cada CMK pode ser usado para criptografar chaves para até 30 WorkSpaces.

> **Nota** Atualmente não há suporte para criar imagens personalizadas de um WorkSpace criptografado. Além disso, o WorkSpaces lançados com criptografia no volume-raiz habilitada podem demorar até uma hora para serem provisionados.

Para obter descrições detalhadas do processo de criptografia do WorkSpaces, veja Overview of Amazon WorkSpaces Encryption Using AWS KMS (Visão geral da criptografia do Amazon WorkSpaces usando AWS KMS). Para obter mais informações sobre as Customer Master Keys e chaves de dados do AWS KMS, veja AWS Key Management Service Concepts (Conceitos de serviço de gerenciamento de chaves da AWS).

Monitoramento ou registro usando Amazon CloudWatch

O monitoramento é parte integral de qualquer infraestrutura, seja rede, servidores ou logs. Clientes que implantam Amazon WorkSpaces precisam monitorar as implantações, mais especificamente o status global de integridade e conexão de cada WorkSpaces.

Métricas do Amazon CloudWatch para WorkSpaces

As métricas do CloudWatch para WorkSpaces são feitas para fornecer aos administradores insights adicionais sobre a integridade global e status de conexão de cada WorkSpace. As métricas estão disponíveis a cada WorkSpace ou agregadas para todos os WorkSpaces de uma organização dentro de determinado diretório (*AD Connector, veja Identidade*).

Essas métricas, assim como todas as métricas do CloudWatch, podem ser vistas no AWS Management Console (Figura 13), acessadas via APIs do CloudWatch e monitoradas por alarmes do CloudWatch e ferramentas de terceiros.

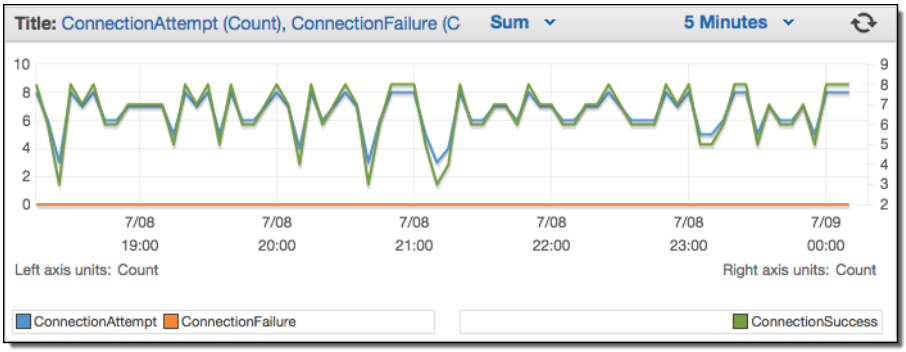

Figura 14: Métricas do CloudWatch – ConnectionAttempt/ConnectionFailure

Por padrão, as métricas a seguir estão habilitadas e disponíveis sem cobranças extra:

- **Available**: Os WorkSpaces que respondem a uma verificação de status são contados nesta métrica.

- **Unhealthy**: Os WorkSpaces que não respondem à mesma verificação de status são contados nesta métrica.
- **ConnectionAttempt**: O número de tentativas de conexão feitas a um WorkSpace.
- **ConnectionSuccess**: O número de tentativas bem-sucedidas de conexão.
- **ConnectionFailure**: O número de tentativas malsucedidas de conexão.
- **SessionLaunchTime**: A quantidade de tempo que leva para iniciar uma sessão, conforme medido pelo cliente dos WorkSpaces.
- **InSessionLatency**: O round-trip time entre o cliente WorkSpaces e o WorkSpaces, conforme medido e reportado pelo cliente.
- **SessionDisconnect**: O número de sessões iniciadas pelo usuário e automaticamente encerradas.

Além disso, podem ser criados alarmes, conforme exibido na Figura 15.

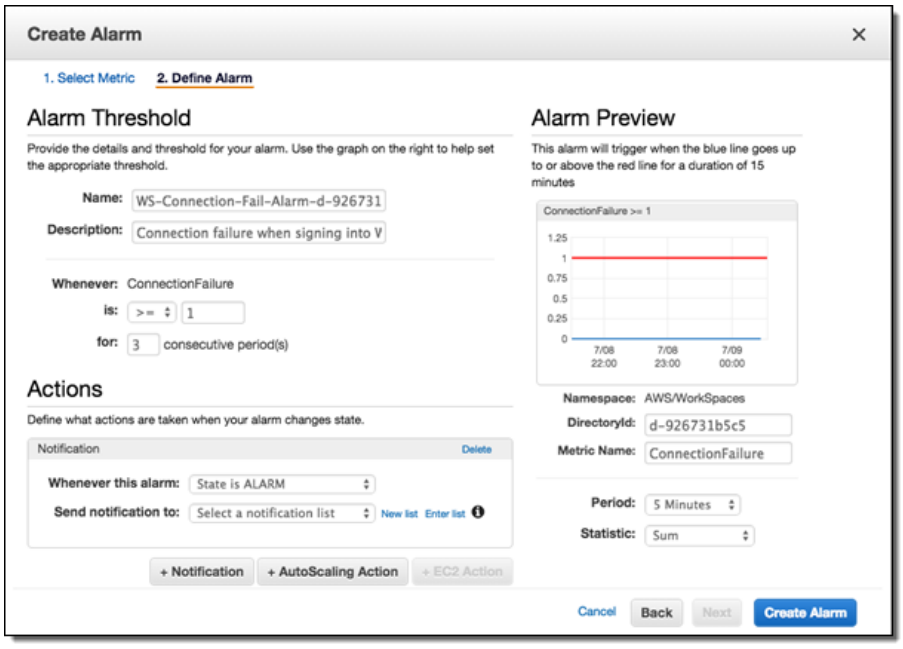

Figura 15: Crie um alarme do CloudWatch para erros de conexão dos WorkSpaces

Resolução de problemas

Problemas comuns de administração e cliente, como "Eu vejo a seguinte mensagem de erro: 'Seu dispositivo não pôde se conectar ao serviço WorkSpaces Registration' ou 'Não foi possível se conectar a um banner de logon interativo'" podem ser encontrados nas páginas Client e Admin de resolução de problemas do *Amazon WorkSpaces Administration Guide (Guia de Administração do Amazon WorkSpaces)*.

O AD Connector não consegue se conectar a um Active Directory

Para o AD Connector se conectar ao diretório local, o firewall para a rede local deverá ter certas portas abertas para os CIDRs das duas sub-redes no VPC (veja AD Connector). Para testar se essas condições foram atendidas, execute as etapas a seguir.

Para verificar a conexão

1. Inicie uma instância do Windows no VPC e conecte-se a ela por RDP. As etapas restantes são executadas na instância do VPC.
2. Baixe e descompacte a aplicação de teste DirectoryServicePortTest. O código-fonte e os arquivos de projeto do Visual Studio são incluídos para que você possa modificar a aplicação de teste, se assim escolher.
3. Pelo prompt de comando do Windows, execute a aplicação de teste DirectoryServicePortTest 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 de floresta e domínio. Se você excluir o nome do domínio, os níveis funcionais não serão testados.

<*server_IP_address*>

O endereço IP de um controlador de domínio no seu domínio local. As portas serão testadas com relação a esse endereço IP. Se você excluir o endereço IP, as portas não serão testadas.

Isso determinará se as portas necessárias estão abertas do VPC para seu domínio. A aplicação de teste também verifica os níveis funcionais mínimos de floresta e domínio.

Como verificar a latência para a Região AWS mais próxima

Em outubro de 2015, o Amazon WorkSpaces lançou o site Connection Health Check. Esse site verifica rapidamente se você consegue acessar todos os serviços para usar o WorkSpaces. Ele também faz uma verificação de desempenho para cada Região AWS na qual os WorkSpaces são executados e permite que os usuários saibam quais serão as mais rápidas para eles.

Conclusão

Estamos vendo uma mudança estratégica na computação do usuário final à medida que as organizações se esforçam para serem mais ágeis, protegerem melhor os dados e ajudarem seus funcionários a serem mais produtivos. Vários dos benefícios já atingidos com a computação de nuvem também se aplicam à computação do usuário final. Ao transferir seus desktops para a Nuvem AWS com o Amazon WorkSpaces, as organizações podem escalar rapidamente à medida que elas adicionam funcionários, melhoram a postura de segurança ao manter os dados longe dos dispositivos e oferecem aos trabalhadores um desktop portátil com acesso de qualquer lugar e de qualquer dispositivo que eles escolherem.

O Amazon WorkSpaces foi feito para ser integrado aos sistemas e processos existentes de TI, e este whitepaper descreve as práticas recomendadas para tal. O resultado de seguir as diretrizes desde whitepaper é uma implantação de desktop na nuvem com boa relação custo-benefício que escala seus negócios na infraestrutura global da AWS.

Colaboradores

As seguintes pessoas contribuíram para este documento:

- Justin Bradley, arquiteto de soluções, Amazon Web Services
- Mahdi Sajjadpour, consultor sênior, AWS Professional Services
- Mauricio Munoz, arquiteto de soluções, Amazon Web Services

Outras fontes de leitura

Para obter mais ajuda, consulte as seguintes fontes:

- Resolução de problemas administrativos do AWS Directory Service
- Resolução de problemas administrativos do Amazon WorkSpaces
- Resolução de problemas de clientes do Amazon WorkSpaces
- Guia de Administração do Amazon WorkSpaces
- Guia do Desenvolvedor do Amazon WorkSpaces
- Plataformas e dispositivos compatíveis
- Como o Amazon WorkSpaces usa AWS KMS
- Referência de comando da CLI do AWS – WorkSpaces
- Monitoramento das métricas do Amazon WorkSpaces