Guia de administração

AWS Directory Service

Versão 1.0

AWS Directory Service: Guia de administração

Table of Contents

O que AWS Directory Serviceé

AWS Directory Service fornece várias maneiras de usar Microsoft Active Directory (AD) com outros AWS serviços. Os diretórios armazenam informações sobre usuários, grupos e dispositivos, e os administradores os usam para gerenciar o acesso a informações e recursos. AWS Directory Service fornece várias opções de diretório para clientes que desejam usar aplicativos existentes com reconhecimento do Microsoft AD ou do Lightweight Directory Access Protocol (LDAP) na nuvem. Ele também oferece essas mesmas opções para os desenvolvedores que precisam de um diretório para gerenciar usuários, grupos, dispositivos e acesso.

Qual escolher

Você pode escolher os serviços de diretório com os recursos e o dimensionamento que melhor atendem às suas necessidades. Use a tabela a seguir para ajudá-lo a determinar qual opção de AWS Directory Service diretório funciona melhor para sua organização.

O que você precisa fazer?	AWS Directory Service Opções recomendadas
Preciso de LDAP ou Active Directory para os meus aplicativos na nuvem	Use o AWS Directory Service for Microsoft Active Directory (Standard Edition ou Enterprise Edition) se precisar de um serviço real Microsoft Active Directory na AWS nuvem que suporte cargas de trabalho com Active Directory reconhecimento de dados, ou AWS aplicativos e serviços como Amazon e WorkSpaces Amazon QuickSight, ou se precisar de suporte LDAP para aplicativos Linux. Use o AD Connector se você só precisar permitir que seus usuários locais façam login em AWS aplicativos e serviços com suas Active Directory credenciais. Você também pode usar o AD Connector para unir instâncias do Amazon EC2 ao seu domínio existenteActive Directory. Use o Simple AD se precisar de um diretório de baixa escala e baixo custo com Active Directory compatibilidade básica que suporte aplicativos compatíveis com o Samba

O que você precisa fazer?	AWS Directory Service Opções recomendadas
	4, ou se precisar de compatibilidade com LDAP para aplicativos compatíveis com LDAP.
Eu desenvolvo aplicativos SaaS	Use o Amazon Cognito se você desenvolve aplicativos SaaS de alta escala e precisa de um diretório escalável para gerenciar e autenticar seus assinantes e que funcione com as identidades de redes sociais.

Para obter mais informações sobre as opções de AWS Directory Service diretório, consulte Como escolher Active Directory soluções em AWS.

AWS Directory Service opções

AWS Directory Service inclui vários tipos de diretórios para escolher. Para obter mais informações, selecione uma das seguintes guias:

AWS Directory Service for Microsoft Active Directory

Também conhecido como AWS Managed Microsoft AD, o AWS Directory Service for Microsoft Active Directory é desenvolvido por um Microsoft Windows Server Active Directory (AD) real, gerenciado pela AWS in the AWS Cloud. Ele permite que você migre uma ampla variedade de aplicativos compatíveis com o Active Directory para a nuvem. AWS AWS O Microsoft AD gerenciado funciona com Microsoft SharePoint grupos de disponibilidade Microsoft SQL Server sempre ativos e muitos aplicativos.NET. Ele também oferece suporte a aplicativos e serviços AWS gerenciados WorkSpaces, incluindo Amazon WorkDocs, Amazon QuickSight, Amazon Chime, Amazon Connect e Amazon Relational Database Service para (Amazon RDS paraSQL Server, Microsoft SQL Server Amazon RDS para e Amazon RDS Oracle for PostgreSQL).

AWS O Microsoft AD gerenciado é aprovado para aplicativos na AWS nuvem que estão sujeitos à conformidade com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde dos EUA (HIPAA) ou com o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) quando você habilita a conformidade para seu diretório.

Todos os aplicativos compatíveis funcionam com credenciais de usuário que você armazena no Microsoft AD AWS gerenciado, ou você pode se conectar à sua infraestrutura existente do

AD com uma relação de confiança e usar credenciais de uma Active Directory execução local ou no EC2 Windows. Se você unir instâncias do EC2 ao seu Microsoft AD AWS gerenciado, seus usuários poderão acessar cargas de trabalho do Windows na AWS nuvem com a mesma experiência de login único (SSO) do Windows de quando acessam cargas de trabalho em sua rede local.

AWS O Microsoft AD gerenciado também oferece suporte a casos de uso federados usando Active Directory credenciais. Sozinho, o AWS Managed Microsoft AD permite que você entre no AWS Management Console. Com AWS IAM Identity Center, você também pode obter credenciais de curto prazo para uso com o AWS SDK e a CLI e usar integrações SAML pré-configuradas para fazer login em vários aplicativos em nuvem. Ao adicionar Microsoft Entra Connect (anteriormente conhecido comoAzure Active Directory Connect) e, opcionalmente, o Serviço de Active Directory Federação (AD FS), você pode entrar Microsoft Office 365 em outros aplicativos em nuvem com credenciais armazenadas no Managed AWS Microsoft AD.

O serviço inclui os principais recursos que permitem estender seu esquema, gerenciar políticas de senha e habilitar as comunicações LDAP por meio de Secure Socket Layer (SSL)/Transport Layer Security (TLS). Você também pode habilitar a autenticação multifator (MFA) para o AWS Managed Microsoft AD para fornecer uma camada adicional de segurança quando os usuários AWS acessam aplicativos pela Internet. Como Active Directory é um diretório LDAP, você também pode usar o AWS Microsoft AD gerenciado para autenticação Linux Secure Shell (SSH) e para outros aplicativos habilitados para LDAP.

AWS fornece monitoramento, instantâneos diários e recuperação como parte do serviço — você adiciona usuários e grupos ao Managed AWS Microsoft AD e administra a Política de Grupo usando Active Directory ferramentas familiares executadas em um Windows computador associado ao domínio Managed AWS Microsoft AD. Você também pode dimensionar o diretório implantando controladores de domínio adicionais e pode ajudar a melhorar o desempenho do aplicativo distribuindo solicitações a um número maior de controladores de domínio.

AWS O Microsoft AD gerenciado está disponível em duas edições: Standard e Enterprise.

- Standard Edition: o AWS Managed Microsoft AD (Standard Edition) é otimizado para ser o diretório principal para empresas de pequeno e médio porte com até 5.000 funcionários. Ele fornece capacidade de armazenamento suficiente para oferecer suporte a até 30.000* objetos de diretório, como usuários, grupos e computadores.
- Enterprise Edition: o AWS Managed Microsoft AD (Enterprise Edition) foi criado para oferecer suporte a empresas com até 500.000* objetos de diretório.

*Os limites superiores são aproximações. Seu diretório pode oferecer suporte a mais ou menos objetos de diretório, dependendo do tamanho dos objetos e do comportamento e das necessidades de desempenho de seus aplicativos.

Quando usar

AWS O Microsoft AD gerenciado é sua melhor opção se você precisar de Active Directory recursos reais para suportar AWS aplicativos ou Windows cargas de trabalho, incluindo o Amazon Relational Database Service for. Microsoft SQL Server Também é melhor se você quiser um diretório autônomo Active Directory na AWS nuvem que ofereça suporte ao Office 365 ou se precisar de um diretório LDAP para suportar seus aplicativos Linux. Para ter mais informações, consulte AWS Microsoft AD gerenciado.

AD Connector

O AD Connector é um serviço de proxy que fornece uma maneira fácil de conectar AWS aplicativos compatíveis, como Amazon WorkSpaces QuickSight, Amazon e Amazon EC2, por exemplo, Windows Server ao seu local existente. Microsoft Active Directory Com o AD Connector, você pode simplesmente adicionar uma conta de serviço à suaActive Directory. O AD Connector também elimina a necessidade de sincronização de diretórios ou o custo e a complexidade da hospedagem de uma infraestrutura de federação.

Quando você adiciona usuários a AWS aplicativos como o Amazon QuickSight, o AD Connector lê seus aplicativos existentes Active Directory para criar listas de usuários e grupos para selecionar. Quando os usuários fazem login nos AWS aplicativos, o AD Connector encaminha as solicitações de login para seus controladores de Active Directory domínio locais para autenticação. O AD Connector funciona com muitos AWS aplicativos e serviços, incluindo Amazon WorkSpaces, Amazon WorkDocs, Amazon QuickSight, Amazon Chime, Amazon Connect e Amazon. WorkMail Você também pode unir suas Windows instâncias do EC2 ao seu Active Directory domínio local por meio do AD Connector usando uma união de domínio perfeita. O AD Connector também permite que seus usuários acessem AWS Management Console e gerenciem AWS os recursos fazendo login com suas Active Directory credenciais existentes. O AD Connector não é compatível com o RDS SQL Server.

Você também pode usar o AD Connector para habilitar a autenticação multifator (MFA) para os usuários do AWS seu aplicativo conectando-a à sua infraestrutura de MFA baseada em RADIUS existente. Isso fornece uma camada adicional de segurança quando os usuários acessam aplicativos da AWS .

Com o AD Connector, você continua gerenciando o seu Active Directory como faz agora. Por exemplo, você adiciona novos usuários e grupos e atualiza senhas usando ferramentas de Active Directory administração padrão em seu localActive Directory. Isso ajuda você a aplicar consistentemente suas políticas de segurança, como expiração de senha, histórico de senhas e bloqueios de contas, independentemente de os usuários estarem acessando recursos no local ou na AWS nuvem.

Quando usar

O AD Connector é sua melhor opção quando você deseja usar seu diretório local existente com AWS serviços compatíveis. Para ter mais informações, consulte AD Connector.

Simple AD

Simple AD é um Microsoft Active Directory diretório compatível com AWS Directory Service o Samba 4. O Simple AD oferece suporte a Active Directory recursos básicos, como contas de usuário, associações a grupos, ingresso em um domínio Linux ou instâncias EC2 Windows baseadas em EC2, SSO baseado em Kerberos e políticas de grupo. AWS fornece monitoramento, instantâneos diários e recuperação como parte do serviço.

O Simple AD é um diretório independente na nuvem que permite criar e gerenciar identidades de usuários e gerenciar o acesso a aplicações. Você pode usar muitos aplicativos Active Directory e ferramentas familiares que exigem Active Directory recursos básicos. O Simple AD é compatível com os seguintes AWS aplicativos: Amazon WorkSpaces WorkDocs, Amazon QuickSight, Amazon e Amazon WorkMail. Você também pode entrar nas contas AWS Management Console de usuário do Simple AD e gerenciar AWS recursos.

O Simple AD não oferece suporte à autenticação multifator (MFA), relações de confiança, atualização dinâmica de DNS, extensões de esquema, comunicação por LDAPS PowerShell , cmdlets do AD ou transferência de função FSMO. O Simple AD não é compatível com o RDS SQL Server. Os clientes que precisam dos recursos de um diretório real Microsoft Active Directory ou que pretendem usar seu diretório com o RDS SQL Server devem usar o AWS Microsoft AD gerenciado em vez disso. Verifique se as aplicações necessárias são totalmente compatíveis com Samba 4 antes de usar o Simple AD. Para obter mais informações, consulte https://www.samba.org.

Quando usar

Você pode usar o Simple AD como um diretório independente na nuvem para oferecer suporte a Windows cargas de trabalho que precisam de Active Directory recursos básicos, AWS aplicativos

compatíveis ou para suportar cargas de trabalho Linux que precisam do serviço LDAP. Para ter mais informações, consulte Simple AD.

Amazon Cognito

O Amazon Cognito é um diretório de usuário que adiciona recursos de registro e login em sua aplicação móvel ou Web usando grupos de usuários do Amazon Cognito.

Quando usar

Você também poderá usar o Amazon Cognito quando precisar criar campos de registro personalizados e armazenar esses metadados em seu diretório de usuários. Esse serviço totalmente gerenciado pode ser dimensionado para oferecer suporte a centenas de milhões de usuários. Para obter mais informações, consulte Grupos de usuários do Amazon Cognito no Guia do desenvolvedor do Amazon Cognito.

Consulte Disponibilidade da região para AWS Directory Service para obter uma lista de tipos de diretório compatíveis por região.

Trabalhar com o Amazon EC2

Uma compreensão básica do Amazon EC2 é essencial para usar o AWS Directory Service. Recomendamos que você comece lendo os seguintes tópicos:

- O que é o Amazon EC2? no Guia do usuário do Amazon EC2.
- Lançamento de instâncias do EC2 no Guia do usuário do Amazon EC2.
- Grupos de segurança no Guia do usuário do Amazon EC2.
- O que é o Amazon VPC? no Guia do usuário do Amazon VPC.
- Adicionar um gateway privado virtual de hardware à sua VPC no Guia do usuário do Amazon VPC.

Começando com AWS Directory Service

Se ainda não tiver feito isso, você também precisará criar uma AWS conta e usar o AWS Identity and Access Management serviço para controlar o acesso.

Para trabalhar com ele AWS Directory Service, você precisa atender aos pré-requisitos do AWS Directory Service for Microsoft Active Directory, AD Connector ou Simple AD. Para obter mais informações, consulte AWS Pré-requisitos gerenciados do Microsoft AD, Pré-requisitos do AD Connector ou Pré-requisitos do Simple AD.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário e use somente o usuário raiz para realizar tarefas que exijam acesso do usuário raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Crie um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para o usuário raiz.c

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Crie um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No IAM Identity Center, conceda acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Faça login como usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribua acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

Para obter instruções, consulte Criar um conjunto de permissões no Guia AWS IAM Identity Center do usuário.

2. Atribua usuários a um grupo e, em seguida, atribua acesso de login único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia AWS IAM Identity Center do usuário.

Mais informações

- Para obter mais informações sobre como fazer login no AWS Management Console como usuário do IAM Identity Center, consulte Fazer login no portal de acesso do IAM Identity Center.
- Para obter mais informações sobre como fazer login no AWS Management Console como usuário do IAM, consulte Fazer login no AWS Management Console como usuário do IAM.
- Para obter mais informações sobre o uso de políticas do IAM para controlar o acesso aos seus AWS Directory Service recursos, consulteUsando políticas baseadas em identidade (políticas do IAM) para AWS Directory Service.

AWS Microsoft AD gerenciado

AWS Directory Service permite que você execute o Microsoft Active Directory (AD) como um serviço gerenciado. AWS O Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD, é desenvolvido pelo Windows Server 2019. Quando você seleciona e executa esse tipo de diretório, ele é criado como um par altamente disponível de controladores de domínio conectados à sua nuvem privada virtual (Amazon VPC). Os controladores de domínio são executados em diferentes zonas de disponibilidade em uma região de sua escolha. O monitoramento e a recuperação de host, a replicação de dados, os snapshots e as atualizações de software são configurados e automaticamente gerenciados para você.

Com o Microsoft AD AWS gerenciado, você pode executar cargas de trabalho com reconhecimento de diretório na AWS nuvem, incluindo Microsoft SharePoint aplicativos personalizados baseados em .NET e SQL Server. Você também pode configurar uma relação de confiança entre o Microsoft AD AWS gerenciado na AWS nuvem e seu local existente MicrosoftActive Directory, fornecendo aos usuários e grupos acesso aos recursos em qualquer domínio, usando AWS IAM Identity Center.

AWS Directory Service facilita a configuração e a execução de diretórios na AWS nuvem ou a conexão de seus AWS recursos a um local Microsoft Active Directory existente. Depois que o diretório é criado, você pode usá-lo para várias tarefas:

- Gerenciar usuários e grupos
- Forneça logon único a aplicativos e serviços
- Criar e aplicar política de grupo
- Simplifique a implantação e o gerenciamento de Linux e cargas de trabalho baseados em nuvem Microsoft Windows
- Você pode usar o AWS Managed Microsoft AD para habilitar a autenticação multifatorial integrando-se à sua infraestrutura de MFA baseada em RADIUS existente para fornecer uma camada adicional de segurança quando os usuários acessam aplicativos. AWS
- Conecte-se com segurança ao Amazon EC2, Linux e instâncias Windows

> **Note**
>
> AWS gerencia o licenciamento de suas instâncias de Windows servidor para você; tudo o que você precisa fazer é pagar pelas instâncias que você usa. Também não há necessidade

de comprar licenças adicionais de acesso para cliente (CALs) do Windows Server, pois o acesso está incluído no preço. Cada instância oferece duas conexões remotas somente para fins administrativos. Se você precisar de mais de duas conexões ou precisar dessas conexões para outros fins que não sejam administrativos, talvez seja necessário trazer CALs adicionais de Remote Desktop Services para usar na AWS.

Leia os tópicos desta seção para começar a criar um diretório AWS gerenciado do Microsoft AD, criar uma relação de confiança entre o AWS Managed Microsoft AD e seus diretórios locais e estender seu esquema Managed AWS Microsoft AD.

Tópicos

- Introdução ao AWS Managed Microsoft AD
- Principais conceitos do AWS Managed Microsoft AD
- Práticas recomendadas para o Microsoft AD AWS gerenciado
- Casos de uso do Microsoft AD AWS gerenciado
- Como administrar o Microsoft AD AWS gerenciado
- AWS Cotas gerenciadas do Microsoft AD
- Compatibilidade de aplicativos para o AWS Managed Microsoft AD
- AWS Tutoriais gerenciados do laboratório de testes do Microsoft AD
- Solução de problemas do Microsoft AD AWS gerenciado

Artigos do blog de AWS segurança relacionados

- Como delegar a administração do seu diretório AWS gerenciado do Microsoft AD aos usuários locais do Active Directory
- Como configurar políticas de senha ainda mais fortes para ajudar a atender aos seus padrões de segurança usando AWS Directory Service o Microsoft AD AWS gerenciado
- Como aumentar a redundância e o desempenho do seu AWS Microsoft AD AWS Directory Service gerenciado adicionando controladores de domínio
- Como habilitar o uso de desktops remotos implantando o gerenciador de licenciamento de desktop remoto da Microsoft no Managed AWS Microsoft AD
- Como acessar o Microsoft AWS Management Console AD AWS gerenciado e suas credenciais locais

- Como habilitar a autenticação multifator para AWS serviços usando o Microsoft AD AWS gerenciado e credenciais locais
- Como fazer login facilmente nos AWS serviços usando seu Active Directory local

Introdução ao AWS Managed Microsoft AD

AWS O Microsoft AD gerenciado cria um ambiente totalmente gerenciado, Microsoft Active Directory no Nuvem AWS e é desenvolvido pelo Windows Server 2019 e opera nos níveis funcionais de 2012 R2 Forest e Domain. Quando você cria um diretório com o AWS Managed Microsoft AD, AWS Directory Service cria dois controladores de domínio e adiciona o serviço DNS em seu nome. Os controladores de domínio são criados em diferentes sub-redes em uma Amazon VPC. Essa redundância ajuda a garantir que seu diretório permaneça acessível mesmo se ocorrer uma falha. Se precisar de mais controladores de domínio, você pode adicioná-los posteriormente. Para ter mais informações, consulte Implantar controladores de domínio adicionais.

Tópicos

- AWS Pré-requisitos gerenciados do Microsoft AD
- Crie seu Microsoft AD AWS gerenciado
- O que é criado com seu Microsoft AD Active Directory AWS gerenciado
- Permissões para a conta de administrador

AWS Pré-requisitos gerenciados do Microsoft AD

Para criar um Microsoft AD AWS gerenciadoActive Directory, você precisa de uma Amazon VPC com o seguinte:

- Pelo menos duas sub-redes. Cada uma das sub-redes deve estar em uma zona de disponibilidade diferente.
- A VPC deve ter uma locação de hardware padrão.
- Você não pode criar um Microsoft AD AWS gerenciado em uma VPC usando endereços no espaço de endereço 198.18.0.0/15.

Se precisar integrar seu domínio AWS gerenciado do Microsoft AD a um Active Directory domínio local existente, você deverá ter os níveis funcionais de Floresta e Domínio para seu domínio local definidos como Windows Server 2003 ou superior.

AWS Directory Service usa uma estrutura de duas VPC. As instâncias do EC2 que compõem seu diretório são executadas fora da sua AWS conta e são gerenciadas pela AWS. Elas têm dois adaptadores de rede `ETH0` e `ETH1`. `ETH0` é o adaptador de gerenciamento e existe fora da sua conta. `ETH1` é criado em sua conta.

O intervalo IP de gerenciamento da rede ETH0 do seu diretório é 198.18.0.0/15.

AWS IAM Identity Center pré-requisitos

Se você planeja usar o IAM Identity Center com o Microsoft AD AWS gerenciado, você precisa garantir que o seguinte seja verdadeiro:

- Seu diretório AWS gerenciado do Microsoft AD está configurado na conta de gerenciamento da sua AWS organização.
- Sua instância do IAM Identity Center está na mesma região em que seu diretório AWS gerenciado do Microsoft AD está configurado.

Para obter mais informações, consulte os pré-requisitos do IAM Identity Center no Guia do AWS IAM Identity Center usuário.

Pré-requisitos da autenticação multifator

Para oferecer suporte à autenticação multifator com seu diretório AWS Managed Microsoft AD, você deve configurar seu servidor RADIUS (Remote Authentication Dial-In User Service) local ou baseado na nuvem da seguinte maneira para que ele possa aceitar solicitações do seu diretório Managed Microsoft AD em. AWS AWS

1. Em seu servidor RADIUS, crie dois clientes RADIUS para representar os dois controladores de domínio (DCs) gerenciados do AWS Microsoft AD em. AWS Você deve configurar os dois clientes usando os seguintes parâmetros comuns (o servidor RADIUS pode variar):
   - Endereço (DNS ou IP): é o endereço DNS de um dos AD DCs gerenciados da AWS Microsoft. Ambos os endereços DNS podem ser encontrados no AWS Directory Service Console na página Detalhes do diretório AWS Managed Microsoft AD no qual você planeja usar o MFA. Os endereços DNS exibidos representam os endereços IP de ambos os AD DCs AWS gerenciados da Microsoft que são usados pelo. AWS

> **Note**
>
> Se seu servidor RADIUS oferecer suporte a endereços de DNS, é necessário criar apenas uma configuração de cliente RADIUS. Caso contrário, você deverá criar uma configuração de cliente RADIUS para cada DC do AWS Managed Microsoft AD.

- Número da porta: configure o número da porta na qual seu servidor do RADIUS aceita conexões de cliente do RADIUS. A porta padrão do RADIUS é 1812.
- Segredo compartilhado: digite ou gere um segredo compartilhado que o servidor do RADIUS usará para conectar-se aos clientes do RADIUS.
- Protocolo: Talvez seja necessário configurar o protocolo de autenticação entre os AD DCs AWS gerenciados da Microsoft e o servidor RADIUS. Os protocolos compatíveis são PAP, CHAP MS-CHAPv1 e MS-CHAPv2. O MS-CHAPv2 é recomendado porque fornece a segurança mais forte das três opções.
- Nome do aplicativo: pode ser opcional em alguns servidores do RADIUS e normalmente identifica o aplicativo em mensagens ou relatórios.

2. Configure sua rede existente para permitir o tráfego de entrada dos clientes RADIUS (endereços DNS gerenciados do AWS Microsoft AD DCs, consulte a Etapa 1) para a porta do servidor RADIUS.
3. Adicione uma regra ao grupo de segurança do Amazon EC2 em seu domínio gerenciado AWS do Microsoft AD que permita tráfego de entrada do endereço DNS e do número da porta do servidor RADIUS definidos anteriormente. Para obter mais informações, consulte Adicionar regras a um grupo de segurança no Guia do usuário do EC2.

Para obter mais informações sobre como usar o Microsoft AD AWS gerenciado com MFA, consulte. Habilite a autenticação multifator para o AWS Managed Microsoft AD

Crie seu Microsoft AD AWS gerenciado

Para criar um novo diretório, execute as seguintes etapas. Antes de iniciar este procedimento, verifique se você concluiu os pré-requisitos identificados em AWS Pré-requisitos gerenciados do Microsoft AD.

Para criar um diretório AWS gerenciado do Microsoft AD

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios e escolha Configurar diretório.
2. Na página Selecionar tipo do diretório, escolha AWS Managed Microsoft AD e, em seguida, Próximo.
3. Na página Enter directory information (Inserir informações do diretório), forneça as seguintes informações:

   Edição

   Escolha entre a Standard Edition ou a Enterprise Edition do AWS Managed Microsoft AD. Para obter mais informações sobre edições, consulte AWS Directory Service for Microsoft Active Directory.

   Nome do DNS do diretório

   O nome completo do diretório, como `corp.example.com`.

   > **Note**
   >
   > Se você planeja usar o Amazon Route 53 para DNS, o nome de domínio do seu Microsoft AD AWS gerenciado deve ser diferente do seu nome de domínio do Route 53. Problemas de resolução de DNS podem ocorrer se o Route 53 e o AWS Managed Microsoft AD compartilharem o mesmo nome de domínio.

   Nome de NetBIOS do diretório

   O nome curto do diretório, como `CORP`.

   Descrição do diretório

   Uma descrição opcional do diretório.

   Senha do Admin

   A senha do administrador do diretório. O processo de criação do diretório cria uma conta de administrador com o nome de usuário `Admin` e essa senha.

   A senha não pode incluir a palavra "admin".

A senha do administrador do diretório diferencia maiúsculas de minúsculas e deve ter de 8 a 64 caracteres, inclusive. Ela também precisa conter pelo menos um caractere de três das quatro categorias a seguir:

- Letras minúsculas (a-z)
- Letras maiúsculas (A-Z)
- Números (0-9)
- Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmar senha

Digite a senha do administrador novamente.

4. Na página Choose VPC and subnets (Selecionar VPC e sub-redes), forneça as seguintes informações e selecione Next (Próximo).

   VPC

   A VPC do diretório.

   Subredes

   Selecione as sub-redes para os controladores de domínio. As duas sub-redes deve estar em diferentes zonas de disponibilidade.

5. Na página Review & create (Revisar e criar), analise as informações do diretório e faça as alterações necessárias. Quando as informações estiverem corretas, escolha Create directory (Criar diretório). A criação do diretório leva de 20 a 40 minutos. Depois de criado, o valor de Status é alterado para Ativo.

O que é criado com seu Microsoft AD Active Directory AWS gerenciado

Quando você cria um Active Directory com o Microsoft AD AWS gerenciado, AWS Directory Service executa as seguintes tarefas em seu nome:

- Cria e associa automaticamente uma interface de rede elástica (ENI) a cada um dos controladores de domínio. Cada um desses ENIs é essencial para a conectividade entre sua VPC AWS Directory Service e os controladores de domínio e nunca deve ser excluído. Você pode identificar todas as interfaces de rede reservadas para uso com AWS Directory Service a descrição: "interface de rede AWS criada para id de diretório". Para obter mais informações, consulte Elastic Network Interfaces no Guia do usuário do Amazon EC2. O servidor DNS padrão do Microsoft AD AWS gerenciado

Active Directory é o servidor VPC DNS em Classless Inter-Domain Routing (CIDR) +2. Para obter mais informações, consulte o servidor Amazon DNS no Guia do usuário da Amazon VPC.

> **Note**
>
> Por padrão, os controladores de domínio são implantados em duas zonas de disponibilidade em uma região e conectados à sua Amazon VPC (VPC). Os backups são feitos automaticamente uma vez por dia, e os volumes do Amazon EBS (EBS) são criptografados para garantir que os dados estejam protegidos em repouso. Os controladores de domínio que falham são substituídos automaticamente na mesma zona de disponibilidade usando o mesmo endereço IP, e uma recuperação completa de desastres pode ser realizada usando-se o backup mais recente.

- Provisiona o Active Directory na VPC usando dois controladores de domínio para tolerância a falhas e alta disponibilidade. Mais controladores de domínio podem ser provisionados para maior resiliência e desempenho depois que o diretório foi criado com êxito e está Ativo. Para ter mais informações, consulte Implantar controladores de domínio adicionais.

  > **Note**
  >
  > AWS não permite a instalação de agentes de monitoramento em controladores de domínio AWS gerenciados do Microsoft AD.

- Cria um grupo de segurança da AWS que estabeleça regras de rede para o tráfego de entrada e de saída dos controladores de domínio. A regra de saída padrão permite todas as ENIs de tráfego ou instâncias anexadas ao grupo de segurança criado AWS . As regras de entrada padrão permitem somente o tráfego por portas que são exigidas pelo Active Directory de qualquer origem (0.0.0.0/0). As regras 0.0.0.0/0 não introduzem vulnerabilidades de segurança, pois o tráfego para os controladores de domínio é limitado ao tráfego da sua VPC, de outras VPCs com peering ou de redes conectadas usando o Transit Gateway ou a Rede Privada Virtual. AWS Direct Connect AWS Para segurança adicional, as ENIs criadas não têm IPs elásticos anexados a elas e você não tem permissão para anexar um IP elástico a essas ENIs. Portanto, o único tráfego de entrada que pode se comunicar com seu Microsoft AD AWS gerenciado é o VPC local e o tráfego roteado de VPC. Tenha muito cuidado se tentar alterar essas regras, pois você pode prejudicar sua capacidade de se comunicar com os controladores de domínio. Para ter mais informações, consulte Práticas recomendadas para o Microsoft AD AWS gerenciado. As seguintes regras do Grupo de AWS Segurança são criadas por padrão:

Regras de entrada

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
ICMP	N/D	0.0.0.0/0	Ping	LDAP Keep Alive, DFS
TCP e UDP	53	0.0.0.0/0	DNS	Autenticação de usuário e computador, resolução de nome, confianças
TCP e UDP	88	0.0.0.0/0	Kerberos	Autenticação de usuário e computador, confianças do nível floresta
TCP e UDP	389	0.0.0.0/0	LDAP	Diretório, replicação, política de grupo de autenticação de usuário e computador, confianças
TCP e UDP	445	0.0.0.0/0	SMB/CIFS	Replicação, autenticação de usuário e computador, política de grupo, confianças

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP e UDP	464	0.0.0.0/0	Alterar/definir senha do Kerberos	Replicação, autenticação de usuário e computador, confianças
TCP	135	0.0.0.0/0	Replicação	RPC, EPM
TCP	636	0.0.0.0/0	LDAP SSL	Diretório, replicação, autenticação de usuário e computador, política de grupo, confianças
TCP	1024-65535	0.0.0.0/0	RPC	Replicação, autenticação de usuário e computador, política de grupo, confianças
TCP	3268 - 3269	0.0.0.0/0	LDAP GC e LDAP GC SSL	Diretório, replicação, autenticação de usuário e computador, política de grupo, confianças

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
UDP	123	0.0.0.0/0	Horário do Windows	Horário do Windows, confianças
UDP	138	0.0.0.0/0	DFSN e NetLogon	DFS, política de grupo
Todos	Todos	sg-###### ############	Todo o tráfego	

Regras de saída

Protocolo	Intervalo de portas	Destination (Destino)	Tipo de tráfego	Uso do Active Directory
Todos	Todos	sg-###### ############	Todo o tráfego	

- Para obter mais informações sobre as portas e os protocolos usados pelo Active Directory, consulte Visão geral do serviço e requisitos de porta de rede para o Windows na documentação da Microsoft.
- Cria uma conta de administrador do diretório com o nome de usuário Admin e a senha especificada. Essa conta está localizada sob a UO Users (por exemplo, Corp > Users). Você usa essa conta para gerenciar seu diretório na AWS nuvem. Para ter mais informações, consulte Permissões para a conta de administrador.

> **Important**
>
> Não se esqueça de salvar essa senha. AWS Directory Service não armazena essa senha e ela não pode ser recuperada. No entanto, você pode redefinir uma senha no AWS Directory Service console ou usando a ResetUserPasswordAPI.

- Cria as seguintes três unidades organizacionais (UOs) na raiz do domínio:

Nome da UO	Descrição
AWS Grupos delegados	Armazena todos os grupos que você pode usar para delegar permissões AWS específicas aos seus usuários.
AWS Reservado	Armazena todas as contas específicas de AWS gerenciamento.

<yourdomainname>	O nome dessa UO é baseado no nome NetBIOS digitado quando você criou seu diretório. Se você não especificar um nome NetBIOS, será usado como padrão a primeira parte do nome DNS do diretório (por exemplo, no caso de corp.example.com, o nome NetBIOS seria corp). Essa OU pertence AWS e contém todos os seus objetos de diretório AWS relacionados, sobre os quais você tem controle total. Duas UOs filhas existem sob essa UO por padrão; Computers (Computadores) e Users (Usuários). Por exemplo: .
	• Corp
	  • Computadores
	  • Usuários

- Cria os seguintes grupos na UO de Grupos AWS Delegados:

Group name	Descrição
AWS Operadores de contas delegadas	Os membros desse grupo de segurança possuem capacidade limitada para gerenciamento de contas, como redefinições de senha
AWS Administradores delegados de ativação baseados no Active Directory	Os membros desse grupo de segurança podem criar objetos de ativação de licenciamento por volume do Active Directory,

Group name	Descrição
	que permite que as empresas ativem os computadores por meio de uma conexão ao seu domínio.
AWS Adição delegada de estações de trabalho aos usuários do domínio	Os membros desse grupo de segurança podem adicionar 10 computadores a um domínio
AWS Administradores delegados	Os membros desse grupo de segurança podem gerenciar o Microsoft AD AWS gerenciado, ter controle total de todos os objetos em sua OU e gerenciar grupos contidos na OU de grupos AWS delegados.
AWS Delegado com permissão para autentica r objetos	Os membros desse grupo de segurança têm a capacidade de se autenticar nos recursos do computador na OU AWS Reservada (necessária somente para objetos locais com Trusts habilitados para Autenticação Seletiva).
AWS Delegado com permissão para autentica ção em controladores de domínio	Os membros desse grupo de segurança recebem a capacidade de autenticar recursos do computador na UO de controladores de domínio (necessária apenas para objetos on-premises com confianças habilitadas para autenticação seletiva).
AWS Administradores delegados de vida útil de objetos excluídos	Os membros desse grupo de segurança podem modificar o DeletedObjectLifetime objeto MSDs-, que define por quanto tempo um objeto excluído estará disponível para ser recuperado da Lixeira do AD.
AWS Administradores delegados de sistemas de arquivos distribuídos	Os membros desse grupo de segurança podem adicionar e remover espaços de nome FRS, DFS-R e DFS.

Group name	Descrição
AWS Administradores de sistemas de nomes de domínio delegados	Os membros desse grupo de segurança podem gerenciar DNS integrado ao Active Directory.
AWS Administradores delegados do Dynamic Host Configuration Protocol	Os membros desse grupo de segurança podem autorizar servidores DHCP do Windows na empresa.
AWS Administradores delegados da Autoridade de Certificação Empresarial	Os membros desse grupo de segurança podem implantar e gerenciar a infraestrutura da Autoridade de Certificação Empresarial da Microsoft.
AWS Administradores delegados de políticas de senhas refinadas	Os membros desse grupo de segurança podem modificar políticas de senhas minuciosas pré-criadas.
AWS Administradores de FSx delegados	Os membros deste grupo de segurança têm a capacidade de gerenciar recursos do Amazon FSx.
AWS Administradores delegados de políticas de grupo	Os membros desse grupo de segurança podem realizar tarefas de gerenciamento de políticas de grupo (criar, editar, excluir, vincular).
AWS Administradores de delegação delegados do Kerberos	Os membros desse grupo de segurança podem permitir a delegação nos objetos de conta de usuário e computador.
AWS Administradores delegados de contas de serviços gerenciados	Os membros desse grupo de segurança podem criar e excluir contas de serviço gerenciado.

Group name	Descrição
AWS Dispositivos delegados não compatíveis com MS-NPRC	Os membros desse grupo de segurança serão excluídos da exigência de comunicaç ão por canais seguros com controladores de domínio. Esse grupo destina-se a contas de computador.
AWS Administradores do serviço de acesso remoto delegado	Os membros desse grupo de segurança podem adicionar e remover servidores RAS do grupo de servidores RAS e IAS.
AWS Administradores de alterações do diretório de replicação delegado	Os membros desse grupo de segurança podem sincronizar as informações do perfil no Active Directory com o SharePoint Server.
AWS Administradores de servidor delegados	Os membros desse grupo de segurança estão inclusos no grupo de administradores local em todos os computadores associados ao domínio.
AWS Administradores de sites e serviços delegados	Os membros desse grupo de segurança podem renomear o objeto Default-First-Site-Name em sites e serviços do Active Directory.
AWS Administradores delegados de gerenciamento de sistemas	Os membros desse grupo de segurança podem criar e gerenciar objetos no contêiner do System Management.
AWS Administradores delegados de licenciam ento do Terminal Server	Os membros desse grupo de segurança podem adicionar e remover servidores de licença do servidor terminal do grupo de servidores de licença do servidor terminal.
AWS Administradores de sufixo de nome principal de usuário delegado	Os membros desse grupo de segurança podem adicionar e remover sufixos do nome da entidade principal do usuário.

- Cria e aplica os seguintes objetos de política de grupo (GPOs):

> **Note**
>
> Você não tem permissões para excluir, modificar ou desvincular estes GPOs. Isso ocorre intencionalmente, pois eles são reservados para AWS uso. Você pode vinculá-los às UOs que você controla, se necessário.

Nome da política de grupo	Aplica-se a	Descrição
Política de domínio padrão	Domínio	Inclui senha de domínio e políticas do Kerberos.
ServerAdmins	Todas as contas de computador que não são de controlador de domínio	Adiciona os 'Administ radores de Servidores AWS Delegados' como membros do Grupo BUILTIN\ Administr ators.
AWS Política reservada: Usuário	AWS Contas de usuário reservadas	Define as configurações de segurança recomendadas em todas as contas de usuário na OU AWS reservada.
AWS Política gerenciada do Active Directory	Todos os controladores de domínio	Define as configurações de segurança recomendadas em todos os controladores de domínio.
TimePolicyNT5DS	Todos os controladores de domínio não PDCe	Define todas as políticas de horário de controladores de domínio não PDCe para usar o Horário do Windows (NT5DS).

Nome da política de grupo	Aplica-se a	Descrição
TimePolicyPDC	O controlador de domínio de PDCe	Define a política de horário do controlador de domínio de PDCe para usar o Network Time Protocol (NTP).
Política de controladores de domínio padrão	Não usado	Provisionada durante a criação do domínio, a Política AWS Gerenciada do Active Directory é usada em seu lugar.

Se quiser ver as configurações de cada GPO, você poderá visualizá-las em uma instância do Windows associada ao domínio com o Console de gerenciamento de política de grupo (GPMC) habilitado.

Permissões para a conta de administrador

Quando você cria um AWS diretório do Directory Service para o Microsoft Active Directory, AWS cria uma unidade organizacional (OU) para armazenar todos os grupos e contas AWS relacionados. Para obter mais informações sobre essa UO, consulte O que é criado com seu Microsoft AD Active Directory AWS gerenciado. Isso inclui a conta de administrador. A conta de administrador tem permissões para executar as seguintes atividades administrativas comuns para sua UO:

- Adicionar, atualizar ou excluir usuários, grupos e computadores. Para ter mais informações, consulte Gerenciar usuários e grupos no AWS Microsoft Managed AD.
- Adicione recursos ao seu domínio, como servidores de arquivos ou de impressão e atribua permissões para esses recursos a usuários e grupos em sua UO.
- Criar UOs adicionais e contêineres.
- Delegue autoridade de UOs e contêineres adicionais. Para ter mais informações, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.
- Criar e vincular políticas de grupo.
- Restaurar objetos excluídos da Lixeira do Active Directory.

- Execute os Windows PowerShell módulos Active Directory e DNS no Serviço Web do Active Directory.
- Criar e configurar contas de serviço gerenciadas pelo grupo. Para ter mais informações, consulte Contas de serviço gerenciadas pelo grupo.
- Configurar a delegação restrita de Kerberos. Para ter mais informações, consulte Delegação restrita de Kerberos.

A conta de administrador também possui direitos para executar as seguintes atividades de domínio:

- Gerenciar configurações de DNS (adicionar, remover ou atualizar registros, zonas e encaminhadores)
- Visualizar logs de eventos de DNS
- Visualizar logs de eventos de segurança

Somente as ações listadas aqui são permitidas na conta de administrador. A conta de administrador também não tem permissões para quaisquer ações relacionadas a diretórios fora da sua UO específica, como a UO pai.

Important

AWS Os administradores de domínio têm acesso administrativo total a todos os domínios hospedados em. AWS Consulte seu contrato AWS e as perguntas frequentes sobre proteção de AWS dados para obter mais informações sobre como AWS lida com o conteúdo, incluindo informações de diretório, que você armazena nos AWS sistemas.

Note

Recomendamos que você não exclua nem renomeie essa conta. Se não desejar mais usar a conta, recomendamos definir uma senha longa (no máximo 64 caracteres aleatórios) e desabilitá-la.

Contas privilegiadas de administrador de empresa e de administrador de domínio

AWS alterna automaticamente a senha de administrador incorporada para uma senha aleatória a cada 90 dias. Sempre que a senha incorporada do administrador é solicitada para uso humano, um AWS ticket é criado e registrado com a AWS Directory Service equipe. As credenciais da conta são criptografadas e gerenciadas por canais seguros. Além disso, as credenciais da conta de administrador só podem ser solicitadas pela equipe AWS Directory Service de gerenciamento.

Para realizar o gerenciamento operacional do seu diretório, AWS tem controle exclusivo de contas com privilégios de administrador corporativo e administrador de domínio. Isso inclui controle exclusivo da conta de administrador do Active Directory. AWS protege essa conta automatizando o gerenciamento de senhas por meio do uso de um cofre de senhas. Durante a rotação automática da senha do administrador, AWS cria uma conta de usuário temporária e concede a ela privilégios de administrador de domínio. Esta conta temporária é usado como um backup em caso de falha na rotação de senhas na conta do administrador. Depois de alternar AWS com sucesso a senha do administrador, AWS exclui a conta temporária do administrador.

Normalmente AWS opera o diretório inteiramente por meio da automação. Caso um processo de automação não consiga resolver um problema operacional, AWS talvez seja necessário que um engenheiro de suporte faça login no seu controlador de domínio (DC) para realizar o diagnóstico. Nesses casos raros, AWS implementa um sistema de solicitação/notificação para conceder acesso. Nesse processo, a AWS automação cria uma conta de usuário com limite de tempo em seu diretório que tem permissões de administrador de domínio. AWS associa a conta do usuário ao engenheiro designado para trabalhar em seu diretório. AWS registra essa associação em nosso sistema de log e fornece ao engenheiro as credenciais a serem usadas. Todas as ações executadas pelo engenheiro serão registradas nos logs de eventos do Windows. Quando o tempo de alocado expirar, a automação excluirá a conta de usuário.

Você pode monitorar as ações de contas administrativas usando o recurso de encaminhamento de log do seu diretório. Esse recurso permite que você encaminhe os eventos de segurança do AD para o seu CloudWatch sistema, onde você pode implementar soluções de monitoramento. Para ter mais informações, consulte Habilitar o encaminhamento de logs.

Os IDs de eventos de segurança 4624, 4672 e 4648 são todos registrados quando alguém faz login em um DC de forma interativa. É possível visualizar o log de eventos de segurança do Windows para cada DC usando o Visualizador de Eventos do Microsoft Management Console (MMC) em um computador Windows associado ao domínio. Você também pode Habilitar o encaminhamento de logs enviar todos os registros de eventos de segurança para o CloudWatch Logs da sua conta.

Ocasionalmente, você pode ver usuários criados e excluídos na OU AWS reservada. AWS é responsável pelo gerenciamento e pela segurança de todos os objetos nesta OU e em qualquer outra OU ou contêiner em que não tenhamos delegado permissões para você acessar e gerenciar. É possível ver criações e exclusões nessa UO. Isso ocorre porque AWS Directory Service usa automação para alternar a senha do administrador do domínio regularmente. Quando a senha é alternada, um backup é criado para o caso da operação falhar. Quando a alternância for bem-sucedida, a conta de backup será excluída automaticamente. Além disso, no caso raro de ser necessário acesso interativo nos DCs para fins de solução de problemas, uma conta de usuário temporária é criada para ser usada por um AWS Directory Service engenheiro. Após o engenheiro concluir seu trabalho, a conta de usuário temporária será excluída. Observe que toda vez que as credenciais interativas são solicitadas para um diretório, a equipe AWS Directory Service de gerenciamento é notificada.

Principais conceitos do AWS Managed Microsoft AD

Você aproveitará ao máximo o AWS Managed Microsoft AD se conhecer seus principais conceitos.

Tópicos

Esquema do Active Directory

Um esquema é a definição de atributos e classes que fazem parte de um diretório distribuído, e é semelhante a campos e tabelas em um banco de dados. Os esquemas incluem um conjunto de regras que determinam o tipo e o formato dos dados que podem ser adicionados ou incluídos no banco de dados. A classe User é um exemplo de uma classe que é armazenada no banco de dados. Alguns exemplos de atributos da classe User podem incluir o nome, o sobrenome, o número do telefone e outras informações do usuário.

Elementos do esquema

Atributos, classes e objetos são os elementos básicos usados para compilar definições de objeto no esquema. Os tópicos a seguir fornecem detalhes sobre os elementos de esquema que você deve conhecer antes de iniciar o processo de estender seu esquema do AWS Managed Microsoft AD.

Atributos

Cada atributo do esquema, que é semelhante a um campo em um banco de dados, tem várias propriedades que definem as características do atributo. Por exemplo, a propriedade usada por clientes LDAP para ler e gravar o atributo é `LDAPDisplayName`. A propriedade `LDAPDisplayName` deve ser exclusiva em todos os atributos e classes. Para obter uma lista completa de características de atributo, consulte Características de atributos no site MSDN. Para obter mais orientações sobre como criar um novo atributo, consulte Definindo um novo atributo no site MSDN.

Classes

As classes são análogas às tabelas em um banco de dados e também têm várias propriedades a serem definidas. Por exemplo, `objectClassCategory` define a categoria de classe. Para obter uma lista completa de características de classe, consulte Características de classes de objeto no site MSDN. Para obter mais informações sobre como criar uma classe nova, consulte Definindo uma nova classe no site MSDN.

Identificador de objeto (OID)

Cada classe e atributo deve ter um OID que seja exclusivo para todos os seus objetos. Os fornecedores de software devem ter seu próprio OID para garantir a unicidade. A unicidade evita conflitos quando o mesmo atributo é usado por mais de um aplicativo para propósitos diferentes. Para garantir a unicidade, você pode obter o OID raiz de uma Autoridade de registro de nome ISO. Como alternativa, você pode obter um OID base da Microsoft. Para obter mais informações sobre OIDs e como obtê-los, consulte Identificadores de objeto no site MSDN.

Atributos vinculados a esquema

Alguns atributos estão vinculados entre duas classes com links sequenciais e regressivos. O melhor exemplo são os grupos. Quando olha para um grupo, você vê os membros do grupo; se olha para um usuário, você vê a que grupos o usuário pertence. Quando você adiciona um usuário a um grupo, o Active Directory cria um link sequencial com o grupo. Então o Active Directory adiciona um link regressivo do grupo até o usuário. Um ID de link exclusivo deve ser gerado ao criar-se um atributo que será vinculado. Para obter mais informações, consulte Atributos vinculados no site MSDN.

Tópicos relacionados

- Quando estender seu esquema do AWS Managed Microsoft AD

- Tutorial: Estendendo seu esquema AWS gerenciado do Microsoft AD

Patches e manutenção do AWS Managed Microsoft AD

O AWS Directory Service for Microsoft Active Directory, também conhecido como AWS DS para AWS Managed Microsoft AD, é, na verdade, o Microsoft Active Directory Domain Services (AD DS) fornecido como um serviço gerenciado. O sistema usa o Microsoft Windows Server 2019 para os controladores de domínio (DCs), e a AWS adiciona software aos DCs para fins de gerenciamento do serviço. A AWS atualiza (aplica patches) aos DCs para adicionar novas funcionalidades e manter o software do Microsoft Windows Server atualizado. Durante o processo de aplicação de patches, seu diretório permanece disponível para uso.

Garantia da disponibilidade

Por padrão, cada diretório consiste em dois DCs, cada um instalado em uma zona de disponibilidade diferente. A seu critério, você pode adicionar DCs para aumentar ainda mais a disponibilidade. Para ambientes críticos que precisam de alta disponibilidade e tolerância a falhas, recomendamos a implantação de DCs adicionais. AWScorrige seus DCs sequencialmente, período durante o qual o DC que AWS está ativamente aplicando patches fica indisponível. Caso um ou mais de seus DCs esteja temporariamente fora de serviço, a AWS adiará a aplicação de patches até que o diretório tenha pelo menos dois DCs operacionais. Isso permite usar os outros DCs operacionais durante o processo de aplicação de patches, o que geralmente leva de 30 a 45 minutos por DC, embora esse tempo possa variar. Para garantir que seus aplicativos possam acessar um DC operacional no caso de um ou mais DCs estarem indisponíveis por qualquer motivo, incluindo a aplicação de patches, seus aplicativos deverão usar o serviço de localizador do Windows DC e não usar endereços DC estáticos.

Noções básicas sobre o cronograma de aplicação de patches

Para manter o software do Microsoft Windows Server atualizado em seus DCs, a AWS utiliza as atualizações da Microsoft. Como a Microsoft disponibiliza o pacote cumulativo de patches mensalmente para o Windows Server, a AWS faz o melhor esforço para testar e aplicar o pacote cumulativo em todos os DCs do cliente dentro de três semanas. Além disso, a AWS revisa as atualizações que a Microsoft libera fora do pacote cumulativo mensal com base na aplicabilidade aos DCs e na urgência. Para patches de segurança que a Microsoft classifica como Críticos ou Importantes e que são relevantes para os DCs, a AWS faz todos os esforços para testar e implantar o patch dentro de cinco dias.

Contas de serviço gerenciadas pelo grupo

Com o Windows Server 2012, a Microsoft apresentou um método novo que os administradores poderiam usar para gerenciar as contas de serviço chamado Contas de serviço gerenciadas pelo grupo (gMSAs). Com o método gMSAs, os administradores de serviço não precisam mais gerenciar manualmente a sincronização da senha entre instâncias do serviço. Em vez disso, um administrador poderia simplesmente criar um gMSA no Active Directory e configurar várias instâncias de serviço para usar aquele mesmo gMSA.

Para conceder permissões de forma que os usuários do AWS Managed Microsoft AD possam criar um gMSA, você deve adicionar suas contas como um membro do grupo de segurança Administradores delegados da conta de serviço gerenciado da AWS. Por padrão, a conta de administrador é um membro desse grupo. Para obter mais informações sobre GMSAs, consulte Visão geral das contas de serviço gerenciadas em grupo no site da Microsoft. TechNet

Postagem do blog de segurança da AWS relacionada

- Como o Microsoft AD gerenciado pela AWS ajuda a simplificar a implantação e melhorar a segurança de aplicativos .NET integrados ao Active Directory

Delegação restrita de Kerberos

A delegação restrita de Kerberos é um recurso do Windows Server. Esse recursos oferece aos administradores de sistema a capacidade de especificar e impor limites de confiança de aplicativo reduzindo o escopo em que os serviços de aplicativo podem atuar em nome de um usuário. Isso pode ser útil quando você precisa configurar quais contas de serviço de front-end podem delegar aos serviços de back-end. A delegação restrita de Kerberos também impede que o gMSA se conecte a todo e qualquer serviço em nome dos seus usuários do Active Directory, o que impede um possível abuso por parte de um desenvolvedor mal-intencionado (invasor).

Por exemplo, digamos que o usuário jsmith faça login em um aplicativo de HR. Você deseja que o SQL Server aplique as permissões de banco de dados de jsmith. No entanto, por padrão, o SQL Server abre a conexão do banco de dados usando as credenciais da conta de serviço que se aplicam às hr-app-service permissões em vez das permissões configuradas pelo jsmith. É necessário possibilitar que o aplicativo de folha de pagamento do RH acesse o banco de dados do SQL Server usando as credenciais de jsmith. Para fazer isso, você habilita a delegação restrita de Kerberos para a conta de hr-app-service serviço em seu diretório gerenciado AWS do Microsoft AD em. AWS Quando jsmith fizer logon, o Active Directory fornecerá um tíquete Kerberos que o Windows usará

automaticamente quando jsmith tentar acessar outros serviços na rede. A delegação do Kerberos permite que a hr-app-service conta reutilize o tíquete jsmith Kerberos ao acessar o banco de dados, aplicando assim permissões específicas ao jsmith ao abrir a conexão do banco de dados.

Para conceder permissões que permitem aos usuários do AWS Managed Microsoft AD configurar uma delegação restrita de Kerberos, é necessário adicionar suas contas como um membro do grupo de segurança Administradores delegados de delegação Kerberos da AWS. Por padrão, a conta de administrador é um membro desse grupo. Para obter mais informações sobre a delegação restrita de Kerberos, consulte Visão geral da delegação restrita de Kerberos no site da Microsoft. TechNet

A delegação restrita baseada em recursos foi apresentada com o Windows Server 2012. Ela fornece ao administrador do serviço de back-end a capacidade de configurar a delegação restrita para o serviço.

Práticas recomendadas para o Microsoft AD AWS gerenciado

Aqui estão algumas sugestões e diretrizes que você deve considerar para evitar problemas e aproveitar ao máximo o AWS Managed Microsoft AD.

Configuração: pré-requisitos

Considere essas diretrizes antes de criar seu diretório.

Verifique se você tem o tipo de diretório correto

AWS Directory Service fornece várias maneiras de usar Microsoft Active Directory com outros AWS serviços. Você pode escolher o serviço de diretório com os recursos necessários a um custo que caiba em seu orçamento:

- AWS O Directory Service for Microsoft Active Directory é um serviço gerenciado rico em recursos Microsoft Active Directory hospedado na AWS nuvem. AWS O Microsoft AD gerenciado é sua melhor opção se você tiver mais de 5.000 usuários e precisar de uma relação de confiança configurada entre um diretório AWS hospedado e seus diretórios locais.
- O AD Connector simplesmente conecta seu local existente Active Directory a. AWS O AD Connector é a melhor opção quando você deseja usar seu diretório on-premises existente com os serviços da AWS .
- Simple AD é um diretório de baixa escala e baixo custo com compatibilidade básicaActive Directory. Ele oferece suporte a até 5.000 usuários, aplicações compatíveis com Samba 4 e compatibilidade com LDAP para aplicações compatíveis com LDAP.

Para uma comparação mais detalhada das AWS Directory Service opções, consulteQual escolher.

Verificar se suas VPCs e instâncias estão configuradas corretamente

Para se conectar, gerenciar e usar seus diretórios, é necessário configurar corretamente as VPCs às quais seus diretórios estão associados. Consulte AWS Pré-requisitos gerenciados do Microsoft AD, Pré-requisitos do AD Connector ou Pré-requisitos do Simple AD para obter informações sobre os requisitos de segurança e de rede da VPC.

Se estiver adicionando uma instância a seu domínio, verifique se você tem conectividade e acesso remoto à sua instância, conforme descrito em Associe uma instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory.

Conhecer seus limites

Saiba mais sobre os vários limites do seu tipo de diretório específico. O armazenamento disponível e o tamanho agregado dos seus objetos são as únicas limitações no número de objetos que você pode armazenar em seu diretório. Consulte AWS Cotas gerenciadas do Microsoft AD, Cotas do AD Connector ou Cotas do Simple AD para obter detalhes sobre o diretório escolhido.

Entenda a configuração e o uso do grupo de AWS segurança do seu diretório

AWS cria um grupo de segurança e o anexa às interfaces de rede elástica do controlador de domínio do seu diretório. Esse grupo de segurança bloqueia tráfego desnecessário para o controlador de domínio e permite o tráfego necessário para as comunicações do Active Directory. A AWS configura o grupo de segurança para abrir somente as portas necessárias para as comunicações do Active Directory. Na configuração padrão, o grupo de segurança aceita tráfego para essas portas a partir de qualquer endereço IP. AWS anexa o grupo de segurança às interfaces dos seus controladores de domínio, que podem ser acessadas de dentro de suas VPCs emparelhadas ou redimensionadas. Essas interfaces não são acessíveis pela Internet, mesmo que você modifique as tabelas de rotas, altere as conexões de rede à sua VPC e configure o Serviço do NAT Gateway. Sendo assim, apenas as instâncias e os computadores que têm um caminho de rede para a VPC podem acessar o diretório. Isso simplifica a configuração eliminando a necessidade de configurar intervalos de endereços específicos. Em vez disso, você configura rotas e grupos de segurança VPC que permitem o tráfego apenas de instâncias e computadores confiáveis.

Modificar o grupo de segurança do diretório

Para aumentar a segurança dos grupos de segurança de seus diretórios, você pode modificá-los para aceitar tráfego de uma lista mais restritiva de endereços IP. Por exemplo, você pode alterar

os endereços aceitos de 0.0.0.0/0 para um intervalo CIDR que seja específico para uma única sub-rede ou computador. Da mesma forma, você pode optar por restringir os endereços de destino com os quais seus controladores de domínio podem se comunicar. Faça essas alterações apenas se você compreender totalmente como funciona a filtragem do grupo de segurança. Para obter mais informações, consulte Grupos de segurança do Amazon EC2 para instâncias do Linux no Guia do usuário do Amazon EC2. Alterações impróprias podem resultar na perda de comunicações com os computadores e instâncias pretendidos. AWS recomenda que você não tente abrir portas adicionais para o controlador de domínio, pois isso diminui a segurança do seu diretório. Reveja cuidadosamente o Modelo de responsabilidade compartilhada da AWS.

> **Warning**
>
> É tecnicamente possível associar os grupos de segurança, que seu diretório usa, a outras instâncias do EC2 que você cria. No entanto, não AWS recomenda essa prática. AWS pode ter motivos para modificar o grupo de segurança sem aviso prévio para atender às necessidades funcionais ou de segurança do diretório gerenciado. Essas alterações afetam todas as instâncias com as quais você associa o grupo de segurança do diretório. Além disso, a associação do grupo de segurança do diretório às suas instâncias do EC2 cria um risco de segurança potencial para essas instâncias do EC2. O grupo de segurança do diretório aceita tráfego nas portas requeridas do Active Directory de qualquer endereço IP. Se você associar o grupo de segurança a uma instância do EC2 que tenha um endereço IP público conectado à Internet, qualquer computador na Internet poderá se comunicar com sua instância do EC2 nas portas abertas.

Configuração: criar seu diretório

Estas são algumas sugestões a serem consideradas ao criar seu diretório.

Lembre-se de seu ID e senha de administrador

Ao configurar o diretório, você fornece uma senha para a conta de administrador. Essa ID da conta é Admin for AWS Managed Microsoft AD. Lembre-se da senha criada para essa conta. Caso contrário, você não poderá adicionar objetos a seu diretório.

Criar um conjunto de opções de DHCP

Recomendamos que você crie um conjunto de opções de DHCP para seu AWS Directory Service diretório e atribua o conjunto de opções de DHCP à VPC em que seu diretório está. Dessa maneira,

todas as instâncias nessa VPC podem apontar para o domínio especificado, e os servidores DNS podem resolver seus nomes de domínio.

Para obter mais informações sobre os conjuntos de opções DHCP, consulte Criar ou alterar um conjunto de opções de DHCP.

Ativar configuração do encaminhador condicional

As seguintes configurações de encaminhamento condicional Armazene esse encaminhador condicional no Active Directory, replique-o da seguinte forma: deve estar habilitado. A ativação dessas configurações evitará que a configuração do encaminhador condicional desapareça quando um nó for substituído devido a uma falha na infraestrutura ou falha de sobrecarga.

Implantar controladores de domínio adicionais

Por padrão, AWS cria dois controladores de domínio que existem em zonas de disponibilidade separadas. Isso fornece resiliência a falhas durante a aplicação de patches de software e outros eventos que podem tornar um controlador de domínio inacessível ou indisponível. Recomendamos que você implante controladores de domínio adicionais para aumentar ainda mais a resiliência e garantir o desempenho da expansão no caso de um evento de longo prazo que afete o acesso a um controlador de domínio ou a uma zona de disponibilidade.

Para ter mais informações, consulte Use o serviço de localização de DCs do Windows.

Entender as restrições de nome de usuário para aplicações da AWS

AWS Directory Service fornece suporte para a maioria dos formatos de caracteres que podem ser usados na construção de nomes de usuário. No entanto, existem restrições de caracteres impostas aos nomes de usuário que serão usados para fazer login em AWS aplicativos, como WorkSpaces Amazon WorkMail, WorkDocs Amazon ou Amazon. QuickSight Essas restrições exigem que os seguintes caracteres não sejam usados:

- Espaços
- Caracteres multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> O símbolo@é permitido, desde que ele preceda um sufixo UPN.

Usar o diretório

Estas são algumas sugestões a serem lembradas ao usar o diretório.

Não altere usuários, grupos e unidades organizacionais predefinidos

Quando você usa AWS Directory Service para iniciar um diretório, AWS cria uma unidade organizacional (OU) que contém todos os objetos do seu diretório. Essa OU, que tem o nome de NetBIOS que você digitou quando criou seu diretório, está localizada na raiz do domínio. A raiz do domínio pertence e é gerenciada por AWS. Vários grupos e um usuário administrativo também são criados.

Não mova, exclua ou altere de qualquer maneira esses objetos predefinidos. Isso pode tornar seu diretório inacessível tanto para você quanto AWS para. Para ter mais informações, consulte O que é criado com seu Microsoft AD Active Directory AWS gerenciado.

Associe automaticamente a domínios

Ao iniciar uma instância do Windows que fará parte de um AWS Directory Service domínio, geralmente é mais fácil ingressar no domínio como parte do processo de criação da instância, em vez de adicioná-la manualmente posteriormente. Para ingressar automaticamente em um domínio, basta selecionar o diretório correto para Domain join directory ao executar uma nova instância. Você pode localizar detalhes em Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory.

Configure relações de confiança corretamente

Ao configurar a relação de confiança entre seu diretório AWS gerenciado do Microsoft AD e outro diretório, tenha em mente estas diretrizes:

- O tipo de confiança deve corresponder em ambos os lados (Floresta ou Externa)
- Verifique se a direção de confiança está configurada corretamente se estiver usando uma confiança unidirecional (Saída em domínio confiável, Entrada em domínio confiável)
- Os nomes de domínio totalmente qualificados (FQDNs) e os nomes NetBIOS devem ser exclusivos entre florestas/domínios

Para obter mais detalhes e instruções específicas sobre como configurar uma relação de confiança, consulte Criar uma relação de confiança.

Gerencie o diretório

Considere estas sugestões para gerenciar o diretório.

Acompanhe a performance do seu controlador de domínio

Para ajudar a otimizar as decisões de escalabilidade e melhorar a resiliência e o desempenho do diretório, recomendamos que você use CloudWatch métricas. Para ter mais informações, consulte Monitorar seus controladores de domínio com métricas de performance.

Para obter instruções sobre como configurar as métricas do controlador de domínio usando o CloudWatch console, consulte Como automatizar o escalonamento AWS gerenciado do Microsoft AD com base nas métricas de utilização no Blog de Segurança. AWS

Planeje cuidadosamente as extensões de esquema

Aplique cuidadosamente extensões de esquema para indexar seu diretório para consultas frequentes e importantes. Cuidado para não indexar em excesso o diretório, pois índices consomem espaço do diretório, e valores indexados que mudam com muita rapidez podem causar problemas de desempenho. Para adicionar índices, crie um arquivo LDIF (Directory Interchange Format) do LDAP (Lightweight Directory Access Protocol) e estenda sua alteração do esquema. Para ter mais informações, consulte Estender seu esquema.

Sobre balanceadores de carga

Não use um balanceador de carga na frente dos endpoints AWS gerenciados do Microsoft AD. A Microsoft desenvolveu o Active Directory (AD) para uso com um algoritmo de descoberta do controlador de domínio (DC) que encontra o DC operacional mais responsivo sem balanceamento de carga externo. Network load balancers externos detectam imprecisamente DCs ativos e podem fazer com que seu aplicativo seja enviado para um DC que esteja chegando, mas não pronto para uso. Para obter mais informações, consulte Balanceadores de carga e Active Directory na Microsoft TechNet , que recomenda corrigir aplicativos para usar o Active Directory corretamente em vez de implementar balanceadores de carga externos.

Faça um backup da sua instância

Se você decidir adicionar manualmente uma instância a um AWS Directory Service domínio existente, primeiro faça um backup ou tire um instantâneo dessa instância. Isso é especialmente importante ao ingressar em uma instância do Linux. Alguns dos procedimentos usados para adicionar uma instância, se não forem executados corretamente, podem tornar sua instância

inacessível ou não utilizável. Para ter mais informações, consulte Criar um snapshot ou restaurar seu diretório.

Configure o sistema de mensagens do SNS

Com o Amazon Simple Notification Service (Amazon SNS), é possível receber mensagens de e-mail ou de texto (SMS) quando o status de seu diretório é alterado. Você será notificado se o status do diretório mudar de Active para Impaired ou Inoperable. Você também recebe uma notificação quando o diretório retorna para um status Active.

Lembre-se também de que, se você tiver um tópico do SNS que recebe mensagens de AWS Directory Service, antes de excluir esse tópico do console do Amazon SNS, você deve associar seu diretório a um tópico do SNS diferente. Caso contrário, você correrá o risco de perder mensagens de status importantes do diretório. Para obter informações sobre como configurar o Amazon SNS, consulte Configurar notificações de status do diretório com o Amazon SNS.

Aplique configurações do serviço de diretório

AWS O Microsoft AD gerenciado permite que você personalize sua configuração de segurança para atender aos requisitos de conformidade e segurança. AWS O Microsoft AD gerenciado implanta e mantém a configuração em todos os controladores de domínio em seu diretório, inclusive ao adicionar novas regiões ou controladores de domínio adicionais. Você pode definir e aplicar essas configurações de segurança para todos os diretórios novos e existentes. Você pode fazer isso no console seguindo as etapas na UpdateSettings API Editar configurações de segurança do diretório ou por meio dela.

Para ter mais informações, consulte Definir configurações de segurança do diretório.

Remova aplicações da Amazon Enterprise antes de excluir um diretório

Antes de excluir um diretório associado a um ou mais aplicativos empresariais da Amazon, como, WorkSpaces Amazon WorkSpaces Application Manager, Amazon WorkDocs, Amazon ou Amazon WorkMail Relational Database Service (Amazon RDS), você deve primeiro remover cada aplicativo. AWS Management Console Para obter mais informações sobre como remover esses aplicativos, consulte Exclua seu Microsoft AD AWS gerenciado.

Use clientes do SMB 2.x ao acessar os compartilhamentos SYSVOL e NETLOGON

Os computadores clientes usam o Server Message Block (SMB) para acessar os compartilhamentos SYSVOL e NETLOGON nos controladores de domínio gerenciados AWS do Microsoft AD para

Política de Grupo, scripts de login e outros arquivos. AWS O Microsoft AD gerenciado oferece suporte somente para SMB versão 2.0 (SMBv2) e versões mais recentes.

Os protocolos SMBv2 e mais recentes adicionam alguns recursos que aprimoram o desempenho do cliente e aumentam a segurança dos controladores de domínio e clientes. Esta alteração segue recomendações da United States Computer Emergency Readiness Team e da Microsoft para desabilitar o SMBv1.

> **Important**
>
> Se você atualmente usa clientes do SMBv1 para acessar os compartilhamentos SYSVOL e NETLOGON do controlador do domínio, será necessário atualizar esses clientes para usar o SMBv2 ou posterior. Seu diretório funcionará corretamente, mas seus clientes SMBv1 não conseguirão se conectar aos compartilhamentos SYSVOL e NETLOGON dos controladores de domínio AWS gerenciados do Microsoft AD e também não conseguirão processar a Política de Grupo.

Os clientes do SMBv1 trabalharão com qualquer outro servidor de arquivos compatível com o SMBv1 que você tiver. No entanto, AWS recomenda que você atualize todos os seus servidores e clientes SMB para SMBv2 ou mais recente. Para saber mais sobre como desabilitar o SMBv1 e atualizá-lo para versões SMB mais recentes em seus sistemas, consulte essas postagens na Microsoft e na Documentação. TechNet Microsoft

Rastrear conexões remotas do SMBv1

Você pode revisar o log de eventos do Microsoft-Windows-SMBServer/Audit do Windows conectando-se remotamente ao controlador de domínio AWS gerenciado do Microsoft AD. Qualquer evento nesse log indica conexões SMBv1. Veja abaixo um exemplo das informações que você poderá ver em um desses logs:

Acesso do SMB1

Endereço do cliente: ###.###.###.###

Orientação:

Este evento indica que um cliente tentou acessar o servidor usando o SMB1. Para parar de auditar o acesso SMB1, use o Windows PowerShell cmdlet Set-. SmbServerConfiguration

Programar suas aplicações

Antes de programar seus aplicativos, considere o seguinte:

Use o serviço de localização de DCs do Windows

Ao desenvolver aplicativos, use o serviço localizador de DC do Windows ou use o serviço DNS dinâmico (DDNS) do seu AWS Microsoft AD gerenciado para localizar controladores de domínio (DCs). Não codifique aplicativos com o endereço de um DC. O serviço de localização de DC ajuda a garantir que a carga do diretório seja distribuída e permite que você aproveite a escalabilidade horizontal, adicionando controladores de domínio à implantação. Se você vincular o aplicativo a um DC fixo, e o DC passar por patches ou recuperação, seu aplicativo perderá acesso ao DC, em vez de usar um dos DCs restantes. Além disso, a codificação do DC pode resultar na criação de um ponto de acesso de um único DC. Em casos graves, a criação do ponto de acesso pode fazer com que o DC não responda. Esses casos também podem fazer com que a automação do AWS diretório sinalize o diretório como prejudicado e desencadeie processos de recuperação que substituam o DC que não responde.

Faça um teste de carga antes de implantar no ambiente de produção

Faça testes laboratoriais com objetos e solicitações que representam sua workload de produção para confirmar se o diretório é dimensionado conforme a carga da aplicação. Se você precisar de capacidade adicional, teste com outros DCs enquanto distribui as solicitações entre os DCs. Para ter mais informações, consulte Implantar controladores de domínio adicionais.

Use consultas LDAP eficientes

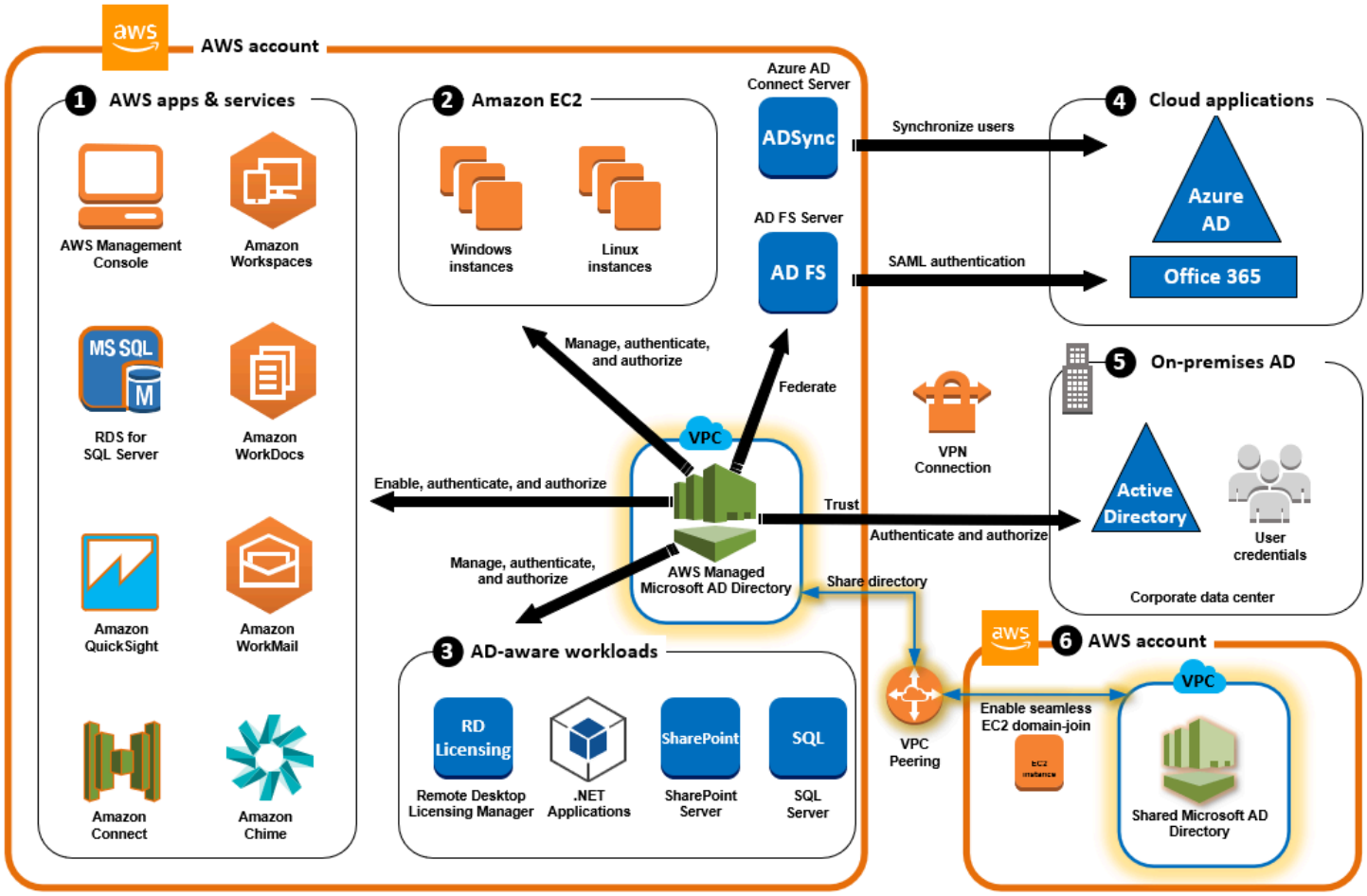
Muitas consultas LDAP para um controlador de domínio em dezenas de milhares de objetos podem consumir ciclos de CPU significativos em um único DC, resultando em pontos de acesso. Isso pode afetar aplicativos que compartilham o mesmo DC durante a consulta.

Casos de uso do Microsoft AD AWS gerenciado

Com o AWS Managed Microsoft AD, você pode compartilhar um único diretório para vários casos de uso. Por exemplo, você pode compartilhar um diretório para autenticar e autorizar o acesso para aplicações .NET, Amazon RDS para SQL Server com a autenticação do Windows habilitada e o Amazon Chime para mensagens e videoconferência.

O diagrama a seguir mostra alguns dos casos de uso do seu diretório AWS gerenciado do Microsoft AD. Isso inclui a capacidade de conceder aos usuários acesso a aplicativos externos na nuvem e

permitir que os usuários locais do Active Directory gerenciem e tenham acesso aos recursos na AWS nuvem.



Use o Microsoft AD AWS gerenciado para qualquer um dos seguintes casos de uso comercial.

Tópicos

- Caso de uso 1: faça login em AWS aplicativos e serviços com credenciais do Active Directory
- Caso de uso 2: Gerencie instâncias do Amazon EC2
- Caso de uso 3: Forneça serviços de diretório para suas cargas de trabalho compatíveis com o Active Directory
- Caso de uso 4: AWS IAM Identity Center para o Office 365 e outros aplicativos em nuvem
- Caso de uso 5: Estenda seu Active Directory local para a nuvem AWS
- Caso de uso 6: compartilhe seu diretório para unir facilmente instâncias do Amazon EC2 a um domínio entre contas AWS

Caso de uso 1: faça login em AWS aplicativos e serviços com credenciais do Active Directory

Você pode habilitar vários AWS aplicativos e serviços AWS Client VPN, como, AWS Management ConsoleAWS IAM Identity Center, Amazon Chime, Amazon Connect, Amazon FSx, Amazon, QuickSight Amazon RDS para SQL Server, Amazon WorkSpaces, WorkDocs WorkMail Amazon e usar AWS seu diretório gerenciado do Microsoft AD. Quando você habilita um AWS aplicativo ou serviço em seu diretório, seus usuários podem acessar o aplicativo ou serviço com suas credenciais do Active Directory.

Por exemplo, você pode permitir que seus usuários entrem no AWS Management Console com suas credenciais do Active Directory. Para fazer isso, você habilita o AWS Management Console como um aplicativo em seu diretório e, em seguida, atribui seus usuários e grupos do Active Directory às funções do IAM. Quando seus usuários fazem login no AWS Management Console, eles assumem uma função do IAM para gerenciar AWS recursos. Isso facilita conceder aos usuários acesso ao AWS Management Console sem a necessidade de configurar e gerenciar uma infraestrutura SAML separada.

Para aprimorar ainda mais a experiência do usuário final, você pode ativar os recursos de login único para a Amazon WorkDocs, que fornecem aos usuários a capacidade de acessar a Amazon a WorkDocs partir de um computador associado ao diretório sem precisar inserir suas credenciais separadamente.

Você pode conceder acesso às contas de usuário no seu diretório ou no Active Directory local, para que eles possam entrar no AWS Management Console ou por meio do AWS CLI usando suas credenciais e permissões existentes para gerenciar AWS recursos atribuindo funções do IAM diretamente às contas de usuário existentes.

Integração do FSx for Windows File Server AWS com o Microsoft AD gerenciado

A integração do FSx for Windows File Server com o AWS Managed Microsoft AD fornece um sistema de arquivos de protocolo Server Message Block (SMB) nativo totalmente gerenciado baseado no Microsoft Windows que permite mover facilmente seus aplicativos e clientes baseados em Windows (que utilizam armazenamento compartilhado de arquivos) para o. AWS Embora o FSx para Windows File Server possa ser integrado a um Microsoft Active Directory autogerenciado, não discutiremos esse cenário aqui.

Casos de uso e recursos comuns do Amazon FSx

Esta seção fornece uma referência aos recursos sobre integrações comuns do FSx for Windows File Server com casos de uso AWS gerenciados do Microsoft AD. Cada um dos casos de uso desta seção começa com uma configuração básica do AWS Managed Microsoft AD e FSx para Windows File Server. Para obter mais informações sobre como criar essas configurações, consulte:

- Introdução ao AWS Managed Microsoft AD
- Conceitos básicos do Amazon FSx

FSx para Windows File Server como armazenamento persistente em contêineres do Windows

O Amazon Elastic Container Service (ECS) oferece suporte a contêineres do Windows em instâncias de contêiner executadas com a AMI do Windows otimizada para Amazon ECS. As instâncias de contêiner do Windows usam sua própria versão do agente de contêiner do Amazon ECS. Na AMI do Windows otimizada para Amazon ECS, o agente de contêiner do Amazon ECS é executado como um serviço no host.

O Amazon ECS é compatível com a autenticação do Active Directory para contêineres do Windows por meio de um tipo especial de conta de serviço denominado Conta de serviço gerenciada pelo grupo (gMSA). Como os contêineres do Windows não podem ser associados ao domínio, os contêineres do Windows devem ser configurados para ser executado com o gMSA.

Itens relacionados

- Usar o FSx para Windows File Server como armazenamento persistente em contêineres do Windows
- Contas de serviço gerenciadas pelo grupo

Suporte ao Amazon AppStream 2.0

O Amazon AppStream 2.0 é um serviço de streaming de aplicativos totalmente gerenciado. Ele fornece toda uma variedade de soluções para os usuários salvarem e acessarem dados por meio de suas aplicações. O Amazon FSx with AppStream 2.0 fornece uma unidade pessoal de armazenamento persistente usando o Amazon FSx e pode ser configurado para fornecer uma pasta compartilhada para acessar arquivos comuns.

Itens relacionados

- Passo a passo 4: Usando o Amazon FSx com o Amazon 2.0 AppStream
- Usando o Amazon FSx com o Amazon 2.0 AppStream
- Usando o Active Directory com AppStream 2.0

Suporte a Microsoft SQL Server

O FSx para Windows File Server pode ser usado como uma opção de armazenamento para o Microsoft SQL Server 2012 (a partir da versão 2012 11.x) e bancos de dados de sistema mais recentes (incluindo Master, Model, MSDB e TempDB) e para bancos de dados de usuários do Database Engine.

Itens relacionados

- Instalar o SQL Server com armazenamento de compartilhamento de arquivos SMB
- Simplifique suas implantações de alta disponibilidade do Microsoft SQL Server usando o FSx para Windows File Server
- Contas de serviço gerenciadas pelo grupo

Suporte a pastas iniciais e perfis de usuário Roaming

O FSx para Windows File Server pode ser usado para armazenar dados das pastas iniciais dos usuários do Active Directory e de Meus Documentos em um local central. O FSx para Windows File Server também pode ser usado para armazenar dados de perfis de usuário Roaming.

Itens relacionados

- Diretórios iniciais do Windows simplificados com o Amazon FSx
- Implantação de perfis de usuário roaming
- Usando o FSx for Windows File Server com WorkSpaces

Suporte ao compartilhamento de arquivos em rede

Os compartilhamentos de arquivos em rede em um FSx para Windows File Server fornecem uma solução de compartilhamento de arquivos gerenciada e escalável. Um caso de uso são unidades mapeadas para clientes que podem ser criadas manualmente ou por meio da política de grupo.

Itens relacionados

- Passo a passo 6: aumentar a performance com fragmentos
- Mapeamento de unidades
- Usando o FSx for Windows File Server com WorkSpaces

Suporte à instalação de software de política de grupo

Como o tamanho e a performance da pasta SYSVOL são limitados, você deve, como prática recomendada, evitar armazenar dados como arquivos de instalação de software nessa pasta. Como possível solução, o FSx para Windows File Server pode ser configurado para armazenar todos os arquivos de software instalados usando a política de grupo.

Itens relacionados

- Use a Política de Grupo para instalar remotamente o software

Suporte a destino do backup do Windows Server

O FSx para Windows File Server pode ser configurado como uma unidade de destino do backup do Windows Server usando o compartilhamento de arquivos UNC. Nesse caso, você especificaria o caminho UNC para seu FSx para Windows File Server em vez de para o volume do EBS anexado.

Itens relacionados

- Executar uma recuperação do estado do sistema do seu servidor

O Amazon FSx também oferece suporte ao compartilhamento gerenciado de diretórios do AWS Microsoft AD. Para obter mais informações, consulte:

- Compartilhar seu diretório
- Usando o Amazon FSx com o Managed AWS Microsoft AD em uma VPC ou conta diferente

Integração do Amazon RDS com o AWS Managed Microsoft AD

O Amazon RDS oferece suporte à autenticação externa de usuários de banco de dados usando o Kerberos e o Microsoft Active Directory. O Kerberos é um protocolo de autenticação de rede que usa tíquetes e criptografia de chave simétrica para eliminar a necessidade de transmitir senhas pela rede. O suporte do Amazon RDS ao Kerberos e ao Active Directory oferece os benefícios de autenticação única e autenticação centralizada dos usuários do banco de dados.

Para começar a usar esse caso de uso, primeiro você precisará definir uma configuração básica do AWS Managed Microsoft AD e do Amazon RDS.

- Introdução ao AWS Managed Microsoft AD
- Conceitos básicos do Amazon RDS

Todos os casos de uso mencionados abaixo começarão com uma base AWS gerenciada do Microsoft AD e do Amazon RDS e abordarão como integrar o Amazon RDS com o AWS Microsoft AD gerenciado.

- Usar a autenticação do Windows com uma instância de banco de dados do Amazon RDS para SQL Server
- Usar a autenticação Kerberos para MySQL
- Usar a autenticação Kerberos com o Amazon RDS para Oracle
- Usar a autenticação Kerberos com o Amazon RDS para PostgreSQL

O Amazon RDS também oferece suporte ao compartilhamento AWS gerenciado de diretórios do Microsoft AD. Para obter mais informações, consulte:

- Compartilhar seu diretório
- Associar instâncias de banco de dados do Amazon RDS a um único domínio compartilhado

Para obter mais informações sobre como associar um Amazon RDS para SQL Server ao seu Active Directory, consulte Associar o Amazon RDS para SQL Server ao seu Active Directory autogerenciado.

Aplicação .NET que usa o Amazon RDS para SQL Server com contas de serviços gerenciados em grupo

É possível integrar o Amazon RDS para SQL Server a uma aplicação .NET básica e a contas de serviços gerenciadas em grupo (gMSAs). Para obter mais informações, consulte Como o Microsoft AD AWS gerenciado ajuda a simplificar a implantação e melhorar a segurança dos aplicativos.NET integrados ao Active Directory

Caso de uso 2: Gerencie instâncias do Amazon EC2

Usando ferramentas familiares de administração do Active Directory, você pode aplicar objetos de política de grupo (GPOs) do Active Directory para gerenciar centralmente suas instâncias do Amazon EC2 para Windows ou Linux unindo suas instâncias ao seu domínio AWS gerenciado do Microsoft AD.

Além disso, seus usuários podem entrar em suas instâncias com suas credenciais do Active Directory. Isso elimina a necessidade de usar credenciais de instâncias individuais ou distribuir arquivos de chave privada (PEM). Isso facilita a concessão ou revogação instantânea do acesso aos usuários usando as ferramentas de administração de usuários do Active Directory que você já usa.

Caso de uso 3: Forneça serviços de diretório para suas cargas de trabalho compatíveis com o Active Directory

AWS O Microsoft AD gerenciado é um Microsoft Active Directory real que permite executar cargas de trabalho tradicionais compatíveis com o Active Directory, como o Remote Desktop Licensing Manager e o SharePoint Microsoft SQL Server Always On in the Cloud. AWS AWS O Microsoft AD gerenciado também ajuda você a simplificar e melhorar a segurança dos aplicativos.NET integrados ao Active Directory usando contas de serviços gerenciados em grupo (GMSAs) e a delegação restrita Kerberos (KCD).

Caso de uso 4: AWS IAM Identity Center para o Office 365 e outros aplicativos em nuvem

Você pode usar o AWS Managed Microsoft AD AWS IAM Identity Center para fornecer aplicativos em nuvem. Você pode usar Microsoft Entra Connect (anteriormente conhecido comoAzure Active Directory Connect) para sincronizar seus usuários com Microsoft Entra (anteriormente conhecido como Azure Active Directory (AzureAD)) e, em seguida, usar os Serviços de Federação do Active Directory (AD FS) para que seus usuários possam acessar o Microsoft Office 365 e outros aplicativos de nuvem SAML 2.0 usando suas credenciais do Active Directory.

A integração do AWS Managed Microsoft AD com o IAM Identity Center adiciona recursos de SAML ao seu AWS Microsoft AD gerenciado e/ou aos seus domínios confiáveis locais. Depois de integrados, seus usuários podem usar o IAM Identity Center com serviços compatíveis com SAML, incluindo aplicativos de nuvem de terceiros, como Office 365, Concur e Salesforce, sem precisar configurar uma infraestrutura SAML. AWS Management Console Para uma demonstração sobre o

processo de permitir que seus usuários locais usem o IAM Identity Center, veja o YouTube vídeo a seguir.

> **Note**
>
> AWS O Single Sign-On foi renomeado para IAM Identity Center.

Caso de uso 5: Estenda seu Active Directory local para a nuvem AWS

Se você já tem uma infraestrutura do Active Directory e deseja usá-la ao migrar cargas de trabalho compatíveis com o Active Directory para a nuvem AWS , o Managed AWS Microsoft AD pode ajudar. Você pode usar relações de confiança do Active Directory para conectar o Microsoft AD AWS gerenciado ao seu Active Directory existente. Isso significa que seus usuários podem acessar AWS aplicativos e aplicativos compatíveis com o Active Directory com suas credenciais locais do Active Directory, sem precisar sincronizar usuários, grupos ou senhas.

Por exemplo, seus usuários podem fazer login no AWS Management Console e na Amazon WorkSpaces usando seus nomes de usuário e senhas existentes do Active Directory. Além disso, quando você usa aplicativos compatíveis com o Active Directory, como SharePoint com o Managed AWS Microsoft AD, seus usuários conectados do Windows podem acessar esses aplicativos sem precisar inserir credenciais novamente.

Você também pode migrar seu domínio local do Active Directory AWS para se livrar da carga operacional de sua infraestrutura do Active Directory usando o Active Directory Migration Toolkit (ADMT) junto com o Password Export Service (PES) para realizar a migração.

Caso de uso 6: compartilhe seu diretório para unir facilmente instâncias do Amazon EC2 a um domínio entre contas AWS

Compartilhar seu diretório em várias AWS contas permite que você gerencie AWS serviços como o Amazon EC2 com facilidade, sem a necessidade de operar um diretório para cada conta e cada VPC. Você pode usar seu diretório de qualquer conta da AWS e de qualquer Amazon VPC dentro de uma região da AWS . Esse recurso torna mais fácil e econômico o gerenciamento de cargas de trabalho com reconhecimento do diretório com um único diretório entre contas e VPCs. Por exemplo, agora você pode gerenciar suas workloads do Windows implantadas em instâncias do EC2 em várias contas e VPCs facilmente usando um único diretório do AWS Managed Microsoft AD.

Ao compartilhar seu diretório AWS gerenciado do Microsoft AD com outra AWS conta, você pode usar o console do Amazon EC2 ou AWS Systems Managerunir facilmente suas instâncias de qualquer Amazon VPC dentro da conta e da região. AWS Você pode implantar rapidamente as cargas de trabalho com reconhecimento do diretório em instâncias do EC2 eliminando a necessidade de incluir manualmente suas instâncias em um domínio ou implantar diretórios em cada conta e VPC. Para ter mais informações, consulte Compartilhar seu diretório.

Como administrar o Microsoft AD AWS gerenciado

Esta seção lista todos os procedimentos para operar e manter um ambiente Microsoft AD AWS gerenciado.

Tópicos

- Proteger seu diretório do AWS Managed Microsoft AD
- Monitorar seu AWS Managed Microsoft AD
- Replicação em várias regiões
- Compartilhar seu diretório
- Associe uma instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory
- Gerenciar usuários e grupos no AWS Microsoft Managed AD
- Conecte-se à sua infraestrutura existente do Active Directory
- Conecte seu Microsoft AD AWS gerenciado ao Microsoft Entra Connect Sync
- Estender seu esquema
- Mantenha seu diretório AWS gerenciado do Microsoft AD
- Conceder a usuários e grupos acesso aos recursos da AWS
- Permita o acesso a AWS aplicativos e serviços
- Habilitar acesso ao AWS Management Console com as credenciais do AD
- Implantar controladores de domínio adicionais
- Migrar usuários do Active Directory para o AWS Managed Microsoft AD

Proteger seu diretório do AWS Managed Microsoft AD

Esta seção descreve considerações para proteger seu ambiente do AWS Managed Microsoft AD.

Tópicos

- Gerenciar políticas de senha para o AWS Managed Microsoft AD
- Habilite a autenticação multifator para o AWS Managed Microsoft AD
- Habilite LDAP ou LDAPS seguros
- Gerencie a conformidade do AWS Managed Microsoft AD
- Melhorar a configuração de segurança de rede do AWS Managed Microsoft AD
- Definir configurações de segurança do diretório
- Configurar o AWS Private CA conector para AD

Gerenciar políticas de senha para o AWS Managed Microsoft AD

AWS O Microsoft AD gerenciado permite que você defina e atribua diferentes políticas de bloqueio de senha e conta (também conhecidas como políticas de senha refinadas) para grupos de usuários que você gerencia em seu domínio gerenciado do AWS Microsoft AD. Quando você cria um diretório AWS gerenciado do Microsoft AD, uma política de domínio padrão é criada e aplicada aoActive Directory. Essa política inclui as seguintes configurações:

Política	Configuração
Aplicar histórico de senha	24 senhas memorizadas
Tempo de vida máximo da senha	42 dias *
Tempo de vida mínimo da senha	1 dia
Tamanho mínimo da senha	7 caracteres
A senha deve atender aos requisitos de complexidade	Habilitado
Armazenar senhas com criptografia reversível	Desabilitado

* Nota: o tempo máximo de 42 dias da senha inclui a senha de administrador.

Por exemplo, você pode atribuir uma configuração de política menos rigorosa a funcionários que têm acesso apenas a informações de baixa de suscetibilidade. Para os gerentes sênior que acessam regularmente informações confidenciais, você poderá aplicar configurações mais restritas.

A seguir estão os recursos para saber mais sobre políticas Microsoft Active Directory de senha e políticas de segurança refinadas:

- Definir as configurações da política de segurança
- Requisitos de complexidade da senha
- Considerações sobre a complexidade da senha e a segurança

AWS fornece um conjunto de políticas de senha refinadas no AWS Microsoft AD gerenciado que você pode configurar e atribuir aos seus grupos. Para configurar as políticas, você pode usar ferramentas de Microsoft política padrão, como o Centro Active Directory Administrativo. Para começar a usar as ferramentas Microsoft políticas, consulteInstale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado.

Como as políticas de senha são aplicadas

Há diferenças na forma como as políticas de senha refinadas são aplicadas, dependendo se a senha foi redefinida ou se a senha foi alterada. Os usuários do domínio podem alterar sua própria senha. Um Active Directory administrador ou usuário com as permissões necessárias pode redefinir as senhas dos usuários. Consulte a tabela a seguir para obter mais informações.

Política	Redefinição de senha	Alteração de senha
Aplicar histórico de senha	 No (Não)	 Yes (Sim)
Tempo de vida máximo da senha	 Yes (Sim)	 Yes (Sim)
Tempo de vida mínimo da senha	 No (Não)	 Yes (Sim)

Política	Redefinição de senha	Alteração de senha
Tamanho mínimo da senha	 Yes (Sim)	 Yes (Sim)
A senha deve atender aos requisitos de complexidade	 Yes (Sim)	 Yes (Sim)

Essas diferenças têm implicações de segurança. Por exemplo, sempre que a senha de um usuário é redefinida, as políticas de imposição do histórico de senhas e da idade mínima da senha não são aplicadas. Para obter mais informações, consulte a documentação da Microsoft sobre as considerações de segurança relacionadas às políticas de imposição do histórico de senhas e da idade mínima da senha.

Tópicos

- Configurações de políticas compatíveis
- Delegar quem pode gerenciar suas políticas de senha
- Atribuir políticas de senha aos usuários

Artigo do blog AWS de segurança relacionado

- Como configurar políticas de senha ainda mais fortes para ajudar a atender aos seus padrões de segurança usando AWS Directory Service o Microsoft AD AWS gerenciado

Configurações de políticas compatíveis

AWS O Microsoft AD gerenciado inclui cinco políticas refinadas com um valor de precedência não editável. As políticas têm algumas propriedades que você pode configurar para reforçar as ações de bloqueio de senhas e conta no caso de falhas de login. Você pode atribuir as políticas a zero ou mais grupos do Active Directory. Se um usuário final é membro de vários grupos e recebe mais de uma política de senha, o Active Directory aplica a política com o menor valor de precedência.

AWS políticas de senha predefinidas

A tabela a seguir lista as cinco políticas incluídas em seu diretório AWS gerenciado do Microsoft AD e seu valor de precedência atribuído. Para ter mais informações, consulte Precedência.

Nome da política	Precedência
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

Propriedades de políticas de senha

Você pode editar as propriedades a seguir em suas políticas de senha a fim de que se adaptem aos padrões de conformidade que atendam às suas necessidades comerciais.

- Nome da política
- Impor o histórico de senhas
- Tamanho mínimo da senha
- Tempo de vida mínimo da senha
- Tempo de vida máximo da senha
- Armazenar senhas com criptografia reversível
- A senha deve atender aos requisitos de complexidade

Você não pode modificar os valores de precedência dessas políticas. Para obter mais detalhes sobre como essas configurações afetam a imposição de senhas, consulte AD DS: políticas de senha refinadas no site da Microsoft. TechNet Para obter informações gerais sobre essas políticas, consulte Política de senha no TechNet site da Microsoft.

Políticas de bloqueio de contas

Você também pode modificar as propriedades a seguir das suas políticas de senha para especificar se e como Active Directory deve bloquear uma conta após falhas de login:

- Número de tentativas de login com falha permitidas
- Duração de bloqueio de conta
- Redefinir tentativas de login com falha após algum período

Para obter informações gerais sobre essas políticas, consulte Política de bloqueio de conta no TechNet site da Microsoft.

Precedência

As políticas com um valor de precedência menor têm prioridade mais alta. Você atribui políticas de senha a grupos de segurança do Active Directory. Embora você deva aplicar uma única política a um grupo de segurança, um único usuário pode receber mais de uma política de senha. Por exemplo, suponha que `jsmith` seja membro dos grupos HR e MANAGERS. Se você atribuir a política CustomerPSO-05 (que tem uma precedência de 50) ao grupo HR e a política CustomerPSO-04 (que tem uma precedência de 40) ao grupo MANAGERS, CustomerPSO-04 terá prioridade e o Active Directory aplicará essa política ao usuário `jsmith`.

Se você atribuir várias políticas a um usuário ou grupo, o Active Directory determinará a política resultante de acordo com o seguinte:

1. Uma política que você atribui diretamente ao objeto de usuário é aplicável.
2. Se nenhuma política é atribuída diretamente ao objeto de usuário, será aplicada a política com o menor valor de precedência entre todas as políticas recebidas pelo usuário como resultado de uma associação de grupos.

Para obter detalhes adicionais, consulte AD DS: políticas de senha refinadas no site da Microsoft. TechNet

Delegar quem pode gerenciar suas políticas de senha

Você pode delegar permissões para gerenciar políticas de senha a contas de usuário específicas criadas no Microsoft AD AWS gerenciado adicionando as contas ao grupo de segurança Administradores de Política de Senha AWS Delegada de Precisão Granular. Quando uma conta

passa a ser membro desse grupo, ela tem permissões para editar e configurar qualquer uma das políticas de senha listadas anteriormente.

Para delegar quem pode gerenciar as políticas de senha

1. Inicie o centro administrativo do Active Directory (ADAC) a partir de qualquer instância EC2 gerenciada que você associou ao seu domínio gerenciado AWS do Microsoft AD.
2. Alterne para a Visualização em árvore e navegue até a UO Grupos delegados da AWS . Para obter mais informações sobre essa UO, consulte O que é criado com seu Microsoft AD Active Directory AWS gerenciado.
3. Encontre o grupo de usuários Administradores delegados de políticas de senhas minuciosas da AWS . Adicione quaisquer usuários ou grupos do domínio a esse grupo.

Atribuir políticas de senha aos usuários

As contas de usuário que são membros do grupo de segurança Administradores delegados de políticas de senhas minuciosas da AWS podem usar o procedimento a seguir para atribuir políticas a usuários e grupos de segurança.

Para atribuir políticas de senha aos usuários

1. Inicie o centro administrativo do Active Directory (ADAC) a partir de qualquer instância EC2 gerenciada que você associou ao seu domínio gerenciado AWS do Microsoft AD.
2. Alterne para a Exibição em árvore e navegue até System\Password Settings Container.
3. Clique duas vezes na política minuciosa que deseja editar. Clique em Add (Adicionar) para editar as propriedades de políticas e adicionar usuários ou grupos de segurança à política. Para mais informações sobre as políticas minuciosas padrão fornecidas com o AWS Managed Microsoft AD consulte AWS políticas de senha predefinidas.
4. Para verificar se a política de senha foi aplicada, execute o seguinte PowerShell comando:

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

> **Note**
>
> Evite usar o comando `net user`, pois seus resultados podem ser imprecisos.

Se você não configurar nenhuma das cinco políticas de senha em seu diretório AWS gerenciado do Microsoft AD, o Active Directory usará a política de grupo de domínio padrão. Para obter mais detalhes sobre como usar o Contêiner de configurações de senha, consulte este post no blog da Microsoft.

Habilite a autenticação multifator para o AWS Managed Microsoft AD

Você pode habilitar a autenticação multifator (MFA) para seu diretório AWS gerenciado do Microsoft AD para aumentar a segurança quando seus usuários especificam suas credenciais do AD para acessar. Aplicações da Amazon Enterprise compatíveis Quando você habilita a MFA, os usuários inserem nome de usuário e senha (primeiro fator) normalmente, depois inserem um código de autenticação (segundo fator) obtido pela sua solução de MFA virtual ou de hardware. Esses fatores juntos proporcionam segurança adicional, impedindo o acesso aos seus aplicativos empresariais da Amazon, a menos que os usuários informem credenciais válidas e um código válido de MFA.

Para habilitar a MFA, é necessário ter uma solução de MFA que seja um servidor Remote Authentication Dial-in User Service (RADIUS) ou MFA, ou ter um plug-in MFA para um servidor RADIUS já implementado na sua infraestrutura on-premises. A solução de MFA deve implementar Senhas únicas (OTP) que os usuários conseguem pelo dispositivo de hardware ou por um software em execução em um dispositivo, como telefone celular.

O RADIUS é um protocolo de cliente/servidor padrão da indústria que fornece autenticação, autorização e gerenciamento de contas para que os usuários se conectem com serviços de rede. AWS O Microsoft AD gerenciado inclui um cliente RADIUS que se conecta ao servidor RADIUS no qual você implementou sua solução de MFA. Seu servidor RADIUS valida o nome de usuário e código OTP. Se o servidor RADIUS validar com êxito o usuário, o Managed AWS Microsoft AD autenticará o usuário no Active Directory. Após a autenticação bem-sucedida do Active Directory, os usuários poderão acessar o AWS aplicativo. A comunicação entre o cliente Microsoft AD RADIUS AWS gerenciado e seu servidor RADIUS exige que você configure grupos de AWS segurança que permitam a comunicação pela porta 1812.

Você pode habilitar a autenticação multifator para seu diretório AWS gerenciado do Microsoft AD executando o procedimento a seguir. Para obter mais informações sobre como configurar seu servidor RADIUS para funcionar com AWS Directory Service e MFA, consulte Pré-requisitos da autenticação multifator.

Considerações

A seguir estão algumas considerações sobre a autenticação multifator para seu AWS Microsoft AD gerenciado:

- A autenticação multifator não está disponível para o Simple AD. No entanto, o MFA pode ser habilitado para seu diretório do AD Connector. Para ter mais informações, consulte Habilitar a autenticação multifator para o AD Connector.
- O MFA é um recurso regional do Managed AWS Microsoft AD. Se você estiver usando a Replicação em várias regiões, os procedimentos a seguir deverão ser aplicados separadamente em cada região. Para ter mais informações, consulte Recursos globais versus regionais.
- Se você pretende usar o Microsoft AD AWS gerenciado para comunicações externas, recomendamos que você configure um Gateway de Internet de Tradução de Endereços de Rede (NAT) ou um Gateway de Internet fora da AWS rede para essas comunicações.
  - Se você deseja oferecer suporte a comunicações externas entre seu Microsoft AD AWS gerenciado e seu servidor RADIUS hospedado na AWS rede, entre em contato com AWS Support.

Habilite a autenticação multifator para o AWS Managed Microsoft AD

O procedimento a seguir mostra como habilitar a autenticação multifator para o AWS Managed Microsoft AD.

1. Identifique o endereço IP do seu servidor RADIUS MFA e seu diretório AWS gerenciado do Microsoft AD.
2. Edite seus grupos de segurança da Virtual Private Cloud (VPC) para permitir a comunicação pela porta 1812 entre seus endpoints IP gerenciados AWS do Microsoft AD e seu servidor RADIUS MFA.
3. No painel de navegação do console do AWS Directory Service selecione Diretórios.
4. Escolha o link da ID do diretório para seu diretório AWS gerenciado do Microsoft AD.
5. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja habilitar a MFA e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
6. Na seção Multi-factor authentication (Autenticação multifator), escolha Actions (Ações) e Enable (Habilitar).
7. Na página Habilitar a autenticação multifator (MFA), forneça os seguintes valores:

Rótulo de exibição

Forneça um nome de rótulo.

Nome de DNS ou endereços IP do servidor RADIUS

O load balancer dos endpoints do servidor RADIUS ou do endereço IP do servidor RADIUS. Você pode inserir vários endereços IP separados por vírgulas (por exemplo, `192.0.0.0,192.0.0.12`).

> **Note**
>
> O RADIUS MFA é aplicável somente para autenticar AWS Management Console o acesso aos aplicativos e serviços da Amazon Enterprise WorkSpaces, como Amazon ou QuickSight Amazon Chime. Ele não fornece MFA para cargas de trabalho do Windows em execução em instâncias do EC2 nem para login em uma instância do EC2. AWS Directory Service não oferece suporte à autenticação RADIUS Challenge/Response.
>
> Os usuários devem ter o código de MFA no momento em que inserem o nome de usuário e a senha. Como alternativa, você deve usar uma solução que realize MFA, out-of-band como verificação de texto por SMS para o usuário. Nas soluções de out-of-band MFA, você deve se certificar de definir o valor de tempo limite do RADIUS de forma adequada para sua solução. Ao usar uma solução de out-of-band MFA, a página de login solicitará ao usuário um código de MFA. Nesse caso, os usuários devem inserir a senha no campo de senha e no campo de MFA.

Porta

A porta que o servidor RADIUS está usando para comunicações. Sua rede local deve permitir tráfego de entrada pela porta padrão do servidor RADIUS (UDP: 1812) dos servidores. AWS Directory Service

Shared secret code (Código secreto compartilhado)

O código secreto compartilhado que foi especificado quando os endpoints do RADIUS foram criados.

Confirm shared secret code (Confirmar código secreto compartilhado)

Confirme o código secreto compartilhado para os endpoints do RADIUS.

Protocolo

Selecione o protocolo que foi especificado quando os endpoints do RADIUS foram criados.

Tempo limite do servidor (em segundos)

O tempo de espera, em segundos, para o servidor RADIUS responder. Esse valor deve estar entre 1 e 50.

> **Note**
>
> Recomendamos configurar o tempo limite do servidor RADIUS para 20 segundos ou menos. Se o tempo limite exceder 20 segundos, o sistema não poderá tentar novamente com outro servidor RADIUS, o que poderá resultar em uma falha de tempo limite.

Máximo de novas tentativas de solicitação RADIUS

O número de tentativas de comunicação com o servidor RADIUS. Esse valor deve estar entre 0 e 10.

A autenticação multifator está disponível quando o Status RADIUS muda para Habilitado.

8. Escolha Habilitar.

Aplicações da Amazon Enterprise compatíveis

Todos os aplicativos de TI da Amazon Enterprise WorkSpaces, incluindo Amazon WorkDocs, Amazon WorkMail, Amazon QuickSight, e o acesso AWS IAM Identity Center e AWS Management Console são suportados ao usar o Microsoft AD AWS gerenciado e o AD Connector com MFA.

Para obter informações sobre como configurar o acesso básico do usuário aos aplicativos Amazon Enterprise, o AWS Single Sign-On e o AWS Management Console uso AWS Directory Service, consulte e. Permita o acesso a AWS aplicativos e serviços Habilitar acesso ao AWS Management Console com as credenciais do AD

Artigo do blog AWS de segurança relacionado

- Como habilitar a autenticação multifator para AWS serviços usando o Microsoft AD AWS gerenciado e credenciais locais

Habilite LDAP ou LDAPS seguros

O LDAP (Lightweight Directory Access Protocol) é um protocolo de comunicações padrão usado para ler e gravar dados no Active Directory. Alguns aplicativos utilizam o LDAP para adicionar, remover ou pesquisar usuários e grupos no Active Directory ou para transportar credenciais para autenticar usuários no Active Directory. Cada comunicação LDAP inclui um cliente (como um aplicativo) e um servidor (como o Active Directory).

Por padrão, as comunicações sobre LDAP não são criptografadas. Isso permite que um usuário malicioso use o software de monitoramento de rede para visualizar pacotes de dados na conexão. Isso explica porque muitas políticas de segurança corporativas geralmente exigem que as organizações criptografem todas as comunicações LDAP.

Para mitigar essa forma de exposição de dados, o AWS Managed Microsoft AD oferece uma opção: você pode habilitar o LDAP via Secure Sockets Layer (SSL) /Transport Layer Security (TLS), também conhecido como LDAPS. Com o LDAPS, é possível aumentar a segurança em toda a rede. Você também pode atender aos requisitos de conformidade criptografando todas as comunicações entre seus aplicativos habilitados para LDAP e o Managed AWS Microsoft AD.

AWS O Microsoft AD gerenciado fornece suporte para LDAPS nos seguintes cenários de implantação:

- O LDAPS do lado do servidor criptografa as comunicações LDAP entre seus aplicativos comerciais ou domésticos compatíveis com LDAP (atuando como clientes LDAP) e o Managed Microsoft AD (atuando como um servidor LDAP). AWS Para ter mais informações, consulte Habilitar o LDAPS do lado do servidor usando o Microsoft AD gerenciado AWS.
- O LDAPS do lado do cliente criptografa as comunicações LDAP entre AWS aplicativos, como WorkSpaces (atuando como clientes LDAP) e seu Active Directory autogerenciado (local) (atuando como servidor LDAP). Para ter mais informações, consulte Habilite o LDAPS do lado do cliente usando o Microsoft AD gerenciado AWS.

Tópicos

- Habilitar o LDAPS do lado do servidor usando o Microsoft AD gerenciado AWS

- Habilite o LDAPS do lado do cliente usando o Microsoft AD gerenciado AWS

Habilitar o LDAPS do lado do servidor usando o Microsoft AD gerenciado AWS

O suporte do Lightweight Directory Access Protocol Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) do lado do servidor criptografa as comunicações LDAP entre seus aplicativos comerciais ou domésticos compatíveis com LDAP e seu diretório gerenciado do Microsoft AD. AWS Isso ajuda a aumentar a segurança em toda a rede e atender aos requisitos de conformidade usando o protocolo criptográfico Secure Sockets Layer (SSL).

Habilitar o LDAPS no lado do servidor

Para obter instruções detalhadas sobre como instalar e configurar o LDAPS do lado do servidor e seu servidor de autoridade de certificação (CA), consulte Como habilitar o LDAPS do lado do servidor para seu diretório AWS gerenciado do Microsoft AD no blog de segurança. AWS

Você deve fazer a maior parte da configuração da instância do Amazon EC2 que você usa para gerenciar os controladores de domínio do AWS Managed Microsoft AD. As etapas a seguir orientam você a habilitar o LDAPS para seu domínio na AWS nuvem.

Se quiser usar a automação para configurar sua infraestrutura de PKI, você pode usar a Infraestrutura de Chave Pública da Microsoft no AWS QuickStart Guia. Especificamente, você deve seguir as instruções no guia para carregar o modelo para Implantar a PKI da Microsoft em uma VPC existente na AWS. Depois de carregar o modelo, certifique-se de escolher **`AWSManaged`** ao acessar a opção Tipo de serviços de domínio do Active Directory. Se você usou o QuickStart guia, você pode pular diretamente paraEtapa 3: Criar um modelo de certificado.

Tópicos

- Etapa 1: delegar quem pode habilitar o LDAPS
- Etapa 2: configurar a autoridade de certificação
- Etapa 3: Criar um modelo de certificado
- Etapa 4: adicionar regras do grupo de segurança

Etapa 1: delegar quem pode habilitar o LDAPS

Para habilitar o LDAPS do lado do servidor, você deve ser membro do grupo Administradores ou Administradores da Autoridade Certificadora Empresarial AWS Delegada em seu diretório gerenciado do Microsoft AD. AWS Como opção, você pode ser o usuário administrativo

padrão (conta de administrador). Se preferir, você poderá ter um usuário diferente do LDAPS de configuração da conta de administrador. Nesse caso, adicione esse usuário ao grupo Administradores ou Administradores da Autoridade de Certificação Empresarial AWS Delegada em seu diretório gerenciado do AWS Microsoft AD.

Etapa 2: configurar a autoridade de certificação

Antes de habilitar o LDAPS no lado do servidor, você deve criar um certificado. Esse certificado deve ser emitido por um servidor CA corporativo da Microsoft que esteja associado ao seu domínio AWS gerenciado do Microsoft AD. Depois de criado, o certificado deve ser instalado em cada um dos controladores de domínio no domínio. Este certificado permite que o serviço LDAP em controladores de domínio escute e aceite automaticamente conexões SSL de clientes LDAP.

> **Note**
>
> O LDAPS do lado do servidor com AWS Microsoft AD gerenciado não oferece suporte a certificados emitidos por uma CA autônoma. Ele também não oferece suporte a certificados emitidos por uma autoridade de certificação de terceiros.

Dependendo de sua necessidade comercial, você tem as seguintes opções para configurar ou conectar uma CA a seu domínio:

- Crie uma CA Microsoft Enterprise subordinada — (Recomendado) Com essa opção, você pode implantar um servidor Microsoft Enterprise CA subordinado na AWS nuvem. O servidor pode usar o Amazon EC2 para funcionar com sua CA raiz da Microsoft existente. Para obter mais informações sobre como configurar uma CA corporativa subordinada da Microsoft, consulte Etapa 4: Adicionar uma CA Microsoft Enterprise ao seu diretório do AWS Microsoft AD em Como habilitar o LDAPS do lado do servidor para seu diretório gerenciado AWS do Microsoft AD.
- Crie uma CA corporativa raiz da Microsoft — Com essa opção, você pode criar uma CA corporativa raiz da Microsoft na AWS nuvem usando o Amazon EC2 e juntá-la ao seu domínio gerenciado AWS do Microsoft AD. Essa CA raiz pode emitir o certificado para seus controladores de domínio. Para obter mais informações sobre como configurar uma nova CA raiz, consulte Etapa 3: Instalar e configurar uma CA offline em Como habilitar o LDAPS do lado do servidor para seu diretório gerenciado do AWS Microsoft AD.

Para obter mais informações sobre como adicionar a instância do EC2 ao domínio, consulte Associe uma instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory.

Etapa 3: Criar um modelo de certificado

Após configurar a CA da empresa, é possível configurar o modelo do certificado de autenticação Kerberos.

Para criar um modelo de certificado

1. Inicie o Microsoft Windows Server Manager. Selecione Ferramentas > Autoridade de certificação.
2. Na janela Autoridade de certificação, expanda a árvore de Autoridade de certificação no painel esquerdo. Clique com o botão direito do mouse em Modelos de certificado e escolha Gerenciar.
3. Na janela Console de modelos de certificado, clique com o botão direito em Autenticação Kerberos e escolha Duplicar modelo.
4. A janela Propriedades do novo modelo será exibida.
5. Na janela Propriedades do novo modelo, vá até a guia Compatibilidade e faça o seguinte:
   a. Altere a Autoridade de certificação para o sistema operacional que corresponde à sua CA.
   b. Se a janela Alterações resultantes for exibida, selecione OK.
   c. Altere o destinatário da certificação para Windows 10/Windows Server 2016.

      > **Note**
      >
      > AWS O Microsoft AD gerenciado é desenvolvido com o Windows Server 2019.

   d. Se a janela Alterações resultantes for exibida, selecione OK.
6. Clique na guia Geral e altere o Nome de exibição do modelo para LDAPOverSSL ou qualquer outro nome que você preferir.
7. Clique na guia Segurança e escolha Controladores de domínio na seção Nomes de grupos ou usuários. Na seção Permissões para controladores de domínio, verifique se as caixas de seleção Permitir para Leitura, Inscrição e Inscrição automática estão marcadas.
8. Escolha OK para criar o modelo de certificado LDAPOverSSL (ou o nome que você especificou acima). Feche a janela do Console de modelos de certificado.
9. Na janela Autoridade de certificação, clique com o botão direito do mouse em Modelos de certificado e escolha Novo > Modelo de certificado para emitir.
10. Na janela Habilitar modelos de certificado, escolha LDAPOverSSL (ou o nome que você especificou acima) e, em seguida, escolha OK.

Etapa 4: adicionar regras do grupo de segurança

Na etapa final, você deve abrir o console do Amazon EC2 e adicionar regras de grupo de segurança. Essas regras permitem que os controladores de domínio se conectem à CA corporativa para solicitar um certificado. Nesse caso, você adiciona regras de entrada de forma que a CA corporativa possa aceitar o tráfego de entrada dos controladores de domínio. Depois, você adiciona regras de saída para permitir o tráfego dos seus controladores de domínio para a CA corporativa.

Quando as duas regras estiverem configuradas, os controladores de domínio solicitarão um certificado da CA corporativa automaticamente e habilitarão o LDAPS para o diretório. O serviço LDAP em seus controladores de domínio agora está pronto para aceitar conexões LDAPS.

Para configurar regras do grupo de segurança

1. Navegue até o console do Amazon EC2 em https://console.aws.amazon.com/ec2 e faça login com credenciais de administrador.
2. No painel esquerdo, escolha Grupos de segurança em Rede e segurança.
3. No painel principal, escolha o grupo AWS de segurança para sua CA.
4. Escolha a guia Inbound e depois Edit.
5. Na caixa de diálogo Edit inbound rules, faça o seguinte:
   - Escolha Add Rule.
   - Escolha All traffic para Type e Custom para Source.
   - Insira o grupo de AWS segurança do seu diretório (por exemplo, sg-123456789) na caixa ao lado de Fonte.
   - Escolha Salvar.
6. Agora, escolha o grupo de AWS segurança do seu diretório AWS Managed Microsoft AD. Escolha a guia Outbound (Saída) e escolha Edit (Editar).
7. Na caixa de diálogo Edit outbound rules, faça o seguinte:
   - Escolha Add Rule.
   - Escolha All traffic para Type e Custom para Destination.
   - Digite o grupo de AWS segurança da sua CA na caixa ao lado de Destino.
   - Escolha Salvar.

Você pode testar a conexão LDAPS com o diretório AWS gerenciado do Microsoft AD usando a ferramenta LDP. A ferramenta LDP vem com as Ferramentas Administrativas do Active Directory. Para ter mais informações, consulte Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado.

> **Note**
>
> Antes de testar a conexão LDAPS, é necessário esperar até 30 minutos para que a CA subordinada emita um certificado para seus controladores de domínio.

Para obter detalhes adicionais sobre o LDAPS do lado do servidor e ver um exemplo de caso de uso sobre como configurá-lo, consulte Como habilitar o LDAPS do lado do servidor para seu diretório AWS gerenciado do Microsoft AD no blog de segurança. AWS

Habilite o LDAPS do lado do cliente usando o Microsoft AD gerenciado AWS

O suporte do Lightweight Directory Access Protocol Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) do lado do cliente no AWS Managed Microsoft AD criptografa as comunicações entre o Microsoft Active Directory (AD) autogerenciado (local) e os aplicativos. AWS Exemplos desses aplicativos incluem WorkSpaces AWS IAM Identity Center QuickSight, Amazon e Amazon Chime. Essa criptografia ajuda você a proteger melhor os dados de identidade da organização e atender aos requisitos de segurança.

Pré-requisitos

Antes de habilitar o LDAPS no lado do cliente, você precisa atender aos requisitos a seguir.

Tópicos

- Crie uma relação de confiança entre seu Microsoft AD AWS gerenciado e o autogerenciado Microsoft Active Directory
- Implantar certificados de servidor no Active Directory
- Requisitos de certificado da Autoridade Certificadora
- Requisitos de rede

Crie uma relação de confiança entre seu Microsoft AD AWS gerenciado e o autogerenciado Microsoft Active Directory

Primeiro, você precisa estabelecer uma relação de confiança entre o Microsoft AD gerenciado e o AWS autogerenciado Microsoft Active Directory para habilitar o LDAPS do lado do cliente. Para ter mais informações, consulte the section called “Criar uma relação de confiança”.

Implantar certificados de servidor no Active Directory

Para habilitar o LDAPS no lado do cliente, é necessário obter e instalar certificados de servidor para cada controlador de domínio no Active Directory. Esses certificados serão usados pelo serviço LDAP para escutar e aceitar automaticamente as conexões SSL de clientes LDAP. Você pode usar os certificados SSL emitidos por uma implantação interna do Active Directory Certificate Services (ADCS) ou comprados de um emissor comercial. Para obter mais informações sobre os requisitos de certificado de servidor do Active Directory, consulte LDAP over SSL (LDAPS) Certificate no site da Microsoft.

Requisitos de certificado da Autoridade Certificadora

Um certificado de autoridade de certificação (CA), que representa o emissor dos certificados de servidor, é necessário para a operação LDAPS no lado do cliente. Os certificados CA são combinados com os certificados de servidor apresentados pelos controladores de domínio do Active Directory para criptografar as comunicações de LDAP. Observe os seguintes requisitos de certificado CA:

- A Autoridade de Certificação Empresarial (CA) é necessária para habilitar o LDAPS do lado do cliente. Você pode usar o Serviço de Active Directory Certificados, uma autoridade de certificação comercial terceirizada ou AWS Certificate Manager. Para obter mais informações sobre a Autoridade Certificadora Microsoft Empresarial, consulte a Microsoftdocumentação.
- Para registrar um certificado, ele deve estar a mais de 90 dias da expiração.
- Os certificados devem estar no formato PEM (Privacy Enhanced Mail). Se exportar certificados CA de dentro do Active Directory, escolha X.509 (.CER) codificado em base64 como o formato de arquivo de exportação.
- No máximo cinco (5) certificados CA podem ser armazenados por diretório AWS gerenciado do Microsoft AD.
- Não há suporte para certificados que usam o algoritmo de assinatura RSASSA-PSS.
- Os certificados CA que são encadeados a cada certificado de servidor em cada domínio confiável devem ser registrados.

Requisitos de rede

AWS o tráfego LDAP do aplicativo será executado exclusivamente na porta TCP 636, sem retorno para a porta LDAP 389. Porém, as comunicações LDAP do Windows que oferecem suporte a replicação, relações de confiança e muito mais continuarão a usar a porta LDAP 389 com segurança nativa do Windows. Configure grupos AWS de segurança e firewalls de rede para permitir comunicações TCP na porta 636 no AWS Microsoft AD gerenciado (saída) e no Active Directory autogerenciado (entrada). Mantenha a porta 389 do LDAP aberta entre o AWS Managed Microsoft AD e o Active Directory autogerenciado.

Habilitar o LDAPS no lado do cliente

Para habilitar o LDAPS no lado do cliente, importe seu certificado de autoridade de certificação (CA) para o AWS Managed Microsoft AD e habilite o LDAPS no seu diretório. Após a habilitação, todo o tráfego LDAP entre os aplicativos da AWS e o seu Active Directory autogerenciado fluirá com a criptografia de canal Secure Sockets Layer (SSL).

É possível usar dois métodos diferentes para habilitar o LDAPS do lado do cliente para seu diretório. Você pode usar o AWS Management Console método ou o AWS CLI método.

> **Note**
>
> O LDAPS do lado do cliente é um recurso regional do Managed AWS Microsoft AD. Se você estiver usando a Replicação em várias regiões, os procedimentos a seguir deverão ser aplicados separadamente em cada região. Para ter mais informações, consulte Recursos globais versus regionais.

Tópicos

Etapa 1: registrar um certificado no AWS Directory Service

Use um dos métodos a seguir para registrar um certificado no AWS Directory Service.

Método 1: Para registrar seu certificado em AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja registrar seu certificado e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Client-side LDAPS (LDAPS do lado do cliente), selecione o menu Actions (Ações) e escolha Register certificate (Registrar certificado).
5. Na caixa de diálogo Register a CA certificate (Registrar um certificado CA), selecione Browse (Procurar), escolha o certificado e selecione Open (Abrir).
6. Escolha Register certificate (Registrar certificado).

Método 2: Para registrar seu certificado em AWS Directory Service (AWS CLI)

- Execute o seguinte comando . Para os dados do certificado, aponte para o local do arquivo de certificado CA. Um ID de certificado será fornecido na resposta.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Etapa 2: verificar o status do registro

Para ver o status de um registro de certificado ou uma lista de certificados registrados, use um dos comandos a seguir.

Método 1: Para verificar o status do registro do certificado em AWS Directory Service (AWS Management Console)

1. Vá para a seção Client-side LDAPS (LDAPS do lado do cliente) na página Directory details (Detalhes do diretório).

2. Revise o estado de registro de certificado atual exibido na coluna Registration status (Status do registro). Quando o valor do status do registro for alterado para Registered (Registrado), seu certificado foi registrado com êxito.

Método 2: Para verificar o status do registro do certificado em AWS Directory Service (AWS CLI)

- Execute o seguinte comando . Se o valor de status retornar `Registered`, seu certificado foi registrado com êxito.

```
aws ds list-certificates --directory-id your_directory_id
```

Etapa 3: habilitar o LDAPS no lado do cliente

Use um dos métodos a seguir para habilitar o LDAPS do lado do cliente em. AWS Directory Service

> **Note**
>
> É necessário ter registrado com êxito pelo menos um certificado para habilitar o LDAPS do lado do cliente.

Método 1: Para habilitar o LDAPS do lado do cliente em () AWS Directory ServiceAWS Management Console

1. Vá para a seção Client-side LDAPS (LDAPS do lado do cliente) na página Directory details (Detalhes do diretório).
2. Escolha Habilitar. Se essa opção não estiver disponível, verifique se um certificado válido foi registrado com êxito e tente novamente.
3. Na caixa de diálogo Enable client-side LDAPS (Habilitar LDAPS do lado do cliente), escolha Enable (Habilitar).

Método 2: Para habilitar o LDAPS do lado do cliente em () AWS Directory ServiceAWS CLI

- Execute o seguinte comando .

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Etapa 4: verificar o status do LDAPS

Use um dos métodos a seguir para verificar o status do LDAPS em AWS Directory Service.

Método 1: Para verificar o status do LDAPS em AWS Directory Service ()AWS Management Console

1. Vá para a seção Client-side LDAPS (LDAPS do lado do cliente) na página Directory details (Detalhes do diretório).
2. Se o valor de status for exibido como Enabled (Habilitado), o LDAPS foi configurado com êxito.

Método 2: Para verificar o status do LDAPS em AWS Directory Service ()AWS CLI

- Execute o seguinte comando . Se o valor de status retornar `Enabled`, o LDAPS foi configurado com êxito.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Gerenciar o LDAPS no lado do cliente

Use estes comandos para gerenciar sua configuração LDAPS.

É possível usar dois métodos diferentes para gerenciar configurações do LDAPS do lado do cliente. Você pode usar o AWS Management Console método ou o AWS CLI método.

Visualizar detalhes do certificado

Use um dos seguintes métodos para ver quando um certificado está definido para expirar.

Método 1: Para ver os detalhes do certificado em AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja visualizar seu certificado e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.

- Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.

4. Na seção Client-side LDAPS (LDAPS do lado do cliente) em CA certificates (Certificados CA), serão exibidas informações sobre o certificado.

Método 2: Para ver os detalhes do certificado em AWS Directory Service (AWS CLI)

- Execute o seguinte comando . Para o ID do certificado, use o identificador retornado por `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Cancelar o registro de um certificado

Use um dos seguintes métodos para cancelar o registro de um certificado.

> **Note**
>
> Se apenas um certificado estiver registrado, será necessário primeiro desabilitar o LDAPS para cancelar o registro do certificado.

Método 1: Para cancelar o registro de um certificado em AWS Directory Service ()AWS Management Console

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:

   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja cancelar o registro do seu certificado e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.

4. Na seção Client-side LDAPS (LDAPS do lado do cliente), escolha Actions (Ações) e selecione Deregister certificate (Cancelar registro do certificado).

5. Na caixa de diálogo Deregister a CA certificate (Cancelar registro de certificado CA), escolha Deregister (Cancelar registro).

Método 2: Para cancelar o registro de um certificado em AWS Directory Service ()AWS CLI

- Execute o seguinte comando . Para o ID do certificado, use o identificador retornado por `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Desabilitar o LDAPS no lado do cliente

Use um dos seguintes métodos para desabilitar o LDAPS do lado do cliente.

Método 1: Para desativar o LDAPS do lado do cliente em () AWS Directory ServiceAWS Management Console

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja desabilitar o LDAPS no lado do cliente e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Client-side LDAPS (LDAPS do cliente), escolha Disable (Desabilitar).
5. Na caixa de diálogo Disable client-side LDAPS (Desabilitar LDAPS do lado do cliente), escolha Disable (Desabilitar).

Método 2: Para desativar o LDAPS do lado do cliente em () AWS Directory ServiceAWS CLI

- Execute o seguinte comando .

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Problemas de inscrição no certificado

O processo para inscrever seus controladores de domínio AWS gerenciados do Microsoft AD com os certificados CA pode levar até 30 minutos. Se você tiver problemas com a inscrição do certificado e quiser reiniciar seus controladores de domínio AWS gerenciados do Microsoft AD, entre em contato com. AWS Support Para criar um caso de suporte, consulte Criação de casos de suporte e gerenciamento de casos.

Gerencie a conformidade do AWS Managed Microsoft AD

Você pode usar o AWS Managed Microsoft AD para oferecer suporte aos seus aplicativos compatíveis com o Active Directory, na AWS nuvem, que estão sujeitos aos seguintes requisitos de conformidade. No entanto, suas aplicações não aderirão aos requisitos de conformidade se você usar o Simple AD.

Padrões de conformidade compatíveis

AWS O Microsoft AD gerenciado passou por uma auditoria para os seguintes padrões e está qualificado para uso como parte de soluções para as quais você precisa obter a certificação de conformidade.

FedRAMP	AWS O Microsoft AD gerenciado atende aos requisitos de segurança do Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP) e recebeu uma Autoridade Provisória para Operar (P-ATO) do FedRAMP Joint Authorization Board (JAB) na linha de base moderada e alta do FedRAMP. Para obter mais informações sobre conformidade com a FedRAMP, consulte Conformidade com a FedRAMP.
PCI Security Standards Council PARTICIPATING ORGANIZATION™	AWS O Microsoft AD gerenciado tem um Atestado de Conformidade para o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI) versão 3.2 no nível 1 do provedor de serviços. Os clientes que usam AWS produtos e serviços para armazenar,

	processar ou transmitir dados do titular do cartão podem usar o Microsoft AD AWS gerenciado para gerenciar sua própria certificação de conformidade com o PCI DSS. Para obter mais informações sobre o PCI DSS, incluindo como solicitar uma cópia do PCI AWS Compliance Package, consulte PCI DSS nível 1. É importante ressaltar que você deve configurar políticas de senha refinadas no Managed AWS Microsoft AD para serem consistentes com os padrões do PCI DSS versão 3.2. Para obter detalhes sobre quais políticas devem ser aplicadas, consulte a seção abaixo intitulada Habilitar a conformidade com PCI para seu diretório gerenciado AWS do Microsoft AD.
	AWS expandiu seu programa de conformidade com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) para incluir o Managed AWS Microsoft AD como um serviço qualificado para a HIPAA. Se você tiver um Acordo de Associado Comercial (BAA) assinado com AWS, você pode usar o AWS Managed Microsoft AD para ajudar a criar seus aplicativos compatíveis com HIPAA. AWS oferece um whitepaper com foco na HIPAA para clientes interessados em saber mais sobre como eles podem aproveitar o processamento e o armazenamento AWS de informações de saúde. Para obter mais informaçõ es, consulte HIPAA compliance.

Responsabilidade compartilhada

A segurança, incluindo a conformidade com HIPAA e PCI, é uma responsabilidade compartilhada. É importante entender que o status de conformidade do AWS Managed Microsoft AD não se aplica automaticamente aos aplicativos que você executa na AWS nuvem. Você precisa garantir que o uso dos AWS serviços esteja em conformidade com os padrões.

Para obter uma lista completa de todos os vários programas de AWS conformidade aos quais o AWS Managed Microsoft AD oferece suporte, consulte AWS serviços no escopo por programa de conformidade.

Habilite a conformidade com PCI para seu diretório AWS gerenciado do Microsoft AD

Para habilitar a conformidade com PCI para seu diretório AWS gerenciado do Microsoft AD, você deve configurar políticas de senha refinadas conforme especificado no documento de Atestado de Conformidade (AOC) e Resumo de Responsabilidade do PCI DSS fornecido pela. AWS Artifact

Para obter mais informações sobre como usar políticas de senha refinadas, consulte Gerenciar políticas de senha para o AWS Managed Microsoft AD.

Melhorar a configuração de segurança de rede do AWS Managed Microsoft AD

O grupo de segurança da AWS que é provisionado para o diretório do AWS Managed Microsoft AD está configurado com as portas de rede de entrada mínimas necessárias para oferecer suporte a todos os casos de uso conhecidos para o diretório do AWS Managed Microsoft AD. Para obter mais informações sobre o grupo de segurança provisionado da AWS, consulte O que é criado com seu Microsoft AD Active Directory AWS gerenciado.

Para melhorar ainda mais a segurança de rede do diretório do AWS Managed Microsoft AD, é possível modificar o grupo de segurança da AWS com base em cenários comuns indicados a seguir.

Tópicos

- Suporte somente a aplicações da AWS
- Somente aplicações da AWS com suporte de confiança
- Suporte a aplicações da AWS e a workloads nativas do Active Directory
- Suporte a aplicações da AWS e a workloads nativas do Active Directory compatíveis com relações de confiança

Suporte somente a aplicações da AWS

Todas as contas de usuário são provisionadas somente no AWS Managed Microsoft AD para serem usadas com aplicações compatíveis da AWS, como os seguintes:

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs

- Amazon WorkMail
- AWS Client VPN
- AWS Management Console

É possível usar a configuração do grupo de segurança da AWS a seguir para bloquear todo o tráfego não essencial para os controladores de domínio do AWS Managed Microsoft AD.

> **Note**
>
> - Os itens a seguir não são compatíveis com essa configuração do grupo de segurança da AWS:
>   - Instâncias do Amazon EC2
>   - Amazon FSx
>   - Amazon RDS para MySQL
>   - Amazon RDS para Oracle
>   - Amazon RDS para PostgreSQL
>   - Amazon RDS para SQL Server
>   - WorkSpaces
>   - Confianças do Active Directory
>   - Clientes ou servidores associados ao domínio

Regras de entrada

Nenhum.

Regras de saída

Nenhum.

Somente aplicações da AWS com suporte de confiança

Todas as contas de usuário são provisionadas no AWS Managed Microsoft AD ou no Active Directory confiável para serem usadas com aplicativos da AWS compatíveis, como os seguintes:

- Amazon Chime

- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

É possível modificar a configuração do grupo de segurança provisionado da AWS para bloquear todo o tráfego não essencial para os controladores de domínio do AWS Managed Microsoft AD.

> **Note**
>
> - Os itens a seguir não são compatíveis com essa configuração do grupo de segurança da AWS:
>   - Instâncias do Amazon EC2
>   - Amazon FSx
>   - Amazon RDS para MySQL
>   - Amazon RDS para Oracle
>   - Amazon RDS para PostgreSQL
>   - Amazon RDS para SQL Server
>   - WorkSpaces
>   - Confianças do Active Directory
>   - Clientes ou servidores associados ao domínio
> - Essa configuração exige que a rede "CIDR on-premises" esteja segura.
> - O TCP 445 é utilizado apenas para criação de confiança e pode ser removido após a confiança ter sido estabelecida.
> - O TCP 636 só é necessário quando o LDAP por SSL está em uso.

Regras de entrada

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP e UDP	53	CIDR on-premises	DNS	Autenticação de usuário e computador, resolução de nome, confianças
TCP e UDP	88	CIDR on-premises	Kerberos	Autenticação de usuário e computador, confianças do nível floresta
TCP e UDP	389	CIDR on-premises	LDAP	Diretório, replicação, política de grupo de autenticação de usuário e computador, confianças
TCP e UDP	464	CIDR on-premises	Alterar/definir senha do Kerberos	Replicação, autenticação de usuário e computador, confianças
TCP	445	CIDR on-premises	SMB/CIFS	Replicação, autenticação de usuário e computador, confianças de política de grupo

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP	135	CIDR on-premises	Replicação	RPC, EPM
TCP	636	CIDR on-premises	LDAP SSL	Diretório, replicação, política de grupo de autenticação de usuário e computador, confianças
TCP	49152 – 65535	CIDR on-premises	RPC	Replicação, autenticação de usuário e computador, política de grupo, confianças
TCP	3268 - 3269	CIDR on-premises	LDAP GC e LDAP GC SSL	Diretório, replicação, política de grupo de autenticação de usuário e computador, confianças
UDP	123	CIDR on-premises	Horário do Windows	Horário do Windows, confianças

Regras de saída

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
Tudo	Tudo	CIDR on-premises	Todo o tráfego	

Suporte a aplicações da AWS e a workloads nativas do Active Directory

As contas de usuário são provisionadas somente no AWS Managed Microsoft AD para serem usadas com aplicações compatíveis da AWS, como os seguintes:

- Amazon Chime
- Amazon Connect
- Instâncias do Amazon EC2
- Amazon FSx
- Amazon QuickSight
- Amazon RDS para MySQL
- Amazon RDS para Oracle
- Amazon RDS para PostgreSQL
- Amazon RDS para SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

É possível modificar a configuração do grupo de segurança provisionado da AWS para bloquear todo o tráfego não essencial para os controladores de domínio do AWS Managed Microsoft AD.

> **Note**
>
> - As relações de confiança no Active Directory não podem ser criadas e mantidas entre o diretório do AWS Managed Microsoft AD e o domínio on-premises.
> - Você deve garantir que a rede "CIDR do cliente" seja segura.
> - O TCP 636 só é necessário quando o LDAP por SSL está em uso.
> - Se deseja usar uma CA empresarial com essa configuração, será necessário criar uma regra de saída "TCP, 443, CA CIDR".

Regras de entrada

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP e UDP	53	CIDR do cliente	DNS	Autenticação de usuário e computador, resolução de nome, confianças
TCP e UDP	88	CIDR do cliente	Kerberos	Autenticação de usuário e computador, confianças do nível floresta
TCP e UDP	389	CIDR do cliente	LDAP	Diretório, replicação, política de grupo de autenticação de usuário e computador, confianças

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP e UDP	445	CIDR do cliente	SMB/CIFS	Replicação, autenticação de usuário e computador, confianças de política de grupo
TCP e UDP	464	CIDR do cliente	Alterar/definir senha do Kerberos	Replicação, autenticação de usuário e computador, confianças
TCP	135	CIDR do cliente	Replicação	RPC, EPM
TCP	636	CIDR do cliente	LDAP SSL	Diretório, replicação, política de grupo de autentica ção de usuário e computador, confianças
TCP	49152 – 65535	CIDR do cliente	RPC	Replicação, autenticação de usuário e computador, política de grupo, confianças

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP	3268 - 3269	CIDR do cliente	LDAP GC e LDAP GC SSL	Diretório, replicação, política de grupo de autentica ção de usuário e computador, confianças
TCP	9389	CIDR do cliente	SOAP	Web services do AD DS
UDP	123	CIDR do cliente	Horário do Windows	Horário do Windows, confianças
UDP	138	CIDR do cliente	DFSN e NetLogon	DFS, política de grupo

Regras de saída

Nenhum.

Suporte a aplicações da AWS e a workloads nativas do Active Directory compatíveis com relações de confiança

Todas as contas de usuário são provisionadas no AWS Managed Microsoft AD ou no Active Directory confiável para serem usadas com aplicativos da AWS compatíveis, como os seguintes:

- Amazon Chime
- Amazon Connect
- Instâncias do Amazon EC2
- Amazon FSx
- Amazon QuickSight
- Amazon RDS para MySQL

- Amazon RDS para Oracle
- Amazon RDS para PostgreSQL
- Amazon RDS para SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

É possível modificar a configuração do grupo de segurança provisionado da AWS para bloquear todo o tráfego não essencial para os controladores de domínio do AWS Managed Microsoft AD.

> **Note**
>
> - As redes "CIDR on-premises" e "CIDR do cliente" devem estar seguras.
> - O TCP 445 com "CIDR on-premises" é usado apenas para criação de confiança e pode ser removido após a confiança ter sido estabelecida.
> - O TCP 445 com "CIDR do cliente" deve ser deixado aberto, uma vez que é necessário para o processamento da política de grupo.
> - O TCP 636 só é necessário quando o LDAP por SSL está em uso.
> - Se deseja usar uma CA empresarial com essa configuração, será necessário criar uma regra de saída "TCP, 443, CA CIDR".

Regras de entrada

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP e UDP	53	CIDR on-premises	DNS	Autenticação de usuário e computador, resolução de

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
				nome, confiança s
TCP e UDP	88	CIDR on-premis es	Kerberos	Autenticação de usuário e computador, confianças do nível floresta
TCP e UDP	389	CIDR on-premis es	LDAP	Diretório, replicação, política de grupo de autentica ção de usuário e computador, confianças
TCP e UDP	464	CIDR on-premis es	Alterar/definir senha do Kerberos	Replicação, autenticação de usuário e computador, confianças
TCP	445	CIDR on-premis es	SMB/CIFS	Replicação, autenticação de usuário e computador, confianças de política de grupo
TCP	135	CIDR on-premis es	Replicação	RPC, EPM

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP	636	CIDR on-premises	LDAP SSL	Diretório, replicação, política de grupo de autenticação de usuário e computador, confianças
TCP	49152 – 65535	CIDR on-premises	RPC	Replicação, autenticação de usuário e computador, política de grupo, confianças
TCP	3268 - 3269	CIDR on-premises	LDAP GC e LDAP GC SSL	Diretório, replicação, política de grupo de autenticação de usuário e computador, confianças
UDP	123	CIDR on-premises	Horário do Windows	Horário do Windows, confianças
TCP e UDP	53	CIDR do cliente	DNS	Autenticação de usuário e computador, resolução de nome, confianças

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP e UDP	88	CIDR do cliente	Kerberos	Autenticação de usuário e computador, confianças do nível floresta
TCP e UDP	389	CIDR do cliente	LDAP	Diretório, replicação, política de grupo de autentica ção de usuário e computador, confianças
TCP e UDP	445	CIDR do cliente	SMB/CIFS	Replicação, autenticação de usuário e computador, confianças de política de grupo
TCP e UDP	464	CIDR do cliente	Alterar/definir senha do Kerberos	Replicação, autenticação de usuário e computador, confianças
TCP	135	CIDR do cliente	Replicação	RPC, EPM

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
TCP	636	CIDR do cliente	LDAP SSL	Diretório, replicação, política de grupo de autentica ção de usuário e computador, confianças
TCP	49152 – 65535	CIDR do cliente	RPC	Replicação, autenticação de usuário e computador, política de grupo, confianças
TCP	3268 - 3269	CIDR do cliente	LDAP GC e LDAP GC SSL	Diretório, replicação, política de grupo de autentica ção de usuário e computador, confianças
TCP	9389	CIDR do cliente	SOAP	Web services do AD DS
UDP	123	CIDR do cliente	Horário do Windows	Horário do Windows, confianças
UDP	138	CIDR do cliente	DFSN e NetLogon	DFS, política de grupo

Regras de saída

Protocolo	Intervalo de portas	Origem	Tipo de tráfego	Uso do Active Directory
Tudo	Tudo	CIDR on-premises	Todo o tráfego	

Definir configurações de segurança do diretório

Você pode definir configurações de diretório refinadas para seu AWS Managed Microsoft AD para atender aos seus requisitos de conformidade e segurança sem nenhum aumento na workload operacional. Nas configurações do diretório, é possível atualizar a configuração do canal seguro para protocolos e cifras usados em seu diretório. Por exemplo, você tem a flexibilidade de desativar cifras herdadas individuais, como RC4 ou DES, e protocolos, como SSL 2.0/3.0 e TLS 1.0/1.1. AWS Em seguida, o Managed Microsoft AD implanta a configuração em todos os controladores de domínio em seu diretório, gerencia as reinicializações do controlador de domínio e mantém essa configuração à medida que você aumenta a escala horizontalmente ou implanta outras Regiões da AWS. Para obter detalhes sobre todas as configurações disponíveis, consulte Lista de configurações de segurança do diretório.

Editar configurações de segurança do diretório

Você pode definir e editar as configurações de qualquer um dos seus diretórios.

Para editar configurações do diretório

1. Faça login no Console de Gerenciamento da AWS e abra o console do AWS Directory Service em https://console.aws.amazon.com/directoryservicev2/.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Em Rede e segurança, encontre Configurações do diretório e escolha Editar configurações.
4. Em Editar configurações, altere o Valor das configurações que deseja editar. Quando você edita uma configuração, seu status muda de Padrão para Pronto para atualizar. Se você editou a configuração anteriormente, seu status muda de Atualizado para Pronto para atualizar. Em seguida, escolha Revisar.
5. Em Revisar e atualizar configurações, consulte Configurações do diretório e verifique se os novos valores estão todos corretos. Se você quiser fazer outras alterações em suas configurações, escolha Editar configurações. Quando estiver satisfeito com suas alterações e

pronto para implementar os novos valores, escolha Atualizar configurações. Em seguida, você será levado de volta à página de ID do diretório.

> **Note**
>
> Em Configurações do diretório, é possível visualizar o Status das configurações atualizadas. Enquanto as configurações são implementadas, o Status exibe Atualizando. Você não pode editar outras configurações enquanto uma configuração exibe Atualizando em Status. O Status mostrará Atualizada se a configuração for atualizada com êxito com sua edição. O Status mostrará Falha se a atualização da sua configuração com sua edição falhar.

Falha na configurações de segurança do diretório

Se um erro ocorrer durante uma atualização de configurações, o Status será exibido como Falha. Em um status de falha, as configurações não são atualizadas para os novos valores e os valores originais permanecem implementados. Você pode tentar atualizar novamente essas configurações ou revertê-las para os valores anteriores.

Para resolver falhas nas configurações atualizadas

- Em Configurações do diretório, escolha Resolver configurações com falha. Depois, siga um destes procedimentos:
  - Para reverter suas configurações de volta ao valor original antes do estado de falha, escolha Reverter configurações com falha. Em seguida, escolha Reverter no modal pop-up.
  - Para tentar atualizar novamente as configurações do diretório, escolha Tentar novamente configurações com falha. Se desejar fazer alterações adicionais nas configurações do diretório antes de tentar novamente as atualizações que falharam, escolha Continuar editando. Em Analisar e tentar novamente atualizações com falha, escolha Atualizar configurações.

Lista de configurações de segurança do diretório

A lista a seguir mostra o tipo, o nome da configuração, o nome da API, os valores potenciais e a descrição da configuração para todas as configurações de segurança de diretório disponíveis.

TLS 1.2 e AES 256/256 são as configurações de segurança de diretório padrão quando todas as outras configurações de segurança estão desativadas. Essas opções não podem ser desabilitadas.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
Autenticação baseada em certificado	Compensação retroativa do certificado	CERTIFICATE_BACKDATING_COMPENSATION	Anos: 0 a 50 Meses: 0 a 11 Dias: 0 a 30 Horas: 0 a 23 Minutos: 0 a 59) Segundos 0 a 59	Especifique um valor para indicar por quanto tempo um certificado pode ser anterior a um usuário no Active Directory e ainda ser usado para autenticação no Active Directory. O valor padrão é 10 minutos. Esse valor pode ser definido de 1 segundo a 50 anos. Para definir essa configuração, você deve selecionar o tipo de Compatibilidade para a Imposição

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
				de vinculação de certificado forte. Para obter mais informações, consulte KB5014754: Alterações na autenticação baseada em certificado em controladores de domínio do Windows na documentação do Suporte Microsoft.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	Imposição de certificado forte	CERTIFICATE_STRONG_ENFORCEMENT	Compatibilidade, Imposição plena	Especifique um dos seguintes tipos de imposição: • Compatibilidade (padrão): a autenticação será permitida se um certificado não puder ser fortemente mapeado para um usuário. Se o certificado for anterior à conta do usuário no Active Directory, também será necessário definir a Compensação de retroatividade do certifica

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
				do. Caso contrário, a autenticação falhará. • Imposição plena: a autenticação não será permitida se um certificado não puder ser fortemente mapeado para um usuário. Se você escolher esse tipo de imposição, a compensação retroativa do certificado não poderá ser configurada. Para obter mais informações, consulte KB5014754:

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
				Alterações na autenticação baseada em certificado em controladores de domínio do Windows na documentação do Suporte Microsoft.
Canal seguro: Cifra	AES 128/128	AES_128_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia AES 128/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	DES 56/56	DES_56_56	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia DES 56/56 para comunicações de canal seguras entre controladores de domínio em seu diretório.
	RC2 40/128	RC2_40_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia RC2 40/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	RC2 56/128	RC2_56_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia RC2 56/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.
	RC2 128/128	RC2_128_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia RC2 128/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	RC4 40/128	RC4_40_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia RC4 40/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.
	RC4 56/128	RC4_56_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia RC4 56/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	RC4 64/128	RC4_64_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia RC4 64/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.
	RC4 128/128	RC4_128_128	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia RC4 128/128 para comunicações de canal seguras entre controladores de domínio em seu diretório.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	Triple DES 168/168	3DES_168_168	Habilitar, Desabilitar	Habilite ou desabilite a cifra de criptografia Triple DES 168/168 para comunicações de canal seguras entre controladores de domínio em seu diretório.
Canal seguro: Protocolo	PCT 1.0	PCT_1_0	Habilitar, Desabilitar	Habilite ou desabilite o protocolo PCT 1.0 para comunicações de canal seguras (servidor e cliente) nos controladores de domínio em seu diretório.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	SSL 2.0	SSL_2_0	Habilitar, Desabilitar	Habilite ou desabilite o protocolo SSL 2.0 para comunicações de canal seguras (servidor e cliente) nos controladores de domínio em seu diretório.
	SSL 3.0	SSL_3_0	Habilitar, Desabilitar	Habilite ou desabilite o protocolo SSL 3.0 para comunicações de canal seguras (servidor e cliente) nos controladores de domínio em seu diretório.

Tipo	Nome da configuração	Nome da API	Valores potenciais	Descrição da configuração
	TLS 1.0	TLS_1_0	Habilitar, Desabilitar	Habilite ou desabilite o protocolo TLS 1.0 para comunicações de canal seguras (servidor e cliente) nos controladores de domínio em seu diretório.
	TLS 1.1	TLS_1_1	Habilitar, Desabilitar	Habilite ou desabilite o protocolo TLS 1.1 para comunicações de canal seguras (servidor e cliente) nos controladores de domínio em seu diretório.

Configurar o AWS Private CA conector para AD

Você pode integrar seu Microsoft AD AWS gerenciado com AWS Private Certificate Authority (CA) para emitir e gerenciar certificados para usuários, grupos e máquinas unidos ao seu domínio do Active Directory. AWS Private CA O Connector for Active Directory permite que você use um

substituto totalmente gerenciado AWS Private CA para suas CAs corporativas autogerenciadas sem a necessidade de implantar, corrigir ou atualizar agentes locais ou servidores proxy.

> **Note**
>
> A inscrição de certificados LDAPS do lado do servidor para controladores de domínio AWS gerenciados do Microsoft AD AWS Private CA com Connector for Active Directory não é suportada. Para habilitar o LDAPS do lado do servidor para seu diretório, consulte Como habilitar o LDAPS do lado do servidor para seu diretório gerenciado do Microsoft AD. AWS

Você pode configurar a AWS Private CA integração com seu diretório por meio do console do Directory Service, do console do AWS Private CA Connector for Active Directory ou chamando a `CreateTemplate`API. Para configurar a integração da CA privada por meio do console do AWS Private CA Connector for Active Directory, consulte Criação de um modelo de conector. Veja abaixo as etapas sobre como configurar essa integração a partir do AWS Directory Service console.

Para configurar o AWS Private CA Conector para AD

1. Faça login no AWS Management Console e abra o AWS Directory Service console emhttps://console.aws.amazon.com/directoryservicev2/.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na guia Rede e Segurança, em AWS Private CA Conector para AD, escolha Configurar AWS Private CA Conector para AD. A página Criar certificado CA privado para Active Directory é exibida. Siga as etapas no console para criar sua CA privada para que o Active Directory conector se registre na sua CA privada. Para obter mais informações, consulte Criar um conector.
4. Depois de criar seu conector, siga as etapas abaixo para visualizar os detalhes, incluindo o status do conector e o status da CA privada associada.

Para visualizar o AWS Private CA Conector para AD

1. Faça login no AWS Management Console e abra o AWS Directory Service console emhttps://console.aws.amazon.com/directoryservicev2/.
2. Na página Directories (Diretórios), escolha o ID do diretório.

3. Em Rede e segurança, em AWS Private CA Connector for AD, você pode visualizar seus conectores de CA privada e a CA privada associada. Por padrão, você vê os seguintes campos:

   a. AWS Private CA ID do conector — O identificador exclusivo de um AWS Private CA conector. Clicar nele leva à página de detalhes desse AWS Private CA conector.

   b. AWS Private CA assunto — Informações sobre o nome distinto da CA. Clicar nele leva à página de detalhes desse AWS Private CA.

   c. Status — Com base em uma verificação de status do AWS Private CA conector e do AWS Private CA. Se ambas as verificações forem aprovadas, Ativo será exibido. Se uma das verificações falhar, 1/2 verificações falhou será exibida. Se as duas verificações falharem, Falha será exibida. Para obter mais informações sobre um status de falha, mova o ponteiro do mouse sobre o hiperlink para saber qual verificação falhou. Siga as instruções no console para fazer a correção.

   d. Data de criação — O dia em que o AWS Private CA conector foi criado.

Para obter mais informações, consulte Visualizar detalhes do conector.

Monitorar seu AWS Managed Microsoft AD

É possível monitorar seu diretório do AWS Managed Microsoft AD com os seguintes métodos:

Tópicos

- Noções básicas sobre o status do diretório
- Configurar notificações de status do diretório com o Amazon SNS
- Analisar logs do diretório do AWS Managed Microsoft AD
- Habilitar o encaminhamento de logs
- Monitorar seus controladores de domínio com métricas de performance

Noções básicas sobre o status do diretório

Os seguintes são os vários status de um diretório.

Ativo

O diretório está funcionando normalmente. Nenhum problema foi detectado pelo AWS Directory Service em seu diretório.

Criando

O diretório está sendo criado no momento. A criação do diretório geralmente leva de 20 a 45 minutos, mas pode variar de acordo com a carga do sistema.

Excluído

O diretório foi excluído. Todos os recursos do diretório foram liberados. Depois que um diretório entra nesse estado, ele não pode ser recuperado.

Deleting

O diretório está sendo excluído no momento. O diretório permanecerá nesse estado até que seja completamente excluído. Depois que um diretório entra nesse estado, a operação de exclusão não pode ser cancelada, e o diretório não pode ser recuperado.

Com falha

O diretório não pôde ser criado. Exclua esse diretório. Se o problema persistir, entre em contato com o AWS Support Center.

Impaired (Degradado)

O diretório está em execução em um estado degradado. Um ou mais problemas foram detectados, e talvez algumas operações do diretório não estejam funcionando com capacidade operacional total. Há muitas razões possíveis para o diretório estar nesse estado. Elas incluem atividade de manutenção operacional normal, como aplicação de patches ou rotação de instâncias do EC2, localização dinâmica temporária por um aplicativo em um de seus controladores de domínio ou alterações que você fez em sua rede que acidentalmente interrompeu as comunicações do diretório. Para obter mais informações, consulte Solução de problemas do Microsoft AD AWS gerenciado, Solução de problemas do AD Connector, Solução de problemas do Simple AD. Para problemas normais relacionados à manutenção, AWS resolva esses problemas em 40 minutos. Se, após a análise do tópico sobre solução de problemas, seu diretório permanecer em um estado Comprometido por mais de 40 minutos, recomendamos entrar em contato com o AWS Support Center.

> **Important**
>
> Não restaure um snapshot enquanto um diretório estiver em um estado degradado. A restauração de snapshot raramente é necessária para solucionar esses problemas. Para ter mais informações, consulte Criar um snapshot ou restaurar seu diretório.

Requested (Solicitado)

Uma solicitação para criar seu diretório está pendente no momento.

RestoreFailed

Falha na restauração do diretório em um snapshot. Tente a operação de restauração novamente. Se o problema continuar, tente usar um snapshot diferente ou entre em contato com o AWS Support Center.

Restoring (Restaurando)

O diretório está sendo restaurado no momento em um snapshot automático ou manual. A restauração em um snapshot geralmente demora vários minutos, dependendo do tamanho dos dados do diretório no snapshot.

Configurar notificações de status do diretório com o Amazon SNS

Com o Amazon Simple Notification Service (Amazon SNS), é possível receber mensagens de e-mail ou de texto (SMS) quando o status de seu diretório é alterado. Você será notificado se seu diretório passar de um status Ativo para um status de Deficiente. Você também recebe uma notificação quando o diretório retorna para um status Active.

Como funciona

O Amazon SNS usa “tópicos” para coletar e distribuir mensagens. Cada tópico tem um ou mais assinantes que recebem as mensagens que foram publicadas para aquele tópico. Usando as etapas abaixo, você pode adicionar AWS Directory Service como editor a um tópico do Amazon SNS. Quando AWS Directory Service detecta uma alteração no status do seu diretório, ele publica uma mensagem nesse tópico, que é então enviada aos assinantes do tópico.

É possível associar vários diretórios como publicadores a um único tópico. Também é possível adicionar mensagens de status de diretório a tópicos criados anteriormente no Amazon SNS. Você pode controlar em detalhes quem pode publicar e ser assinante de um tópico. Para obter mais informações sobre o Amazon SNS, consulte O que é o Amazon SNS?.

> **Note**
>
> As notificações de status do diretório são um recurso regional do AWS Managed Microsoft AD. Se você estiver usando a Replicação em várias regiões, os procedimentos a seguir

deverão ser aplicados separadamente em cada região. Para ter mais informações, consulte Recursos globais versus regionais.

Para habilitar a troca de mensagens do SNS para o seu diretório

1. Faça login no AWS Management Console e abra o AWS Directory Service console.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja habilitar as mensagens do SNS e, em seguida, escolha a guia Manutenção. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Manutenção.
4. Na seção Monitoramento de diretórios, escolha Ações e, em seguida, selecione Criar notificação.
5. Na página Criar notificação, selecione Escolher um tipo de notificação e, em seguida, escolha Criar uma notificação. Como opção, se você já tem um tópico do SNS, escolha Associar a tópico do SNS existente para enviar mensagens de status deste diretório para o tópico existente.

   > **Note**
   >
   > Se você escolher Criar uma notificação, mas então usar o mesmo nome de um tópico do SNS que já existe, o Amazon SNS não criará um novo tópico, mas apenas adicionará as informações da nova assinatura ao tópico existente.
   > Se você escolher Associar a tópico do SNS existente, somente poderá escolher um tópico do SNS que esteja na mesma região que o diretório.

6. Escolha o Tipo de destinatário e insira as informações de contato do Destinatário. Se você inserir um número de telefone para SMS, use somente números. Não inclua traços, espaços ou parênteses.
7. (Opcional) Forneça um nome para seu tópico e um nome para exibição do SNS. O nome para exibição é um nome curto com até 10 caracteres que é incluído em todas as mensagens de SMS deste tópico. Quando a opção de SMS é usada, o nome de exibição é obrigatório.

> **Note**
>
> Se você estiver logado usando um usuário ou uma função do IAM que tenha somente a política DirectoryServiceFullAccessgerenciada, o nome do tópico deve começar com “DirectoryMonitoring”. Caso queira personalizar ainda mais o nome do tópico, precisará de privilégios adicionais no SNS.

8. Escolha Criar.

Se você quiser designar assinantes adicionais do SNS, como um endereço de e-mail adicional, filas do Amazon SQS AWS Lambda ou, você pode fazer isso no console do Amazon SNS.

Para remover as mensagens de status do diretório de um tópico

1. Faça login no AWS Management Console e abra o AWS Directory Service console.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja remover as mensagens de status e, em seguida, escolha a guia Manutenção. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Manutenção.
4. Na seção Monitoramento de diretórios, selecione um nome de tópico do SNS na lista, escolha Ações e selecione Remover.
5. Escolha Remover.

Isso remove o seu diretório enquanto publicador do tópico do SNS selecionado. Se quiser excluir o tópico inteiro, você pode fazer isso no console do Amazon SNS.

> **Note**
>
> Antes de excluir um tópico do Amazon SNS usando o console do SNS, certifique-se de que o diretório não esteja enviando mensagens de status para aquele tópico.
> Se você excluir um tópico do Amazon SNS usando o console do SNS, essa alteração não será refletida imediatamente no console do Directory Services. Você será notificado somente

na próxima vez que um diretório publicar uma notificação para o tópico excluído, quando verá o status atualizado na guia Monitoring do diretório indicando que o tópico não foi encontrado. Portanto, para evitar a perda de mensagens importantes de status do diretório, antes de excluir qualquer tópico do qual receba mensagens AWS Directory Service, associe seu diretório a um tópico diferente do Amazon SNS.

Analisar logs do diretório do AWS Managed Microsoft AD

Os logs de segurança das instâncias dos controladores de domínio do AWS Managed Microsoft AD são arquivados durante um ano. Você também pode configurar seu diretório do AWS Managed Microsoft AD para encaminhar logs do controlador de domínio para o Amazon CloudWatch Logs quase em tempo real. Para obter mais informações, consulte Habilitar o encaminhamento de logs.

A AWS registra os seguintes eventos em log para fins de conformidade.

Categoria do monitoramento	Configuração de políticas	Estado da auditoria
Login de conta	Auditoria de validação de credenciais	Êxito, falha
	Auditoria de outros eventos de logon de conta	Êxito, falha
Gerenciamento de contas	Auditoria de gerenciamento de conta de computador	Êxito, falha
	Auditoria de outros eventos de gerenciamento de contas	Êxito, falha
	Auditoria de gerenciamento de grupo de segurança	Êxito, falha
	Auditoria de gerenciamento de conta de usuário	Êxito, falha
Acompanhamento detalhado	Auditoria de atividade de DPAPI	Êxito, falha

Categoria do monitoramento	Configuração de políticas	Estado da auditoria
	Auditoria de atividade de PNP	Bem-sucedida
	Auditoria de criação de processo	Êxito, falha
Acesso ao DS	Auditoria de acesso ao Directory Service	Êxito, falha
	Auditoria de alterações no Directory Service	Êxito, falha
Login/Logoff	Auditoria de bloqueio de conta	Êxito, falha
	Auditoria de logoff	Bem-sucedida
	Auditoria de login	Êxito, falha
	Auditoria de outros eventos de logon/logoff	Êxito, falha
	Auditoria de login especial	Êxito, falha
Acesso a objetos	Auditoria de outros eventos de acesso a objetos	Êxito, falha
	Auditoria de armazenamento removível	Êxito, falha
	Auditoria de preparação de política de acesso central	Êxito, falha
Alteração de política	Auditoria de alteração de política	Êxito, falha
	Auditoria de alteração de política de autenticação	Êxito, falha

Categoria do monitoramento	Configuração de políticas	Estado da auditoria
	Auditoria de alteração de política de autorização	Êxito, falha
	Auditoria de alteração de política em nível de regra de MPSSVC	Bem-sucedida
	Auditoria de outros eventos de alteração de política	Falha
Uso de privilégio	Auditoria de uso sensível de privilégio confidencial	Êxito, falha
Sistema	Auditoria de driver IPsec	Êxito, falha
	Auditoria de outros eventos do sistema	Êxito, falha
	Auditoria de alteração de estado de segurança	Êxito, falha
	Auditoria de extensão do sistema de segurança	Êxito, falha
	Auditoria de integridade do sistema	Êxito, falha

Habilitar o encaminhamento de logs

Você pode usar o console ou as APIs do AWS Directory Service para encaminhar logs de eventos de segurança do controlador de domínio para o Amazon CloudWatch Logs. Isso ajuda a cumprir requisitos de políticas de monitoramento de segurança, auditoria e retenção de logs, proporcionando transparência dos eventos de segurança em um diretório.

O CloudWatch Logs também pode encaminhar esses eventos para outras contas da AWS, serviços da AWS ou aplicativos de terceiros. Assim, fica mais fácil monitorar e configurar alertas de forma centralizada para detectar e responder proativamente a atividades incomuns quase em tempo real.

Uma vez habilitado, você pode usar o console do CloudWatch Logs para recuperar os dados do grupo de logs que você especificou quando habilitou o serviço. Esse grupo de logs contém os logs de segurança de seus controladores de domínio.

Para obter mais informações sobre grupos de log e como ler seus dados, consulte Trabalhar com grupos de logs e fluxos de log no Guia do usuário do Amazon CloudWatch Logs.

> **Note**
>
> O encaminhamento de logs é um recurso regional do AWS Managed Microsoft AD. Se você estiver usando a Replicação em várias regiões, os procedimentos a seguir deverão ser aplicados separadamente em cada região. Para obter mais informações, consulte Recursos globais versus regionais.

Para habilitar o encaminhamento de logs

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Escolha o ID do diretório do AWS Managed Microsoft AD que deseja compartilhar.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja habilitar o encaminhamento de logs e, em seguida, escolha a guia Rede e segurança. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Log forwarding (Encaminhamento de logs), escolha Enable (Habilitar).
5. Na caixa de diálogo Enable log forwarding to CloudWatch (Habilitar o encaminhamento de logs para o CloudWatch), selecione uma das seguintes opções:
   a. Selecione Criar um grupo de logs do CloudWatch e, em Nome do grupo de logs, especifique um nome ao qual você pode se referir no CloudWatch Logs.
   b. Selecione Choose an existing CloudWatch log group (Selecionar um grupo de logs do CloudWatch existente) e, em Existing CloudWatch log groups (Grupos de logs do CloudWatch existentes), selecione um grupo de logs no menu.
6. Revise as informações sobre a definição de preços e o link e escolha Enable (Habilitar).

Para desabilitar o encaminhamento de logs

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Escolha o ID do diretório do AWS Managed Microsoft AD que deseja compartilhar.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja desabilitar o encaminhamento de logs e, em seguida, escolha a guia Rede e segurança. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Log forwarding (Encaminhamento de logs), escolha Disable (Desabilitar).
5. Depois de ler as informações na caixa de diálogo Disable log forwarding (Desabilitar o encaminhamento de logs), escolha Disable (Desabilitar).

Usar a CLI para habilitar o encaminhamento de logs

Antes de usar o comando `ds create-log-subscription`, você deverá primeiro criar um grupo de logs do Amazon CloudWatch e criar uma política de recursos do IAM que concederá a permissão necessária a esse grupo. Para habilitar o encaminhamento de logs usando a CLI, conclua todas as etapas abaixo.

Etapa 1: criar um grupo de logs no CloudWatch Logs

Crie um grupo de logs que será usado para receber os logs de segurança dos controladores de domínio. Recomendamos o acréscimo de prefixos ao nome `/aws/directoryservice/`, mas isso não é necessário. Por exemplo:

EXAMPLE CLI COMMAND (EXEMPLO DE COMANDO DA CLI)

```
aws logs create-log-group --log-group-name '/aws/directoryservice/
d-9876543210'
```

EXAMPLE POWERSHELL COMMAND (EXEMPLO DE COMANDO DO POWERSHELL)

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-9876543210'
```

Para obter mais informações sobre como criar um grupo de logs do CloudWatch, consulte Criar um grupo de logs no CloudWatch Logs no Guia do usuário do Amazon CloudWatch Logs.

Etapa 2: criar uma política de recursos do CloudWatch Logs no IAM

Crie uma política de recursos do CloudWatch Logs que conceda ao AWS Directory Service direitos para adicionar logs ao novo grupo de logs que você criou na Etapa 1. Você pode especificar o ARN exato para o grupo de logs para limitar o acesso do AWS Directory Service a outros grupos de logs ou usar um caractere curinga para incluir todos os grupos de logs. A política de exemplo a seguir usa o método curinga para identificar todos os grupos de logs que começam com `/aws/directoryservice/` para que a conta da AWS em que seu diretório reside seja incluída.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ds.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/*"
        }
    ]
}
```

Você precisará salvar essa política em um arquivo de texto (por exemplo, DSPolicy.json) na sua estação de trabalho local, porque precisará executá-la na CLI. Por exemplo:

EXAMPLE CLI COMMAND (EXEMPLO DE COMANDO DA CLI)

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-
document file://DSPolicy.json
```

EXAMPLE POWERSHELL COMMAND (EXEMPLO DE COMANDO DO POWERSHELL)

```
$PolicyDocument = Get-Content .\DSPolicy.json –Raw

Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument
$PolicyDocument
```

Etapa 3: criar uma assinatura de log do AWS Directory Service

Nesta etapa final, agora você poderá prosseguir para habilitar o encaminhamento de log, criando a assinatura de log. Por exemplo:

EXAMPLE CLI COMMAND (EXEMPLO DE COMANDO DA CLI)

```
aws ds create-log-subscription --directory-id 'd-9876543210' --log-group-name '/aws/directoryservice/d-9876543210'
```

EXAMPLE POWERSHELL COMMAND (EXEMPLO DE COMANDO DO POWERSHELL)

```
New-DSLogSubscription -DirectoryId 'd-9876543210' -LogGroupName '/aws/directoryservice/d-9876543210'
```

Monitorar seus controladores de domínio com métricas de performance

AWS Directory Service se integra à Amazon CloudWatch para ajudar a fornecer métricas de desempenho importantes para cada controlador de domínio em seuActive Directory. Isso significa que você pode monitorar os contadores de performance do controlador de domínio, como a utilização de CPU e de memória. Você também pode configurar alarmes e iniciar ações automatizadas para responder a períodos de alta utilização. Por exemplo, é possível configurar um alarme para a utilização da CPU do controlador de domínio acima de 70% e criar um tópico do SNS para você receber uma notificação quando isso ocorrer. Você pode usar esse tópico do SNS para iniciar a automação, como AWS Lambda funções, para aumentar o número de controladores de domínio do seu. Active Directory

Para obter mais informações sobre o monitoramento de controladores de domínio, consulte Determine quando adicionar controladores de domínio com métricas CloudWatch .

Há taxas associadas à Amazon CloudWatch. Para obter mais informações, consulte CloudWatchfaturamento e custo.

> **Important**
>
> As métricas de desempenho do controlador de domínio com CloudWatch não estão disponíveis na região Oeste do Canadá (Calgary).

Encontre métricas de desempenho do controlador de domínio em CloudWatch

No CloudWatch console da Amazon, as métricas de um determinado serviço são agrupadas primeiro pelo namespace do serviço. É possível adicionar filtros métricos subordinados a esse namespace. Use o procedimento a seguir para localizar o namespace e a métrica subordinada corretos necessários para configurar as métricas do controlador de domínio gerenciado do AWS Microsoft AD no. CloudWatch

Para encontrar métricas do controlador de domínio no CloudWatch console

1. Faça login no AWS Management Console e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Na lista de métricas, selecione o namespace Directory Service e, na lista, selecione a métrica AWS Managed Microsoft AD.

Para obter instruções sobre como configurar as métricas do controlador de domínio usando o CloudWatch console, consulte Como automatizar o escalonamento AWS gerenciado do Microsoft AD com base nas métricas de utilização no Blog de Segurança. AWS

Determine quando adicionar controladores de domínio com métricas CloudWatch

O balanceamento de carga em todos os seus controladores de domínio é importante para a resiliência e o desempenho do seu. Active Directory Para ajudá-lo a otimizar o desempenho de seus controladores de domínio no Microsoft AD AWS gerenciado, recomendamos que você primeiro monitore métricas importantes CloudWatch para formar uma linha de base. Durante esse processo, você analisa sua utilização Active Directory ao longo do tempo para identificar sua Active Directory utilização média e máxima. Depois de determinar sua linha de base, você pode monitorar essas métricas regularmente para ajudar a determinar quando adicionar um controlador de domínio à suaActive Directory.

É importante monitorar regularmente as métricas a seguir. Para obter uma lista completa das métricas de controladores de domínio disponíveis em CloudWatch, consulteAWS Contadores de desempenho gerenciados do Microsoft AD.

- Métricas específicas do controlador de domínio, como:
  - Processador
  - Memória

  - Disco lógico
  - Interface de rede
- AWS Métricas específicas do diretório Microsoft AD gerenciadas, como:
  - Pesquisas LDAP
  - Vinculações
  - Consultas ao DNS
  - Leituras de diretório
  - Gravações em diretórios

Para obter instruções sobre como configurar as métricas do controlador de domínio usando o CloudWatch console, consulte Como automatizar o escalonamento AWS gerenciado do Microsoft AD com base nas métricas de utilização no Blog de Segurança. AWS Para obter informações gerais sobre métricas em CloudWatch, consulte Usando CloudWatch métricas da Amazon no Guia CloudWatch do usuário da Amazon.

Para obter informações gerais sobre o planejamento do controlador de domínio, consulte Planejamento de capacidade para serviços de Active Directory domínio no site da Microsoft.

AWS Contadores de desempenho gerenciados do Microsoft AD

A tabela a seguir lista todos os contadores de desempenho disponíveis na Amazon CloudWatch para rastrear o desempenho do controlador de domínio e do diretório no AWS Managed Microsoft AD.

Categoria métrica	Nome da métrica
Banco de dados ==> Instâncias (NTDSA)	% de acertos no cache do banco de dados
	Latência média das leituras do banco de dados de E/S
	Leituras/segundo do banco de dados de E/S
	Latência média das gravações em log de E/S
DirectoryServices (NTDS)	Tempo de vinculação de LDAP
	Operações de replicação pendentes do DRA

Categoria métrica	Nome da métrica
	Sincronizações de replicação pendentes do DRA
DNS	Consultas recursivas/segundo
	Falhas de consultas recursivas do DNS/segundo
	Consultas de TCP recebidas/segundo
	Total de consultas recebidas/segundo
	Total de respostas enviadas/segundo
	Consultas de UDP recebidas/segundo
LogicalDisk	Média Comprimento da fila de discos
	% de espaço livre
Memória	% de bytes em uso confirmados
	Tempo de vida médio do cache em espera de longo prazo (segundos)
Interface de rede	Bytes enviados/segundo
	Bytes recebidos/segundo
	Largura de banda atual
NTDS	Atraso estimado na fila de ATQ
	Latência da solicitação de ATQ
	Leituras de diretório DS/segundo
	Pesquisas de diretório DS/segundo
	Gravações em diretório DS por segundo

Categoria métrica	Nome da métrica
	Sessões do cliente LDAP
	Pesquisas LDAP/segundo
	Vinculações de LDAP bem-sucedidas/segundo
Processador	% do tempo de processador
Estatísticas abrangendo todo o sistema de segurança	Autenticações Kerberos
	Autenticações NTLM

Replicação em várias regiões

A replicação multirregional pode ser usada para replicar automaticamente os dados do diretório gerenciado do AWS Microsoft AD em vários. Regiões da AWSEssa replicação pode melhorar o desempenho de usuários e aplicativos em localizações geográficas dispersas. AWS O Microsoft AD gerenciado usa a replicação nativa do Active Directory para replicar os dados do seu diretório com segurança na nova região.

A replicação multirregional só é compatível com a Enterprise Edition do Managed AWS Microsoft AD.

Você pode usar a replicação em várias regiões automatizada na maioria das regiões em que o AWS Managed Microsoft AD está disponível.

Important

A replicação multirregional não está disponível nas seguintes regiões opcionais:

- África (Cidade do Cabo) af-south-1
- Ásia-Pacífico (Hong Kong) ap-east-1
- Ásia-Pacífico (Hyderabad) ap-south-2
- Ásia-Pacífico (Jacarta) ap-southeast-3
- Ásia-Pacífico (Melbourne) (ap-southeast-4)
- Oeste do Canadá (Calgary) ca-west-1
- Europa (Milão) eu-south-1

- Europa (Espanha) eu-south-2
- Europa (Zurique) eu-central-2
- Israel (Tel Aviv) no centro-1
- Oriente Médio (Bahrein) me-south-1
- Oriente Médio (EAU) me-central-1

Para obter mais informações sobre regiões opcionais e como habilitá-las, consulte Especificar qual Regiões da AWS sua conta pode usar no AWS Account Management Guia.

Benefícios

Com a replicação multirregional no AWS Microsoft AD gerenciado, os aplicativos compatíveis com o Active Directory usam o diretório localmente para alto desempenho e o recurso multirregional para resiliência. Você pode usar a replicação multirregional com aplicativos compatíveis com o Active Directory, como o SQL Server Always On, bem como AWS serviços como Amazon RDS for SQL Server SharePoint e FSx for Windows File Server. Veja a seguir outros benefícios da replicação em várias regiões.

- Ele permite que você implante uma única instância AWS gerenciada do Microsoft AD globalmente, de forma rápida, e elimina o trabalho pesado de autogerenciar uma infraestrutura global do Active Directory.
- Isso torna mais fácil e econômico implantar e gerenciar cargas de trabalho do Windows e do Linux em várias AWS regiões. A replicação automatizada em várias regiões permite um desempenho ideal em seus aplicativos globais compatíveis com o Active Directory. Todos os aplicativos implantados em instâncias Windows ou Linux usam o Microsoft AD AWS gerenciado localmente na região, o que permite respostas às solicitações dos usuários da região mais próxima possível.
- Isso oferece uma resiliência proporcionada por várias regiões. Implantado na infraestrutura AWS gerenciada de alta disponibilidade, o AWS Managed Microsoft AD gerencia atualizações automatizadas de software, monitoramento, recuperação e segurança da infraestrutura subjacente do Active Directory em todas as regiões. Isso permite que você se concentre na criação de aplicações.

Tópicos

- Recursos globais versus regionais

- Regiões principais versus adicionais
- Como a replicação em várias regiões funciona
- Adicionar uma região replicada
- Excluir uma região replicada

Recursos globais versus regionais

Quando você adiciona uma AWS região ao seu diretório usando a replicação multirregional, AWS Directory Service aprimora o escopo de todos os recursos para que eles se tornem sensíveis à região. Esses recursos estão listados em várias guias da página de detalhes que aparece quando você escolhe o ID de um diretório no console do AWS Directory Service . Isso significa que todos os recursos são habilitados, configurados ou gerenciados com base na região selecionada na seção Replicação em várias regiões do console. As alterações feitas nos recursos em cada região são aplicadas globalmente ou por região.

A replicação multirregional só é compatível com a Enterprise Edition do Managed AWS Microsoft AD.

Características globais

Todas as alterações que você fizer nos recursos globais enquanto o Região principal estiver selecionado serão aplicadas em todas as regiões.

É possível identificar os recursos que são usados globalmente na página Detalhes do diretório porque eles exibem Aplicados a todas as regiões replicadas ao lado deles. Como alternativa, se você selecionou outra região na lista diferente da região principal, poderá identificar os recursos usados globalmente porque eles exibem Herdado da região principal.

Recursos regionais

Quaisquer alterações que você fizer em um recurso em uma Região adicional serão aplicadas somente a essa região.

É possível identificar os recursos regionais na página Detalhes do diretório porque eles não exibem Aplicados a todas as regiões replicadas ou Herdado da região principal ao lado deles.

Regiões principais versus adicionais

Com a replicação multirregional, o AWS Microsoft AD gerenciado usa os dois tipos de regiões a seguir para diferenciar como os recursos globais ou regionais devem ser aplicados em seu diretório.

Região principal

A região inicial em que você criou seu diretório pela primeira vez é chamada de região principal. Você pode realizar somente operações em nível de diretório global, como criar relações de confiança do Active Directory e atualizar o esquema do AD a partir da região principal.

A região principal sempre pode ser identificada como a primeira região exibida no topo da lista na seção de Replicação em várias regiões e é terminada por - Primary. Por exemplo, Leste dos EUA (Norte da Virgínia) - Primary.

Todas as alterações que você fizer em Características globais enquanto a região principal estiver selecionada serão aplicadas em todas as regiões.

Somente é possível adicionar regiões enquanto a região principal está selecionada. Para ter mais informações, consulte Adicionar uma região replicada.

Região adicional

Todas as regiões que você adicionou ao seu diretório são chamadas de regiões adicionais.

Embora alguns recursos possam ser gerenciados globalmente para todas as regiões, outros são gerenciados individualmente por região. Para gerenciar um recurso para uma região adicional (região não principal), primeiro é necessário selecionar a região adicional na lista na seção Replicação em várias regiões na página Detalhes do diretório. Em seguida, você pode prosseguir para o gerenciamento do recurso.

Todas as alterações que você fizer na Recursos regionais enquanto uma região adicional for selecionada serão aplicadas somente a essa região.

Como a replicação em várias regiões funciona

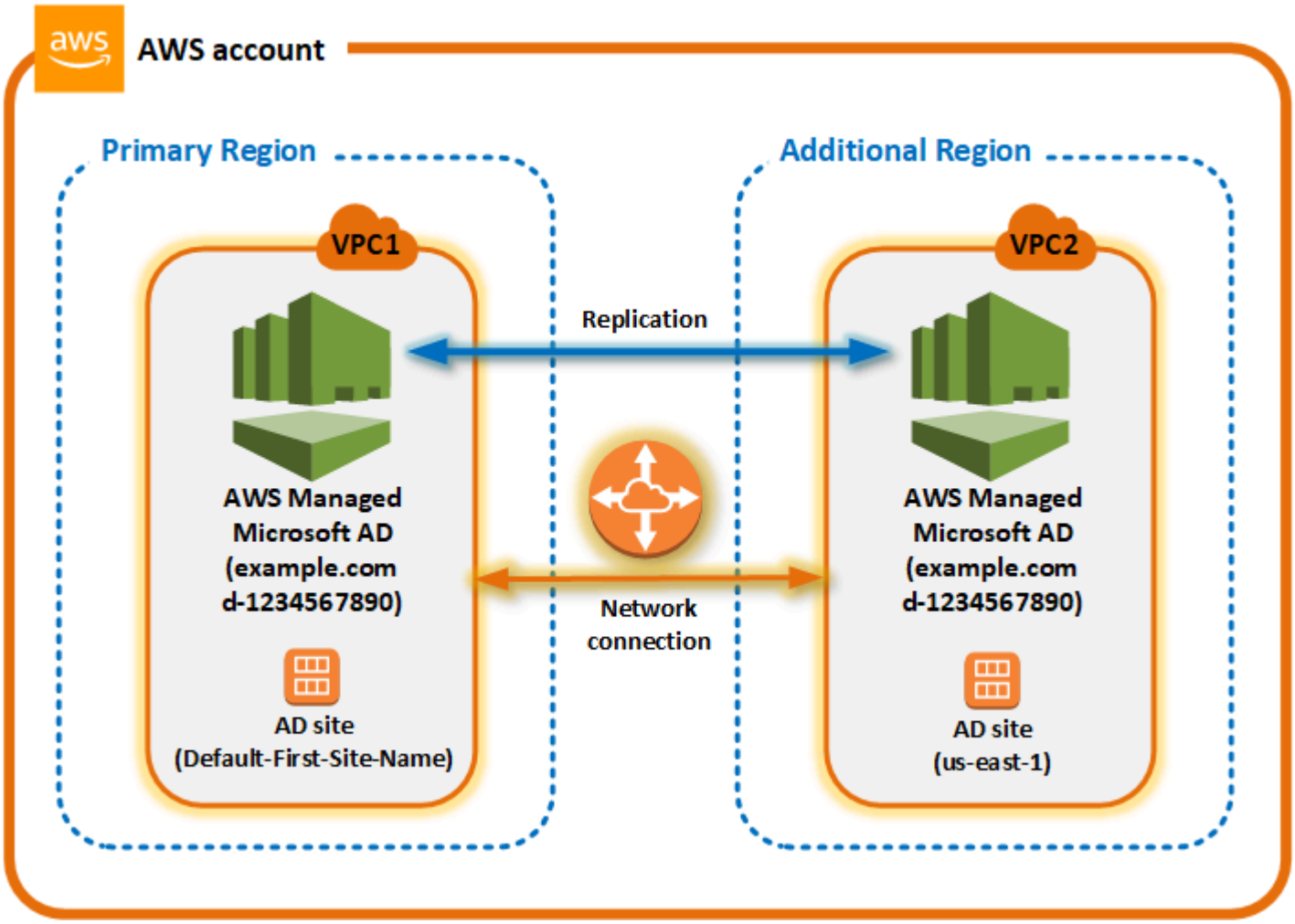
Com o recurso de replicação multirregional, o AWS Managed Microsoft AD elimina o trabalho pesado indiferenciado de gerenciar uma infraestrutura global do Active Directory. Quando configurado, AWS replica todos os dados do diretório de clientes, incluindo usuários, grupos, políticas de grupo e esquema em várias AWS regiões.

Depois que uma nova região é adicionada, as seguintes operações ocorrem automaticamente, conforme mostrado na ilustração:

- AWS O Microsoft AD gerenciado cria dois controladores de domínio na VPC selecionada e os implanta na nova região na mesma conta. AWS Seu identificador de diretório (`directory_id`)

permanece o mesmo em todas as regiões. Se desejar, você poderá adicionar outros controladores de domínio posteriormente.

- AWS O Microsoft AD gerenciado configura a conexão de rede entre a região principal e a nova região.
- AWS O Microsoft AD gerenciado cria um novo site do Active Directory e dá a ele o mesmo nome da Região, como us-east-1. Você também poderá renomeá-lo posteriormente usando a ferramenta Sites e Serviços do Active Directory.
- AWS O Microsoft AD gerenciado replica todos os objetos e configurações do Active Directory para a nova região, incluindo usuários, grupos, políticas de grupo, relações de confiança do Active Directory, unidades organizacionais e esquema do Active Directory. Os links do site do Active Directory são configurados para usar a Notificação de alteração. Com a notificação de alterações entre sites habilitada, as alterações se propagam para o local remoto com a mesma frequência com que são propagadas no site de origem, incluindo alterações que exigem replicação urgente.
- Se essa for a primeira região que você adicionou, o Microsoft AD AWS gerenciado torna todos os recursos compatíveis com várias regiões. Para ter mais informações, consulte Recursos globais versus regionais.



Sites do Active Directory

A replicação multirregional oferece suporte a vários sites do Active Directory (um site do Active Directory por região). Quando uma nova região é adicionada, ela recebe o mesmo nome da região, por exemplo, us-east-1. Você também poderá renomeá-la posteriormente usando a ferramenta Sites e Serviços do Active Directory.

AWS serviços

AWS serviços como o Amazon RDS for SQL Server e o Amazon FSx se conectam às instâncias locais do diretório global. Isso permite que seus usuários façam login uma vez em aplicativos compatíveis com o Active Directory que são executados, bem AWS como em AWS serviços como o Amazon RDS for SQL Server em qualquer região. AWS Para fazer isso, os usuários precisam de credenciais do Microsoft AD AWS gerenciado ou do Active Directory local quando você tem uma relação de confiança com seu AWS Microsoft AD gerenciado.

Você pode usar os seguintes AWS serviços com o recurso de replicação multirregional.

- Amazon EC2
- FSx para Windows File Server
- Amazon RDS para SQL Server
- Amazon RDS para Oracle
- Amazon RDS para MySQL
- Amazon RDS para PostgreSQL
- Amazon RDS para MariaDB
- Amazon Aurora para MySQL
- Amazon Aurora para PostgreSQL

Failover

Caso todos os controladores de domínio em uma região estejam inativos, o Microsoft AD AWS gerenciado recupera os controladores de domínio e replica os dados do diretório automaticamente. Enquanto isso, os controladores de domínio em outras regiões continuam funcionando.

Adicionar uma região replicada

Quando você adiciona uma região usando o Replicação em várias regiões recurso, o Microsoft AD AWS gerenciado cria dois controladores de domínio na AWS região selecionada, Amazon Virtual Private Cloud (VPC) e sub-rede. AWS O Microsoft AD gerenciado também cria os grupos de segurança relacionados que permitem que as cargas de trabalho do Windows se conectem ao seu diretório na nova região. Ele também cria esses recursos usando a mesma AWS conta em que seu diretório já está implantado. Você faz isso escolhendo a região, especificando a VPC e fornecendo as configurações para a nova região.

A replicação multirregional só é compatível com a Enterprise Edition do Managed AWS Microsoft AD.

Pré-requisitos

Antes de prosseguir com as etapas para adicionar uma nova região de replicação, recomenda-se analisar antes as tarefas de pré-requisito a seguir.

- Verifique se você tem as permissões AWS Identity and Access Management (IAM) necessárias, a configuração da Amazon VPC e a configuração da sub-rede na nova região para a qual você deseja replicar o diretório.

- Se você quiser usar suas credenciais locais existentes do Active Directory para acessar e gerenciar cargas de trabalho compatíveis com o Active Directory AWS, você deve criar uma relação de confiança do Active Directory entre o AWS Microsoft AD gerenciado e sua infraestrutura local do AD. Para obter mais informações sobre relações de confiança, consulte Conecte-se à sua infraestrutura existente do Active Directory.
- Se você tem uma relação de confiança existente entre seu Active Directory local e deseja adicionar uma região replicada, você precisa verificar se tem a configuração necessária da Amazon VPC e da sub-rede na nova região para a qual deseja replicar o diretório.

Adicionar uma região

Use o procedimento a seguir para adicionar uma região replicada ao seu diretório AWS gerenciado do Microsoft AD.

Para adicionar uma região replicada

1. No painel de navegação do console doAWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, em Replicação em várias regiões, escolha a região Principal na lista e, em seguida, escolha Adicionar região.

   > **Note**
   >
   > Somente é possível adicionar regiões enquanto a região Principal está selecionada. Para ter mais informações, consulte Região principal.

4. Na página Adicionar região, em Região, escolha a região que você deseja adicionar na lista.
5. Em VPC, escolha a VPC a ser usada para essa região.

   > **Note**
   >
   > Essa VPC não deve ter um Encaminhamento entre Domínios Sem Classificação (CIDR) que se sobreponha a uma VPC usada por esse diretório em outra região.

6. Em Sub-redes, escolha a sub-rede a ser usada para essa região.
7. Revise as informações em Preços e escolha Adicionar.

8. Quando o Microsoft AD AWS gerenciado concluir o processo de implantação do controlador de domínio, a Região exibirá o status Ativo. Agora você pode fazer atualizações nessa região conforme necessário.

Próximas etapas

Após adicionar sua nova região, você deverá considerar as seguintes próximas etapas:

- Implante controladores de domínio adicionais (até 20) em sua nova região conforme necessário. O número de controladores de domínio quando você adiciona uma nova região é 2 por padrão, que é o mínimo necessário para fins de tolerância a falhas e alta disponibilidade. Para ter mais informações, consulte Adicionar ou remover controladores de domínio adicionais.
- Compartilhe seu diretório com mais AWS contas por região. As configurações de compartilhamento de diretórios não são replicadas automaticamente da região principal. Para ter mais informações, consulte Compartilhar seu diretório.
- Ative o encaminhamento de registros para recuperar os registros de segurança do seu diretório usando o Amazon CloudWatch Logs da nova região. Ao habilitar o encaminhamento de logs, é necessário fornecer um nome de grupo de logs em cada região em que replicou seu diretório. Para ter mais informações, consulte Habilitar o encaminhamento de logs.
- Habilite o monitoramento do Amazon Simple Notification Service (Amazon SNS) da nova região para rastrear o status de integridade do seu diretório por região. Para ter mais informações, consulte Configurar notificações de status do diretório com o Amazon SNS.

Excluir uma região replicada

Use o procedimento a seguir para excluir uma região do seu diretório AWS gerenciado do Microsoft AD. Antes de excluir uma região, verifique se ela não apresenta nenhuma das seguintes condições:

- Aplicações autorizadas anexadas a ela.
- Diretórios compartilhados associados a ela.

Para excluir uma região replicada

1. No painel de navegação do console doAWS Directory Service, escolha Diretórios.
2. Na barra de navegação, escolha o seletor Regiões e, em seguida, escolha a região em que seu diretório está armazenado.

3. Na página Directories (Diretórios), escolha o ID do diretório.
4. Na página Detalhes do diretório, em Replicação em várias regiões, escolha Excluir região.
5. Na caixa de diálogo Excluir região, revise as informações e insira o nome da região para confirmar. Em seguida, selecione Excluir.

> **Note**
>
> Não é possível fazer atualizações na região enquanto ela está sendo excluída.

Compartilhar seu diretório

O AWS Managed Microsoft AD integra-se totalmente ao AWS Organizations para permitir o compartilhamento direto de diretórios entre várias contas da AWS. Você pode compartilhar um único diretório com outras contas confiáveis da AWS dentro da mesma organização ou compartilhar o diretório com outras contas da AWS que estão fora da sua organização. Você também poderá compartilhar seu diretório quando sua conta da AWS não for membro atual de uma organização.

> **Note**
>
> A AWS cobra uma taxa adicional pelo compartilhamento de diretório. Para saber mais, consulte a página Definição de preço no site do AWS Directory Service.

O compartilhamento de diretórios torna o AWS Managed Microsoft AD uma maneira mais econômica de fazer a integração com o Amazon EC2 em várias contas e VPCs. O compartilhamento de diretórios está disponível em todas as regiões da AWS em que o AWS Microsoft AD é oferecido.

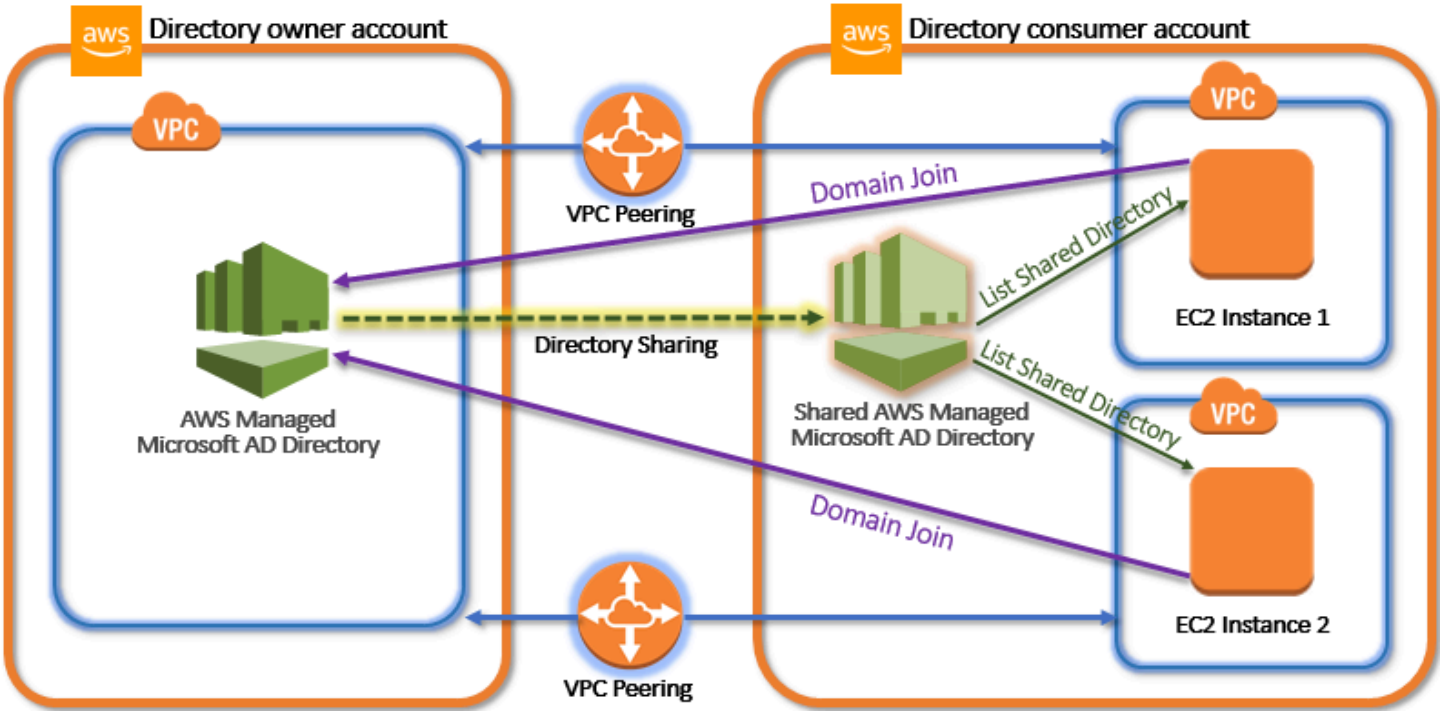
> **Note**
>
> Na região China (Ningxia) da AWS, esse recurso está disponível somente ao usar o AWS Systems Manager (SSM) para associar diretamente suas instâncias do Amazon EC2.

Para obter mais informações sobre o compartilhamento de diretórios e como estender o alcance do seu diretório do AWS Managed Microsoft AD além dos limites da conta da AWS, consulte os tópicos a seguir.

Tópicos

Principais conceitos do compartilhamento de diretórios

Você vai aproveitar mais o recurso de compartilhamento de diretório se conhecer os conceitos principais a seguir.



Conta de proprietário do diretório

Um proprietário de diretório é o titular da Conta da AWS que possui o diretório de origem na relação do diretório compartilhado. Um administrador nesta conta inicia o fluxo de trabalho do compartilhamento de diretório especificando com quais Contas da AWS o diretório deve ser compartilhado. Proprietários de diretórios podem ver com quem eles compartilharam um diretório usando a guia Scale & Share (Dimensionar e compartilhar) para um determinado diretório no console do AWS Directory Service.

Conta de consumidor de diretório

Em uma relação de diretório compartilhado, um consumidor de diretório representa a Conta da AWS com a qual o proprietário do diretório o compartilhou. Dependendo do método de compartilhamento usado, um administrador nesta conta poderá ter que aceitar um convite enviado pelo proprietário do diretório antes de começar a usar o diretório compartilhado.

O processo de compartilhamento de diretório cria um diretório compartilhado na conta de consumidor do diretório. Esse diretório compartilhado contém os metadados que permitem que as instâncias do EC2 integrem perfeitamente o domínio, que localiza o diretório de origem na conta do proprietário de diretório. Cada diretório compartilhado na conta de consumidor do diretório tem um identificador exclusivo (Shared directory ID (ID do diretório compartilhado)).

Métodos de compartilhamento

O AWS Managed Microsoft AD fornece estes dois métodos de compartilhamento de diretórios:

- AWS Organizations: esse método facilita o compartilhamento de diretórios dentro da sua organização, pois é possível localizar e validar as contas de consumidor do diretório. Para usar essa opção, sua organização deve ter a opção Todos os recursos habilitada e seu diretório deve estar na conta de gerenciamento da organização. Esse método de compartilhamento simplifica a configuração, pois não exige que as contas de consumidor do diretório aceitem a solicitação de compartilhamento do diretório. No console, esse método é chamado de Compartilhar este diretório com Contas da AWS dentro da sua organização.
- Handshake: esse método habilita o compartilhamento de diretórios quando você não está usando o AWS Organizations. O método do aperto de mãos requer que a conta de consumidor do diretório aceite a solicitação de compartilhamento do diretório. No console, esse método é chamado de Compartilhar este diretório com outras Contas da AWS.

Conectividade de rede

A conectividade de rede é um pré-requisito para usar uma relação de compartilhamento de diretórios entre Contas da AWS. A AWS oferece suporte a muitas soluções para conectar suas VPCs, algumas delas incluem emparelhamento de VPC, gateways de trânsito e VPN. Para começar, consulte o Tutorial: Compartilhando seu diretório AWS gerenciado do Microsoft AD para uma associação perfeita ao domínio EC2.

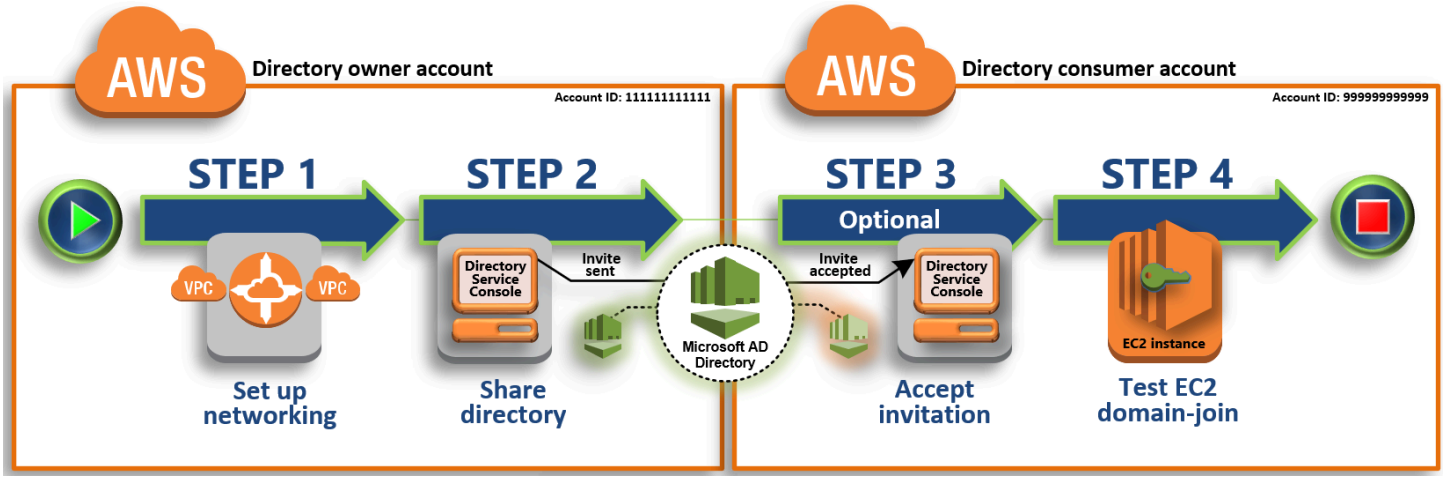
Tutorial: Compartilhando seu diretório AWS gerenciado do Microsoft AD para uma associação perfeita ao domínio EC2

Este tutorial mostra como compartilhar seu diretório AWS gerenciado do Microsoft AD (a conta do proprietário do diretório) com outro Conta da AWS (a conta do consumidor do diretório). Depois que os pré-requisitos de rede forem concluídos, você compartilhará um diretório entre dois. Contas da AWS Depois, você aprenderá como associar diretamente uma instância do EC2 a um domínio na conta de consumidor do diretório.

Recomendamos que você primeiro revise os principais conceitos do compartilhamento de diretório e conteúdo do caso de uso antes de começar a trabalhar neste tutorial. Para ter mais informações, consulte Principais conceitos do compartilhamento de diretórios.

O processo para compartilhar seu diretório difere dependendo se você compartilha o diretório com outra pessoa Conta da AWS na mesma AWS organização ou com uma conta que esteja fora da AWS organização. Para obter mais informações sobre como o compartilhamento funciona, consulte Métodos de compartilhamento.

Esse fluxo de trabalho tem quatro etapas básicas.



Etapa 1: configurar o ambiente de rede

Na conta de proprietário do diretório, configure todos os pré-requisitos de rede necessários para o processo de compartilhamento de diretório.

Etapa 2: compartilhar seu diretório

Enquanto estiver conectado com credenciais de administrador de proprietário do diretório, abra o console do AWS Directory Service e inicie o fluxo de trabalho de compartilhamento de diretório, que envia um convite para a conta de consumidor do diretório.

Etapa 3: aceitar o convite do diretório compartilhado - Opcional

Enquanto estiver conectado com as credenciais de administrador do consumidor do diretório, você abre o AWS Directory Service console e aceita o convite de compartilhamento do diretório.

Etapa 4: testar a associação direta de uma instância do EC2 para Windows Server a um domínio

Por fim, como administrador de consumidor do diretório, tente inserir uma instância do EC2 ao seu domínio e verifique se isso funciona.

Recursos adicionais

- Caso de uso: compartilhar seu diretório para associar diretamente instâncias do Amazon EC2 a um domínio em várias Contas da AWS
- AWS Artigo do blog de segurança: Como unir instâncias do Amazon EC2 de várias contas e VPCs em um único diretório gerenciado AWS do Microsoft AD

Etapa 1: configurar o ambiente de rede

Antes de começar a realizar as etapas deste tutorial, primeiro faça o seguinte:

- Crie dois novos Contas da AWS para fins de teste na mesma região. Quando você cria uma Conta da AWS, ela cria automaticamente uma nuvem privada virtual (VPC) dedicada em cada conta. Anote o ID da VPC em cada conta. Você precisará disso mais tarde.
- Crie uma conexão de emparelhamento da VPC entre duas VPCs em cada conta usando os procedimentos desta etapa.

> **Note**
>
> Embora existam muitas maneiras de conectar o proprietário do diretório e as VPCs da conta de consumidor do diretório, este tutorial usará o método de emparelhamento da VPC. Para obter opções adicionais de conectividade da VPC, consulte Conectividade de rede.

Configure uma conexão de emparelhamento da VPC entre a conta de proprietário do diretório e a conta de consumidor do diretório

A conexão de emparelhamento da VPC que você criará será entre as VPCs do proprietário do diretório e do consumidor do diretório. Siga estas etapas para configurar uma conexão de emparelhamento da VPC para conectividade com a conta de consumidor do diretório. Com essa conexão, é possível rotear o tráfego entre as duas VPCs usando endereços IP privados.

Para criar uma conexão de emparelhamento da VPC entre a conta de proprietário do diretório e a conta de consumidor do diretório.

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/. Faça login como um usuário com credenciais de administrador na conta de proprietário do diretório.
2. No painel de navegação, escolha Peering Connections. Depois, selecione Create Peering Connection (Criar conexão de emparelhamento).
3. Configure as seguintes informações:
   - Peering connection name tag (Tag de nome da conexão de emparelhamento): forneça um nome que identifica claramente essa conexão com a VPC na conta de consumidor do diretório.
   - VPC (Requester) (VPC (Solicitante)): selecione o ID da VPC da conta de proprietário do diretório.
   - Em Select another VPC to peer with (Selecionar outra VPC para fazer o emparelhamento), verifique se My account (Minha conta) e This region (Esta região) estão selecionados.
   - VPC (Accepter) (VPC (Aceitante)): selecione o ID da VPC da conta de consumidor do diretório.
4. Selecione Create Peering Connection (Criar conexão de emparelhamento). Na caixa de diálogo de confirmação, escolha OK.

Como as duas VPCs estão na mesma região, o administrador da conta de proprietário do diretório que enviou a solicitação de emparelhamento da VPC também pode aceitar a solicitação de emparelhamento em nome da conta de consumidor do diretório.

Para aceitar a solicitação de emparelhamento em nome da conta de consumidor do diretório

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Peering Connections.

3. Selecione a conexão pendente de emparelhamento da VPC. (Seu status está como Pending Acceptance (Aceitação pendente).) Selecione Actions (Ações), Accept Request (Aceitar solicitação).
4. Na caixa de diálogo de confirmação, escolha Yes, Accept. Na próxima caixa de diálogo de confirmação, selecione Modify my route tables now (Modificar minhas tabelas de rotas agora) para acessar diretamente a página de tabelas de rotas.

Agora que sua conexão de emparelhamento de VPC está ativa, é preciso adicionar uma entrada à tabela de rotas de VPC na conta de proprietário do diretório. Isso permite que o tráfego seja direcionado à VPC na conta de consumidor do diretório.

Para adicionar uma entrada à tabela de rotas da VPC na conta de proprietário do diretório

1. Na seção Tabelas de rotas do console da Amazon VPC, selecione a tabela de rotas da VPC do proprietário do diretório.
2. Escolha a guia Rotas, escolha Editar rotas e, em seguida, escolha Adicionar rota.
3. Na coluna Destination (Destino), insira o bloco CIDR da VPC do consumidor do diretório.
4. Na coluna Target (Destino), insira o ID da conexão de emparelhamento da VPC (como **`pcx-123456789abcde000`**) para a conexão de emparelhamento que você criou anteriormente na conta de proprietário do diretório.
5. Escolha Salvar alterações.

Para adicionar uma entrada à tabela de rotas da VPC na conta de consumidor do diretório

1. Na seção Tabelas de rotas do console da Amazon VPC, selecione a tabela de rotas da VPC do consumidor do diretório.
2. Escolha a guia Rotas, escolha Editar rotas e, em seguida, escolha Adicionar rota.
3. Na coluna Destination (Destino), insira o bloco CIDR da VPC do proprietário do diretório.
4. Na coluna Target (Destino), insira o ID da conexão de emparelhamento da VPC (como **`pcx-123456789abcde001`**) para a conexão de emparelhamento que você criou anteriormente na conta de consumidor do diretório.
5. Escolha Salvar alterações.

Certifique-se de configurar o grupo de segurança das VPCs do consumidor do diretório para habilitar tráfego de saída adicionando os protocoles e portas do Active Directory à tabela de regras de saída.

Para obter mais informações, consulte Grupos de segurança da VPC e Pré-requisitos do AWS Managed Microsoft AD.

Próxima etapa

Etapa 2: compartilhar seu diretório

Etapa 2: compartilhar seu diretório

Use os procedimentos a seguir para iniciar o fluxo de trabalho do compartilhamento de diretório a partir da conta de proprietário do diretório.

> **Note**
>
> O compartilhamento de diretórios é um recurso regional do AWS Managed Microsoft AD. Se você estiver usando a Replicação em várias regiões, os procedimentos a seguir deverão ser aplicados separadamente em cada região. Para ter mais informações, consulte Recursos globais versus regionais.

Para compartilhar seu diretório da conta de proprietário do diretório

1. Faça login no AWS Management Console com credenciais de administrador na conta do proprietário do diretório e abra o AWS Directory Service console em https://console.aws.amazon.com/directoryservicev2/.
2. No painel de navegação, selecionar Diretórios.
3. Escolha a ID do diretório AWS Managed Microsoft AD que você deseja compartilhar.
4. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja compartilhar seu diretório e, em seguida, escolha a guia Escalar e compartilhar. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Escalar e compartilhar.
5. Na seção Diretórios compartilhados, selecione Ações e, em seguida, selecione Criar diretório compartilhado.
6. Na página Escolha com quem Contas da AWS compartilhar, escolha um dos seguintes métodos de compartilhamento, dependendo das necessidades da sua empresa:

a. Compartilhe este diretório com Contas da AWS dentro da sua organização — Com essa opção, você pode selecionar o Contas da AWS diretório com o qual deseja compartilhar seu diretório em uma lista que mostra tudo Contas da AWS dentro da sua AWS organização. Você deve habilitar o acesso confiável AWS Directory Service antes de compartilhar um diretório. Para obter mais informações, consulte Como habilitar ou desabilitar o acesso confiável.

> **Note**
>
> Para usar essa opção, sua organização deve ter a opção Todos os recursos habilitada e seu diretório deve estar na conta de gerenciamento da organização.

   i. Contas da AWS Em sua organização, selecione o diretório com Contas da AWS o qual você deseja compartilhar o diretório e clique em Adicionar.

   ii. Examine os detalhes de preço e, então, selecione Share (Compartilhar).

   iii. Prossiga para a Etapa 4 deste guia. Como todos Contas da AWS estão na mesma organização, você não precisa seguir a Etapa 3.

b. Compartilhe esse diretório com outros Contas da AWS - Com essa opção, você pode compartilhar um diretório com contas dentro ou fora da sua AWS organização. Você também pode usar essa opção quando seu diretório não é membro de uma AWS organização e você deseja compartilhar com outra Conta da AWS.

   i. Em ID(s) de Conta da AWS , insira todas as IDs de Conta da AWS com as quais você deseja compartilhar o diretório e clique em Adicionar.

   ii. Em Enviar uma nota, digite uma mensagem para o administrador da outra Conta da AWS.

   iii. Examine os detalhes de preço e, então, selecione Share (Compartilhar).

   iv. Prossiga para a Etapa 3.

Próxima etapa

Etapa 3: aceitar o convite do diretório compartilhado - Opcional

Etapa 3: aceitar o convite do diretório compartilhado - Opcional

Se você selecionou a opção Compartilhar esse diretório com outras Contas da AWS (método de handshake) no procedimento anterior, é necessário usar este procedimento para finalizar o fluxo de trabalho do diretório compartilhado. Se você escolheu a opção Compartilhar este diretório com Contas da AWS dentro da sua organização, pule esta etapa e vá para a Etapa 4.

Para aceitar o convite do diretório compartilhado

1. Faça login AWS Management Console com credenciais de administrador na conta do consumidor do diretório e abra o AWS Directory Service console em https://console.aws.amazon.com/directoryservicev2/.
2. No painel de navegação, selecione Directories shared with me (Diretórios compartilhados comigo).
3. Na coluna Shared directory ID (ID do diretório compartilhado), selecione o ID do diretório que está no estado Pending acceptance (Aceitação pendente).
4. Na página Shared directory details (Detalhes do diretório compartilhado), selecione Review (Revisar).
5. Na caixa de diálogo Pending shared directory invitation (Convite de diretório compartilhado pendente), revise a nota, os detalhes do proprietário do diretório e as informações sobre definição de preço. Se você concordar, selecione Accept (Aceitar) para começar a usar o diretório.

Próxima etapa

Etapa 4: testar a associação direta de uma instância do EC2 para Windows Server a um domínio

Etapa 4: testar a associação direta de uma instância do EC2 para Windows Server a um domínio

Você pode usar um dos dois métodos a seguir para testar a associação direta de uma instância do EC2 a um domínio.

Método 1: testar a associação ao domínio usando o console do Amazon EC2

Siga estas etapas na conta de consumidor do diretório.

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o mesmo Região da AWS que o diretório existente.

3. No Painel do EC2, na seção Iniciar instância, escolha Iniciar instância.
4. Na página Iniciar uma instância, na seção Nome e tags, insira o nome que você gostaria de usar para sua instância do Windows EC2.
5. (Opcional) Escolha Adicionar tags extras para um ou mais pares chave-valor de tag para organizar, monitorar ou controlar o acesso para esta instância do EC2.
6. Na seção Imagem da aplicação e do sistema operacional (imagem de máquina da Amazon), escolha Windows no painel Início rápido. É possível alterar a imagem de máquina da Amazon (AMI) do Windows na lista suspensa Imagem de máquina da Amazon (AMI).
7. Na seção Tipo de instância, escolha o tipo de instância que você gostaria de usar na lista suspensa Tipo de instância.
8. Na seção Par de chaves: login, é possível optar por criar um novo par de chaves ou escolher um par de chaves existente.

    a. Para criar um novo par de chaves, escolha Criar par de chaves.

    b. Insira um nome para o par de chaves e selecione uma opção para Tipo de par de chaves e Formato do arquivo de chave privada.

    c. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha .pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha .ppk.

    d. Escolha Criar par de chaves.

    e. O arquivo de chave privada é baixado automaticamente pelo navegador. Salve o arquivo de chave privada em um lugar seguro.

    > **Important**
    >
    > Esta é a única chance de você salvar o arquivo de chave privada.

9. Na página Iniciar uma instância, na seção Configurações de rede, escolha Editar. Escolha a VPC na qual seu diretório foi criado na lista suspensa VPC: obrigatório.
10. Escolha uma das sub-redes públicas em sua VPC na lista suspensa Sub-rede. A sub-rede escolhida deve ter todo o tráfego externo ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.

    Para obter mais informações sobre como conectar a um gateway da Internet, consulte Conectar à Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.

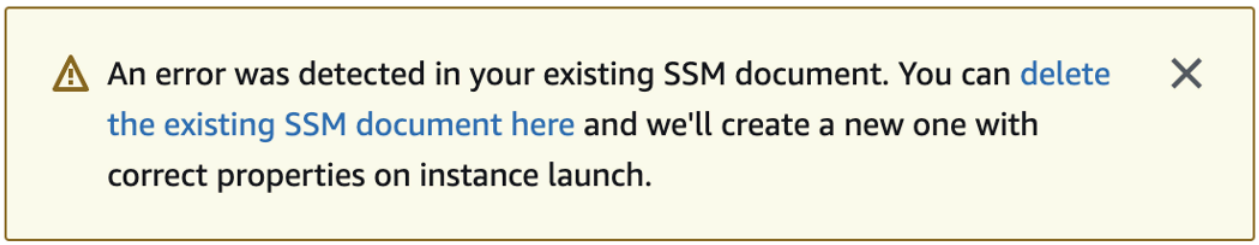
11. Em Atribuir IP público automaticamente, escolha Habilitar.

    Para obter mais informações sobre endereçamento IP público e privado, consulte Endereçamento IP de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.

12. Para configurações de Firewall (grupos de segurança), é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.

13. Para opções de Configurar armazenamento, é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.

14. Selecione a seção Detalhes avançados, escolha seu domínio na lista suspensa Diretório de associação ao domínio.

    > **Note**
    >
    > Depois de escolher o diretório de ingresso no domínio, você poderá ver:
    >
    > 
    >
    >
    > Esse erro ocorre se o assistente de inicialização do EC2 identificar um documento SSM existente com propriedades inesperadas. Você pode executar uma das seguintes ações:
    >
    > - Se você editou anteriormente o documento SSM e as propriedades são esperadas, escolha fechar e continue a executar a instância do EC2 sem alterações.
    > - Selecione o link excluir o documento SSM existente aqui para excluir o documento SSM. Isso permitirá a criação de um documento SSM com as propriedades corretas. O documento SSM será criado automaticamente quando você iniciar a instância do EC2.

15. Para Perfil de instância do IAM, é possível selecionar um perfil de instância do IAM existente ou criar um novo. Selecione um perfil de instância do IAM que tenha as políticas AWS gerenciadas AmazonSSM ManagedInstanceCore e AmazonSSM DirectoryServiceAccess anexadas a ele na lista suspensa do perfil da instância do IAM. Para criar um novo, escolha Criar novo link de perfil do IAM e faça o seguinte:

    1. Selecione Criar função.

2. Em Selecionar entidade confiável, escolha serviço da AWS .
3. Em Use case (Caso de uso), selecione EC2.
4. Em Adicionar permissões, na lista de políticas, selecione as políticas do AmazonSSM ManagedInstanceCore e do AmazonSSM. DirectoryServiceAccess Para filtrar a lista, digite **`SSM`** na caixa de pesquisa. Escolha Próximo.

   > **Note**
   >
   > O AmazonSSM DirectoryServiceAccess fornece as permissões para unir instâncias a uma Active Directory instância gerenciada por. AWS Directory Service O AmazonSSM ManagedInstanceCore fornece as permissões mínimas necessárias para usar o serviço. AWS Systems Manager Para obter mais informações sobre a criação de um perfil com essas permissões e sobre outras permissões e políticas que você pode atribuir ao seu perfil do IAM, consulte Criar um perfil de instância do IAM para Systems Manager no Guia do usuário do AWS Systems Manager .

5. Na página Nomear, revisar e criar, insira um Nome de perfil. Você precisará desse nome de perfil para anexar à instância do EC2.
6. (Opcional) Você pode fornecer uma descrição do perfil de instância do IAM no campo Descrição.
7. Selecione Criar função.
8. Volte para a página Iniciar uma instância e escolha o ícone de atualização ao lado do Perfil de instância do IAM. Seu novo perfil de instância do IAM deve estar visível na lista suspensa do Perfil de instância do IAM. Escolha o novo perfil e mantenha o resto das configurações com seus valores padrão.

16. Escolha Iniciar instância.

Método 2: testar a adesão ao domínio usando AWS Systems Manager

Siga estas etapas na conta de consumidor do diretório. Para concluir esse procedimento, você precisará de algumas informações sobre a conta do proprietário do diretório, como ID do diretório, nome do diretório e endereços IP do DNS.

Pré-requisitos

- Configuração AWS Systems Manager.

  - Para obter mais informações sobre o Systems Manager, consulte Configuração geral do AWS Systems Manager.
- As instâncias nas quais você deseja ingressar no domínio AWS gerenciado do Microsoft Active Directory devem ter uma função do IAM anexada contendo as políticas gerenciadas do AmazonSSM ManagedInstanceCore e do DirectoryServiceAccessAmazonSSM.
  - Para obter mais informações sobre essas políticas gerenciadas e outras políticas que podem ser anexadas a um perfil de instância do IAM para o Systems Manager, consulte Criar um perfil de instância do IAM para o Systems Manager no Guia do usuário do AWS Systems Manager . Para obter mais informações sobre políticas gerenciadas, consulte Políticas gerenciadas pela AWSno Guia do usuário do IAM.

Para obter mais informações sobre o uso do Systems Manager para unir instâncias do EC2 a um domínio AWS gerenciado do Microsoft Active Directory, consulte Como eu uso AWS Systems Manager para unir uma instância do EC2 Windows em execução ao meu domínio do AWS Directory Service? .

1. Abra o AWS Systems Manager console emhttps://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, em Gerenciamento de nós, selecione Executar comando.
3. Selecione Run command.
4. Na página Executar um comando, pesquise por `AWS-JoinDirectoryServiceDomain`. Quando ele for exibido nos resultados da pesquisa, selecione a opção `AWS-JoinDirectoryServiceDomain`.
5. Role para baixo até a seção Command parameters (Parâmetros de comando). Você deve fornecer os parâmetros a seguir:

   > **Note**
   >
   > Você pode localizar o ID do diretório, o nome do diretório e os endereços IP do DNS voltando ao AWS Directory Service console, selecionando Diretórios compartilhados comigo e selecionando seu diretório. Seu ID do diretório pode ser encontrado na seção Detalhes do diretório compartilhado. Você pode localizar os valores de Nome do diretório e Endereços IP de DNS na seção Detalhes do diretório do proprietário.

   - Em ID do diretório, insira o nome do Microsoft Active Directory AWS gerenciado.

- Em Nome do diretório, insira o nome do AWS Managed Microsoft Active Directory (para a conta de proprietário do diretório).
- Em Endereços IP DNS, insira os endereços IP dos servidores DNS no AWS Microsoft Active Directory Gerenciado (para a conta do proprietário do diretório).

6. Em Destinos, selecione Escolher instâncias manualmente e, em seguida, selecione as instâncias que deseja associar ao domínio.
7. Deixe o restante do formulário configurado como seus valores padrão, role a página para baixo e escolha Run (Executar).
8. O status do comando mudará de Pendente para Êxito quando as instâncias forem associadas com êxito ao domínio. Você pode visualizar a saída do comando selecionando o ID da instância da instância que foi associada ao domínio e Visualizar a saída.

Após a conclusão de qualquer uma dessas etapas, você poderá ingressar sua instância do EC2 no domínio. Depois de fazer isso, você pode entrar na sua instância usando um cliente RDP (Remote Desktop Protocol) com as credenciais da sua conta de usuário gerenciada do AWS Microsoft AD.

Descompartilhar seu diretório

Use o procedimento a seguir para descompartilhar o diretório do AWS Managed Microsoft AD.

Para descompartilhar seu diretório

1. No painel de navegação do console do AWS Directory Service, em Active Directory, selecione Diretórios.
2. Escolha o ID do diretório do AWS Managed Microsoft AD que deseja descompartilhar.
3. Na página Detalhes do diretório, siga um destes procedimentos:

   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja descompartilhar seu diretório e, em seguida, escolha a guia Escalar e compartilhar. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Escalar e compartilhar.

4. Na seção Shared directories (Diretórios compartilhados), selecione o diretório compartilhado que você deseja descompartilhar, selecione Actions (Ações) e Unshare (Descompartilhar).
5. Na caixa de diálogo Unshare directory (Descompartilhar diretório), selecione Unshare (Descompartilhar).

Recursos adicionais

- Caso de uso: compartilhar seu diretório para associar diretamente instâncias do Amazon EC2 a um domínio entre contas da AWS
- Artigo do blog de segurança da AWS: Como inserir instâncias do Amazon EC2 de várias contas e VPCs em um único diretório do AWS Managed Microsoft AD
- Associar instâncias de banco de dados do Amazon RDS a um único domínio compartilhado

Associe uma instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory

Você pode unir facilmente uma instância do Amazon EC2 ao Active Directory seu domínio quando a instância é executada. Para ter mais informações, consulte Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory. Você também pode iniciar uma instância do EC2 e associá-la a um Active Directory domínio diretamente do AWS Directory Service console com a AWS Systems Manager automação.

Se você precisar associar manualmente uma instância do EC2 ao seu Active Directory domínio, deverá iniciar a instância na região e no grupo de segurança ou sub-rede adequados e, em seguida, associar a instância ao domínio.

Para se conectar de modo remoto a essas instâncias, você deve ter conectividade IP com as instâncias da rede da qual está se conectando. Na maioria dos casos, é necessário que um gateway da Internet esteja conectado à sua VPC e que a instância tenha um endereço IP público.

Tópicos

- Inicie a instância de administração de diretórios em seu Microsoft AD AWS gerenciado Active Directory
- Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory
- Associe manualmente uma Windows instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory
- Associe perfeitamente uma instância Linux do Amazon EC2 ao seu Microsoft AD Active AWS Directory gerenciado
- Associe manualmente uma instância Linux do Amazon EC2 ao seu AWS Microsoft AD Active Directory gerenciado

- Associe manualmente uma instância Linux do Amazon EC2 ao seu AWS Microsoft AD Active Directory gerenciado usando o Winbind
- Associe manualmente uma instância Mac do Amazon EC2 ao seu AWS Microsoft AD Active Directory gerenciado
- Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD
- Criar ou alterar um conjunto de opções de DHCP

Inicie a instância de administração de diretórios em seu Microsoft AD AWS gerenciado Active Directory

Esse procedimento inicia uma Windows instância de administração de diretórios do Amazon EC2 AWS Management Console usando a AWS Systems Manager automação para gerenciar seus diretórios. Você também pode fazer isso executando a automação AWS-CreateDS diretamente ManagementInstance no console de AWS Systems Manager automação.

Pré-requisitos

Para iniciar uma instância EC2 de administração de diretórios via console, é necessário ter as seguintes permissões habilitadas em sua conta.

- `ds:DescribeDirectories`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2:DeleteSecurityGroup`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`

- iam:CreateInstanceProfile
- iam:CreateRole
- iam:DeleteInstanceProfile
- iam:DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfiles
- iam:ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm:DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:GetDocument

Para iniciar uma instância EC2 de administração de diretórios no AWS Management Console

1. Faça login no console do AWS Directory Service.
2. Em Active Directory, escolha Diretórios.

3. Escolha o ID do diretório em que você deseja iniciar uma instância EC2 de administração de diretórios.
4. Na página do diretório, no canto superior direito, escolha Ações.
5. Na lista suspensa Ações, escolha Iniciar instância EC2 de administração de diretórios.
6. Na página Iniciar instância do EC2 de administração de diretórios, em Parâmetros de entrada, preencha os campos necessários.

    a. (Opcional) Você pode fornecer um par de chaves para a instância. Na lista suspensa Nome do par de chaves - opcional, selecione um par de chaves.

    b. (Opcional) Escolha AWS CLI o comando Exibir para ver um exemplo que você usa no AWS CLI para executar essa automação.
7. Escolha Enviar.
8. Você será levado de volta à página do diretório. Uma barra de flash verde é exibida na parte superior da tela para indicar que você iniciou a execuçaõ com êxito.

Para visualizar a instância EC2 de administração de diretórios

Se você não tiver iniciado nenhuma instância do EC2 para um diretório, um traço (-) será exibido em Instância do EC2 de administração de diretórios.

1. Em Active Directory, escolha Diretórios e selecione o diretório que deseja visualizar.
2. Em Detalhes do diretório, em Instância do EC2 de administração de diretórios, escolha uma ou todas as suas instâncias para visualizar.
3. Ao escolher uma instância, você é direcionado para a página Conectar a instância do EC2 para conectar um desktop remoto à sua instância.

Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory

Esse procedimento une perfeitamente uma instância do Amazon Windows EC2 ao seu Microsoft AD AWS gerenciado. Se você precisar realizar uma junção perfeita de domínios em vários Contas da AWS, consulteTutorial: Compartilhando seu diretório AWS gerenciado do Microsoft AD para uma associação perfeita ao domínio EC2. Para obter mais informações sobre o Amazon EC2, consulte O que é o Amazon EC2?.

Para ingressar perfeitamente em uma instância do Amazon EC2 Windows

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o mesmo Região da AWS que o diretório existente.
3. No Painel do EC2, na seção Iniciar instância, escolha Iniciar instância.
4. Na página Iniciar uma instância, na seção Nome e tags, insira o nome que você gostaria de usar para sua instância do Windows EC2.
5. (Opcional) Escolha Adicionar tags extras para um ou mais pares chave-valor de tag para organizar, monitorar ou controlar o acesso para esta instância do EC2.
6. Na seção Imagem da aplicação e do sistema operacional (imagem de máquina da Amazon), escolha Windows no painel Início rápido. É possível alterar a imagem de máquina da Amazon (AMI) do Windows na lista suspensa Imagem de máquina da Amazon (AMI).
7. Na seção Tipo de instância, escolha o tipo de instância que você gostaria de usar na lista suspensa Tipo de instância.
8. Na seção Par de chaves: login, é possível optar por criar um novo par de chaves ou escolher um par de chaves existente.

    a. Para criar um novo par de chaves, escolha Criar par de chaves.

    b. Insira um nome para o par de chaves e selecione uma opção para Tipo de par de chaves e Formato do arquivo de chave privada.

    c. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha .pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha .ppk.

    d. Escolha Criar par de chaves.

    e. O arquivo de chave privada é baixado automaticamente pelo navegador. Salve o arquivo de chave privada em um lugar seguro.

    > **Important**
    >
    > Esta é a única chance de você salvar o arquivo de chave privada.

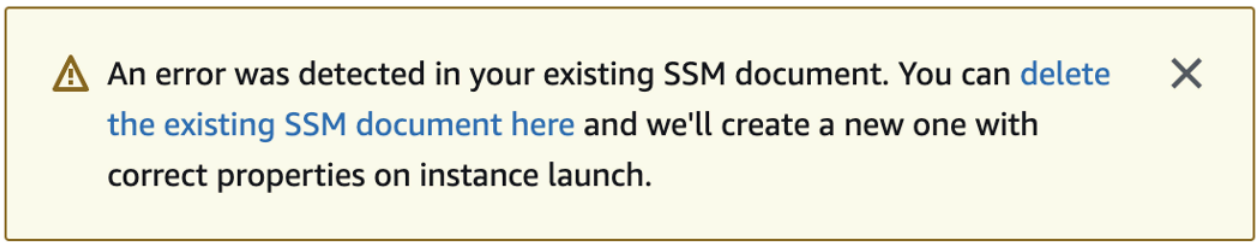
9. Na página Iniciar uma instância, na seção Configurações de rede, escolha Editar. Escolha a VPC na qual seu diretório foi criado na lista suspensa VPC: obrigatório.
10. Escolha uma das sub-redes públicas em sua VPC na lista suspensa Sub-rede. A sub-rede escolhida deve ter todo o tráfego externo ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.

Para obter mais informações sobre como conectar a um gateway da Internet, consulte Conectar à Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.

11. Em Atribuir IP público automaticamente, escolha Habilitar.

    Para obter mais informações sobre endereçamento IP público e privado, consulte Endereçamento IP de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.

12. Para configurações de Firewall (grupos de segurança), é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
13. Para opções de Configurar armazenamento, é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
14. Selecione a seção Detalhes avançados, escolha seu domínio na lista suspensa Diretório de associação ao domínio.

> **Note**
>
> Depois de escolher o diretório de ingresso no domínio, você poderá ver:
>
> 
>
>
> Esse erro ocorre se o assistente de inicialização do EC2 identificar um documento SSM existente com propriedades inesperadas. Você pode executar uma das seguintes ações:
>
> - Se você editou anteriormente o documento SSM e as propriedades são esperadas, escolha fechar e continue a executar a instância do EC2 sem alterações.
> - Selecione o link excluir o documento SSM existente aqui para excluir o documento SSM. Isso permitirá a criação de um documento SSM com as propriedades corretas. O documento SSM será criado automaticamente quando você iniciar a instância do EC2.

15. Para Perfil de instância do IAM, é possível selecionar um perfil de instância do IAM existente ou criar um novo. Selecione um perfil de instância do IAM que tenha as políticas AWS gerenciadas AmazonSSM ManagedInstanceCore e AmazonSSM DirectoryServiceAccess anexadas a ele na

lista suspensa do perfil da instância do IAM. Para criar um novo, escolha Criar novo link de perfil do IAM e faça o seguinte:

1. Selecione Criar função.
2. Em Selecionar entidade confiável, escolha serviço da AWS .
3. Em Use case (Caso de uso), selecione EC2.
4. Em Adicionar permissões, na lista de políticas, selecione as políticas do AmazonSSM ManagedInstanceCore e do AmazonSSM. DirectoryServiceAccess Para filtrar a lista, digite **`SSM`** na caixa de pesquisa. Escolha Próximo.

   > **Note**
   >
   > O AmazonSSM DirectoryServiceAccess fornece as permissões para unir instâncias a uma Active Directory instância gerenciada por. AWS Directory Service O AmazonSSM ManagedInstanceCore fornece as permissões mínimas necessárias para usar o serviço. AWS Systems Manager Para obter mais informações sobre a criação de um perfil com essas permissões e sobre outras permissões e políticas que você pode atribuir ao seu perfil do IAM, consulte Criar um perfil de instância do IAM para Systems Manager no Guia do usuário do AWS Systems Manager .

5. Na página Nomear, revisar e criar, insira um Nome de perfil. Você precisará desse nome de perfil para anexar à instância do EC2.
6. (Opcional) Você pode fornecer uma descrição do perfil de instância do IAM no campo Descrição.
7. Selecione Criar função.
8. Volte para a página Iniciar uma instância e escolha o ícone de atualização ao lado do Perfil de instância do IAM. Seu novo perfil de instância do IAM deve estar visível na lista suspensa do Perfil de instância do IAM. Escolha o novo perfil e mantenha o resto das configurações com seus valores padrão.

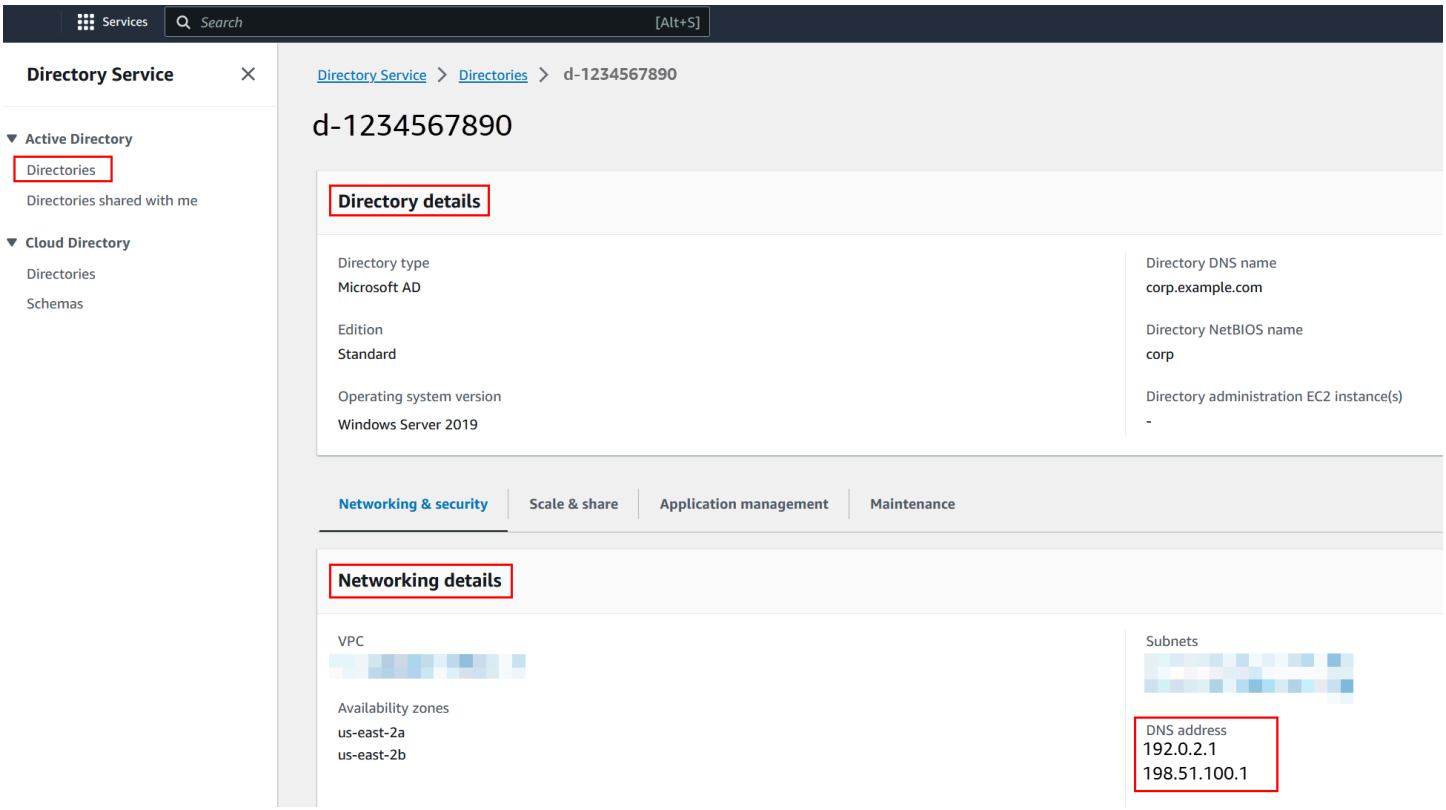
16. Escolha Iniciar instância.

Associe manualmente uma Windows instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory

Para unir manualmente uma Windows instância existente do Amazon EC2 a um AWS Microsoft AD gerenciadoActive Directory, a instância deve ser executada usando os parâmetros especificados

em. [Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory]

Você precisará dos endereços IP dos servidores DNS AWS gerenciados do Microsoft AD. Essas informações podem ser encontradas em Serviços de diretório > Diretórios > o link ID do diretório do seu diretório > seções Detalhes do diretório e Rede e segurança.



Para unir uma instância do Windows a um Microsoft AD AWS gerenciado Active Directory

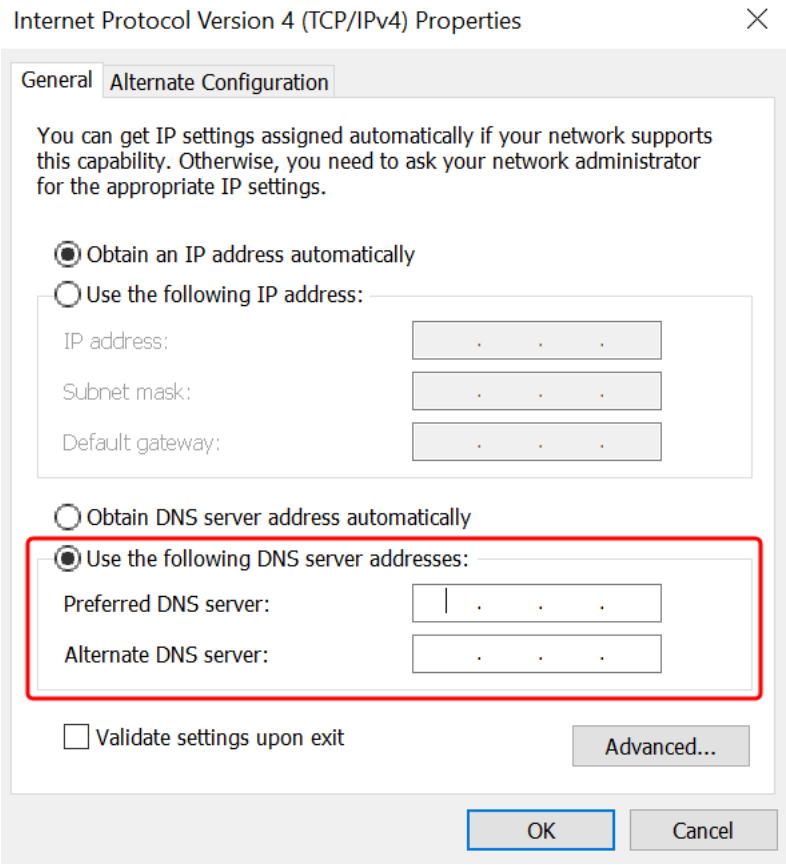
1. Conecte-se à instância usando qualquer cliente Remote Desktop Protocol.
2. Abra a caixa de diálogo de propriedades TCP/IPv4 na instância.
   a. Abra Conexões de rede.

> **Tip**
>
> Você pode abrir Conexões de rede de maneira direta executando o seguinte comando a partir de um prompt de comando na instância.
>
> ```
> %SystemRoot%\system32\control.exe ncpa.cpl
> ```

b. Abra o menu de contexto (clique com o botão direito do mouse) de qualquer conexão de rede habilitada e escolha Propriedades.

c. Na caixa de diálogo de propriedades da conexão, abra (clique duas vezes) Protocolo de Internet versão 4.

3. Selecione Usar os seguintes endereços de servidor DNS, altere os endereços do servidor DNS preferencial e do servidor DNS alternativo para os endereços IP dos seus servidores DNS gerenciados fornecidos pelo AWS Microsoft AD e escolha OK.



4. Abra a caixa de diálogo Propriedades do sistema da instância, selecione a guia Nome do computador e escolha Alterar.

> **Tip**
>
> Você pode abrir a caixa de diálogo Propriedades do sistema de maneira direta executando o seguinte comando a partir de um prompt de comando na instância.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. No campo Membro de, selecione Domínio, insira o nome totalmente qualificado do seu Microsoft AD Active Directory AWS gerenciado e escolha OK.
6. Quando solicitado a fornecer o nome e a senha do administrador do domínio, digite o nome de usuário e a senha de uma conta que tenha privilégios de ingresso no domínio. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

   > **Note**
   >
   > Você pode inserir o nome totalmente qualificado do seu domínio ou o nome NetBIOS, seguido por uma barra invertida (\) e, em seguida, o nome de usuário. O nome de usuário seria Admin. Por exemplo, o **`corp.example.com\admin`** ou o **`corp\admin`**.

7. Depois que você receber a mensagem de boas-vindas ao domínio, reinicie a instância para que as alterações entrem em vigor.

Agora que sua instância foi associada ao domínio AWS gerenciado do Microsoft AD Active Directory, você pode fazer login nessa instância remotamente e instalar utilitários para gerenciar o diretório, como adicionar usuários e grupos. As Ferramentas de Administração do Active Directory podem ser usadas para criar usuários e grupos. Para ter mais informações, consulte Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado.

> **Note**
>
> Você também pode usar o Amazon Route 53 para processar consultas de DNS em vez de alterar manualmente os endereços DNS em suas instâncias do Amazon EC2. Para obter mais informações, consulte Integrando a resolução de DNS do seu serviço de diretório Amazon Route 53 Resolver e encaminhando consultas DNS de saída para sua rede.

Associe perfeitamente uma instância Linux do Amazon EC2 ao seu Microsoft AD Active AWS Directory gerenciado

Esse procedimento une perfeitamente uma instância Linux do Amazon EC2 ao seu Microsoft AD Active AWS Directory gerenciado. Se você precisar realizar uma união de domínio perfeita em várias AWS contas, opcionalmente, você pode optar por ativar o compartilhamento de diretórios.

As seguintes distribuições e versões de instância do Linux são suportadas:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> As distribuições anteriores ao Ubuntu 14 e ao Red Hat Enterprise Linux 7 não oferecem suporte ao recurso de associação direta a domínios.

Para uma demonstração do processo de unir perfeitamente uma instância Linux ao seu Microsoft AD Active Directory AWS gerenciado, veja o YouTube vídeo a seguir.

Demonstração de associação direta de domínio ao Amazon EC2 para Linux

Pré-requisitos

Antes de configurar a união de domínio perfeita em uma instância Linux, você precisa concluir os procedimentos nesta seção.

Selecionar sua conta de serviço para associação direta ao domínio

Você pode unir perfeitamente computadores Linux ao seu domínio AWS gerenciado do Microsoft AD Active Directory. Para fazer isso, é necessário usar uma conta de usuário com permissões de criação de conta de computador para associar as máquinas ao domínio. Embora os membros do grupo Administradores delegados da AWS ou outros grupos possam ter privilégios suficientes para associar computadores ao domínio, não recomendamos fazer isso. Como prática recomendada, sugerimos usar uma conta de serviço que tenha os privilégios mínimos necessários para associar os computadores ao domínio.

Para delegar uma conta com os privilégios mínimos necessários para associar os computadores ao domínio, você pode executar os seguintes PowerShell comandos. Você deve executar esses comandos em um computador Windows associado ao domínio com as Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado instaladas. Além disso, você

deve usar uma conta que tenha permissão para modificar as permissões na UO ou no contêiner do seu Computador. O PowerShell comando define permissões que permitem que a conta de serviço crie objetos de computador no contêiner de computadores padrão do seu domínio.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Se você preferir usar uma interface gráfica de usuário (GUI), poderá usar o processo manual descrito em Delegar privilégios para sua conta de serviço.

Criar os segredos para armazenar a conta de serviço do domínio

Você pode usar AWS Secrets Manager para armazenar a conta de serviço de domínio.

Para criar segredos e armazenar as informações da conta de serviço do domínio

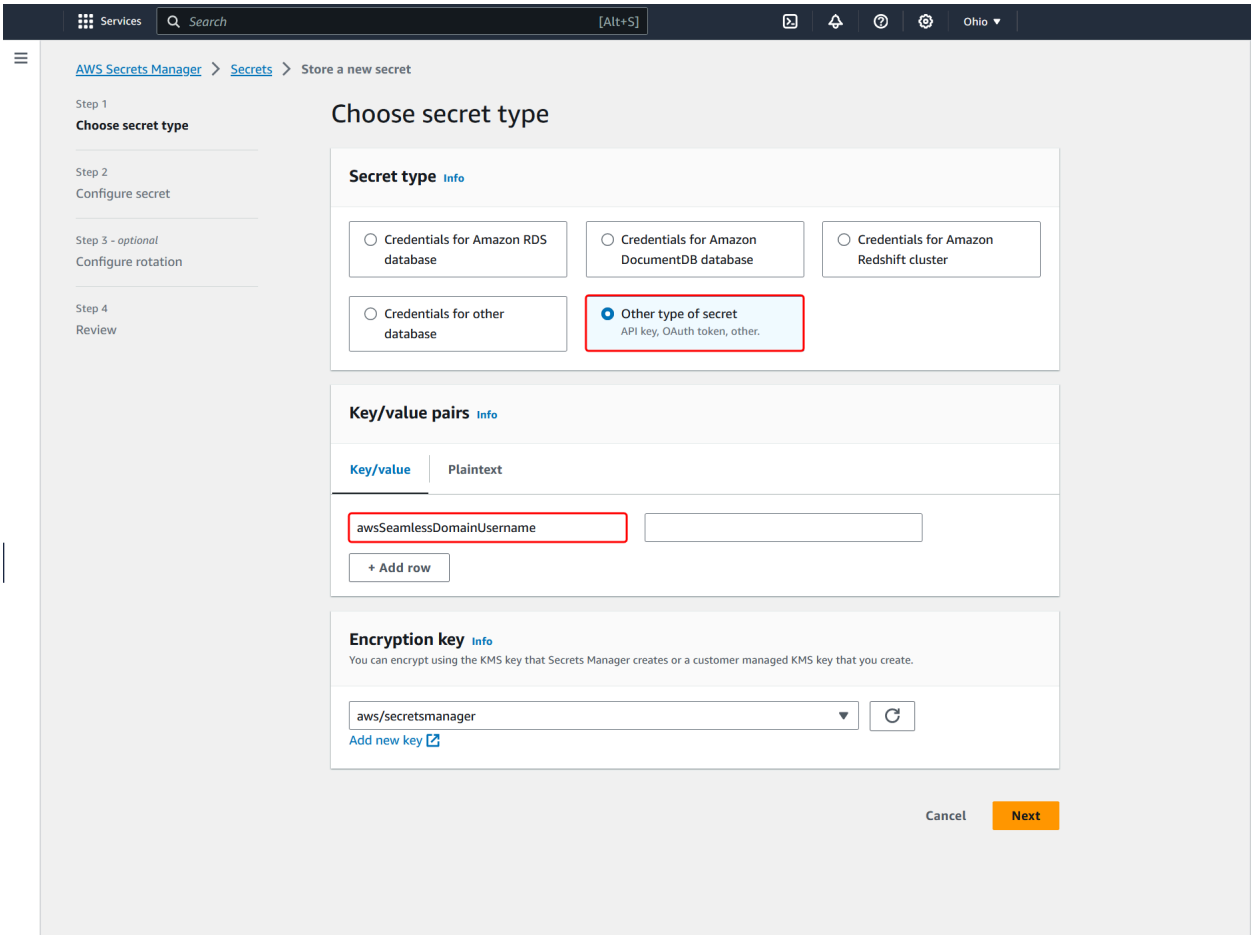
1. Faça login no AWS Management Console e abra o AWS Secrets Manager console em https://console.aws.amazon.com/secretsmanager/.
2. Selecione Armazenar um novo segredo.
3. Na página Store a new secret (Armazenar um novo segredo), faça o seguinte:

a. Em Tipo de segredo, escolha Outro tipo de segredos.

b. Em Pares de chave/valor, faça o seguinte:

i. Na primeira caixa, insira **`awsSeamlessDomainUsername`**. Na mesma linha, na próxima caixa, insira o nome de usuário da sua conta de serviço. Por exemplo, se você usou o PowerShell comando anteriormente, o nome da conta de serviço seria**`awsSeamlessDomain`**.

> **Note**
>
> Você deve inserir **`awsSeamlessDomainUsername`** exatamente como está. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.



ii. Escolha Adicionar linha.

iii. Na nova linha, na primeira caixa, insira **awsSeamlessDomainPassword**. Na mesma linha, na próxima caixa, insira a senha da sua conta de serviço.

> **Note**
>
> Você deve inserir **awsSeamlessDomainPassword** exatamente como está. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.

iv. Em Chave de criptografia, deixe o valor padrão`aws/secretsmanager`. AWS Secrets Manager sempre criptografa o segredo quando você escolhe essa opção. Também é possível escolher uma chave criada por você.

> **Note**
>
> Existem taxas associadas AWS Secrets Manager, dependendo de qual segredo você usa. Para obter a lista de preços atual completa, consulte Definição de preço do AWS Secrets Manager.
> Você pode usar a chave AWS gerenciada `aws/secretsmanager` que o Secrets Manager cria para criptografar seus segredos gratuitamente. Se você criar suas próprias chaves KMS para criptografar seus segredos, AWS cobrará a taxa atual AWS KMS . Para obter mais informações, consulte Preços do AWS Key Management Service.

v. Escolha Próximo.

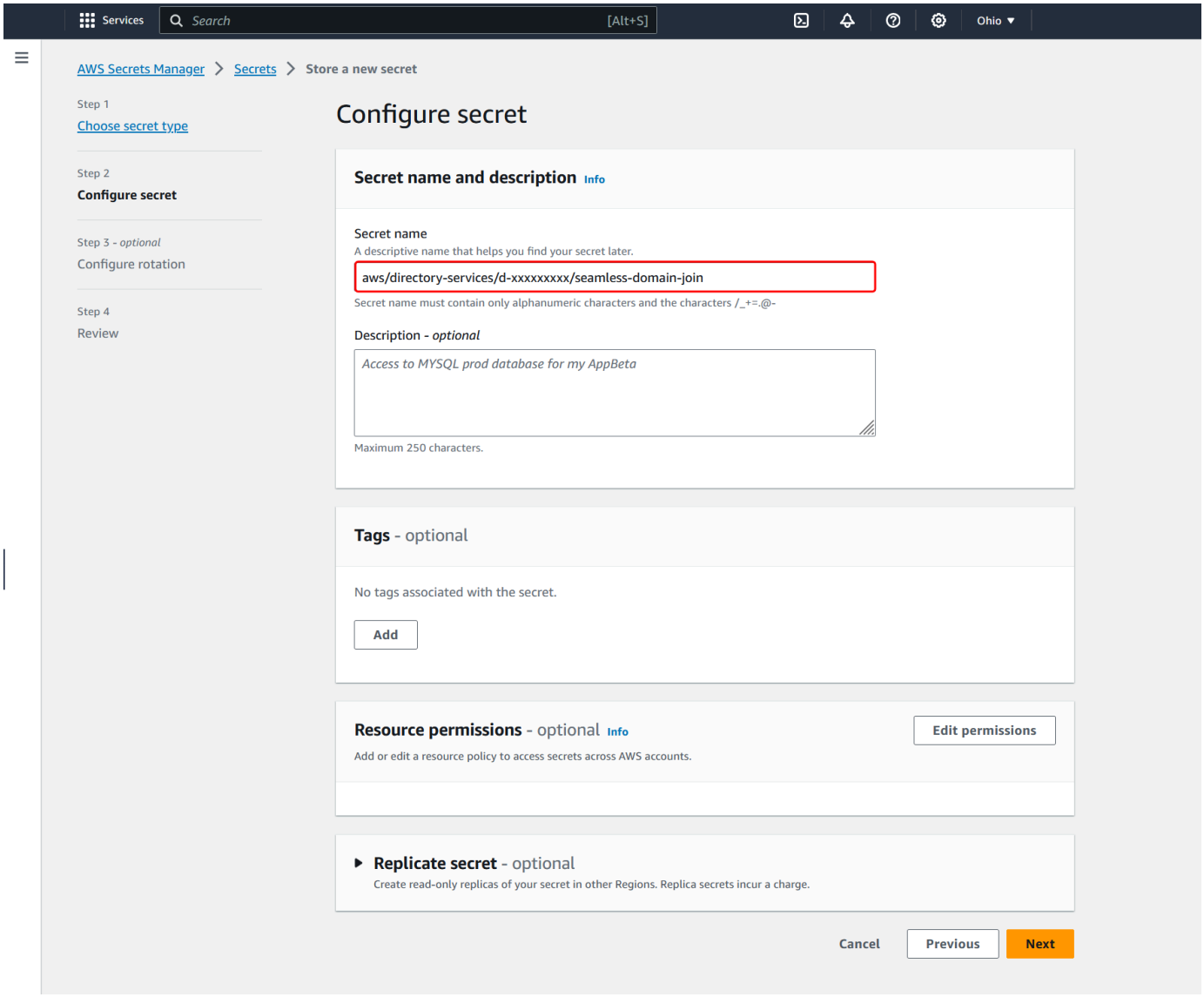
4. Em Nome secreto, insira um nome secreto que inclua sua ID de diretório usando o seguinte formato, substituindo *d-xxxxxxxxx* pela ID do diretório:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Ele será usado para recuperar segredos no aplicativo.

> **Note**
>
> Você deve inserir **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** exatamente como está, mas substituir *d-xxxxxxxxxx* pelo ID do diretório.

Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.



5. Mantenha todo o resto definido como padrão e, em seguida, escolha Próximo.
6. Em Configurar rotação automática, mantenha a opção Desabilitar rotação automática selecionada e escolha Próximo.

   Você pode ativar a rotação desse segredo depois de armazená-lo.
7. Revise as configurações e escolha Armazenar para salvar as alterações. O console do Secrets Manager leva você de volta para a lista de segredos da sua conta com o novo segredo agora incluído na lista.

8. Escolha seu nome de segredo recém-criado na lista e anote o valor do ARN do segredo. Ele será necessário na próxima seção.

Ativar a rotação para o segredo da conta de serviço de domínio

Recomendamos que você alterne regularmente os segredos para melhorar sua postura de segurança.

Para ativar a rotação do segredo da conta de serviço de domínio

- Siga as instruções em Configurar a rotação automática para AWS Secrets Manager segredos no Guia do AWS Secrets Manager usuário.

  Para a Etapa 5, use o modelo de rotação das credenciais do Microsoft Active Directory no Guia do AWS Secrets Manager Usuário.

  Para obter ajuda, consulte Solucionar problemas AWS Secrets Manager de rotação no Guia do AWS Secrets Manager usuário.

Criar a política e o perfil do IAM necessários

Use as etapas de pré-requisito a seguir para criar uma política personalizada que permita acesso somente de leitura ao seu segredo de junção de domínio contínuo do Secrets Manager (que você criou anteriormente) e para criar uma nova função LinuxEC2 IAM. DomainJoin

Criar a política de leitura do IAM para o Secrets Manager

Você usa o console do IAM para criar uma política que concede acesso somente de leitura ao seu segredo do Secrets Manager.

Para criar a política de leitura do IAM para o Secrets Manager

1. Faça login no AWS Management Console como um usuário que tem permissão para criar políticas do IAM. Em seguida, abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, Gerenciamento de acesso, escolha Políticas.
3. Escolha Criar política.
4. Escolha a guia JSON e copie o texto do documento de política JSON a seguir. Em seguida, cole-o na caixa de texto JSON.

> **Note**
>
> Certifique-se de substituir o ARN da região e do recurso pela região e o ARN reais do segredo que você criou anteriormente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Quando terminar, escolha Próximo. O validador de política indica se há qualquer erro de sintaxe. Para obter mais informações, consulte Validar políticas do IAM.
6. Na página Revisar política, insira um nome de política, como **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Revise a seção Resumo para ver as permissões que são concedidas pela política. Em seguida, selecione Criar política para salvar suas alterações. A nova política aparece na lista de políticas gerenciadas e está pronta para ser anexada a uma identidade.

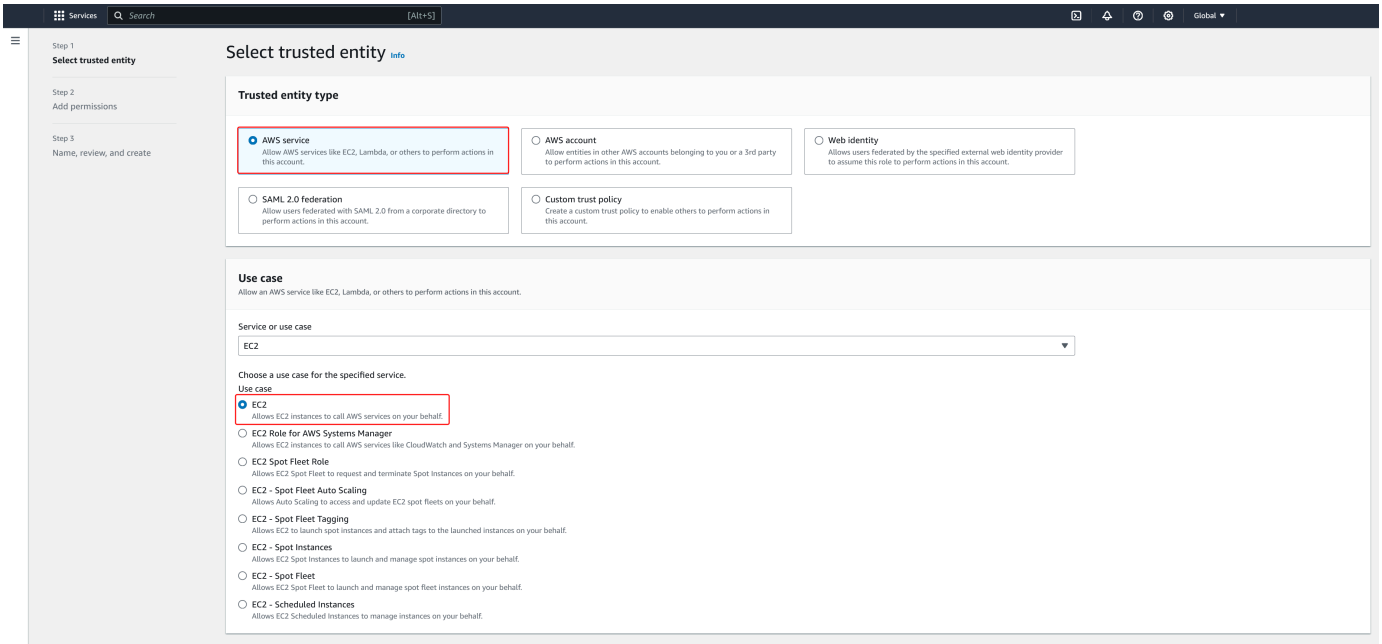
> **Note**
>
> Recomendamos criar uma política por segredo. Isso garante que as instâncias tenham acesso somente ao segredo apropriado e minimiza o impacto em caso de comprometimento de uma instância.

Crie a função LinuxEC2 DomainJoin

Você usa o console do IAM para criar o perfil que usará para associar sua instância do EC2 do Linux ao domínio.

Para criar a função LinuxEC2 DomainJoin

1. Faça login no AWS Management Console como um usuário que tem permissão para criar políticas do IAM. Em seguida, abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, em Gerenciamento de acesso, escolha Perfis.
3. No painel de conteúdo, escolha Criar perfil.
4. Em Select type of trusted entity (Selecionar o tipo de entidade confiável), escolha AWS service (serviço).
5. Em Caso de uso, escolha EC2 e, em seguida, escolha Avançar.



6. Em Políticas de filtro, faça o seguinte:

   a. Insira **`AmazonSSMManagedInstanceCore`**. Em seguida, marque a caixa de seleção para esse item na lista.

   b. Insira **`AmazonSSMDirectoryServiceAccess`**. Em seguida, marque a caixa de seleção para esse item na lista.

   c. Insira **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (ou o nome da política que você criou no procedimento anterior). Em seguida, marque a caixa de seleção para esse item na lista.

d. Depois de adicionar as três políticas listadas acima, selecione Criar função.

> **Note**
>
> O AmazonSSM DirectoryServiceAccess fornece as permissões para unir instâncias a uma Active Directory instância gerenciada por. AWS Directory Service O AmazonSSM ManagedInstanceCore fornece as permissões mínimas necessárias para usar o serviço. AWS Systems Manager Para obter mais informações sobre a criação de um perfil com essas permissões e sobre outras permissões e políticas que você pode atribuir ao seu perfil do IAM, consulte Criar um perfil de instância do IAM para Systems Manager no Guia do usuário do AWS Systems Manager .

7. Insira um nome para sua nova função, como **`LinuxEC2DomainJoin`** ou outro nome de sua preferência no campo Nome da função.
8. (Opcional) Em Role description (Descrição da função), insira uma descrição.
9. (Opcional) Escolha Adicionar nova tag na Etapa 3: Adicionar tags para adicionar tags. Os pares de chave-valor de tag são usados para organizar, rastrear ou controlar o acesso a essa função.
10. Selecione Criar função.

Junte-se perfeitamente à sua instância Linux

Agora que você configurou todas as tarefas de pré-requisito, você pode usar o procedimento a seguir para unir perfeitamente sua instância do EC2 Linux.

Para unir perfeitamente sua instância Linux

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No seletor de região na barra de navegação, escolha o mesmo Região da AWS que o diretório existente.
3. No Painel do EC2, na seção Iniciar instância, escolha Iniciar instância.
4. Na página Iniciar uma instância, na seção Nome e tags, insira o nome que você gostaria de usar para sua instância Linux EC2.
5. (Opcional) Escolha Adicionar tags extras para um ou mais pares chave-valor de tag para organizar, monitorar ou controlar o acesso para esta instância do EC2.

6. Na seção Imagem do aplicativo e do sistema operacional (Amazon Machine Image), escolha uma AMI Linux que você deseja iniciar.

> **Note**
>
> A AMI usada deve ter AWS Systems Manager (SSM Agent) versão 2.3.1644.0 ou superior. Para verificar a versão do SSM Agent instalada em sua AMI iniciando uma instância por essa AMI, consulte Obter a versão do SSM Agent instalada. Se você precisar atualizar o SSM Agent, consulte Instalar e configurar o SSM Agent em instâncias do EC2 para Linux.
> O SSM usa o `aws:domainJoin` plug-in ao unir uma instância Linux a um Active Directory domínio. *`O plug-in altera o nome do host das instâncias Linux para o formato EC2AMAZ- XXXXXXX.`* Para obter mais informações sobre`aws:domainJoin`, consulte a referência do plug-in do documento de AWS Systems Manager comando no Guia AWS Systems Manager do usuário.

7. Na seção Tipo de instância, escolha o tipo de instância que você gostaria de usar na lista suspensa Tipo de instância.
8. Na seção Par de chaves: login, é possível optar por criar um novo par de chaves ou escolher um par de chaves existente. Para criar um novo par de chaves, escolha Criar par de chaves. Insira um nome para o par de chaves e selecione uma opção para Tipo de par de chaves e Formato do arquivo de chave privada. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha .pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha .ppk. Escolha Criar par de chaves. O arquivo de chave privada é baixado automaticamente pelo navegador. Salve o arquivo de chave privada em um lugar seguro.

> **Important**
>
> Esta é a única chance de você salvar o arquivo de chave privada.

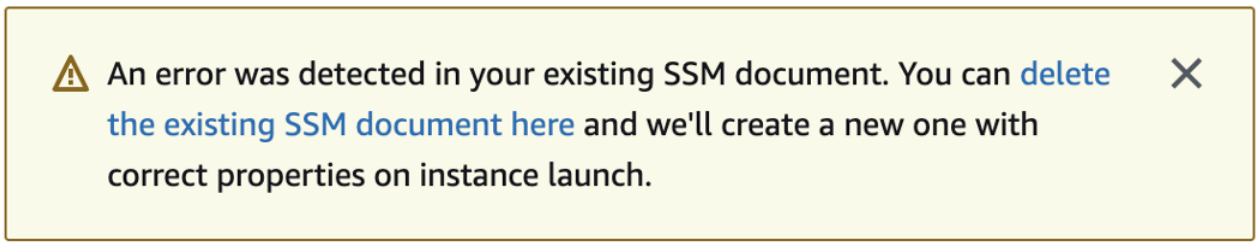
9. Na página Iniciar uma instância, na seção Configurações de rede, escolha Editar. Escolha a VPC na qual seu diretório foi criado na lista suspensa VPC: obrigatório.
10. Escolha uma das sub-redes públicas em sua VPC na lista suspensa Sub-rede. A sub-rede escolhida deve ter todo o tráfego externo ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.

Para obter mais informações sobre como conectar a um gateway da Internet, consulte Conectar à Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.

11. Em Atribuir IP público automaticamente, escolha Habilitar.

    Para obter mais informações sobre endereçamento IP público e privado, consulte Endereçamento IP de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.

12. Para configurações de Firewall (grupos de segurança), é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
13. Para opções de Configurar armazenamento, é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
14. Selecione a seção Detalhes avançados, escolha seu domínio na lista suspensa Diretório de associação ao domínio.

> **Note**
>
> Depois de escolher o diretório de ingresso no domínio, você poderá ver:
>
> 
>
>
> Esse erro ocorre se o assistente de inicialização do EC2 identificar um documento SSM existente com propriedades inesperadas. Você pode executar uma das seguintes ações:
>
> - Se você editou anteriormente o documento SSM e as propriedades são esperadas, escolha fechar e continue a executar a instância do EC2 sem alterações.
> - Selecione o link excluir o documento SSM existente aqui para excluir o documento SSM. Isso permitirá a criação de um documento SSM com as propriedades corretas. O documento SSM será criado automaticamente quando você iniciar a instância do EC2.

15. Para o perfil da instância do IAM, escolha a função do IAM que você criou anteriormente na seção de pré-requisitos Etapa 2: Criar a função LinuxEC2. DomainJoin
16. Escolha Iniciar instância.

> **Note**
>
> Se você estiver realizando uma associação direta a domínio com o SUSE Linux, uma reinicialização será necessária antes que as autenticações funcionem. Para reinicializar o SUSE via terminal Linux, digite sudo reboot.

Associe manualmente uma instância Linux do Amazon EC2 ao seu AWS Microsoft AD Active Directory gerenciado

Além das instâncias Windows do Amazon EC2, você também pode unir determinadas instâncias Linux do Amazon EC2 ao seu Microsoft AD Active AWS Directory gerenciado. As seguintes distribuições e versões de instância do Linux são suportadas:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI do Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Outras distribuições e versões do Linux podem funcionar, mas não foram testadas.

Associe uma instância Linux ao seu Microsoft AD AWS gerenciado

Antes de associar uma instância do Amazon Linux, CentOS, Red Hat ou Ubuntu ao seu diretório, a instância deve primeiro ser iniciada conforme especificado em Junte-se perfeitamente à sua instância Linux.

> **Important**
>
> Alguns dos procedimentos a seguir, se não forem executados corretamente, podem tornar sua instância inacessível ou não utilizável. Portanto, nós sugerimos enfaticamente

que você faça um backup ou tire um snapshot da sua instância antes de executar esses procedimentos.

Para associar uma instância do Linux ao seu diretório

Siga as etapas para a sua instância do Linux específica usando uma das seguintes guias:

Amazon Linux

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Verifique se sua instância do Amazon Linux de 64 bits está atualizada.

```
sudo yum -y update
```

4. Instale os pacotes do Amazon Linux necessários em sua instância do Linux.

> **Note**
>
> Alguns desses pacotes já podem estar instalados.
> Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração.
> Você geralmente pode deixar os campos nessas telas em branco.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Para obter ajuda para determinar a versão do Amazon Linux que você está usando, consulte Como identificar imagens do Amazon Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

5. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Uma conta no domínio *example.com* com privilégios de associação a domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

6. Ajuste o serviço SSH para permitir autenticação de senha.
   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

   b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

   c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

7. Depois que a instância for reiniciada, conecte-se a ela com qualquer cliente SSH e adicione o grupo Administradores AWS Delegados à lista de sudoers executando as seguintes etapas:

   a. Abra o arquivo `sudoers` com o seguinte comando:

   ```
   sudo visudo
   ```

   b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

CentOS

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Verifique se sua instância do CentOS 7 está atualizada.

   ```
   sudo yum -y update
   ```

4. Instale os pacotes do CentOS 7 necessários na sua instância do Linux.

   > **Note**
   >
   > Alguns desses pacotes já podem estar instalados.

Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração. Você geralmente pode deixar os campos nessas telas em branco.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Uma conta no domínio *example.com* com privilégios de associação a domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

6. Ajuste o serviço SSH para permitir autenticação de senha.
   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

   b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

   c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

7. Depois que a instância for reiniciada, conecte-se a ela com qualquer cliente SSH e adicione o grupo Administradores AWS Delegados à lista de sudoers executando as seguintes etapas:

   a. Abra o arquivo `sudoers` com o seguinte comando:

   ```
   sudo visudo
   ```

   b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

Red Hat

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Certifique-se de que a instância do Red Hat - 64 bits está atualizada.

   ```
   sudo yum -y update
   ```

4. Instale os pacotes do Red Hat necessários na sua instância do Linux.

   > **Note**
   >
   > Alguns desses pacotes já podem estar instalados.

Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração. Você geralmente pode deixar os campos nessas telas em branco.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

O SaM AccountName para uma conta no domínio *example.com* que tem privilégios de associação de domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

6. Ajuste o serviço SSH para permitir autenticação de senha.
   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

   b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

   c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

7. Depois que a instância for reiniciada, conecte-se a ela com qualquer cliente SSH e adicione o grupo Administradores AWS Delegados à lista de sudoers executando as seguintes etapas:

   a. Abra o arquivo `sudoers` com o seguinte comando:

   ```
   sudo visudo
   ```

   b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

SUSE

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância do Linux para usar os endereços IP dos servidores de DNS fornecidos pelo AWS Directory Service. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Verifique se sua instância do SUSE Linux 15 está atualizada.

   a. Conecte o repositório de pacotes.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Atualize o SUSE.

   ```
   sudo zypper update -y
   ```

4. Instale os pacotes SUSE Linux 15 necessários em sua instância do Linux.

> **Note**
>
> Alguns desses pacotes já podem estar instalados.
> Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração.
> Você geralmente pode deixar os campos nessas telas em branco.

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-
client
```

5. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -U join_account example.com --verbose
```

join_account

O SaM AccountName no domínio *example.com* que tem privilégios de associação de domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome do DNS totalmente qualificado do seu diretório.

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Observe que espera-se ambos os retornos a seguir.

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Habilite manualmente o SSSD no PAM.

```
sudo pam-config --add --sss
```

7. Edite o nsswitch.conf para habilitar o SSSD no nsswitch.conf

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. Adicione a seguinte linha a /etc/pam.d/common-session para criar automaticamente um diretório inicial no login inicial

```
sudo vi /etc/pam.d/common-session
```

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Reinicialize a instância para concluir o processo de ingresso no domínio.

```
sudo reboot
```

10. Reconecte-se à instância usando qualquer cliente SSH para verificar se o acesso ao domínio foi concluído com êxito e finalizar etapas adicionais

    a. Como verificar se a instância foi inscrita no domínio

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

    b. Como verificar o status do daemon SSSD

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
 Main PID: 479 (sssd)
    Tasks: 4
   CGroup: /system.slice/sssd.service
           ##479 /usr/sbin/sssd -i --logger=files
           ##505 /usr/lib/sssd/sssd_be --domain example.com --uid 0 --gid 0 --
logger=files
           ##548 /usr/lib/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           ##549 /usr/lib/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11. Como permitir o acesso de um usuário via SSH e console

```
sudo realm permit join_account@example.com
```

Como permitir acesso a um grupo de domínios via SSH e console

```
sudo realm permit -g 'AWS Delegated Administrators'
```

Ou como permitir que todos os usuários acessem

```
sudo realm permit --all
```

12. Ajuste o serviço SSH para permitir autenticação de senha.

a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

13.13. Depois que a instância for reiniciada, conecte-se a ela com qualquer cliente SSH e adicione o grupo Administradores AWS Delegados à lista de sudoers executando as seguintes etapas:

a. Abra o arquivo sudoers com o seguinte comando:

```
sudo visudo
```

b. Adicione o seguinte ao final do arquivo sudoers e salve-o.

```
## Add the "Domain Admins" group from the awsad.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Certifique-se de que a instância do Ubuntu - 64 bits está atualizada.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Instale os pacotes do Ubuntu necessários na sua instância do Linux.

> **Note**
>
> Alguns desses pacotes já podem estar instalados.

Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração. Você geralmente pode deixar os campos nessas telas em branco.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Desabilite a resolução de DNS reverso e defina o realm padrão para o FQDN do domínio. Instâncias do Ubuntu devem ser capazes de fazer a resolução inversa no DNS para que um realm possa funcionar. Caso contrário, você precisa desabilitar DNS reverso no /etc/krb5.conf, como a seguir:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

O SaM AccountName para uma conta no domínio *example.com* que tem privilégios de associação de domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

7. Ajuste o serviço SSH para permitir autenticação de senha.

   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

8. Depois que a instância for reiniciada, conecte-se a ela com qualquer cliente SSH e adicione o grupo Administradores AWS Delegados à lista de sudoers executando as seguintes etapas:

a. Abra o arquivo `sudoers` com o seguinte comando:

```
sudo visudo
```

b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

Restringir o acesso de login da conta

Como todas as contas estão definidas no Active Directory, por padrão, todos os usuários no diretório podem fazer login na instância. Você pode permitir que somente usuários específicos façam login na instância com ad_access_filter em sssd.conf. Por exemplo: .

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica que os usuários só podem ter acesso à instância se participarem de um grupo específico.

cn

O nome comum do grupo que deve ter acesso. Neste exemplo, o nome do grupo é *admins*.

ou

Essa é a unidade organizacional na qual o grupo acima está localizado. Neste exemplo, a UO é *Testou*.

dc

Este é o componente de domínio do seu domínio. Neste exemplo, *example*.

dc

Este é um componente adicional de domínio. Neste exemplo, *com*.

Você deve adicionar manualmente ad_access_filter ao /etc/sssd/sssd.conf.

Abra o arquivo /etc/sssd/sssd.conf em um editor de textos.

```
sudo vi /etc/sssd/sssd.conf
```

Depois disso, seu sssd.conf pode ficar da seguinte forma:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Para que a configuração entre em vigor, é necessário reiniciar o serviço sssd:

```
sudo systemctl restart sssd.service
```

Você também poderia usar o:

```
sudo service sssd restart
```

Como todas as contas estão definidas no Active Directory, por padrão, todos os usuários no diretório podem fazer login na instância. Você pode permitir que somente usuários específicos façam login na instância com ad_access_filter em sssd.conf.

Por exemplo: .

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica que os usuários só podem ter acesso à instância se participarem de um grupo específico.

cn

O nome comum do grupo que deve ter acesso. Neste exemplo, o nome do grupo é *admins*.

ou

Essa é a unidade organizacional na qual o grupo acima está localizado. Neste exemplo, a UO é *Testou*.

dc

Este é o componente de domínio do seu domínio. Neste exemplo, *example*.

dc

Este é um componente adicional de domínio. Neste exemplo, *com*.

Você deve adicionar manualmente ad_access_filter ao /etc/sssd/sssd.conf.

1. Abra o arquivo /etc/sssd/sssd.conf em um editor de textos.

   ```
   sudo vi /etc/sssd/sssd.conf
   ```

2. Depois disso, seu sssd.conf pode ficar da seguinte forma:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. Para que a configuração entre em vigor, é necessário reiniciar o serviço sssd:

```
sudo systemctl restart sssd.service
```

   Você também poderia usar o:

```
sudo service sssd restart
```

Mapeamento de ID

O mapeamento de ID pode ser realizado por dois métodos para manter uma experiência unificada entre as identidades Unix/Linux User Identifier (UID) e Group Identifier (GID) e Windows e Active Directory Security Identifier (SID).

1. Centralizado
2. Distribuído

> **Note**
>
> O mapeamento centralizado da identidade do usuário Active Directory requer uma interface de sistema operacional portátil ou POSIX.

Mapeamento centralizado da identidade do usuário

Active Directoryou outro serviço do Lightweight Directory Access Protocol (LDAP) fornece UID e GID aos usuários do Linux. EmActive Directory, esses identificadores são armazenados nos atributos dos usuários:

- UID - O nome de usuário do Linux (String)
- Número UID - O número de ID do usuário Linux (inteiro)
- Número GID - O número de ID do grupo Linux (inteiro)

Para configurar uma instância Linux para usar o UID e o GID deActive Directory, defina `ldap_id_mapping = False` no arquivo sssd.conf. Antes de definir esse valor, verifique se você adicionou um UID, um número UID e um número GID aos usuários e grupos em. Active Directory

Mapeamento distribuído de identidade de usuário

Se Active Directory não tiver a extensão POSIX ou se você optar por não gerenciar centralmente o mapeamento de identidade, o Linux poderá calcular os valores de UID e GID. O Linux usa o Identificador de Segurança (SID) exclusivo do usuário para manter a consistência.

Para configurar o mapeamento distribuído de ID de usuário, defina `ldap_id_mapping = True` no arquivo sssd.conf.

Conecte-se à instância Linux

Quando um usuário se conectar à instância usando um cliente SSH, será solicitado seu nome de usuário. O usuário pode informar o nome de usuário no formato `username@example.com` ou `EXAMPLE\username`. A resposta será semelhante à seguinte, dependendo da distribuição Linux que você estiver usando:

Amazon Linux, Red Hat Enterprise Linux e CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
```

```
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Associe manualmente uma instância Linux do Amazon EC2 ao seu AWS Microsoft AD Active Directory gerenciado usando o Winbind

Você pode usar o serviço Winbind para unir manualmente suas instâncias Linux do Amazon EC2 a um domínio AWS gerenciado do Microsoft AD Active Directory. Isso permite que seus usuários locais existentes do Active Directory usem suas credenciais do Active Directory ao acessar as instâncias Linux associadas ao seu AWS Microsoft AD Active Directory gerenciado. As seguintes distribuições e versões de instância do Linux são suportadas:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI do Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Outras distribuições e versões do Linux podem funcionar, mas não foram testadas.

Associe uma instância Linux ao seu Microsoft AD Active Directory AWS gerenciado

> **Important**
>
> Alguns dos procedimentos a seguir, se não forem executados corretamente, podem tornar sua instância inacessível ou não utilizável. Portanto, nós sugerimos enfaticamente que você faça um backup ou tire um snapshot da sua instância antes de executar esses procedimentos.

Para associar uma instância do Linux ao seu diretório

Siga as etapas para a sua instância do Linux específica usando uma das seguintes guias:

Amazon Linux/CENTOS/REDHAT

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância do Linux para usar os endereços IP dos servidores de DNS fornecidos pelo AWS Directory Service. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.

3. Verifique se sua instância do Linux está atualizada.

```
sudo yum -y update
```

4. Instale os pacotes do Samba/Winbind necessários na sua instância do Linux.

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-
clients
```

5. Faça um backup do arquivo `smb.conf` principal para que você possa voltar a ele em caso de falha:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Abra o arquivo de configuração original [`/etc/samba/smb.conf`] em um editor de texto.

```
sudo vim /etc/samba/smb.conf
```

   Preencha as informações do ambiente de domínio do Active Directory conforme mostrado no exemplo abaixo:

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Abra o arquivo de hosts [`/etc/hosts`]em um editor de texto.

```
sudo vim /etc/hosts
```

   Adicione o endereço IP privado da sua instância Linux da seguinte forma:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Se você não especificou seu endereço IP no arquivo `/etc/hosts`, talvez receba o seguinte erro de DNS ao associar a instância ao domínio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Esse erro significa que a associação foi bem-sucedida, mas o comando [net ads] não conseguiu registrar o registro de DNS no DNS.

8. Associe a instância do Linux ao Active Directory usando o utilitário net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Uma conta no domínio *example.com* com privilégios de associação a domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifique o arquivo de configuração do PAM. Use o comando abaixo para adicionar as entradas necessárias para a autenticação winbind:

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10. Configure o serviço de SSH para permitir autenticação de senha editando o arquivo `/etc/ssh/sshd_config`.

    a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

11 Após a instância reiniciar, conecte-a com qualquer cliente SSH e adicione os privilégios de usuário raiz para um usuário ou grupo do domínio à lista de sudoers executando as seguintes etapas:

a. Abra o arquivo `sudoers` com o seguinte comando:

```
sudo visudo
```

b. Adicione os grupos ou usuários necessários do seu domínio confiante ou confiável conforme descrito a seguir e salve-os.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

SUSE

1. Conecte-se à instância usando qualquer cliente SSH.

2. Configure a instância do Linux para usar os endereços IP dos servidores de DNS fornecidos pelo AWS Directory Service. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Verifique se sua instância do SUSE Linux 15 está atualizada.
   a. Conecte o repositório de pacotes.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Atualize o SUSE.

   ```
   sudo zypper update -y
   ```

4. Instale os pacotes do Samba/Winbind necessários na sua instância do Linux.

   ```
   sudo zypper in -y samba samba-winbind
   ```

5. Faça um backup do arquivo `smb.conf` principal para que você possa voltar a ele em caso de falha:

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. Abra o arquivo de configuração original [`/etc/samba/smb.conf`] em um editor de texto.

   ```
   sudo vim /etc/samba/smb.conf
   ```

   Preencha as informações do ambiente de domínio do Active Directory conforme mostrado no exemplo abaixo:

   ```
   [global]
    workgroup = example
    security = ads
    realm = example.com
    idmap config * : rangesize = 1000000
    idmap config * : range = 1000000-19999999
    idmap config * : backend = autorid
    winbind enum users = no
    winbind enum groups = no
   ```

```
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Abra o arquivo de hosts [`/etc/hosts`]em um editor de texto.

```
sudo vim /etc/hosts
```

Adicione o endereço IP privado da sua instância Linux da seguinte forma:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Se você não especificou seu endereço IP no arquivo `/etc/hosts`, talvez receba o seguinte erro de DNS ao associar a instância ao domínio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Esse erro significa que a associação foi bem-sucedida, mas o comando [net ads] não conseguiu registrar o registro de DNS no DNS.

8. Associe a instância do Linux ao diretório com o comando a seguir.

```
sudo net ads join -U join_account@example.com
```

join_account

O SaM AccountName no domínio *example.com* que tem privilégios de associação de domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome do DNS totalmente qualificado do seu diretório.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifique o arquivo de configuração do PAM. Use o comando abaixo para adicionar as entradas necessárias para a autenticação Winbind:

```
sudo pam-config --add --winbind --mkhomedir
```

10. Abra o arquivo de configuração do Name Service Switch [`/etc/nsswitch.conf`] em um editor de texto.

```
vim /etc/nsswitch.conf
```

Adicione a diretiva Winbind conforme mostrado abaixo.

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11. Configure o serviço de SSH para permitir autenticação de senha editando o arquivo `/etc/ssh/sshd_config`.

a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vim /etc/ssh/sshd_config
```

b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

12. Após a instância reiniciar, conecte-a com qualquer cliente SSH e adicione privilégios de usuário raiz para um usuário ou grupo do domínio à lista de sudoers executando as seguintes etapas:

a. Abra o arquivo `sudoers` com o seguinte comando:

```
sudo visudo
```

b. Adicione os grupos ou usuários necessários do seu domínio confiante ou confiável conforme descrito a seguir e salve-os.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

Ubuntu

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância do Linux para usar os endereços IP dos servidores de DNS fornecidos pelo AWS Directory Service. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se você quiser configurá-lo manualmente, consulte Como atribuo um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimento para obter orientação sobre como configurar AWS o servidor DNS persistente para sua distribuição e versão específicas do Linux.
3. Verifique se sua instância do Linux está atualizada.

```
sudo yum -y update
```

```
sudo apt-get -y upgrade
```

4. Instale os pacotes do Samba/Winbind necessários na sua instância do Linux.

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. Faça um backup do arquivo `smb.conf` principal para que você possa voltar a ele em caso de falha.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Abra o arquivo de configuração original [`/etc/samba/smb.conf`] em um editor de texto.

```
sudo vim /etc/samba/smb.conf
```

Preencha as informações do ambiente de domínio do Active Directory conforme mostrado no exemplo abaixo:

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Abra o arquivo de hosts [`/etc/hosts`]em um editor de texto.

```
sudo vim /etc/hosts
```

Adicione o endereço IP privado da sua instância Linux da seguinte forma:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Se você não especificou seu endereço IP no arquivo `/etc/hosts`, talvez receba o seguinte erro de DNS ao associar a instância ao domínio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Esse erro significa que a associação foi bem-sucedida, mas o comando [net ads] não conseguiu registrar o registro de DNS no DNS.

8. Associe a instância do Linux ao Active Directory usando o utilitário net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Uma conta no domínio *example.com* com privilégios de associação a domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifique o arquivo de configuração do PAM. Use o comando abaixo para adicionar as entradas necessárias para a autenticação Winbind:

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Abra o arquivo de configuração do Name Service Switch [`/etc/nsswitch.conf`] em um editor de texto.

```
vim /etc/nsswitch.conf
```

Adicione a diretiva Winbind conforme mostrado abaixo.

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. Configure o serviço de SSH para permitir autenticação de senha editando o arquivo `/etc/ssh/sshd_config`.

a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vim /etc/ssh/sshd_config
```

b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

12 Após a instância reiniciar, conecte-a com qualquer cliente SSH e adicione privilégios de usuário raiz para um usuário ou grupo do domínio à lista de sudoers executando as seguintes etapas:

a. Abra o arquivo `sudoers` com o seguinte comando:

```
sudo visudo
```

b. Adicione os grupos ou usuários necessários do seu domínio confiante ou confiável conforme descrito a seguir e salve-os.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

Conecte-se à instância Linux

Quando um usuário se conectar à instância usando um cliente SSH, será solicitado seu nome de usuário. O usuário pode informar o nome de usuário no formato `username@example.com` ou `EXAMPLE\username`. A resposta será semelhante à seguinte, dependendo da distribuição Linux que você estiver usando:

Amazon Linux, Red Hat Enterprise Linux e CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Associe manualmente uma instância Mac do Amazon EC2 ao seu AWS Microsoft AD Active Directory gerenciado

Esse procedimento une manualmente uma instância Mac do Amazon EC2 ao seu Microsoft AD Active AWS Directory gerenciado.

Pré-requisitos

- As instâncias Mac do Amazon EC2 exigem hosts dedicados do Amazon EC2. Você deve alocar um host dedicado e executar uma instância no host. Para obter mais informações, consulte Iniciar uma instância Mac no Guia do usuário do Amazon EC2.
- Recomendamos criar um conjunto de opções DHCP para seu Microsoft AD Active Directory AWS gerenciado. Isso permitirá que qualquer instância em sua Amazon VPC aponte para o domínio especificado e servidores DNS para resolver seus nomes de domínio. Consulte Criar ou alterar um conjunto de opções de DHCP Para mais informações.

> **Note**
>
> O preço do Host dedicado varia de acordo com a opção de pagamento que você seleciona. Para obter mais informações, consulte Preços e cobrança no Guia do usuário do Amazon EC2.

Para ingressar manualmente em uma instância do Mac

1. Use o comando SSH a seguir para se conectar à sua instância Mac. Para obter mais informações sobre como se conectar à sua instância Mac, consulte Conectar à sua instância Mac.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
   ```

2. Depois de se conectar à sua instância Mac, crie uma senha para a conta *ec2-user* usando o seguinte comando:

   ```
   sudo passwd ec2-user
   ```

3. Quando solicitado na linha de comando, forneça uma senha para a conta *ec2-user*. Você pode atualizar seu sistema operacional e software seguindo o procedimento em Atualizar o sistema operacional e o software no Guia do usuário do Amazon EC2.
4. Use o comando *dsconfigad* a seguir para unir sua instância Mac ao domínio gerenciado do AWS Microsoft AD Active Directory. Certifique-se de substituir o nome do domínio, o nome do computador e a unidade organizacional pelas informações de domínio AWS gerenciado do

Microsoft AD Active Directory. Para obter mais informações, consulte Configurando o acesso ao domínio no Utilitário de Diretório no Mac no site da Apple.

> **Warning**
>
> O nome do computador não deve conter um hífen. Os hífens podem impedir a associação ao AWS Microsoft AD Active Directory gerenciado.

```
sudo dsconfigad -add domainName -computer computerName -username Username -
ou "Your-AWS-Delegated-Organizational-Unit"
```

O exemplo a seguir mostra a aparência do comando ao unir um usuário administrativo em uma instância do Mac nomeada **myec2mac01** para o **example.com** domínio:

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. Use o comando a seguir para adicionar os administradores AWS delegados ao usuário administrativo na sua instância Mac:

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators
```

6. Use o comando a seguir para confirmar que a adesão ao domínio AWS gerenciado do Microsoft AD Active Directory foi bem-sucedida:

```
dsconfigad -show
```

Você uniu com sucesso sua instância Mac ao seu Microsoft AD Active Directory AWS gerenciado. Agora você pode fazer login na sua instância Mac usando suas credenciais AWS gerenciadas do Microsoft AD Active Directory.

Ao fazer login pela primeira vez na sua instância Mac, você deve ter a opção de fazer login como o usuário “Outro”. Nesse ponto, você pode usar suas credenciais de domínio do Active Directory para fazer login na instância do Mac. Se você não receber “Outro” na tela de login após concluir essas etapas, faça login como ec2-user e depois saia.

Para fazer login usando a interface gráfica do usuário com um usuário de domínio, siga as etapas em Conecte-se à interface gráfica do usuário (GUI) da sua instância no Guia do usuário do Amazon EC2.

Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD

Para fazer com que um computador passe a integrar seu diretório, você precisa de uma conta com privilégios para integrar computadores ao diretório.

Com o AWS Directory Service for Microsoft Active Directory, os membros dos grupos Admins e AWS Delegated Server Administrators têm esses privilégios.

No entanto, a prática recomendada é que você deve usar uma conta que tenha apenas os privilégios mínimos necessários. O procedimento a seguir demonstra como criar um novo grupo chamado `Joiners` e delegar a ele os privilégios necessários para integrar computadores ao diretório.

Execute este procedimento em um computador que esteja integrado ao seu diretório e possua o snap-in do MMC Usuário e Computadores do Active Directory) instalado. Você também deve estar conectado como administrador de domínio.

Para delegar privilégios de associação para o Managed AWS Microsoft AD

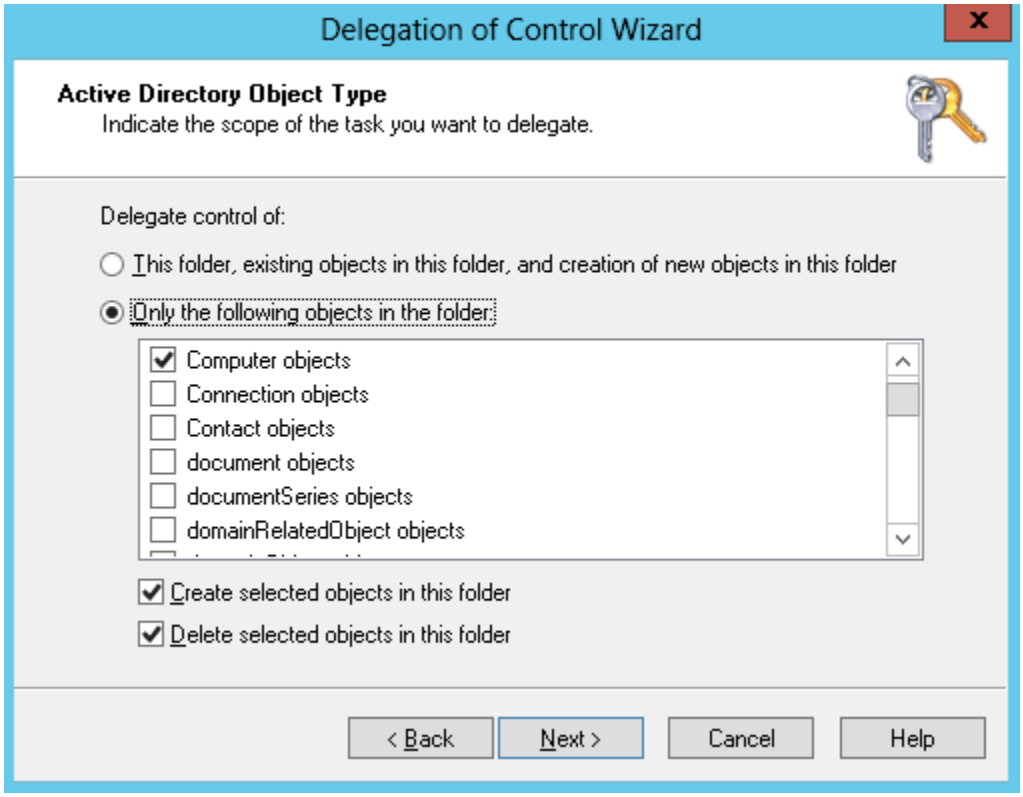
1. Abra Usuários e computadores do Active Directory e selecione a unidade organizacional (UO) que tem o nome do seu NetBIOS na árvore de navegação. Em seguida, selecione a UO Users.

   > **Important**
   >
   > Quando você inicia um AWS Directory Service para o Microsoft Active Directory, AWS cria uma unidade organizacional (OU) que contém todos os objetos do seu diretório. Essa OU, que tem o nome de NetBIOS que você digitou quando criou seu diretório, está localizada na raiz do domínio. A raiz do domínio pertence e é gerenciada por AWS. Você não pode fazer alterações na raiz do domínio, portanto, crie um grupo **`Joiners`** na UO com o nome de seu NetBIOS.

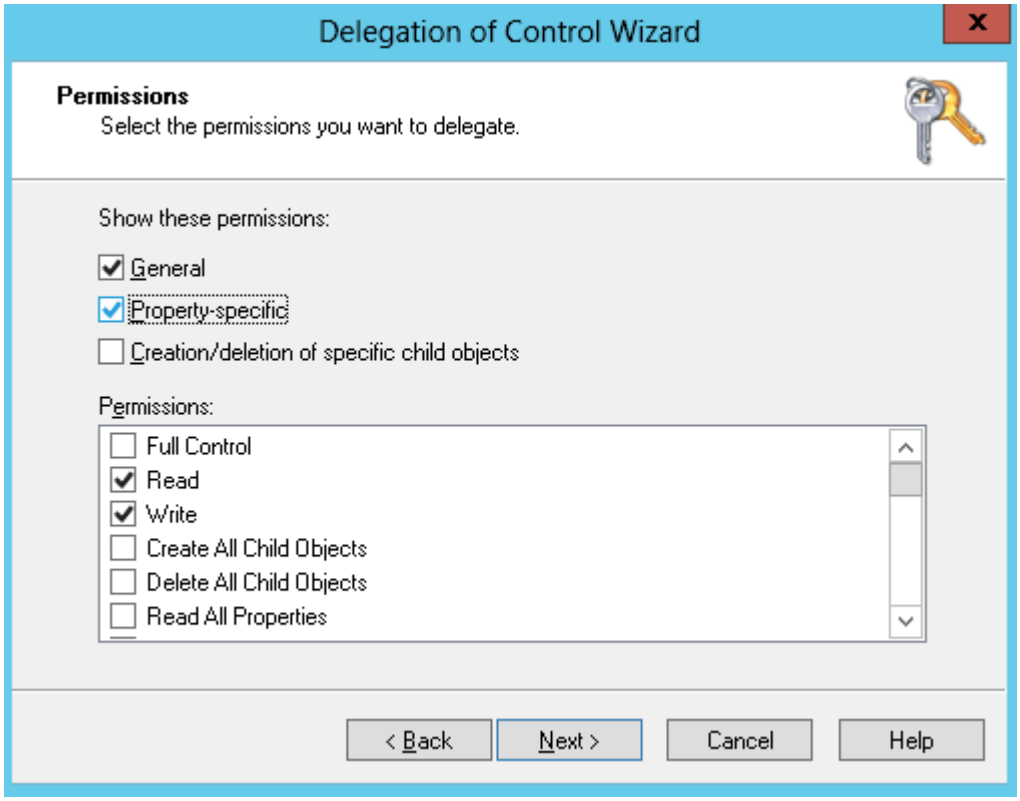
2. Abra o menu de contexto (clique com o botão direito) para Users, escolha New e escolha Group.
3. Na caixa New Object - Group, digite o seguinte, e escolha OK.
   - Em Group name (Nome do grupo), digite **`Joiners`**.
   - Em Group scope, escolha Global.

- Em Group type, escolha Security.

4. Na árvore de navegação, selecione o contêiner Computers (Computadores) sob o nome do seu NetBIOS. No menu Action, escolha Delegate Control.
5. Na página Delegation of Control Wizard, escolha Next e escolha Add.
6. Na caixa Select Users, Computers, or Groups (Selecionar usuários, computadores ou grupos), digite `Joiners` e escolha OK. Se mais de um objeto for encontrado, selecione o grupo `Joiners` criado acima. Escolha Próximo.
7. Na página Tasks to Delegate, selecione Create a custom task to delegate e escolha Next.
8. Selecione Only the following objects in the folder e selecione Computer objects.
9. Selecione Create selected objects in this folder e Delete selected objects in this folder. Em seguida, escolha Próximo.



10. Selecione Read e Write e escolha Next.



11. Verifique as informações da página Completing the Delegation of Control Wizard e escolha Finish.
12. Crie um usuário com uma senha forte e adicione-o ao grupo `Joiners`. Este usuário deve estar no contêiner Users que está sob o nome do seu NetBIOS. O usuário agora terá privilégios suficientes para conectar instâncias ao diretório.

Criar ou alterar um conjunto de opções de DHCP

AWS recomenda que você crie um conjunto de opções de DHCP para seu AWS Directory Service diretório e atribua o conjunto de opções de DHCP à VPC em que seu diretório está. Dessa maneira, todas as instâncias nessa VPC podem apontar para o domínio especificado e os servidores DNS para resolver seus nomes de domínio.

Para obter mais informações sobre os conjuntos de opções de DHCP, consulte Conjuntos de opções de DHCP no Guia do usuário do Amazon VPC.

Para criar um conjunto de opções de DHCP para o seu diretório

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, selecione Conjuntos de opções DHCP e, então, selecione Criar conjuntos de opções DHCP.
3. Na página Criar conjunto de opções de DHCP, forneça os seguintes valores para o seu diretório:

   Nome

   Um tag opcional para o conjunto de opções.

   Domain name

   O nome totalmente qualificado do diretório, como `corp.example.com`.

   Servidores de nomes de domínio

   Os endereços IP dos AWS servidores DNS do seu diretório fornecido.

   > **Note**
   >
   > Para encontrar esses endereços, vá para o painel de navegação do console do AWS Directory Service, selecione Diretórios e escolha o ID do diretório correto.

   Servidores NTP

   Deixe esse campo em branco.

   Servidores de nomes NetBIOS

   Deixe esse campo em branco.

   Tipo de nó NetBIOS

   Deixe esse campo em branco.
4. Escolha Create DHCP Options set. O novo conjunto de opções DHCP aparece na sua lista de opções DHCP.
5. Anote o ID do novo conjunto de opções DHCP (dopt-*xxxxxxxx*). Você precisará usá-lo para associar o novo conjunto de opções à sua VPC.

Para alterar o conjunto de opções DHCP associado a uma VPC

Depois de criar um conjunto de opções DHCP, você não pode modificá-las. Se você quiser que sua VPC use um conjunto diferente de opções DHCP, será necessário criar um novo conjunto e associá-lo a sua VPC. Você também pode configurar sua VPC para não usar nenhuma opção DHCP.

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione a VPC e, em seguida, escolha Ações, Editar configurações de VPC.
4. Em Conjunto de opções DHCP, selecione um conjunto de opções ou escolha Nenhum conjunto de opções de DHCP e escolha Salvar.

Para alterar o conjunto de opções DHCP associado a uma VPC usando a linha de comando, consulte o seguinte:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Gerenciar usuários e grupos no AWS Microsoft Managed AD

Os usuários representam pessoas ou entidades individuais que têm acesso ao seu diretório. Os grupos são muito úteis para conceder ou negar privilégios a grupos de usuários, em vez de ter que aplicar esses privilégios a cada usuário individual. Se um usuário for transferido para uma organização diferente, transfira-o para um grupo diferente e ele receberá os privilégios necessários para a nova organização automaticamente.

Para criar usuários e grupos em um diretório do AWS Directory Service, é necessário usar qualquer instância (on-premises ou EC2) que tenha sido associada a seu diretório do AWS Directory Service e esteja conectada como um usuário com privilégios de criação de usuários e grupos. Você também precisará instalar ferramentas do Active Directory em sua instância do EC2 para que possa adicionar seus usuários e grupos com o snap-in Usuários e Computadores do Active Directory.

Você pode implantar uma instância do EC2 pré-configurada com ferramentas administrativas do Active Directory pré-instaladas usando o console de gerenciamento do AWS Directory Service. Para obter mais informações, consulte Inicie a instância de administração de diretórios em seu Microsoft AD AWS gerenciado Active Directory.

Se você precisar implantar uma instância do EC2 autogerenciada com ferramentas administrativas e instalar as ferramentas necessárias, consulte Etapa 3: Implantar uma instância do Amazon EC2 para gerenciar seu AWS Microsoft AD Active Directory gerenciado.

> **Note**
>
> Suas contas de usuário devem ter a pré-autenticação Kerberos habilitada. Essa é a configuração padrão para contas de usuário novas, mas ela não deve ser modificada. Para obter mais informações sobre essa configuração, vá para Preauthentication no Microsoft TechNet.

Os tópicos a seguir incluem instruções sobre como criar e gerenciar usuários e grupos.

Tópicos

- Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado
- Criar um usuário
- Excluir um usuário
- Redefinir uma senha de usuário
- Criar um grupo
- Adicionar um usuário a um grupo

Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado

Para gerenciar seu Active Directory a partir de uma instância Windows Server do Amazon EC2, você precisa instalar o Active Directory Domain Services and Active Directory Lightweight Directory Services Tools na instância. Use o procedimento a seguir para instalar essas ferramentas em uma instância EC2 do Windows Server.

Pré-requisitos

Antes de começar esse procedimento, faça o seguinte:

1. Crie um Microsoft AD AWS gerenciadoActive Directory. Para ter mais informações, consulte Crie seu Microsoft AD AWS gerenciado.

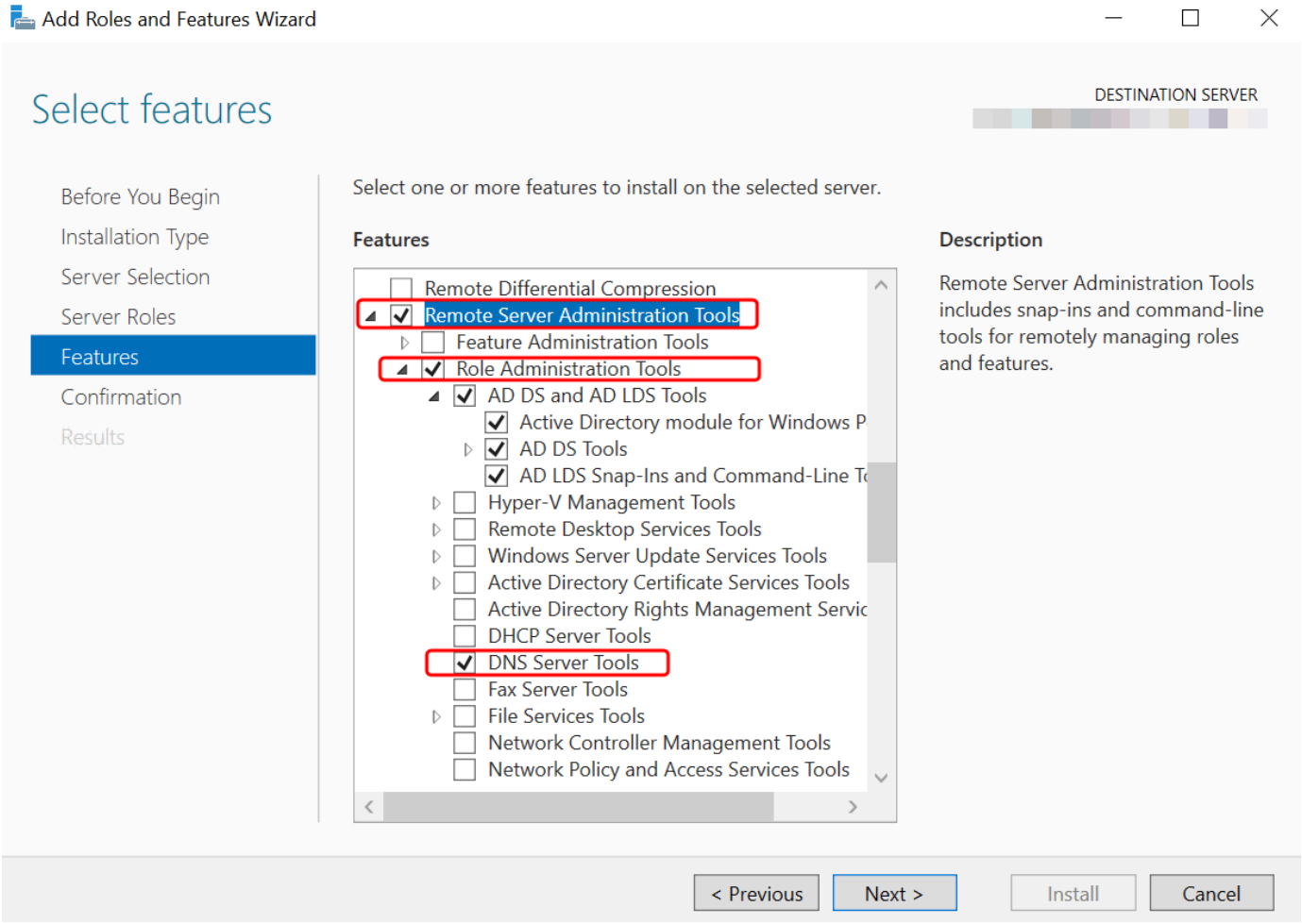
2. Inicie e associe uma instância do EC2 Windows Server ao seu Microsoft AD Active Directory AWS gerenciado. A instância EC2 precisa das seguintes políticas para criar usuários e grupos: **`AWSSSMManagedInstanceCore`** e. **`AmazonSSMDirectoryServiceAccess`** Para obter mais informações, consulte Inicie a instância de administração de diretórios em seu Microsoft AD AWS gerenciado Active Directory e Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory.
3. Você precisará das credenciais do administrador do seu Active Directory domínio. Essas credenciais foram criadas quando o AWS Managed Microsoft AD foi criado. Se você seguiu o procedimento emCrie seu Microsoft AD AWS gerenciado, seu nome de usuário de administrador inclui seu nome NetBIOS,. **`corp\admin`**

Instale as Ferramentas de Administração do Active Directory na instância EC2 do Windows Server

Para instalar as ferramentas de administração do Active Directory na instância do EC2 Windows Server

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No console do Amazon EC2, escolha Instâncias, selecione a instância do Windows Server e escolha Conectar.
3. Na página Conectar a instância, escolha Cliente RDP.
4. Na guia Cliente RDP, escolha Baixar arquivo de área de trabalho remota e escolha Obter senha para recuperar sua senha.
5. Em Obter senha do Windows, escolha Fazer upload de arquivo de chave privada. Escolha o arquivo de chave privada .pem associado à instância do Windows Server. Depois de fazer upload do arquivo de chave privada, selecione Descriptografar senha.
6. Na caixa de diálogo Segurança do Windows, copie suas credenciais de administrador local para o computador Windows Server entrar. O nome de usuário pode estar nos seguintes formatos: ***`NetBIOS-Name`*`\admin`** ou***`DNS-Name`*`\admin`**. Por exemplo, **`corp\admin`** seria o nome de usuário se você seguisse o procedimento emCrie seu Microsoft AD AWS gerenciado.
7. Depois de entrar na instância do Windows Server, abra o Gerenciador do Servidor no menu Iniciar, escolhendo Gerenciador do Servidor.
8. No Painel do Gerenciador do Servidor, escolha Adicionar funções e recursos.
9. No Add Roles and Features Wizard (Adicionar assistente de funções e recursos), selecione Installation Type (Tipo de instalação), selecione Role-based or feature-based installation (Instalação baseada em função ou em recurso) e, em seguida, Next (Avançar).

10. Em Server Selection (Seleção de servidor), verifique se o servidor local está selecionado e escolha Features (Recursos) no painel de navegação esquerdo.
11. Na árvore Recursos, abra Ferramentas de administração do servidor remoto, Ferramentas de administração de funções e Ferramentas de AD DS e AD LDS. Com as Ferramentas AD DS e AD LDS selecionadas, o Active Directorymódulo para Windows PowerShell, Ferramentas AD DS e Snap-ins e Ferramentas de Linha de Comando do AD LDS são selecionados. Role para baixo e selecione Ferramentas de servidor de DNS e escolha Próximo.



12. Revise as informações e selecione Instalar. Quando a instalação do recurso for concluída, o Active Directory Domain Services e as Active Directory Lightweight Directory Services Tools estarão disponíveis no menu Iniciar na pasta Ferramentas administrativas.

Métodos alternativos para instalar as ferramentas de administração do Active Directory na instância do EC2 Windows Server

- Aqui estão alguns outros métodos para instalar as Ferramentas de Administração do Active Directory:
  - Opcionalmente, você pode optar por instalar as Ferramentas de Administração do Active Directory usandoWindows PowerShell. Por exemplo, você pode instalar as ferramentas de administração remota do Active Directory a partir de um PowerShell prompt usando`Install-WindowsFeature RSAT-ADDS`. Para obter mais informações, consulte Instalar-WindowsFeature no site da Microsoft.
  - Você também pode iniciar uma instância EC2 de administração de diretórios na AWS Management Console que já tenha as ferramentas Active Directory Domain Services e Active Directory Lightweight Directory Services instaladas seguindo os procedimentos emInicie a instância de administração de diretórios em seu Microsoft AD AWS gerenciado Active Directory.

Criar um usuário

Use o procedimento a seguir para criar um usuário com uma instância do EC2 associada ao seu diretório do AWS Microsoft Managed AD. Antes de criar usuários, é necessário concluir os procedimentos em Instalar as ferramentas de administração do Active Directory.

Você pode usar qualquer um dos métodos a seguir para criar um usuário:

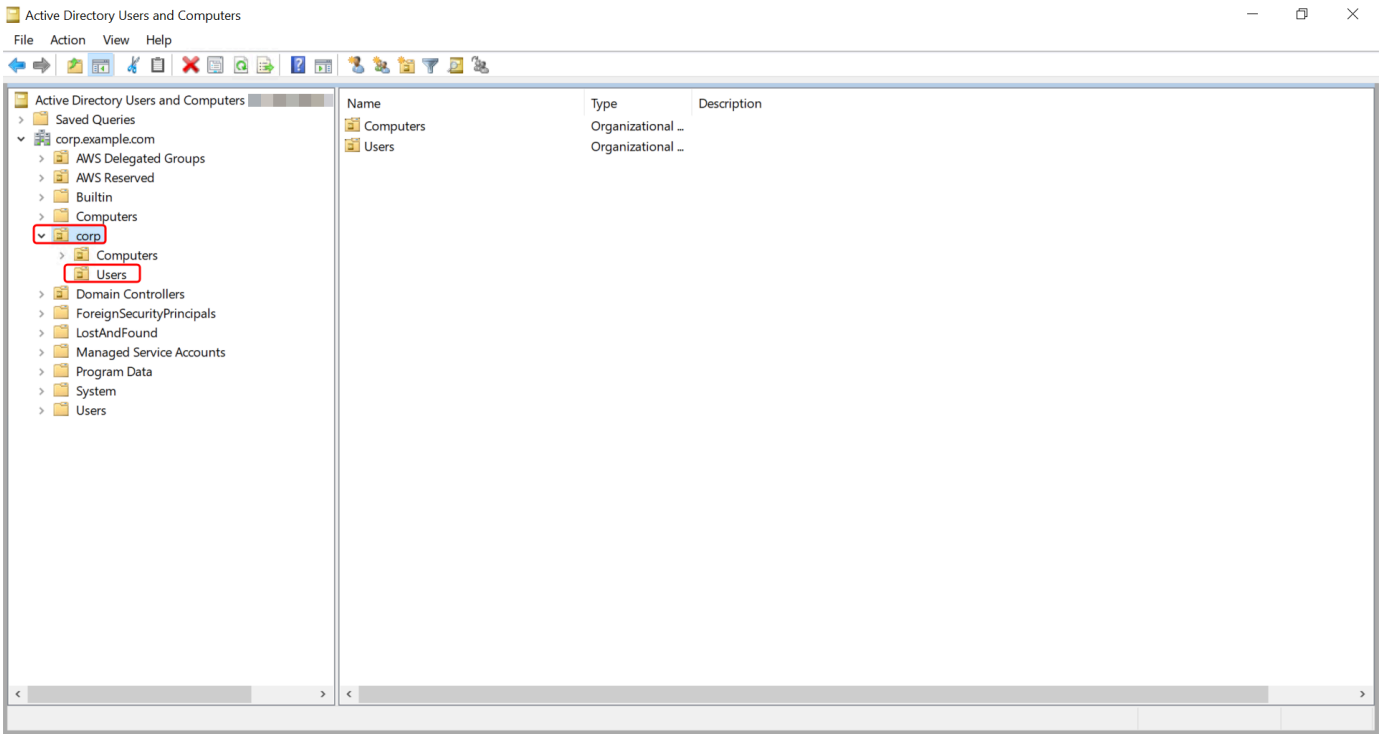
- Active DirectoryFerramentas de administração
- Windows PowerShell

Crie um usuário com as Ferramentas Active Directory Administrativas

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.
2. Abra a ferramenta Usuários e Computadores do Active Directory no menu Iniciar do Windows. Há um atalho para essa ferramenta encontrado na pasta Ferramentas Administrativas do Windows.

> **Tip**
>
> É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Na árvore de diretórios, selecione uma OU sob o nome NetBIOS do seu diretório ou onde você deseja armazenar seu usuário (por exemplo,**`corp\Users`**). Para obter mais informações sobre a estrutura de UO usada pelos diretórios em AWS, consulteO que é criado com seu Microsoft AD Active Directory AWS gerenciado.



4. No menu Ação, escolha Novo. Em seguida, clique em Usuário para abrir o assistente de novo usuário.
5. Na primeira página do assistente, insira os valores dos campos a seguir e escolha Próximo.
   - Nome
   - Sobrenome
   - Nome de logon do usuário

6. Na segunda página do assistente, insira uma senha temporária em Senha e em Confirmar senha. Certifique-se de que a opção O usuário deve alterar a senha no próximo login esteja selecionada. Nenhuma das outras opções deve ser selecionada. Escolha Próximo.
7. Na terceira página do assistente, verifique se as informações do novo usuário estão corretas e clique em Concluir. O novo usuário será exibido na pasta Usuários.

Crie um usuário em Windows PowerShell

1. Conecte-se à instância associada ao seu Active Directory domínio como Active Directory administrador.
2. Abra o Windows PowerShell.
3. Digite o comando a seguir substituindo o nome **`jane.doe`** de usuário pelo nome de usuário do usuário que você deseja criar. Você será solicitado Windows PowerShell a fornecer uma senha para o novo usuário. Para obter mais informações sobre os requisitos de complexidade de Active Directory senhas, consulte a Microsoftdocumentação. Para obter mais informações sobre o comando New-ADUser, consulte a documentação. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Excluir um usuário

Use o procedimento a seguir para excluir um usuário que está associado ao seu Microsoft AD AWS gerenciadoActive Directory.

Você pode usar qualquer um dos seguintes métodos para excluir um usuário:

- Active DirectoryFerramentas de administração
- Windows PowerShell

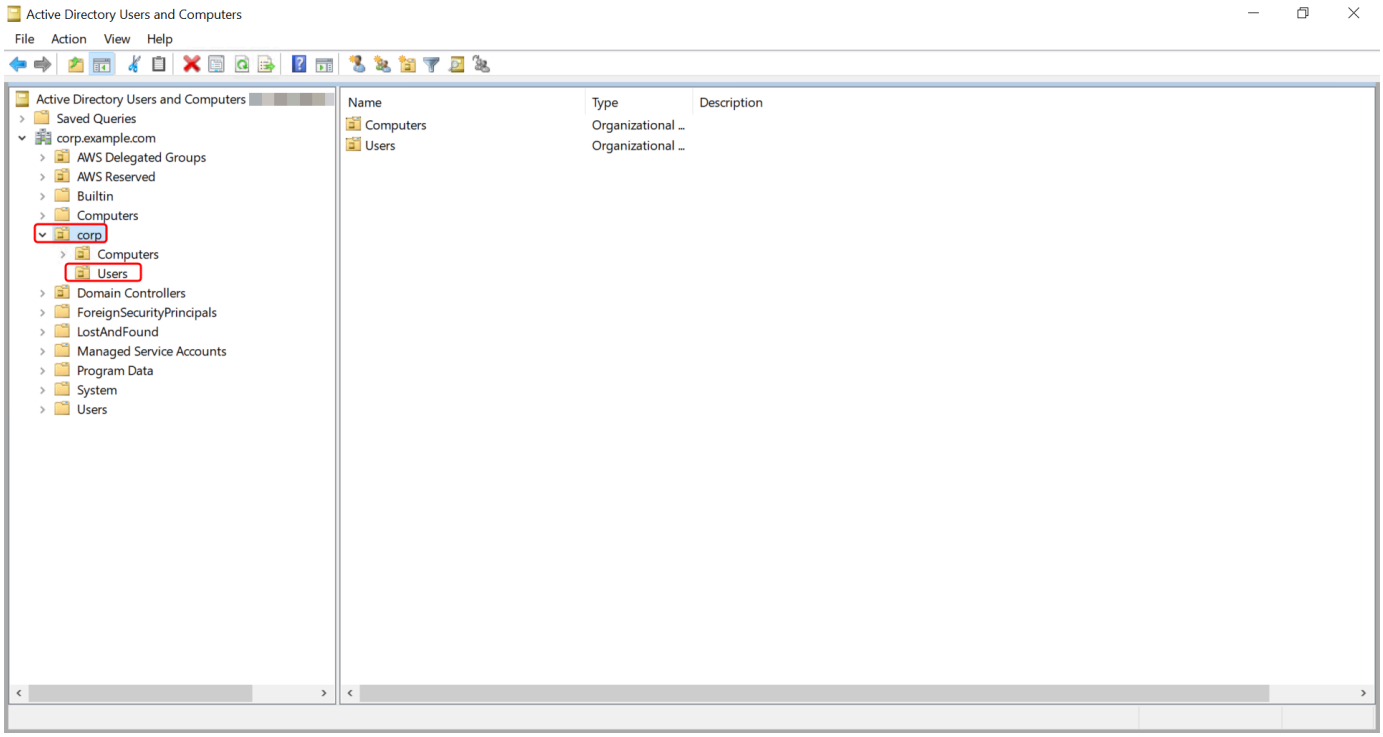
Excluir um usuário com as Ferramentas Active Directory Administrativas

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.

2. Abra a ferramenta Usuários e Computadores do Active Directory no menu Iniciar do Windows. Há um atalho para essa ferramenta encontrado na pasta Ferramentas Administrativas do Windows.

> **Tip**
>
> É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Na árvore de diretórios, selecione a OU que contém o usuário que você deseja excluir (por exemplo,**`corp\Users`**).



4. Selecione o usuário que deseja excluir. No menu Ação, escolha Excluir.

5. Uma caixa de diálogo aparecerá solicitando que você confirme que deseja excluir o usuário. Escolha Sim para excluir o usuário. Isso exclui permanentemente o usuário selecionado.

Excluir um usuário em Windows PowerShell

1. Conecte-se à instância associada ao seu Active Directory domínio como Active Directory administrador.
2. Abra o Windows PowerShell.
3. Digite o comando a seguir substituindo o nome **`jane.doe`** de usuário pelo nome de usuário do usuário que você deseja excluir. Para obter mais informações sobre o comando Remove-ADUser, consulte a documentação. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Considerações sobre a lixeira do AD

Os usuários excluídos são armazenados temporariamente na Lixeira do AD. Para obter mais informações sobre a lixeira do AD, consulte A lixeira do AD: entendendo, implementando, melhores práticas e solução de problemas no blog Pergunte à equipe Microsoft de serviços de diretório.

Redefinir uma senha de usuário

Os usuários devem seguir as políticas de senha, conforme definido noActive Directory. Às vezes, isso pode tirar o melhor proveito dos usuários, incluindo o Active Directory administrador, e eles esquecem a senha. Quando isso acontece, você pode redefinir rapidamente a senha do usuário usando AWS Directory Service se o usuário residir no AWS Managed Microsoft AD.

Você deve estar conectado como um usuário com as permissões necessárias para redefinir senhas. Para obter mais informações sobre permissões, consulte Visão geral do gerenciamento de permissões de acesso aos seus AWS Directory Service recursos.

Você pode redefinir a senha de qualquer usuário do seu, Active Directory com as seguintes exceções:

- Você pode redefinir a senha de qualquer usuário dentro da Unidade Organizacional (OU) baseada no nome NetBIOS que você usou ao criar seu. Active Directory Por exemplo, se você seguisse o procedimento em Crie seu Microsoft AD AWS gerenciado seu NetBIOS, o nome seria CORP e as senhas dos usuários que você poderia redefinir seriam membros da OU Corp/Users.
- Você não pode redefinir a senha de nenhum usuário fora da OU que seja baseada no nome NetBIOS que você usou quando criou o seu. Active Directory Por exemplo, você não pode redefinir

a senha de um usuário na UO AWS Reservada. Para obter mais informações sobre a estrutura de UO do Microsoft AD AWS gerenciado, consulteO que é criado com seu Microsoft AD Active Directory AWS gerenciado.

Para obter mais informações sobre como as políticas de senha são aplicadas quando uma senha é redefinida no AWS Managed Microsoft AD, consulteComo as políticas de senha são aplicadas.

Você pode usar qualquer um dos métodos a seguir para redefinir uma senha de usuário:

- AWS Management Console
- AWS CLI
- Windows PowerShell

Redefinir uma senha de usuário no AWS Management Console

1. No painel de navegação do AWS Directory Service console, em Active Directory, escolha Diretórios e selecione o Active Directory na lista em que você deseja redefinir uma senha de usuário.
2. Na página Detalhes do usuário, escolha Ações, Redefinir senha.
3. Na caixa de diálogo Redefinir senha do usuário, em Nome de usuário, digite o nome de usuário do usuário cuja senha precisa ser alterada.
4. Digite uma senha em Nova senha e Confirmar senha e escolha Redefinir senha.

Redefinir uma senha de usuário em AWS CLI

1. Para instalar o AWS CLI, consulte Instalar ou atualizar a versão mais recente do AWS CLI.
2. Abra AWS CLI o.
3. Digite o comando a seguir e substitua o ID do diretório, o nome de usuário **`jane.doe`** e a senha **`P@ssw0rd`** pelo ID Active Directory do diretório e pelas credenciais desejadas. Consulte reset-user-passworda Referência de AWS CLI Comandos para obter mais informações.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

Redefinir uma senha de usuário em Windows PowerShell

1. Conecte-se à instância associada ao seu Active Directory domínio como Active Directory administrador.
2. Abra o Windows PowerShell.
3. Digite o comando a seguir substituindo o nome de usuário**`jane.doe`**, o ID do diretório e a senha **`P@ssw0rd`** pelo ID Active Directory do diretório e pelas credenciais desejadas. Consulte Reset-DS UserPassword Cmdlet para obter mais informações.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Criar um grupo

Use o procedimento a seguir para criar um grupo de segurança com uma instância do EC2 associada ao seu diretório AWS gerenciado do Microsoft AD. Antes de criar grupos de segurança, é necessário concluir os procedimentos em Instalar as ferramentas de administração do Active Directory.

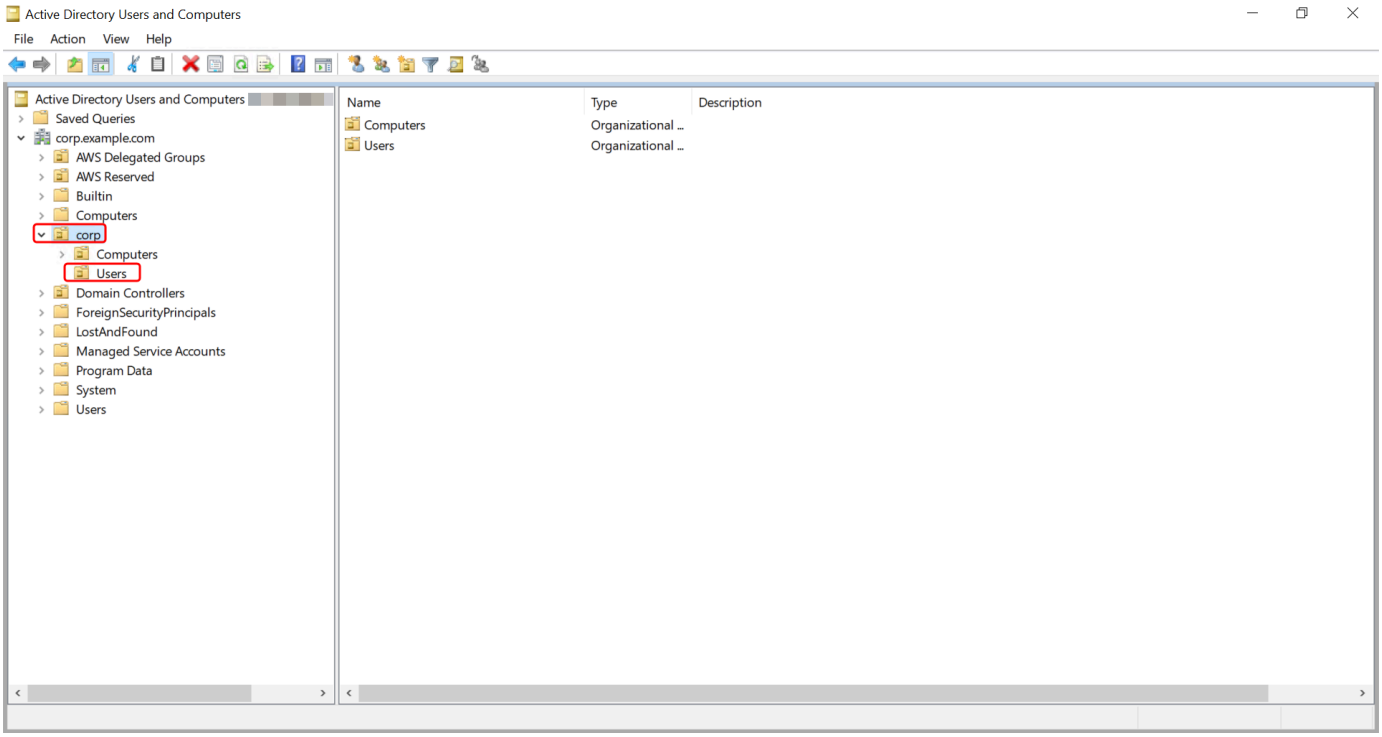
Você também pode usar Windows PowerShell comandos para criar grupos. Para obter mais informações, consulte New-AdGroup na documentação do Windows Server 2022. PowerShell

Para criar um grupo

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.
2. Abra a ferramenta Usuários e Computadores do Active Directory. Um atalho para essa ferramenta está disponível na pasta Ferramentas Administrativas.

> **Tip**
>
> É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Na árvore de diretórios, selecione uma UO sob a UO do nome NetBIOS do seu diretório em que você deseja armazenar o grupo (por exemplo, Corp\Users). Para obter mais informações sobre a estrutura de UO usada pelos diretórios em AWS, consulteO que é criado com seu Microsoft AD Active Directory AWS gerenciado.



4. No menu Ação, clique em Novo. Em seguida, clique em Grupo para abrir o assistente de novo grupo.
5. Digite um nome para o grupo em Nome do grupo, selecione um Escopo de grupo que atenda às suas necessidades e selecione Segurança para o Tipo de grupo. Para obter mais informações sobre o escopo do grupo e os grupos de segurança do Active Directory, consulte Grupos de segurança do Active Directory na documentação do Microsoft Windows Server.
6. Clique em OK. O novo grupo de segurança será exibido na pasta Usuários.

Adicionar um usuário a um grupo

Use o procedimento a seguir para adicionar um usuário a um grupo de segurança com uma instância do EC2 associada ao seu diretório do AWS Microsoft Managed AD.

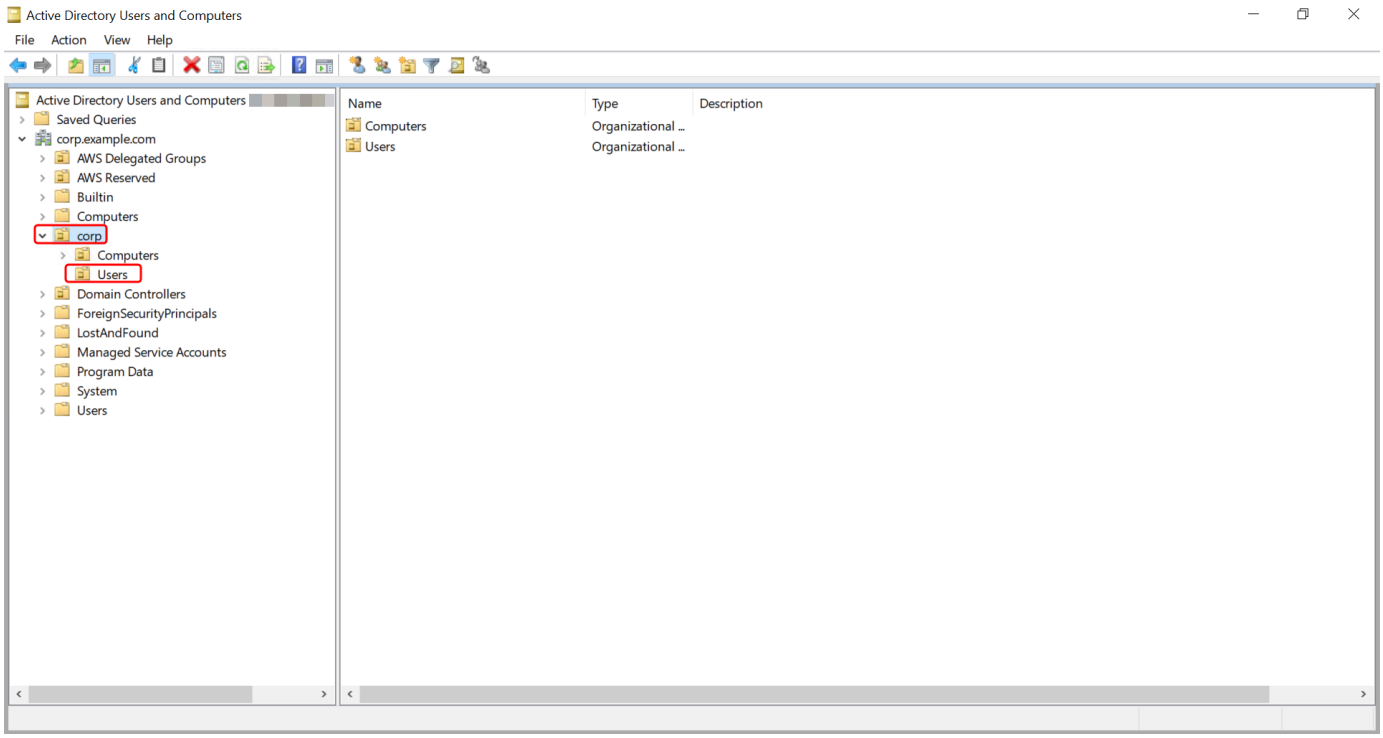
Como adicionar um usuário a um grupo

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.

2. Abra a ferramenta Usuários e Computadores do Active Directory. Um atalho para essa ferramenta está disponível na pasta Ferramentas Administrativas.

> **Tip**
>
> É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Na árvore de diretórios, selecione a UO sob a UO do nome NetBIOS do seu diretório em que você armazenou seu grupo e selecione o grupo ao qual deseja adicionar um usuário como membro.



4. No menu Ação, clique em Propriedades para abrir a caixa de diálogo de propriedades do grupo.
5. Selecione a guia Membros e clique em Adicionar.
6. Em Digite os nomes dos objetos a serem selecionados, digite o nome de usuário que você deseja adicionar e clique em OK. O nome será exibido na lista Membros. Clique em OK novamente para atualizar a associação ao grupo.
7. Verifique se o usuário agora é membro do grupo selecionando o usuário na pasta Usuários e clicando em Propriedades no menu Ação para abrir a caixa de diálogo de propriedades.

Selecione a guia Membro de. Você deverá ver o nome do grupo na lista de grupos aos quais o usuário pertence.

Conecte-se à sua infraestrutura existente do Active Directory

Esta seção descreve como configurar relações de confiança entre o Microsoft AD AWS gerenciado e sua infraestrutura existente do Active Directory.

Tópicos

- Criar uma relação de confiança
- Adicionar rotas IP ao usar endereços IP públicos
- Tutorial: criar uma relação de confiança entre o diretório do AWS Managed Microsoft AD e seu domínio autogerenciado do Active Directory .
- Tutorial: criar uma relação de confiança entre dois domínios do AWS Managed Microsoft AD

Criar uma relação de confiança

Você pode configurar relações de confiança externas e florestais unidirecionais e bidirecionais entre o AWS Directory Service for Microsoft Active Directory e os diretórios autogerenciados (locais), bem como entre vários diretórios gerenciados AWS do Microsoft AD na nuvem. AWS AWS O Microsoft AD gerenciado oferece suporte a todas as três direções de relacionamento de confiança: entrada, saída e bidirecional (bidirecional).

Para obter mais informações sobre relações de confiança, consulte Tudo o que você queria saber sobre relações de confiança com o Microsoft AD AWS gerenciado.

> **Note**
>
> Ao configurar relações de confiança, você deve garantir que seu diretório autogerenciado seja e permaneça compatível com AWS Directory Service s. Para obter mais informações sobre suas responsabilidades, consulte nosso modelo de responsabilidade compartilhada.

AWS O Microsoft AD gerenciado oferece suporte a relações de confiança externas e florestais. Para ver um cenário de exemplo que mostra como criar uma confiança de floresta, consulte Tutorial: criar uma relação de confiança entre o diretório do AWS Managed Microsoft AD e seu domínio autogerenciado do Active Directory ..

É necessária uma confiança bidirecional para aplicativos AWS corporativos, como Amazon Chime, QuickSight Amazon Connect AWS IAM Identity Center, Amazon WorkDocs, Amazon WorkMail, WorkSpaces Amazon e o. AWS Management Console AWS O Microsoft AD gerenciado deve ser capaz de consultar os usuários e grupos em seu autogerenciamentoActive Directory.

O Amazon EC2, o Amazon RDS e o Amazon FSx funcionarão com uma relação de confiança unidirecional ou bidirecional.

Pré-requisitos

Para criar a confiança são necessárias apenas algumas etapas, mas antes você deve atender a vários pré-requisitos para configurar a confiança.

> **Note**
>
> AWS O Microsoft AD gerenciado não oferece suporte à confiança em domínios de rótulo único.

Conectar-se à VPC

Se você estiver criando uma relação de confiança com seu diretório autogerenciado, você deve primeiro conectar sua rede autogerenciada à Amazon VPC contendo seu Microsoft AD gerenciado AWS . O firewall de suas redes autogerenciadas e AWS gerenciadas do Microsoft AD deve ter as portas de rede abertas listadas no WindowsServer 2008 e em versões posteriores na Microsoft documentação.

Para usar seu nome NetBIOS em vez de seu nome de domínio completo para autenticação com seus AWS aplicativos como Amazon ou WorkDocs Amazon QuickSight, você deve permitir a porta 9389. Para obter mais informações sobre portas e protocolos do Active Directory, consulte Visão geral do serviço e requisitos de porta de rede Windows na Microsoft documentação.

Essas são as portas mínimas necessárias para conectar ao diretório. Sua configuração específica pode exigir que portas adicionais sejam abertas.

Configurar a VPC

A VPC que contém seu AWS Microsoft AD gerenciado deve ter as regras de entrada e saída apropriadas.

Para configurar as regras de saída da VPC

1. No AWS Directory Service console, na página Detalhes do diretório, anote seu ID de diretório AWS gerenciado do Microsoft AD.
2. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
3. Escolha Grupos de segurança.
4. Pesquise seu ID de diretório AWS gerenciado do Microsoft AD. Nos resultados da pesquisa, selecione o item com a descrição "grupo de segurança AWS criado para controladores de diretório ID de diretório".

   > **Note**
   >
   > O grupo de segurança selecionado é criado automaticamente quando você cria inicialmente o diretório.

5. Acesse a guia Oubound Rules (Regras de saída) daquele grupo de segurança. Selecione Editar e Adicionar outra regra. Insira os seguintes valores para a nova regra:

   - Tipo: Todo o tráfego
   - Protocol (Protocolo): Todos
   - Destino determina o tráfego concedido aos seus controladores de domínio e onde eles podem ir em sua rede autogerenciada. Especifique um único endereço IP ou intervalo de endereços IP em notação CIDR (por exemplo, 203.0.113.5/32). Você também pode especificar o nome ou o ID de outro grupo de segurança na mesma região. Para ter mais informações, consulte Entenda a configuração e o uso do grupo de AWS segurança do seu diretório.
6. Selecione Save (Salvar).

Habilitar a pré-autenticação Kerberos

Suas contas de usuário devem ter a pré-autenticação Kerberos habilitada. Para obter mais informações sobre essa configuração, consulte Pré-autenticação na Microsoft TechNet.

Configurar encaminhadores condicionais de DNS para o domínio autogerenciado

Você deve configurar encaminhadores condicionais de DNS em seu domínio autogerenciado. Consulte Atribuir um encaminhador condicional para um nome de domínio na Microsoft TechNet para obter detalhes sobre encaminhadores condicionais.

Para executar as etapas a seguir, é necessário ter acesso às seguintes ferramentas do Windows Server para seu domínio autogerenciado:

- Ferramentas do AD DS e do AD LDS
- DNS

Para configurar encaminhadores condicionais de DNS para seu domínio autogerenciado

1. Primeiro, você deve obter algumas informações sobre seu Microsoft AD AWS gerenciado. Faça login no AWS Management Console e abra o console do AWS Directory Service.
2. No painel de navegação, selecione Directories (Diretórios).
3. Escolha o ID do diretório do seu Microsoft AD AWS gerenciado.
4. Anote o nome de domínio totalmente qualificado (FQDN) e o endereço DNS do diretório.
5. Agora, retorne ao seu controlador de domínio autogerenciado. Abra o Gerenciador de Servidores.
6. No menu Ferramentas, escolha DNS.
7. Na árvore do console, expanda o servidor DNS do domínio para o qual você está configurando a confiança.
8. Na árvore do console, escolha Encaminhadores condicionais.
9. No menu Ação, escolha Novo encaminhador condicional.
10. No domínio DNS, digite o nome de domínio totalmente qualificado (FQDN) do seu AWS Microsoft AD gerenciado, que você anotou anteriormente.
11. Escolha os endereços IP dos servidores primários e digite os endereços DNS do seu diretório AWS gerenciado do Microsoft AD, que você anotou anteriormente.

    Depois de digitar o endereço DNS, você pode obter um erro como “tempo limite” ou “não foi possível resolver”. Em geral, você pode ignorar esses erros.
12. Selecione Armazenar este encaminhador condicional no Active Directory e replicar como: Todos os servidores DNS neste domínio. Escolha OK.

Senha de relação de confiança

Se você está criando uma relação de confiança com um domínio existente, configure a relação de confiança nesse domínio usando as ferramentas de administração do Windows Server. Durante esse

processo, anote a senha de confiança que você usará. Você precisará usar essa mesma senha ao configurar a relação de confiança no Microsoft AD AWS gerenciado. Para obter mais informações, consulte Gerenciando relações de confiança na Microsoft TechNet.

Agora você está pronto para criar a relação de confiança em seu Microsoft AD AWS gerenciado.

Nomes NetBIOS e de domínio

Os nomes NetBIOS e de domínio devem ser exclusivos e não podem ser os mesmos para estabelecer uma relação de confiança.

Criar, verificar ou excluir uma relação de confiança

> **Note**
>
> Relações de confiança são um recurso global do AWS Managed Microsoft AD. Se você estiver usando o Replicação em várias regiões, os procedimentos a seguir deverão ser executados no Região principal. As alterações serão aplicadas automaticamente em todas as regiões replicadas. Para ter mais informações, consulte Recursos globais versus regionais.

Para criar uma relação de confiança com seu Microsoft AD AWS gerenciado

1. Abra o console de AWS Directory Service.
2. Na página Diretórios, escolha seu Microsoft AD ID AWS gerenciado.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Trust relationships (Relações de confiança), selecione Action (Ação) e selecione Add trust relationship (Adicionar relação de confiança).
5. Na página Add a trust relationship (Adicionar uma relação de confiança), forneça as informações necessárias, incluindo o tipo de confiança, o nome de domínio totalmente qualificado (FQDN) do seu domínio confiável, a senha de confiança e o sentido da confiança.

6. (Opcional) Se você quiser permitir que somente usuários autorizados acessem recursos em seu diretório AWS gerenciado do Microsoft AD, você pode, opcionalmente, escolher a caixa de seleção Autenticação seletiva. Para obter informações gerais sobre autenticação seletiva, consulte Considerações de segurança para relações de confiança na Microsoft. TechNet
7. Em Encaminhador condicional, digite o endereço IP do servidor DNS autogerenciado. Se você já tiver criado encaminhadores condicionais, poderá digitar o FQDN do domínio autogerenciado em vez de um endereço IP de DNS.
8. (Opcional) Selecione Adicionar outro endereço IP e digite o endereço IP de um servidor de DNS autogerenciado adicional. Você pode repetir esta etapa para cada endereço de servidor DNS aplicável para um total de quatro endereços.
9. Escolha Adicionar.
10. Se o servidor DNS ou a rede do seu domínio autogerenciado usa um espaço de endereço IP público (não compatível com RFC 1918), acesse a seção Roteamento IP, selecione Ações e selecione Adicionar rota. Digite o bloco de endereço IP do servidor DNS ou da rede autogerenciada usando o formato CIDR, por exemplo, 203.0.113.0/24. Esta etapa não é necessária se o servidor DNS e a rede autogerenciada estiverem usando espaços de endereço IP compatíveis com RFC 1918.

    > **Note**
    >
    > Ao usar um espaço de endereço IP público, não use nenhum dos intervalos de endereço IP da AWS, já que eles não podem ser usados.

11. (Opcional) Recomendamos que, enquanto você está na página Adicionar rotas, você também selecione Adicionar rotas ao grupo de segurança para a VPC deste diretório. Isso configurará os grupos de segurança conforme a detalhado em “Configurar a VPC”. Essas regras de segurança têm impacto na interface de rede interna que não é exposta publicamente. Se essa opção não estiver disponível, você verá uma mensagem indicando que já personalizou seus grupos de segurança.

Você deve configurar a relação de confiança em ambos os domínios. As relações devem ser complementares. Por exemplo, se você criar uma relação de confiança de saída em um domínio, deverá criar uma relação de confiança de entrada em outro.

Se você está criando uma relação de confiança com um domínio existente, configure a relação de confiança nesse domínio usando as ferramentas de administração do Windows Server.

Você pode criar várias relações de confiança entre seu Microsoft AD AWS gerenciado e vários domínios do Active Directory. Contudo, pode existir somente uma relação de confiança por par de cada vez. Por exemplo, se você tem uma relação de confiança unidirecional no sentido de entrada e deseja configurar outra relação de confiança na direção de saída, precisará excluir a relação de confiança existente e criar uma nova relação bidirecional.

Para verificar uma relação de confiança de saída

1. Abra o console de AWS Directory Service.
2. Na página Diretórios, escolha seu Microsoft AD ID AWS gerenciado.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Trust relationships (Relações de confiança), selecione a confiança que você deseja verificar, selecione Actions (Ações) e selecione Verify trust relationship (Verificar relação de confiança).

Esse processo verifica somente a direção de saída de uma relação de confiança bidirecional. AWS não suporta a verificação de fundos fiduciários recebidos. Para obter mais informações sobre como verificar uma relação de confiança de ou para seu Active Directory autogerenciado, consulte Verificar uma relação de confiança na Microsoft TechNet.

Para excluir uma relação de confiança existente

1. Abra o console de AWS Directory Service.
2. Na página Diretórios, escolha seu Microsoft AD ID AWS gerenciado.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.

4. Na seção Trust relationships (Relações de confiança), selecione a confiança que você deseja excluir, selecione Actions (Ações) e selecione Delete trust relationship (Excluir relação de confiança).
5. Escolha Excluir.

Adicionar rotas IP ao usar endereços IP públicos

Você pode usar o AWS Directory Service for Microsoft Active Directory para se beneficiar de muitos recursos avançados do Active Directory, incluindo o estabelecimento de relações de confiança com outros diretórios. No entanto, se os servidores DNS para as redes de outros diretórios usarem endereços IP públicos (não compatíveis com RFC 1918), você deverá especificar esses endereços IP como parte da configuração de confiança. As instruções para fazer isso podem ser localizadas em Criar uma relação de confiança.

Da mesma maneira, você também deve inserir as informações dos endereços IP ao rotear tráfego de seu AWS Managed Microsoft AD na AWS para uma VPC par da AWS se a VPC usar intervalos IP públicos.

Quando você adiciona os endereços IP, conforme descrito em Criar uma relação de confiança, você tem a opção de selecionar Adicionar rota ao grupo de segurança para a VPC deste diretório. Essa opção deve ser selecionada, a menos que você tenha personalizado anteriormente seu grupo de segurança para permitir o tráfego necessário conforme mostrado a seguir. Para obter mais informações, consulte Entenda a configuração e o uso do grupo de AWS segurança do seu diretório.

Tutorial: criar uma relação de confiança entre o diretório do AWS Managed Microsoft AD e seu domínio autogerenciado do Active Directory .

Este tutorial descreve todas as etapas necessárias para configurar uma relação de confiança entre o AWS Directory Service for Microsoft Active Directory e seu Microsoft Active Directory autogerenciado (on-premises). Embora a criação de confiança exija apenas algumas etapas, você deve primeiro concluir as etapas de pré-requisito a seguir.

Tópicos

Consulte também

Criar uma relação de confiança

Pré-requisitos

Este tutorial pressupõe que você já tenha o seguinte:

> **Note**
>
> O AWS Managed Microsoft AD não oferece suporte a relações de confiança com Domínios de rótulo único.

- Um diretório do AWS Managed Microsoft AD criado na AWS. Se precisar de ajuda para isso, consulte Introdução ao AWS Managed Microsoft AD.
- Uma instância do EC2 executando o Windows adicionada ao AWS Managed Microsoft AD. Se precisar de ajuda para isso, consulte Associe manualmente uma Windows instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory.

  > **Important**
  >
  > A conta de administrador do AWS Managed Microsoft AD deve ter acesso administrativo a essa instância.

- As seguintes ferramentas do Windows Server instaladas nessa instância:
  - Ferramentas do AD DS e do AD LDS
  - DNS

  Se precisar de ajuda para isso, consulte Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado.
- Um Microsoft Active Directory autogerenciado (on-premises)

  Você deve ter acesso administrativo a esse diretório. As mesmas ferramentas do Windows Server listadas acima também devem estar disponíveis para esse diretório.
- Uma conexão ativa entre sua rede autogerenciada e a VPC que contém seu AWS Managed Microsoft AD Se você precisar de ajuda para isso, consulte Amazon nuvem virtual privada Connectivity Options.

- Uma política de segurança local definida corretamente. Marque `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` e verifique se a opção contém pelo menos estes três pipes nomeados:
  - netlogon
  - samr
  - lsarpc
- Os nomes NetBIOS e de domínio devem ser exclusivos e não podem ser os mesmos para estabelecer uma relação de confiança

Para obter mais informações sobre os pré-requisitos para criar uma relação de confiança, consulte Criar uma relação de confiança.

Configuração do tutorial

Para este tutorial, já criamos um AWS Managed Microsoft AD e um domínio autogerenciado. A rede autogerenciada está conectada à VPC do AWS Managed Microsoft AD. As seguintes são as propriedades dos dois diretórios:

AWS Managed Microsoft AD em execução na AWS

- Nome do domínio (FQDN): MyManagedAD.example.com
- Nome NetBIOS: MyManagedAD
- Endereços DNS: 10.0.10.246, 10.0.20.121
- CIDR da VPC: 10.0.0.0/16

O AWS Managed Microsoft AD reside na VPC ID: vpc-12345678.

Domínio autogerenciado ou do AWS Managed Microsoft AD

- Nome do domínio (FQDN): corp.example.com
- Nome NetBIOS: CORP
- Endereços DNS: 172.16.10.153
- CIDR autogerenciado: 172.16.0.0/16

Próxima etapa

[Etapa 1: preparar o domínio autogerenciado do AD]

Etapa 1: preparar o domínio autogerenciado do AD

Primeiro, é necessário seguir várias etapas obrigatórias em seu domínio autogerenciado (on-premises).

Configurar o firewall autogerenciado

Você deve configurar seu firewall autogerenciado para que as seguintes portas estejam abertas para os CIDRs de todas as sub-redes usadas pela VPC que contém seu Microsoft AD gerenciado. AWS Neste tutorial, permitimos tráfego de entrada e saída de 10.0.0.0/16 (o bloco CIDR da VPC do nosso AWS Microsoft AD gerenciado) nas seguintes portas:

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticação de Kerberos
- TCP/UDP 389 - Lightweight Directory Access Protocol (LDAP)
- TCP 445 - Bloco de mensagens do servidor (SMB)
- TCP 9389 - Serviços Web do Active Directory (ADWS) (Opcional - Essa porta precisa estar aberta se você quiser usar seu nome NetBIOS em vez do nome de domínio completo para autenticação com aplicativos como AWS Amazon ou Amazon.) WorkDocs QuickSight

> **Note**
>
> SMBv1 não é mais compatível.
> Essas são as portas mínimas necessárias para conectar a VPC ao diretório autogerenciado. Sua configuração específica pode exigir que portas adicionais sejam abertas.

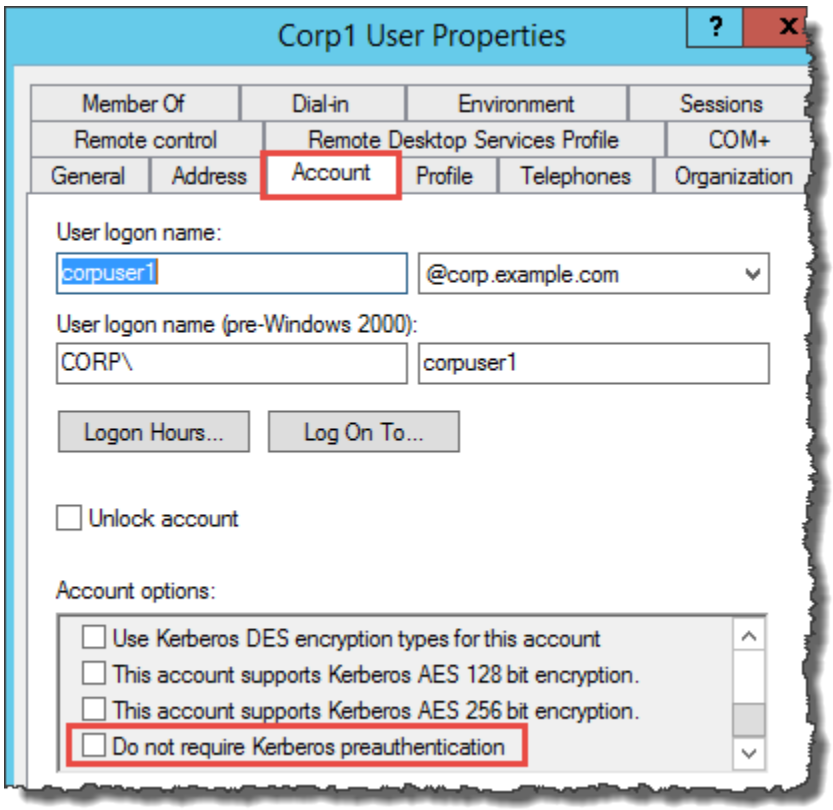
Verificar se a pré-autenticação Kerberos está habilitada

As contas de usuário nos dois diretórios devem ter a pré-autenticação Kerberos habilitada. Esse é o padrão, mas vamos verificar as propriedades de qualquer usuário aleatório para ter certeza de que nada foi alterado.

Para visualizar as configurações do Kerberos do usuário

1. No controlador de domínio autogerenciado, abra o Gerenciador de servidores.

2. No menu Tools, escolha Active Directory Users and Computers (Usuários e computadores do Active Directory).
3. Escolha a pasta Users (Usuários) e abra o menu de contexto (clique com o botão direito do mouse). Selecione qualquer conta de usuário aleatória listada no painel direito. Escolha Properties (Propriedades).
4. Selecione a guia Account (Conta). Na lista Account options, role para baixo e confirme se a opção Do not require Kerberos preauthentication não está marcada.



Configurar encaminhadores condicionais de DNS para o domínio autogerenciado

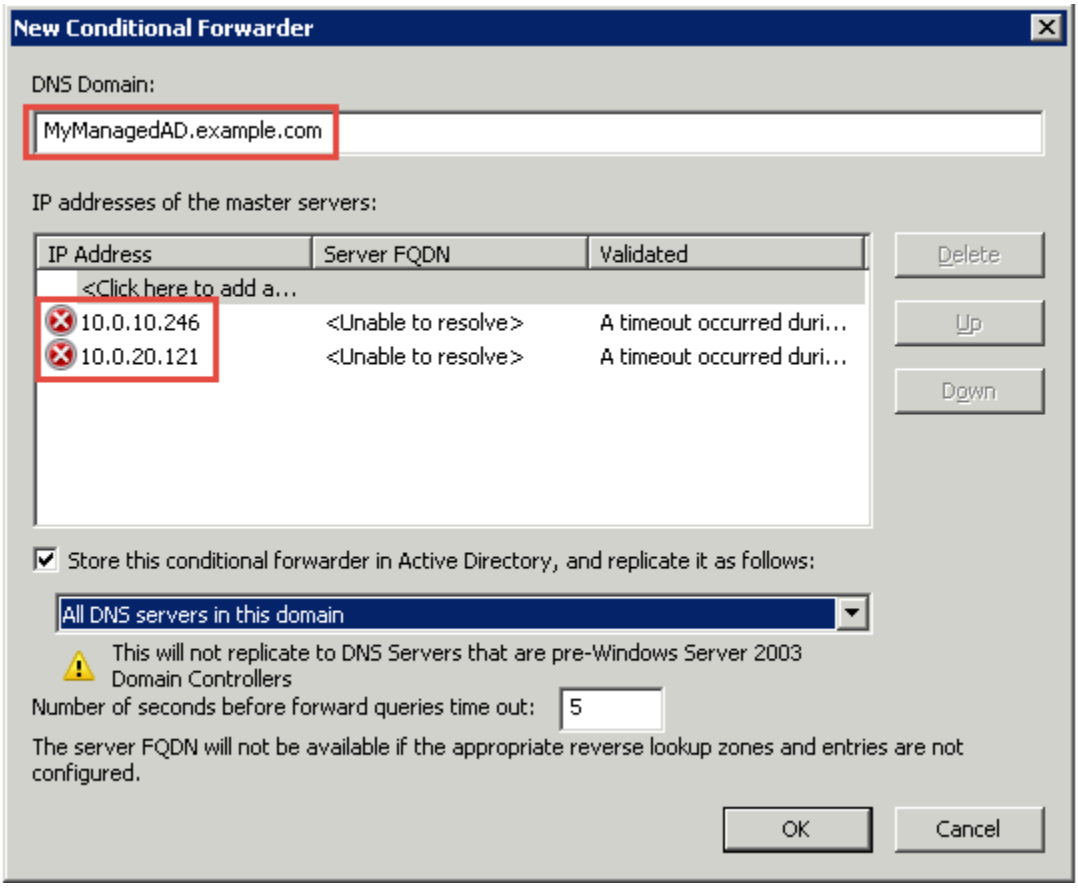
Você deve configurar encaminhadores condicionais de DNS em cada domínio. Antes de fazer isso em seu domínio autogerenciado, primeiro você obterá algumas informações sobre seu Microsoft AD AWS gerenciado.

Para configurar encaminhadores condicionais de DNS para seu domínio autogerenciado

1. Faça login no AWS Management Console e abra o AWS Directory Service console.
2. No painel de navegação, selecione Directories (Diretórios).
3. Escolha o ID do diretório do seu Microsoft AD AWS gerenciado.

4. Na página Details (Detalhes), anote os valores em Directory name (Nome do diretório) e o DNS address (Endereço DNS) do seu diretório.
5. Agora, retorne ao seu controlador de domínio autogerenciado. Abra o Gerenciador de Servidores.
6. No menu Ferramentas, escolha DNS.
7. Na árvore do console, expanda o servidor DNS do domínio para o qual você está configurando a confiança. Nosso servidor é WIN-5V70CN7VJ0.corp.example.com.
8. Na árvore do console, escolha Encaminhadores condicionais.
9. No menu Ação, escolha Novo encaminhador condicional.
10. No domínio DNS, digite o nome de domínio totalmente qualificado (FQDN) do seu AWS Microsoft AD gerenciado, que você anotou anteriormente. Neste exemplo, o FQDN é MyManaged Ad.example.com.
11. Escolha os endereços IP dos servidores primários e digite os endereços DNS do seu diretório AWS gerenciado do Microsoft AD, que você anotou anteriormente. Neste exemplo, são eles: 10.0.10.246, 10.0.20.121

    Depois de digitar o endereço DNS, você pode obter um erro como “tempo limite” ou “não foi possível resolver”. Em geral, você pode ignorar esses erros.



12. Selecione Store this conditional forwarder in Active Directory, and replicate it as follows.
13. Selecione All DNS servers in this domain e escolha OK.

Próxima etapa

Etapa 2: preparar o AWS Managed Microsoft AD

Etapa 2: preparar o AWS Managed Microsoft AD

Agora, vamos preparar seu Microsoft AD AWS gerenciado para a relação de confiança. Muitas das etapas a seguir são quase idênticas ao que você acabou de concluir para seu domínio autogerenciado. Desta vez, no entanto, você está trabalhando com seu Microsoft AD AWS gerenciado.

Configurar as sub-redes e os grupos de segurança da VPC

Você deve permitir o tráfego da sua rede autogerenciada para a VPC que contém seu Microsoft AD AWS gerenciado. Para fazer isso, você precisará garantir que as ACLs associadas às sub-redes usadas para implantar seu AWS Microsoft AD gerenciado e as regras de grupo de segurança

configuradas em seus controladores de domínio permitam o tráfego necessário para suportar relações de confiança.

Os requisitos de porta variam de acordo com a versão do Windows Server usada pelos seus controladores de domínio e pelos serviços ou aplicativos que utilizarão a confiança. Para fins deste tutorial, você precisará abrir as seguintes portas:

Entrada

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticação de Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - autenticação do Kerberos
- TCP 636 - LDAPS (LDAP por TLS/SSL)
- TCP 3268-3269 - catálogo global
- TCP/UDP 49152-65535 - portas efêmeras para RPC

> **Note**
>
> SMBv1 não é mais compatível.

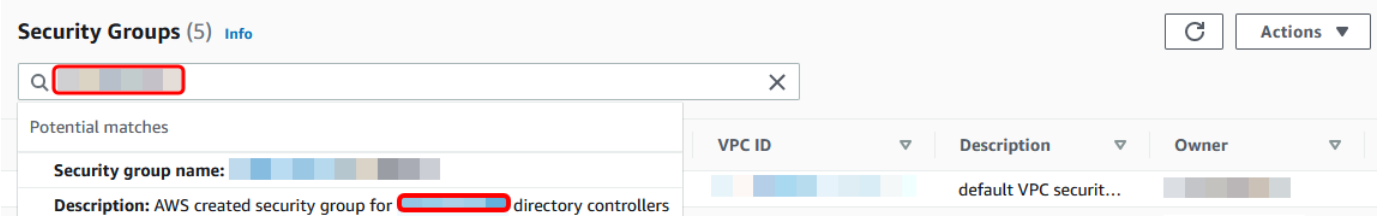
Saída

- ALL

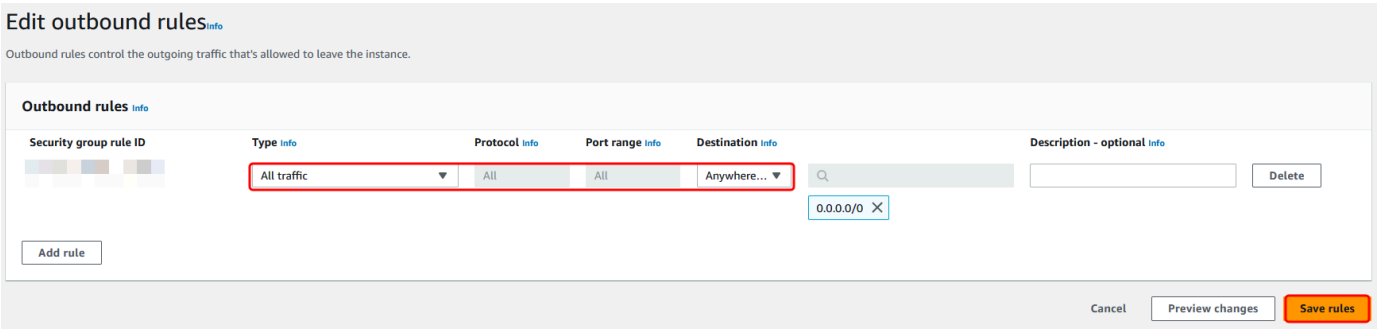
> **Note**
>
> Essas são as portas mínimas necessárias para poder conectar a VPC e o diretório autogerenciado. Sua configuração específica pode exigir que portas adicionais sejam abertas.

Para configurar suas regras de entrada e saída do controlador de domínio Microsoft AD AWS gerenciado

1. Retorne para o console do AWS Directory Service. Na lista de diretórios, anote a ID do diretório do seu diretório AWS Managed Microsoft AD.
2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
3. No painel de navegação, selecione Security Groups.(Grupos de segurança).
4. Use a caixa de pesquisa para pesquisar seu ID de diretório AWS gerenciado do Microsoft AD. Nos resultados da pesquisa, selecione o Grupo de Segurança com a descrição**`AWS created security group for yourdirectoryID directory controllers`**.



5. Vá para a guia Outbound Rules desse grupo de segurança. Selecione Editar regras de saída e Adicionar regra. Insira os seguintes valores para a nova regra:
   - Type: Todo o tráfego
   - Protocol (Protocolo): TODOS
   - Destination determina o tráfego que pode sair dos controladores de domínio e para onde ele pode ir. Especifique um único endereço IP ou intervalo de endereços IP em notação CIDR (por exemplo, 203.0.113.5/32). Você também pode especificar o nome ou o ID de outro grupo de segurança na mesma região. Para ter mais informações, consulte Entenda a configuração e o uso do grupo de AWS segurança do seu diretório.
6. Selecione Salvar regra.

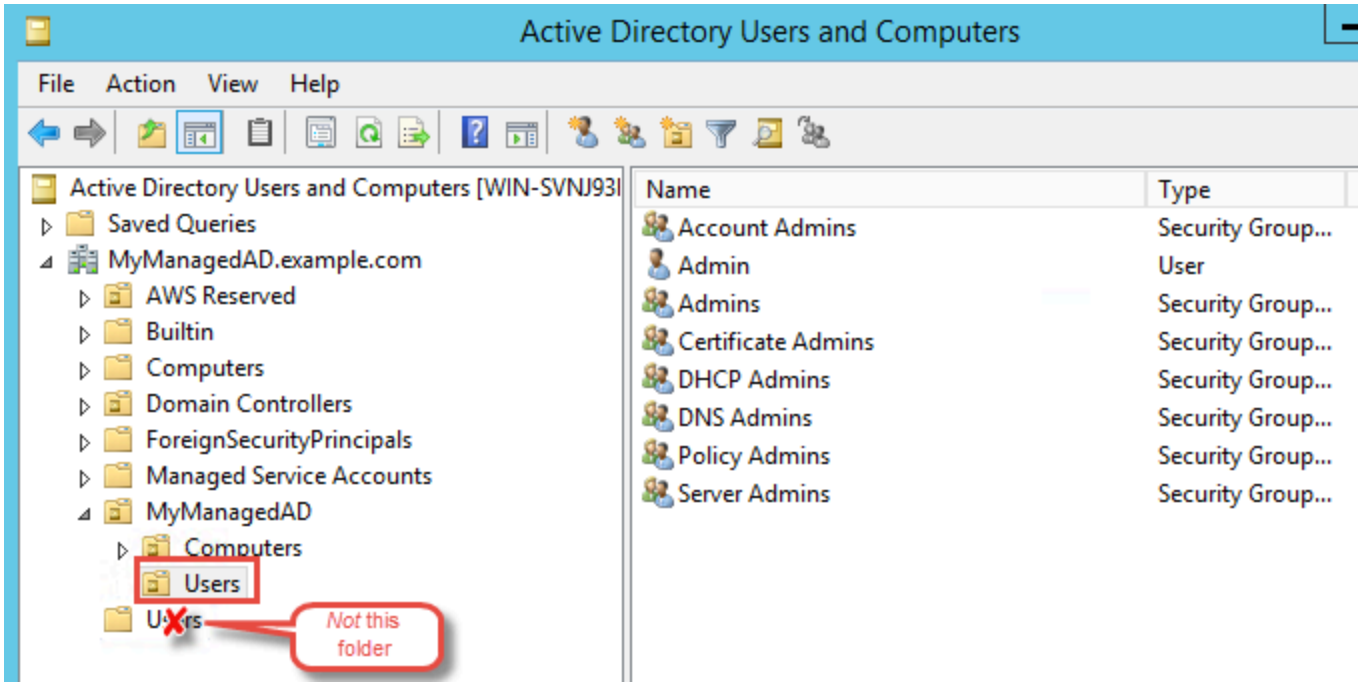


Verificar se a pré-autenticação Kerberos está habilitada

Agora você quer confirmar se os usuários em seu Microsoft AD AWS gerenciado também têm a pré-autenticação Kerberos habilitada. Este é o mesmo processo que você concluiu para o diretório autogerenciado. Este é o padrão, mas vamos verificar para ter certeza de que nada foi alterado.

Para visualizar as configurações de Kerberos do usuário

1. Faça login em uma instância que seja membro do seu diretório AWS gerenciado do Microsoft AD usando o Permissões para a conta de administrador para o domínio ou uma conta à qual foram delegadas permissões para gerenciar usuários no domínio.
2. Se ainda não estiverem instaladas, instale a ferramenta Usuários de computadores do Active Directory e a ferramenta do DNS. Saiba como instalar essas ferramentas em Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado.
3. Abra o Gerenciador de Servidores. No menu Tools, escolha Active Directory Users and Computers (Usuários e computadores do Active Directory).
4. Escolha a pasta Users em seu domínio. Observe que essa é a pasta Users (Usuários) sob seu nome NetBIOS, e não a pasta Users (Usuários) sob o nome do domínio totalmente qualificado (FQDN).



5. Na lista de usuários, clique com o botão direito do mouse em um usuário e selecione Properties (Propriedades).

6. Selecione a guia Account (Conta). Na lista Account options, confirme se Do not require Kerberos preauthentication não está marcada.

Próxima etapa

Etapa 3: criar a relação de confiança

Etapa 3: criar a relação de confiança

Agora que o trabalho de preparação está concluído, as etapas finais são para criar as confianças. Crie a confiança em seu domínio autogerenciado e, depois, no AWS Managed Microsoft AD. Se você tiver problemas durante o processo de criação de confiança, consulte Motivos do status da criação de relações de confiança para obter assistência.

Configurar a confiança no seu Active Directory autogerenciado

Neste tutorial, você configura uma confiança de floresta bidirecional. Contudo, se você criar uma confiança de floresta unidirecional, lembre-se de que as direções de confiança em cada um dos domínios deve ser complementar. Por exemplo, se você criar uma confiança unidirecional de saída em seu domínio autogerenciado, precisará também criar uma confiança unidirecional de entrada no AWS Managed Microsoft AD.

> **Note**
>
> O AWS Managed Microsoft AD também oferece suporte a relações de confiança externas. Contudo, para os propósitos deste tutorial, você criará uma confiança de floresta bidirecional.

Para configurar a confiança em seu Active Directory autogerenciado

1. Abra o Gerenciador de Servidores e, no menu Tools, escolha Active Directory Domains and Trusts.
2. Abra o menu de contexto (clique com o botão direito do mouse) do domínio e escolha Properties.
3. Escolha a guia Trusts (Confianças) e escolha New trust (Nova confiança). Digite o nome do AWS Managed Microsoft AD e escolha Próximo.
4. Escolha Forest trust. Selecione Next (Próximo).
5. Escolha Two-way. Selecione Next (Próximo).

6. Escolha This domain only. Selecione Next (Próximo).
7. Escolha Forest-wide authentication. Selecione Next (Próximo).
8. Digite uma Trust password. Lembre-se dessa senha, pois você precisará dela ao configurar a confiança para o AWS Managed Microsoft AD.
9. Na caixa de diálogo seguinte, confirme suas configurações e escolha Next. Confirme se a confiança foi criada com êxito e escolha Next novamente.
10. Escolha No, do not confirm the outgoing trust. Selecione Next (Próximo).
11. Escolha No, do not confirm the incoming trust. Selecione Next (Próximo).

Configure a confiança em seu diretório do AWS Managed Microsoft AD

Finalmente, configure a relação de confiança da floresta com o seu diretório do AWS Managed Microsoft AD. Como você criou uma confiança de floresta bidirecional no domínio autogerenciado, você também criou uma confiança bidirecional usando seu diretório do AWS Managed Microsoft AD.

> **Note**
>
> Relações de confiança são um recurso global do AWS Managed Microsoft AD. Se você estiver usando o Replicação em várias regiões, os procedimentos a seguir deverão ser executados no Região principal. As alterações serão aplicadas automaticamente em todas as regiões replicadas. Para obter mais informações, consulte Recursos globais versus regionais.

Para configurar a confiança em seu diretório do AWS Managed Microsoft AD

1. Retorne para o console doAWS Directory Service.
2. Na página Diretórios, selecione o ID do seu AWS Managed Microsoft AD.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Trust relationships (Relações de confiança), selecione Action (Ação) e selecione Add trust relationship (Adicionar relação de confiança).

5. Na página Adicionar uma relação de confiança, especifique o tipo de confiança. Nesse caso, escolhemos Confiança de floresta. Digite o FQDN do seu domínio autogerenciado (neste tutorial, **`corp.example.com`**). Digite a mesma senha de confiança que você usou ao criar a confiança em seu domínio autogerenciado. Especifique a direção. Neste caso, selecionamos Bidirecional.
6. No campo Encaminhador condicional, digite o endereço IP do servidor de DNS local. Neste exemplo, digite 172.16.10.153.
7. (Opcional) Escolha Adicionar outro endereço IP e digite um segundo endereço IP para o seu servidor de DNS local. Você pode especificar até um total de quatro servidores DNS.
8. Escolha Adicionar.

Parabéns. Agora você tem uma relação de confiança entre seu domínio autogerenciado (corp.exemplo.com) e seu AWS Microsoft AD gerenciado (AD.exemplo.com). MyManaged Somente uma relação pode ser configurada entre esses dois domínios. Se, por exemplo, você desejar alterar a direção da confiança para unidirecional, você precisará primeiro excluir essa relação de confiança existente e criar uma nova.

Para obter mais informações, incluindo instruções sobre a verificação ou a exclusão de confianças, consulte Criar uma relação de confiança.

Tutorial: criar uma relação de confiança entre dois domínios do AWS Managed Microsoft AD

Este tutorial descreve todas as etapas necessárias para configurar uma relação de confiança entre dois domínios do AWS Directory Service for Microsoft Active Directory.

Tópicos

- Etapa 1: preparar o AWS Managed Microsoft AD
- Etapa 2: criar a relação de confiança com outro domínio do AWS Managed Microsoft AD

Consulte também

Criar uma relação de confiança

Etapa 1: preparar o AWS Managed Microsoft AD

Nesta seção, você preparará seu Microsoft AD AWS gerenciado para a relação de confiança com outro Microsoft AD AWS gerenciado. Muitas das etapas a seguir são quase idênticas à você

acabou de concluir em Tutorial: criar uma relação de confiança entre o diretório do AWS Managed Microsoft AD e seu domínio autogerenciado do Active Directory .. Desta vez, no entanto, você está configurando seus ambientes AWS gerenciados do Microsoft AD para trabalharem uns com os outros.

Configurar as sub-redes e os grupos de segurança da VPC

Você deve permitir o tráfego de uma rede AWS gerenciada do Microsoft AD para a VPC que contém seu outro AWS Microsoft AD gerenciado. Para fazer isso, você precisará garantir que as ACLs associadas às sub-redes usadas para implantar seu AWS Microsoft AD gerenciado e as regras de grupo de segurança configuradas em seus controladores de domínio permitam o tráfego necessário para suportar relações de confiança.

Os requisitos de porta variam de acordo com a versão do Windows Server usada pelos seus controladores de domínio e pelos serviços ou aplicativos que utilizarão a confiança. Para fins deste tutorial, você precisará abrir as seguintes portas:

Entrada

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticação de Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

> **Note**
>
> SMBv1 não é mais compatível.

- TCP/UDP 464 - autenticação do Kerberos
- TCP 636 - LDAPS (LDAP por TLS/SSL)
- TCP 3268-3269 - catálogo global
- TCP/UDP 1024-65535 - portas efêmeras para RPC

Saída

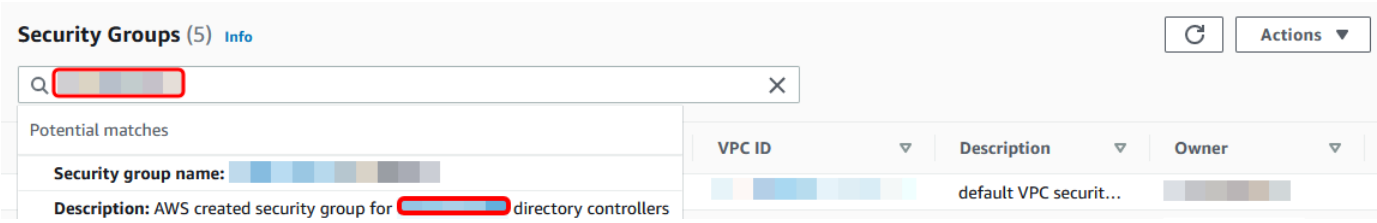
- ALL

> **Note**
>
> Essas são as portas mínimas necessárias para poder conectar as VPCs de ambos os AWS Managed Microsoft ADs. Sua configuração específica pode exigir que portas adicionais sejam abertas. Para obter mais informações, consulte Como configurar um firewall para domínios e relações de confiança do Active Directory no site da Microsoft.

Para configurar as regras de saída do controlador de domínio AWS gerenciado do Microsoft AD

> **Note**
>
> Repita as etapas 1 a 6 abaixo para cada diretório.

1. Acesse o console do AWS Directory Service. Na lista de diretórios, anote a ID do diretório do seu diretório AWS Managed Microsoft AD.
2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
3. No painel de navegação, selecione Security Groups.(Grupos de segurança).
4. Use a caixa de pesquisa para pesquisar seu ID de diretório AWS gerenciado do Microsoft AD. Nos resultados da pesquisa, selecione o item com a descrição**`AWS created security group for yourdirectoryID directory controllers`**.

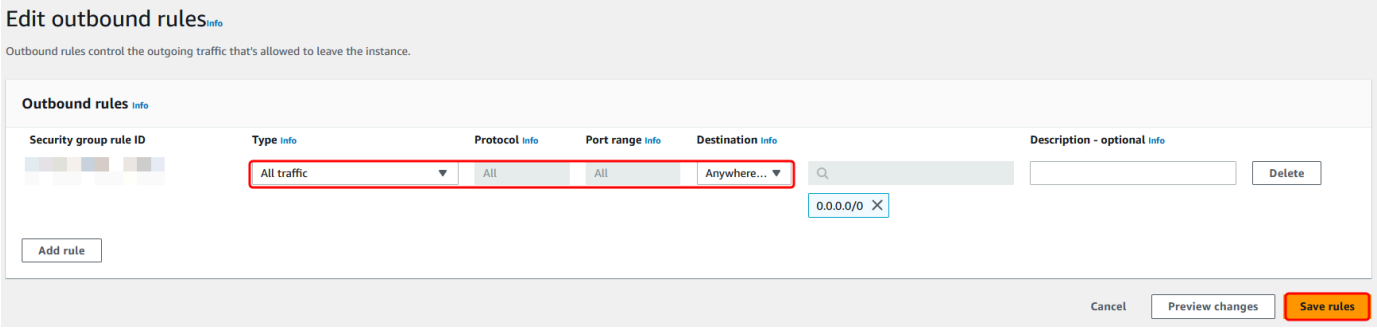


5. Vá para a guia Outbound Rules desse grupo de segurança. Escolha Edit e Add another rule. Insira os seguintes valores para a nova regra:

   - Type: Todo o tráfego
   - Protocol (Protocolo): TODOS
   - Destination determina o tráfego que pode sair dos controladores de domínio e para onde ele pode ir. Especifique um único endereço IP ou intervalo de endereços IP em notação CIDR

(por exemplo, 203.0.113.5/32). Você também pode especificar o nome ou o ID de outro grupo de segurança na mesma região. Para ter mais informações, consulte Entenda a configuração e o uso do grupo de AWS segurança do seu diretório.

6. Selecione Save (Salvar).

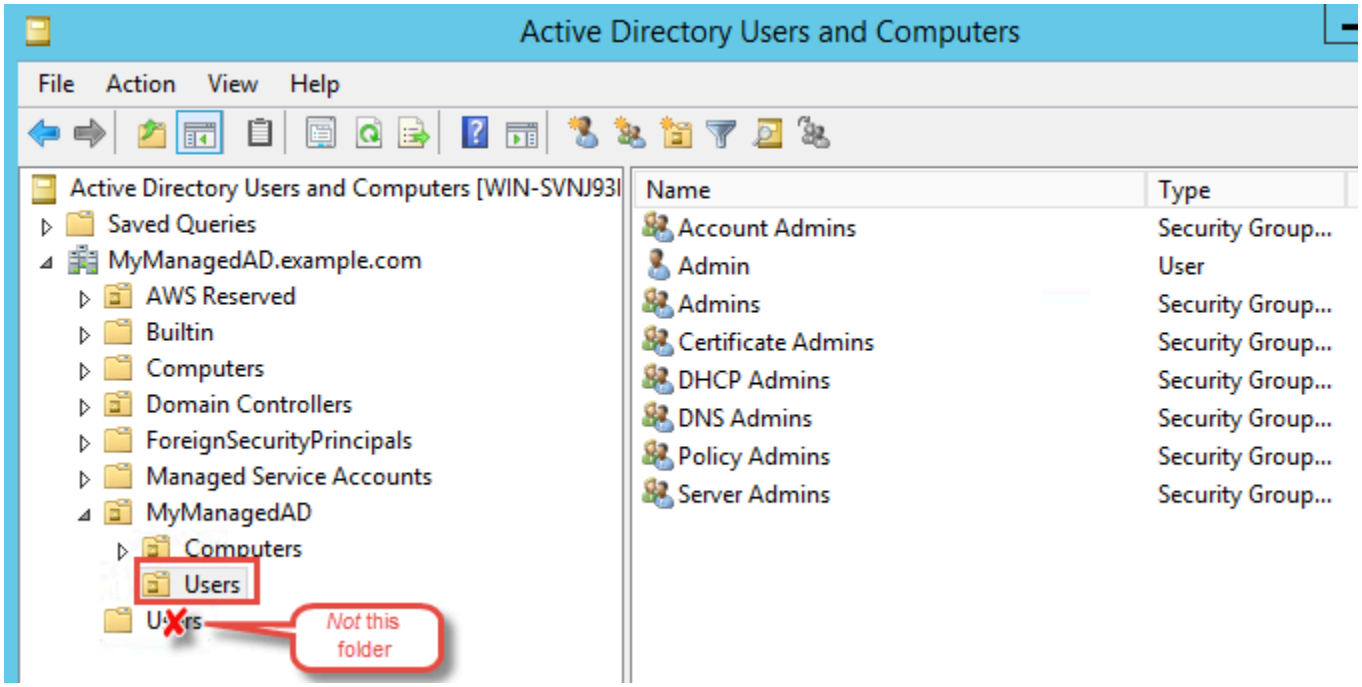


Verificar se a pré-autenticação Kerberos está habilitada

Agora você quer confirmar se os usuários em seu Microsoft AD AWS gerenciado também têm a pré-autenticação Kerberos habilitada. Este é o mesmo processo que você concluiu para o diretório on-premises. Este é o padrão, mas vamos verificar para ter certeza de que nada foi alterado.

Para visualizar as configurações de Kerberos do usuário

1. Faça login em uma instância que seja membro do seu diretório AWS gerenciado do Microsoft AD usando o Permissões para a conta de administrador para o domínio ou uma conta à qual foram delegadas permissões para gerenciar usuários no domínio.
2. Se ainda não estiverem instaladas, instale a ferramenta Usuários de computadores do Active Directory e a ferramenta do DNS. Saiba como instalar essas ferramentas em Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado.
3. Abra o Gerenciador de Servidores. No menu Tools, escolha Active Directory Users and Computers (Usuários e computadores do Active Directory).
4. Escolha a pasta Users em seu domínio. Observe que essa é a pasta Users (Usuários) sob seu nome NetBIOS, e não a pasta Users (Usuários) sob o nome do domínio totalmente qualificado (FQDN).



5. Na lista de usuários, clique com o botão direito do mouse em um usuário e selecione Properties (Propriedades).
6. Selecione a guia Account (Conta). Na lista Account options, confirme se Do not require Kerberos preauthentication não está marcada.

Próxima etapa

Etapa 2: criar a relação de confiança com outro domínio do AWS Managed Microsoft AD

Etapa 2: criar a relação de confiança com outro domínio do AWS Managed Microsoft AD

Agora que o trabalho de preparação está concluído, as etapas finais destinam-se a criar as confianças entre seus dois domínios do AWS Managed Microsoft AD. Se você tiver problemas durante o processo de criação de confiança, consulte Motivos do status da criação de relações de confiança para obter assistência.

Configure a confiança em seu primeiro domínio do AWS Managed Microsoft AD

Neste tutorial, você configura uma confiança de floresta bidirecional. Contudo, se você criar uma confiança de floresta unidirecional, lembre-se de que as direções de confiança em cada um dos domínios deve ser complementar. Por exemplo, se você criar uma confiança unidirecional de saída em seu primeiro domínio, precisará também criar uma confiança unidirecional de entrada em seu segundo domínio do AWS Managed Microsoft AD.

> **Note**
>
> O AWS Managed Microsoft AD também oferece suporte a relações de confiança externas. Contudo, para os propósitos deste tutorial, você criará uma confiança de floresta bidirecional.

Para configurar a confiança em seu primeiro domínio do AWS Managed Microsoft AD

1. Abra o console do AWS Directory Service.
2. Na página Diretórios, selecione o ID do seu primeiro AWS Managed Microsoft AD.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Trust relationships (Relações de confiança), selecione Action (Ação) e selecione Add trust relationship (Adicionar relação de confiança).
5. Na página Adicionar uma relação de confiança, digite o FQDN do seu segundo domínio do AWS Managed Microsoft AD. Lembre-se dessa senha, pois você precisará dela ao configurar a confiança para o segundo AWS Managed Microsoft AD. Especifique a direção. Neste caso, escolha Bidirecional.
6. No campo Encaminhador condicional, digite o endereço IP do servidor de DNS do segundo AWS Managed Microsoft AD.
7. (Opcional) Escolha Adicionar outro endereço IP e insira um segundo endereço IP para o seu segundo servidor de DNS do AWS Managed Microsoft AD. Você pode especificar até um total de quatro servidores DNS.
8. Escolha Add (Adicionar). A confiança falhará neste ponto, o que é esperado até criarmos o outro lado da confiança.

Configure a confiança em seu segundo domínio do AWS Managed Microsoft AD

Agora, configure a relação de confiança da floresta com o seu segundo diretório do AWS Managed Microsoft AD. Como você criou uma confiança de floresta bidirecional no primeiro domínio do AWS

Managed Microsoft AD, você também criou uma confiança bidirecional usando este domínio do AWS Managed Microsoft AD.

Para configurar a confiança em seu segundo domínio do AWS Managed Microsoft AD

1. Retorne para o console doAWS Directory Service.
2. Na página Diretórios, selecione o ID do seu segundo AWS Managed Microsoft AD.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Trust relationships (Relações de confiança), selecione Action (Ação) e selecione Add trust relationship (Adicionar relação de confiança).
5. Na página Adicionar uma relação de confiança, digite o FQDN do seu primeiro domínio do AWS Managed Microsoft AD. Digite a mesma senha de confiança que você usou ao criar a confiança em seu domínio on-premises. Especifique a direção. Neste caso, escolha Bidirecional.
6. No campo Encaminhador condicional, digite o endereço IP do servidor de DNS do primeiro AWS Managed Microsoft AD.
7. (Opcional) Escolha Adicionar outro endereço IP e insira um segundo endereço IP para o seu primeiro servidor de DNS do AWS Managed Microsoft AD. Você pode especificar até um total de quatro servidores DNS.
8. Escolha Add (Adicionar). A confiança deve ser verificada logo em seguida.
9. Agora, volte para a relação de confiança que você criou no primeiro domínio e verifique a relação de confiança novamente.

Parabéns. Você agora tem uma relação de confiança entre seus dois domínios do AWS Managed Microsoft AD. Somente uma relação pode ser configurada entre esses dois domínios. Se, por exemplo, você desejar alterar a direção da confiança para unidirecional, você precisará primeiro excluir essa relação de confiança existente e criar uma nova.

Conecte seu Microsoft AD AWS gerenciado ao Microsoft Entra Connect Sync

Este tutorial orienta você pelas etapas necessárias de instalação Microsoft Entra Connect Syncpara Microsoft Entra IDsincronizá-lo com seu Microsoft AD AWS gerenciado.

Neste tutorial, você faz o seguinte:

1. Crie um usuário de domínio AWS gerenciado do Microsoft AD.
2. Baixar Entra Connect Sync.
3. Use Windows PowerShell para executar um script para provisionar as permissões apropriadas para o usuário recém-criado.
4. Instalar o Entra Connect Sync.

Pré-requisitos

Você precisará do seguinte para concluir este tutorial:

- Um Microsoft AD AWS gerenciado. Para ter mais informações, consulte the section called “Crie seu Microsoft AD AWS gerenciado”.
- Uma instância do Amazon EC2 Windows Server associada ao seu AWS Microsoft AD gerenciado. Para ter mais informações, consulte Junte-se perfeitamente a uma instância do Windows.
- Um Windows servidor EC2 Active Directory Administration Tools instalado para gerenciar seu Microsoft AD AWS gerenciado. Para ter mais informações, consulte the section called “Instale as ferramentas de administração do AD para o Microsoft AD AWS gerenciado”.

Etapa 1: criar um usuário Active Directory de domínio

Este tutorial pressupõe que você já tenha um Microsoft AD AWS gerenciado, bem como uma instância Windows do EC2 Server instalada. Active Directory Administration Tools Para ter mais informações, consulte the section called “Instale as ferramentas de administração do AD para o Microsoft AD AWS gerenciado”.

1. Conecte-se à instância em que Active Directory Administration Tools foram instalados.

2. Crie um usuário de domínio AWS gerenciado do Microsoft AD. Esse usuário se tornará o Active Directory Directory Service (AD DS) Connector account forEntra Connect Sync. Para obter etapas detalhadas desse processo, consultethe section called “Criar um usuário”.

Etapa 2: Baixar Entra Connect Sync

- Faça o download Entra Connect Sync do Microsoftsite para a instância EC2 que é a AWS administradora do Microsoft AD gerenciado.

> **Warning**
>
> Não abra nem corra neste Entra Connect Sync momento. As próximas etapas fornecerão as permissões necessárias para o usuário do seu domínio criado na Etapa 1.

Etapa 3: Executar Windows PowerShell script

- Abra PowerShell como administrador e execute o script a seguir. Enquanto o script estiver em execução, você deverá inserir o SaM AccountNamepara o usuário do domínio recém-criado na Etapa 1.

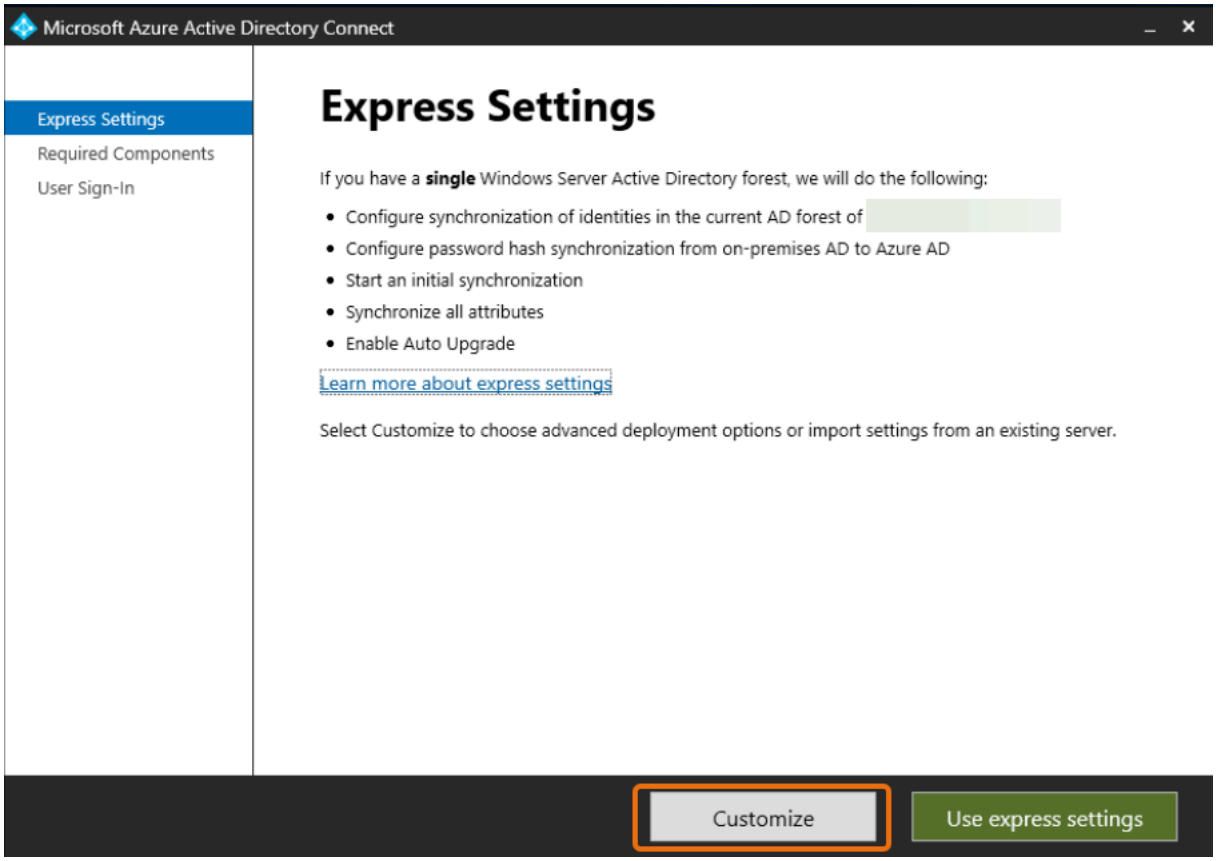
```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"

try {
    # Attempt to import the module
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."
    Import-Module $modulePath -ErrorAction Stop
    Write-Host -ForegroundColor Green "Success!"
}
catch {
    # Display the exception message
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"
}

Function Set-EntraConnectSvcPerms {
    [CmdletBinding()]
    Param (
```

```
        [String]$ServiceAccountName
    )

    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator

    Try {
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }

    $BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
    $Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

    Try {
        $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
    }

    Try {
        $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
 Stop | Select-Object -ExpandProperty 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get service account DN $_"
    }

    Foreach ($OU in $OUs) {
        try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
 $ADConnectorAccountDN -ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
 on OU $OU"
    }
    catch {
        Write-Host "An error occurred while setting permissions for
 $ADConnectorAccountDN on OU $OU : $_"
    }
```

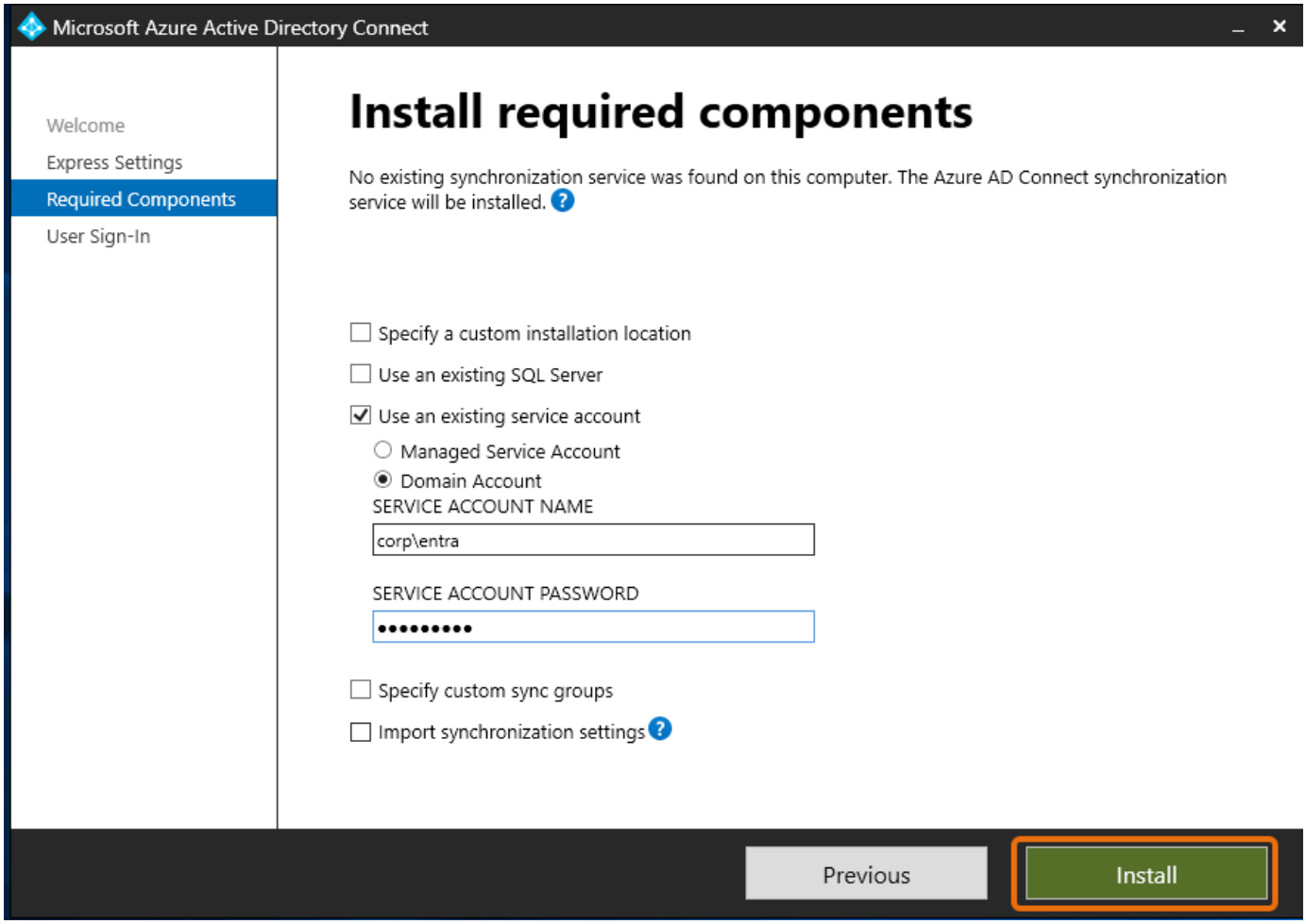
```
    }
}
```

Etapa 4: instalar Entra Connect Sync

1. Depois que o script for concluído, você poderá executar o arquivo de configuração baixado Microsoft Entra Connect (anteriormente conhecido comoAzure Active Directory Connect).
2. Uma Microsoft Azure Active Directory Connect janela é aberta após a execução do arquivo de configuração da etapa anterior. Na janela Configurações expressas, selecione Personalizar.



3. Na janela Instalar componentes necessários, marque a caixa de seleção Usar uma conta de serviço existente. Em NOME DA CONTA DE SERVIÇO e SENHA DA CONTA DE SERVIÇO, insira o AD DS Connector account nome e a senha do usuário que você criou na Etapa 1. Por exemplo, se seu AD DS Connector account nome for`entra`, o nome da conta seria`corp\entra`. Em seguida, selecione Instalar.



4. Na janela Login do usuário, selecione uma das seguintes opções:

   a. Autenticação de passagem - Essa opção permite que você faça login Active Directory com seu nome de usuário e senha.

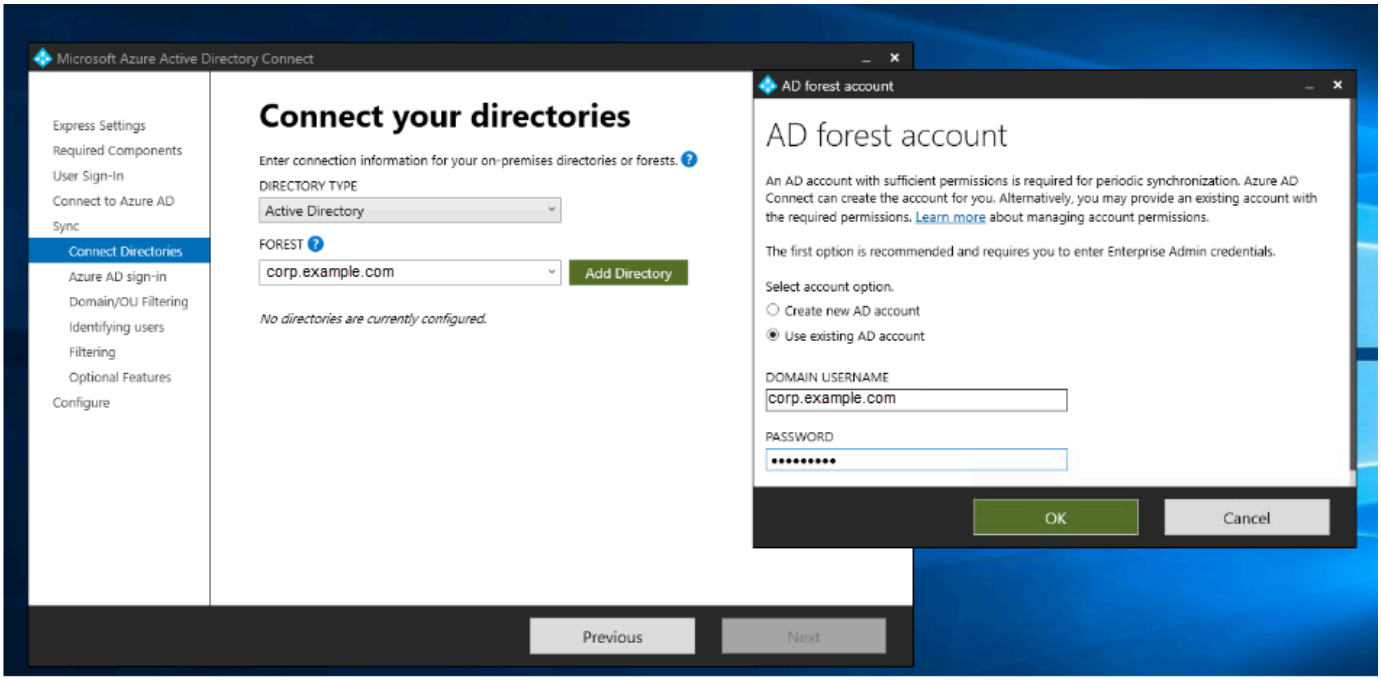
   b. Não configurar - Isso permite que você use o login federado com Microsoft Entra (anteriormente conhecido como Azure Active Directory (AzureAD)) ou. Office 365

   Depois, selecione Próximo.

5. Na Azure janela Connect to, digite seu nome de usuário e senha de administrador global Entra ID e selecione Avançar.

6. Na janela Conectar seus diretórios, escolha TIPO Active DirectoryDE DIRETÓRIO. Escolha a floresta para seu Microsoft AD AWS gerenciado para FOREST. Em seguida, selecione Adicionar diretório.

7. Uma caixa pop-up aparece solicitando as opções da sua conta. Selecione Usar conta AD existente. Digite o AD DS Connector account nome de usuário e a senha criados na Etapa 1 e selecione OK. Depois, selecione Próximo.



8. Azure ADNa janela de login, selecione Continuar sem associar todos os sufixos UPN aos domínios verificados, somente se você não tiver um domínio personalizado verificado adicionado. Entra ID Depois, selecione Próximo.
9. Na janela de filtragem de domínio/OU, selecione as opções que atendem às suas necessidades. Para obter mais informações, consulte Entra Connect Sync: Configurar a filtragem na Microsoft documentação. Depois, selecione Próximo.
10. Na janela Identificação de usuários, filtragem e recursos opcionais, mantenha os valores padrão e selecione Avançar.
11. Na janela Configurar, revise as configurações e selecione Configurar. A instalação do formulário Entra Connect Sync será finalizada e os usuários começarão a sincronizar com. Microsoft Entra ID

Estender seu esquema

O AWS Managed Microsoft AD usa esquemas para organizar e impor a maneira como os dados do diretório são armazenados. O processo de adicionar definições ao esquema é conhecido como "estendendo o esquema". As extensões do esquema possibilitam modificar o esquema do diretório do AWS Managed Microsoft AD usando um arquivo LDAP Data Interchange Format (LDIF) válido.

Para obter mais informações sobre os esquemas do AD e como estender seu esquema, consulte os tópicos listados a seguir.

Tópicos

- Quando estender seu esquema do AWS Managed Microsoft AD
- Tutorial: Estendendo seu esquema AWS gerenciado do Microsoft AD

Quando estender seu esquema do AWS Managed Microsoft AD

Você pode estender o esquema do AWS Managed Microsoft AD adicionando novas classes e atributos de objeto. Por exemplo, você pode fazer isso quando tiver um aplicativo que exija alterações no esquema para oferecer suporte aos recursos de logon único.

Você também pode usar extensões de esquema para permitir suporte para aplicativos que dependem de classes e atributos de objetos específicos ao Active Directory. Isso pode ser especialmente útil quando você precisa migrar aplicações corporativas que são dependentes do AWS Managed Microsoft AD para a Nuvem AWS.

Cada atributo ou classe adicionado a um esquema do Active Directory existente deve ser definido com um ID exclusivo. Dessa forma quando as empresas adicionarem extensões ao esquema, elas poderão ter a garantia de serem exclusivas e não entrarem em conflito umas com as outras. Esses IDs são conhecidos como identificadores de objetos do AD (OIDs) e são armazenados no AWS Managed Microsoft AD.

Para começar, consulte o Tutorial: Estendendo seu esquema AWS gerenciado do Microsoft AD.

Tópicos relacionados

- Estender seu esquema
- Elementos do esquema

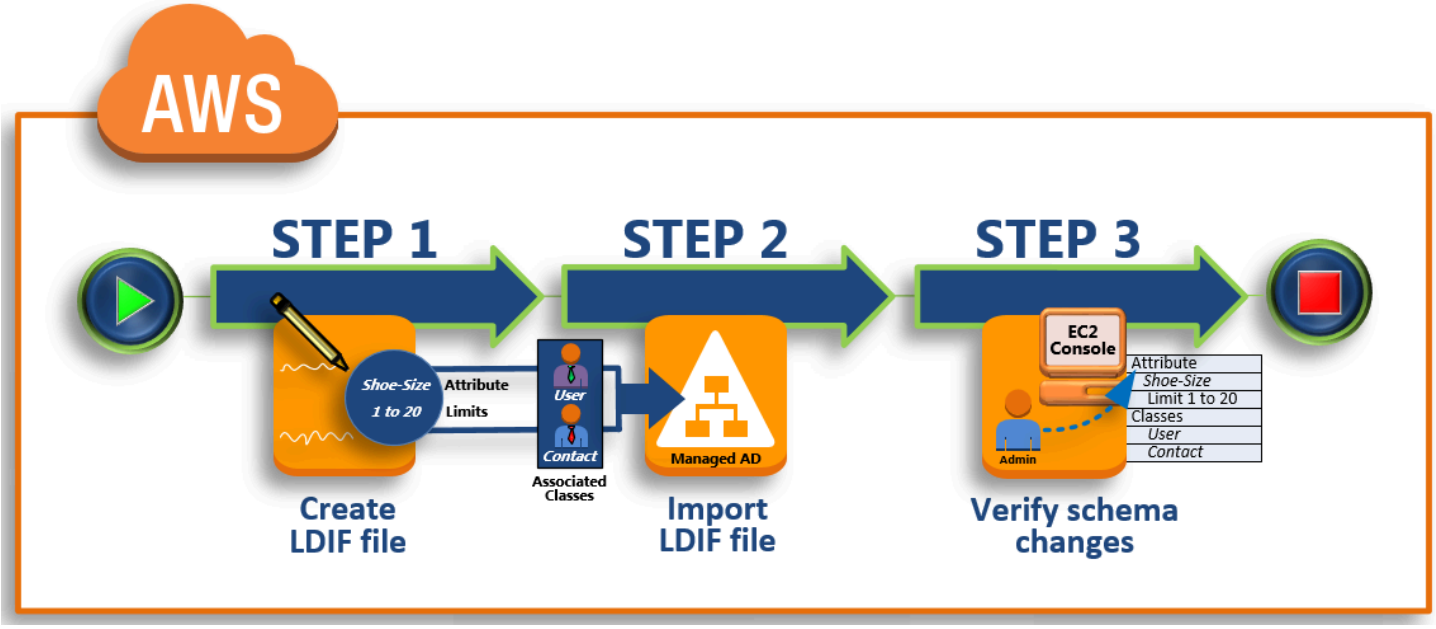
Tutorial: Estendendo seu esquema AWS gerenciado do Microsoft AD

Neste tutorial, você aprenderá como estender o esquema do AWS diretório Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD, adicionando atributos e classes exclusivos que atendam aos seus requisitos específicos. AWS As extensões de esquema gerenciadas do Microsoft AD só podem ser carregadas e aplicadas usando um arquivo de script LDIF (Lightweight Directory Interchange Format) válido.

Os atributos (attributeSchema) definem os campos no banco de dados, enquanto as classes (classSchema) definem as tabelas no banco de dados. Por exemplo, todos os objetos de usuário no Active Directory estão definidos pela classe de esquema User, enquanto as propriedades individuais do usuário, como endereço de e-mail ou número de telefone, são definidas por um atributo.

Se você quiser adicionar uma nova propriedade, como Shoe-Size, seria preciso definir um novo atributo do tipo integer. Você também pode definir limites inferior e superior, como 1 a 20. Após o objeto attributeSchema Shoe-Size ser criado, você alteraria o objeto de classSchema User para conter o atributo. Atributos podem ser vinculados a várias classes. O Shoe-Size também poderia ser adicionado à classe Contact, por exemplo. Para obter mais informações sobre esquemas do Active Directory, consulte Quando estender seu esquema do AWS Managed Microsoft AD.

Esse fluxo de trabalho tem três etapas básicas.



Etapa 1: criar seu arquivo LDIF

Primeiro, crie um arquivo LDIF e defina os novos atributos e todas as classes aos quais os atributos devem ser adicionados. Você usa esse arquivo para a próxima fase do trabalho.

Etapa 2: importar seu arquivo LDIF

Nesta etapa, você usa o AWS Directory Service console para importar o arquivo LDIF para seu ambiente Microsoft Active Directory.

Etapa 3: verificar se a extensão do esquema obteve êxito

Por fim, como administrador, você usa uma instância do EC2 para verificar se as novas extensões são exibidas no snap-in do esquema do Active Directory.

Etapa 1: criar seu arquivo LDIF

Um arquivo LDIF é um formato de intercâmbio de dados de texto simples padrão para representar o conteúdo do diretório do LDAP e atualizar solicitações. O LDIF transporta conteúdo do diretório como conjunto de registros, um registro para cada objeto (ou entrada). Isso também representa solicitações de atualização, como Adicionar, Modificar, Excluir e Renomear, como um conjunto de registros – um registro para cada solicitação de atualização.

As AWS Directory Service importações do arquivo LDIF com as alterações de esquema ao executar o `ldifde.exe` aplicativo em seu diretório gerenciado do AWS Microsoft AD. Portanto, você achará útil entender a sintaxe do script em LDIF. Para obter mais informações, consulte Scripts em LDIF.

Diversas ferramentas de LDIF de terceiros podem extrair, limpar e atualizar suas atualizações do esquema. Independentemente da ferramenta a ser usada, é importante compreender que todos os identificadores usados no arquivo LDIF devem ser exclusivos.

Recomendamos enfaticamente que você revise os conceitos e dicas a seguir antes de criar seu arquivo LDIF.

- Elementos do esquema: saiba mais sobre elementos do esquema, como atributos, classes, IDs de objeto e atributos vinculados. Para ter mais informações, consulte Elementos do esquema.

- Sequência itens: certifique-se de que a ordem na qual os itens do seu arquivo LDIF são apresentados segue a Directory Information Tree (DIT) de cima para baixo. As regras gerais para o sequenciamento em um arquivo LDIF incluem o seguinte:

  - Itens separados com uma linha em branco.
  - Liste os itens-filho de lista após os itens-pai.
  - Verifique se itens como atributos ou classes de objeto existem no esquema. Se não estiverem presentes, será preciso adicioná-los ao esquema antes de serem usados. Por exemplo, antes de você atribuir um atributo a uma classe, o atributo deverá ser criado.
- Formato do DN: para cada instrução nova no arquivo LDIF, defina o nome diferenciado (DN) como a primeira linha da instrução. O DN identifica um objeto do Active Directory dentro da árvore

de objeto do Active Directory e deve conter os componentes de domínio do seu diretório. Por exemplo, os componentes de domínio do diretório neste tutorial são `DC=example,DC=com`.

O DN também deve conter o nome comum (CN) do objeto do Active Directory. A primeira entrada de NC é o nome de classe ou atributo. Depois, você deve usar `CN=Schema,CN=Configuration`. Esse CN garante que você possa expandir o esquema do Active Directory. Como mencionado antes, você não pode adicionar nem modificar o conteúdo dos objetos do Active Directory. O formato geral para um DN vem a seguir.

```
dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
```

Para este tutorial, o DN para o novo atributo Shoe-Size seria da seguinte forma:

```
dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
```

- Avisos – Reveja os avisos abaixo antes de ampliar seu esquema.
  - Antes de você estender seu esquema do Active Directory, é importante analisar os avisos da Microsoft sobre o impacto dessa operação. Para obter mais informações, consulte O que você precisa saber antes de ampliar o esquema.
  - Você não pode excluir um atributo nem uma classe do esquema. Portanto, se cometer um erro e não quiser restaurar a partir backup, só poderá desabilitar o objeto. Para mais informações, consulte Desabilitação de classes e atributos existentes.
  - As alterações em não defaultSecurityDescriptor são suportadas.

Para saber mais sobre como os arquivos LDIF são criados e ver um exemplo de arquivo LDIF que pode ser usado para testar extensões do esquema gerenciado AWS do Microsoft AD, consulte o artigo Como estender seu esquema de diretório gerenciado do AWS Microsoft AD no blog de segurança. AWS

Próxima etapa

Etapa 2: importar seu arquivo LDIF

Etapa 2: importar seu arquivo LDIF

Você pode estender seu esquema importando um arquivo LDIF do AWS Directory Service console ou usando a API. Para obter mais informações sobre como fazer isso com as APIs de extensão do esquema, consulte Referência da API do AWS Directory Service . No momento, a AWS não oferece

suporte a aplicativos externos, como Microsoft Exchange, para executar diretamente atualizações do esquema.

> **Important**
>
> Quando você faz uma atualização no esquema de diretório AWS gerenciado do Microsoft AD, a operação não é reversível. Em outras palavras: assim que você criar uma classe ou um atributo novos, o Active Directory não permitirá que você os remova. No entanto, você poderá desabilitá-lo.
>
> Se você precisar excluir as alterações do esquema, uma opção é restaurar o diretório de um snapshot anterior. Restaurar um snapshot rola tanto o esquema quanto os dados do diretório de volta para um ponto anterior, não apenas o esquema. Observe que a idade máxima aceita para um snapshot é 180 dias. Para obter mais informações, consulte Prazo de validade útil de um backup de estado do sistema do Active Directory no site da Microsoft.

Antes do início do processo de atualização, o AWS Managed Microsoft AD tira um instantâneo para preservar o estado atual do seu diretório.

> **Note**
>
> As extensões de esquema são um recurso global do AWS Managed Microsoft AD. Se você estiver usando o Replicação em várias regiões, os procedimentos a seguir deverão ser executados no Região principal. As alterações serão aplicadas automaticamente em todas as regiões replicadas. Para ter mais informações, consulte Recursos globais versus regionais.

Para importar seu arquivo LDIF

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:

   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Manutenção. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Manutenção.

4. Na seção Schema extensions (Extensões do esquema), selecione Actions (Ações) e selecione Upload and update schema (Carregar e atualizar esquema).
5. Na caixa de diálogo, clique em Browse, selecione um arquivo LDIF válido, digite uma descrição e escolha Update Schema.

> **Important**
>
> Estender o esquema é uma operação essencial. Não aplique nenhuma atualização do esquema no ambiente de produção sem primeiro testá-lo com seu aplicativo em um ambiente de desenvolvimento ou de teste.

Como o arquivo LDIF é aplicado

Após o upload do arquivo LDIF, o AWS Managed Microsoft AD toma medidas para proteger seu diretório contra erros, pois aplica as alterações na seguinte ordem.

1. Valida o arquivo LDIF. Como os scripts LDIF podem manipular qualquer objeto no domínio, o Managed AWS Microsoft AD executa verificações logo após o upload para ajudar a garantir que a operação de importação não falhe. Isso inclui verificações para garantir o seguinte:
   - Os objetos a serem atualizados são mantidos somente no contêiner do esquema
   - A parte DC (controladores de domínio) corresponde ao nome de domínio onde o script de LDIF está sendo executado
2. Faz um snapshot do seu diretório. Você pode usar o snapshot para restaurar seu diretório no caso de encontra problemas com seu aplicativo após atualizar o esquema.
3. Aplica as alterações a um único DC. AWS O Microsoft AD gerenciado isola um de seus DCs e aplica as atualizações no arquivo LDIF ao DC isolado. Em seguida, ele seleciona um dos seus DCs para ser o esquema principal, remove esse DC da replicação de diretórios e aplica seu arquivo LDIF usando. `Ldifde.exe`
4. A replicação ocorre em todos os DCs. AWS O Microsoft AD gerenciado adiciona o DC isolado novamente à replicação para concluir a atualização. Quando isso tudo estiver acontecendo, seu diretório continuará a prestar o serviço do Active Directory aos seus aplicativos sem interrupções.

Próxima etapa

Etapa 3: verificar se a extensão do esquema obteve êxito

Etapa 3: verificar se a extensão do esquema obteve êxito

Depois de concluir o processo de importação, é importante verificar se as atualizações do esquema foram aplicadas ao diretório. Isso é especialmente crítico antes de migrar ou atualizar qualquer aplicativo que depende da atualização do esquema. Você pode fazer isso usando uma variedade de ferramentas diferentes de LDAP ou gravando uma ferramenta de teste que emita os comandos LDAP apropriados.

Esse procedimento usa o Snap-in do Esquema do Active Directory e/ou PowerShell para verificar se as atualizações do esquema foram aplicadas. Você deve executar essas ferramentas em um computador que esteja associado ao seu Microsoft AD AWS gerenciado. Isso pode ser um Windows Server em execução na sua rede on-premises com acesso à sua nuvem privada virtual (VPC) ou por meio de uma conexão de rede privada virtual (VPN). Você também pode executar essas ferramentas em uma instância Windows do Amazon EC2 (consulte Como executar uma nova instância do EC2 com associação direta a um domínio).

Para verificar usando o snap-in do esquema do Active Directory

1. Instale o Snap-In do Esquema do Active Directory usando as instruções no site. TechNet
2. Abra o Microsoft Management Console (MMC) e expanda a árvore AD Schema para o seu diretório.
3. Navegue nas pastas Classes e Attributes até encontrar as alterações do esquema feitas anteriormente.

Para verificar usando PowerShell

1. Abra uma PowerShell janela.
2. Use o cmdlet `Get-ADObject` como mostrado abaixo para verificar a alteração do esquema. Por exemplo: .

```
get-adobject -Identity 'CN=Shoe-
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

Etapa opcional

Adicionar um valor ao novo atributo - Opcional

Adicionar um valor ao novo atributo - Opcional

Use essa etapa opcional quando tiver criado um novo atributo e quiser adicionar um novo valor ao atributo em seu diretório AWS gerenciado do Microsoft AD.

Para adicionar um valor a um atributo

1. Abra o utilitário de linha de Windows PowerShell comando e defina o novo atributo com o comando a seguir. Neste exemplo, nós adicionaremos o novo valor de EC2InstanceID ao atributo para um computador específico.

   ```
   PS C:\> set-adcomputer -Identity computer name -add @{example-
   EC2InstanceID = 'EC2 instance ID'}
   ```

2. É possível validar se o valor de EC2InstanceID foi adicionado ao objeto do computador executando o seguinte comando:

   ```
   PS C:\> get-adcomputer -Identity computer name –Property example-
   EC2InstanceID
   ```

Recursos relacionados

Os links de recursos a seguir estão localizados no site da Microsoft e fornecem informações relacionadas.

- Estendendo o esquema (Windows)
- Esquema do Active Directory (Windows)
- Esquema do Active Directory
- Administração do Windows: Estendendo o Active Directory Schema
- Restrições sobre a extensão do esquema (Windows)
- Ldifde

Mantenha seu diretório AWS gerenciado do Microsoft AD

Esta seção descreve como manter tarefas administrativas comuns em seu ambiente Microsoft AD AWS gerenciado.

Tópicos

- Adicionar sufixos UPN alternativos
- Exclua seu Microsoft AD AWS gerenciado
- Renomear o site do diretório
- Criar um snapshot ou restaurar seu diretório
- Atualize seu Microsoft AD AWS gerenciado
- Visualizar informações do diretório

Adicionar sufixos UPN alternativos

É possível simplificar o gerenciamento dos nomes de login do Active Directory (AD) e melhorar a experiência de login do usuário ao adicionar sufixos alternativos de nome principal do usuário (UPN) ao diretório do AWS Managed Microsoft AD. Para fazer isso, você deve fazer login com a conta de Admin ou com uma conta que seja membro do grupo de Administradores delegados de sufixo de nome de entidade principal de usuário da AWS. Para obter mais informações sobre esse grupo, consulte O que é criado com seu Microsoft AD Active Directory AWS gerenciado.

Para adicionar sufixos UPN alternativos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Localize uma instância da instância do Amazon EC2 associada a seu diretório do AWS Managed Microsoft AD. Selecione a instância e escolha Conectar.
3. Na janela Server Manager (Gerenciador de servidores), escolha Tools (Ferramentas). Depois, escolha Active Directory Domains and Trusts (Domínios e confianças do Ative Directory).
4. No painel esquerdo, clique com o botão direito do mouse em Active Directory Domains and Trusts (Domínios e confianças do Ative Directory) e escolha Properties (Propriedades).
5. Na guia UPN Suffixes (Sufixos UPN), digite um sufixo UPN alternativo (como **`sales.example.com`**). Escolha Add (Adicionar) e escolha Apply (Aplicar).
6. Se for necessário adicionar mais sufixos UPN alternativos, repita a etapa 5 até ter os sufixos UPN necessários.

Exclua seu Microsoft AD AWS gerenciado

Quando um Microsoft AD AWS gerenciado é excluído, todos os dados e instantâneos do diretório são excluídos e não podem ser recuperados. Após a exclusão do diretório, todas as instâncias agregadas ao diretório permanecem intactas. No entanto, você não pode usar as credenciais do

diretório para fazer login nessas instâncias. Em tais instâncias, você deve fazer login com uma conta de usuário local para a instância.

Como excluir um diretório

1. No painel de navegação do console do AWS Directory Service selecione Diretórios. Certifique-se de que você está no Região da AWS local onde o seu Active Directory está implantado. Para obter mais informações, consulte Escolha de uma região.
2. Certifique-se de que nenhum AWS aplicativo esteja habilitado para o diretório que você pretende excluir. AWS Os aplicativos habilitados impedirão que você exclua seu AWS Managed Microsoft AD ou Simple AD.

   a. Na página Directories (Diretórios), escolha o ID do diretório.

   b. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos). Na seção AWS aplicativos e serviços, você vê quais AWS aplicativos estão habilitados para o seu diretório.

      - Desative AWS Management Console o acesso. Para ter mais informações, consulte Desabilitar o acesso ao AWS Management Console.
      - Para desativar a Amazon WorkSpaces, você deve cancelar o registro do serviço no diretório no WorkSpaces console. Para obter mais informações, consulte Cancelamento do registro de um diretório no Amazon WorkSpaces Administration Guide.
      - Para desativar a Amazon WorkDocs, você deve excluir o WorkDocs site da Amazon no WorkDocs console da Amazon. Para obter mais informações, consulte Excluir um site no Guia de WorkDocs Administração da Amazon.
      - Para desativar a Amazon WorkMail, você deve remover a WorkMail organização da Amazon no WorkMail console da Amazon. Para obter mais informações, consulte Remover uma organização no Amazon WorkMail Administrator Guide.
      - Para desabilitar o Amazon FSx para Windows File Server, é necessário remover o sistema de arquivos Amazon FSx do domínio. Para obter mais informações, consulte Trabalhando com Active Directory o FSx for Windows File Server no Guia do usuário do Amazon FSx for Windows File Server.
      - Para desabilitar o Amazon Relational Database Service, é necessário remover a instância do Amazon RDS do domínio. Para obter mais informações, consulte Gerenciar uma instância de banco de dados em um domínio no Guia do usuário do Amazon RDS.

- Para desativar o AWS Client VPN serviço, você deve remover o serviço de diretório do Client VPN Endpoint. Para obter mais informações, consulte Active DirectoryAutenticação no Guia AWS Client VPN do Administrador.
- Para desabilitar o Amazon Connect, exclua a instância do Amazon Connect. Para obter mais informações, consulte Excluir uma instância do Amazon Connect no Guia de administração do Amazon Connect.
- Para desativar a Amazon QuickSight, você deve cancelar a assinatura da Amazon QuickSight. Para obter mais informações, consulte Fechar sua Amazon QuickSight conta no Guia QuickSight do usuário da Amazon.

> **Note**
>
> Se você o estiver usando AWS IAM Identity Center e já o tiver conectado ao diretório AWS gerenciado do Microsoft AD que planeja excluir, primeiro altere a fonte de identidade antes de excluí-la. Para obter mais informações, consulte Alterar sua fonte de identidade no Guia do usuário do Centro de Identidade do IAM.

3. No painel de navegação, selecionar Diretórios.
4. Selecione somente o diretório a ser excluído e clique em Excluir. A exclusão do diretório demora vários minutos. Quando o diretório for excluído, ele será removido da sua lista de diretórios.

Renomear o site do diretório

Você pode renomear o site padrão do diretório do AWS Managed Microsoft AD para que ele corresponda aos nomes de sites do Microsoft Active Directory (AD) existente. Assim, o AWS Managed Microsoft AD pode encontrar e autenticar com mais rapidez os usuários existentes do AD em seu on-premises. O resultado é uma melhor experiência quando os usuários acessam recursos da AWS, como instâncias do Amazon EC2 e Amazon RDS para SQL Server que você associou ao diretório do AWS Managed Microsoft AD.

Para fazer isso, você deve estar conectado à conta de Admin ou uma conta que seja membro do grupo de Administradores de sites e serviços delegados da AWS. Para obter mais informações sobre esse grupo, consulte O que é criado com seu Microsoft AD Active Directory AWS gerenciado.

Para ver os benefícios adicionais de renomear o site em relação a confianças, consulte Domain Locator Across a Forest Trust no site da Microsoft.

Para renomear o site do AWS Managed Microsoft AD

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Localize uma instância da instância do Amazon EC2 associada a seu diretório do AWS Managed Microsoft AD. Selecione a instância e escolha Conectar.
3. Na janela Server Manager (Gerenciador de servidores), escolha Tools (Ferramentas). E escolha Active Directory Sites and Services (Sites e serviços do Ative Directory).
4. No painel esquerdo, expanda a pasta Sites, clique com o botão direito do mouse no nome do site (o padrão é Default-Site-Name) e escolha Renomear.
5. Digite o novo nome do site e escolha Inserir.

Criar um snapshot ou restaurar seu diretório

AWS Directory Service fornece instantâneos diários automatizados e a capacidade de tirar instantâneos manuais dos dados para seu AWS Microsoft AD Active Directory gerenciado. Esses instantâneos podem ser usados para realizar uma point-in-time restauração para o Active Directory. Você está limitado a cinco instantâneos manuais para cada Microsoft AD Active Directory AWS gerenciado. Se já tiver atingido esse limite, deverá excluir um dos snapshots manuais existentes para poder criar outros. Não é possível criar snapshots de diretórios do AD Connector.

> **Note**
>
> O Snapshot é um recurso global do AWS Managed Microsoft AD. Se você estiver usando o Replicação em várias regiões, os procedimentos a seguir deverão ser executados no Região principal. As alterações serão aplicadas automaticamente em todas as regiões replicadas. Para ter mais informações, consulte Recursos globais versus regionais.

Tópicos

- Criar um snapshot do diretório
- Restaurar o diretório de um snapshot
- Excluir um snapshot

Criar um snapshot do diretório

Um snapshot pode ser usado para restaurar o diretório para o que ele era no momento em que o snapshot foi criado. Para criar um snapshot manual de seu diretório, execute as seguintes etapas.

> **Note**
>
> Há um limite de 5 snapshots manuais para cada diretório. Se já tiver atingido esse limite, deverá excluir um dos snapshots manuais existentes para poder criar outros.

Para criar um snapshot manual

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, escolha a guia Manutenção.
4. Na seção Snapshots, escolha Ações e, em seguida, selecione Criar snapshot.
5. Na caixa de diálogo Criar snapshot do diretório, forneça uma descrição do snapshot, se desejado. Quando estiver pronto, escolha Criar.

Dependendo do tamanho do diretório, vários minutos podem ser necessários para que o snapshot seja criado. Quando o snapshot estiver pronto, o valor do Status é alterado para `Completed`.

Restaurar o diretório de um snapshot

Restaurar um diretório a partir de um snapshot é equivalente a mover o diretório de volta no tempo. Cada snapshot de diretório é exclusivo do diretório do qual ele foi criado. Um snapshot só pode ser restaurado para o diretório do qual ele foi criado. Além disso, a idade máxima aceita para um snapshot manual é 180 dias. Para obter mais informações, consulte Prazo de validade útil de um backup de estado do sistema do Active Directory no site da Microsoft.

> **Warning**
>
> Recomendamos entrar em contato com o AWS Support Center antes de qualquer restauração de snapshot; talvez possamos ajudar a evitar a necessidade de fazer uma restauração de snapshot. Todas as restaurações de um snapshot podem causar perda de dados, pois elas são de um momento em específico. É importante compreender que todos

os servidores de DCs e DNS associados ao diretório ficarão offline até que a operação de restauração seja concluída.

Para restaurar o diretório a partir de um snapshot, execute as seguintes etapas.

Para restaurar um diretório a partir de um snapshot

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, escolha a guia Manutenção.
4. Na seção Snapshots, selecione um snapshot na lista, escolha Ações e, em seguida, selecione Restaurar snapshot.
5. Analise as informações na caixa de diálogo Restaurar snapsho de diretório e escolha Restaurar.

Para um diretório AWS gerenciado do Microsoft AD, pode levar de duas a três horas para que o diretório seja restaurado. Quando a restauração for concluída com êxito, o valor de Status do diretório será alterado para `Active`. Todas as alterações feitas no diretório depois da data do snapshot serão sobrescritas.

Excluir um snapshot

Para excluir um snapshot

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, escolha a guia Manutenção.
4. Na seção Snapshots, escolha Ações e, em seguida, selecione Excluir snapshot.
5. Verifique se você deseja excluir o snapshot e escolha Excluir.

Atualize seu Microsoft AD AWS gerenciado

Você pode atualizar sua edição Standard AWS Managed Microsoft AD Active Directory para a edição Enterprise entrando em contato com AWS Support. Para obter mais informações, consulte Criação de casos de suporte e gerenciamento de casos no Guia AWS Support do usuário.

Note

A replicação multirregional só está disponível na edição AWS Managed Microsoft AD Enterprise para as seguintes regiões:

- Leste dos EUA (Ohio)
- Leste dos EUA (N. da Virgínia)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- África (Cidade do Cabo)
- Ásia-Pacífico (Hong Kong)
- Asia Pacific (Mumbai)
- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Osaka)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Oeste do Canadá (Calgary)
- China (Pequim)
- China (Ningxia)
- Europa (Frankfurt)
- Europa (Zurique)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Paris)
- Europa (Estocolmo)
- Europa (Milão)
- Europa (Espanha)

- Israel (Tel Aviv)
- Oriente Médio (Barém)
- Oriente Médio (Emirados Árabes Unidos)
- América do Sul (São Paulo)
- AWS GovCloud (Oeste dos EUA)
- AWS GovCloud (Leste dos EUA)

Há algumas limitações a serem observadas ao atualizar seu Microsoft AD AWS gerenciado. Eles são:

- O upgrade terá um custo adicional. Consulte Definição de preço do AWS Directory Service para obter mais informações.
- Depois que o Active Directory for atualizado, ele não poderá ser revertido para a edição anterior.
- Os instantâneos anteriores não podem ser usados para restaurar o Active Directory após o upgrade.
- Os upgrades ocorrem em uma data e hora programadas acordadas com AWS Support. Os upgrades ocorrem de segunda a sexta-feira, das 9h às 17h, horário padrão do Pacífico.
- O processo de atualização requer de quatro a cinco horas.
- Durante o processo de atualização, os controladores de domínio do seu Microsoft AD AWS gerenciado são atualizados um por vez. Isso pode afetar negativamente seu desempenho e causar tempo de inatividade durante a janela de manutenção.
- Se seus aplicativos estiverem usando os nomes de host ou endereços IP dos controladores de domínio em vez do nome de domínio do Active Directory, esses aplicativos precisarão ser atualizados.
- Se você estiver usando LDAPS (Lightweight Directory Access Protocol over SSL), os controladores de domínio precisarão de novos certificados.

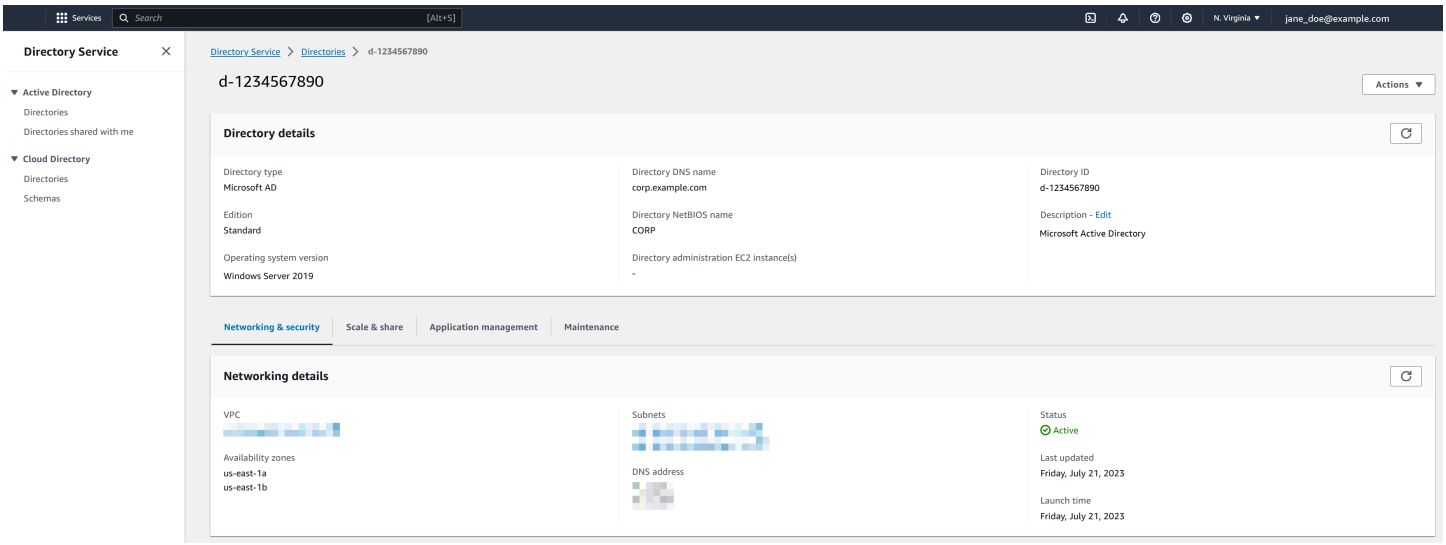
Visualizar informações do diretório

É possível visualizar informações detalhadas sobre um diretório.

Para visualizar informações detalhadas do diretório

1. No painel de navegação do AWS Directory Service console, em Active Directory, selecione Diretórios.
2. Clique no link de ID de seu diretório. As informações sobre o diretório são exibidas na página Detalhes do diretório.

Para obter mais informações sobre o campo Status, consulte Noções básicas sobre o status do diretório.



Conceder a usuários e grupos acesso aos recursos da AWS

AWS Directory Service fornece a capacidade de dar aos usuários e grupos do seu diretório acesso a AWS serviços e recursos, como acesso ao console do Amazon EC2. Semelhante à concessão aos usuários do IAM acesso para gerenciar diretórios conforme descrito emPolíticas baseadas em identidade (políticas do IAM), para que os usuários do seu diretório tenham acesso a outros AWS recursos, como o Amazon EC2, você deve atribuir funções e políticas do IAM a esses usuários e grupos. Para obter mais informações, consulte Funções do IAM no Guia do usuário do IAM.

Para obter informações sobre como conceder aos usuários acesso ao AWS Management Console, consulteHabilitar acesso ao AWS Management Console com as credenciais do AD.

Tópicos

- Criar um perfil
- Editar a relação de confiança para um perfil existente

- Atribuir usuários ou grupos a um perfil existente
- Visualizar usuários e grupos atribuídos a um perfil
- Remover um usuário ou grupo de um perfil
- Usar as políticas gerenciadas da AWS com o AWS Directory Service

Criar um perfil

Se precisar criar uma nova função do IAM para uso com AWS Directory Service, você deve criá-la usando o console do IAM. Depois que a função for criada, você deverá configurar uma relação de confiança com essa função antes de poder vê-la no AWS Directory Service console. Para ter mais informações, consulte Editar a relação de confiança para um perfil existente.

> **Note**
>
> O usuário que executa essa tarefa deve ter permissão para executar as seguintes ações do IAM Para ter mais informações, consulte Políticas baseadas em identidade (políticas do IAM).
>
> - objetivo: PassRole
> - objetivo: GetRole
> - objetivo: CreateRole
> - objetivo: PutRolePolicy

Para criar um novo perfil no console do IAM

1. No painel de navegação do console do IAM, escolha Perfis. Para obter mais informações, consulte Criar um perfil (AWS Management Console) no Guia do usuário do IAM.
2. Selecione Criar função.
3. Em Choose the service that will use this role (Selecionar o serviço que usará esta função), selecione Directory Service (Serviço de diretório) e Next: Permissions (Próximo: Permissões).
4. Marque a caixa de seleção ao lado da política (por exemplo, AmazonEC2 FullAccess) que você deseja aplicar aos usuários do seu diretório e, em seguida, escolha Avançar.
5. Se necessário, adicione uma tag à função e selecione Next (Próximo).
6. Forneça um Role name (Nome de função) e uma Description (Descrição) opcional e selecione Create role (Criar função).

Exemplo: criar uma função para habilitar o acesso ao AWS Management Console

A lista de verificação a seguir fornece um exemplo das tarefas que você deve concluir para criar uma nova função que concederá a usuários específicos do diretório acesso ao console do Amazon EC2.

1. Crie uma função com o console do IAM usando o procedimento anterior. Quando solicitado a fornecer uma política, escolha FullAccessAmazonEC2.
2. Use as etapas em Editar a relação de confiança para um perfil existente para editar a função que você acabou de criar e adicione as informações necessárias da relação de confiança ao documento de política. Essa etapa é necessária para que a função fique visível imediatamente após você habilitar o acesso à AWS Management Console na próxima etapa.
3. Siga as etapas em Habilitar acesso ao AWS Management Console com as credenciais do AD para configurar o acesso geral ao AWS Management Console.
4. Siga as etapas em Atribuir usuários ou grupos a um perfil existente para adicionar os usuários que precisam de acesso total aos recursos do EC2 à nova função.

Editar a relação de confiança para um perfil existente

Você pode atribuir suas funções existentes do IAM aos seus AWS Directory Service usuários e grupos. Para fazer isso, no entanto, a função deve ter uma relação de confiança com AWS Directory Service. Quando você usa AWS Directory Service para criar uma função usando o procedimento emCriar um perfil, essa relação de confiança é definida automaticamente. Basta estabelecer essa relação de confiança para os perfis do IAM que não são criados pelo AWS Directory Service.

Para estabelecer uma relação de confiança para uma função existente para AWS Directory Service

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, em Gerenciamento de acesso, escolha Perfis.

   O console exibe as funções de sua conta.
3. Escolha o nome da função que deseja modificar e, uma vez na página do perfil, selecione a guia Relações de confiança.
4. Escolha Editar política de confiança.
5. Em Editar política de confiança, cole o conteúdo a seguir e selecione Atualizar política.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Também é possível atualizar este documento de política usando a AWS CLI. Para obter mais informações, consulte update-trust na Referência de comandos da AWS CLI .

Atribuir usuários ou grupos a um perfil existente

Você pode atribuir uma função existente do IAM a um AWS Directory Service usuário ou grupo. Para fazer isso, verifique se você concluiu o seguinte.

Pré-requisitos

- Crie um Microsoft AD AWS gerenciado.
- Crie um usuário ou crie um grupo.
- Crie uma função que tenha uma relação de confiança com AWS Directory Service. Você pode editar a relação de confiança de uma função existente.

> **Note**
>
> O acesso para usuários em grupos aninhados no diretório não tem suporte. Os membros de grupo pai têm acesso ao console, mas os membros de grupos filho não têm.

Para atribuir usuários ou grupos a uma função do IAM existente

1. No painel de navegação do console do AWS Directory Service, em Active Directory, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.

3. Na página Detalhes do diretório, siga um destes procedimentos:

   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Gerenciamento de aplicações.
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja fazer suas atribuições e, em seguida, escolha a guia Gerenciamento de aplicações. Para ter mais informações, consulte Regiões principais versus adicionais.
4. Role para baixo até a AWS Management Consoleseção, escolha Ações e Ativar.
5. Na seção Acesso ao console de delegação, escolha o nome da função do IAM para a função existente do IAM à qual você deseja atribuir usuários.
6. Na página Selected role (Função selecionada), em Manage users and groups for this role (Gerenciar usuários e grupos para esta função), escolha Add (Adicionar).
7. Na página Adicionar usuários e grupos à função, em Selecionar floresta do Active Directory, escolha a floresta do AWS Microsoft Managed AD (esta floresta) ou a floresta on-premises (floresta confiável), a que contiver as contas que precisam de acesso ao AWS Management Console. Para obter mais informações sobre como configurar uma floresta confiável, consulte Tutorial: criar uma relação de confiança entre o diretório do AWS Managed Microsoft AD e seu domínio autogerenciado do Active Directory ..
8. Em Specify which users or groups to add (Especificar quais usuários ou grupos adicionar), selecione Find by user (Localizar por usuário) ou Find by group (Localizar por grupo) e digite o nome do usuário ou do grupo. Na lista de correspondências possíveis, escolha o usuário ou o grupo que você deseja adicionar.
9. Escolha Add (Adicionar) para concluir a atribuição dos usuários e grupos à função.

Visualizar usuários e grupos atribuídos a um perfil

Para visualizar os usuários e grupos atribuídos a uma função, execute as etapas a seguir.

Pré-requisitos

- Atribua seus usuários ou grupos a uma função existente.

Para visualizar usuários e grupos atribuídos a uma função

1. No painel de navegação do console do AWS Directory Service, em Active Directory, escolha Diretórios.

2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:

   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja visualizar suas atribuições e, em seguida, escolha a guia Gerenciamento de aplicações. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Gerenciamento de aplicações.
4. Na seção Delegar acesso ao console, escolha o perfil do IAM que deseja visualizar.
5. Na página Perfil selecionado, em Gerenciar usuários e grupos para este perfil, é possível visualizar os usuários e os grupos atribuídos ao perfil.

Remover um usuário ou grupo de um perfil

Para remover um usuário ou um grupo de uma função, execute as etapas a seguir.

Para remover um usuário ou grupo de uma função

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:

   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja remover suas atribuições e, em seguida, escolha a guia Gerenciamento de aplicações. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Gerenciamento de aplicações.
4. Na seção AWS Management Console, escolha o perfil que deseja visualizar.
5. Na página Selected role (Função selecionada), em Manage users and groups for this role (Gerenciar usuários e grupos para esta função), selecione os usuários ou grupos dos quais remover a função e escolha Remove (Remover). A função é removida dos usuários e grupos especificados, mas a função não é removida de sua conta.

Usar as políticas gerenciadas da AWS com o AWS Directory Service

O AWS Directory Service fornece as seguintes políticas gerenciadas da AWS para oferecer aos usuários e grupos acesso aos serviços e recursos da AWS, como acesso ao console do Amazon EC2. Você deve fazer login no AWS Management Console para poder visualizar essas políticas.

- Acesso somente leitura
- Acesso de usuário avançado
- Acesso total ao AWS Directory Service
- Acesso somente leitura ao AWS Directory Service
- Acesso total ao Amazon Cloud Directory
- Acesso somente leitura ao Amazon Cloud Directory
- Acesso total ao Amazon EC2
- Acesso somente leitura ao Amazon EC2
- Acesso total ao Amazon VPC
- Acesso somente leitura ao Amazon VPC
- Acesso total ao Amazon RDS
- Acesso somente leitura ao Amazon RDS
- Acesso total ao Amazon DynamoDB
- Acesso somente leitura ao Amazon DynamoDB
- Acesso total ao Amazon S3
- Acesso somente leitura ao Amazon S3
- Acesso total ao AWS CloudTrail
- Acesso somente leitura ao AWS CloudTrail
- Acesso total ao Amazon CloudWatch
- Acesso somente leitura ao Amazon CloudWatch
- Acesso total ao Amazon CloudWatch Logs
- Acesso somente leitura ao Amazon CloudWatch Logs

Para obter mais informações sobre como criar suas próprias políticas, consulte Políticas de exemplo para administração dos recursos da AWS no Guia do usuário do IAM.

Permita o acesso a AWS aplicativos e serviços

Os usuários podem autorizar o AWS Managed Microsoft AD a fornecer aos AWS aplicativos e serviços, como a Amazon WorkSpaces, acesso ao seuActive Directory. Os AWS aplicativos e serviços a seguir podem ser ativados ou desativados para funcionar com o Microsoft AD AWS gerenciado.

AWS aplicativo/serviço	Mais informações...
Amazon Chime	Para obter mais informações, consulte o Guia de administração do Amazon Chime.
Amazon Connect	Para obter mais informações, consulte o Guia de administração do Amazon Connect.
Amazon FSx para Windows File Server	Para obter mais informações, consulte Usando o Amazon FSx com o AWS Directory Service for Microsoft Active Directory.
Amazon QuickSight	Para obter mais informações, consulte o Guia QuickSight do usuário da Amazon.
Amazon Relational Database Service	Para obter mais informações, consulte o Guia do usuário do Amazon RDS.
Amazon WorkDocs	Para obter mais informações, consulte o Guia de WorkDocs administração da Amazon.
Amazon WorkMail	Para obter mais informações, consulte o Amazon WorkMail Administrator Guide.
Amazon WorkSpaces	Você pode criar um Simple AD, AWS Managed Microsoft AD ou AD Connector diretamente do WorkSpaces. Basta iniciar o Advanced Setup ao criar seu Workspace. Para obter mais informações, consulte o Guia de WorkSpaces administração da Amazon.

AWS aplicativo/serviço	Mais informações...
AWS Client VPN	Para mais informações, consulte o Guia do usuário do AWS Client VPN.
AWS IAM Identity Center	Para mais informações, consulte o Guia do usuário do AWS IAM Identity Center.
AWS License Manager	Para obter mais informações, consulte o Manual do usuário do License Manager.
AWS Management Console	Para ter mais informações, consulte Habilitar acesso ao AWS Management Console com as credenciais do AD.
AWS Private Certificate Authority	Para obter mais informações, consulte AWS Private CA Conector para Active Directory.
AWS Transfer Family	Para mais informações, consulte o Guia do usuário do AWS Transfer Family.

Após habilitado, você controla o acesso aos diretórios no console da aplicação ou do serviço ao qual deseja fornecer acesso ao diretório. Para encontrar os links de AWS aplicativos e serviços descritos acima no AWS Directory Service console, execute as etapas a seguir.

Para exibir os aplicativos e serviços para um diretório

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Revise a lista na seção de Aplicações e serviços da AWS .

Para obter mais informações sobre como autorizar ou desautorizar o uso AWS Directory Service de AWS aplicativos e serviços, consulte. Autorização para AWS aplicativos e serviços usando AWS Directory Service

Tópicos

Criar um URL de acesso

Um URL de acesso é usado com aplicações e serviços da AWS, como o Amazon WorkDocs, para acessar uma página de login associada a seu diretório. O URL deve ser globalmente exclusivo. Você pode criar uma URL de acesso para o diretório executando as seguintes etapas.

> **Warning**
>
> Depois de criar um URL de acesso ao aplicativo para esse diretório, ele não poderá ser alterado. Após o URL ser criado, ele não poderá ser usada por terceiros. Se você excluir o diretório, a URL de acesso também será excluída e poderá ser usada por qualquer outra conta.

> **Note**
>
> O URL de acesso só pode ser configurado a partir da região principal quando diretórios em várias regiões são usados.

Para criar uma URL de acesso

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Gerenciamento de aplicações. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Gerenciamento de aplicações.
4. Na seção Application access URL (URL de acesso ao aplicativo), se um URL de acesso não tiver sido atribuído ao diretório, o botão Create (Criar) será exibido. Digite um alias do diretório

e escolha Create (Criar). Se o erro A entidade já existe for retornado, o alias do diretório especificado já foi alocado. Escolha outro alias e repita esse procedimento.

Seu URL de acesso é exibido no formato *<alias>*.awsapps.com. Por padrão, esse URL levará você à página de login do Amazon WorkDocs.

Autenticação única

AWS Directory Service fornece a capacidade de permitir que seus usuários acessem a Amazon WorkDocs a partir de um computador associado ao diretório sem precisar inserir suas credenciais separadamente.

Antes de habilitar a autenticação única, é necessário executar etapas adicionais para permitir que os navegadores da Web dos usuários ofereçam suporte à autenticação única. Os usuários podem precisar modificar suas configurações de navegador da Web para habilitar a autenticação única.

> **Note**
>
> O logon único só funciona quando usado em um computador ingressado no diretório do AWS Directory Service . Não pode ser usado em computadores que não estão ingressados no diretório.

Se o diretório for um diretório do AD Connector e a conta de serviço do AD Connector não tiver a permissão para adicionar ou remover o atributo do nome da entidade principal de serviço, você terá duas opções para as etapas 5 e 6 abaixo:

1. Você poderá continuar e será solicitado o nome de usuário e a senha de um usuário do diretório que tenha essa permissão para adicionar ou remover o atributo do nome principal de serviço na conta de serviço do AD Connector. Essas credenciais são usadas apenas para habilitar a autenticação única e não são armazenadas pelo serviço. As permissões da conta de serviço do AD Connector não são alteradas.
2. Você pode delegar permissões para permitir que a conta de serviço do AD Connector adicione ou remova o atributo do nome principal do serviço em si mesma. Você pode executar os PowerShell comandos abaixo em um computador associado ao domínio usando uma conta que tenha permissões para modificar as permissões na conta de serviço do AD Connector. O comando abaixo permitirá que a conta de serviço do AD Connector adicione e remova um atributo de nome de entidade principal de serviço somente na própria conta.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Para ativar ou desativar o login único com a Amazon WorkDocs

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Na seção URL de acesso ao aplicativo, escolha Habilitar para habilitar o login único para a Amazon. WorkDocs

   Se você não vir o botão Habilitar, talvez seja necessário criar primeiro um URL de acesso para que essa opção seja exibida. Para obter mais informações sobre como criar uma URL de acesso, consulte Criar um URL de acesso.
5. Na caixa de diálogo Habilitar autenticação única para este diretório, escolha Habilitar. O logon único é habilitado para o diretório.
6. Se mais tarde você quiser desativar o login único com a Amazon WorkDocs, escolha Desativar e, na caixa de diálogo Desativar login único para este diretório, escolha Desativar novamente.

Tópicos

Autenticação única para IE e Chrome

Para permitir que os navegadores Microsoft Internet Explorer (IE) e o Google Chrome ofereçam suporte à autenticação única, as seguintes tarefas devem ser executadas no computador cliente:

- Adicione o URL de acesso (por exemplo, https://*<aliás>*.awsapps.com) à lista de sites aprovados para autenticação única.
- Ative o script ativo (JavaScript).
- Permita o login automático.
- Habilitar a autenticação integrada.

Você ou seus usuários podem executar essas tarefas manualmente, ou você pode alterar essas configurações usando as configurações da Política de grupo.

Tópicos

Atualização manual para autenticação única no Windows

Para habilitar manualmente a autenticação única em um computador Windows, execute as seguintes etapas no computador cliente. Algumas dessas configurações já podem estar definidas corretamente.

Para habilitar manualmente o logon único para o Internet Explorer e o Chrome no Windows

1. Para abrir a caixa de diálogo Internet Properties, feche o menu Start, digite `Internet Options` na caixa de pesquisa e escolha Internet Options.
2. Adicione a URL de acesso à lista de sites aprovados para logon único executando as etapas a seguir:

a. Na caixa de diálogo Internet Properties, selecione a guia Security.
b. Selecione Local intranet e escolha Sites.
c. Na caixa de diálogo Local intranet, escolha Advanced.
d. Adicione a URL de acesso à lista de sites e escolha Close.
e. Na caixa de diálogo Local intranet, escolha OK.

3. Para habilitar scripts ativos, execute as seguintes etapas:

a. Na guia Security da caixa de diálogo Internet Properties, escolha Custom level.
b. Na caixa de diálogo Security Settings - Local Intranet Zone, role para baixo até Scripting e selecione Enable em Active scripting.
c. Na caixa de diálogo Security Settings - Local Intranet Zone, escolha OK.

4. Para habilitar o login automático, execute as seguintes etapas:

a. Na guia Security da caixa de diálogo Internet Properties, escolha Custom level.
b. Na caixa de diálogo Security Settings - Local Intranet Zone, role para baixo até User Authentication e selecione Automatic logon only in Intranet zone em Logon.
c. Na caixa de diálogo Security Settings - Local Intranet Zone, escolha OK.
d. Na caixa de diálogo Security Settings - Local Intranet Zone, escolha OK.

5. Para habilitar a autenticação integrada, execute as seguintes etapas:

a. Na caixa de diálogo Internet Properties, selecione a guia Advanced.
b. Role para baixo até Security e selecione Enable Integrated Windows Authentication.
c. Na caixa de diálogo Internet Properties, escolha OK.

6. Feche e abra seu navegador novamente para que essas alterações entrem em vigor.

Atualização manual para autenticação única no OS X

Para habilitar manualmente a autenticação única para o Chrome no OS X, execute as seguintes etapas no computador cliente. Você precisará ter direitos de administrador no computador para concluir estas etapas.

Para habilitar manualmente logon único para o Chrome no OS X

1. Adicione seu URL de acesso à AuthServerAllowlistpolítica executando o seguinte comando:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Abra System Preferences, vá para o painel Profiles e exclua o perfil `Chrome Kerberos Configuration`.
3. Reinicie o Chrome e abra chrome://policy no Chrome para confirmar se as configurações estão implantadas.

Configurações da política de grupo para autenticação única

O administrador do domínio pode implementar as configurações da Política de grupo para fazer as alterações de logon único em computadores cliente ingressados no domínio.

> **Note**
>
> Se você gerencia os navegadores da Web Chrome nos computadores do seu domínio com as políticas do Chrome, você deve adicionar seu URL de acesso à AuthServerAllowlistpolítica. Para obter mais informações sobre como definir políticas do Chrome, acesse Configurações de políticas no Chrome.

Para habilitar o logon único manualmente para o Internet Explorer e o Chrome usando as configurações de Política de grupo

1. Crie um novo objeto de Política de grupo executando as seguintes etapas:
   a. Abra a ferramenta de gerenciamento de políticas de grupo, navegue até seu domínio e selecione Group Policy Objects.
   b. No menu principal, escolha Action e selecione New.
   c. Na caixa de diálogo Novo GPO, digite um nome descritivo para o objeto de política de grupo, como `IAM Identity Center Policy` e mantenha GPO iniciador de origem definido como (nenhum). Clique em OK.
2. Adicione a URL de acesso à lista de sites aprovados para logon único executando as etapas a seguir:
   a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Objetos de política de grupo, abra o menu de contexto (clique com o botão direito do mouse) da sua política do Centro de Identidade do IAM e escolha Editar.

b. Na árvore de políticas, navegue para User Configuration > Preferences > Windows Settings.

c. Na lista Windows Settings, abra o menu de contexto (clique com o botão direito do mouse) de Registry e escolha New registry item.

d. Na caixa de diálogo New Registry Properties, insira as configurações a seguir e escolha OK:

   Ação

   `Update`

   Hive

   `HKEY_CURRENT_USER`

   Path

   `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\`*`<alias>`*

   O valor de *`<alias>`* é derivado do URL de acesso. Se sua URL de acesso for `https://examplecorp.awsapps.com`, o alias será `examplecorp`, e a chave do registro será `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

   Value name

   `https`

   Tipo de valor

   `REG_DWORD`

   Value data

   `1`

3. Para habilitar scripts ativos, execute as seguintes etapas:

   a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Objetos de política de grupo, abra o menu de contexto (clique com o botão direito do mouse) da sua política do Centro de Identidade do IAM e escolha Editar.

   b. Na árvore de políticas, navegue para Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

c. Na lista Intranet Zone, abra o menu de contexto (clique com o botão direito do mouse) de Allow active scripting e escolha Edit.

d. Na caixa de diálogo Allow active scripting, insira as configurações a seguir e escolha OK:

- Selecione o botão de opção Enabled.
- Em Options, defina Allow active scripting como Enable.

4. Para habilitar o login automático, execute as seguintes etapas:

a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Group Policy Objects, abra o menu de contexto (clique com o botão direito do mouse) de sua política de SSO e escolha Edit.

b. Na árvore de políticas, navegue para Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

c. Na lista Intranet Zone, abra o menu de contexto (clique com o botão direito do mouse) de Logon options e escolha Edit.

d. Na caixa de diálogo Logon options, insira as configurações a seguir e escolha OK:

- Selecione o botão de opção Enabled.
- Em Options defina Logon options como Automatic logon only in Intranet zone.

5. Para habilitar a autenticação integrada, execute as seguintes etapas:

a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Objetos de política de grupo, abra o menu de contexto (clique com o botão direito do mouse) da sua política do Centro de Identidade do IAM e escolha Editar.

b. Na árvore de políticas, navegue para User Configuration > Preferences > Windows Settings.

c. Na lista Windows Settings, abra o menu de contexto (clique com o botão direito do mouse) de Registry e escolha New registry item.

d. Na caixa de diálogo New Registry Properties, insira as configurações a seguir e escolha OK:

Ação

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

Path

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

Value name

```
EnableNegotiate
```

Tipo de valor

```
REG_DWORD
```

Value data

```
1
```

6. Feche a janela Group Policy Management Editor se ainda estiver aberta.
7. Atribua a nova política a seu domínio seguindo estas etapas:
   a. Na árvore de gerenciamento de políticas de grupo, abra o menu contexto (clique com o botão direito do mouse) de seu domínio e escolha Link an Existing GPO.
   b. Na lista Objetos da política de grupo, selecione sua política do Centro de Identidade do IAM e escolha OK.

Essas alterações entrarão em vigor depois da próxima atualização de Política de grupo no cliente, ou na próxima vez que o usuário fizer login.

Autenticação única para o Firefox

Para permitir que o navegador Mozilla Firefox ofereça suporte à autenticação única, adicione o URL de acesso (por exemplo, https://*<alias>*.awsapps.com) à lista de sites aprovados para autenticação única. Isso pode ser feito manualmente ou ser automatizado com um script.

Tópicos

- Atualização manual para autenticação única
- Atualização automática para autenticação única

Atualização manual para autenticação única

Para adicionar a URL de acesso manualmente à lista de sites aprovados no Firefox, execute as seguintes etapas no computador cliente.

Para adicionar manualmente a URL de acesso à lista de sites aprovados no Firefox

1. Abra o Firefox e abra a página `about:config`.
2. Abra a preferência `network.negotiate-auth.trusted-uris` e adicione seu URL de acesso à lista de sites. Use uma vírgula (,) para separar várias entradas.

Atualização automática para autenticação única

Como um administrador de domínio, você pode usar um script para adicionar o URL de acesso à preferência de usuário `network.negotiate-auth.trusted-uris` do Firefox a todos os computadores na rede. Para obter mais informações, acesse https://support.mozilla.org/en-US/questions/939037.

Habilitar acesso ao AWS Management Console com as credenciais do AD

O AWS Directory Service permite que você conceda acesso ao AWS Management Console aos membros de seu diretório. Por padrão, os membros do diretório não têm acesso a nenhum recurso da AWS. Você atribui perfis do IAM aos membros do diretório para conceder a eles acesso a vários serviços e recursos da AWS. O perfil do IAM define os serviços, os recursos e o nível de acesso dos membros do seu diretório.

Para que seja possível conceder acesso ao console aos membros do diretório, o diretório deve ter um URL de acesso. Para obter mais informações sobre como visualizar detalhes do diretório e obter seu URL de acesso, consulte Visualizar informações do diretório. Para obter mais informações sobre como criar uma URL de acesso, consulte Criar um URL de acesso.

Para obter mais informações sobre como criar e atribuir perfis do IAM aos membros do diretório, consulte Conceder a usuários e grupos acesso aos recursos da AWS.

Tópicos

- Habilitar acesso ao AWS Management Console
- Desabilitar o acesso ao AWS Management Console
- Definir a duração da sessão de login

Artigo relacionado do blog de segurança da AWS

- Como acessar o AWS Management Console usando o AWS Managed Microsoft AD e suas credenciais on-premises

> **Note**
>
> O acesso ao AWS Management Console é um recurso regional do AWS Managed Microsoft AD. Se você estiver usando a Replicação em várias regiões, os procedimentos a seguir deverão ser aplicados separadamente em cada região. Para obter mais informações, consulte Recursos globais versus regionais.

Habilitar acesso ao AWS Management Console

Por padrão, o acesso ao console não é habilitado para nenhum diretório. Para habilitar o acesso ao console para os usuários e grupos de seu diretório, execute as seguintes etapas:

Para habilitar acesso ao console

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja habilitar o acesso ao AWS Management Console e, em seguida, escolha a guia Gerenciamento de aplicações. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Gerenciamento de aplicações.
4. Na seção AWS Management Console, escolha Habilitar. O acesso ao console agora está habilitado para o diretório.

   Antes que os usuários possam entrar no console com seu URL de acesso, primeiro é necessário adicionar seus usuários ao perfil. Para obter mais informações sobre a atribuição de usuários a recursos do IAM, consulte Atribuir usuários ou grupos a um perfil existente. Depois que os perfis do IAM forem atribuídos, os usuários poderão acessar o console usando seu URL de acesso. Por exemplo, se o URL de acesso do diretório for example-corp.awsapps.com, o URL para acessar o console será https://example-corp.awsapps.com/console/.

Desabilitar o acesso ao AWS Management Console

Para desabilitar o acesso ao console para os usuários e grupos de seu diretório, execute as seguintes etapas:

Para desabilitar o acesso ao console

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja desabilitar o acesso ao AWS Management Console e, em seguida, escolha a guia Gerenciamento de aplicações. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Gerenciamento de aplicações.
4. Na seção AWS Management Console, escolha Desabilitar. O acesso ao console agora está desabilitado para o diretório.
5. Se algum perfil do IAM tiver sido atribuído a usuários ou grupos no diretório, o botão Desabilitar poderá não estar disponível. Nesse caso, será necessário remover todas as atribuições de perfis do IAM para o diretório antes de continuar, incluindo atribuições para usuários ou grupos no diretório que foram excluídos, os quais serão mostrados em Usuário excluído ou Grupo excluído.

   Após a remoção de todas as atribuições de perfis do IAM repita as etapas acima.

Definir a duração da sessão de login

Por padrão, os usuários têm 1 hora para usar sua sessão após terem feito login com êxito no console antes de serem desconectados. Depois disso, os usuários deverão fazer login novamente para iniciar a próxima sessão de 1 hora antes de serem desconectados novamente. Você pode usar o procedimento a seguir para alterar a duração para até 12 horas por sessão.

Para definir a duração da sessão de login

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.

3. Na página Detalhes do diretório, siga um destes procedimentos:

   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja definir a duração da sessão de login e, em seguida, escolha a guia Gerenciamento de aplicações. Para obter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Gerenciamento de aplicações.
4. Na seção Aplicações e serviços da AWS, escolha Console de Gerenciamento da AWS.
5. Na caixa de diálogo Gerenciar acesso a recurso da AWS, escolha Continuar.
6. Na página Assign users and groups to IAM roles, em Set login session length, edite o valor numerado e escolha Save.

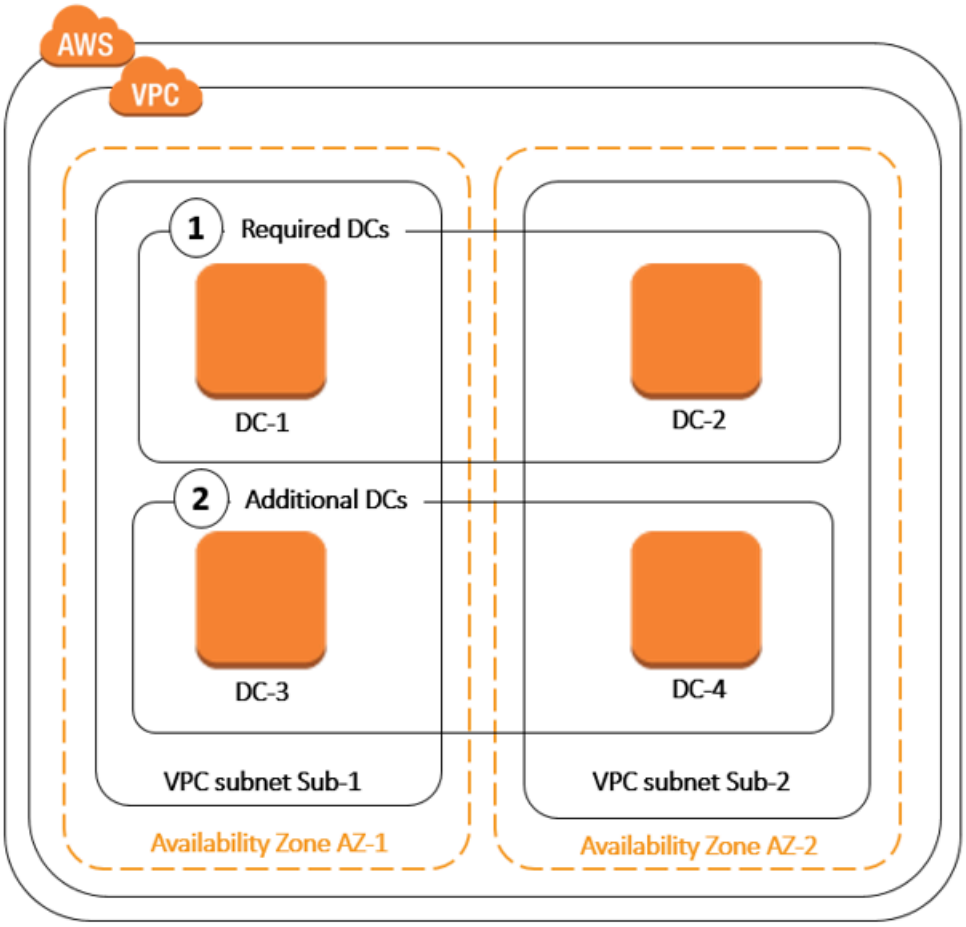
Implantar controladores de domínio adicionais

A implantação de controladores de domínio adicionais aumenta a redundância, o que resulta em maior resiliência e alta disponibilidade. Isso também melhora o desempenho do diretório oferecendo suporte a um maior número de solicitações do Active Directory. Por exemplo, agora você pode usar o AWS Managed Microsoft AD para oferecer suporte a vários aplicativos.NET implantados em grandes frotas de instâncias do Amazon EC2 e do Amazon RDS for SQL Server.

Quando você cria seu diretório pela primeira vez, o AWS Managed Microsoft AD implanta dois controladores de domínio em várias zonas de disponibilidade, o que é necessário para fins de alta disponibilidade. Posteriormente, você pode implantar facilmente controladores de domínio adicionais por meio do AWS Directory Service console, especificando apenas o número total de controladores de domínio que você deseja. AWS O Microsoft AD gerenciado distribui os controladores de domínio adicionais para as zonas de disponibilidade e sub-redes da Amazon VPC nas quais seu diretório está sendo executado.

Por exemplo, na ilustração a seguir, o DC-1 e o DC-2 representam dois controladores de domínio que foram criados originalmente com o diretório. O AWS Directory Service console se refere a esses controladores de domínio padrão como Obrigatórios. AWS O Microsoft AD gerenciado localiza intencionalmente cada um desses controladores de domínio em zonas de disponibilidade separadas durante o processo de criação do diretório. Mais tarde, você pode decidir adicionar mais dois controladores de domínio para ajudar a distribuir a carga de autenticação em períodos de pico de login. O DC-3 e o DC-4 representam os controladores de domínio aos quais o console se refere como Additional. Como antes, o AWS Managed Microsoft AD novamente coloca automaticamente

os novos controladores de domínio em diferentes zonas de disponibilidade para garantir a alta disponibilidade do seu domínio.



Esse processo elimina a necessidade de configurar manualmente a replicação de dados do diretório, os snapshots diários automatizados ou o monitoramento de controladores de domínio adicionais. Também é mais fácil migrar e executar workloads de missão crítica integradas ao Active Directory na Nuvem AWS sem precisar implantar e manter sua própria infraestrutura do Active Directory. Você também pode implantar ou remover controladores de domínio adicionais para o AWS Managed Microsoft AD usando a UpdateNumberOfDomainControllersAPI.

> **Note**
>
> Controladores de domínio adicionais são um recurso regional do AWS Managed Microsoft AD. Se você estiver usando a Replicação em várias regiões, os procedimentos a seguir deverão ser aplicados separadamente em cada região. Para ter mais informações, consulte Recursos globais versus regionais.

Adicionar ou remover controladores de domínio adicionais

Antes de adicionar ou remover outros controladores de domínio, veja aqui mais informações sobre os requisitos do controlador de domínio:

- Após ter implantado controladores de domínio adicionais, você pode reduzir o número de controladores de domínio para dois, que é o mínimo exigido para fins de tolerância a falhas e de alta disponibilidade.
- Os controladores de domínio excluídos serão removidos da lista de controladores de domínio adicionais. Os controladores de domínio principal e secundário são obrigatórios e não podem ser excluídos.
- Se você configurou seu Microsoft AD AWS gerenciado para habilitar o LDAPS, todos os controladores de domínio adicionais adicionados também terão o LDAPS ativado automaticamente. Para ter mais informações, consulte Habilite LDAP ou LDAPS seguros.

Use o procedimento a seguir para implantar ou remover controladores de domínio adicionais no diretório do AWS Managed Microsoft AD.

Para adicionar ou remover controladores de domínio adicionais

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região em que deseja adicionar ou remover controladores de domínio e, em seguida, escolha a guia Escalar e compartilhar. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Escalar e compartilhar.
4. Na seção Domain controllers (Controladores de domínio), selecione Edit (Editar).
5. Especifique o número de controladores de domínio para adicionar ou remover do diretório e selecione Modify (Alterar).
6. Quando o AWS Managed Microsoft AD conclui o processo de implantação, todos os controladores de domínio mostram o status Ativo e as sub-redes atribuídas da Zona de Disponibilidade e da Amazon VPC aparecem. Os novos controladores de domínio são

distribuídos igualmente nas zonas de disponibilidade e nas sub-redes onde o diretório já está implantado.

Artigo relacionado ao blog de AWS segurança

- Como aumentar a redundância e o desempenho do seu AWS Microsoft AD AWS Directory Service gerenciado adicionando controladores de domínio

Migrar usuários do Active Directory para o AWS Managed Microsoft AD

Você pode usar o Active Directory Migration Toolkit (ADMT) junto com o Password Export Service (PES) para migrar usuários do Active Directory autogerenciado para o diretório Managed AWS Microsoft AD. Isso permite que você migre objetos do Active Directory e senhas criptografadas para seus usuários com mais facilidade.

Para obter instruções detalhadas, consulte Como migrar seu domínio on-premises para o AWS Managed Microsoft AD usando ADMT no Blog de segurança da AWS.

AWS Cotas gerenciadas do Microsoft AD

A seguir estão as cotas padrão para o AWS Managed Microsoft AD. A menos que especificado de outra forma, cada cota é aplicada por região.

AWS Cotas gerenciadas do Microsoft AD

Recurso	Cota padrão
AWS Diretórios gerenciados do Microsoft AD	20
Snapshots manuais*	5 por Microsoft AD AWS gerenciado
Idade dos snapshots manuais **	180 dias
Número máximo de controladores de domínio por diretório	20
Domínios compartilhados por Standard Microsoft AD ***	5

Recurso	Cota padrão
Domínios compartilhados por Enterprise Microsoft AD ***	125
Número máximo de certificados de autoridade de certificação (CA) registrados por diretório	5
Número máximo do total de AWS regiões em um único diretório AWS gerenciado do Microsoft AD (Enterprise Edition) ****	5

* A cota de snapshots manuais não pode ser alterada.

** A idade máxima aceita para um snapshot manual é 180 dias e não pode ser alterada. Isso se deve ao atributo Tombstone-Lifetime de objetos excluídos que define a vida útil de um backup de estado do sistema do Active Directory. Não é possível fazer a restauração a partir de um snapshot com mais de 180 dias. Para obter mais informações, consulte Prazo de validade útil de um backup de estado do sistema do Active Directory no site da Microsoft.

*** A cota padrão do domínio compartilhado refere-se ao número de contas com as quais um diretório individual pode ser compartilhado.

**** Isso inclui 1 região principal e até 4 regiões adicionais. Para ter mais informações, consulte Regiões principais versus adicionais.

> **Note**
>
> Você não pode anexar um endereço IP público à sua interface de rede AWS elástica (ENI).

Para obter informações sobre o design de aplicativos e a distribuição de carga, consulte Programar suas aplicações.

Para cotas de armazenamento e objeto, consulte a Tabela de comparação na página Preços do AWS Directory Service.

Compatibilidade de aplicativos para o AWS Managed Microsoft AD

AWS O Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) é compatível com vários AWS serviços e aplicativos de terceiros.

Veja a seguir uma lista de AWS aplicativos e serviços compatíveis:

- Amazon Chime: para obter instruções detalhadas, consulte Conectar ao Active Directory.
- Amazon Connect: para obter mais informações, consulte Como o Amazon Connect funciona.
- Amazon EC2: para obter mais informações, consulte Associe uma instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory.
- Amazon QuickSight - Para obter mais informações, consulte Gerenciamento de contas de usuário na Amazon QuickSight Enterprise Edition.
- Amazon RDS para MySQL: para obter mais informações, consulte Usar a autenticação Kerberos para MySQL.
- Amazon RDS para Oracle: para obter mais informações, consulte Usar a autenticação Kerberos com o Amazon RDS para Oracle.
- Amazon RDS para PostgreSQL: para obter mais informações, consulte Usar a autenticação Kerberos com o Amazon RDS para PostgreSQL.
- Amazon RDS para SQL Server: para obter mais informações, consulte Usar a autenticação do Windows com uma instância de banco de dados do Microsoft SQL Server do Amazon RDS.
- Amazon WorkDocs — Para obter instruções detalhadas, consulte Conectando-se ao seu diretório local com o AWS Managed Microsoft AD.
- Amazon WorkMail — Para obter instruções detalhadas, consulte Integrar a Amazon WorkMail com um diretório existente (configuração padrão).
- AWS Client VPN - Para obter instruções detalhadas, consulte Autenticação e autorização do cliente.
- AWS IAM Identity Center - Para obter instruções detalhadas, consulte Connect IAM Identity Center a um Active Directory local.
- AWS License Manager - Para obter mais informações, consulte Assinaturas baseadas no usuário em. AWS License Manager
- AWS Management Console — Para obter mais informações, consulteHabilitar acesso ao AWS Management Console com as credenciais do AD.

- FSx para Windows File Server: para obter mais informações, consulte O que é FSx para Windows File Server?.
- WorkSpaces - Para obter instruções detalhadas, consulte Iniciar um WorkSpace usando o Microsoft AD AWS gerenciado.

Devido à magnitude dos off-the-shelf aplicativos personalizados e comerciais que usam o Active Directory, AWS não realiza nem pode realizar a verificação formal ou ampla da compatibilidade de aplicativos de terceiros com o AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Embora AWS trabalhe com clientes na tentativa de superar quaisquer possíveis desafios de instalação de aplicativos que eles possam encontrar, não podemos garantir que nenhum aplicativo seja ou continue sendo compatível com o AWS Managed Microsoft AD.

Os seguintes aplicativos de terceiros são compatíveis com o AWS Managed Microsoft AD:

- ADBA (Active Directory-Based Activation, Ativação baseada no Active Directory)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server (.NET)
- Microsoft Entra(anteriormente conhecido como Azure Active Directory (AzureAD))
- Microsoft Entra Connect(anteriormente conhecido comoAzure Active Directory Connect)
- DFSR (Distributed File System Replication, Replicação do sistema de arquivos distribuídos)
- DFSN (Distributed File System Namespaces, Namespaces do sistema de arquivos distribuídos)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(incluindo grupos de disponibilidade do SQL Server Always On)
- Microsoft System Center Configuration Manager(SCCM) - O usuário que está implantando o SCCM deve ser membro do grupo Administradores AWS Delegados de Gerenciamento do Sistema.
- Microsoft Windows and Windows Server OS
- Office 365

Observe que nem todas as configurações desses aplicativos têm suporte.

Diretrizes de compatibilidade

Embora os aplicativos possam ter configurações que são incompatíveis, as configurações de implantação do aplicativo podem, muitas vezes, superar a incompatibilidade. A tabela a seguir descreve os motivos mais comuns para a incompatibilidade de aplicativos. Os clientes podem usar essas informações para analisar características de compatibilidade de um aplicativo desejado e identificar possíveis alterações de implantação.

- Administrador de domínio ou outras permissões privilegiadas - Alguns aplicativos indicam que você deve instalá-los como administrador de domínio. Como AWS deve manter o controle exclusivo desse nível de permissão para fornecer o Active Directory como um serviço gerenciado, você não pode atuar como administrador do domínio para instalar esses aplicativos. No entanto, muitas vezes você pode instalar esses aplicativos delegando permissões específicas, menos privilegiadas e AWS suportadas à pessoa que executa a instalação. Para obter mais detalhes sobre as permissões precisas que seu aplicativo exige, fale com o provedor do aplicativo. Para obter mais informações sobre permissões que AWS permitem delegar, consulteO que é criado com seu Microsoft AD Active Directory AWS gerenciado.
- Acesso a Active Directory contêineres privilegiados — Em seu diretório, o Microsoft AD AWS gerenciado fornece uma Unidade Organizacional (OU) sobre a qual você tem controle administrativo total. Você não precisa criar nem gravar permissões, e pode ter permissões de leitura limitadas a contêineres que estão mais no topo da árvore do Active Directory do que sua UO. Os aplicativos que criam ou acessam contêineres para os quais você não têm permissões podem não funcionar. No entanto, esses aplicativos geralmente têm uma capacidade de usar um contêiner que você cria em sua UO como alternativa. Fale com seu provedor do aplicativo para encontrar maneiras de criar e usar um contêiner em sua UO como alternativa. Para obter mais informações sobre como gerenciar sua UO, consulte Como administrar o Microsoft AD AWS gerenciado.
- Alterações no esquema durante o fluxo de trabalho de instalação — Alguns Active Directory aplicativos exigem alterações no esquema padrão do Active Directory e podem tentar instalar essas alterações como parte do fluxo de trabalho de instalação do aplicativo. Devido à natureza privilegiada das extensões de esquema, AWS torna isso possível importando arquivos Lightweight Directory Interchange Format (LDIF) somente por meio do console AWS Directory Service , CLI ou SDK. Esses aplicativos geralmente vêm com um arquivo LDIF que você pode aplicar ao diretório por meio do processo de atualização do AWS Directory Service esquema. Para obter mais informações sobre como funciona o processo de importação de LDIF, consulte Tutorial: Estendendo seu esquema AWS gerenciado do Microsoft AD. Você pode instalar o aplicativo de maneira que ignore a instalação do esquema durante o processo de instalação.

Aplicações incompatíveis conhecidas

A seguir, listamos os off-the-shelf aplicativos comerciais comumente solicitados para os quais não encontramos uma configuração que funcione com o AWS Managed Microsoft AD. AWS atualiza essa lista periodicamente, a seu exclusivo critério, como cortesia para ajudá-lo a evitar esforços improdutivos. AWS forneça essas informações sem garantia ou reclamações relacionadas à compatibilidade atual ou futura.

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

AWS Tutoriais gerenciados do laboratório de testes do Microsoft AD

Esta seção fornece uma série de tutoriais guiados para ajudá-lo a estabelecer um ambiente de laboratório de teste no AWS qual você pode experimentar o Managed AWS Microsoft AD.

Tópicos

- Tutorial: Configurando seu laboratório de teste básico do AWS Managed Microsoft AD em AWS
- Tutorial: Criando uma relação de confiança do Microsoft AD AWS gerenciado para uma instalação autogerenciada do Active Directory no Amazon EC2

Tutorial: Configurando seu laboratório de teste básico do AWS Managed Microsoft AD em AWS

Este tutorial ensina como configurar seu AWS ambiente para se preparar para uma nova instalação AWS gerenciada do Microsoft AD que usa uma nova instância do Amazon EC2 executando o Windows Server 2019. Em seguida, ele ensina você a usar as ferramentas de administração típicas do Active Directory para gerenciar seu ambiente Microsoft AD AWS gerenciado a partir de sua instância EC2 Windows. Ao concluir o tutorial, você terá configurado os pré-requisitos de rede e configurado uma nova floresta gerenciada AWS do Microsoft AD.

Conforme mostrado na ilustração a seguir, o laboratório que você cria a partir deste tutorial é o componente fundamental para o aprendizado prático sobre o Managed AWS Microsoft AD. Mais adiante, você poderá acrescentar outros tutoriais a fim de ganhar ainda mais experiência prática. Esta série de tutoriais é ideal para qualquer iniciante em AWS Managed Microsoft AD e que deseja ter um laboratório de teste para fins de avaliação. Este tutorial leva aproximadamente 1 hora para ser concluído.

Etapa 1: Configurar seu AWS ambiente para o Microsoft AD Active Directory AWS gerenciado

Depois de concluir suas tarefas de pré-requisito, você cria e configura uma Amazon VPC na sua instância do EC2.

Etapa 2: Criar seu Microsoft AD Active Directory AWS gerenciado

Nesta etapa, você configura o AWS Managed Microsoft AD in AWS pela primeira vez.

Etapa 3: Implantar uma instância do Amazon EC2 para gerenciar seu AWS Microsoft AD Active Directory gerenciado

Aqui, você passará por diversas tarefas pós-implantação necessárias para que os computadores cliente se conectem ao seu novo domínio e configurem um novo sistema do Windows Server no EC2.

Etapa 4: verificar se o laboratório de teste básico está operacional

Finalmente, como administrador, você verificará que pode fazer login e se conectar ao AWS Managed Microsoft AD partindo do sistema do Windows Server no EC2. Depois de testar com êxito que o laboratório está operacional, você poderá continuar adicionando outros módulos de guia de laboratório de teste.

Pré-requisitos

Se você planeja usar somente as etapas da interface de usuário neste tutorial para criar seu laboratório de teste, pule esta seção de pré-requisitos e vá para a Etapa 1. No entanto, se você planeja usar AWS CLI comandos ou AWS Tools for Windows PowerShell módulos para criar seu ambiente de laboratório de teste, primeiro configure o seguinte:

- Usuário do IAM com a chave de acesso e acesso secreta — Um usuário do IAM com uma chave de acesso é necessário se você quiser usar os AWS Tools for Windows PowerShell módulos AWS CLI ou. Se você não tiver uma chave de acesso, consulte Criar, modificar e visualizar chaves de acesso (AWS Management Console).
- AWS Command Line Interface (opcional) — Baixe e instale o AWS CLI no Windows. Depois de instalado, abra o prompt de comando ou a Windows PowerShell janela e digite`aws configure`. Observe que você precisa da chave de acesso e da chave secreta para concluir a configuração. Veja o primeiro pré-requisito para as etapas sobre como fazer isso. Será solicitado o seguinte:
  - AWS ID da chave de acesso [Nenhum]: `AKIAIOSFODNN7EXAMPLE`
  - AWS chave de acesso secreta [Nenhuma]: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - Nome da região padrão [Nenhum]: `us-west-2`
  - Formato de saída padrão [Nenhum]: `json`
- AWS Tools for Windows PowerShell (opcional): baixe e instale a versão mais recente do AWS Tools for Windows PowerShell de https://aws.amazon.com/powershell/ e execute o comando a

seguir. Observe que você precisa da sua chave de acesso e da chave secreta para concluir a configuração. Veja o primeiro pré-requisito para as etapas sobre como fazer isso.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

Etapa 1: Configurar seu AWS ambiente para o Microsoft AD Active Directory AWS gerenciado

Antes de criar o AWS Managed Microsoft AD em seu laboratório de AWS teste, primeiro você precisa configurar seu par de chaves do Amazon EC2 para que todos os dados de login sejam criptografados.

Criar um par de chaves

Se você já tiver um par de chaves, ignore esta etapa. Para obter mais informações sobre os pares de chaves do Amazon EC2, consulte Criar pares de chaves.

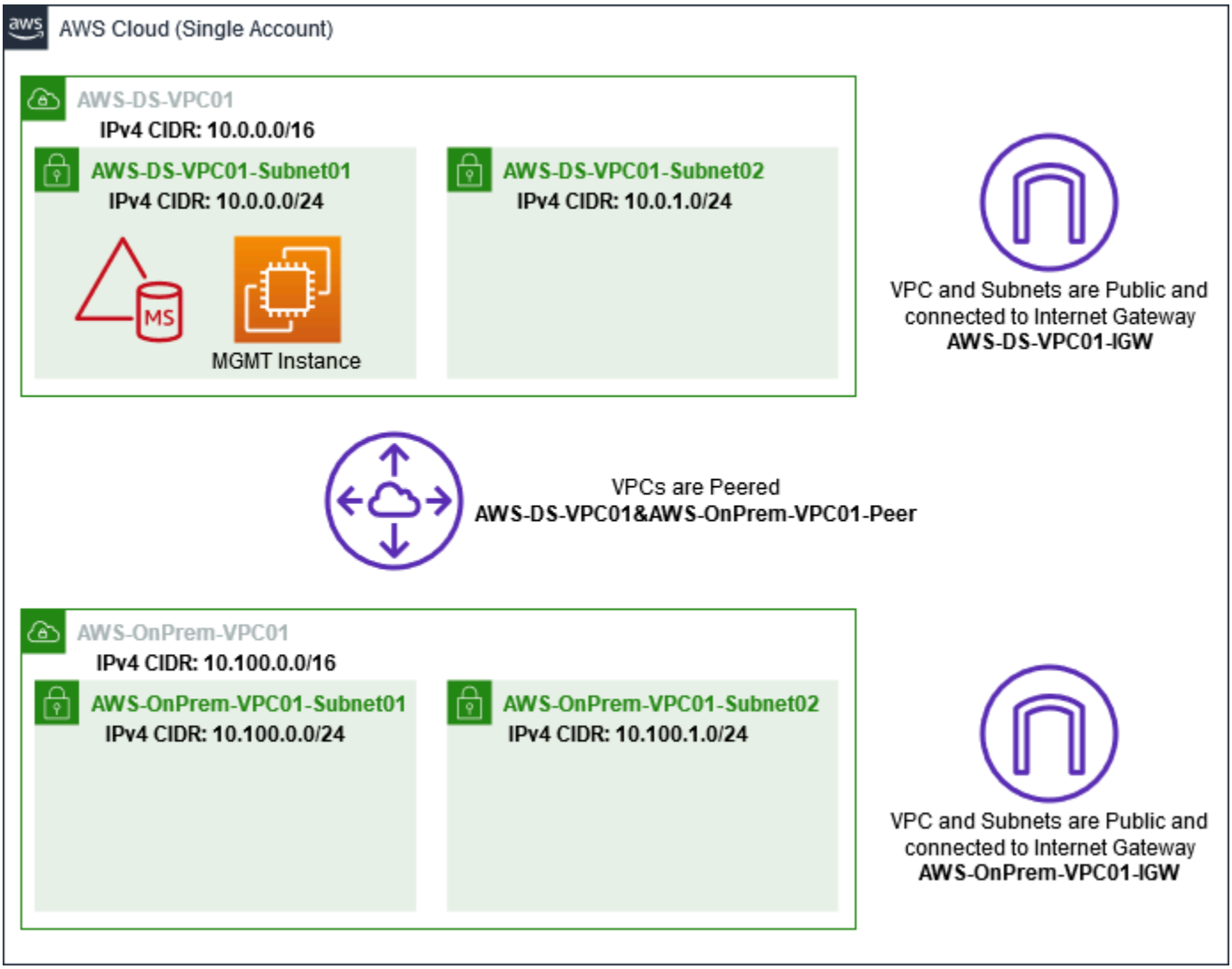
Para criar um par de chaves

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Rede e segurança, escolha Key Pairs (Pares de chaves) e Create Key Pair (Criar par de chaves).
3. Em Key pair name (Nome do par de chaves), digite **`AWS-DS-KP`**. Em Key pair file format (Formato do arquivo do par de chaves), selecione pem e Create (Criar).
4. O arquivo de chave privada é baixado automaticamente pelo navegador. O nome de arquivo é o nome que você especificou quando criou seu par de chaves com uma extensão `.pem`. Salve o arquivo de chave privada em um lugar seguro.

> **Important**
>
> Esta é a única chance de você salvar o arquivo de chave privada. Você precisará fornecer o nome do par de chaves ao iniciar uma instância e a chave privada correspondente sempre que descriptografar a senha para a instância.

Crie, configure e emparelhe duas Amazon VPCs

Conforme mostrado na ilustração a seguir, ao concluir esse processo de várias etapas, você terá criado e configurado duas VPCs públicas, duas sub-redes públicas por VPC, um gateway da Internet por VPC e uma conexão de emparelhamento de VPC entre as VPCs. Optamos por usar VPCs e sub-redes públicas para fins de simplicidade e custo. Para cargas de trabalho de produção, recomendamos que você use VPCs privadas. Para obter mais informações sobre como melhorar a segurança da VPC, consulte Segurança na Amazon Virtual Private Cloud.



Todos os AWS CLI PowerShell exemplos usam as informações de VPC abaixo e são criados em us-west-2. Você pode escolher qualquer região compatível para criar seu ambiente. Para obter informações gerais, consulte O que é a Amazon VPC?.

Etapa 1: criar duas VPCs

Nesta etapa, você precisa criar duas VPCs na mesma conta usando os parâmetros especificados na tabela a seguir. AWS O Microsoft AD gerenciado suporta o uso de contas separadas com o Compartilhar seu diretório recurso. A primeira VPC será usada para o AWS Microsoft AD gerenciado. A segunda VPC será usada para recursos que podem ser usados posteriormente em Tutorial: Criando uma relação de confiança do Microsoft AD AWS gerenciado para uma instalação autogerenciada do Active Directory no Amazon EC2.

Informações gerenciadas da VPC do Active Directory	Informações da VPC on-premises
Etiqueta de nome: AWS-DS-VPC01 Bloco CIDR IPv4: 10.0.0.0/16 IPv6 CIDR block (Bloco CIDR IPv6): nenhum bloco CIDR IPv6 Locação: Padrão	Etiqueta de nome: AWS- OnPrem -VPC01 Bloco CIDR IPv4: 10.100.0.0/16 IPv6 CIDR block (Bloco CIDR IPv6): nenhum bloco CIDR IPv6 Locação: Padrão

Para obter instruções detalhadas, consulte Criar uma VPC.

Etapa 2: criar duas sub-redes por VPC

Depois de criar as VPCs, será necessário criar duas sub-redes por VPC usando os parâmetros especificados na tabela a seguir. Para este laboratório de teste, cada sub-rede será um /24. Isso permitirá que até 256 endereços sejam emitidos por sub-rede. Cada sub-rede deve estar em uma zona de disponibilidade separada. Colocar cada sub-rede em uma zona de disponibilidade separada é um dos AWS Pré-requisitos gerenciados do Microsoft AD.

Informações da sub-rede AWS-DS-VPC01:	AWS- OnPrem -Informações da sub-rede VPC01
Etiqueta de nome: AWS-DS-VPC01-Subnet01 VPC: vpc-xxxxxxxxxxxxxxxxxxx-DS-VPC01 AWS Zona de disponibilidade: us-west-2a	Etiqueta de nome: AWS- OnPrem -VPC01-Subnet01 VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem Zona de disponibilidade: us-west-2a

Informações da sub-rede AWS-DS-VPC01:	AWS- OnPrem -Informações da sub-rede VPC01
Bloco CIDR IPv4: 10.0.0.0/24	Bloco CIDR IPv4: 10.100.0.0/24
Etiqueta de nome: AWS-DS-VPC01-Subnet02 VPC: vpc-xxxxxxxxxxxxxxxxxxx-DS-VPC01 AWS Zona de disponibilidade: us-west-2b Bloco CIDR IPv4: 10.0.1.0/24	Etiqueta de nome: AWS- OnPrem -VPC01-Subnet02 VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem Zona de disponibilidade: us-west-2b Bloco CIDR IPv4: 10.100.1.0/24

Para obter instruções detalhadas, consulte Criar uma sub-rede na VPC.

Etapa 3: criar e anexar um gateway da Internet às VPCs

Como estamos usando VPCs públicas, será necessário criar e anexar um gateway da Internet às VPCs usando os parâmetros especificados na tabela a seguir. Isso permitirá que você seja capaz de se conectar e gerenciar as instâncias do EC2.

Informações do gateway da Internet AWS-DS-VPC01	AWS- OnPrem -Informações sobre o Gateway de Internet VPC01
Etiqueta de nome: AWS-DS-VPC01-IGW VPC: vpc-xxxxxxxxxxxxxxxxxxx-DS-VPC01 AWS	Etiqueta de nome: AWS- OnPrem -VPC01-IGW VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem

Para obter instruções detalhadas, consulte Gateways da Internet.

Etapa 4: Configurar uma conexão de emparelhamento de VPC entre AWS-DS-VPC01 e - -VPC01 AWS OnPrem

Como você já criou duas VPCs, será necessário conectá-las em rede usando o emparelhamento de VPC usando os parâmetros especificados na tabela a seguir. Embora existam várias maneiras de conectar suas VPCs, este tutorial usará o VPC Peering. AWS O Microsoft AD gerenciado oferece

suporte a várias soluções para conectar suas VPCs, algumas delas incluem emparelhamento de VPC, Transit Gateway e VPN.

Etiqueta de nome da conexão de emparelhamento: AWS-DS-VPC01& -AWS-VPC01-peer OnPrem

VPC (solicitante): vpc-xxxxxxxxxxxxxxxxxxxx -DS-VPC01 AWS

Conta: minha conta

Região: esta região

VPC (aceitador): vpc-xxxxxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Para obter instruções sobre como criar uma conexão de emparelhamento de VPC com outra VPC em sua conta, consulte Criar uma conexão de emparelhamento de VPC com outra VPC em sua conta.

Etapa 5: adicionar duas rotas à tabela de rotas principal de cada VPC

Para que os gateways da Internet e a conexão de emparelhamento de VPC criados nas etapas anteriores sejam funcionais, será necessário atualizar a tabela de rotas principal de ambas as VPCs usando os parâmetros especificados na tabela a seguir. Você adicionará duas rotas: 0.0.0.0/0, que roteará para todos os destinos não explicitamente conhecidos na tabela de rotas e 10.0.0.0/16 ou 10.100.0.0/16, que roteará para cada VPC pela conexão de emparelhamento de VPC estabelecida acima.

Você pode encontrar facilmente a tabela de rotas correta para cada VPC filtrando pela etiqueta de nome da VPC (-DS-VPC01 ou AWS- -VPC01). AWS OnPrem

Informações da rota 1 de AWS-DS-VPC01	Informações da rota 2 de AWS-DS-VPC01	AWS- OnPrem - Informações sobre a rota 1 do VPC01	AWS- OnPrem - Informações sobre a rota 2 do VPC01
Destino: 0.0.0.0/0 Alvo: igw-xxxxx xxxxxxxxxxxx -DS-VPC01-IGW AWS	Destino: 10.100.0.0/16 Alvo: pcx-xxxxx xxxxxxxxxxxx -DS-	Destino: 0.0.0.0/0 Alvo: AWS igw-xxxxxxxxxxxxxxxxx - OnPrem-VPC01	Destino: 10.0.0.0/16 Alvo: pcx-xxxxx xxxxxxxxxxxx -DS-VPC01& AWS- -

Informações da rota 1 de AWS-DS-VPC01	Informações da rota 2 de AWS-DS-VPC01	AWS- OnPrem - Informações sobre a rota 1 do VPC01	AWS- OnPrem - Informações sobre a rota 2 do VPC01
	VPC01& AWS- - VPC01-Peer AWS OnPrem		VPC01-Peer AWS OnPrem

Para obter instruções sobre como adicionar rotas a uma tabela de rotas da VPC, consulte Adicionar e remover rotas de uma tabela de rotas.

Crie grupos de segurança para instâncias do Amazon EC2

Por padrão, o AWS Managed Microsoft AD cria um grupo de segurança para gerenciar o tráfego entre seus controladores de domínio. Nesta seção, será necessário criar dois grupos de segurança (um para cada VPC) que serão usados para gerenciar o tráfego dentro da VPC para as instâncias do EC2 usando os parâmetros especificados nas tabelas a seguir. Você também adicionará uma regra que permite a entrada de um RDP (3389) de qualquer lugar e a entrada de todos os tipos de tráfego a partir da VPC local. Para obter mais informações, consulte Grupos de segurança do Amazon EC2 para instâncias do Windows.

Informações do grupo de segurança de AWS-DS-VPC01:
Nome do grupo de segurança: AWS DS Test Lab Security Group
Descrição: Grupo de segurança do AWS DS Test Lab
VPC: vpc-xxxxxxxxxxxxxxxxxxx-DS-VPC01 AWS

Regras de entrada do grupo de segurança para AWS-DS-VPC01

Tipo	Protocolo	Intervalo de portas	Origem	Tipo de tráfego
Regra personalizada de TCP	TCP	3389	Meu IP	Área de trabalho remota

Tipo	Protocolo	Intervalo de portas	Origem	Tipo de tráfego
Todo o tráfego	Tudo	Todos	10.0.0.0/16	Todo o tráfego de VPC local

Regras de saída do grupo de segurança para AWS-DS-VPC01

Tipo	Protocolo	Intervalo de portas	Destino	Tipo de tráfego
Todo o tráfego	Tudo	Tudo	0.0.0.0/0	Todo o tráfego

AWS- OnPrem -Informações do grupo de segurança VPC01:
Nome do grupo de segurança: Grupo de Segurança do AWS OnPrem Test Lab.
Descrição: Grupo de Segurança do AWS OnPrem Test Lab.
VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem

Regras de entrada do grupo de segurança para AWS- OnPrem -VPC01

Tipo	Protocolo	Intervalo de portas	Origem	Tipo de tráfego
Regra personalizada de TCP	TCP	3389	Meu IP	Área de trabalho remota
Regra personalizada de TCP	TCP	53	10.0.0.0/16	DNS
Regra personalizada de TCP	TCP	88	10.0.0.0/16	Kerberos

Tipo	Protocolo	Intervalo de portas	Origem	Tipo de tráfego
Regra personalizada de TCP	TCP	389	10.0.0.0/16	LDAP
Regra personalizada de TCP	TCP	464	10.0.0.0/16	Alterar/definir senha do Kerberos
Regra personalizada de TCP	TCP	445	10.0.0.0/16	SMB/CIFS
Regra personalizada de TCP	TCP	135	10.0.0.0/16	Replicação
Regra personalizada de TCP	TCP	636	10.0.0.0/16	LDAP SSL
Regra personalizada de TCP	TCP	49152 – 65535	10.0.0.0/16	RPC
Regra personalizada de TCP	TCP	3268 - 3269	10.0.0.0/16	LDAP GC e LDAP GC SSL
Regra personalizada de UDP	UDP	53	10.0.0.0/16	DNS
Regra personalizada de UDP	UDP	88	10.0.0.0/16	Kerberos
Regra personalizada de UDP	UDP	123	10.0.0.0/16	Horário do Windows
Regra personalizada de UDP	UDP	389	10.0.0.0/16	LDAP

Tipo	Protocolo	Intervalo de portas	Origem	Tipo de tráfego
Regra personalizada de UDP	UDP	464	10.0.0.0/16	Alterar/definir senha do Kerberos
Todo o tráfego	Tudo	Todos	10.100.0.0/16	Todo o tráfego de VPC local

Regras de saída do grupo de segurança para AWS- OnPrem -VPC01

Tipo	Protocolo	Intervalo de portas	Destino	Tipo de tráfego
Todo o tráfego	Tudo	Tudo	0.0.0.0/0	Todo o tráfego

Para obter instruções detalhadas sobre como criar e adicionar regras aos grupos de segurança, consulte Trabalhar com grupos de segurança:

Etapa 2: Criar seu Microsoft AD Active Directory AWS gerenciado

Você pode usar três métodos diferentes para criar o seu diretório. Você pode usar o AWS Management Console procedimento (recomendado para este tutorial) ou usar os AWS Tools for Windows PowerShell procedimentos AWS CLI ou para criar seu diretório.

Método 1: Para criar seu diretório AWS gerenciado do Microsoft AD (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios e escolha Configurar diretório.
2. Na página Selecionar tipo do diretório, escolha AWS Managed Microsoft AD e, em seguida, Próximo.
3. Na página Enter directory information (Inserir informações do diretório), forneça as informações a seguir e selecione Next (Próximo).

   - Em Edition (Edição), selecione Standard Edition ou Enterprise Edition. Para obter mais informações sobre edições, consulte AWS Directory Service for Microsoft Active Directory.

- Em Directory DNS name (Nome do DNS do diretório), digite **`corp.example.com`**.
- Em Directory NetBIOS name (Nome NetBIOS do diretório), digite **`corp`**.
- Em Directory description (Descrição do diretório), digite **`AWS DS Managed`**.
- Em Senha do administrador, digite a senha que deseja usar para esta conta. Em Confirmar senha, digite novamente a senha. Esta conta de administrador é criada automaticamente durante o processo de criação do diretório. A senha não pode incluir a palavra admin. A senha do administrador do diretório diferencia maiúsculas de minúsculas e deve ter de 8 a 64 caracteres, inclusive. Ela também precisa conter pelo menos um caractere de três das quatro categorias a seguir:
  - Letras minúsculas (a-z)
  - Letras maiúsculas (A-Z)
  - Números (0-9)
  - Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

4. Na página Choose VPC and subnets (Selecionar VPC e sub-redes), forneça as seguintes informações e selecione Next (Próximo).
   - Em VPC, escolha a opção que começa com AWS-DS-VPC01 e termina com (10.0.0.0/16).
   - Em Subnets (Sub-redes), escolha as sub-redes públicas 10.0.0.0/24 e 10.0.1.0/24.
5. Na página Review & create (Revisar e criar), analise as informações do diretório e faça as alterações necessárias. Quando as informações estiverem corretas, escolha Create directory (Criar diretório). A criação do diretório leva de 20 a 40 minutos. Depois de criado, o valor de Status é alterado para Ativo.

Método 2: Para criar seu Microsoft AD AWS gerenciado (Windows PowerShell) (opcional)

1. Abra o Windows PowerShell.
2. Digite o seguinte comando. Certifique-se de usar os valores fornecidos na Etapa 4 do AWS Management Console procedimento anterior.

```
New-DSMicrosoftAD -Name corp.example.com –ShortName corp –Password P@ssw0rd
 –Description “AWS DS Managed” - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

Método 3: Para criar seu Microsoft AD AWS gerenciado (AWS CLI) (opcional)

1. Abra AWS CLI o.
2. Digite o seguinte comando. Certifique-se de usar os valores fornecidos na Etapa 4 do AWS Management Console procedimento anterior.

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

Etapa 3: Implantar uma instância do Amazon EC2 para gerenciar seu AWS Microsoft AD Active Directory gerenciado

Para este laboratório, estamos usando instâncias do Amazon EC2 que têm endereços IP públicos para facilitar o acesso à instância de gerenciamento de qualquer lugar. Em uma configuração de produção, você pode usar instâncias que estão em uma VPC privada que só podem ser acessadas por meio de uma VPN ou AWS Direct Connect link. Não é necessário que a instância tenha um endereço IP público.

Nesta seção você passará por diversas tarefas pós-implantação necessárias para que os computadores cliente se conectem ao seu domínio usando o Windows Server na nova instância do EC2. Você usará o Windows Server na próxima etapa para verificar se o laboratório está operacional.

Opcional: crie um conjunto de opções de DHCP em AWS-DS-VPC01 para seu diretório

Neste procedimento opcional, você configura um escopo de opção DHCP para que as instâncias do EC2 em sua VPC usem automaticamente seu AWS Microsoft AD gerenciado para resolução de DNS. Para obter mais informações, consulte Conjuntos de opções de DHCP.

Para criar um conjunto de opções de DHCP para o seu diretório

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conjuntos de opções DHCP e, então, selecione Criar conjuntos de opções DHCP.
3. Na página Create DHCP options set (Criar conjunto de opções DHCP), forneça os seguintes valores para o seu diretório:

- Para Name (Nome), digite **`AWS DS DHCP`**.
- Em Domain name (Nome do domínio), digite **`corp.example.com`**.
- Em Servidores de nomes de domínio, digite os endereços IP dos servidores DNS do diretório da AWS fornecido.

> **Note**
>
> Para encontrar esses endereços, acesse a página AWS Directory Service Diretórios e escolha a ID do diretório aplicável. Na página Detalhes, identifique e use os IPs que são exibidos no Endereço de DNS.
> Opcionalmente, para encontrar esses endereços, acesse a página Diretórios do AWS Directory Service e escolha o ID do diretório aplicável. Em seguida, escolha Escalar e compartilhar. Em Controladores de domínio, identifique e use os IPs que são exibidos em Endereço IP.

- Deixe em branco as configurações dos campos Servidores NTP, Servidores de nomes NetBIOS e Tipo de nó NetBIOS.

4. Selecione Create DHCP options set (Criar conjunto de opções DHCP) e selecione Close (Fechar). O novo conjunto de opções de DHCP é exibido na sua lista de opções de DHCP.
5. Anote o ID do novo conjunto de opções de DHCP (dopt-***xxxxxxxx***). Você usará esse ID no final deste procedimento quando associar o novo conjunto de opções à sua VPC.

> **Note**
>
> A associação direta a domínios funciona sem que seja necessário configurar um conjunto de opções de DHCP.

6. No painel de navegação, escolha Your VPCs (Suas VPCs).
7. Na lista de VPCs, selecione AWS DS VPC, Ações e Editar conjunto de opções de DHCP.
8. Na página Edit DHCP options set (Editar o conjunto de opções DHCP), selecione o conjunto de opções que você gravou na etapa 5 e selecione Save (Salvar).

Crie uma função para unir instâncias do Windows ao seu domínio AWS gerenciado do Microsoft AD

Use esse procedimento para configurar uma função que une uma instância Windows do Amazon EC2 a um domínio. Para ter mais informações, consulte Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory.

Para configurar o EC2 para ingressar instâncias do Windows em seu domínio

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Perfis e, em seguida, Criar perfil.
3. Em Select type of trusted entity (Selecionar o tipo de entidade confiável), escolha AWS service (serviço).
4. Imediatamente em Choose the service that will use this role (Escolher o serviço que usará essa função), selecione EC2 e Next: Permissions (Próximo: permissões).
5. Na página Attached permissions policy (Política de permissões anexada), faça o seguinte:

   - Selecione a caixa ao lado da política gerenciada do AmazonSSM. ManagedInstanceCore Essa política fornece as permissões mínimas necessárias para usar o serviço Systems Manager.
   - Selecione a caixa ao lado da política gerenciada do AmazonSSM. DirectoryServiceAccess A política fornece as permissões para ingressar instâncias em um Active Directory gerenciado pelo AWS Directory Service.

   Para obter informações sobre essas políticas gerenciadas e outras políticas que podem ser anexadas a um perfil de instância do IAM para o Systems Manager, consulte Criar um perfil de instância do IAM para o Systems Manager no Guia do usuário do AWS Systems Manager . Para obter mais informações sobre políticas gerenciadas, consulte Políticas gerenciadas pela AWSno Guia do usuário do IAM.
6. Escolha Next: Tags (Próximo: tags).
7. (Opcional) Adicione um ou mais pares de chave-valor de tag para organizar, rastrear ou controlar o acesso para esta função e selecione Next: Review (Próximo: revisar).
8. Em Nome da função, insira um nome para a função que descreva que ela é usada para unir instâncias a um domínio, como EC2 DomainJoin.
9. (Opcional) Em Role description (Descrição da função), insira uma descrição.
10. Selecione Create role (Criar função). O sistema faz com que você retorne para a página Roles.

Crie uma instância do Amazon EC2 e entre automaticamente no diretório

Neste procedimento, você configura um sistema Windows Server em uma instância do EC2 que pode ser usada posteriormente para administrar usuários, grupos e políticas no Active Directory.

Para criar uma instância do EC2 e ingressar automaticamente no diretório

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Executar instância.
3. Na página Step 1 (Etapa 1), ao lado de Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx***, selecione Select (Escolher).
4. Na página Step 2 (Etapa 2), selecione t3.micro (observe que você pode escolher um tipo de instância maior) e selecione Next: Configure Instance Details (Próximo: configurar os detalhes da instância).
5. Na página Etapa 3, faça o seguinte:
   - Em Rede, escolha a VPC que termina com AWS-DS-VPC01 (por exemplo, vpc-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01).
   - Em Sub-rede, selecione Sub-rede pública 1, que deve estar pré-configurada para a sua zona de disponibilidade preferencial (por exemplo, subnet-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01-Subnet01 | ***us-west-2a***).
   - Em Atribuir IP público automaticamente, escolha Habilitar (se a configuração de sub-rede não estiver definida por padrão).
   - Em Diretório de ingresso em domínio, escolha corp.example.com (d-***xxxxxxxxxx***).
   - Para a função do IAM, escolha o nome em que você atribuiu à função da instânciaCrie uma função para unir instâncias do Windows ao seu domínio AWS gerenciado do Microsoft AD, como EC2 DomainJoin.
   - Deixe as demais configurações com os valores padrão.
   - Escolha Next: Add Storage (Próximo: adicionar armazenamento).
6. Na página Etapa 4, mantenha as configurações padrão e escolha Próximo: adicionar tags.
7. Na página Etapa 5, selecione Adicionar tag. Em Chave, digite **`corp.example.com-mgmt`** e escolha Próximo: configurar grupo de segurança.
8. Na página Etapa 6, escolha Selecionar um grupo de segurança existente, selecione Grupo de segurança do laboratório de teste do AWS DS) (que você configurou anteriormente no Tutorial básico) e escolha Revisar e iniciar para revisar sua instância.

9. Na página Etapa 7, examine a página e escolha Iniciar.
10. Na caixa de diálogo Selecionar um par de chaves existente ou criar um novo par de chaves, faça o seguinte:

    - Escolha Selecionar um par de chaves existente.

    - Em Selecionar um par de chaves, escolha AWS-DS-KP.
    - Marque a caixa de seleção Eu reconheço....
    - Selecione Launch Instances.
11. Escolha Visualizar instâncias para retornar ao console do Amazon EC2 e visualizar o status da implantação.

Instalar as ferramentas do Active Directory na instância do EC2

Há dois métodos para instalar as ferramentas de gerenciamento de domínio do Active Directory em sua instância do EC2. Você pode usar a interface do usuário do Gerenciador de Servidores (recomendada para este tutorial) ouWindows PowerShell.

Para instalar as ferramentas do Active Directory na instância do EC2 (Gerenciador de servidores)

1. No console do Amazon EC2, escolha Instâncias, selecione a instância que você acabou de criar e escolha Conectar.
2. Na caixa de diálogo Connect To Your Instance (Conectar-se à sua instância), selecione Get Password (Obter senha) para recuperar sua senha, se ainda não tiver feito isso, e selecione Download Remote Desktop File (Fazer download do arquivo da Área de Trabalho Remota).
3. Na caixa de diálogo Segurança do Windows, digite suas credenciais de administrador local para o computador do Windows Server fazer login (por exemplo, **`administrator`**).
4. No menu Iniciar, escolha Gerenciador de servidores.
5. No Painel, escolha Adicionar funções e recursos.
6. No Assistente de adição de funções e recursos, selecione Próximo.
7. Na página Selecionar tipo de instalação, escolha Instalação baseada em função ou recurso e Próximo.
8. Na página Select destination server (Selecionar servidor de destino), verifique se o servidor local está selecionado e escolha Next (Próximo).
9. Na página Selecionar funções de servidor, escolha Próximo.

10. Na página Selecionar recursos, faça o seguinte:

    - Marque a caixa de seleção Gerenciamento de políticas de grupo.
    - Expanda Ferramentas de administração de servidores remotos e Ferramentas de administração de funções.
    - Marque a caixa de seleção Ferramentas AD DS e AD LDS.
    - Marque a caixa de seleção Ferramentas do servidor DNS.
    - Escolha Próximo.
11. Na página Confirmar seleções de instalação, reveja informações e escolha Instalar. Quando a instalação do recurso for concluída, as novas ferramentas ou snap-ins a seguir estarão disponíveis na pasta de ferramentas administrativas do Windows no menu Iniciar.

    - Central Administrativa do Active Directory
    - Domínios e confianças do Ative Directory
    - Módulo Active Directory para Windows PowerShell
    - Sites e serviços do Active Directory
    - Usuários e computadores do Active Directory
    - ADSI Edit
    - DNS
    - Gerenciamento de políticas de grupo

Para instalar as ferramentas do Active Directory em sua instância do EC2 (Windows PowerShell) (opcional)

1. Inicie Windows PowerShell.
2. Digite o seguinte comando.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-Tools,RSAT-DNS-Server
```

Etapa 4: verificar se o laboratório de teste básico está operacional

Use o procedimento a seguir para verificar o laboratório de teste foi configurado com êxito antes de acrescentar módulos guia de laboratórios de teste adicionais. Esse procedimento verifica se o

Windows Server está configurado adequadamente, pode se conectar ao domínio corp.example.com e ser usado para administrar sua floresta gerenciada do Microsoft AD. AWS

Para verificar se o laboratório de teste está operacional

1. Saia da instância do EC2 em que você estava registrado como o administrador local.
2. De volta ao console do Amazon EC2, escolha Instâncias no painel de navegação. Depois, selecione a instância que você criou. Selecione Conectar.
3. Na caixa de diálogo Conectar à sua instância, escolha Fazer download do Remote Desktop File.
4. Na caixa de diálogo Segurança do Windows, digite suas credenciais de administrador para o domínio CORP fazer login (por exemplo, **`corp\admin`**).
5. Assim que tiver feito log in, no menu Start (Iniciar), em Windows Administrative Tools (Ferramentas administrativas do Windows), escolha Active Directory Users and Computers (Usuários e computadores do Active Directory).
6. Você deve ver corp.example.com exibido com todas as UOs e contas padrão associadas a um novo domínio. Em Controladores de domínio, observe os nomes dos controladores de domínio que foram criados automaticamente quando você criou seu AWS Microsoft AD gerenciado na Etapa 2 deste tutorial.

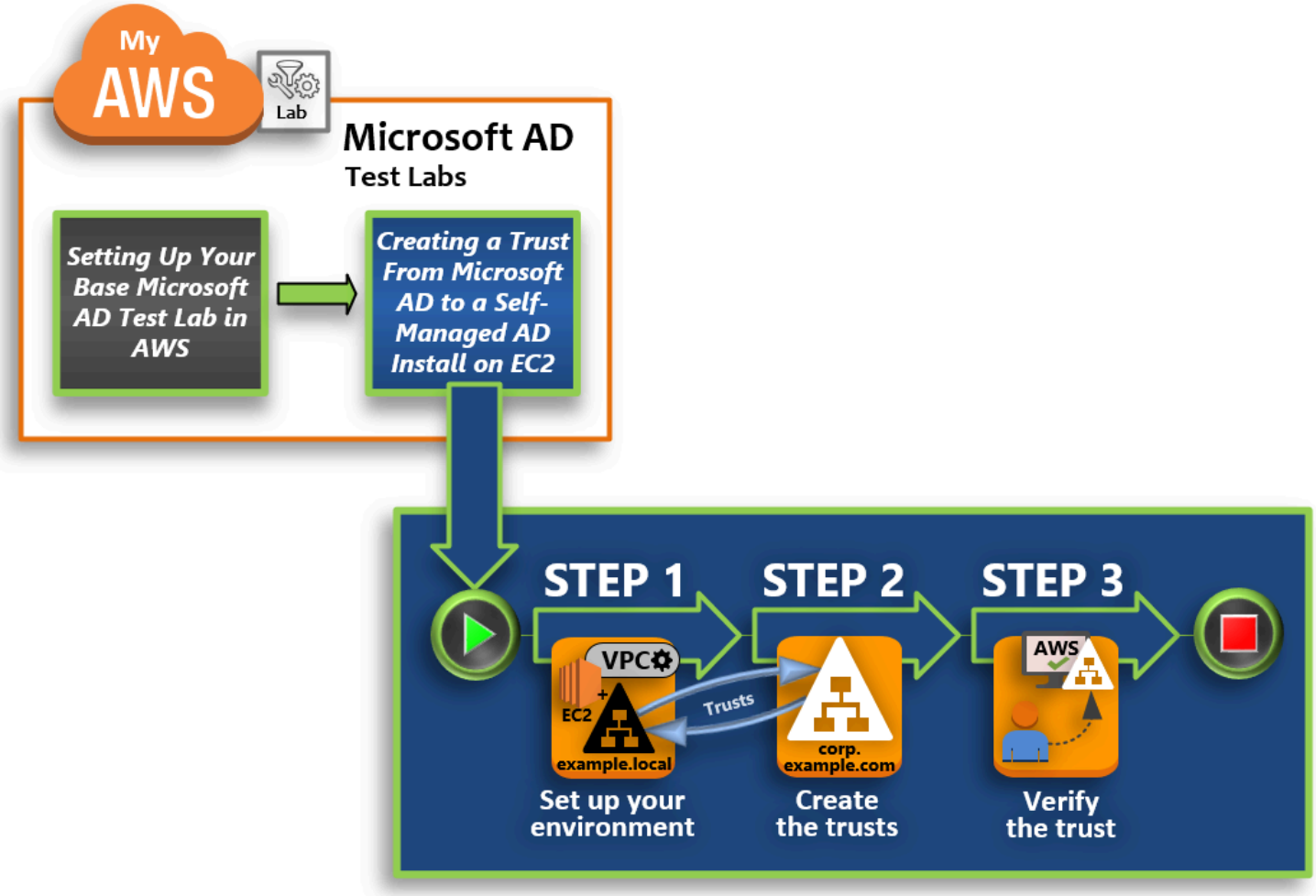
Parabéns! Seu ambiente de laboratório de teste base do Microsoft AD AWS gerenciado agora foi configurado. Você está pronto para começar a adicionar o próximo laboratório de teste na série.

Próximo tutorial: Tutorial: Criando uma relação de confiança do Microsoft AD AWS gerenciado para uma instalação autogerenciada do Active Directory no Amazon EC2

Tutorial: Criando uma relação de confiança do Microsoft AD AWS gerenciado para uma instalação autogerenciada do Active Directory no Amazon EC2

Neste tutorial, você aprende como criar uma relação de confiança entre a floresta do AWS Directory Service for Microsoft Active Directory que você criou no tutorial do Base. Você também aprenderá a criar uma nova floresta nativa do Active Directory em um Windows Server no Amazon EC2. Conforme mostrado na ilustração a seguir, o laboratório que você cria a partir deste tutorial é o segundo alicerce necessário ao configurar um laboratório de teste completo do Microsoft AD AWS gerenciado. Você pode usar o laboratório de testes para testar suas soluções baseadas AWS em nuvem pura ou híbrida.

Você só precisará criar este tutorial uma vez. Depois disso, você poderá adicionar tutoriais opcionais quando necessário para obter mais experiência.



Etapa 1: configurar o ambiente para relações de confiança

Antes de estabelecer relações de confiança entre uma nova floresta do Active Directory e a floresta do AWS Managed Microsoft AD criada no Tutorial básico, será necessário preparar o ambiente do Amazon EC2. Para fazer isso, primeiro crie um servidor do Windows Server 2019, promova esse servidor a um controlador de domínio e configure a VPC adequadamente.

Etapa 2: criar as relações de confiança

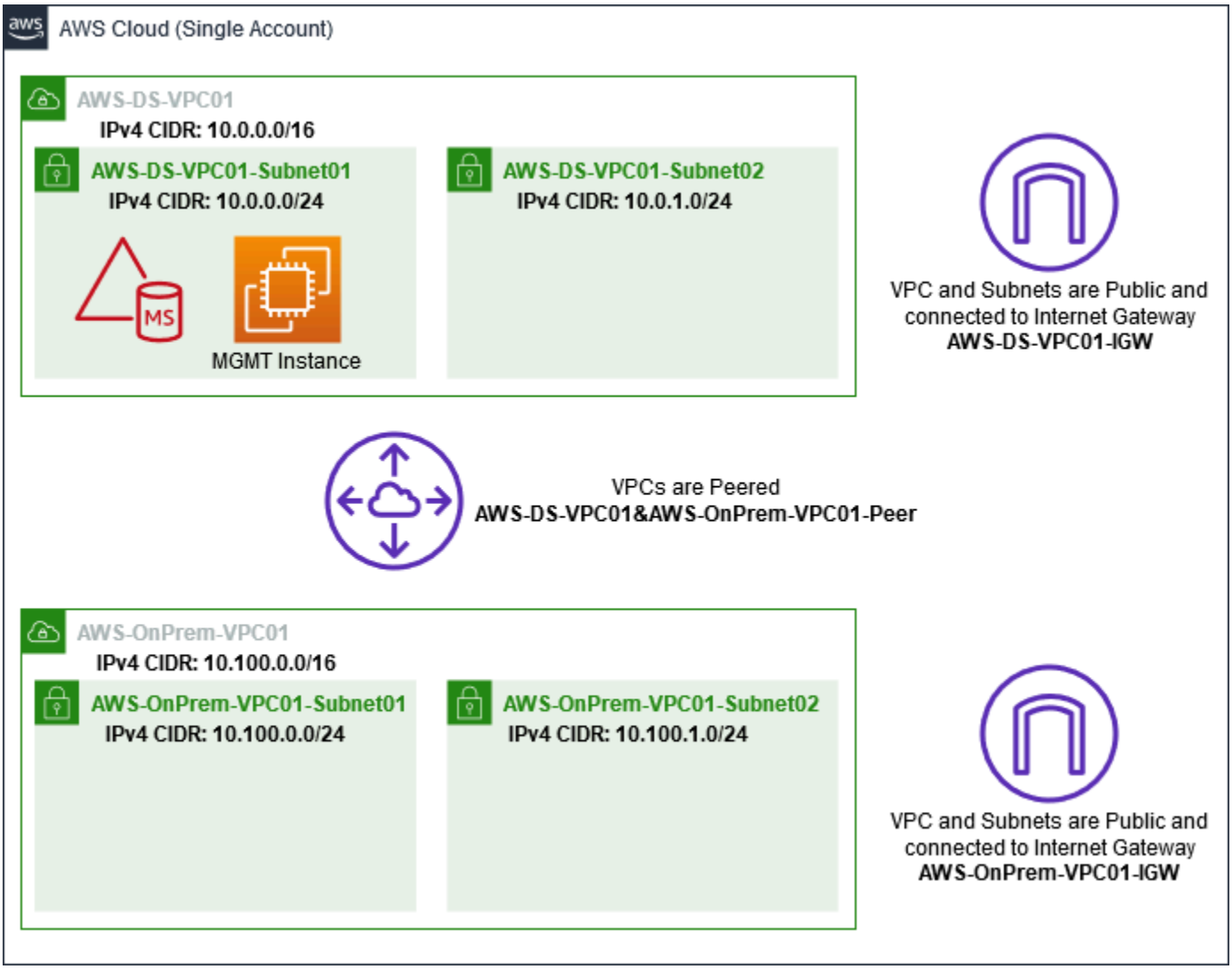
Nesta etapa, você cria uma relação de confiança florestal bidirecional entre sua floresta recém-criada do Active Directory hospedada no Amazon EC2 e sua floresta AWS gerenciada do Microsoft AD no. AWS

Etapa 3: verificar a confiança

Finalmente, como administrador, você usa o AWS Directory Service console para verificar se as novas relações de confiança estão operacionais.

Etapa 1: configurar o ambiente para relações de confiança

Nesta seção, você configura seu ambiente Amazon EC2, implanta sua nova floresta e prepara sua VPC para relações de confiança. AWS



Criar uma instância do EC2 do Windows Server 2019

Siga o procedimento a seguir para criar um servidor membro do Windows Server 2019 no Amazon EC2.

Como criar uma instância do EC2 do Windows Server 2019

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No console do Amazon EC2, escolha Iniciar instância.
3. Na página Step 1 (Etapa 1), localize Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx*** na lista. Em seguida, escolha Selecionar.
4. Na página Etapa 2, selecione t2.large e escolha Próximo: configurar os detalhes da instância.
5. Na página Etapa 3, faça o seguinte:
   - Em Rede, selecione vpc- ***xxxxxxxxxxxxxxxxx*** AWS- OnPrem -VPC01 (que você configurou anteriormente no tutorial do Base).
   - Em Sub-rede, selecione sub-rede - ***xxxxxxxxxxxxxxxxx*** | - -VPC01-Subnet01 | AWS - - VPC01. OnPrem AWS OnPrem
   - Para a lista Atribuir IP público automaticamente, escolha Habilitar (se a configuração de sub-rede não estiver definida como Habilitar por padrão).
   - Deixe as demais configurações com os valores padrão.
   - Escolha Next: Add Storage (Próximo: adicionar armazenamento).
6. Na página Etapa 4, mantenha as configurações padrão e escolha Próximo: adicionar tags.
7. Na página Etapa 5, selecione Adicionar tag. Em Chave, digite **`example.local-DC01`** e escolha Próximo: configurar grupo de segurança.
8. Na página Etapa 6, escolha Selecionar um grupo de segurança existente, selecione Grupo de segurança do laboratório de teste do AWS on premises) (que você configurou anteriormente no Tutorial básico) e escolha Revisar e iniciar para revisar sua instância.
9. Na página Etapa 7, examine a página e escolha Iniciar.
10. Na caixa de diálogo Selecionar um par de chaves existente ou criar um novo par de chaves, faça o seguinte:
    - Escolha Selecionar um par de chaves existente.
    - Em Selecionar um par de chaves, escolha AWS-DS-KP (que você configurou anteriormente no Tutorial básico).
    - Marque a caixa de seleção Eu reconheço....
    - Selecione Launch Instances.
11. Escolha Visualizar instâncias para retornar ao console do Amazon EC2 e visualizar o status da implantação.

Promover seu servidor a um controlador de domínio

Antes de criar confianças, você deve criar e implantar o primeiro controlador de domínio para uma nova floresta. Durante esse processo, configure uma nova floresta do Active Directory, instale o DNS e defina esse servidor para usar o servidor DNS local para resolução de nome. Você deve reiniciar o servidor no final deste procedimento.

> **Note**
>
> Se você quiser criar um controlador de domínio AWS que se replique com sua rede local, primeiro você deve unir manualmente a instância do EC2 ao seu domínio local. Depois disso, você pode promover o servidor a um controlador de domínio.

Para promover seu servidor a um controlador de domínio

1. No console do Amazon EC2, escolha Instâncias, selecione a instância que você acabou de criar e escolha Conectar.
2. Na caixa de diálogo Conectar à sua instância, escolha Fazer download do Remote Desktop File.
3. Na caixa de diálogo Segurança do Windows, digite suas credenciais de administrador local para o computador do Windows Server fazer login (por exemplo, **`administrator`**). Se você ainda não tem a senha de administrador local, volte ao console do Amazon EC2, clique com o botão direito na instância e escolha Obter senha do Windows. Navegue até seu `AWS DS KP.pem` arquivo ou sua chave pessoal `.pem` e escolha Descriptografar senha.
4. No menu Iniciar, escolha Gerenciador de servidores.
5. No Painel, escolha Adicionar funções e recursos.
6. No Assistente de adição de funções e recursos, selecione Próximo.
7. Na página Selecionar tipo de instalação, escolha Instalação baseada em função ou recurso e Próximo.
8. Na página Select destination server (Selecionar servidor de destino), verifique se o servidor local está selecionado e escolha Next (Próximo).
9. Na página Selecionar funções do servidor, selecione Serviços de domínio do Active Directory. Na caixa de diálogo Assistente de adição de funções e recursos, verifique se a caixa de seleção Incluir ferramentas de gerenciamento (se aplicável) está marcada. Escolha Adicionar recursos e Próximo.
10. Na página Select features, escolha Next.

11. Na página Serviços do domínio do Active Directory, escolha Próximo.
12. Na página Confirmar seleções de instalação, escolha Instalar.
13. Depois que os binários do Active Directory estiverem instalados, escolha Fechar.
14. Quando o Gerenciador de Servidores for aberto, procure um sinalizador na parte superior, ao lado da palavra Gerenciar. Quando o sinalizador ficar amarelo, o servidor estará pronto para ser promovido.
15. Escolha o sinalizador amarelo e Promover este servidor a um controlador de domínio.
16. Na página Configuração de implantação, escolha Adicionar uma nova floresta. Em Nome do domínio raiz, digite **`example.local`** e escolha Próximo.
17. Na página Opções do controlador de domínio, faça o seguinte:
    - Em Nível funcional da floresta e Nível funcional do domínio, escolha Windows Server 2016.
    - Em Especificar recursos do controlador de domínio, verifique se o servidor DNS e o Catálogo Global (GC) estão selecionados.
    - Digite e confirme uma senha do Directory Services Restore Mode (DSRM). Em seguida, escolha Próximo.
18. Na página Opções de DNS, ignore o aviso sobre a delegação e escolha Próximo.
19. Na página Opções adicionais, verifique se EXAMPLE está listado como nome de NetBios domínio.
20. Na página Caminhos, mantenha os padrões e escolha Próximo.
21. Na página Opções de análise, escolha Próximo. Agora o servidor verifica se todos os pré-requisitos do controlador de domínio foram atendidos. Alguns avisos podem ser exibidos, mas você pode ignorá-los.
22. Escolha Instalar. Após a conclusão da instalação, o servidor é reiniciado e se transforma em um controlador de domínio funcional.

Configurar a VPC

Os três procedimentos a seguir orientam sobre as etapas para configurar sua VPC para conectividade com a AWS.

Para configurar as regras de saída da VPC

1. No AWS Directory Service console, anote o ID do diretório AWS gerenciado do Microsoft AD para corp.example.com que você criou anteriormente no tutorial do Base.

2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
3. No painel de navegação, selecione Security Groups.(Grupos de segurança).
4. Pesquise seu ID de diretório AWS gerenciado do Microsoft AD. Nos resultados da pesquisa, selecione o item com a descrição Grupo de segurança criado pela AWS para controladores de diretório d-***xxxxxx***.

> **Note**
>
> Esse grupo de segurança foi criado automaticamente quando você criou seu diretório.

5. Escolha a guia Outbond Rules (Regras de saída) daquele grupo de segurança. Escolha Editar, Adicionar outra regra e adicione os seguintes valores:

   - Em Tipo, escolha Todo o tráfego.
   - Em Destination, digite **`0.0.0.0/0`**.
   - Deixe as demais configurações com os valores padrão.
   - Selecione Save (Salvar).

Para verificar se a pré-autenticação Kerberos está habilitada

1. No controlador de domínio example.local, abra o Gerenciador de Servidores.
2. No menu Tools, escolha Active Directory Users and Computers (Usuários e computadores do Active Directory).
3. Navegue até o diretório Users (Usuários), clique com o botão direito do mouse em qualquer usuário e selecione Properties (Propriedades) e escolha a guia Account (Conta). Na lista Account options (Opções de conta), role para baixo e confirme se a opção Do not require Kerberos preauthentication (Não exige pré-autenticação do Kerberos) não está selecionada.
4. Siga as mesmas etapas para o domínio corp.example.com da instância corp.example.com-mgmt.

Para configurar encaminhadores condicionais de DNS

> **Note**
>
> Um encaminhador condicional é um servidor DNS em uma rede que é usado para encaminhar consultas DNS de acordo com o nome de domínio DNS na consulta. Por

exemplo, um servidor DNS pode ser configurado para encaminhar todas as consultas recebidas para nomes terminados com widgets.example.com para o endereço IP de um servidor DNS específico ou para os endereços IP de vários servidores DNS.

1. Abra o console de AWS Directory Service.
2. No painel de navegação, selecionar Diretórios.
3. Selecione o ID do diretório do seu Microsoft AD AWS gerenciado.
4. Anote o nome completo do domínio (FQDN), corp.example.com e os endereços DNS do seu diretório.
5. Agora, retorne ao controlador de domínio example.local e abra o Gerenciador de Servidores.
6. No menu Ferramentas, escolha DNS.
7. Na árvore do console, expanda o servidor DNS do domínio para o qual você está configurando a confiança e navegue até Encaminhadores condicionais.
8. Clique com o botão direito em Encaminhadores condicionais e escolha Novo encaminhador condicional.
9. No domínio DNS, digite **`corp.example.com`**.
10. Em Endereços IP dos servidores primários, escolha <Clique aqui para adicionar... >, digite o primeiro endereço DNS do seu diretório AWS gerenciado do Microsoft AD (que você anotou no procedimento anterior) e pressione Enter. Faça o mesmo para o segundo endereço DNS. Depois de digitar os endereços DNS, você poderá ver um erro como "tempo limite" ou "não foi possível resolver". Em geral, você pode ignorar esses erros.
11. Marque a caixa de seleção Store this conditional forwarder in Active Directory, and replicate it as follows. No menu suspenso, escolha Todos os servidores DNS nesta floresta e OK.

Etapa 2: criar as relações de confiança

Nesta seção, você cria duas confianças separadas para a floresta. Uma relação de confiança é criada a partir do domínio do Active Directory na sua instância do EC2 e a outra a partir do seu Microsoft AD AWS gerenciado em AWS.

Para criar a confiança do seu domínio EC2 em seu Microsoft AD AWS gerenciado

1. Faça login em example.local.
2. Abra o Gerenciador de Servidores e, na árvore do console, escolha DNS. Anote o endereço IPv4 listado para o servidor. Você precisará dele no próximo procedimento, quando criar um encaminhador condicional de corp.example.com para o diretório example.local.
3. No menu Ferramentas, escolha Domínios e confianças do Ative Directory.
4. Na árvore do console, clique com o botão direito em example.local e escolha Propriedades.
5. Na guia Confianças, escolha Nova confiança e escolha Próximo.
6. Na página Nome da confiança, digite **`corp.example.com`** e escolha Próximo.
7. Na página Tipo de confiança, escolha Confiança da floresta e Próximo.

   > **Note**
   >
   > AWS O Microsoft AD gerenciado também oferece suporte a relações de confiança externas. Contudo, para os propósitos deste tutorial, você criará uma confiança de floresta bidirecional.

8. Na página Direção da confiança, escolha Bidirecional e Próximo.

   > **Note**
   >
   > Se você decidir tentar isso posteriormente com uma confiança unidirecional, as direções de confiança deverão estar configuradas corretamente (Saída em domínio confiável, Entrada em domínio confiável). Para obter informações gerais, consulte Entender a direção da relação de confiança no site da Microsoft.

9. Na página Lados da confiança, escolha Apenas este domínio e Próximo.
10. Na página Nível de autenticação de confiança de saída, escolha Autenticação em toda a floresta e, depois, Próximo.

> **Note**
>
> Embora a Selective authentication (Autenticação seletiva) seja uma opção, para a simplicidade deste tutorial, recomendamos que você não a habilite aqui. Quando configurada, ela restringe o acesso por uma confiança externa ou de floresta apenas aos usuários em um domínio ou uma floresta confiável que receberam explicitamente permissões de autenticação a objetos de computador (computadores de recurso) residentes no domínio ou na floresta confiável. Para obter mais informações, consulte Configurar autenticação seletiva.

11. Na página Senha da confiança, digite a senha da confiança duas vezes e escolha Próximo. Você usará essa mesma senha no próximo procedimento.
12. Na página Seleções de confiança concluídas, revise os resultados e escolha Próximo.
13. Na página Criação da confiança concluída, revise os resultados e escolha Próximo.
14. Na página Confirmar confiança de saída, escolha Não confirmar a confiança de saída. Em seguida, escolha Próximo
15. Na página Confirmar confiança de entrada, escolha Não confirmar a confiança de entrada. Em seguida, escolha Próximo
16. Na página Assistente de conclusão da nova confiança, escolha Concluir.

> **Note**
>
> Relações de confiança são um recurso global do AWS Managed Microsoft AD. Se você estiver usando o Replicação em várias regiões, os procedimentos a seguir deverão ser executados no Região principal. As alterações serão aplicadas automaticamente em todas as regiões replicadas. Para ter mais informações, consulte Recursos globais versus regionais.

Para criar a confiança do seu Microsoft AD AWS gerenciado em seu domínio EC2

1. Abra o console de AWS Directory Service.
2. Escolha o diretório corp.example.com.
3. Na página Detalhes do diretório, siga um destes procedimentos:

- Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
- Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.

4. Na seção Trust relationships (Relações de confiança), selecione Action (Ação) e selecione Add trust relationship (Adicionar relação de confiança).
5. Na caixa de diálogo Adicionar uma relação de confiança, faça o seguinte:

- Em Trust type (Tipo de confiança), selecione Forest trust (Confiança de floresta).

> **Note**
>
> Certifique-se de que o tipo de confiança escolhido aqui corresponda ao mesmo tipo de confiança configurado no procedimento anterior (Para criar a confiança do seu domínio EC2 para o Microsoft AD AWS gerenciado).

- Em Existing or new remote domain name (Nome de domínio remoto existente ou novo), digite example.local.
- Em Senha da confiança, digite a mesma senha que você forneceu no procedimento anterior.
- Em Trust direction (Direção da confiança), selecione Two-Way (Bidirecional).

> **Note**
>
> - Se você decidir tentar isso posteriormente com uma confiança unidirecional, as direções de confiança deverão estar configuradas corretamente (Saída em domínio confiável, Entrada em domínio confiável). Para obter informações gerais, consulte Entender a direção da relação de confiança no site da Microsoft.
> - Embora a Selective authentication (Autenticação seletiva) seja uma opção, para a simplicidade deste tutorial, recomendamos que você não a habilite aqui. Quando configurada, ela restringe o acesso por uma confiança externa ou de floresta apenas aos usuários em um domínio ou uma floresta confiável que receberam explicitamente permissões de autenticação a objetos de computador (computadores de recurso) residentes no domínio ou na floresta confiável. Para obter mais informações, consulte Configurar autenticação seletiva.

- Em Conditional forwarder (Encaminhador condicional), digite o endereço IP do servidor DNS na floresta example.local (que você anotou no procedimento anterior).

> **Note**
>
> Um encaminhador condicional é um servidor DNS em uma rede que é usado para encaminhar consultas DNS de acordo com o nome de domínio DNS na consulta. Por exemplo, um servidor DNS pode ser configurado para encaminhar todas as consultas recebidas para nomes terminados com widgets.example.com para o endereço IP de um servidor DNS específico ou para os endereços IP de vários servidores DNS.

6. Escolha Adicionar.

Etapa 3: verificar a confiança

Nesta seção, você testará se as relações de confiança foram configuradas com êxito entre a AWS e o Active Directory no Amazon EC2.

Para verificar a confiança

1. Abra o console de AWS Directory Service.
2. Escolha o diretório corp.example.com.
3. Na página Detalhes do diretório, siga um destes procedimentos:
   - Se houver várias regiões exibidas em Replicação em várias regiões, selecione a região principal e, em seguida, escolha a guia Rede e segurança. Para ter mais informações, consulte Regiões principais versus adicionais.
   - Se não houver nenhuma região exibida em Replicação em várias regiões, escolha a guia Rede e segurança.
4. Na seção Trust relationships (Relações de confiança), selecione a relação de confiança que você acabou de criar.
5. Escolha Ações e Verificar relação de confiança.

Após a conclusão da verificação, você deverá ver Verificada na coluna Status.

Parabéns por concluir este tutorial! Agora você tem um ambiente do Active Directory multifloresta funcional a partir do qual você pode começar a testar vários cenários. Outros tutoriais de laboratório de teste estão planejados para 2018. Portanto, fique atento às novidades.

Solução de problemas do Microsoft AD AWS gerenciado

Os tópicos a seguir podem ajudá-lo a solucionar alguns problemas comuns que podem ser encontrados ao criar ou usar o diretório.

Problemas com seu Microsoft AD AWS gerenciado

Algumas tarefas de solução de problemas só podem ser concluídas por AWS Support. Aqui estão algumas das tarefas:

- Reiniciando seus AWS Directory Service controladores de domínio fornecidos.
- Atualize seu Microsoft AD AWS gerenciado.

Para criar um caso de suporte, consulte Criação de casos de suporte e gerenciamento de casos.

Problemas com o Netlogon e comunicações por canais seguros

Como uma mitigação contra o CVE-2020-1472, a Microsoft lançou um patch que modifica a forma como as comunicações por canal seguro do Netlogon são processadas pelos controladores de domínio. Desde a introdução dessas alterações seguras do Netlogon, algumas conexões do Netlogon (servidores, estações de trabalho e validações de confiança) podem não ser aceitas pelo seu Microsoft AD gerenciado. AWS

Para verificar se seu problema está relacionado ao Netlogon ou às comunicações por canais seguros, pesquise no Amazon CloudWatch Logs as IDs de evento 5827 (para problemas relacionados à autenticação do dispositivo) ou 5828 (para problemas relacionados à validação de confiança do AD). Para obter informações sobre o CloudWatch AWS Managed Microsoft AD, consulteHabilitar o encaminhamento de logs.

Para obter mais informações sobre a mitigação contra o CVE-2020-1472, consulte Como gerenciar as alterações nas conexões por canais seguros do Netlogon associadas ao CVE-2020-1472 no site da Microsoft.

Problemas com a redefinição da senha do usuário

Você recebe uma mensagem de erro semelhante à seguinte ao tentar redefinir a senha de um usuário:

```
Response Status: 400 Bad Request
```

Você pode enfrentar esse problema quando há objetos duplicados em sua Unidade Organizacional (OU) AWS gerenciada do Microsoft AD com nomes de logon de usuário idênticos. Os nomes de login do usuário devem ser exclusivos. Consulte Solução de problemas de dados do diretório na Microsoft documentação para obter mais informações.

Recuperação de senha

Se um usuário esquecer uma senha ou estiver tendo problemas para entrar no diretório Simple AD ou AWS Managed Microsoft AD, você poderá redefinir a senha usando o AWS Management Console, Windows PowerShell ou o. AWS CLI

Para obter mais informações, consulte Redefinir uma senha de usuário.

Recursos adicionais

Os recursos a seguir podem ajudá-lo a solucionar problemas enquanto você trabalha com AWS.

- AWS Centro de conhecimento — encontre perguntas frequentes e links para outros recursos para ajudá-lo a solucionar problemas.
- AWS Support Center — Obtenha suporte técnico.
- AWS Premium Support Center — Obtenha suporte técnico premium.

Os recursos a seguir podem ajudá-lo a solucionar Active Directory problemas comuns.

- Documentação do Active Directory
- AD DSSolução de problemas

Tópicos

- Monitorar o servidor de DNS com o Visualizador de Eventos da Microsoft
- Erros de associação a domínios do Linux

- Pouco espaço de armazenamento disponível no Active Directory
- Erros de extensões de esquema
- Motivos do status da criação de relações de confiança

Monitorar o servidor de DNS com o Visualizador de Eventos da Microsoft

Você pode auditar eventos de DNS do seu AWS Managed Microsoft AD, o que o torna mais fácil identificar e solucionar problemas de DNS. Por exemplo, se um registro do DNS estiver ausente, você poderá usar o log de eventos de auditoria do DNS para ajudar a identificar a causa principal e corrigir o problema. Você também pode usar logs de eventos de auditoria de DNS para melhorar a segurança detectando e bloqueando solicitações de endereços IP suspeitos.

Para fazer isso, é necessário fazer login com a conta de Admin ou com uma conta que seja membro do grupo de Administradores do AWS Domain Name System. Para obter mais informações sobre esse grupo, consulte O que é criado com seu Microsoft AD Active Directory AWS gerenciado.

Para acessar o Visualizador de Eventos para seu DNS do AWS Managed Microsoft AD

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Localize uma instância da instância do Amazon EC2 associada a seu diretório do AWS Managed Microsoft AD. Selecione a instância e escolha Conectar.
4. Depois de conectado à instância do Amazon EC2, abra o menu Iniciar e selecione a pasta Ferramentas Administrativas do Windows. Na pasta Ferramentas Administrativas, selecione Visualizador de Eventos.
5. Na janela Visualizador de eventos, escolha Ação e escolha Conectar a outro computador.
6. Selecione Outro computador, digite o nome ou endereço IP de um dos servidores DNS do AWSManaged Microsoft AD e escolha OK.
7. No painel esquerdo, acesse Logs de aplicativos e serviços>Microsoft>Windows>DNS-Server e selecione Auditoria.

Erros de associação a domínios do Linux

As informações a seguir podem ajudar a solucionar algumas mensagens de erro que você pode encontrar ao incluir uma instância EC2 do Linux ao seu diretório do AWS Managed Microsoft AD.

Não foi possível autenticar ou incluir instâncias do Linux ao domínio

As instâncias do Ubuntu 14.04, 16.04 e 18.04 devem ter resolução reversa no DNS para que um realm possa funcionar com o Microsoft Active Directory. Caso contrário, você poderá enfrentar um dos dois cenários a seguir:

Cenário 1: instâncias do Ubuntu que ainda não estão associadas a um realm

Para instâncias do Ubuntu que estão tentando ingressar em um realm, o comando `sudo realm join` pode não fornecer as permissões necessárias para ingressar no domínio e pode exibir o seguinte erro:

! Não foi possível autenticar para o diretório ativo: SASL(-1): falha genérica: Erro de GSSAPI: um nome inválido foi fornecido (Sucesso) adcli: não foi possível conectar ao domínio EXAMPLE.COM: Não foi possível autenticar para o diretório ativo: SASL(-1): falha genérica: Erro de GSSAPI: Um nome inválido foi fornecido (Êxito) ! Permissões insuficientes para ingressar no realm do domínio: não foi possível ingressar no realm: permissões insuficientes para ingressar no domínio

Cenário 2: instâncias do Ubuntu que estão associadas a um realm

Para instâncias do Ubuntu que já estão associadas a um domínio do Microsoft Active Directory, as tentativas de SSH na instância usando as credenciais do domínio podem falhar com os seguintes erros:

$ ssh admin@EXAMPLE.COM@198.51.100

identidade inexistente: /Users/username/.ssh/id_ed25519: Arquivo ou diretório inexistente

admin@EXAMPLE.COM@198.51.100's password:

Permissão negada, tente novamente.

admin@EXAMPLE.COM@198.51.100's password:

Se você fizer login na instância com uma chave pública e verificar o arquivo `/var/log/auth.log`, poderá visualizar os seguintes erros sobre a incapacidade de localizar o usuário:

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_unix(sshd:auth): falha na autenticação; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): falha na autenticação; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0 user=admin@EXAMPLE.COM

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): recebido para o usuário admin@EXAMPLE.COM: 10 (Usuário não reconhecido pelo módulo de autenticação subjacente)

May 12 01:02:14 ip-192-0-2-0 sshd[2251]: falha na senha para usuário inválido admin@EXAMPLE.COM from 203.0.113.0 port 13344 ssh2

May 12 01:02:15 ip-192-0-2-0 sshd[2251]: Conexão fechada por 203.0.113.0 [preauth]

No entanto, o `kinit` para o usuário ainda funciona. Veja este exemplo:

ubuntu@ip-192-0-2-0:~$ kinit admin@EXAMPLE.COM Senha para admin@EXAMPLE.COM: ubuntu@ip-192-0-2-0:~$ klist Cache do ticket: FILE:/tmp/krb5cc_1000 Principal padrão: admin@EXAMPLE.COM

Solução temporária

A solução recomendada atual para ambos os cenários é desabilitar o DNS reverso em `/etc/krb5.conf` na seção [libdefaults] conforme mostrado a seguir:

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Problema de autenticação confiável unidirecional com associação direta ao domínio

Se você tiver uma relação de confiança de saída unidirecional estabelecida entre seu AWS Microsoft AD gerenciado e seu Active Directory local, você pode encontrar um problema de autenticação ao tentar se autenticar na instância Linux associada ao domínio usando suas credenciais confiáveis do Active Directory com o Winbind.

Erros

Jul 31 00:00:00 EC2AMAZ-LSMWqT sshd[23832]: Falha na senha para user@corp.example.com de xxx.xxx.xxx.xxx porta 18309 ssh2

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): ao obter senha (0x00000390)

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): pam_get_item retornou uma senha

31 de julho 00:05:00 EC2AMAZ-LSMWQT sshd [23832]: pam_winbind (sshd:auth): falha na solicitação: WBC_ERR_AUTH_ERROR, erro PAM: PAM_SYSTEM_ERR (4), NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**, A mensagem de erro foi: O nome do wbcLogonUser objeto não foi encontrado.

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): erro de módulo interno (retval = PAM_SYSTEM_ERR(4), user = 'CORP\user')

Solução temporária

Para resolver esse problema, você precisará comentar ou remover uma diretiva do arquivo de configuração do módulo PAM (`/etc/security/pam_winbind.conf`) de acordo com as etapas a seguir.

1. Abra o arquivo `/etc/security/pam_winbind.conf` em um editor de textos.

   ```
   sudo vim /etc/security/pam_winbind.conf
   ```

2. Comente ou remova a seguinte diretiva krb5_auth = yes.

   ```
   [global]

   cached_login = yes
   krb5_ccache_type = FILE
   #krb5_auth = yes
   ```

3. Pare o serviço Winbind e inicie-o novamente.

   ```
   service winbind stop or systemctl stop winbind
   net cache flush
   service winbind start or systemctl start winbind
   ```

Pouco espaço de armazenamento disponível no Active Directory

Quando seu Microsoft AD AWS gerenciado está comprometido devido ao fato de o Active Directory ter pouco espaço de armazenamento disponível, é necessária uma ação imediata para retornar o diretório ao estado ativo. As duas causas mais comuns desse problema são abordadas nas seções abaixo:

1. A pasta SYSVOL está armazenando mais do que objetos essenciais da política de grupo

2. O banco de dados do Active Directory preencheu o volume

Para obter informações sobre preços sobre o armazenamento AWS gerenciado do Microsoft AD, consulte AWS Directory Service Preços.

A pasta SYSVOL está armazenando mais do que objetos essenciais da política de grupo

Uma causa comum desse problema é o armazenamento de arquivos não essenciais para processamento da política de grupo na pasta SYSVOL. Esses arquivos não essenciais podem ser EXEs, MSIs ou qualquer outro arquivo que não seja essencial para a política de grupo processar. Os objetos essenciais para a política de grupo processar são os objetos da política de grupo, os scripts de logon\logoff e o Repositório central para objetos da política de grupo. Todos os arquivos não essenciais devem ser armazenados em um (s) servidor (es) de arquivos diferente dos controladores de domínio AWS gerenciados do Microsoft AD.

Se forem necessários arquivos para a Instalação do software da política de grupo, você deverá usar um servidor de arquivos para armazenar esses arquivos de instalação. Se você preferir não autogerenciar um servidor de arquivos, AWS fornece uma opção de servidor de arquivos gerenciado, o Amazon FSx.

Para remover quaisquer arquivos desnecessários, você pode acessar o compartilhamento SYSVOL através do caminho UNC (Universal naming convention, Convenção de nomenclatura universal). Por exemplo, se o FQDN (Fully qualified domain name, Nome de domínio totalmente qualificado) for example.com, o caminho UNC para SYSVOL será “\\example.local\SYSVOL\example.local\”. Depois de localizar e remover os objetos não essenciais para a política de grupo processar o diretório, ele deve regressar a um estado Active (Ativo) dentro de 30 minutos. Se após 30 minutos o diretório não estiver ativo, entre em contato com o AWS Support.

Armazenar apenas arquivos essenciais da política de grupo em seu compartilhamento SYSVOL garantirá que você não prejudique seu diretório devido à sobrecarga do SYSVOL.

O banco de dados do Active Directory preencheu o volume

Uma causa comum desse problema é o banco de dados do Active Directory preencher o volume. Para verificar se é esse o caso, você pode revisar a contagem total de objetos no seu diretório. A palavra total está em negrito para garantir que você entenda que os objetos deleted (excluídos) ainda são contabilizados no número total de objetos em um diretório.

Por padrão, o Microsoft AD AWS gerenciado mantém os itens na lixeira do AD por 180 dias antes de se tornarem um objeto reciclado. Depois de se tornar um Objeto reciclado (para exclusão), o objeto é retido por mais 180 dias antes de ser finalmente eliminado do diretório. Portanto, quando um objeto é excluído, ele fica no banco de dados do diretório por 360 dias antes de ser limpo. É por isso que o número total de objetos precisa ser avaliado.

Para obter mais detalhes sobre as contagens de objetos compatíveis com o Microsoft AD AWS gerenciado, consulte AWS Directory Service Preços.

Para obter o número total de objetos em um diretório que inclui os objetos excluídos, você pode executar o PowerShell comando a seguir em uma instância do Windows associada ao domínio. Para obter as etapas de configuração de uma instância de gerenciamento, consulte Gerenciar usuários e grupos no AWS Microsoft Managed AD.

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
 Select-Object -Property 'Count'
```

Veja abaixo um exemplo de saída do comando acima:

```
Count
10000
```

Se a contagem total estiver acima da contagem de objetos compatível com o tamanho do diretório listado na observação acima, você excedeu a capacidade do diretório.

Veja abaixo as opções para resolver esse problema:

1. Limpeza AD
   a. Excluir todos os objetos indesejados do AD.
   b. Remover todos os objetos indesejados da Lixeira do AD. Observe que trata-se de uma ação destrutiva e a única maneira de recuperar esses objetos excluídos será executar uma restauração do diretório.
   c. O comando a seguir removerá todos os objetos excluídos da Lixeira do AD.

> **Important**
>
> Use este comando com extrema cautela, pois trata-se de um comando destrutivo e a única maneira de recuperar esses objetos excluídos será executar uma restauração do diretório.

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
 'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
 { ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
 '*\0ADEL:*') }
ForEach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
 $ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

d. Abra um caso com o AWS Support para solicitar que AWS Directory Service recupere o espaço livre.

2. Se seu tipo de diretório for Standard Edition, abra um caso com o AWS Support solicitando que seu diretório seja atualizado para a Enterprise Edition. Isso também aumentará o custo do seu diretório. Para obter informações sobre a definição de preço, consulte Definição de preço do AWS Directory Service.

No AWS Managed Microsoft AD, os membros do grupo AWS Delegated Deleted Object Lifetime Administrators têm a capacidade de modificar o `msDS-DeletedObjectLifetime` atributo que define por quanto tempo, em dias, os objetos excluídos são mantidos na Lixeira do AD antes de se tornarem Objetos Reciclados.

> **Note**
>
> Este é um tópico avançado. Se for configurado incorretamente, ele poderá resultar em perda de dados. É altamente recomendável que você consulte primeiro A Lixeira do AD: noções básicas, implementação, práticas recomendadas e solução de problemas para obter uma melhor compreensão desses processos.

A capacidade de alterar o valor do atributo `msDS-DeletedObjectLifetime` para um número menor pode ajudar a garantir que a contagem de objetos não exceda os níveis com suporte. O menor valor válido em que este atributo pode ser definido é 2 dias. Depois que esse valor for excedido, você não poderá mais recuperar o objeto excluído usando a Lixeira do AD. Isso exigirá a restauração do seu diretório a partir de um snapshot para recuperar o(s) objeto(s). Para ter mais informações, consulte Criar um snapshot ou restaurar seu diretório. Todas as restaurações de um snapshot podem causar perda de dados, pois elas são de um momento em específico.

Para alterar o tempo de vida do objeto excluído do diretório, execute o comando a seguir:

> **Note**
>
> Se você executar o comando como ele está, ele definirá o valor do atributo Deleted Object Lifetime como 30 dias. Se você quiser tornar esse período mais longo ou mais curto, substitua “30” pelo número que preferir. No entanto, recomendamos que você não ultrapasse o número padrão de 180.

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows
 NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -
Replace:@{"msDS-DeletedObjectLifetime" = $DeletedObjectLifetime}
```

Erros de extensões de esquema

As informações a seguir podem ajudar a solucionar algumas mensagens de erro que você pode encontrar ao ampliar o esquema do seu diretório do AWS Managed Microsoft AD.

Referência

Erro

> Adicione o erro na entrada a partir da linha 1: Referência O erro do lado do servidor é: 0x202b Uma referência foi retornada do servidor. O erro de servidor estendido é: 0000202B: RefErr: DSID-0310082F, dados 0, 1 pontos de acesso \tref 1: ‘example.com’ Número de objetos modificados: 0

Solução de problemas

Verifique se todos os campos de nome diferenciados têm o nome de domínio correto. No exemplo acima, `DC=example,dc=com` deve ser substituído pelo `DistinguishedName` mostrado pelo cmdlet `Get-ADDomain`.

Não é possível ler o arquivo de importação

Erro

Não é possível ler o arquivo de importação. Número de objetos modificados: 0

Solução de problemas

O arquivo LDIF importado está vazio (0 byte). Verifique se o arquivo correto foi carregado.

Erro de sintaxe

Erro

Há um erro de sintaxe no arquivo de entrada Falha na linha 21. O último token começa com "q". Número de objetos modificados: 0

Solução de problemas

O texto na linha 21 não está formatado corretamente. A primeira letra do texto inválido é `A`. Atualize a linha 21 com uma sintaxe LDIF válida. Para obter mais informações sobre como formatar o arquivo LDIF, consulte Etapa 1: criar seu arquivo LDIF.

Um atributo ou valor existe

Erro

Adicione o erro na entrada a partir da linha 1: Um atributo ou valor existe O erro do lado do servidor é: 0x2083 O valor especificado já existe. O erro de servidor estendido é: 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, problema 1006 (ATT_OR_VALUE_EXISTS), dados 0, Att 20019 (mayContain):len 4 Número de objetos modificados: 0

Solução de problemas

A alteração do esquema já foi aplicada.

Esse atributo não existe

Erro

Adicione o erro na entrada a partir da linha 1: Esse atributo não existe O erro do lado do servidor é: 0x2085 O valor do atributo não pode ser removido porque não está presente no objeto. O erro de servidor estendido é: 00002085: AtrErr: DSID-03152367, #1: \t0: 00002085: DSID-03152367, problema 1001 (NO_ATTRIBUTE_OR_VAL), dados 0, Att 20019 (mayContain):len 4 Número de objetos modificados: 0

Solução de problemas

O arquivo LDIF está tentando remover um atributo de uma classe, mas esse atributo não está vinculado à classe no momento. A alteração do esquema provavelmente já foi aplicada.

Erro

Adicione o erro na entrada a partir da linha 41: Esse atributo não existe 0x57 O parâmetro está incorreto. O erro de servidor estendido é: 0x208d O objeto do diretório não foi encontrado. O erro de servidor estendido é: "00000057: LdapErr: DSID-0C090D8A, comentário: Erro na operação de conversão do atributo, dados 0, v2580" Número de objetos modificados: 0

Solução de problemas

O atributo listado na linha 41 está incorreto. Verifique a ortografia novamente.

Esse objeto não existe

Erro

Adicione o erro na entrada a partir da linha 1: Esse objeto não existe O erro do lado do servidor é: 0x208d O objeto do diretório não foi encontrado. O erro de servidor estendido é: 0000208D: NameErr: DSID-03100238, problema 2001 (NO_OBJECT), dados 0, melhor correspondência de: "CN=Schema, CN=Configuration,DC=example,DC=com" Número de objetos modificados: 0

Solução de problemas

O objeto referenciado pelo nome distinto (DN) não existe.

Motivos do status da criação de relações de confiança

Quando a criação da confiança falha, a mensagem de status contém informações adicionais. O seguinte ajuda a compreender o que essas mensagens significam.

O acesso é negado

O acesso foi negado ao tentar criar a confiança. A senha da confiança está incorreta ou as configurações de segurança de domínio remoto não permitem que uma confiança seja configurada. Para resolver esse problema, tente o seguinte:

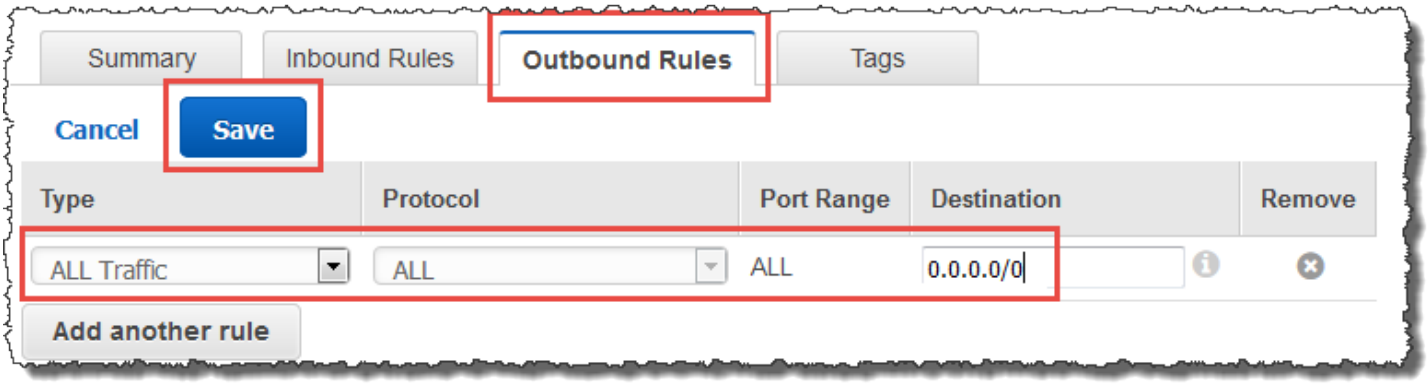
- O Microsoft AD AWS gerenciado Active Directory e o autogerenciado com o Active Directory qual você deseja criar uma relação de confiança devem ter o mesmo nome de primeiro site. O nome do primeiro site está definido como`Default-First-Site-Name`. Um erro de acesso negado ocorre se esses nomes variarem entre os domínios.
- Verifique se você está usando a mesma senha de confiança usada ao criar a confiança correspondente no domínio remoto.
- Verifique se as configurações de segurança do domínio permitem a criação de confiança.
- Verifique se a política de segurança local está definida corretamente. Marque especificamente `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` e verifique se a opção contém pelo menos os três pipes nomeados a seguir:
  - netlogon
  - samr
  - lsarpc
- Verifique se os pipes nomeados acima existem como valores na chave do registro que está no caminho NullSessionPipesdo registro HKLM\ SYSTEM\\ services\CurrentControlSet\ Parameters LanmanServer. Esses valores devem ser inseridos em linhas separadas.

> **Note**
>
> Por padrão, a opção `Network access: Named Pipes that can be accessed anonymously` não está definida e exibe `Not Defined`. Isso é normal, uma vez que as configurações efetivas do controlador de domínio para `Network access: Named Pipes that can be accessed anonymously` são `netlogon`, `samr`, `lsarpc`.

- Verifique a seguinte configuração de assinatura do Server Message Block (SMB) na política de controladores de domínio padrão. Essas configurações podem ser encontradas em Configuração do computador > Configurações do Windows > Configurações de segurança > Políticas locais/ Opções de segurança. Eles devem corresponder às seguintes configurações:
  - Microsoftcliente de rede: assine digitalmente as comunicações (sempre): Padrão: Ativado
  - Microsoftcliente de rede: assine digitalmente as comunicações (se o servidor concordar): Padrão: Ativado
  - Microsoftservidor de rede: assine digitalmente as comunicações (sempre): Ativado
  - Microsoftservidor de rede: assine digitalmente as comunicações (se o cliente concordar): Padrão: Ativado

O nome do domínio especificado não existe ou não pôde ser contatado.

Para resolver o problema, verifique se as configurações do grupo de segurança de seu domínio e a lista de controle de acesso (ACL) da sua VPC estão corretas e se você inseriu as informações de maneira precisa para o encaminhador condicional. A AWS configura o grupo de segurança para abrir somente as portas necessárias para as comunicações do Active Directory. Na configuração padrão, o grupo de segurança aceita o tráfego para essas portas de qualquer endereço IP. O tráfego de saída é restrito ao grupo de segurança. Você precisará atualizar a regra de saída no grupo de segurança para permitir o tráfego para sua rede on-premises. Para obter mais informações sobre requisitos de segurança, consulte Etapa 2: preparar o AWS Managed Microsoft AD.



Se os servidores de DNS das redes dos outros diretórios usarem endereços IP públicos (não RFC 1918), será necessário adicionar uma rota IP no diretório do console dos Directory Services aos servidores de DNS. Para obter mais informações, consulte Pré-requisitos e Criar, verificar ou excluir uma relação de confiança.

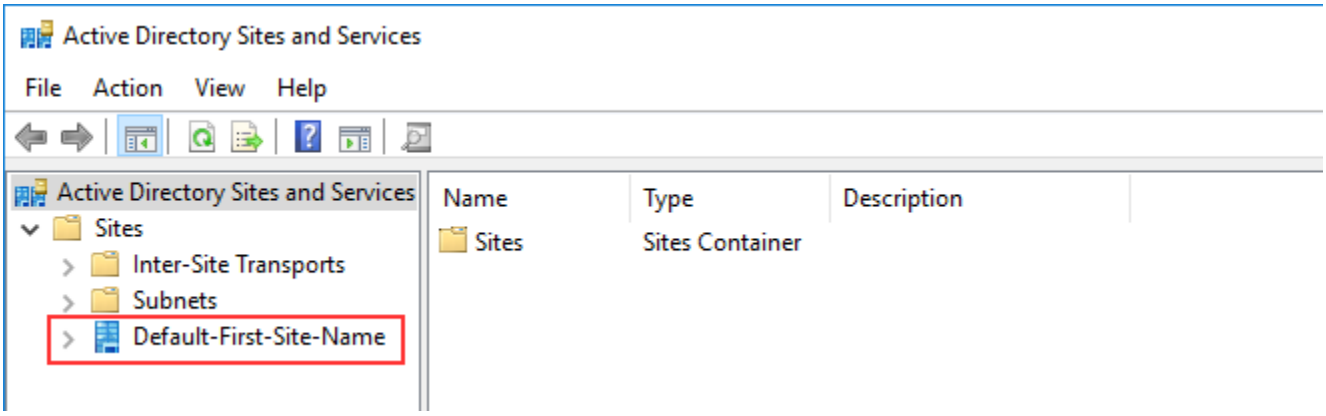
A Internet Assigned Numbers Authority (IANA) reservou os seguintes três blocos do espaço de endereço IP para internets privadas:

- 10.0.0.0 - 10.255.255.255 (prefixo 10/8)
- 172.16.0.0 - 172.31.255.255 (prefixo 172.16/12)
- 192.168.0.0 - 192.168.255.255 (prefixo 192.168/16)

Para obter mais informações, consulte https://tools.ietf.org/html/rfc1918.

Verifique se o nome padrão do site AD para seu Microsoft AD AWS gerenciado corresponde ao nome do site AD padrão em sua infraestrutura local. O computador determina o nome do site usando um domínio do qual o computador é membro, e não o domínio do usuário. Renomear o site para corresponder ao on-premises mais próximo garante que o localizador de DCs use um controlador de domínio do site mais próximo. Se isso não resolver o problema, é possível que as informações de um encaminhador condicional criado anteriormente tenham sido armazenadas em cache, impedindo a criação de uma nova confiança. Espere alguns minutos e tente criar a confiança e o encaminhador condicional novamente.

Para obter mais informações sobre como isso funciona, consulte Domain Locator Across a Forest Trust no Microsoft site.



Não foi possível executar a operação neste domínio

Para resolver isso, certifique-se de que os dois domínios/diretórios não tenham nomes NETBIOS sobrepostos. Se os domínios/diretórios tiverem nomes NETBIOS sobrepostos, recrie um deles com um nome NETBIOS diferente e tente novamente.

A criação de confiança está falhando devido ao erro "Nome de domínio válido obrigatório"

Os nomes de DNS só podem conter caracteres alfabéticos (A - Z), caracteres numéricos (0 - 9), o sinal de subtração (-) e ponto (.). Caracteres de ponto final são permitidos somente quando usados para delimitar os componentes dos nomes de estilo de domínio. Considere também o seguinte:

- AWS O Microsoft AD gerenciado não oferece suporte a relações de confiança com domínios de rótulo único. Para obter mais informações, consulte o Microsoftsuporte para domínios de rótulo único.
- De acordo com a RFC 1123 (https://tools.ietf.org/html/rfc1123), os únicos caracteres que podem ser usados em rótulos de DNS são "A" a "Z", "a" a "z", "0" a "9" e hífen ("-"). Um ponto [.] também pode ser usado em nomes de DNS, mas somente entre rótulos de DNS e no final de um FQDN.
- De acordo com a RFC 952 (https://tools.ietf.org/html/rfc952), um "nome" (de rede, host, gateway ou domínio) é uma sequência de texto com até 24 caracteres extraída do alfabeto (A-Z), dígitos (0-9), sinal de subtração (-) e ponto (.). Observe que os pontos só são permitidos para delimitar componentes de "nomes de estilo de domínio".

Para obter mais informações, consulte Conformidade com restrições de nome para hosts e domínios no Microsoft site.

Ferramentas gerais para testar relações de confiança

As ferramentas a seguir podem ser usadas para solucionar vários problemas relacionados a confiança.

AWS Ferramenta de solução de problemas do Systems Manager Automation

Os fluxos de trabalho do Support Automation (SAW) utilizam o AWS Systems Manager Automation para fornecer a você um runbook predefinido para. AWS Directory ServiceA ferramenta AWSSupport- TroubleshootDirectoryTrust runbook ajuda você a diagnosticar problemas comuns de criação de confiança entre o AWS Microsoft AD gerenciado e um local. Microsoft Active Directory

DirectoryServicePortTest ferramenta

A ferramenta DirectoryServicePortTestde teste pode ser útil na solução de problemas de criação de confiança entre o Microsoft AD AWS gerenciado e o Active Directory local. Para obter um exemplo de como a ferramenta pode ser usada, consulte Testar o AD Connector.

Ferramenta NETDOM e NLTEST

Os administradores podem usar as ferramentas de linha de comando Netdom e Nltest para encontrar, exibir, criar, remover e gerenciar relações de confiança. Essas ferramentas se comunicam diretamente com a autoridade LSA em um controlador de domínio. Para obter um exemplo de como usar essas ferramentas, consulte Netdom e NLTEST no site. Microsoft

Ferramenta de captura de pacotes

O utilitário integrado de captura de pacotes do Windows pode ser usado para investigar e solucionar um possível problema de rede. Para obter mais informações, consulte Capturar um trace de rede sem instalar nada.

AD Connector

O AD Connector é um gateway de diretório com o qual você pode redirecionar solicitações de diretório para seu local Microsoft Active Directory sem armazenar nenhuma informação em cache na nuvem. O AD Connector é fornecido em dois tamanhos, pequeno e grande. Um AD Connetor pequeno é projetado para organizações menores e destina-se a lidar com um número baixo de operações por segundo. Um AD Connector grande é projetado para organizações maiores e destina-se a lidar com um número moderado a alto de operações por segundo. Você pode distribuir cargas de aplicativo entre vários AD Connectors para dimensionar para as suas necessidades de desempenho. Não há limites impostos de conexão ou usuário.

O AD Connector não oferece suporte a relações de confiança transitivas do Active Directory. Os AD Connectors e seus domínios locais do Active Directory têm uma relação de 1 para 1. Ou seja, para cada domínio local, incluindo domínios secundários em uma floresta do Active Directory na qual você deseja se autenticar, você deve criar um AD Connector exclusivo.

> **Note**
>
> O AD Connector não pode ser compartilhado com outras AWS contas. Se isso for um requisito, considere usar o Microsoft AD AWS gerenciado paraCompartilhar seu diretório. O AD Connector também não reconhece várias VPCs, o que significa que AWS aplicativos como WorkSpacesesse precisam ser provisionados na mesma VPC do AD Connector.

Depois de configurado, o AD Connector oferece os seguintes benefícios:

- Seus usuários finais e administradores de TI podem usar suas credenciais corporativas existentes para fazer login em AWS aplicativos como WorkSpaces Amazon ou Amazon WorkDocs. WorkMail
- Você pode gerenciar AWS recursos como instâncias do Amazon EC2 ou buckets do Amazon S3 por meio do acesso baseado em funções do IAM ao. AWS Management Console
- Você pode aplicar consistentemente as políticas de segurança existentes (como expiração de senha, histórico de senhas e bloqueios de contas), independentemente de usuários ou administradores de TI estarem acessando recursos em sua infraestrutura local ou na nuvem. AWS
- Você pode usar o AD Connector para habilitar a autenticação multifatorial integrando-se à sua infraestrutura de MFA baseada em RADIUS existente para fornecer uma camada adicional de segurança quando os usuários acessam aplicativos. AWS

Continue a ler os tópicos desta seção para saber como se conectar a um diretório e aproveitar ao máximo os recursos do AD Connector.

Tópicos

Conceitos básicos do AD Connector

Com o AD Connector, você pode se conectar AWS Directory Service à sua empresa existenteActive Directory. Quando conectado ao diretório existente, todos os dados do diretório permanecem nos controladores de domínio. AWS Directory Service não replica nenhum dos dados do seu diretório.

Tópicos

Pré-requisitos do AD Connector

Para conectar ao seu diretório existente com o AD Connector, você precisa do seguinte:

Amazon VPC

Configure uma VPC com o seguinte:

- Pelo menos duas sub-redes. Cada uma das sub-redes deve estar em uma zona de disponibilidade diferente.
- A VPC deve estar conectada à sua rede existente por meio de uma conexão de rede privada virtual (VPN) ou AWS Direct Connect.
- A VPC deve ter uma locação de hardware padrão.

AWS Directory Service usa uma estrutura de duas VPC. As instâncias do EC2 que compõem seu diretório são executadas fora da sua AWS conta e são gerenciadas pela AWS. Elas têm dois adaptadores de rede `ETH0` e `ETH1`. `ETH0` é o adaptador de gerenciamento e existe fora da sua conta. `ETH1` é criado em sua conta.

O intervalo de IP de gerenciamento da `ETH0` rede do seu diretório é escolhido de maneira programática para garantir que não entre em conflito com a VPC em que seu diretório está implantado. Esse intervalo de IP pode estar em qualquer um dos seguintes pares (já que os diretórios são executados em duas sub-redes):

- 10.0.1.0/24 e 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 e 192.168.2.0/24

Evitamos conflitos verificando o primeiro octeto do CIDR `ETH1`. Se ele começar com 10, escolheremos uma VPC 192.168.0.0/16 com sub-redes 192.168.1.0/24 e 192.168.2.0/24. Se o primeiro octeto for diferente de 10, escolheremos uma VPC 10.0.0.0/16 com sub-redes 10.0.1.0/24 e 10.0.2.0/24.

O algoritmo de seleção não inclui rotas em sua VPC. Portanto, é possível que um conflito de roteamento IP resulte desse cenário.

Para obter mais informações, consulte um dos tópicos a seguir no Guia do usuário da Amazon VPC.

- O que é Amazon VPC?
- Sub-redes na sua VPC
- Adicionar um hardware de gateway privado virtual à VPC

Para obter mais informações sobre AWS Direct Connect, consulte o Guia AWS Direct Connect do usuário.

Existente Active Directory

Você precisará se conectar a uma rede existente com um Active Directory domínio.

> **Note**
>
> O AD Connector não é compatível com domínios de rótulo único.

O nível funcional desse Active Directory domínio deve ser igual `Windows Server 2003` ou superior. O AD Connector também oferece suporte à conexão a um domínio hospedado em uma instância do Amazon EC2.

> **Note**
>
> O AD Connector não oferece suporte a controladores de domínio somente leitura (RODC) quando usados em combinação com o recurso de associação a domínio do Amazon EC2.

Conta de serviço

Você deve ter credenciais para uma conta de serviço no diretório existente delegada com os privilégios a seguir:

- Ler os usuários e grupos — Obrigatório
- Associar computadores ao domínio - Obrigatório somente ao usar o Seamless Domain Join e WorkSpaces
- Crie objetos de computador - Obrigatório somente ao usar o Seamless Domain Join e WorkSpaces
- A senha da conta de serviço deve estar em conformidade com os requisitos de AWS senha. AWS as senhas devem ser:
  - Entre 8 e 128 caracteres, inclusive.
  - Contenha pelo menos um caractere de três das quatro categorias a seguir:
    - Letras minúsculas (a-z)
    - Letras maiúsculas (A-Z)
    - Números (0-9)
    - Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Para ter mais informações, consulte Delegar privilégios para sua conta de serviço.

> **Note**
>
> O AD Connector usa Kerberos para autenticação e autorização de aplicações da AWS . O LDAP é usado somente para pesquisas de objetos de usuários e grupos (operações de leitura). Com as transações LDAP, nada é mutável e as credenciais não são passadas

em texto não criptografado. A autenticação é feita por um serviço AWS interno, que usa tíquetes Kerberos para realizar operações LDAP como usuário.

Permissões de usuário

Todos os usuários do Active Directory devem ter permissões para ler seus próprios atributos. Especificamente os seguintes atributos:

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

Por padrão, os usuários do Active Directory têm permissão de leitura para esses atributos. No entanto, os administradores podem alterar essas permissões ao longo do tempo, de modo que você pode verificar se seus usuários têm essas permissões de leitura antes de configurar o AD Connector pela primeira vez.

Endereços IP

Obtenha os endereços IP de dois servidores DNS ou controladores de domínio no seu diretório existente.

O AD Connector obtém os registros SRV `_ldap._tcp.<DnsDomainName>` e `_kerberos._tcp.<DnsDomainName>` desses servidores ao se conectar ao seu diretório, de forma que esses servidores devem conter esses registros de SRV. O AD Connector tenta encontrar um controlador comum de domínio que fornece serviços de LDAP e Kerberos; portanto, esses registros de SRV devem incluir pelo menos um controlador de domínio em comum. Para obter mais informações sobre registros SRV, acesse SRV Resource Records na Microsoft. TechNet

Portas para sub-redes

Para que o AD Connector redirecione as solicitações de diretório para seus controladores de Active Directory domínio existentes, o firewall da sua rede atual deve ter as seguintes portas abertas para os CIDRs de ambas as sub-redes em sua Amazon VPC.

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

Essas são as portas mínimas necessárias para que o AD Connector possa se conectar ao seu diretório. Sua configuração específica pode exigir que portas adicionais sejam abertas.

Se você quiser usar o AD Connector e a Amazon WorkSpaces, o atributo disableVlvSupportLDAP precisa ser definido como 0 para seus controladores de domínio. Essa é a configuração padrão para os controladores de domínio. O AD Connector não poderá consultar usuários no diretório se o atributo disableVlvSupportLDAP estiver habilitado. Isso impede que o AD Connector funcione com Amazon WorkSpaces o.

> **Note**
>
> Se os servidores DNS ou os servidores do controlador de domínio do seu Active Directory domínio existente estiverem dentro da VPC, os grupos de segurança associados a esses servidores deverão ter as portas acima abertas para os CIDRs de ambas as sub-redes na VPC.

Para obter requisitos adicionais de porta, consulte Requisitos de porta do AD e do AD DS na Microsoft documentação.

Pré-autenticação do Kerberos

Suas contas de usuário devem ter a pré-autenticação Kerberos habilitada. Para obter instruções detalhadas sobre como habilitar essa configuração, consulte Verificar se a pré-autenticação Kerberos está habilitada. Para obter informações gerais sobre essa configuração, acesse Pré-autenticação em Microsoft TechNet.

Tipos de criptografia

O AD Connector é compatível com os seguintes tipos de criptografia ao fazer a autenticação via Kerberos em seus controladores de domínio do Active Directory:

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center pré-requisitos

Se você planeja usar o Centro de Identidade do IAM com o AD Connector, é necessário garantir que o seguinte seja verdadeiro:

- Seu AD Connector está configurado na conta de gerenciamento da sua AWS organização.
- Sua instância do Centro de Identidade do IAM está na mesma região em que o AD Connector está configurado.

Para obter mais informações, consulte os pré-requisitos do IAM Identity Center no Guia do AWS IAM Identity Center usuário.

Pré-requisitos da autenticação multifator

Para oferecer suporte à autenticação multifator com o seu diretório do AD Connector, é necessário o seguinte:

- Um servidor Remote Authentication Dial-In User Service (RADIUS) na sua rede existente que tenha dois endpoints clientes. Os endpoints clientes do RADIUS têm os seguintes requisitos:
  - Para criar os endpoints, são necessários os endereços IP dos servidores do AWS Directory Service . Esses endereços IP podem ser obtidos no campo Directory IP Address dos detalhes do seu diretório.
  - Ambos os endpoints do RADIUS devem usar o mesmo código secreto compartilhado.
- Sua rede existente deve permitir tráfego de entrada pela porta padrão do servidor RADIUS (1812) dos servidores. AWS Directory Service
- Os nomes de usuário entre o servidor RADIUS e o diretório existente devem ser idênticos.

Para obter mais informações sobre como usar o AD Connector com MFA, consulte Habilitar a autenticação multifator para o AD Connector.

Delegar privilégios para sua conta de serviço

Para se conectar ao seu diretório existente, é necessário ter as credenciais para sua conta de serviço do AD Connector no diretório existente com determinados privilégios delegados a elas. Embora os membros do grupo Domain Admins (Administradores do domínio) tenham privilégios suficientes para se conectar ao diretório, como uma melhor prática, use uma conta de serviço que tenha apenas os privilégios mínimos necessários para conectar-se ao diretório. O procedimento

a seguir demonstra como criar um novo grupo chamado`Connectors`, delegar os privilégios necessários para se conectar AWS Directory Service a esse grupo e, em seguida, adicionar uma nova conta de serviço a esse grupo.

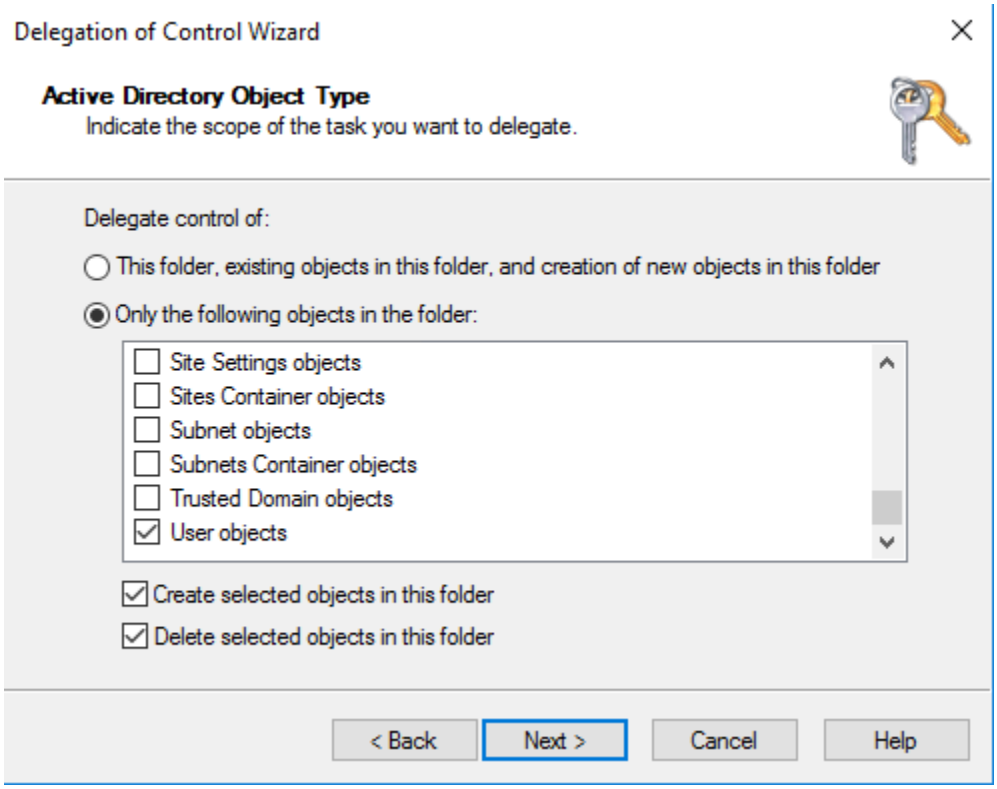
Este procedimento deve ser executado em uma máquina que esteja integrada ao seu diretório e tenha o snap-in do MMC Active Directory User and Computers (Usuário e computadores do Active Directory) instalado. Você também deve estar conectado como administrador de domínio.

Para delegar privilégios para sua conta de serviço

1. Abra Active Directory User and Computers (Usuário e computadores do Active Directory) e selecione a raiz do domínio na árvore de navegação.
2. Na lista no painel de trabalho à esquerda, clique com o botão direito do mouse sobre Users, selecione New e selecione Group.
3. Na caixa de diálogo New Object - Group, digite o que está a seguir e clique em OK.

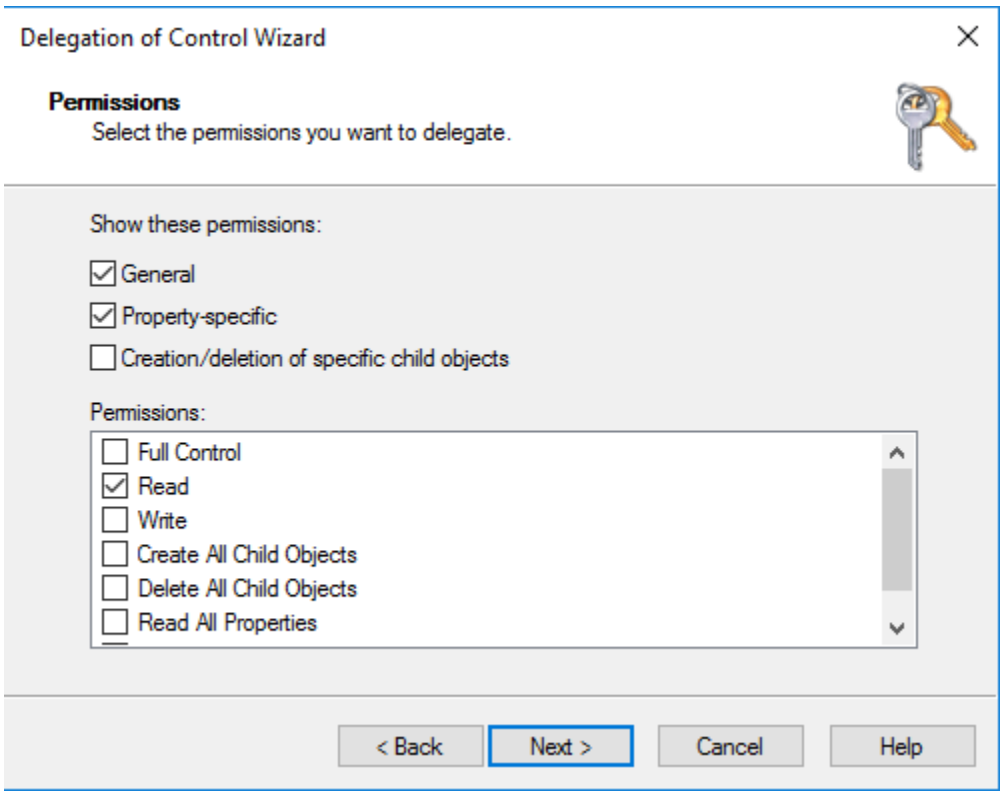
Campo	Valor/Seleção
Group name	`Connectors`
Escopo do grupo	Global
Tipo de grupo	Segurança

4. Na árvore de navegação de Active Directory User and Computers (Usuário e computadores do Active Directory), selecione a raiz do seu domínio. No menu, selecione Action e Delegate Control. Se o AD Connector estiver conectado ao AWS Managed Microsoft AD, você não terá acesso para delegar controle no nível raiz do domínio. Nesse caso, para delegar o controle, selecione a UO na UO do diretório em que os objetos do seu computador serão criados.
5. Na página Delegation of Control Wizard, clique em Next e em Add.
6. Na caixa de diálogo Select Users, Computers, or Groups (Selecionar usuários, computadores ou grupos), digite `Connectors` e clique em OK. Se mais de um objeto for encontrado, selecione o grupo `Connectors` criado acima. Clique em Next.
7. Na página Tasks to Delegate, selecione Create a custom task to delegate e escolha Next.
8. Selecione Only the following objects in the folder e selecione Computer objects e User objects.
9. Selecione Create selected objects in this folder e Delete selected objects in this folder. Em seguida, escolha Próximo.



10. Selecione Read (Ler) e depois escolha Next (Próximo).

> **Note**
>
> Se você estiver usando o Seamless Domain Join or WorkSpaces, você também deverá habilitar as permissões de gravação para que o Active Directory possa criar objetos de computador.



11. Verifique as informações da página Completing the Delegation of Control Wizard e clique em Finish.
12. Crie uma conta de usuário com uma senha forte e adicione o usuário ao grupo `Connectors`. Esse usuário será conhecido como sua conta de serviço do AD Connector e, como agora é membro do `Connectors` grupo, agora tem privilégios suficientes para se conectar AWS Directory Service ao diretório.

Testar o AD Connector

Para o AD Connector se conectar ao diretório existente, o firewall da rede existente deve ter certas portas abertas para os CIDRs de ambas as sub-redes na VPC. Para testar se essas condições são atendidas, execute as etapas a seguir:

Para testar a conexão com a

1. Inicie uma instância do Windows na VPC e conecte-se a ela por RDP. A instância deve ser membro do seu domínio existente. As etapas restantes são executadas nesta instância da VPC.

2. Baixe e descompacte o aplicativo DirectoryServicePortTestde teste. O código-fonte e os arquivos de projeto do Visual Studio são incluídos para que você possa modificar o aplicativo de teste, se desejar.

> **Note**
>
> Este script não tem suporte no Windows Server 2003 nem em um sistemas operacionais mais antigos.

3. Pelo prompt de comando do Windows, execute a aplicativo de teste DirectoryServicePortTest com as seguintes opções:

> **Note**
>
> O aplicativo DirectoryServicePortTest de teste só pode ser usado quando os níveis funcionais do domínio e da floresta estão definidos para Windows Server 2012 R2 e versões anteriores.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
 "53,88,389" -udp "53,88,389"
```

<domain_name>

O nome de domínio totalmente qualificado. Ele é 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 existente. As portas serão testadas com relação a esse endereço IP. Se você excluir o endereço IP, as portas não serão testadas.

Este aplicativo de testes determina se as portas necessárias estão abertas na VPC para seu domínio e também verifica os níveis funcionais mínimos de floresta e domínio.

A saída será semelhante ao seguinte:

```
Testing forest functional level.
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
Domain Functional Level = Windows2008R2Domain : PASSED

Testing required TCP ports to <server_IP_address>:
Checking TCP port 53: PASSED
Checking TCP port 88: PASSED
Checking TCP port 389: PASSED

Testing required UDP ports to <server_IP_address>:
Checking UDP port 53: PASSED
Checking UDP port 88: PASSED
Checking UDP port 389: PASSED
```

O seguinte é o código-fonte do aplicativo DirectoryServicePortTest.

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;
```

```
        private static string _domain = "";
        private static IPAddress _ipAddr = null;

        static void Main(string[] args)
        {
            if (ParseArgs(args))
            {
                try
                {
                    if (_domain.Length > 0)
                    {
                        try
                        {
                            TestForestFunctionalLevel();

                            TestDomainFunctionalLevel();
                        }
                        catch (ActiveDirectoryObjectNotFoundException)
                        {
                            Console.WriteLine("The domain {0} could not be found.\n",
_domain);
                        }
                    }

                    if (null != _ipAddr)
                    {
                        if (_tcpPorts.Count > 0)
                        {
                            TestTcpPorts(_tcpPorts);
                        }

                        if (_udpPorts.Count > 0)
                        {
                            TestUdpPorts(_udpPorts);
                        }
                    }
                }
                catch (AuthenticationException ex)
                {
                    Console.WriteLine(ex.Message);
                }
            }
            else
            {
```

```
                PrintUsage();
            }

            Console.Write("Press <enter> to continue.");
            Console.ReadLine();
        }

        static void PrintUsage()
        {
            string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
            Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
        }

        static bool ParseArgs(string[] args)
        {
            bool fReturn = false;
            string ipAddress = "";

            try
            {
                _tcpPorts = new List<int>();
                _udpPorts = new List<int>();

                for (int i = 0; i < args.Length; i++)
                {
                    string arg = args[i];

                    if ("-tcp" == arg | "/tcp" == arg)
                    {
                        i++;
                        string portList = args[i];
                        _tcpPorts = ParsePortList(portList);
                    }

                    if ("-udp" == arg | "/udp" == arg)
                    {
                        i++;
                        string portList = args[i];
                        _udpPorts = ParsePortList(portList);
                    }
```

```
                if ("-d" == arg | "/d" == arg)
                {
                    i++;
                    _domain = args[i];
                }

                if ("-ip" == arg | "/ip" == arg)
                {
                    i++;
                    ipAddress = args[i];
                }
            }
        }
        catch (ArgumentOutOfRangeException)
        {
            return false;
        }

        if (_domain.Length > 0 || ipAddress.Length > 0)
        {
            fReturn = true;
        }

        if (ipAddress.Length > 0)
        {
            _ipAddr = IPAddress.Parse(ipAddress);
        }

        return fReturn;
    }

    static List<int> ParsePortList(string portList)
    {
        List<int> ports = new List<int>();

        char[] separators = {',', ';', ':'};

        string[] portStrings = portList.Split(separators);
        foreach (string portString in portStrings)
        {
            try
            {
                ports.Add(Convert.ToInt32(portString));
            }
```

```
                catch (FormatException)
                {
                }
            }

            return ports;
        }

        static void TestForestFunctionalLevel()
        {
            Console.WriteLine("Testing forest functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
            Forest forestContext = Forest.GetForest(dirContext);

            Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

            if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static void TestDomainFunctionalLevel()
        {
            Console.WriteLine("Testing domain functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
            Domain domainObject = Domain.GetDomain(dirContext);

            Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

            if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
            {
                Console.WriteLine("PASSED");
```

```
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static List<int> TestTcpPorts(List<int> portList)
        {
            Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking TCP port {0}: ", port);

                TcpClient tcpClient = new TcpClient();

                try
                {
                    tcpClient.Connect(_ipAddr, port);

                    tcpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }

        static List<int> TestUdpPorts(List<int> portList)
        {
            Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());
```

```
            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking UDP port {0}: ", port);

                UdpClient udpClient = new UdpClient();

                try
                {
                    udpClient.Connect(_ipAddr, port);
                    udpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }
    }
}
```

Criar um AD Connector

Para se conectar ao seu diretório existente com o AD Connector, siga as etapas a seguir. Antes de iniciar este procedimento, verifique se você concluiu os pré-requisitos identificados em Pré-requisitos do AD Connector.

> **Note**
>
> Não é possível criar um AD Connector com um modelo do Cloud Formation.

Para se conectar com o AD Connector

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios e escolha Configurar diretório.
2. Na página Selecionar tipo do diretório, selecione AD Connector e, em seguida, selecione Próximo.
3. Na página Enter AD Connector information (Inserir informações do AD Connector), forneça as seguintes informações:

   Tamanho do diretório

   Selecione a opção de tamanho Small (Pequeno) ou Large (Grande). Para obter mais informações sobre os tamanhos, consulte AD Connector.

   Descrição do diretório

   Uma descrição opcional do diretório.
4. Na página Choose VPC and subnets (Selecionar VPC e sub-redes), forneça as seguintes informações e selecione Next (Próximo).

   VPC

   A VPC do diretório.

   Subredes

   Selecione as sub-redes para os controladores de domínio. As duas sub-redes deve estar em diferentes zonas de disponibilidade.
5. Na página Connect to AD (Conectar ao AD), forneça as seguintes informações:

   Nome do DNS do diretório

   O nome completo do seu diretório existente, como `corp.example.com`.

   Nome de NetBIOS do diretório

   O nome curto do seu diretório existente, como `CORP`.

   Endereços IP do DNS

   O endereço IP de pelo menos um servidor DNS em seu diretório existente. Esses servidores devem ser acessados a partir de cada sub-rede especificada na etapa 4. Esses servidores

podem estar localizados fora do AWS, desde que haja conectividade de rede entre as sub-redes especificadas e os endereços IP do servidor DNS.

Nome de usuário da conta de serviço

O nome de usuário de um usuário no diretório existente. Para obter mais informações sobre esta conta, consulte Pré-requisitos do AD Connector.

Senha da conta de serviço

A senha para a conta de usuário existente. Essa senha diferencia maiúsculas de minúsculas e deve ter entre 8 e 128 caracteres, inclusive. Ela também precisa conter pelo menos um caractere de três das quatro categorias a seguir:

- Letras minúsculas (a-z)
- Letras maiúsculas (A-Z)
- Números (0-9)
- Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Confirmar senha

Digite novamente a senha para a conta de usuário existente.

6. Na página Review & create (Revisar e criar), analise as informações do diretório e faça as alterações necessárias. Quando as informações estiverem corretas, escolha Create directory (Criar diretório). A criação do diretório leva vários minutos. Depois de criado, o valor de Status é alterado para Ativo.

O que é criado com seu AD Connector

Quando você cria um AD Connector, cria e associa AWS Directory Service automaticamente uma interface de rede elástica (ENI) a cada uma das suas instâncias do AD Connector. Cada um desses ENIs é essencial para a conectividade entre sua VPC e o AD AWS Directory Service Connector e nunca deve ser excluído. Você pode identificar todas as interfaces de rede reservadas para uso com AWS Directory Service a descrição: "interface de rede AWS criada para id de diretório". Para obter mais informações, consulte Interfaces de rede elástica no Guia do usuário do Amazon EC2.

> **Note**
>
> As instância do AD Connector são implantadas em duas zonas de disponibilidade em uma região e conectadas à sua Amazon Virtual Private Cloud (VPC). As instâncias do AD

Connector que falham são substituídas automaticamente na mesma zona de disponibilidade usando o mesmo endereço IP.

Quando você entra em qualquer AWS aplicativo ou serviço integrado com um AD Connector (AWS IAM Identity Center incluído), o aplicativo ou serviço encaminha sua solicitação de autenticação para o AD Connector, que então encaminha a solicitação para um controlador de domínio em seu Active Directory autogerenciado para autenticação. Se você for autenticado com êxito no seu Active Directory autogerenciado, o AD Connector retornará um token de autenticação para o aplicativo ou serviço (semelhante a um token Kerberos). Nesse ponto, agora você pode acessar o AWS aplicativo ou serviço.

Como administrar o AD Connector

Esta seção lista todos os procedimentos para operar e manter um ambiente do AD Connector.

Tópicos

Proteger seu diretório do AD Connector

Esta seção descreve considerações para proteger seu ambiente do AD Connector.

Tópicos

Atualizar suas credenciais da conta de serviço do AD Connector no AWS Directory Service

As credenciais do AD Connector que você fornece no AWS Directory Service representam a conta de serviço que é usada para acessar seu diretório existente on-premises. Você pode modificar as credenciais da conta de serviço no AWS Directory Service executando as etapas a seguir.

> **Note**
>
> Se o AWS IAM Identity Center estiver habilitado para o diretório, o AWS Directory Service deverá transferir o nome da entidade principal do serviço (SPN) da conta de serviço atual para a nova conta de serviço. Se a conta de serviço atual não tiver permissão para excluir o SPN ou se a nova conta de serviço não tiver permissão para adicionar o SPN, serão solicitadas as credenciais de uma conta do diretório que tenha permissão para executar as duas ações. Essas credenciais são usadas apenas para transferir o SPN e não são armazenadas pelo serviço.

Para atualizar suas credenciais da conta de serviço do AD Connector no AWS Directory Service

1. No painel de navegação do console do AWS Directory Service, em Active Directory, escolha Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Detalhes do diretório, role para baixo até a seção Credenciais da conta de serviço.
4. Na seção Credenciais da conta de serviço, escolha Atualizar.
5. Na caixa de diálogo Atualizar credenciais da conta de serviço, digite o nome de usuário e a senha da conta de serviço. Digite novamente a senha para confirmá-la e escolha Atualizar.

Habilitar a autenticação multifator para o AD Connector

Você poderá habilitar a autenticação multifator para o AD Connector quando o Active Directory estiver em execução on-premises ou em instâncias do EC2. Para obter mais informações sobre o uso da autenticação multifator com o AWS Directory Service, consulte Pré-requisitos do AD Connector.

> **Note**
>
> A autenticação multifator não está disponível para o Simple AD. No entanto, a MFA pode ser habilitada para seu diretório do AWS Managed Microsoft AD. Para obter mais informações, consulte Habilite a autenticação multifator para o AWS Managed Microsoft AD.

Para habilitar a autenticação multifator para o AD Connector

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link de ID do diretório do AD Connector.
3. Na página Directory details (Detalhes do diretório), selecione a guia Networking & security (Redes e segurança).
4. Na seção Multi-factor authentication (Autenticação multifator), escolha Actions (Ações) e Enable (Habilitar).
5. Na página Habilitar a autenticação multifator (MFA), forneça os seguintes valores:

   Rótulo de exibição

   Forneça um nome de rótulo.

   Nome de DNS ou endereços IP do servidor RADIUS

   O load balancer dos endpoints do servidor RADIUS ou do endereço IP do servidor RADIUS. Você pode inserir vários endereços IP separados por vírgulas (por exemplo, `192.0.0.0,192.0.0.12`).

   > **Note**
   >
   > O RADIUS MFA é aplicável somente para autenticar AWS Management Console o acesso aos aplicativos e serviços da Amazon Enterprise WorkSpaces, como Amazon ou QuickSight Amazon Chime. Ele não fornece MFA para workloads do Windows em execução em instâncias do EC2 nem para login em uma instância do EC2. O AWS Directory Service não é compatível com autenticação Desafio/Resposta do RADIUS. Os usuários devem ter o código MFA no momento em que inserem o nome de usuário e a senha. Como alternativa, você deve usar uma solução que realize MFA, out-of-band como verificação de texto por SMS para o usuário. Nas soluções de out-of-band MFA, você deve se certificar de definir o valor de tempo limite do RADIUS

de forma adequada para sua solução. Ao usar uma solução de out-of-band MFA, a página de login solicitará ao usuário um código de MFA. Nesse caso, a prática recomendada é que os usuários insiram a senha no campo de senha e no campo de MFA.

Porta

A porta que o servidor RADIUS está usando para comunicações. Sua rede on-premises deve permitir tráfego de entrada pela porta do servidor RADIUS padrão (UDP: 1812) dos servidores do AWS Directory Service.

Shared secret code (Código secreto compartilhado)

O código secreto compartilhado que foi especificado quando os endpoints do RADIUS foram criados.

Confirm shared secret code (Confirmar código secreto compartilhado)

Confirme o código secreto compartilhado para os endpoints do RADIUS.

Protocolo

Selecione o protocolo que foi especificado quando os endpoints do RADIUS foram criados.

Tempo limite do servidor (em segundos)

O tempo de espera, em segundos, para o servidor RADIUS responder. Esse valor deve estar entre 1 e 50.

Máximo de novas tentativas de solicitação RADIUS

O número de tentativas de comunicação com o servidor RADIUS. Esse valor deve estar entre 0 e 10.

A autenticação multifator está disponível quando o Status RADIUS muda para Habilitado.

6. Escolha Habilitar.

Habilitar o LDAPS no lado do cliente usando o AD Connector

O suporte ao LDAPS do lado do cliente no AD Connector criptografa as comunicações entre o Microsoft Active Directory (AD) e as aplicações da AWS. Exemplos dessas aplicações incluem

WorkSpaces, AWS IAM Identity Center, Amazon QuickSight e Amazon Chime. Essa criptografia ajuda você a proteger melhor os dados de identidade da organização e atender aos requisitos de segurança.

Tópicos

Pré-requisitos

Antes de habilitar o LDAPS no lado do cliente, você precisa atender aos requisitos a seguir.

Tópicos

Implantar certificados de servidor no Active Directory

Para habilitar o LDAPS no lado do cliente, é necessário obter e instalar certificados de servidor para cada controlador de domínio no Active Directory. Esses certificados serão usados pelo serviço LDAP para escutar e aceitar automaticamente as conexões SSL de clientes LDAP. Você pode usar os certificados SSL emitidos por uma implantação interna do Active Directory Certificate Services (ADCS) ou comprados de um emissor comercial. Para obter mais informações sobre os requisitos de certificado de servidor do Active Directory, consulte LDAP over SSL (LDAPS) Certificate no site da Microsoft.

Requisitos de certificado de CA

Um certificado de autoridade de certificação (CA), que representa o emissor dos certificados de servidor, é necessário para a operação LDAPS no lado do cliente. Os certificados CA são combinados com os certificados de servidor apresentados pelos controladores de domínio do Active Directory para criptografar as comunicações de LDAP. Observe os seguintes requisitos de certificado CA:

- Para registrar um certificado, ele deve estar a mais de 90 dias da expiração.

- Os certificados devem estar no formato PEM (Privacy Enhanced Mail). Se exportar certificados CA de dentro do Active Directory, escolha X.509 (.CER) codificado em base64 como o formato de arquivo de exportação.
- No máximo, cinco (5) certificados de CA podem ser armazenados por diretório do AD Connector.
- Não há suporte para certificados que usam o algoritmo de assinatura RSASSA-PSS.

Requisitos de rede

O tráfego LDAP do aplicativo da AWS será executado exclusivamente na porta TCP 636, sem fallback para a porta LDAP 389. Porém, as comunicações LDAP do Windows que oferecem suporte a replicação, relações de confiança e muito mais continuarão a usar a porta LDAP 389 com segurança nativa do Windows. Configure grupos de segurança da AWS e firewalls de rede para permitir comunicações TCP na porta 636 no AD Connector (saída) e no Active Directory autogerenciado (entrada).

Habilitar o LDAPS no lado do cliente

Para habilitar o LDAPS no lado do cliente, importe seu certificado de autoridade de certificação (CA) para o AD Connector e habilite o LDAPS no seu diretório. Após a habilitação, todo o tráfego LDAP entre os aplicativos da AWS e o seu Active Directory autogerenciado fluirá com a criptografia de canal Secure Sockets Layer (SSL).

É possível usar dois métodos diferentes para habilitar o LDAPS do lado do cliente para seu diretório. É possível usar o método AWS Management Console ou o método AWS CLI.

Tópicos

Etapa 1: registrar o certificado no AWS Directory Service

Use um dos seguintes métodos para registrar um certificado no AWS Directory Service.

Método 1: Como registrar seu certificado no AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.

2. Escolha o link do ID de seu diretório.
3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).
4. Na seção Client-side LDAPS (LDAPS do lado do cliente), selecione o menu Actions (Ações) e escolha Register certificate (Registrar certificado).
5. Na caixa de diálogo Register a CA certificate (Registrar um certificado CA), selecione Browse (Procurar), escolha o certificado e selecione Open (Abrir).
6. Escolha Register certificate (Registrar certificado).

Método 2: Como registrar seu certificado no AWS Directory Service (AWS CLI)

- Execute o comando a seguir. Para os dados do certificado, aponte para o local do arquivo de certificado CA. Um ID de certificado será fornecido na resposta.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Etapa 2: verificar o status do registro

Para ver o status de um registro de certificado ou uma lista de certificados registrados, use um dos comandos a seguir.

Método 1: Como verificar o status do registro do certificado no AWS Directory Service (AWS Management Console)

1. Vá para a seção Client-side LDAPS (LDAPS do lado do cliente) na página Directory details (Detalhes do diretório).
2. Revise o estado de registro de certificado atual exibido na coluna Registration status (Status do registro). Quando o valor do status do registro for alterado para Registered (Registrado), seu certificado foi registrado com êxito.

Método 2: Como verificar o status do registro do certificado no AWS Directory Service (AWS CLI)

- Execute o comando a seguir. Se o valor de status retornar `Registered`, seu certificado foi registrado com êxito.

```
aws ds list-certificates --directory-id your_directory_id
```

Etapa 3: habilitar o LDAPS no lado do cliente

Use um dos métodos a seguir para habilitar o LDAPS no lado do cliente no AWS Directory Service.

> **Note**
>
> É necessário ter registrado com êxito pelo menos um certificado para habilitar o LDAPS do lado do cliente.

Método 1: Como habilitar o LDAPS do lado do cliente no AWS Directory Service (AWS Management Console)

1. Vá para a seção Client-side LDAPS (LDAPS do lado do cliente) na página Directory details (Detalhes do diretório).
2. Escolha Enable (Habilitar). Se essa opção não estiver disponível, verifique se um certificado válido foi registrado com êxito e tente novamente.
3. Na caixa de diálogo Enable client-side LDAPS (Habilitar LDAPS do lado do cliente), escolha Enable (Habilitar).

Método 2: Como habilitar o LDAPS do lado do cliente no AWS Directory Service (AWS CLI)

- Execute o comando a seguir.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Etapa 4: verificar o status do LDAPS

Use um dos métodos a seguir para verificar o status do LDAPS no AWS Directory Service.

Método 1: Como verificar o status do LDAPS no AWS Directory Service (AWS Management Console)

1. Vá para a seção Client-side LDAPS (LDAPS do lado do cliente) na página Directory details (Detalhes do diretório).

2. Se o valor de status for exibido como Enabled (Habilitado), o LDAPS foi configurado com êxito.

Método 2: Como verificar o status do LDAPS no AWS Directory Service (AWS CLI)

- Execute o comando a seguir. Se o valor de status retornar `Enabled`, o LDAPS foi configurado com êxito.

```
aws ds describe-ldaps-settings -directory-id your_directory_id
```

Gerenciar o LDAPS no lado do cliente

Use estes comandos para gerenciar sua configuração LDAPS.

É possível usar dois métodos diferentes para gerenciar configurações do LDAPS do lado do cliente. É possível usar o método AWS Management Console ou o método AWS CLI.

Visualizar detalhes do certificado

Use um dos seguintes métodos para ver quando um certificado está definido para expirar.

Método 1: Como exibir detalhes do certificado no AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).
4. Na seção Client-side LDAPS (LDAPS do lado do cliente) em CA certificates (Certificados CA), serão exibidas informações sobre o certificado.

Método 2: Como exibir detalhes do certificado no AWS Directory Service (AWS CLI)

- Execute o comando a seguir. Para o ID do certificado, use o identificador retornado por `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Cancelar o registro de um certificado

Use um dos seguintes métodos para cancelar o registro de um certificado.

> **Note**
>
> Se apenas um certificado estiver registrado, será necessário primeiro desabilitar o LDAPS para cancelar o registro do certificado.

Método 1: Como cancelar o registro de um certificado no AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).
4. Na seção Client-side LDAPS (LDAPS do lado do cliente), escolha Actions (Ações) e selecione Deregister certificate (Cancelar registro do certificado).
5. Na caixa de diálogo Deregister a CA certificate (Cancelar registro de certificado CA), escolha Deregister (Cancelar registro).

Método 2: Como cancelar o registro de um certificado no AWS Directory Service (AWS CLI)

- Execute o comando a seguir. Para o ID do certificado, use o identificador retornado por `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Desabilitar o LDAPS no lado do cliente

Use um dos seguintes métodos para desabilitar o LDAPS do lado do cliente.

Método 1: Como desabilitar o LDAPS do lado do cliente no AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.

2. Escolha o link do ID de seu diretório.
3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).
4. Na seção Client-side LDAPS (LDAPS do cliente), escolha Disable (Desabilitar).
5. Na caixa de diálogo Disable client-side LDAPS (Desabilitar LDAPS do lado do cliente), escolha Disable (Desabilitar).

Método 2: Como desabilitar o LDAPS do lado do cliente no AWS Directory Service (AWS CLI)

- Execute o comando a seguir.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Habilitar a autenticação mTLS no AD Connector para usar com cartões inteligentes

Você pode usar a autenticação mútua de Transport Layer Security (mTLS) baseada em certificado com cartões inteligentes para autenticar usuários na WorkSpaces Amazon por meio do Active Directory (AD) e do AD Connector autogerenciados. Quando ativado, os usuários selecionam seu cartão inteligente na tela de WorkSpaces login e inserem um PIN para autenticar, em vez de usar um nome de usuário e senha. Assim, a área de trabalho virtual do Windows ou Linux usa o cartão inteligente para se autenticar no AD desde o sistema operacional nativo para desktop.

> **Note**
>
> A autenticação por cartão inteligente no AD Connector está disponível somente nas seguintes opções Regiões da AWS e somente com WorkSpaces. Outros AWS aplicativos não são suportados no momento.
>
> - Leste dos EUA (Norte da Virgínia)
> - Oeste dos EUA (Oregon)
> - Ásia-Pacífico (Sydney)
> - Ásia-Pacífico (Tóquio)
> - Europa (Irlanda)
> - AWS GovCloud (Oeste dos EUA)

Tópicos

Pré-requisitos

Para habilitar a autenticação mútua de Transport Layer Security (mTLS) baseada em certificado usando cartões inteligentes para o WorkSpaces cliente Amazon, você precisa de uma infraestrutura operacional de cartões inteligentes integrada à sua autogestão. Active Directory Para obter mais informações sobre como configurar a autenticação por cartão inteligente com a Amazon WorkSpaces Active Directory, consulte o Guia de WorkSpaces Administração da Amazon.

Antes de habilitar a autenticação por cartão inteligente para WorkSpaces, analise as seguintes considerações:

- Requisitos de certificado de CA
- Requisitos de certificado de TLS
- Processo de verificação da revogação do certificado
- Outras considerações

Requisitos de certificado de CA

O AD Connector exige um certificado de autoridade de certificação (CA), o qual representa o emissor dos seus certificados de usuário, para autenticação por cartão inteligente. O AD Connector combina os certificados de CA com os certificados apresentados pelos usuários com seus cartões inteligentes. Observe os seguintes requisitos de certificado CA:

- Para registrar um certificado de CA, ele deve estar a mais de 90 dias da expiração.
- Os certificados de CA devem estar no formato PEM (Privacy Enhanced Mail). Se você exportar certificados de CA de dentro do Active Directory, escolha Base64-encoded X.509 (.CER) como o formato do arquivo de exportação.
- Todos os certificados de CA raiz e intermediários encadeados de uma CA emissora a certificados de usuário devem ser carregados para que a autenticação por cartão inteligente seja bem-sucedida.
- No máximo, 100 certificados de CA podem ser armazenados por diretório do AD Connector

- O AD Connector não oferece suporte ao algoritmo de assinatura RSASSA-PSS para certificados de CA.
- Verifique se o Serviço de Propagação de Certificados está definido como Automático e em execução.

Requisitos de certificado de TLS

A seguir estão alguns dos requisitos para o certificado de usuário:

- O certificado de cartão inteligente do usuário tem um nome alternativo de assunto (SAN) do usuário userPrincipalName (UPN).
- O certificado de cartão inteligente do usuário tem uso aprimorado de chaves como login do cartão inteligente (1.3.6.1.4.1.311.20.2.2) Autenticação do cliente (1.3.6.1.5.5.7.3.2).
- As informações do Online Certificate Status Protocol (OCSP) do certificado de cartão inteligente do usuário devem ser Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) no Authority Information Access.

Para obter mais informações sobre os requisitos de autenticação do AD Connector e do cartão inteligente, consulte Requisitos no Guia de WorkSpaces Administração da Amazon. Para obter ajuda na solução de WorkSpaces problemas da Amazon, como fazer login WorkSpaces, redefinir a senha ou conectar-se a WorkSpaces, consulte Solucionar problemas WorkSpaces do cliente no Guia WorkSpaces do usuário da Amazon.

Processo de verificação da revogação do certificado

Para realizar a autenticação por cartão inteligente, o AD Connector deve verificar o status de revogação dos certificados do usuário usando o Online Certificate Status Protocol (OCSP). Para realizar a verificação da revogação do certificado, o URL de um respondente OCSP deve ser acessível via Internet. Se estiver usando um nome de DNS, o URL de um respondente OCSP deverá usar um domínio de nível superior encontrado no banco de dados da zona raiz da Internet Assigned Numbers Authority (IANA).

A verificação de revogação de certificados do AD Connector usa o seguinte processo:

- O AD Connector deve verificar a extensão Authority Information Access (AIA) no certificado do usuário para ver se há algum URL de respondente OCSP e, em seguida, o AD Connector usa o URL para verificar a revogação.

- Se o AD Connector não conseguir resolver o URL encontrado na extensão AIA do certificado do usuário ou encontrar um URL de respondente OCSP no certificado do usuário, o AD Connector usará o URL do OCSP opcional fornecido durante o registro do certificado de CA raiz.

  Se o URL na extensão AIA do certificado do usuário for resolvido, mas não responder, a autenticação do usuário falhará.
- Se o URL do respondente OCSP fornecido durante o registro do certificado CA raiz não puder ser resolvido, não estiver respondendo ou se nenhum URL do respondente OCSP tiver sido fornecido, a autenticação do usuário falhará.
- O servidor OCSP deve ser compatível com a RFC 6960. Além disso, o servidor OCSP deve oferecer suporte a solicitações usando o método GET para solicitações menores ou iguais a 255 bytes no total.

> **Note**
>
> O AD Connector exige um URL HTTP para o URL do respondente OCSP.

Outras considerações

Antes de habilitar a autenticação por cartão inteligente no AD Connector, considere os seguintes itens:

- O AD Connector usa autenticação mútua de Transport Layer Security (TLS) baseada em certificado para autenticar usuários no Active Directory usando certificados de cartão inteligente baseados em hardware ou software. No momento, somente cartões de acesso comuns (CAC) e cartões de verificação de identidade pessoal (PIV) podem ser usados. Outros tipos de cartões inteligentes baseados em hardware ou software podem funcionar, mas não foram testados para uso com o protocolo de WorkSpaces streaming.
- A autenticação por cartão inteligente substitui a autenticação por nome de usuário e senha por WorkSpaces.

  Se você tiver outros AWS aplicativos configurados no diretório do AD Connector com a autenticação por cartão inteligente ativada, esses aplicativos ainda apresentarão a tela de entrada de nome de usuário e senha.
- A habilitação da autenticação por cartão inteligente limita a duração da sessão do usuário à vida útil máxima dos tíquetes de serviço Kerberos. Você pode definir essa configuração usando uma

política de grupo, e a duração é definida como 10 horas por padrão. Para obter mais informações sobre configurações e opções, consulte a documentação da Microsoft.

- O tipo de criptografia Kerberos compatível com a conta de serviço do AD Connector deve corresponder a cada tipo de criptografia Kerberos compatível com o controlador de domínio.

Habilitar a autenticação por cartão inteligente

Para habilitar a autenticação por cartão inteligente WorkSpaces em seu AD Connector, primeiro você precisa importar seus certificados de autoridade de certificação (CA) para o AD Connector. Você pode importar seus certificados CA para o AD Connector usando AWS Directory Service console, API ou CLI. Use as etapas a seguir para importar seus certificados de CA e, posteriormente, habilitar a autenticação por cartão inteligente.

Tópicos

- Etapa 1: habilitar a delegação restrita de Kerberos para a conta de serviço do AD Connector
- Etapa 2: registrar o certificado de CA no AD Connector
- Etapa 3: habilitar a autenticação por cartão inteligente para aplicações e serviços da AWS compatíveis

Etapa 1: habilitar a delegação restrita de Kerberos para a conta de serviço do AD Connector

Para usar a autenticação por cartão inteligente com o AD Connector, é necessário habilitar a Delegação restrita de Kerberos (KCD) da conta do AD Connector Service para o serviço LDAP no diretório autogerenciado do AD.

A delegação restrita de Kerberos é um recurso do Windows Server. Esse recurso permite aos administradores especificar e impor limites de confiança de aplicações reduzindo o escopo em que os serviços da aplicação podem atuar em nome de um usuário. Para ter mais informações, consulte Delegação restrita de Kerberos.

> **Note**
>
> A Delegação Restrita Kerberos (KCD) exige que a parte do nome de usuário da conta de serviço do AD Connector corresponda ao SaM AccountName do mesmo usuário. O SaM AccountName é restrito a 20 caracteres. SaM AccountName é um atributo do Microsoft

Active Directory usado como nome de login para versões anteriores de clientes e servidores Windows.

1. Use o comando `SetSpn` para definir um nome de entidade principal de serviço (SPN) para a conta de serviço do AD Connector no AD autogerenciado. Isso habilita a conta de serviço para configuração de delegação.

   O SPN pode ser qualquer combinação de serviço ou nome, mas não uma duplicata de um SPN existente. A opção `-s` verifica duplicatas.

   ```
   setspn -s my/spn service_account
   ```

2. Em Usuários e computadores do AD, abra o menu de contexto (clique com o botão direito), escolha a conta de serviço do AD Connector e escolha Propriedades.
3. Escolha a guia Delegação.
4. Escolha as opções Confiar neste usuário para delegação somente ao serviço especificado e Usar qualquer protocolo de autenticação.
5. Escolha Adicionar e, em seguida, Usuários ou computadores para localizar o controlador de domínio.
6. Escolha OK para exibir uma lista dos serviços disponíveis usados para delegação.
7. Escolha o tipo de serviço ldap e escolha OK.
8. Escolha OK novamente para salvar a nova configuração.
9. Repita esse processo para outros controladores de domínio no Active Directory. Como alternativa, você pode automatizar o processo usando o. PowerShell

Etapa 2: registrar o certificado de CA no AD Connector

Use um dos métodos a seguir para registrar um certificado de CA para o diretório do AD Connector.

Método 1: para registrar seu certificado de CA no AD Connector (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).

4. Na seção Autenticação por cartão inteligente, escolha Ações e, em seguida, escolha Registrar certificado.
5. Na caixa de diálogo Registrar um certificado de CA, selecione Escolher arquivo e escolha o certificado e selecione Abrir. Opcionalmente, é possível realizar a verificação de revogação desse certificado fornecendo um URL de resposta do Online Certificate Status Protocol (OCSP). Para ter mais informações sobre o OCSP, consulte Processo de verificação da revogação do certificado.
6. Escolha Register certificate (Registrar certificado). Quando o status do certificado mudar para Registrado, o processo de registro foi concluído com êxito.

Método 2: para registrar seu certificado de CA no AD Connector (AWS CLI)

- Execute o seguinte comando . Para os dados do certificado, aponte para o local do arquivo de certificado CA. Para fornecer um endereço de respondente OCSP secundário, use o objeto `ClientCertAuthSettings` opcional.

```
aws ds register-certificate --directory-id your_directory_id --certificate-
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings
 OCSPUrl=http://your_OCSP_address
```

Se for bem-sucedida, a resposta fornecerá um ID de certificado. Você também pode verificar se seu certificado de CA foi registrado com êxito executando o seguinte comando da CLI:

```
aws ds list-certificates --directory-id your_directory_id
```

Se o valor de status retornar `Registered`, seu certificado foi registrado com êxito.

Etapa 3: habilitar a autenticação por cartão inteligente para aplicações e serviços da AWS compatíveis

Use um dos métodos a seguir para registrar um certificado de CA para o diretório do AD Connector.

Método 1: para habilitar a autenticação por cartão inteligente no AD Connector (AWS Management Console)

1. Navegue até a seção Autenticação por cartão inteligente na página Detalhes do diretório e escolha Habilitar. Se essa opção não estiver disponível, verifique se um certificado válido foi registrado com êxito e tente novamente.
2. Na caixa de diálogo Habilitar autenticação por cartão inteligente, selecione Habilitar.

Método 2: para habilitar a autenticação por cartão inteligente no AD Connector (AWS CLI)

- Execute o seguinte comando .

```
aws ds enable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

  Se for bem-sucedido, o AD Connector retornará uma resposta `HTTP 200` com um corpo HTTP vazio.

Gerenciar configurações de autenticação por cartão inteligente

É possível usar dois métodos diferentes para gerenciar configurações de cartão inteligente. Você pode usar o AWS Management Console método ou o AWS CLI método.

Tópicos

- Visualizar detalhes do certificado
- Cancelar o registro de um certificado
- Desabilitar a autenticação por cartão inteligente

Visualizar detalhes do certificado

Use um dos seguintes métodos para ver quando um certificado está definido para expirar.

Método 1: Para ver os detalhes do certificado em AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link de ID do diretório do AD Connector.

3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).
4. Na seção Autenticação por cartão inteligente, em Certificados de CA, escolha o ID do certificado para exibir detalhes sobre esse certificado.

Método 2: Para ver os detalhes do certificado em AWS Directory Service (AWS CLI)

- Execute o seguinte comando . Para o ID do certificado, use o identificador retornado por `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Cancelar o registro de um certificado

Use um dos seguintes métodos para cancelar o registro de um certificado.

> **Note**
>
> Se apenas um certificado estiver registrado, será necessário primeiro desabilitar o cartão inteligente para cancelar o registro do certificado.

Método 1: Para cancelar o registro de um certificado em AWS Directory Service ()AWS Management Console

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link de ID do diretório do AD Connector.
3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).
4. Na seção Autenticação por cartão inteligente, em Certificados de CA, selecione o certificado cujo registro você deseja cancelar, escolha Ações e, em seguida, escolha Cancelar registro do certificado.

> **Important**
>
> Verifique se o certificado cujo registro está prestes a cancelar não está ativo ou está sendo usado como parte de uma cadeia de certificados de CA para autenticação por cartão inteligente.

5. Na caixa de diálogo Deregister a CA certificate (Cancelar registro de certificado CA), escolha Deregister (Cancelar registro).

Método 2: Para cancelar o registro de um certificado em AWS Directory Service ()AWS CLI

- Execute o seguinte comando . Para o ID do certificado, use o identificador retornado por `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Desabilitar a autenticação por cartão inteligente

Use um dos métodos a seguir para desabilitar a autenticação por cartão inteligente.

Método 1: Para desativar a autenticação por cartão inteligente em AWS Directory Service (AWS Management Console)

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Escolha o link de ID do diretório do AD Connector.
3. Na página Directory details (Detalhes do diretório), escolha a guia Networking & security (Redes e segurança).
4. Na seção Autenticação por cartão inteligente, escolha Desabilitar.
5. Na seção Desabilitar autenticação por cartão inteligente, escolha Desabilitar.

Método 2: Para desativar a autenticação por cartão inteligente em AWS Directory Service (AWS CLI)

- Execute o seguinte comando .

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Configurar o AWS Private CA conector para AD

Você pode integrar seu Active Directory (AD) autogerenciado com AWS Private Certificate Authority (CA) com o AD Connector para emitir e gerenciar certificados para usuários, grupos e máquinas unidos ao seu domínio AD. AWS Private CA O Connector for AD permite que você use um substituto direto AWS Private CA totalmente gerenciado para suas CAs corporativas autogerenciadas sem a necessidade de implantar, corrigir ou atualizar agentes locais ou servidores proxy.

Você pode configurar a AWS Private CA integração com seu diretório por meio do console do Directory Service, do console AWS Private CA Connector for AD ou chamando a `CreateTemplate`API. Para configurar a integração da CA privada por meio do console do AWS Private CA Connector for Active Directory, consulte AWS Private CA Connector for Active Directory. Veja abaixo as etapas sobre como configurar essa integração a partir do AWS Directory Service console.

Pré-requisitos

Ao usar o AD Connector, você precisa delegar permissões adicionais à conta de serviço. Defina a lista de controle de acesso (ACL) em sua conta de serviço para que você possa concluir os passos a seguir.

- Adicione e remova um nome de entidade principal do serviço (SPN) a si mesmo.
- Crie e atualize autoridades de certificação nos seguintes contêineres:

```
#containers
CN=Public Key Services,CN=Services,CN=Configuration
CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration
CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration
```

- Crie e atualize um objeto da Autoridade de AuthCertificates Certificação NT, como no exemplo abaixo. Se o objeto da Autoridade de AuthCertificates Certificação NT existir, você deverá delegar permissões para ele. Se o objeto não existir, você deverá delegar a capacidade de criar objetos secundários no contêiner de serviços de chave pública.

```
#objects
```

```
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

> **Note**
>
> Se você estiver usando o AWS Managed Microsoft AD, as permissões adicionais serão delegadas automaticamente quando você autorizar o serviço AWS Private CA Connector for AD com seu diretório.

Você pode usar o PowerShell script a seguir para delegar as permissões adicionais e criar o objeto de autoridade de AuthCertifiates certificação do NT. Substitua "myconnectoraccount" pelo nome da conta de serviço.

```
$AccountName = 'myconnectoraccount'

# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module -Name 'ActiveDirectory'
$RootDSE = Get-ADRootDSE

# Getting AD Connector service account Information
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
$AccountAclPath = $AccountProperties.DistinguishedName

# Getting ACL settings for AD Connector service account.
$AccountAcl = Get-ACL -Path "AD:\$AccountAclPath"

# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AccountAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGuid, 'None'
$AccountAcl.AddAccessRule($AccountAccessRule)
Set-ACL -AclObject $AccountAcl -Path "AD:\$AccountAclPath"
```

```
# Add ACLs allowing AD Connector service account the ability to create certification
 authorities
[System.GUID]$CertificationAuthorityGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'certificationAuthority' }
 -Properties 'schemaIDGUID').schemaIDGUID
$CAAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty,CreateChild,DeleteChild', 'Allow',
 $CertificationAuthorityGuid, 'None'
$PKSDN = "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$PKSACL = Get-ACL -Path "AD:\$PKSDN"
$PKSACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $PKSACL -Path "AD:\$PKSDN"

$AIADN = "CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$AIAACL = Get-ACL -Path "AD:\$AIADN"
$AIAACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $AIAACL -Path "AD:\$AIADN"

$CertificationAuthoritiesDN = "CN=Certification Authorities,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
$CertificationAuthoritiesACL = Get-ACL -Path "AD:\$CertificationAuthoritiesDN"
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

$NTAuthCertificatesDN = "CN=NTAuthCertificates,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
If (-Not (Test-Path -Path "AD:\$NTAuthCertificatesDN")) {
New-ADObject -Name 'NTAuthCertificates' -Type 'certificationAuthority' -OtherAttributes
 @{certificateRevocationList=[byte[]]'00';authorityRevocationList=[byte[]]'00';cACertificate=[b
 -Path "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
}

$NTAuthCertificatesACL = Get-ACL -Path "AD:\$NTAuthCertificatesDN"
$NullGuid = [System.GUID]'00000000-0000-0000-0000-000000000000'
$NTAuthAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty', 'Allow', $NullGuid, 'None'
$NTAuthCertificatesACL.AddAccessRule($NTAuthAccessRule)
Set-ACL -AclObject $NTAuthCertificatesACL -Path "AD:\$NTAuthCertificatesDN"
```

Para configurar o AWS Private CA Conector para AD

1. Faça login no AWS Management Console e abra o AWS Directory Service console emhttps://console.aws.amazon.com/directoryservicev2/.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na guia Rede e Segurança, em AWS Private CA Conector para AD, escolha Configurar AWS Private CA Conector para AD. A página Criar certificado CA privado para Active Directory é exibida. Siga as etapas no console para criar sua CA privada para que o Active Directory conector se registre na sua CA privada. Para obter mais informações, consulte Criar um conector.
4. Depois de criar seu conector, siga as etapas abaixo para visualizar os detalhes, incluindo o status do conector e o status da CA privada associada.

Para visualizar o AWS Private CA Conector para AD

1. Faça login no AWS Management Console e abra o AWS Directory Service console emhttps://console.aws.amazon.com/directoryservicev2/.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Em Rede e segurança, em AWS Private CA Connector for AD, você pode visualizar seus conectores de CA privada e a CA privada associada. Por padrão, você vê os seguintes campos:

    a. AWS Private CA ID do conector — O identificador exclusivo de um AWS Private CA conector. Clicar nele leva à página de detalhes desse AWS Private CA conector.

    b. AWS Private CA assunto — Informações sobre o nome distinto da CA. Clicar nele leva à página de detalhes desse AWS Private CA.

    c. Status — Com base em uma verificação de status do AWS Private CA conector e do AWS Private CA. Se ambas as verificações forem aprovadas, Ativo será exibido. Se uma das verificações falhar, 1/2 verificações falhou será exibida. Se as duas verificações falharem, Falha será exibida. Para obter mais informações sobre um status de falha, mova o ponteiro do mouse sobre o hiperlink para saber qual verificação falhou. Siga as instruções no console para fazer a correção.

    d. Data de criação — O dia em que o AWS Private CA conector foi criado.

Para obter mais informações, consulte Visualizar detalhes do conector.

Monitore seu diretório do AD Connector

É possível monitorar seu diretório do AD Connector com os seguintes métodos:

Tópicos

Noções básicas sobre o status do diretório

Os seguintes são os vários status de um diretório.

Ativo

O diretório está funcionando normalmente. Nenhum problema foi detectado pelo AWS Directory Service em seu diretório.

Criando

O diretório está sendo criado no momento. A criação do diretório geralmente leva de 20 a 45 minutos, mas pode variar de acordo com a carga do sistema.

Excluído

O diretório foi excluído. Todos os recursos do diretório foram liberados. Depois que um diretório entra nesse estado, ele não pode ser recuperado.

Deleting

O diretório está sendo excluído no momento. O diretório permanecerá nesse estado até que seja completamente excluído. Depois que um diretório entra nesse estado, a operação de exclusão não pode ser cancelada, e o diretório não pode ser recuperado.

Com falha

O diretório não pôde ser criado. Exclua esse diretório. Se o problema persistir, entre em contato com o AWS Support Center.

Impaired (Degradado)

O diretório está em execução em um estado degradado. Um ou mais problemas foram detectados, e talvez algumas operações do diretório não estejam funcionando com capacidade operacional total. Há muitas razões possíveis para o diretório estar nesse estado. Elas

incluem atividade de manutenção operacional normal, como aplicação de patches ou rotação de instâncias do EC2, localização dinâmica temporária por um aplicativo em um de seus controladores de domínio ou alterações que você fez em sua rede que acidentalmente interrompeu as comunicações do diretório. Para obter mais informações, consulte Solução de problemas do Microsoft AD AWS gerenciado, Solução de problemas do AD Connector, Solução de problemas do Simple AD. Para problemas normais relacionados à manutenção, AWS resolva esses problemas em 40 minutos. Se, após a análise do tópico sobre solução de problemas, seu diretório permanecer em um estado Comprometido por mais de 40 minutos, recomendamos entrar em contato com o AWS Support Center.

> **Important**
>
> Não restaure um snapshot enquanto um diretório estiver em um estado degradado. A restauração de snapshot raramente é necessária para solucionar esses problemas. Para ter mais informações, consulte Criar um snapshot ou restaurar seu diretório.

Inoperable (Inoperável)

O diretório não está funcional. Todos os endpoints do diretório relataram problemas.

Requested (Solicitado)

Uma solicitação para criar seu diretório está pendente no momento.

Configurar notificações de status do diretório com o Amazon SNS

Com o Amazon Simple Notification Service (Amazon SNS), é possível receber mensagens de e-mail ou de texto (SMS) quando o status de seu diretório é alterado. Você receberá uma notificação se o status do diretório for alterado de um status Ativo para um status Degradado ou Inoperável. Você também recebe uma notificação quando o diretório retorna para um status Active.

Como funciona

O Amazon SNS usa “tópicos” para coletar e distribuir mensagens. Cada tópico tem um ou mais assinantes que recebem as mensagens que foram publicadas para aquele tópico. Usando as etapas abaixo, você pode adicionar AWS Directory Service como editor a um tópico do Amazon SNS. Quando AWS Directory Service detecta uma alteração no status do seu diretório, ele publica uma mensagem nesse tópico, que é então enviada aos assinantes do tópico.

É possível associar vários diretórios como publicadores a um único tópico. Também é possível adicionar mensagens de status de diretório a tópicos criados anteriormente no Amazon SNS. Você pode controlar em detalhes quem pode publicar e ser assinante de um tópico. Para obter mais informações sobre o Amazon SNS, consulte O que é o Amazon SNS?.

Para habilitar a troca de mensagens do SNS para o seu diretório

1. Faça login no AWS Management Console e abra o AWS Directory Service console.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Selecione a guia Manutenção.
4. Na seção Monitoramento de diretórios, escolha Ações e, em seguida, selecione Criar notificação.
5. Na página Criar notificação, selecione Escolher um tipo de notificação e, em seguida, escolha Criar uma notificação. Como opção, se você já tem um tópico do SNS, escolha Associar a tópico do SNS existente para enviar mensagens de status deste diretório para o tópico existente.

   > **Note**
   >
   > Se você escolher Criar uma notificação, mas então usar o mesmo nome de um tópico do SNS que já existe, o Amazon SNS não criará um novo tópico, mas apenas adicionará as informações da nova assinatura ao tópico existente.
   > Se você escolher Associar a tópico do SNS existente, somente poderá escolher um tópico do SNS que esteja na mesma região que o diretório.

6. Escolha o Tipo de destinatário e insira as informações de contato do Destinatário. Se você inserir um número de telefone para SMS, use somente números. Não inclua traços, espaços ou parênteses.
7. (Opcional) Forneça um nome para seu tópico e um nome para exibição do SNS. O nome para exibição é um nome curto com até 10 caracteres que é incluído em todas as mensagens de SMS deste tópico. Quando a opção de SMS é usada, o nome de exibição é obrigatório.

   > **Note**
   >
   > Se você estiver logado usando um usuário ou uma função do IAM que tenha somente a política DirectoryServiceFullAccessgerenciada, o nome do tópico deve começar com

> “DirectoryMonitoring”. Caso queira personalizar ainda mais o nome do tópico, precisará de privilégios adicionais no SNS.

8. Escolha Criar.

Se você quiser designar assinantes adicionais do SNS, como um endereço de e-mail adicional, filas do Amazon SQS AWS Lambdaou, você pode fazer isso no console do Amazon SNS.

Para remover as mensagens de status do diretório de um tópico

1. Faça login no AWS Management Console e abra o AWS Directory Service console.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Selecione a guia Manutenção.
4. Na seção Monitoramento de diretórios, selecione um nome de tópico do SNS na lista, escolha Ações e selecione Remover.
5. Escolha Remover.

Isso remove o seu diretório enquanto publicador do tópico do SNS selecionado. Se quiser excluir o tópico inteiro, você pode fazer isso no console do Amazon SNS.

> **Note**
>
> Antes de excluir um tópico do Amazon SNS usando o console do SNS, certifique-se de que o diretório não esteja enviando mensagens de status para aquele tópico.
> Se você excluir um tópico do Amazon SNS usando o console do SNS, essa alteração não será refletida imediatamente no console do Directory Services. Você será notificado somente na próxima vez que um diretório publicar uma notificação para o tópico excluído, quando verá o status atualizado na guia Monitoring do diretório indicando que o tópico não foi encontrado. Portanto, para evitar a perda de mensagens importantes de status do diretório, antes de excluir qualquer tópico do qual receba mensagens AWS Directory Service, associe seu diretório a um tópico diferente do Amazon SNS.

Associe uma instância do Amazon EC2 à sua Active Directory

O AD Connector é um gateway de diretório com o qual você pode redirecionar solicitações de diretório para seu local Microsoft Active Directory sem armazenar nenhuma informação em cache na nuvem. Aqui estão mais informações sobre como você pode associar um Amazon EC2 a um domínio do Active Directory:

- Você pode unir facilmente uma instância do Amazon EC2 ao Active Directory seu domínio quando a instância é executada. Para ter mais informações, consulte Associe perfeitamente uma instância do Amazon Windows EC2 ao seu Microsoft AD AWS gerenciado com o AD Connector.
- Se precisar unir manualmente uma instância do EC2 ao seu Active Directory domínio, inicie a instância no grupo ou sub-rede de segurança adequado Região da AWS e, em seguida, associe a instância ao Active Directory domínio.
- Para se conectar de modo remoto a essas instâncias, você deve ter conectividade IP com as instâncias da rede da qual está se conectando. Na maioria dos casos, é necessário que um gateway da Internet esteja conectado à sua Amazon VPC e que a instância tenha um endereço IP público. Para obter mais informações sobre como conectar à Internet usando um gateway da Internet, consulte Conectar com a Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.

> **Note**
>
> Depois de unir uma instância à sua autogerenciada Active Directory (local), a instância se comunica diretamente com você Active Directory e ignora o AD Connector.

Tópicos

Associe perfeitamente uma instância do Amazon Windows EC2 ao seu Microsoft AD AWS gerenciado com o AD Connector

Esse procedimento une perfeitamente uma instância do Amazon Windows EC2 ao seu Microsoft AD AWS gerenciado. Active Directory

Para ingressar perfeitamente em uma instância do EC2 Windows

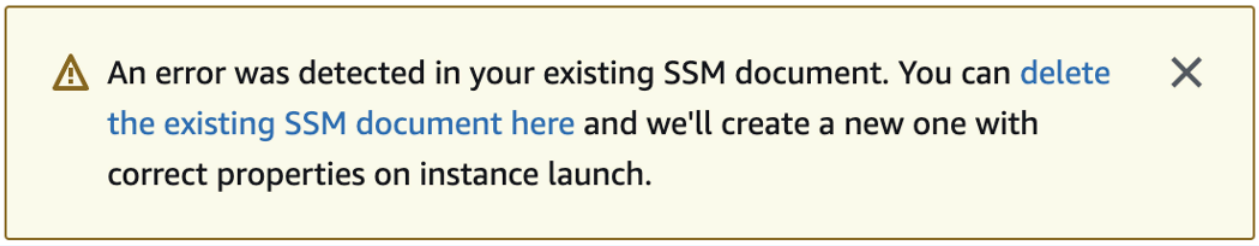
1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o mesmo Região da AWS que o diretório existente.
3. No Painel do EC2, na seção Iniciar instância, escolha Iniciar instância.
4. Na página Iniciar uma instância, na seção Nome e tags, insira o nome que você gostaria de usar para sua instância do Windows EC2.
5. (Opcional) Escolha Adicionar tags extras para um ou mais pares chave-valor de tag para organizar, monitorar ou controlar o acesso para esta instância do EC2.
6. Na seção Imagem da aplicação e do sistema operacional (imagem de máquina da Amazon), escolha Windows no painel Início rápido. É possível alterar a imagem de máquina da Amazon (AMI) do Windows na lista suspensa Imagem de máquina da Amazon (AMI).
7. Na seção Tipo de instância, escolha o tipo de instância que você gostaria de usar na lista suspensa Tipo de instância.
8. Na seção Par de chaves: login, é possível optar por criar um novo par de chaves ou escolher um par de chaves existente.
    a. Para criar um novo par de chaves, escolha Criar par de chaves.
    b. Insira um nome para o par de chaves e selecione uma opção para Tipo de par de chaves e Formato do arquivo de chave privada.
    c. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha .pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha .ppk.
    d. Escolha Criar par de chaves.
    e. O arquivo de chave privada é baixado automaticamente pelo navegador. Salve o arquivo de chave privada em um lugar seguro.

> **Important**
>
> Esta é a única chance de você salvar o arquivo de chave privada.

9. Na página Iniciar uma instância, na seção Configurações de rede, escolha Editar. Escolha a VPC na qual seu diretório foi criado na lista suspensa VPC: obrigatório.
10. Escolha uma das sub-redes públicas em sua VPC na lista suspensa Sub-rede. A sub-rede escolhida deve ter todo o tráfego externo ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.

    Para obter mais informações sobre como conectar a um gateway da Internet, consulte Conectar à Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.
11. Em Atribuir IP público automaticamente, escolha Habilitar.

    Para obter mais informações sobre endereçamento IP público e privado, consulte Endereçamento IP de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.
12. Para configurações de Firewall (grupos de segurança), é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
13. Para opções de Configurar armazenamento, é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
14. Selecione a seção Detalhes avançados, escolha seu domínio na lista suspensa Diretório de associação ao domínio.

> **Note**
>
> Depois de escolher o diretório de ingresso no domínio, você poderá ver:
>
> 
>
>
> Esse erro ocorre se o assistente de inicialização do EC2 identificar um documento SSM existente com propriedades inesperadas. Você pode executar uma das seguintes ações:
>
> - Se você editou anteriormente o documento SSM e as propriedades são esperadas, escolha fechar e continue a executar a instância do EC2 sem alterações.

- Selecione o link excluir o documento SSM existente aqui para excluir o documento SSM. Isso permitirá a criação de um documento SSM com as propriedades corretas. O documento SSM será criado automaticamente quando você iniciar a instância do EC2.

15. Para Perfil de instância do IAM, é possível selecionar um perfil de instância do IAM existente ou criar um novo. Selecione um perfil de instância do IAM que tenha as políticas AWS gerenciadas AmazonSSM ManagedInstanceCore e AmazonSSM DirectoryServiceAccess anexadas a ele na lista suspensa do perfil da instância do IAM. Para criar um novo, escolha Criar novo link de perfil do IAM e faça o seguinte:

    1. Selecione Criar função.
    2. Em Selecionar entidade confiável, escolha serviço da AWS .
    3. Em Use case (Caso de uso), selecione EC2.
    4. Em Adicionar permissões, na lista de políticas, selecione as políticas do AmazonSSM ManagedInstanceCore e do AmazonSSM. DirectoryServiceAccess Para filtrar a lista, digite **`SSM`** na caixa de pesquisa. Escolha Próximo.

    > **Note**
    >
    > O AmazonSSM DirectoryServiceAccess fornece as permissões para unir instâncias a uma Active Directory instância gerenciada por. AWS Directory Service O AmazonSSM ManagedInstanceCore fornece as permissões mínimas necessárias para usar o serviço. AWS Systems Manager Para obter mais informações sobre a criação de um perfil com essas permissões e sobre outras permissões e políticas que você pode atribuir ao seu perfil do IAM, consulte Criar um perfil de instância do IAM para Systems Manager no Guia do usuário do AWS Systems Manager .

    5. Na página Nomear, revisar e criar, insira um Nome de perfil. Você precisará desse nome de perfil para anexar à instância do EC2.
    6. (Opcional) Você pode fornecer uma descrição do perfil de instância do IAM no campo Descrição.
    7. Selecione Criar função.
    8. Volte para a página Iniciar uma instância e escolha o ícone de atualização ao lado do Perfil de instância do IAM. Seu novo perfil de instância do IAM deve estar visível na lista suspensa do

Perfil de instância do IAM. Escolha o novo perfil e mantenha o resto das configurações com seus valores padrão.

16. Escolha Iniciar instância.

Associe perfeitamente uma instância Linux do Amazon EC2 ao seu Microsoft AD AWS gerenciado com o AD Connector

Esse procedimento une perfeitamente uma instância Linux do Amazon EC2 ao seu diretório AWS gerenciado do Microsoft AD.

As seguintes distribuições e versões de instância do Linux são suportadas:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> As distribuições anteriores ao Ubuntu 14 e ao Red Hat Enterprise Linux 7 não oferecem suporte ao recurso de associação direta a domínios.

Pré-requisitos

Antes de configurar a união de domínio perfeita em uma instância Linux do EC2, você precisa concluir os procedimentos nesta seção.

Selecionar sua conta de serviço para associação direta ao domínio

Você pode unir perfeitamente computadores Linux ao seu Active Directory domínio local por meio do AD Connector. Para fazer isso, é necessário criar uma conta de usuário com permissões de criação de conta de computador para associar os computadores ao domínio. Se preferir, você poderá usar sua conta de serviço do AD Connector. Ou você pode usar qualquer outra conta que tenha privilégios suficientes para associar computadores ao domínio. Embora os membros do grupo Administradores

de Domínio ou outros grupos possam ter privilégios suficientes para associar computadores ao domínio, não recomendamos fazer isso. Como prática recomendada, sugerimos usar uma conta de serviço que tenha os privilégios mínimos necessários para associar computadores ao domínio.

Para delegar uma conta com os privilégios mínimos necessários para associar computadores ao domínio, você pode executar os seguintes PowerShell comandos. Você deve executar esses comandos em um Windows computador associado ao domínio com o instalado. Instale as ferramentas de administração do Active Directory para o Microsoft AD AWS gerenciado Além disso, você deve usar uma conta que tenha permissão para modificar as permissões na UO ou no contêiner do seu Computador. O PowerShell comando define permissões que permitem que a conta de serviço crie objetos de computador no contêiner de computadores padrão do seu domínio. Se você preferir usar uma interface gráfica de usuário (GUI), poderá usar o processo manual descrito em Delegar privilégios para sua conta de serviço.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Se você preferir usar uma interface gráfica de usuário (GUI), poderá usar o processo manual descrito em Delegar privilégios para sua conta de serviço.

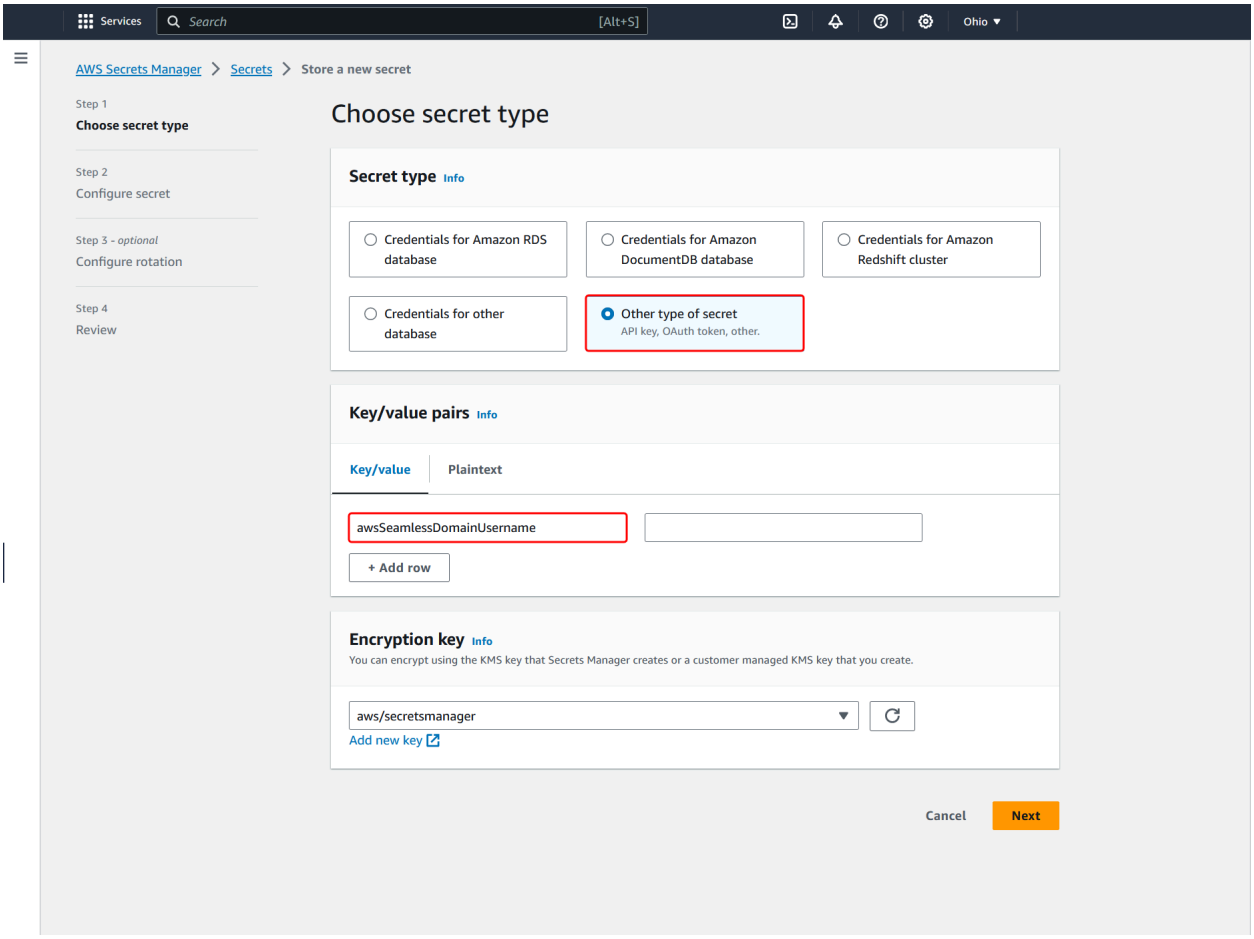
Criar os segredos para armazenar a conta de serviço do domínio

Você pode usar AWS Secrets Manager para armazenar a conta de serviço de domínio.

Para criar segredos e armazenar as informações da conta de serviço do domínio

1. Faça login no AWS Management Console e abra o AWS Secrets Manager console em https://console.aws.amazon.com/secretsmanager/.
2. Selecione Armazenar um novo segredo.
3. Na página Store a new secret (Armazenar um novo segredo), faça o seguinte:
   a. Em Tipo de segredo, escolha Outro tipo de segredos.
   b. Em Pares de chave/valor, faça o seguinte:
      i. Na primeira caixa, insira **`awsSeamlessDomainUsername`**. Na mesma linha, na próxima caixa, insira o nome de usuário da sua conta de serviço. Por exemplo, se você usou o PowerShell comando anteriormente, o nome da conta de serviço seria**`awsSeamlessDomain`**.

> **Note**
>
> Você deve inserir **`awsSeamlessDomainUsername`** exatamente como está. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.



ii. Escolha Adicionar linha.

iii. Na nova linha, na primeira caixa, insira **`awsSeamlessDomainPassword`**. Na mesma linha, na próxima caixa, insira a senha da sua conta de serviço.

> **Note**
>
> Você deve inserir **`awsSeamlessDomainPassword`** exatamente como está. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.

iv. Em Chave de criptografia, deixe o valor padrão`aws/secretsmanager`. AWS Secrets Manager sempre criptografa o segredo quando você escolhe essa opção. Também é possível escolher uma chave criada por você.

> **Note**
>
> Existem taxas associadas AWS Secrets Manager, dependendo de qual segredo você usa. Para obter a lista de preços atual completa, consulte Definição de preço do AWS Secrets Manager.
> Você pode usar a chave AWS gerenciada `aws/secretsmanager` que o Secrets Manager cria para criptografar seus segredos gratuitamente. Se você criar suas próprias chaves KMS para criptografar seus segredos, AWS cobrará a taxa atual AWS KMS . Para obter mais informações, consulte Preços do AWS Key Management Service.

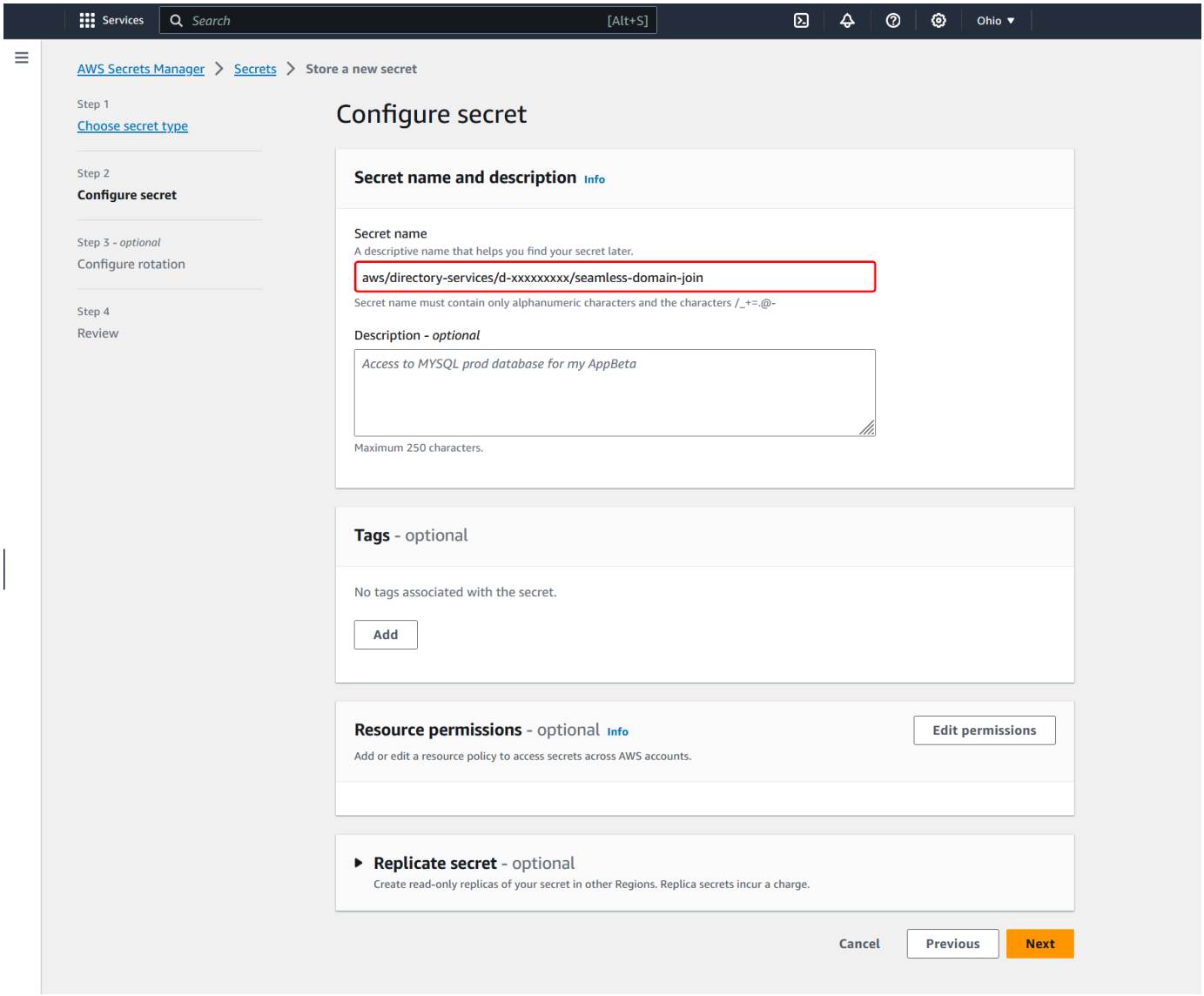
v. Escolha Próximo.

4. Em Nome secreto, insira um nome secreto que inclua sua ID de diretório usando o seguinte formato, substituindo *d-xxxxxxxxx* pela ID do diretório:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Ele será usado para recuperar segredos no aplicativo.

> **Note**
>
> Você deve inserir **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** exatamente como está, mas substituir *d-xxxxxxxxx* pelo ID do diretório. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.



5. Mantenha todo o resto definido como padrão e, em seguida, escolha Próximo.
6. Em Configurar rotação automática, mantenha a opção Desabilitar rotação automática selecionada e escolha Próximo.

   Você pode ativar a rotação desse segredo depois de armazená-lo.
7. Revise as configurações e escolha Armazenar para salvar as alterações. O console do Secrets Manager leva você de volta para a lista de segredos da sua conta com o novo segredo agora incluído na lista.
8. Escolha seu nome de segredo recém-criado na lista e anote o valor do ARN do segredo. Ele será necessário na próxima seção.

Ative a rotação para o segredo da conta de serviço de domínio

Recomendamos que você alterne regularmente os segredos para melhorar sua postura de segurança.

Para ativar a rotação do segredo da conta de serviço de domínio

- Siga as instruções em Configurar a rotação automática para AWS Secrets Manager segredos no Guia do AWS Secrets Manager usuário.

  Para a Etapa 5, use o modelo de rotação das credenciais do Microsoft Active Directory no Guia do AWS Secrets Manager Usuário.

  Para obter ajuda, consulte Solucionar problemas AWS Secrets Manager de rotação no Guia do AWS Secrets Manager usuário.

Criar a política e o perfil do IAM necessários

Use as etapas de pré-requisito a seguir para criar uma política personalizada que permita acesso somente de leitura ao seu segredo de junção de domínio contínuo do Secrets Manager (que você criou anteriormente) e para criar uma nova função LinuxEC2 IAM. DomainJoin

Criar a política de leitura do IAM para o Secrets Manager

Você usa o console do IAM para criar uma política que concede acesso somente de leitura ao seu segredo do Secrets Manager.

Para criar a política de leitura do IAM para o Secrets Manager

1. Faça login no AWS Management Console como um usuário que tem permissão para criar políticas do IAM. Em seguida, abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, Gerenciamento de acesso, escolha Políticas.
3. Escolha Criar política.
4. Escolha a guia JSON e copie o texto do documento de política JSON a seguir. Em seguida, cole-o na caixa de texto JSON.

> **Note**
>
> Certifique-se de substituir o ARN da região e do recurso pela região e o ARN reais do segredo que você criou anteriormente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Quando terminar, escolha Próximo. O validador de política indica se há qualquer erro de sintaxe. Para obter mais informações, consulte Validar políticas do IAM.
6. Na página Revisar política, insira um nome de política, como **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Revise a seção Resumo para ver as permissões que são concedidas pela política. Em seguida, selecione Criar política para salvar suas alterações. A nova política aparece na lista de políticas gerenciadas e está pronta para ser anexada a uma identidade.

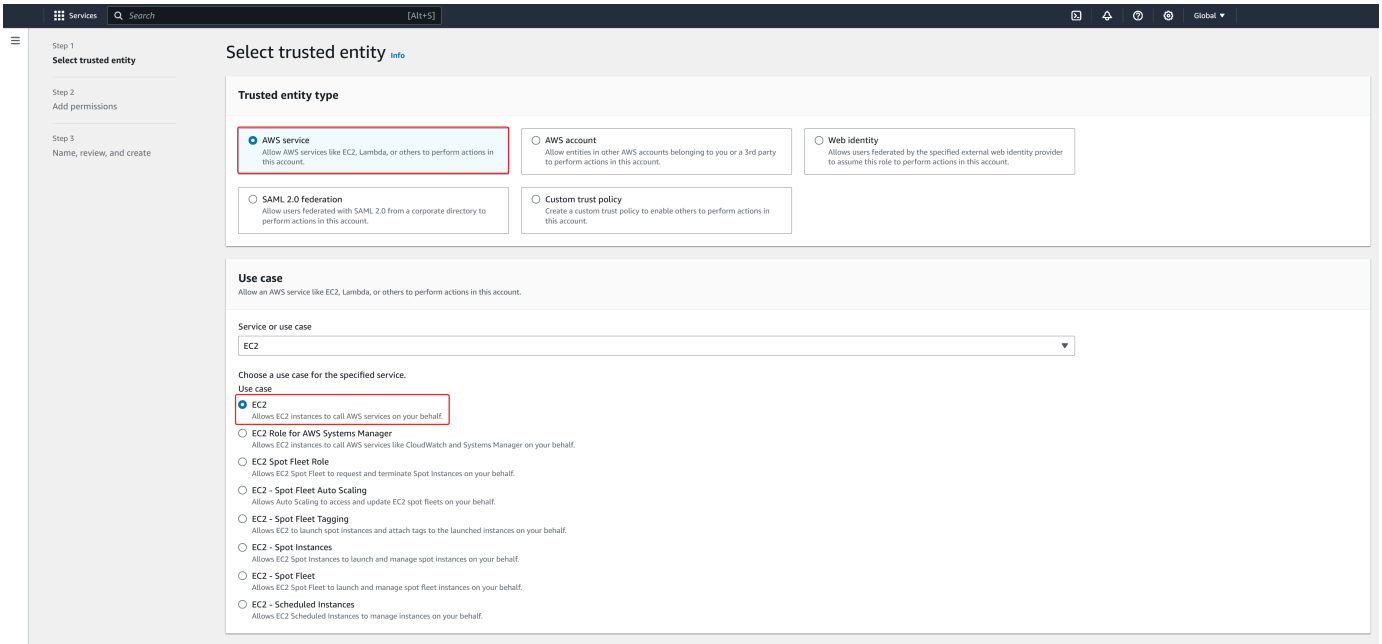
> **Note**
>
> Recomendamos criar uma política por segredo. Isso garante que as instâncias tenham acesso somente ao segredo apropriado e minimiza o impacto em caso de comprometimento de uma instância.

Crie a função LinuxEC2 DomainJoin

Você usa o console do IAM para criar o perfil que usará para associar sua instância do EC2 do Linux ao domínio.

Para criar a função LinuxEC2 DomainJoin

1. Faça login no AWS Management Console como um usuário que tem permissão para criar políticas do IAM. Em seguida, abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, em Gerenciamento de acesso, escolha Perfis.
3. No painel de conteúdo, escolha Criar perfil.
4. Em Select type of trusted entity (Selecionar o tipo de entidade confiável), escolha AWS service (serviço).
5. Em Caso de uso, escolha EC2 e, em seguida, escolha Avançar.



6. Em Políticas de filtro, faça o seguinte:

   a. Insira **`AmazonSSMManagedInstanceCore`**. Em seguida, marque a caixa de seleção para esse item na lista.

   b. Insira **`AmazonSSMDirectoryServiceAccess`**. Em seguida, marque a caixa de seleção para esse item na lista.

   c. Insira **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (ou o nome da política que você criou no procedimento anterior). Em seguida, marque a caixa de seleção para esse item na lista.

d. Depois de adicionar as três políticas listadas acima, selecione Criar função.

> **Note**
>
> O AmazonSSM DirectoryServiceAccess fornece as permissões para unir instâncias a uma Active Directory instância gerenciada por. AWS Directory Service O AmazonSSM ManagedInstanceCore fornece as permissões mínimas necessárias para usar o serviço. AWS Systems Manager Para obter mais informações sobre a criação de um perfil com essas permissões e sobre outras permissões e políticas que você pode atribuir ao seu perfil do IAM, consulte Criar um perfil de instância do IAM para Systems Manager no Guia do usuário do AWS Systems Manager .

7. Insira um nome para sua nova função, como **`LinuxEC2DomainJoin`** ou outro nome de sua preferência no campo Nome da função.
8. (Opcional) Em Role description (Descrição da função), insira uma descrição.
9. (Opcional) Escolha Adicionar nova tag na Etapa 3: Adicionar tags para adicionar tags. Os pares de chave-valor de tag são usados para organizar, rastrear ou controlar o acesso a essa função.
10. Selecione Criar função.

Associe perfeitamente sua instância Linux do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory

Agora que você configurou todas as tarefas de pré-requisito, você pode usar o procedimento a seguir para unir perfeitamente sua instância do EC2 Linux.

Para unir perfeitamente sua instância Linux

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No seletor de região na barra de navegação, escolha o mesmo Região da AWS que o diretório existente.
3. No Painel do EC2, na seção Iniciar instância, escolha Iniciar instância.
4. Na página Iniciar uma instância, na seção Nome e tags, insira o nome que você gostaria de usar para sua instância Linux EC2.

5. (Opcional) Escolha Adicionar tags extras para um ou mais pares chave-valor de tag para organizar, monitorar ou controlar o acesso para esta instância do EC2.
6. Na seção Imagem do aplicativo e do sistema operacional (Amazon Machine Image), escolha uma AMI Linux que você deseja iniciar.

> **Note**
>
> A AMI usada deve ter AWS Systems Manager (SSM Agent) versão 2.3.1644.0 ou superior. Para verificar a versão do SSM Agent instalada em sua AMI iniciando uma instância por essa AMI, consulte Obter a versão do SSM Agent instalada. Se você precisar atualizar o SSM Agent, consulte Instalar e configurar o SSM Agent em instâncias do EC2 para Linux.
> O SSM usa o `aws:domainJoin` plug-in ao unir uma instância Linux a um Active Directory domínio. *O plug-in altera o nome do host das instâncias Linux para o formato EC2AMAZ- XXXXXXX.* Para obter mais informações sobre`aws:domainJoin`, consulte a referência do plug-in do documento de AWS Systems Manager comando no Guia AWS Systems Manager do usuário.

7. Na seção Tipo de instância, escolha o tipo de instância que você gostaria de usar na lista suspensa Tipo de instância.
8. Na seção Par de chaves: login, é possível optar por criar um novo par de chaves ou escolher um par de chaves existente. Para criar um novo par de chaves, escolha Criar par de chaves. Insira um nome para o par de chaves e selecione uma opção para Tipo de par de chaves e Formato do arquivo de chave privada. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha .pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha .ppk. Escolha Criar par de chaves. O arquivo de chave privada é baixado automaticamente pelo navegador. Salve o arquivo de chave privada em um lugar seguro.

> **Important**
>
> Esta é a única chance de você salvar o arquivo de chave privada.

9. Na página Iniciar uma instância, na seção Configurações de rede, escolha Editar. Escolha a VPC na qual seu diretório foi criado na lista suspensa VPC: obrigatório.

10. Escolha uma das sub-redes públicas em sua VPC na lista suspensa Sub-rede. A sub-rede escolhida deve ter todo o tráfego externo ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.

    Para obter mais informações sobre como conectar a um gateway da Internet, consulte Conectar à Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.

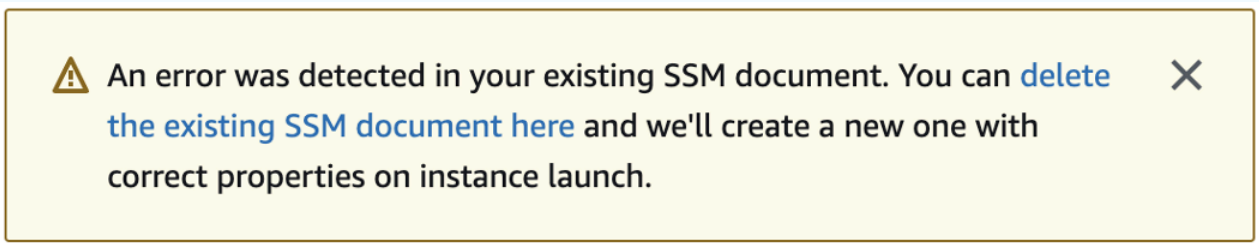
11. Em Atribuir IP público automaticamente, escolha Habilitar.

    Para obter mais informações sobre endereçamento IP público e privado, consulte Endereçamento IP de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.

12. Para configurações de Firewall (grupos de segurança), é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.

13. Para opções de Configurar armazenamento, é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.

14. Selecione a seção Detalhes avançados, escolha seu domínio na lista suspensa Diretório de associação ao domínio.

> **Note**
>
> Depois de escolher o diretório de ingresso no domínio, você poderá ver:
>
> 
>
>
> Esse erro ocorre se o assistente de inicialização do EC2 identificar um documento SSM existente com propriedades inesperadas. Você pode executar uma das seguintes ações:
>
> - Se você editou anteriormente o documento SSM e as propriedades são esperadas, escolha fechar e continue a executar a instância do EC2 sem alterações.
> - Selecione o link excluir o documento SSM existente aqui para excluir o documento SSM. Isso permitirá a criação de um documento SSM com as propriedades corretas. O documento SSM será criado automaticamente quando você iniciar a instância do EC2.

15. Para o perfil da instância do IAM, escolha a função do IAM que você criou anteriormente na seção de pré-requisitos Etapa 2: Criar a função LinuxEC2. DomainJoin
16. Escolha Iniciar instância.

> **Note**
>
> Se você estiver realizando uma associação direta a domínio com o SUSE Linux, uma reinicialização será necessária antes que as autenticações funcionem. Para reinicializar o SUSE via terminal Linux, digite sudo reboot.

Manter seu diretório do AD Connector

Esta seção descreve como manter tarefas administrativas comuns para o seu ambiente do AD Connector.

Tópicos

- Excluir seu AD Connector
- Visualizar informações do diretório

Excluir seu AD Connector

Quando um diretório do AD Connector é excluído, seu diretório on-premises permanece intacto. Todas as instâncias agregadas ao diretório também continuam intactas e permanecem agregadas ao diretório local. Você ainda pode usar as credenciais do diretório para fazer login nessas instâncias.

Para excluir o AD Connector

1. No painel de navegação do console do AWS Directory Service selecione Diretórios. Verifique se você está no Região da AWS local onde seu AD Connector está implantado. Para obter mais informações, consulte Escolha de uma região.
2. Certifique-se de que nenhum AWS aplicativo esteja habilitado para o AD Connector que você pretende excluir. AWS Os aplicativos habilitados impedirão que você exclua seu AD Connector.

    a. Na página Directories (Diretórios), escolha o ID do diretório.

b. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos). Na seção de AWS aplicativos e serviços, você vê quais AWS aplicativos estão habilitados para o seu AD Connector.

- Desative AWS Management Console o acesso. Para ter mais informações, consulte Desabilitar o acesso ao AWS Management Console.
- Para desativar a Amazon WorkSpaces, você deve cancelar o registro do serviço no diretório no WorkSpaces console. Para obter mais informações, consulte Cancelamento do registro de um diretório no Amazon WorkSpaces Administration Guide.
- Para desativar a Amazon WorkDocs, você deve excluir o WorkDocs site da Amazon no WorkDocs console da Amazon. Para obter mais informações, consulte Excluir um site no Guia de WorkDocs Administração da Amazon.
- Para desativar a Amazon WorkMail, você deve remover a WorkMail organização da Amazon no WorkMail console da Amazon. Para obter mais informações, consulte Remover uma organização no Amazon WorkMail Administrator Guide.
- Para desabilitar o Amazon FSx para Windows File Server, é necessário remover o sistema de arquivos Amazon FSx do domínio. Para obter mais informações, consulte Trabalhando com Active Directory o FSx for Windows File Server no Guia do usuário do Amazon FSx for Windows File Server.
- Para desabilitar o Amazon Relational Database Service, é necessário remover a instância do Amazon RDS do domínio. Para obter mais informações, consulte Gerenciar uma instância de banco de dados em um domínio no Guia do usuário do Amazon RDS.
- Para desativar o AWS Client VPN serviço, você deve remover o serviço de diretório do Client VPN Endpoint. Para obter mais informações, consulte Active DirectoryAutenticação no Guia AWS Client VPN do Administrador.
- Para desabilitar o Amazon Connect, exclua a instância do Amazon Connect. Para obter mais informações, consulte Excluir uma instância do Amazon Connect no Guia de administração do Amazon Connect.
- Para desativar a Amazon QuickSight, você deve cancelar a assinatura da Amazon QuickSight. Para obter mais informações, consulte Fechar sua Amazon QuickSight conta no Guia QuickSight do usuário da Amazon.

> **Note**
>
> Se você o estiver usando AWS IAM Identity Center e já o tiver conectado ao diretório AWS gerenciado do Microsoft AD que planeja excluir, primeiro altere a fonte de identidade antes de excluí-la. Para obter mais informações, consulte Alterar sua fonte de identidade no Guia do usuário do Centro de Identidade do IAM.

3. No painel de navegação, selecionar Diretórios.
4. Selecione somente o AD Connector a ser excluído e clique em Excluir. A exclusão do AD Connector pode demorar alguns minutos. Quando o AD Connector tiver sido excluído, ele será removido da sua lista de diretórios.

Visualizar informações do diretório

É possível visualizar informações detalhadas sobre um diretório.

Para visualizar informações detalhadas do diretório

1. No painel de navegação do AWS Directory Service console, em Active Directory, selecione Diretórios.
2. Clique no link de ID de seu diretório. As informações sobre o diretório são exibidas na página Detalhes do diretório.

Para obter mais informações sobre o campo Status, consulte Noções básicas sobre o status do diretório.

Permita o acesso a AWS aplicativos e serviços

Os usuários podem autorizar o AD Connector a fornecer aos AWS aplicativos e serviços, como a Amazon WorkSpaces, acesso ao seuActive Directory. Os AWS aplicativos e serviços a seguir podem ser ativados ou desativados para funcionar com o AD Connector.

AWS aplicativo/serviço	Mais informações...
Amazon Chime	Para obter mais informações, consulte o Guia de administração do Amazon Chime.

AWS aplicativo/serviço	Mais informações...
Amazon Connect	Para obter mais informações, consulte o Guia de administração do Amazon Connect.
Amazon WorkDocs	Para obter mais informações, consulte o Guia de WorkDocs administração da Amazon.
Amazon WorkMail	Para obter mais informações, consulte o Amazon WorkMail Administrator Guide.
Amazon WorkSpaces	Você pode criar um Simple AD, AWS Managed Microsoft AD ou AD Connector diretamente do WorkSpaces. Basta iniciar o Advanced Setup ao criar seu Workspace. Para obter mais informações, consulte o Guia de WorkSpaces administração da Amazon.
AWS Client VPN	Para obter mais informações, consulte o AWS Client VPN Guia do Usuário.
AWS IAM Identity Center	Para obter mais informações, consulte o AWS IAM Identity Center Guia do Usuário.
AWS Management Console	Para ter mais informações, consulte Habilitar acesso ao AWS Management Console com as credenciais do AD.
AWS Transfer Family	Para obter mais informações, consulte o AWS Transfer Family Guia do Usuário.

Após habilitado, você controla o acesso aos diretórios no console da aplicação ou do serviço ao qual deseja fornecer acesso ao diretório. Para encontrar os links de AWS aplicativos e serviços descritos acima no AWS Directory Service console, execute as etapas a seguir.

Para exibir os aplicativos e serviços para um diretório

1. No painel de navegação do console doAWS Directory Service, escolha Diretórios.

2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Revise a lista na seção de Aplicações e serviços daAWS .

Para obter mais informações sobre como autorizar ou desautorizar o uso AWS Directory Servicede AWS aplicativos e serviços, consulte. Autorização para AWS aplicativos e serviços usando AWS Directory Service

Atualizar o endereço de DNS para o AD Connector

Use as etapas a seguir para atualizar os endereços de DNS para os quais o seu AD Connector está apontando.

> **Note**
>
> Se você tiver uma atualização em andamento, aguarde até que ela seja concluída antes de enviar outra atualização.
> Se você estiver usando o WorkSpaces com seu AD Connector, certifique-se de que os endereços de DNS do WorkSpace também estejam atualizados. Para obter mais informações, consulte Atualizar servidores de DNS para WorkSpaces.

Para atualizar as configurações de DNS do AD Connector

1. No painel de navegação do console do AWS Directory Service, em Active Directory, escolha Diretórios.
2. Escolha o link do ID de seu diretório.
3. Na página Detalhes do diretório, escolha a guia Redes e segurança.
4. Role para a seção Configurações de DNS existentes e escolha Atualizar.
5. Na caixa de diálogo Update existing DNS addresses (Atualizar endereços DNS existentes), digite os endereços IP atualizados do DNS e escolha Update (Atualizar).

Para obter mais informações sobre a solução de problemas do AD Connector, consulte Solução de problemas do AD Connector.

Práticas recomendadas para o AD Connector

Estas são algumas sugestões e orientações que devem ser consideradas para evitar problemas e aproveitar ao máximo o AD Connector.

Configuração: pré-requisitos

Considere essas diretrizes antes de criar seu diretório.

Verifique se você tem o tipo de diretório correto

AWS Directory Service fornece várias maneiras de usar Microsoft Active Directory com outros AWS serviços. Você pode escolher o serviço de diretório com os recursos necessários a um custo que caiba em seu orçamento:

- AWS O Directory Service for Microsoft Active Directory é um serviço gerenciado rico em recursos Microsoft Active Directory hospedado na AWS nuvem. AWS O Microsoft AD gerenciado é sua melhor opção se você tiver mais de 5.000 usuários e precisar de uma relação de confiança configurada entre um diretório AWS hospedado e seus diretórios locais.
- O AD Connector simplesmente conecta seu local existente Active Directory a. AWS O AD Connector é a melhor opção quando você deseja usar seu diretório on-premises existente com os serviços da AWS .
- Simple AD é um diretório de baixa escala e baixo custo com compatibilidade básicaActive Directory. Ele oferece suporte a até 5.000 usuários, aplicações compatíveis com Samba 4 e compatibilidade com LDAP para aplicações compatíveis com LDAP.

Para uma comparação mais detalhada das AWS Directory Service opções, consulteQual escolher.

Verificar se suas VPCs e instâncias estão configuradas corretamente

Para se conectar, gerenciar e usar seus diretórios, é necessário configurar corretamente as VPCs às quais seus diretórios estão associados. Consulte AWS Pré-requisitos gerenciados do Microsoft AD, Pré-requisitos do AD Connector ou Pré-requisitos do Simple AD para obter informações sobre os requisitos de segurança e de rede da VPC.

Se estiver adicionando uma instância a seu domínio, verifique se você tem conectividade e acesso remoto à sua instância, conforme descrito em Associe uma instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory.

Conhecer seus limites

Saiba mais sobre os vários limites do seu tipo de diretório específico. O armazenamento disponível e o tamanho agregado dos seus objetos são as únicas limitações no número de objetos que você pode armazenar em seu diretório. Consulte AWS Cotas gerenciadas do Microsoft AD, Cotas do AD Connector ou Cotas do Simple AD para obter detalhes sobre o diretório escolhido.

Entenda a configuração e o uso do grupo de AWS segurança do seu diretório

AWS cria um grupo de segurança e o anexa às interfaces de rede elástica do seu diretório, que podem ser acessadas de dentro de suas VPCs emparelhadas ou redimensionadas. AWS configura o grupo de segurança para bloquear tráfego desnecessário para o diretório e permite o tráfego necessário.

Modificar o grupo de segurança do diretório

Se você deseja modificar a segurança dos grupos de segurança de seus diretórios, você pode fazê-lo. Faça essas alterações apenas se você compreender totalmente como funciona a filtragem do grupo de segurança. Para obter mais informações, consulte Grupos de segurança do Amazon EC2 para instâncias do Linux no Guia do usuário do Amazon EC2. Alterações impróprias podem resultar na perda de comunicações com os computadores e instâncias pretendidos. AWS recomenda que você não tente abrir portas adicionais para seu diretório, pois isso diminui a segurança do seu diretório. Reveja cuidadosamente o Modelo de responsabilidade compartilhada da AWS.

> **Warning**
>
> Tecnicamente, é possível associar os grupos de segurança do diretório a outras instâncias do EC2 que você criar. No entanto, não AWS recomenda essa prática. AWS pode ter motivos para modificar o grupo de segurança sem aviso prévio para atender às necessidades funcionais ou de segurança do diretório gerenciado. Essas alterações afetam as instâncias às quais você associa o grupo de segurança do diretório e podem interromper a operação das instâncias associadas. Além disso, a associação do grupo de segurança do diretório às suas instâncias do EC2 cria um possível risco de segurança para essas instâncias do EC2.

Configurar corretamente os sites e sub-redes on-premises ao usar o AD Connector

Se sua rede on-premises tiver sites do Active Directory definidos, você deverá verificar se as sub-redes da VPC em que o AD Connector reside estão definidas em um site do Active Directory e se não existem conflitos entre as sub-redes da VPC e as sub-redes dos outros sites.

Para descobrir controladores de domínio, o AD Connector usa o site do Active Directory cujos intervalos de endereços IP de sub-rede estão próximos dos da VPC que contém o AD Connector. Se você tiver um site cujas sub-redes têm os mesmos intervalos de endereços IP que os de sua VPC, o AD Connector descobrirá os controladores de domínio nesse site, o qual pode não estar fisicamente próximo de sua região.

Entenda as restrições de nome de usuário para AWS aplicativos

AWS Directory Service fornece suporte para a maioria dos formatos de caracteres que podem ser usados na construção de nomes de usuário. No entanto, existem restrições de caracteres impostas aos nomes de usuário que serão usados para fazer login em AWS aplicativos, como WorkSpaces Amazon WorkMail, WorkDocs Amazon ou Amazon. QuickSight Essas restrições exigem que os seguintes caracteres não sejam usados:

- Espaços
- Caracteres multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> O símbolo@é permitido, desde que ele preceda um sufixo UPN.

Programar suas aplicações

Antes de programar seus aplicativos, considere o seguinte:

Faça um teste de carga antes de implantar no ambiente de produção

Faça testes laboratoriais com aplicativos e solicitações que representem sua workload de produção para confirmar se o diretório é dimensionado de acordo com a carga da aplicação. Se precisar de capacidade adicional, distribua suas cargas em vários diretórios do AD Connector.

Usar o diretório

Estas são algumas sugestões a serem lembradas ao usar o diretório.

Alterne as credenciais de administrador regularmente

Altere sua senha de administrador da conta de serviço do AD Connector regularmente e certifique-se de que a senha seja consistente com as políticas de senha do Active Directory existentes. Para obter instruções sobre como alterar a senha da conta de serviço, consulte Atualizar suas credenciais da conta de serviço do AD Connector no AWS Directory Service.

Use AD Connectors exclusivos para cada domínio

Os AD Connectors e seus domínios do AD on-premises têm uma relação de um para um. Ou seja, para cada domínio on-premises, incluindo domínios filhos em uma floresta do AD na qual você deseja se autenticar, é necessário criar um AD Connector exclusivo. Cada AD Connector que você criar deverá usar uma conta de serviço diferente, mesmo se estiver conectado ao mesmo diretório.

Verifique a compatibilidade

Ao usar o AD Connector, você deve garantir que seu diretório local seja e permaneça compatível com AWS Directory Service s. Para obter mais informações sobre suas responsabilidades, consulte nosso modelo de responsabilidade compartilhada.

Cotas do AD Connector

A seguir estão os limites padrão para o AD Connector. A menos que especificado de outra forma, cada cota é aplicada por região.

Cotas do AD Connector

Recurso	Cota padrão
Diretórios do AD Connector	10
Número máximo de certificados de autoridade de certificação (CA) registrados por diretório	5

Política de compatibilidade de aplicações do AD Connector

Como alternativa ao AWS Directory Service for Microsoft Active Directory (AWS Microsoft AD gerenciado), o AD Connector é um proxy de Active Directory somente para aplicações e serviços criados pela AWS. Você configura o proxy para usar determinado domínio do Active Directory. Quando a aplicação precisa procurar um usuário ou grupo no Active Directory, o AD Connector retransmite a solicitação para o diretório. Da mesma forma, quando um usuário faz login no aplicativo, o AD Connector retransmite a solicitação de autenticação para o diretório. Não existem aplicações de terceiros que funcionem com o AD Connector.

Veja a seguir uma lista de aplicativos e serviços da AWS compatíveis:

- Amazon Chime: para obter instruções detalhadas, consulte Conectar ao Active Directory.
- Amazon Connect: para obter mais informações, consulte Como o Amazon Connect funciona.
- Amazon EC2 para Windows ou Linux — Você pode usar o recurso contínuo de associação de domínios do Active Directory do Amazon EC2 Windows ou Linux para unir sua instância ao seu Active Directory autogerenciado (local). Uma vez associada, a instância se comunica diretamente com o Active Directory e ignora o AD Connector. Para obter mais informações, consulte Associe uma instância do Amazon EC2 à sua Active Directory.
- AWS Management Console: é possível usar o AD Connector para autenticar usuários do AWS Management Console com suas credenciais do Active Directory sem configurar a infraestrutura SAML. Para obter mais informações, consulte Habilitar acesso ao AWS Management Console com as credenciais do AD.
- Amazon QuickSight - Para obter mais informações, consulte Gerenciamento de contas de usuário na Amazon QuickSight Enterprise Edition.
- AWS IAM Identity Center: para obter instruções detalhadas, consulte Conectar o Centro de Identidade do IAM a um Active Directory on-premises.
- AWS Transfer Family: para obter instruções detalhadas, consulte Trabalhar com o AWS Directory Service para Microsoft Active Directory.
- AWS Client VPN: para obter instruções detalhadas, consulte Autenticação e autorização do cliente.
- Amazon WorkDocs — Para obter instruções detalhadas, consulte Conectando-se ao seu diretório local com o AD Connector.
- Amazon WorkMail — Para obter instruções detalhadas, consulte Integrar a Amazon WorkMail com um diretório existente (configuração padrão).

- WorkSpaces - Para obter instruções detalhadas, consulte Iniciar um WorkSpace usando o AD Connector.

> **Note**
>
> O Amazon RDS é compatível somente com o AWS Managed Microsoft AD. Ele não é compatível com o AD Connector. Para obter mais informações, consulte a seção AWS Managed Microsoft AD na página de AWS Directory Serviceperguntas frequentes.

Solução de problemas do AD Connector

O que segue pode ajudá-lo a solucionar alguns problemas comuns que você pode encontrar ao criar ou usar seu AD Connector.

Tópicos

Problemas de criação

A seguir estão os problemas comuns de criação do AD Connector

Recebo um erro de "AZ Constrained" quando crio um diretório

Algumas AWS contas criadas antes de 2012 podem ter acesso às zonas de disponibilidade nas regiões Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Norte da Califórnia) ou Ásia-Pacífico (Tóquio) que não oferecem suporte a AWS Directory Service diretórios. Se você receber um erro

como esse ao criar umActive Directory, escolha uma sub-rede em uma zona de disponibilidade diferente e tente criar o diretório novamente.

Eu recebo o erro “Problemas de conectividade detectados” quando tento criar o AD Connector

Se você receber o erro “Problema de conectividade detectado” ao tentar criar um AD Connector, o erro pode ser devido à disponibilidade da porta ou à complexidade da senha do AD Connector. Você pode testar a conexão do seu AD Connector para ver se as seguintes portas estão disponíveis:

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

Para testar sua conexão, consulteTestar o AD Connector. O teste de conexão deve ser realizado na instância associada às duas sub-redes às quais os endereços IP do AD Connector estão associados.

Se o teste de conexão for bem-sucedido e a instância ingressar no domínio, verifique a senha do AD Connector. O AD Connector deve atender aos requisitos de complexidade da AWS senha. Para obter mais informações, consulte Conta de serviço emPré-requisitos do AD Connector.

Se o AD Connector não atender a esses requisitos, recrie seu AD Connector com uma senha que esteja em conformidade com esses requisitos.

Problemas de conectividade

A seguir estão os problemas comuns de conectividade do AD Connector

- Eu recebo um erro "Problemas de conectividade detectados" quando tento me conectar ao meu diretório on-premises
- Eu recebo um erro de "DNS indisponível" quando tento me conectar ao meu diretório on-premises
- Eu recebo um erro "Registro SRV" quando tento me conectar ao meu diretório on-premises

Eu recebo um erro "Problemas de conectividade detectados" quando tento me conectar ao meu diretório on-premises

Você recebe uma mensagem de erro semelhante à seguinte quando se conecta ao seu diretório local:

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP address>
 Kerberos/authentication unavailable (TCP port 88) for IP: <IP address> Please ensure
 that the listed ports are available and retry the operation.
```

O AD Connector deve ser capaz de se comunicar com seus controladores de domínio on-premises via TCP e UDP nas portas a seguir. Verifique se seus grupos de segurança e firewalls on-premises permitem a comunicação de TCP e UDP por estas portas. Para ter mais informações, consulte Pré-requisitos do AD Connector.

- 88 (Kerberos)
- 389 (LDAP)

Você pode precisar de portas TCP/UDP adicionais, dependendo de suas necessidades. Consulte a lista a seguir para ver algumas dessas portas. Para obter mais informações sobre portas usadas porActive Directory, consulte Como configurar um firewall para Active Directory domínios e relações de confiança na Microsoft documentação.

- 135 (mapeador de pontos finais RPC)
- 646 (SSL LDAP)
- 3268 (PULSAÇÃO DE BANDA)
- 3269 (LDAP GC SSL)

Eu recebo um erro de "DNS indisponível" quando tento me conectar ao meu diretório on-premises

Você recebe uma mensagem de erro semelhante à seguinte quando se conecta ao seu diretório local:

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

O AD Connector deve ser capaz de se comunicar com seus servidores de DNS on-premises via TCP e UDP na porta 53. Verifique se seus grupos de segurança e firewalls on-premises permitem a comunicação de TCP e UDP por essa porta. Para ter mais informações, consulte Pré-requisitos do AD Connector.

Eu recebo um erro "Registro SRV" quando tento me conectar ao meu diretório on-premises

Você recebe uma mensagem de erro semelhante a uma ou mais das seguintes quando se conecta ao seu diretório on-premises:

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos
 does not exist for IP: <DNS IP address>
```

O AD Connector precisa obter os registros de SRV `_ldap._tcp.<DnsDomainName>` e `_kerberos._tcp.<DnsDomainName>` ao se conectar ao seu diretório. Você receberá esse erro se o serviço não conseguir obter esses registros dos servidores DNS que você especificou ao se conectar ao seu diretório. Para obter mais informações sobre esses registros SRV, consulte SRV record requirements.

Problemas de autenticação

Aqui estão alguns problemas comuns de autenticação com o AD Connector:

- Eu recebo o erro “Falha na validação do certificado” quando tento entrar Amazon WorkSpaces com um cartão inteligente
- Recebo um erro "Credenciais inválidas" quando a conta de serviço usada pelo AD Connector tenta se autenticar
- Eu recebo o erro “Não é possível autenticar” ao usar AWS aplicativos para pesquisar usuários ou grupos
- Eu recebo um erro sobre minhas credenciais de diretório quando tento atualizar a conta de serviço do AD Connector
- Alguns dos meus usuários não podem se autenticar com meu diretório

Eu recebo o erro “Falha na validação do certificado” quando tento entrar Amazon WorkSpaces com um cartão inteligente

Você recebe uma mensagem de erro semelhante à seguinte ao tentar entrar no seu WorkSpaces com um cartão inteligente:

```
ERROR: Certificate Validation failed. Please try again by restarting your browser or
 application and make sure you select the correct certificate.
```

O erro ocorre se o certificado do cartão inteligente não estiver armazenado adequadamente no cliente que usa os certificados. Para obter mais informações sobre os requisitos do AD Connector e do cartão inteligente, consultePré-requisitos.

Use os procedimentos a seguir para solucionar problemas com a capacidade do cartão inteligente de armazenar certificados no repositório de certificados do usuário:

1. No dispositivo que está tendo problemas para acessar os certificados, acesse o Microsoft Management Console (MMC).

   > **Important**
   >
   > Antes de prosseguir, crie uma cópia do certificado do cartão inteligente.

2. Navegue até o repositório de certificados no MMC. Exclua o certificado de cartão inteligente do usuário do repositório de certificados. Para obter mais informações sobre como visualizar o repositório de certificados no MMC, consulte Como: Exibir certificados com o snap-in do MMC na documentação. Microsoft
3. Remova o cartão inteligente.
4. Reinsira o cartão inteligente para que ele possa preencher novamente o certificado do cartão inteligente no armazenamento de certificados do usuário.

   > **Warning**
   >
   > Se o cartão inteligente não estiver preenchendo novamente o certificado no armazenamento do usuário, ele não poderá ser usado para autenticação do cartão WorkSpaces inteligente.

A conta de serviço do AD Connector deve ter o seguinte:

- `my/spn`adicionado ao nome do princípio de serviço
- Delegado para o serviço LDAP

Depois que o certificado for preenchido novamente no cartão inteligente, o controlador de domínio local deverá ser verificado para determinar se ele está bloqueado do mapeamento do nome principal do usuário (UPN) para o nome alternativo do assunto. Para obter mais informações sobre essa

alteração, consulte Como desativar o nome alternativo do assunto para mapeamento de UPN na Microsoft documentação.

Use o procedimento a seguir para verificar a chave de registro do seu controlador de domínio:

1. No Editor do Registro, navegue até a seguinte chave de seção

   HKEY_LOCAL_MACHINE\ SYSTEM\\ Serviços\ Kdc\ CurrentControlSet UseSubjectAltName
2. Selecione UseSubjectAltName. Certifique-se de que o valor esteja definido como 0.

> **Note**
>
> Se a chave do registro estiver definida nos controladores de domínio locais, o AD Connector não conseguirá localizar os usuários Active Directory e resultar na mensagem de erro acima.

Os certificados da Autoridade Certificadora (CA) devem ser enviados para o certificado de cartão inteligente AD Connector. O certificado deve conter informações do OCSP. A seguir, listamos os requisitos adicionais para a CA:

- O certificado deve estar na Autoridade Raiz Confiável do Controlador de Domínio, do Servidor da Autoridade de Certificação e do WorkSpaces.
- Os certificados offline e de CA raiz não conterão as informações do OSCP. Esses certificados contêm informações sobre sua revogação.
- Se você estiver usando um certificado CA de terceiros para autenticação por cartão inteligente, os certificados CA e intermediários precisarão ser publicados no repositório Active Directory NTAuth. Eles devem ser instalados na autoridade raiz confiável de todos os controladores de domínio, servidores de autoridade de certificação e. WorkSpaces
  - Você pode usar o comando a seguir para publicar certificados no repositório Active Directory NTauth:

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

Para obter mais informações sobre a publicação de certificados na loja NTAuth, consulte Importar o certificado CA emissor para a loja Enterprise NTAuth no Access Amazon WorkSpaces with Common Access Cards Installation Guide.

Você pode verificar se o certificado do usuário ou os certificados da cadeia CA são verificados pelo OCSP seguindo este procedimento:

1. Exporte o certificado do cartão inteligente para um local na máquina local, como a unidade C:.
2. Abra um prompt de linha de comando e navegue até o local onde o certificado de cartão inteligente exportado está armazenado.
3. Digite o comando :

```
certutil -URL Certficate_name.cer
```

4. Uma janela pop-up deve aparecer após o comando. Selecione a opção OCSP no canto direito e selecione Recuperar. O status deve retornar conforme verificado.

Para obter mais informações sobre o comando certutil, consulte certutil na documentação Microsoft

Recebo um erro "Credenciais inválidas" quando a conta de serviço usada pelo AD Connector tenta se autenticar

Isso pode ocorrer se o disco rígido no controlador de domínio ficar sem espaço. Verifique se os discos rígidos do controlador de domínio não estão cheios.

Eu recebo o erro “Não é possível autenticar” ao usar AWS aplicativos para pesquisar usuários ou grupos

Você pode encontrar erros ao pesquisar usuários ao usar AWS aplicativos, como WorkSpaces o Amazon QuickSight, mesmo quando o status do AD Connector estava ativo. As credenciais expiradas podem impedir que o AD Connector conclua consultas de objetos em seu Active Directory. Atualize a senha da conta de serviço usando as etapas ordenadas fornecidas emA união perfeita de domínios para instâncias do Amazon EC2 parou de funcionar.

Eu recebo um erro sobre minhas credenciais de diretório quando tento atualizar a conta de serviço do AD Connector

Você recebe uma mensagem de erro semelhante a uma ou mais das seguintes ao tentar atualizar a conta de serviço do AD Connector:

```
Message:An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials.
```

```
An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials
following Update your AD Connector Service Account Credentials
```

```
Message:
An Error Has Occurred
Your request has a problem. Please see the following details.
There was an error with the service account/password combination
```

Pode haver um problema com a sincronização de horário e o Kerberos. O AD Connector envia solicitações de autenticação Kerberos para o. Active Directory Essas solicitações são urgentes e, se atrasarem, falharão. Para resolver esse problema, consulte Recomendação - Configurar o PDC raiz com uma fonte de tempo autorizada e evitar distorções de tempo generalizadas na documentação. Microsoft Para obter mais informações sobre serviço de horário e sincronização, veja abaixo:

- Como funciona o serviço de Windows horário
- Tolerância máxima para sincronização do relógio do computador
- WindowsFerramentas e configurações do serviço de horário

Alguns dos meus usuários não podem se autenticar com meu diretório

Suas contas de usuário devem ter a pré-autenticação Kerberos habilitada. Essa é a configuração padrão para contas de usuário novas, mas ela não deve ser modificada. Para obter mais informações sobre essa configuração, acesse Pré-autenticação em Microsoft TechNet.

Problemas de manutenção

A seguir estão os problemas comuns de manutenção do AD Connector

- Meu diretório está travado no estado "Requested"
- A união perfeita de domínios para instâncias do Amazon EC2 parou de funcionar

Meu diretório está travado no estado "Requested"

Se você tiver um diretório que está no estado “solicitado” por mais de cinco minutos, tente excluir o diretório e recriá-lo. Se esse problema continuar, entre em contato com o AWS Support.

A união perfeita de domínios para instâncias do Amazon EC2 parou de funcionar

Se a associação direta a domínios para instâncias do EC2 estava funcionando e foi interrompida enquanto o AD Connector estava ativo, as credenciais para sua conta de serviço do AD Connector podem ter expirado. Credenciais expiradas podem impedir que o AD Connector crie objetos de computador em seu. Active Directory

Para resolver esse problema, atualize as senhas da conta de serviço na seguinte ordem para que as senhas correspondam:

1. Atualize a senha da conta de serviço em seuActive Directory.
2. Atualize a senha da conta de serviço em seu AD Connector em AWS Directory Service. Para ter mais informações, consulte Atualizar suas credenciais da conta de serviço do AD Connector no AWS Directory Service.

> **Important**
>
> Atualizar a senha somente em AWS Directory Service não envia a alteração da senha para o local existenteActive Directory, portanto, é importante fazer isso na ordem mostrada no procedimento anterior.

Não consigo excluir meu AD Connector

Se o AD Connector mudar para um estado inoperável, você não terá mais acesso aos seus controladores de domínio. Bloqueamos a exclusão de um AD Connector quando ainda há aplicações vinculadas a ele porque uma dessas aplicações ainda pode estar usando o diretório. Para obter uma lista de aplicativos que você precisa desativar para excluir seu AD Connector, consulteExcluir seu AD Connector. Se ainda não conseguir excluir seu AD Connector, você pode solicitar ajuda por meio de AWS Support.

Simple AD

O Simple AD é um diretório gerenciado autônomo baseado em um servidor compatível com o Samba 4 Active Directory. Ele está disponível em dois tamanhos.

- Pequeno – oferece suporte a até 500 usuários (aproximadamente 2.000 objetos, incluindo usuários, grupos e computadores).
- Grande – oferece suporte a até 5.000 usuários (aproximadamente 20.000 objetos, incluindo usuários, grupos e computadores).

O Simple AD fornece um subconjunto dos recursos oferecidos pelo AWS Managed Microsoft AD, incluindo a capacidade de gerenciar contas de usuário e associações de grupos, criar e aplicar políticas de grupo, conectar-se com segurança às instâncias do Amazon EC2 e fornecer login único (SSO) baseado em Kerberos. No entanto, observe que o Simple AD não oferece suporte a recursos como autenticação multifator (MFA), relações de confiança com outros domínios, Centro Administrativo do Active Directory, suporte PowerShell , lixeira do Active Directory, contas de serviço gerenciadas por grupos e extensões de esquema para aplicativos POSIX e Microsoft.

O Simple AD oferece muitas vantagens:

- O Simple AD facilita o gerenciamento de instâncias do Amazon EC2 executando Linux e Windows e a implantação de aplicativos Windows na AWS nuvem.
- Muitos dos aplicativos e ferramentas que você usa hoje que exigem suporte do Microsoft Active Directory podem ser usados com Simple AD.
- As contas de usuário no Simple AD permitem acesso a AWS aplicativos como WorkSpaces Amazon WorkDocs ou Amazon WorkMail.
- Você pode gerenciar AWS recursos por meio do acesso baseado em funções do IAM ao. AWS Management Console
- Instantâneos automatizados diários permitem a point-in-time recuperação.

O Simple AD não é compatível com:

- Amazon AppStream 2.0
- Amazon Chime
- Amazon RDS para SQL Server

- Amazon RDS para Oracle
- AWS IAM Identity Center
- Relações de confiança com outros domínios
- Central Administrativa do Active Directory
- PowerShell
- Lixeira do Active Directory
- Contas de serviço gerenciadas pelo grupo
- Extensões de esquema para aplicativos Microsoft e POSIX

Continue a ler os tópicos desta seção para saber como criar seu próprio Simple AD.

Tópicos

Conceitos básicos do Simple AD

O Simple AD cria um diretório totalmente gerenciado baseado em Samba na nuvem. AWS Quando você cria um diretório com o Simple AD, AWS Directory Service cria dois controladores de domínio e servidores DNS em seu nome. Os controladores de domínio são criados em diferentes sub-redes em uma Amazon VPC. Essa redundância ajuda a garantir que seu diretório permaneça acessível mesmo se ocorrer uma falha.

Tópicos

Pré-requisitos do Simple AD

Para criar um Simple ADActive Directory, você precisa de uma Amazon VPC com o seguinte:

- A VPC deve ter uma locação de hardware padrão.
- A VPC não deve estar configurada com os seguintes VPC endpoints:
  - Endpoints VPC Route53 que incluem substituições condicionais de DNS para *.amazonaws.com, que se resolvem para endereços IP não públicos AWS
  - CloudWatch Endpoint VPC
  - Endpoint da VPC do Systems Manager
  - Endpoint da VPC Security Token Service
- Pelo menos duas sub-redes em duas zonas de disponibilidade diferentes. As sub-redes devem estar no mesmo intervalo de roteamento entre domínios sem classe (CIDR). Se você deseja estender ou redimensionar a VPC para seu diretório, certifique-se de selecionar as duas sub-redes do controlador de domínio para o intervalo estendido de CIDR da VPC. Quando você cria um Simple AD, AWS Directory Service cria dois controladores de domínio e servidores DNS em seu nome.
  - Para obter mais informações sobre o intervalo CIDR, consulte o endereçamento IP para suas VPCs e sub-redes no Guia do usuário da Amazon VPC.
- Se você precisar de suporte a LDAPS com o Simple AD, recomendamos configurá-lo usando um Network Load Balancer conectado à porta 389. Esse modelo permite que você use um certificado forte para a conexão LDAPS, simplifique o acesso ao LDAPS por meio de um único endereço IP do NLB e faça failover automático via NLB. O Simple AD não é compatível com o uso de certificados autoassinados na porta 636. Para obter mais informações sobre como configurar o LDAPS com o Simple AD, consulte Como configurar um endpoint do LDAPS para o Simple AD no Blog de segurança da AWS .
- Os seguintes tipos de criptografia devem estar habilitados no diretório:
  - RC4_HMAC_MD5
  - AES128_HMAC_SHA1
  - AES256_HMAC_SHA1
  - Futuros tipos de criptografia

> **Note**
>
> Desabilitar esses tipos de criptografia pode causar problemas de comunicação com o RSAT (Remote Server Administration Tools) e afetar a disponibilidade ou o seu diretório.

- Para obter mais informações, consulte O que é a Amazon VPC? no Guia do usuário da Amazon VPC.

AWS Directory Service usa uma estrutura de duas VPC. As instâncias do EC2 que compõem seu diretório são executadas fora da sua AWS conta e são gerenciadas pela AWS. Elas têm dois adaptadores de rede `ETH0` e `ETH1`. `ETH0` é o adaptador de gerenciamento e existe fora da sua conta. `ETH1` é criado em sua conta.

O intervalo de IP de gerenciamento da `ETH0` rede do seu diretório é escolhido de maneira programática para garantir que não entre em conflito com a VPC em que seu diretório está implantado. Esse intervalo de IP pode estar em qualquer um dos seguintes pares (já que os diretórios são executados em duas sub-redes):

- 10.0.1.0/24 e 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 e 192.168.2.0/24

Evitamos conflitos verificando o primeiro octeto do CIDR `ETH1`. Se ele começar com 10, escolheremos uma VPC 192.168.0.0/16 com sub-redes 192.168.1.0/24 e 192.168.2.0/24. Se o primeiro octeto for diferente de 10, escolheremos uma VPC 10.0.0.0/16 com sub-redes 10.0.1.0/24 e 10.0.2.0/24.

O algoritmo de seleção não inclui rotas em sua VPC. Portanto, é possível que um conflito de roteamento IP resulte desse cenário.

Crie seu Simple AD Active Directory

Para criar um novo Simple ADActive Directory, execute as etapas a seguir. Antes de iniciar este procedimento, verifique se você concluiu os pré-requisitos identificados em Pré-requisitos do Simple AD.

Para criar um Simple AD Active Directory

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios e escolha Configurar diretório.
2. Na página Selecionar tipo do diretório, escolha Simple AD e, em seguida, escolha Próximo.
3. Na página Enter directory information (Inserir informações do diretório), forneça as seguintes informações:

   Tamanho do diretório

   Selecione a opção de tamanho Small (Pequeno) ou Large (Grande). Para obter mais informações sobre os tamanhos, consulte Simple AD.

   Nome da organização

   Um nome de organização exclusivo para seu diretório que será usado para registrar dispositivos clientes.

   Esse campo só estará disponível se você estiver criando seu diretório como parte do lançamento WorkSpaces.

   Nome do DNS do diretório

   O nome completo do diretório, como `corp.example.com`.

   Nome de NetBIOS do diretório

   O nome curto do diretório, como `CORP`.

   Senha do administrador

   A senha do administrador do diretório. O processo de criação do diretório cria uma conta de administrador com o nome de usuário `Administrator` e essa senha.

   A senha do administrador do diretório diferencia maiúsculas de minúsculas e deve ter de 8 a 64 caracteres, inclusive. Ela também precisa conter pelo menos um caractere de três das quatro categorias a seguir:

   - Letras minúsculas (a-z)
   - Letras maiúsculas (A-Z)
   - Números (0-9)
   - Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Confirmar senha

Digite a senha do administrador novamente.

Descrição do diretório

Uma descrição opcional do diretório.

4. Na página Choose VPC and subnets (Selecionar VPC e sub-redes), forneça as seguintes informações e selecione Next (Próximo).

   VPC

   A VPC do diretório.

   Subredes

   Selecione as sub-redes para os controladores de domínio. As duas sub-redes deve estar em diferentes zonas de disponibilidade.

5. Na página Review & create (Revisar e criar), analise as informações do diretório e faça as alterações necessárias. Quando as informações estiverem corretas, escolha Create directory (Criar diretório). A criação do diretório leva vários minutos. Depois de criado, o valor de Status é alterado para Ativo.

O que é criado com seu Simple AD Active Directory

Quando você cria um Active Directory com o Simple AD, AWS Directory Service executa as seguintes tarefas em seu nome:

- Configura de um diretório baseado em Samba na VPC.
- Cria de uma conta de administrador do diretório com o nome de usuário `Administrator` e a senha especificada. Use essa conta para gerenciar seu diretório.

> **Important**
>
> Certifique-se de salvar essa senha. AWS Directory Service não armazena essa senha e ela não pode ser recuperada. No entanto, você pode redefinir uma senha no AWS Directory Service console ou usando a ResetUserPasswordAPI.

- Cria um grupo de segurança para os controladores do diretório.

- Crie uma conta com o nome `AWSAdminD-xxxxxxxx` que tenha privilégios de administração de domínio. Essa conta é usada AWS Directory Service para realizar operações automatizadas para operações de manutenção de diretórios, como tirar instantâneos do diretório e transferir funções FSMO. As credenciais para essa conta são armazenadas com segurança pelo AWS Directory Service.
- Cria e associa automaticamente uma interface de rede elástica (ENI) a cada um dos controladores de domínio. Cada um desses ENIs é essencial para a conectividade entre sua VPC AWS Directory Service e os controladores de domínio e nunca deve ser excluído. Você pode identificar todas as interfaces de rede reservadas para uso com AWS Directory Service a descrição: "interface de rede AWS criada para id de diretório". Para obter mais informações, consulte Elastic Network Interfaces no Guia do usuário do Amazon EC2. O servidor DNS padrão do Microsoft AD AWS gerenciado Active Directory é o servidor VPC DNS em Classless Inter-Domain Routing (CIDR) +2. Para obter mais informações, consulte o servidor Amazon DNS no Guia do usuário da Amazon VPC.

> **Note**
>
> Por padrão, os controladores de domínio são implantados em duas zonas de disponibilidade em uma região e conectados à sua Amazon Virtual Private Cloud (VPC). Os backups são feitos automaticamente uma vez por dia, e os volumes do Amazon Elastic Block Store (EBS) são criptografados para garantir que os dados estejam protegidos em repouso. Os controladores de domínio que falham são substituídos automaticamente na mesma zona de disponibilidade usando o mesmo endereço IP, e uma recuperação completa de desastres pode ser realizada usando-se o backup mais recente.

Configurar o DNS para Simple AD

O Simple AD encaminha as solicitações de DNS para o endereço IP dos servidores de DNS fornecidos pela Amazon para sua Amazon VPC. Esses servidores de DNS resolverão os nomes configurados nas zonas hospedadas privadas do Amazon Route 53. Ao apontar os computadores on-premises para o Simple AD, agora é possível resolver solicitações de DNS para a zona hospedada privada. Para obter mais informações sobre o Route 53, consulte O que é o Route 53.

Observe que para habilitar o Simple AD para responder a consultas de DNS externas, a lista de controle de acesso (ACL) da VPC que contém o Simple AD deve ser configurada para permitir tráfego de fora da VPC.

- Se você não estiver usando zonas hospedadas privadas do Route 53, suas solicitações de DNS serão encaminhadas para servidores de DNS públicos.
- Se você estiver usando servidores DNS personalizados que estão fora da sua VPC e quiser usar um DNS privado, deverá reconfigurar para usar servidores DNS personalizados nas instâncias do EC2 em sua VPC. Para obter mais informações, consulte Como trabalhar com zonas hospedadas privadas.
- Se desejar que o Simple AD resolva nomes usando servidores de DNS em sua VPC e servidores de DNS privados fora de sua VPC, você poderá fazer isso usando um conjunto de opções de DHCP. Para obter um exemplo detalhado, consulte este artigo.

> **Note**
>
> As atualizações dinâmicas de DNS não são compatíveis com domínios do Simple AD. Você pode fazer alterações conectando-se diretamente ao seu diretório usando o Gerenciador DNS em uma instância que integrada em seu domínio.

Como administrar o Simple AD

Esta seção lista todos os procedimentos necessários para operar e manter um ambiente do Simple AD.

Tópicos

Gerenciar usuários e grupos no Simple AD

Os usuários representam pessoas ou entidades individuais que têm acesso ao seu diretório. Os grupos são muito úteis para conceder ou negar privilégios a grupos de usuários, em vez de ter

que aplicar esses privilégios a cada usuário individual. Se um usuário for transferido para uma organização diferente, transfira-o para um grupo diferente e ele receberá os privilégios necessários para a nova organização automaticamente.

Para criar usuários e grupos em um diretório do AWS Directory Service, é necessário usar qualquer instância (on-premises ou EC2) que tenha sido associada a seu diretório do AWS Directory Service e esteja conectada como um usuário com privilégios de criação de usuários e grupos. Você também precisará instalar ferramentas do Active Directory em sua instância do EC2 para que possa adicionar seus usuários e grupos com o snap-in Usuários e Computadores do Active Directory. Para obter mais informações sobre como configurar uma instância do EC2 e instalar as ferramentas necessárias, consulte Associe uma instância do Amazon EC2 ao seu Simple AD Active Directory.

> **Note**
>
> Suas contas de usuário devem ter a pré-autenticação Kerberos habilitada. Essa é a configuração padrão para contas de usuário novas, mas ela não deve ser modificada. Para obter mais informações sobre essa configuração, acesse Pré-autenticação na Microsoft TechNet.

Os tópicos a seguir incluem instruções sobre como criar e gerenciar usuários e grupos.

Tópicos

- Instale as ferramentas de administração do Active Directory para Simple AD
- Criar um usuário do Simple AD
- Excluir um usuário do Simple AD
- Redefinir uma senha de usuário do Simple AD
- Crie um grupo Simple AD
- Adicionar um usuário do Simple AD a um grupo

Instale as ferramentas de administração do Active Directory para Simple AD

Para gerenciar seu Active Directory a partir de uma instância Windows Server do Amazon EC2, você precisa instalar as ferramentas Active Directory Domain Services e Active Directory Lightweight Directory Services na instância. Use o procedimento a seguir para instalar essas ferramentas em uma instância EC2 do Windows Server.

Pré-requisitos

Antes de começar esse procedimento, faça o seguinte:

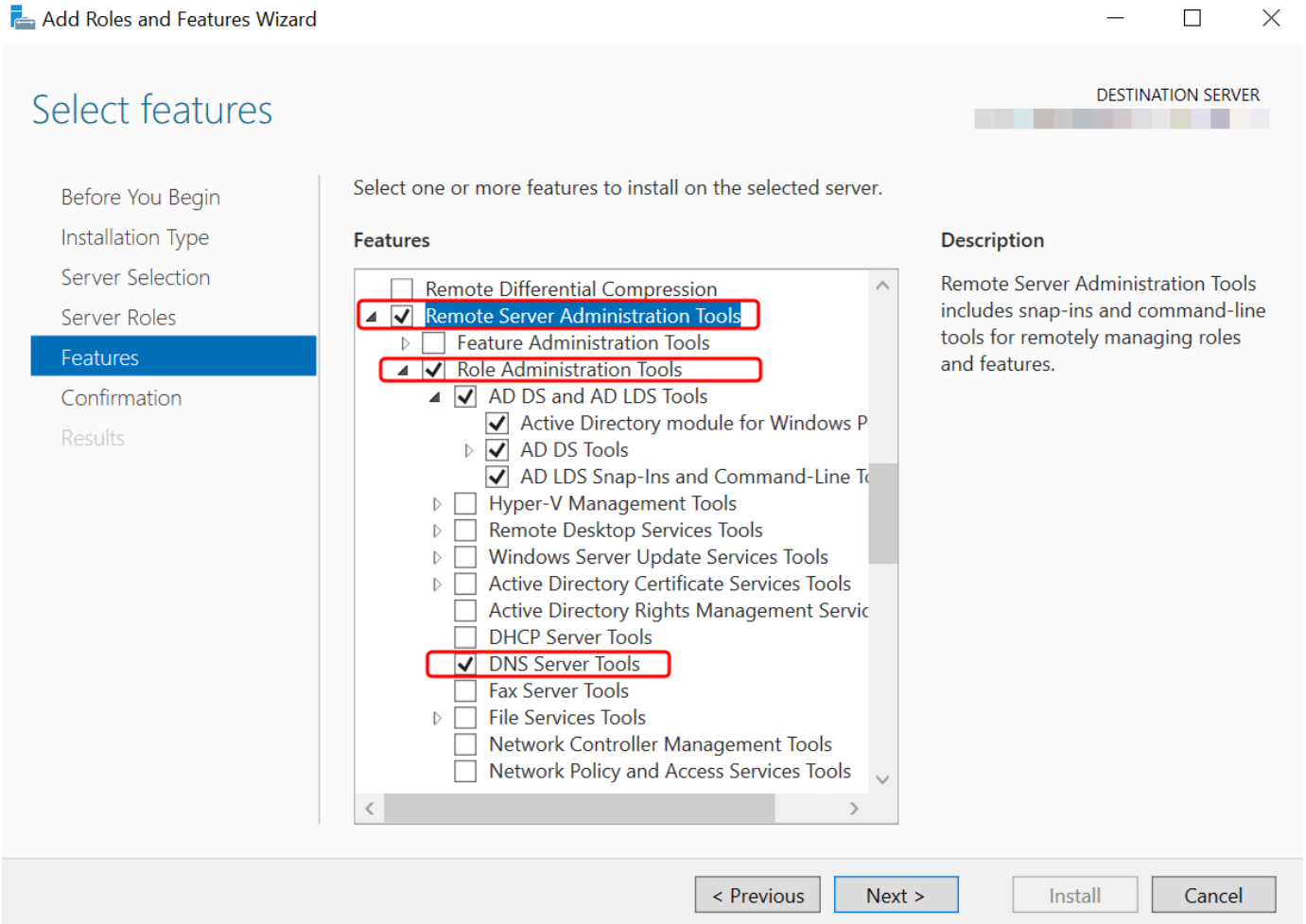
1. Crie um Simple AD Active Directory. Para ter mais informações, consulte Crie seu Simple AD Active Directory.
2. Inicie e junte uma instância do EC2 Windows Server ao seu Simple AD Active Directory. A instância EC2 precisa das seguintes políticas para criar usuários e grupos: **`AWSSSMManagedInstanceCore`** e. **`AmazonSSMDirectoryServiceAccess`** Para ter mais informações, consulte Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Simple AD Active Directory.
3. Você precisará das credenciais do administrador do domínio do Active Directory. Essas credenciais foram criadas quando o Simple AD foi criado. Se você seguiu o procedimento emCrie seu Simple AD Active Directory, seu nome de usuário de administrador inclui seu nome NetBIOS,. **`corp\administrator`**

Instale as Ferramentas de Administração do Active Directory na instância EC2 do Windows Server

Para instalar as ferramentas de administração do Active Directory na instância do EC2 Windows Server

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No console do Amazon EC2, escolha Instâncias, selecione a instância do Windows Server e escolha Conectar.
3. Na página Conectar a instância, escolha Cliente RDP.
4. Na guia Cliente RDP, escolha Baixar arquivo de área de trabalho remota e escolha Obter senha para recuperar sua senha.
5. Em Obter senha do Windows, escolha Fazer upload de arquivo de chave privada. Escolha o arquivo de chave privada .pem associado à instância do Windows Server. Depois de fazer upload do arquivo de chave privada, selecione Descriptografar senha.
6. Na caixa de diálogo Segurança do Windows, copie suas credenciais de administrador local para o computador Windows Server entrar. O nome de usuário pode estar nos seguintes formatos: ***`NetBIOS-Name`*`\administrator`** ou***`DNS-Name`*`\administrator`**. Por exemplo, **`corp\administrator`** seria o nome de usuário se você seguisse o procedimento emCrie seu Simple AD Active Directory.

7. Depois de entrar na instância do Windows Server, abra o Gerenciador do Servidor no menu Iniciar, escolhendo Gerenciador do Servidor.
8. No Painel do Gerenciador do Servidor, escolha Adicionar funções e recursos.
9. No Add Roles and Features Wizard (Adicionar assistente de funções e recursos), selecione Installation Type (Tipo de instalação), selecione Role-based or feature-based installation (Instalação baseada em função ou em recurso) e, em seguida, Next (Avançar).
10. Em Server Selection (Seleção de servidor), verifique se o servidor local está selecionado e escolha Features (Recursos) no painel de navegação esquerdo.
11. Na árvore Recursos, abra Ferramentas de administração do servidor remoto, Ferramentas de administração de funções e Ferramentas de AD DS e AD LDS. Com as Ferramentas AD DS e AD LDS selecionadas, o Active Directorymódulo para Windows PowerShell, Ferramentas AD DS e Snap-ins e Ferramentas de Linha de Comando do AD LDS são selecionados. Role para baixo e selecione Ferramentas de servidor de DNS e escolha Próximo.



12. Revise as informações e selecione Instalar. Quando a instalação do recurso for concluída, o Active Directory Domain Services e as Active Directory Lightweight Directory Services Tools estarão disponíveis no menu Iniciar na pasta Ferramentas administrativas.

Método alternativo para instalar as ferramentas de administração do Active Directory na instância do EC2 Windows Server

- Aqui está outro método para instalar as Ferramentas de Administração do Active Directory:
  - Opcionalmente, você pode optar por instalar as ferramentas de administração do Active Directory usando o. Windows PowerShell Por exemplo, você pode instalar as ferramentas de administração remota do Active Directory a partir de um PowerShell prompt usando`Install-WindowsFeature RSAT-ADDS`. Para obter mais informações, consulte Instalar-WindowsFeature no site da Microsoft.

Criar um usuário do Simple AD

Use o procedimento a seguir para criar um usuário com uma instância do Amazon EC2 associada ao seu diretório Simple AD. Antes de criar usuários, é necessário concluir os procedimentos em Instalar as ferramentas de administração do Active Directory.

> **Note**
>
> Ao usar o Simple AD, se você criar uma conta de usuário em uma instância do Linux com a opção "Forçar usuário a alterar a senha no primeiro login", esse usuário não poderá alterar inicialmente sua senha usando o comando kpasswd. Para alterar a senha pela primeira vez, um administrador de domínio deverá atualizar a senha de usuário usando as ferramentas de gerenciamento do Active Directory.

Você pode usar qualquer um dos métodos a seguir para criar um usuário:

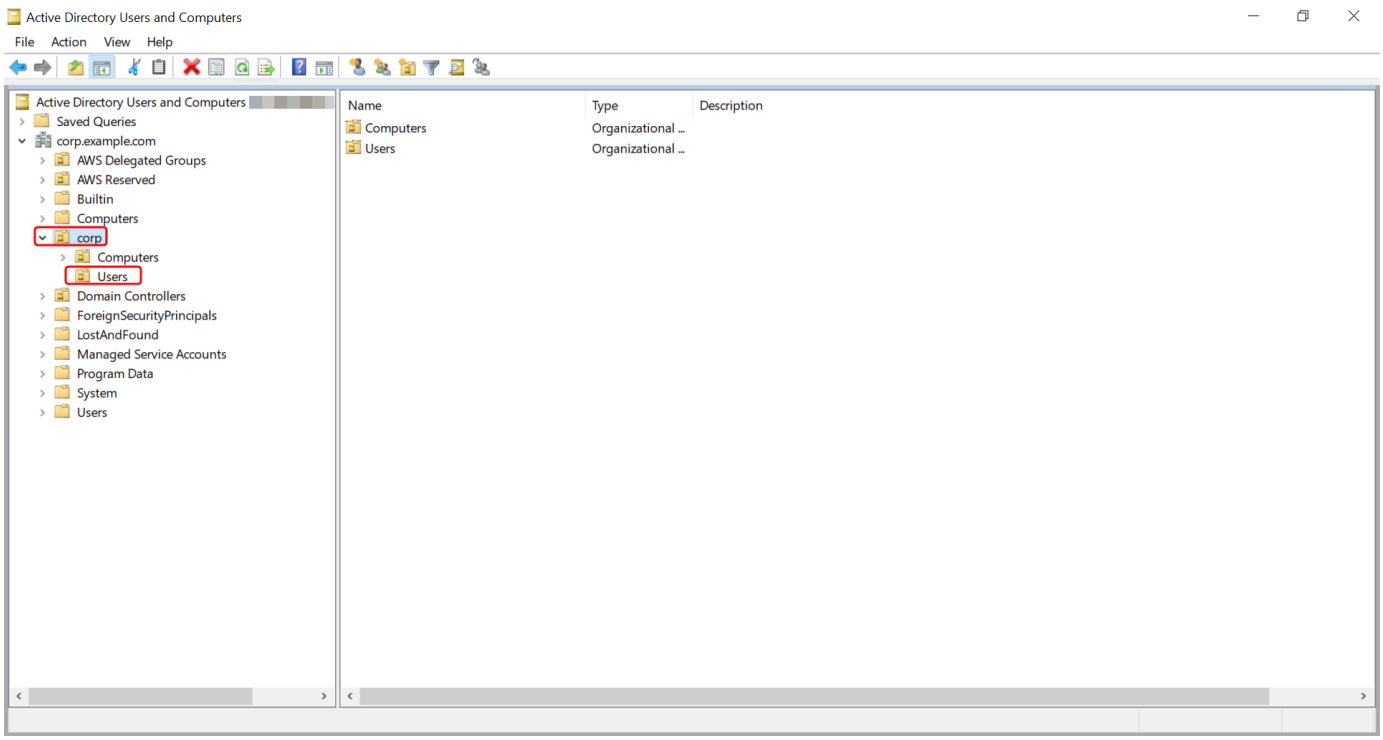
- Active DirectoryFerramentas de administração
- Windows PowerShell

Crie um usuário com as Ferramentas Active Directory Administrativas

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.
2. Abra a ferramenta Usuários e Computadores do Active Directory no menu Iniciar do Windows. Há um atalho para essa ferramenta encontrado na pasta Ferramentas Administrativas do Windows.

> **Tip**
>
> É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Na árvore de diretórios, selecione uma OU sob o nome NetBIOS do seu diretório ou onde você deseja armazenar seu usuário (por exemplo,**`corp\Users`**). Para obter mais informações sobre a estrutura de UO usada pelos diretórios em AWS, consulteO que é criado com seu Microsoft AD Active Directory AWS gerenciado.



4. No menu Ação, escolha Novo. Em seguida, clique em Usuário para abrir o assistente de novo usuário.

5. Na primeira página do assistente, insira os valores dos campos a seguir e escolha Próximo.
   - Nome
   - Sobrenome
   - Nome de logon do usuário
6. Na segunda página do assistente, insira uma senha temporária em Senha e em Confirmar senha. Certifique-se de que a opção O usuário deve alterar a senha no próximo login esteja selecionada. Nenhuma das outras opções deve ser selecionada. Escolha Próximo.
7. Na terceira página do assistente, verifique se as informações do novo usuário estão corretas e clique em Concluir. O novo usuário será exibido na pasta Usuários.

Crie um usuário em Windows PowerShell

1. Conecte-se à instância associada ao seu Active Directory domínio como Active Directory administrador.
2. Abra o Windows PowerShell.
3. Digite o comando a seguir substituindo o nome **`jane.doe`** de usuário pelo nome de usuário do usuário que você deseja criar. Você será solicitado Windows PowerShell a fornecer uma senha para o novo usuário. Para obter mais informações sobre os requisitos de complexidade de Active Directory senhas, consulte a Microsoftdocumentação. Para obter mais informações sobre o comando New-ADUser, consulte a documentação. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Excluir um usuário do Simple AD

Use o procedimento a seguir para excluir um usuário com uma instância Windows do Amazon EC2 que está associada ao seu diretório Simple AD.

Você pode usar qualquer um dos métodos a seguir para excluir um usuário:

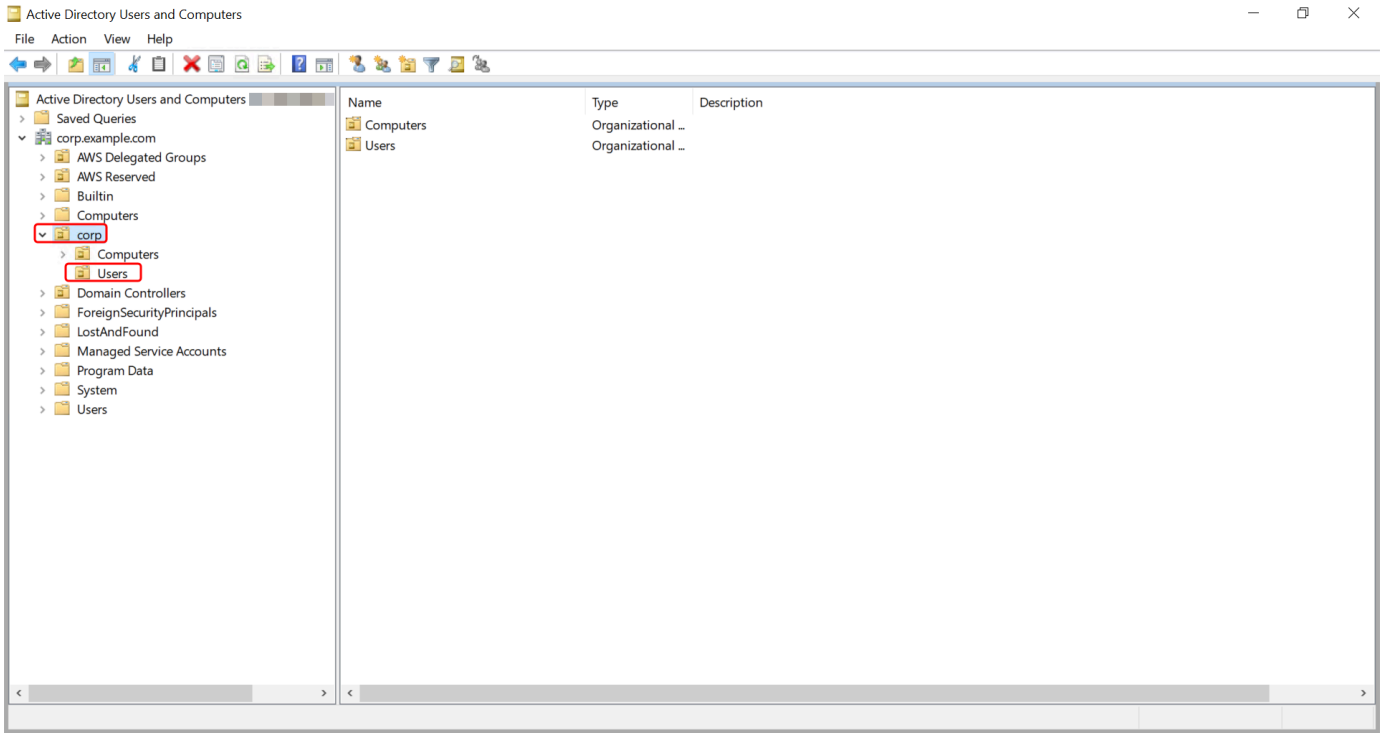
- Active DirectoryFerramentas de administração
- Windows PowerShell

Excluir um usuário com as Ferramentas Active Directory Administrativas

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.
2. Abra a ferramenta Usuários e Computadores do Active Directory no menu Iniciar do Windows. Há um atalho para essa ferramenta encontrado na pasta Ferramentas Administrativas do Windows.

> **Tip**
>
> É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Na árvore de diretórios, selecione a OU que contém o usuário que você deseja excluir (por exemplo,**`corp\Users`**).



4. Selecione o usuário que deseja excluir. No menu Ação, escolha Excluir.
5. Uma caixa de diálogo aparecerá solicitando que você confirme que deseja excluir o usuário. Escolha Sim para excluir o usuário. Isso exclui permanentemente o usuário selecionado.

Excluir um usuário em Windows PowerShell

1. Conecte-se à instância associada ao seu Active Directory domínio como Active Directory administrador.
2. Abra o Windows PowerShell.
3. Digite o comando a seguir substituindo o nome **`jane.doe`** de usuário pelo nome de usuário do usuário que você deseja excluir. Para obter mais informações sobre o comando Remove-ADUser, consulte a documentação. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Redefinir uma senha de usuário do Simple AD

Os usuários devem seguir as políticas de senha, conforme definido noActive Directory. Às vezes, isso pode tirar o melhor proveito dos usuários, incluindo o Active Directory administrador, e eles esquecem a senha. Quando isso acontece, você pode redefinir rapidamente a senha do usuário usando AWS Directory Service se o usuário residir no Simple AD.

Você deve estar conectado como um usuário com as permissões necessárias para redefinir senhas. Para obter mais informações sobre permissões, consulte Visão geral do gerenciamento de permissões de acesso aos seus AWS Directory Service recursos.

Você pode redefinir a senha de qualquer usuário do seu, Active Directory com as seguintes exceções:

- Você pode redefinir a senha de qualquer usuário dentro da Unidade Organizacional (OU) baseada no nome NetBIOS que você usou ao criar seu. Active Directory Por exemplo, se você seguisse o procedimento emCrie seu Simple AD Active Directory, seu nome NetBIOS seria CORP e as senhas dos usuários que você poderia redefinir seriam membros da OU Corp/Users.
- Você não pode redefinir a senha de nenhum usuário fora da OU que seja baseada no nome NetBIOS que você usou quando criou o seu. Active Directory Para obter mais informações sobre a estrutura de OU do Simple AD, consulteO que é criado com seu Simple AD Active Directory.
- Você não pode redefinir a senha de nenhum usuário que seja membro de dois domínios. Você também não pode redefinir a senha de nenhum usuário que seja membro do grupo Administradores de Domínio ou Administradores de Empresa, exceto o usuário Administrador.

- Você não pode redefinir a senha de nenhum usuário que seja membro do grupo Administradores de Domínio ou Administradores Corporativos, exceto do usuário administrador.

Você pode usar qualquer um dos métodos a seguir para redefinir uma senha de usuário:

- AWS Management Console
- AWS CLI
- Windows PowerShell

Redefinir uma senha de usuário no AWS Management Console

1. No painel de navegação do AWS Directory Service console, em Active Directory, escolha Diretórios e selecione o Active Directory na lista em que você deseja redefinir uma senha de usuário.
2. Na página Detalhes do usuário, escolha Ações, Redefinir senha.
3. Na caixa de diálogo Redefinir senha do usuário, em Nome de usuário, digite o nome de usuário do usuário cuja senha precisa ser alterada.
4. Digite uma senha em Nova senha e Confirmar senha e escolha Redefinir senha.

Redefinir uma senha de usuário em AWS CLI

1. Para instalar o AWS CLI, consulte Instalar ou atualizar a versão mais recente do AWS CLI.
2. Abra AWS CLI o.
3. Digite o comando a seguir e substitua o ID do diretório, o nome de usuário **`jane.doe`** e a senha **`P@ssw0rd`** pelo ID Active Directory do diretório e pelas credenciais desejadas. Consulte reset-user-passworda Referência de AWS CLI Comandos para obter mais informações.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

Redefinir uma senha de usuário em Windows PowerShell

1. Conecte-se à instância associada ao seu Active Directory domínio como Active Directory administrador.
2. Abra o Windows PowerShell.

3. Digite o comando a seguir substituindo o nome de usuário**`jane.doe`**, o ID do diretório e a senha **`P@ssw0rd`** pelo ID Active Directory do diretório e pelas credenciais desejadas. Consulte Reset-DS UserPassword Cmdlet para obter mais informações.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Crie um grupo Simple AD

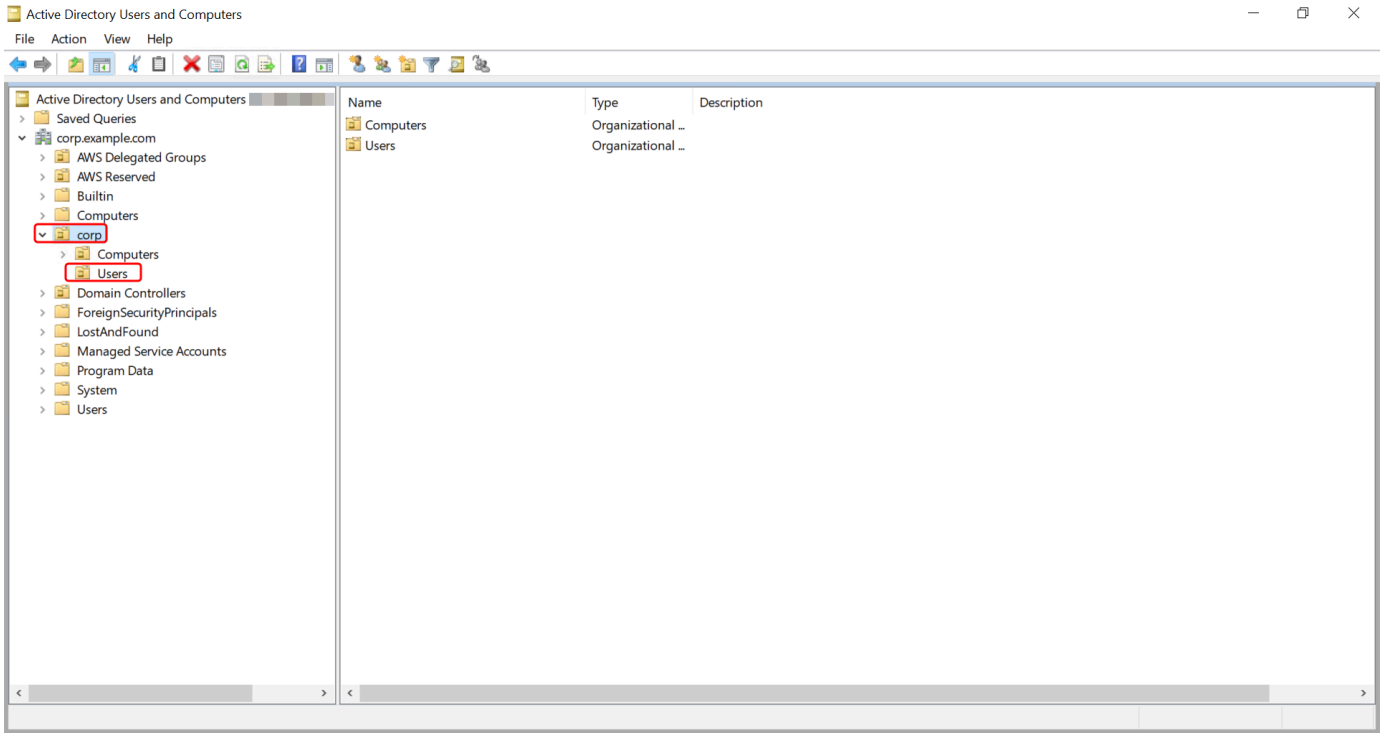
Use o procedimento a seguir para criar um grupo de segurança com uma instância do Amazon EC2 associada ao seu diretório Simple AD. Antes de criar grupos de segurança, é necessário concluir os procedimentos em Instalar as ferramentas de administração do Active Directory.

Para criar um grupo

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.
2. Abra a ferramenta Usuários e Computadores do Active Directory. Um atalho para essa ferramenta está disponível na pasta Ferramentas Administrativas.

   > **Tip**
   >
   > É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Na árvore de diretórios, selecione uma UO sob a UO do nome NetBIOS do seu diretório em que você deseja armazenar o grupo (por exemplo, Corp\Users). Para obter mais informações sobre a estrutura de UO usada pelos diretórios em AWS, consulteO que é criado com seu Microsoft AD Active Directory AWS gerenciado.



4. No menu Ação, clique em Novo. Em seguida, clique em Grupo para abrir o assistente de novo grupo.
5. Digite um nome para o grupo em Nome do grupo, selecione um Escopo de grupo que atenda às suas necessidades e selecione Segurança para o Tipo de grupo. Para obter mais informações sobre o escopo do grupo e os grupos de segurança do Active Directory, consulte Grupos de segurança do Active Directory na documentação do Microsoft Windows Server.
6. Clique em OK. O novo grupo de segurança será exibido na pasta Usuários.

Adicionar um usuário do Simple AD a um grupo

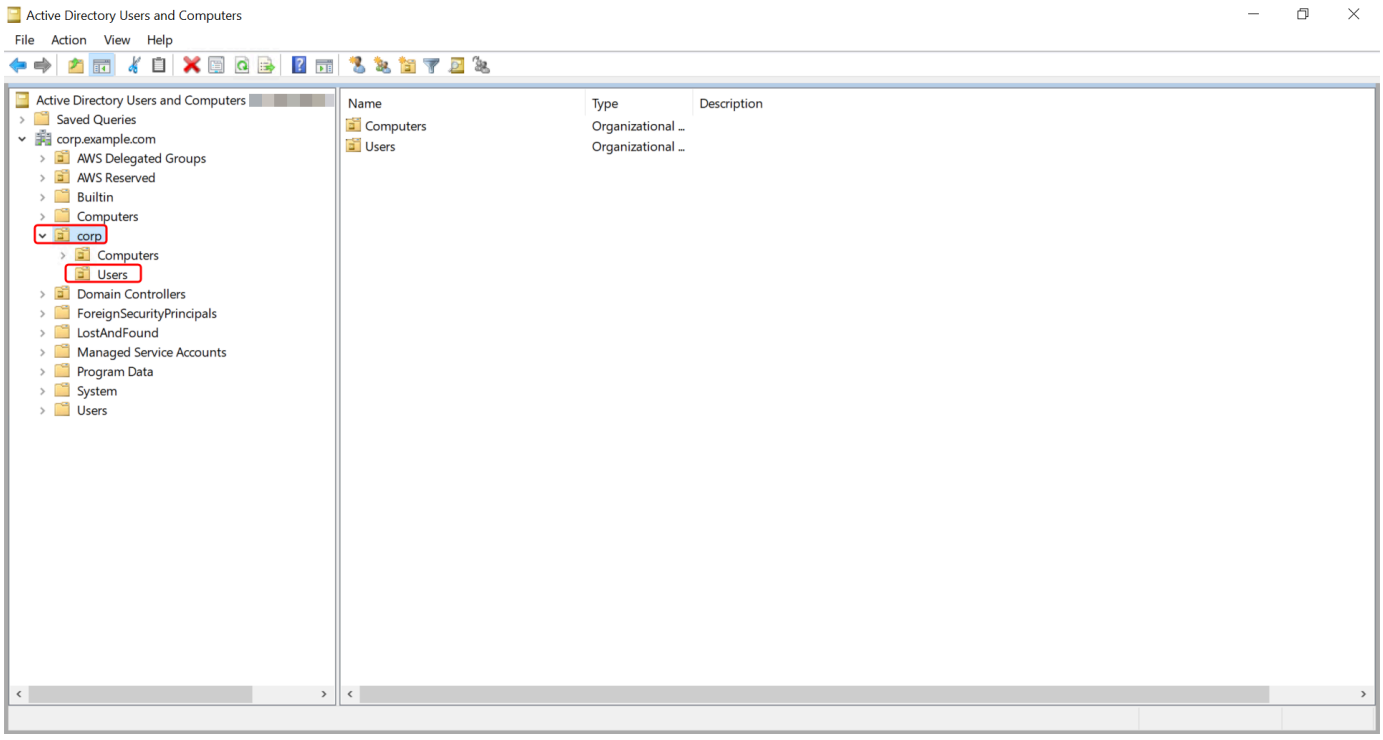
Use o procedimento a seguir para adicionar um usuário a um grupo de segurança com uma instância do EC2 que esteja associada ao seu diretório do Simple AD.

Como adicionar um usuário a um grupo

1. Conecte-se à instância em que as ferramentas de administração do Active Directory foram instaladas.
2. Abra a ferramenta Usuários e Computadores do Active Directory. Um atalho para essa ferramenta está disponível na pasta Ferramentas Administrativas.

> **Tip**
>
> É possível executar o seguinte em um prompt de comando na instância para abrir diretamente a caixa de ferramentas Usuários e Computadores do Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Na árvore de diretórios, selecione a UO sob a UO do nome NetBIOS do seu diretório em que você armazenou seu grupo e selecione o grupo ao qual deseja adicionar um usuário como membro.



4. No menu Ação, clique em Propriedades para abrir a caixa de diálogo de propriedades do grupo.
5. Selecione a guia Membros e clique em Adicionar.
6. Em Digite os nomes dos objetos a serem selecionados, digite o nome de usuário que você deseja adicionar e clique em OK. O nome será exibido na lista Membros. Clique em OK novamente para atualizar a associação ao grupo.
7. Verifique se o usuário agora é membro do grupo selecionando o usuário na pasta Usuários e clicando em Propriedades no menu Ação para abrir a caixa de diálogo de propriedades. Selecione a guia Membro de. Você deverá ver o nome do grupo na lista de grupos aos quais o usuário pertence.

Monitorar seu diretório do Simple AD

É possível monitorar seu diretório do Simple AD com os seguintes métodos:

Tópicos

Noções básicas sobre o status do diretório

Os seguintes são os vários status de um diretório.

Ativo

O diretório está funcionando normalmente. Nenhum problema foi detectado pelo AWS Directory Service em seu diretório.

Criando

O diretório está sendo criado no momento. A criação do diretório geralmente leva de 20 a 45 minutos, mas pode variar de acordo com a carga do sistema.

Excluído

O diretório foi excluído. Todos os recursos do diretório foram liberados. Depois que um diretório entra nesse estado, ele não pode ser recuperado.

Deleting

O diretório está sendo excluído no momento. O diretório permanecerá nesse estado até que seja completamente excluído. Depois que um diretório entra nesse estado, a operação de exclusão não pode ser cancelada, e o diretório não pode ser recuperado.

Com falha

O diretório não pôde ser criado. Exclua esse diretório. Se o problema persistir, entre em contato com o AWS Support Center.

Impaired (Degradado)

O diretório está em execução em um estado degradado. Um ou mais problemas foram detectados, e talvez algumas operações do diretório não estejam funcionando com capacidade operacional total. Há muitas razões possíveis para o diretório estar nesse estado. Elas incluem atividade de manutenção operacional normal, como aplicação de patches ou rotação

de instâncias do EC2, localização dinâmica temporária por um aplicativo em um de seus controladores de domínio ou alterações que você fez em sua rede que acidentalmente interrompeu as comunicações do diretório. Para obter mais informações, consulte Solução de problemas do Microsoft AD AWS gerenciado, Solução de problemas do AD Connector, Solução de problemas do Simple AD. Para problemas normais relacionados à manutenção, AWS resolva esses problemas em 40 minutos. Se, após a análise do tópico sobre solução de problemas, seu diretório permanecer em um estado Comprometido por mais de 40 minutos, recomendamos entrar em contato com o AWS Support Center.

> **Important**
>
> Não restaure um snapshot enquanto um diretório estiver em um estado degradado. A restauração de snapshot raramente é necessária para solucionar esses problemas. Para ter mais informações, consulte Criar um snapshot ou restaurar seu diretório.

Inoperable (Inoperável)

O diretório não está funcional. Todos os endpoints do diretório relataram problemas.

Requested (Solicitado)

Uma solicitação para criar seu diretório está pendente no momento.

RestoreFailed

Falha na restauração do diretório em um snapshot. Tente a operação de restauração novamente. Se o problema continuar, tente usar um snapshot diferente ou entre em contato com o AWS Support Center.

Restoring (Restaurando)

O diretório está sendo restaurado no momento em um snapshot automático ou manual. A restauração em um snapshot geralmente demora vários minutos, dependendo do tamanho dos dados do diretório no snapshot.

Para ter mais informações, consulte Motivos para status de diretórios do Simple AD.

Configurar notificações de status do diretório com o Amazon SNS

Com o Amazon Simple Notification Service (Amazon SNS), é possível receber mensagens de e-mail ou de texto (SMS) quando o status de seu diretório é alterado. Você receberá uma notificação se o

status do diretório for alterado de um status Ativo para um status Degradado ou Inoperável. Você também recebe uma notificação quando o diretório retorna para um status Active.

Como funciona

O Amazon SNS usa “tópicos” para coletar e distribuir mensagens. Cada tópico tem um ou mais assinantes que recebem as mensagens que foram publicadas para aquele tópico. Usando as etapas abaixo, você pode adicionar AWS Directory Service como editor a um tópico do Amazon SNS. Quando AWS Directory Service detecta uma alteração no status do seu diretório, ele publica uma mensagem nesse tópico, que é então enviada aos assinantes do tópico.

É possível associar vários diretórios como publicadores a um único tópico. Também é possível adicionar mensagens de status de diretório a tópicos criados anteriormente no Amazon SNS. Você pode controlar em detalhes quem pode publicar e ser assinante de um tópico. Para obter mais informações sobre o Amazon SNS, consulte O que é o Amazon SNS?.

Para habilitar a troca de mensagens do SNS para o seu diretório

1. Faça login no AWS Management Console e abra o AWS Directory Service console.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Selecione a guia Manutenção.
4. Na seção Monitoramento de diretórios, escolha Ações e, em seguida, selecione Criar notificação.
5. Na página Criar notificação, selecione Escolher um tipo de notificação e, em seguida, escolha Criar uma notificação. Como opção, se você já tem um tópico do SNS, escolha Associar a tópico do SNS existente para enviar mensagens de status deste diretório para o tópico existente.

   > **Note**
   >
   > Se você escolher Criar uma notificação, mas então usar o mesmo nome de um tópico do SNS que já existe, o Amazon SNS não criará um novo tópico, mas apenas adicionará as informações da nova assinatura ao tópico existente.
   > Se você escolher Associar a tópico do SNS existente, somente poderá escolher um tópico do SNS que esteja na mesma região que o diretório.

6. Escolha o Tipo de destinatário e insira as informações de contato do Destinatário. Se você inserir um número de telefone para SMS, use somente números. Não inclua traços, espaços ou parênteses.

7. (Opcional) Forneça um nome para seu tópico e um nome para exibição do SNS. O nome para exibição é um nome curto com até 10 caracteres que é incluído em todas as mensagens de SMS deste tópico. Quando a opção de SMS é usada, o nome de exibição é obrigatório.

   > **Note**
   >
   > Se você estiver logado usando um usuário ou uma função do IAM que tenha somente a política DirectoryServiceFullAccessgerenciada, o nome do tópico deve começar com "DirectoryMonitoring". Caso queira personalizar ainda mais o nome do tópico, precisará de privilégios adicionais no SNS.

8. Escolha Criar.

Se você quiser designar assinantes adicionais do SNS, como um endereço de e-mail adicional, filas do Amazon SQS AWS Lambdaou, você pode fazer isso no console do Amazon SNS.

Para remover as mensagens de status do diretório de um tópico

1. Faça login no AWS Management Console e abra o AWS Directory Service console.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Selecione a guia Manutenção.
4. Na seção Monitoramento de diretórios, selecione um nome de tópico do SNS na lista, escolha Ações e selecione Remover.
5. Escolha Remover.

Isso remove o seu diretório enquanto publicador do tópico do SNS selecionado. Se quiser excluir o tópico inteiro, você pode fazer isso no console do Amazon SNS.

> **Note**
>
> Antes de excluir um tópico do Amazon SNS usando o console do SNS, certifique-se de que o diretório não esteja enviando mensagens de status para aquele tópico.
> Se você excluir um tópico do Amazon SNS usando o console do SNS, essa alteração não será refletida imediatamente no console do Directory Services. Você será notificado somente na próxima vez que um diretório publicar uma notificação para o tópico excluído, quando verá o status atualizado na guia Monitoring do diretório indicando que o tópico não foi encontrado.

Portanto, para evitar a perda de mensagens importantes de status do diretório, antes de excluir qualquer tópico do qual receba mensagens AWS Directory Service, associe seu diretório a um tópico diferente do Amazon SNS.

Associe uma instância do Amazon EC2 ao seu Simple AD Active Directory

Você pode unir facilmente uma instância do Amazon EC2 ao Active Directory seu domínio quando a instância é executada. Para ter mais informações, consulte Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Microsoft AD AWS gerenciado Active Directory. Você também pode iniciar uma instância do EC2 e associá-la a um Active Directory domínio diretamente do AWS Directory Service console com a AWS Systems Manager automação.

Se você precisar associar manualmente uma instância do EC2 ao seu Active Directory domínio, deverá iniciar a instância na região e no grupo de segurança ou sub-rede adequados e, em seguida, unir a instância ao domínio.

Para se conectar de modo remoto a essas instâncias, você deve ter conectividade IP com as instâncias da rede da qual está se conectando. Na maioria dos casos, é necessário que um gateway da Internet esteja conectado à sua VPC e que a instância tenha um endereço IP público.

Tópicos

- Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Simple AD Active Directory
- Associe manualmente uma instância Windows do Amazon EC2 ao seu Simple AD Active Directory
- Associe perfeitamente uma instância Linux do Amazon EC2 ao seu Simple AD Active Directory
- Associe manualmente uma instância Linux do Amazon EC2 ao seu Simple AD Active Directory
- Delegar privilégios de associação a diretório para o Simple AD
- Criar um conjunto de opções de DHCP

Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Simple AD Active Directory

Esse procedimento une perfeitamente uma instância Windows do Amazon EC2 ao seu Simple AD Active Directory.

Para ingressar perfeitamente em uma instância EC2 do Windows

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o mesmo Região da AWS que o diretório existente.
3. No Painel do EC2, na seção Iniciar instância, escolha Iniciar instância.
4. Na página Iniciar uma instância, na seção Nome e tags, insira o nome que você gostaria de usar para sua instância do Windows EC2.
5. (Opcional) Escolha Adicionar tags extras para um ou mais pares chave-valor de tag para organizar, monitorar ou controlar o acesso para esta instância do EC2.
6. Na seção Imagem da aplicação e do sistema operacional (imagem de máquina da Amazon), escolha Windows no painel Início rápido. É possível alterar a imagem de máquina da Amazon (AMI) do Windows na lista suspensa Imagem de máquina da Amazon (AMI).
7. Na seção Tipo de instância, escolha o tipo de instância que você gostaria de usar na lista suspensa Tipo de instância.
8. Na seção Par de chaves: login, é possível optar por criar um novo par de chaves ou escolher um par de chaves existente.

    a. Para criar um novo par de chaves, escolha Criar par de chaves.

    b. Insira um nome para o par de chaves e selecione uma opção para Tipo de par de chaves e Formato do arquivo de chave privada.

    c. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha .pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha .ppk.

    d. Escolha Criar par de chaves.

    e. O arquivo de chave privada é baixado automaticamente pelo navegador. Salve o arquivo de chave privada em um lugar seguro.

    > **Important**
    >
    > Esta é a única chance de você salvar o arquivo de chave privada.

9. Na página Iniciar uma instância, na seção Configurações de rede, escolha Editar. Escolha a VPC na qual seu diretório foi criado na lista suspensa VPC: obrigatório.
10. Escolha uma das sub-redes públicas em sua VPC na lista suspensa Sub-rede. A sub-rede escolhida deve ter todo o tráfego externo ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.

Para obter mais informações sobre como conectar a um gateway da Internet, consulte Conectar à Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.

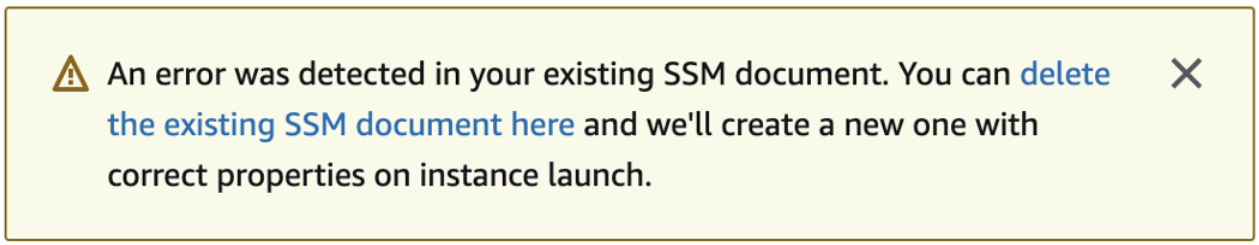
11. Em Atribuir IP público automaticamente, escolha Habilitar.

    Para obter mais informações sobre endereçamento IP público e privado, consulte Endereçamento IP de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.

12. Para configurações de Firewall (grupos de segurança), é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.

13. Para opções de Configurar armazenamento, é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.

14. Selecione a seção Detalhes avançados, escolha seu domínio na lista suspensa Diretório de associação ao domínio.

> **Note**
>
> Depois de escolher o diretório de ingresso no domínio, você poderá ver:
>
> 
>
>
> Esse erro ocorre se o assistente de inicialização do EC2 identificar um documento SSM existente com propriedades inesperadas. Você pode executar uma das seguintes ações:
>
> - Se você editou anteriormente o documento SSM e as propriedades são esperadas, escolha fechar e continue a executar a instância do EC2 sem alterações.
> - Selecione o link excluir o documento SSM existente aqui para excluir o documento SSM. Isso permitirá a criação de um documento SSM com as propriedades corretas. O documento SSM será criado automaticamente quando você iniciar a instância do EC2.

15. Para Perfil de instância do IAM, é possível selecionar um perfil de instância do IAM existente ou criar um novo. Selecione um perfil de instância do IAM que tenha as políticas AWS gerenciadas AmazonSSM ManagedInstanceCore e AmazonSSM DirectoryServiceAccess anexadas a ele na

lista suspensa do perfil da instância do IAM. Para criar um novo, escolha Criar novo link de perfil do IAM e faça o seguinte:

1. Selecione Criar função.
2. Em Selecionar entidade confiável, escolha serviço da AWS .
3. Em Use case (Caso de uso), selecione EC2.
4. Em Adicionar permissões, na lista de políticas, selecione as políticas do AmazonSSM ManagedInstanceCore e do AmazonSSM. DirectoryServiceAccess Para filtrar a lista, digite **`SSM`** na caixa de pesquisa. Escolha Próximo.

   > **Note**
   >
   > O AmazonSSM DirectoryServiceAccess fornece as permissões para unir instâncias a uma Active Directory instância gerenciada por. AWS Directory Service O AmazonSSM ManagedInstanceCore fornece as permissões mínimas necessárias para usar o serviço. AWS Systems Manager Para obter mais informações sobre a criação de um perfil com essas permissões e sobre outras permissões e políticas que você pode atribuir ao seu perfil do IAM, consulte Criar um perfil de instância do IAM para Systems Manager no Guia do usuário do AWS Systems Manager .

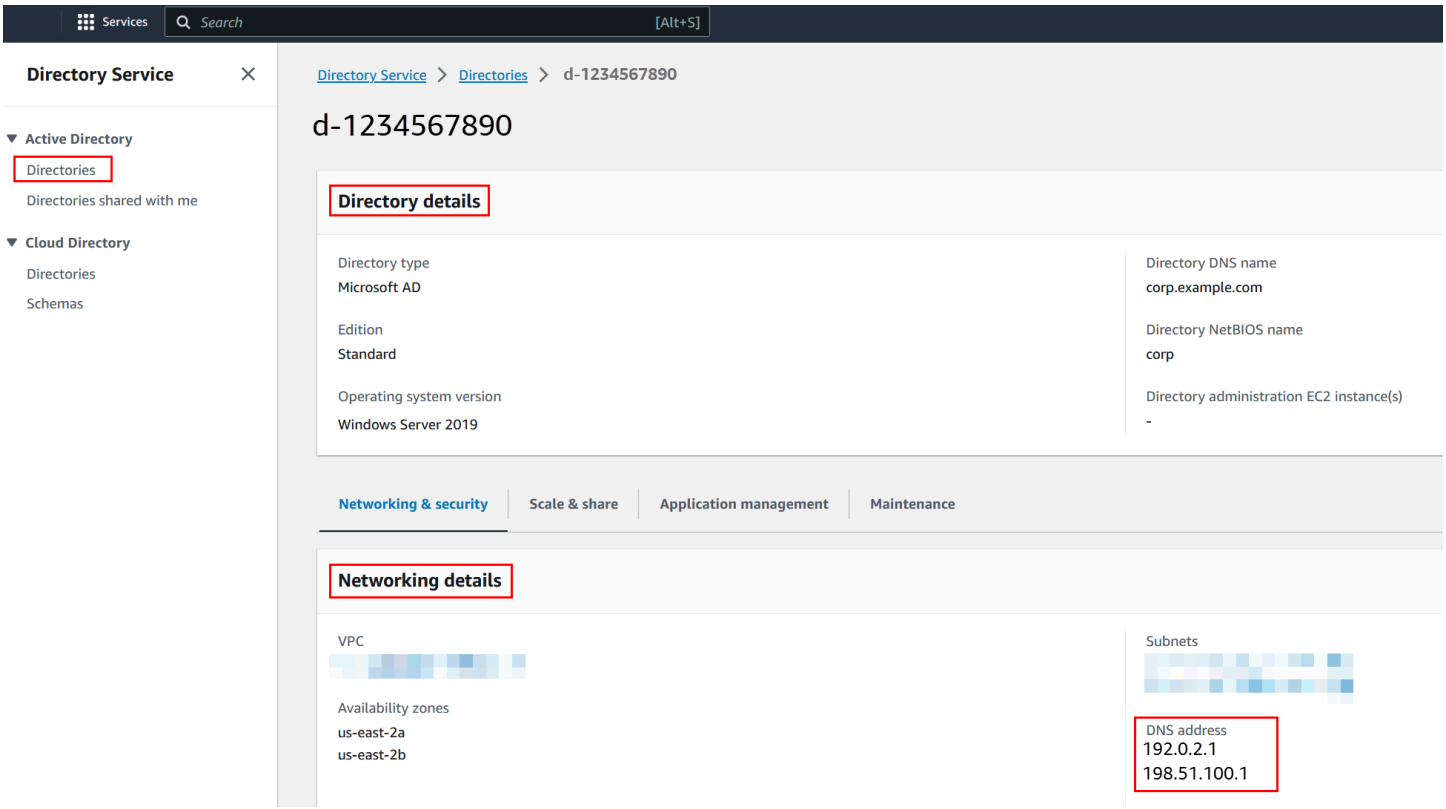
5. Na página Nomear, revisar e criar, insira um Nome de perfil. Você precisará desse nome de perfil para anexar à instância do EC2.
6. (Opcional) Você pode fornecer uma descrição do perfil de instância do IAM no campo Descrição.
7. Selecione Criar função.
8. Volte para a página Iniciar uma instância e escolha o ícone de atualização ao lado do Perfil de instância do IAM. Seu novo perfil de instância do IAM deve estar visível na lista suspensa do Perfil de instância do IAM. Escolha o novo perfil e mantenha o resto das configurações com seus valores padrão.

16. Escolha Iniciar instância.

Associe manualmente uma instância Windows do Amazon EC2 ao seu Simple AD Active Directory

Para unir manualmente uma instância Windows existente do Amazon EC2 a um Simple AD Active Directory, a instância deve ser executada usando os parâmetros especificados em. Associe perfeitamente uma instância Windows do Amazon EC2 ao seu Simple AD Active Directory

Você precisará dos endereços IP dos servidores Simple AD DNS. Essas informações podem ser encontradas em Serviços de diretório > Diretórios > o link ID do diretório do seu diretório > seções Detalhes do diretório e Rede e segurança.



Para unir uma instância do Windows a um Simple AD Active Directory

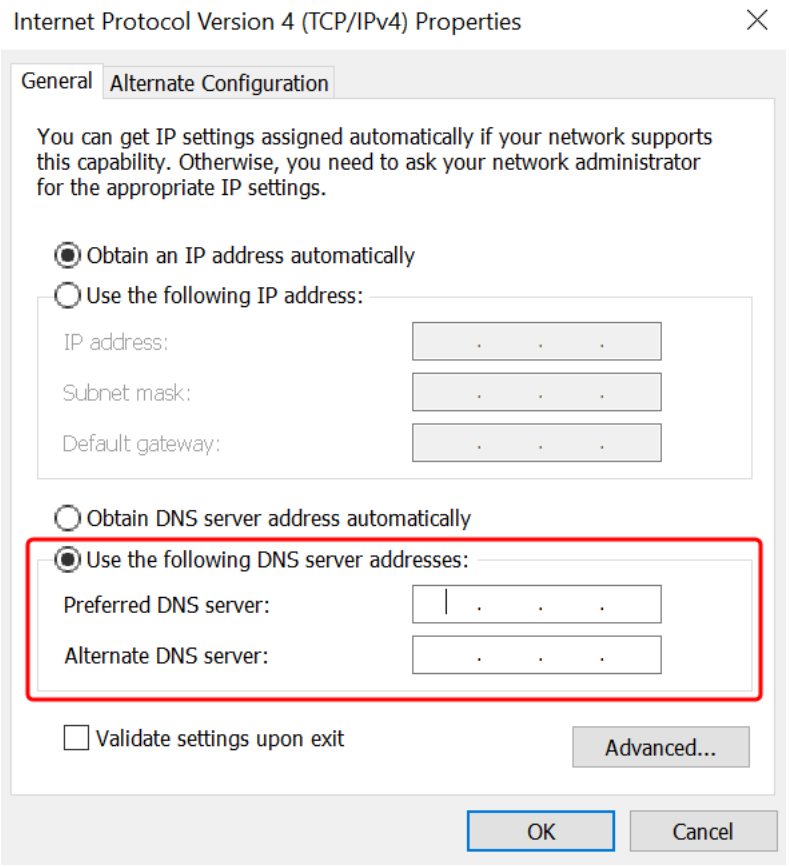
1. Conecte-se à instância usando qualquer cliente Remote Desktop Protocol.
2. Abra a caixa de diálogo de propriedades TCP/IPv4 na instância.
    a. Abra Conexões de rede.

> **Tip**
>
> Você pode abrir Conexões de rede de maneira direta executando o seguinte comando a partir de um prompt de comando na instância.
>
> ```
> %SystemRoot%\system32\control.exe ncpa.cpl
> ```

b. Abra o menu de contexto (clique com o botão direito do mouse) de qualquer conexão de rede habilitada e escolha Propriedades.

c. Na caixa de diálogo de propriedades da conexão, abra (clique duas vezes) Protocolo de Internet versão 4.

3. Selecione Usar os seguintes endereços de servidor DNS, altere os endereços do servidor DNS preferencial e do servidor DNS alternativo para os endereços IP dos seus servidores DNS fornecidos pelo Simple AD e escolha OK.



4. Abra a caixa de diálogo Propriedades do sistema da instância, selecione a guia Nome do computador e escolha Alterar.

> **Tip**
>
> Você pode abrir a caixa de diálogo Propriedades do sistema de maneira direta executando o seguinte comando a partir de um prompt de comando na instância.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. No campo Membro de, selecione Domínio, insira o nome totalmente qualificado do seu Simple AD Active Directory e escolha OK.
6. Quando solicitado a fornecer o nome e a senha do administrador do domínio, insira o nome de usuário e a senha de uma conta que tenha privilégios de ingresso no domínio. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação a diretório para o Simple AD.

   > **Note**
   >
   > Você pode inserir o nome totalmente qualificado do seu domínio ou o nome NetBIOS, seguido por uma barra invertida (\) e, em seguida, o nome de usuário. O nome de usuário seria Administrador. Por exemplo, o **`corp.example.com\administrator`** ou o **`corp\administrator`**.

7. Depois que você receber a mensagem de boas-vindas ao domínio, reinicie a instância para que as alterações entrem em vigor.

Agora que sua instância foi associada ao domínio Simple AD Active Directory, você pode fazer login nessa instância remotamente e instalar utilitários para gerenciar o diretório, como adicionar usuários e grupos. As Ferramentas de Administração do Active Directory podem ser usadas para criar usuários e grupos. Para ter mais informações, consulte Instale as ferramentas de administração do Active Directory para Simple AD.

Associe perfeitamente uma instância Linux do Amazon EC2 ao seu Simple AD Active Directory

Esse procedimento une perfeitamente uma instância Linux do Amazon EC2 ao seu Simple AD Active Directory.

As seguintes distribuições e versões de instância do Linux são suportadas:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> As distribuições anteriores ao Ubuntu 14 e ao Red Hat Enterprise Linux 7 não oferecem suporte ao recurso de associação direta a domínios.

Pré-requisitos

Antes de configurar a união de domínio perfeita em uma instância Linux, você precisa concluir os procedimentos nesta seção.

Selecionar sua conta de serviço para associação direta ao domínio

É possível associar diretamente computadores Linux ao seu domínio do Simple AD. Para fazer isso, é necessário criar uma conta de usuário com permissões de criação de conta de computador para associar os computadores ao domínio. Embora os membros do grupo Administradores de Domínio ou outros grupos possam ter privilégios suficientes para associar computadores ao domínio, não recomendamos fazer isso. Como prática recomendada, sugerimos usar uma conta de serviço que tenha os privilégios mínimos necessários para associar os computadores ao domínio.

Para obter informações sobre como processar e delegar permissões à sua conta de serviço para criar uma conta de computador, consulte Delegar privilégios para sua conta de serviço.

Criar os segredos para armazenar a conta de serviço do domínio

Você pode usar AWS Secrets Manager para armazenar a conta de serviço de domínio.

Para criar segredos e armazenar as informações da conta de serviço do domínio

1. Faça login no AWS Management Console e abra o AWS Secrets Manager console em https://console.aws.amazon.com/secretsmanager/.

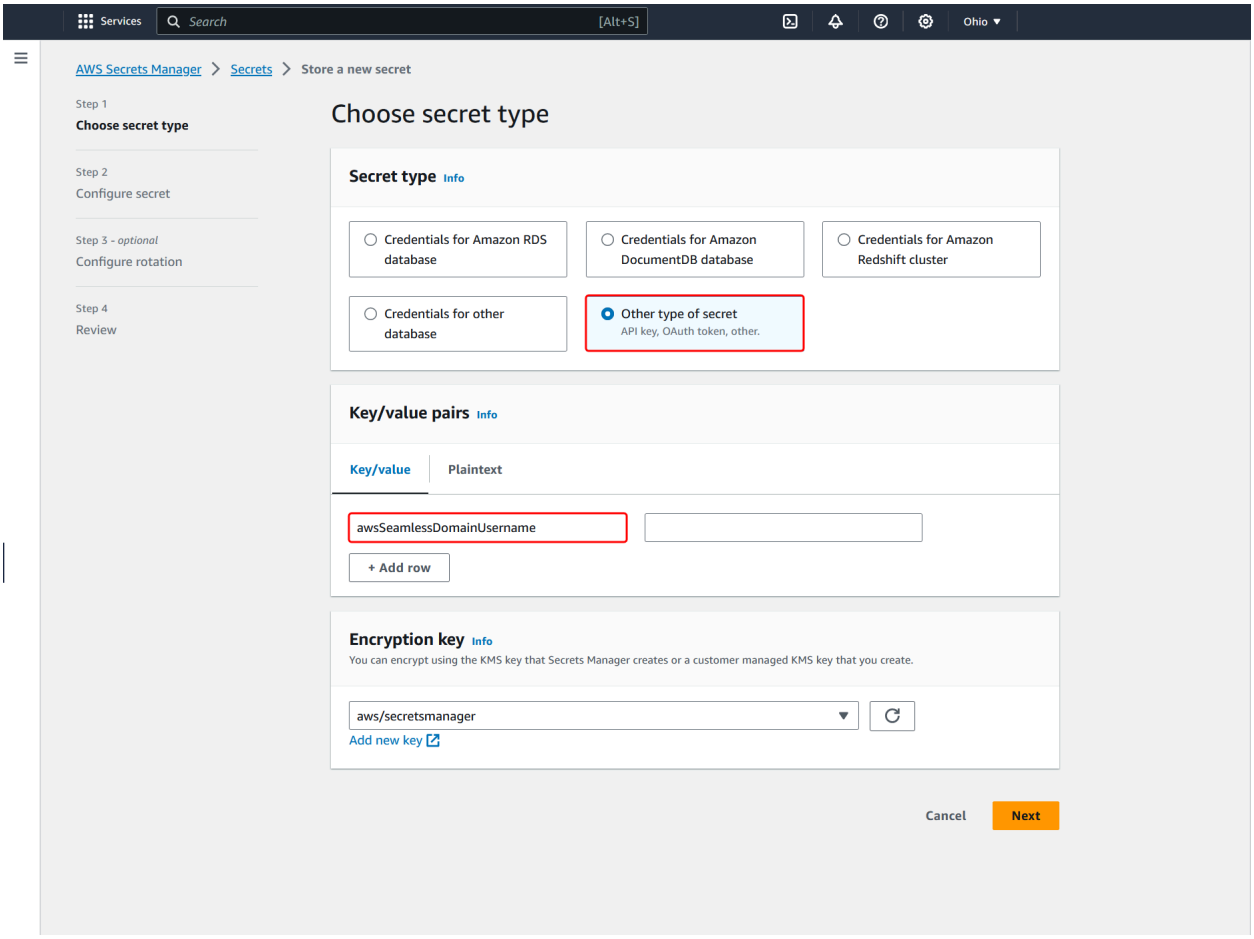
2. Selecione Armazenar um novo segredo.
3. Na página Store a new secret (Armazenar um novo segredo), faça o seguinte:

   a. Em Tipo de segredo, escolha Outro tipo de segredos.

   b. Em Pares de chave/valor, faça o seguinte:

      i. Na primeira caixa, insira **`awsSeamlessDomainUsername`**. Na mesma linha, na próxima caixa, insira o nome de usuário da sua conta de serviço. Por exemplo, se você usou o PowerShell comando anteriormente, o nome da conta de serviço seria**`awsSeamlessDomain`**.

      > **Note**
      >
      > Você deve inserir **`awsSeamlessDomainUsername`** exatamente como está. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.



ii. Escolha Adicionar linha.

iii. Na nova linha, na primeira caixa, insira **`awsSeamlessDomainPassword`**. Na mesma linha, na próxima caixa, insira a senha da sua conta de serviço.

> **Note**
>
> Você deve inserir **`awsSeamlessDomainPassword`** exatamente como está. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.

iv. Em Chave de criptografia, deixe o valor padrão`aws/secretsmanager`. AWS Secrets Manager sempre criptografa o segredo quando você escolhe essa opção. Também é possível escolher uma chave criada por você.

> **Note**
>
> Existem taxas associadas AWS Secrets Manager, dependendo de qual segredo você usa. Para obter a lista de preços atual completa, consulte Definição de preço do AWS Secrets Manager.
> Você pode usar a chave AWS gerenciada `aws/secretsmanager` que o Secrets Manager cria para criptografar seus segredos gratuitamente. Se você criar suas próprias chaves KMS para criptografar seus segredos, AWS cobrará a taxa atual AWS KMS . Para obter mais informações, consulte Preços do AWS Key Management Service.

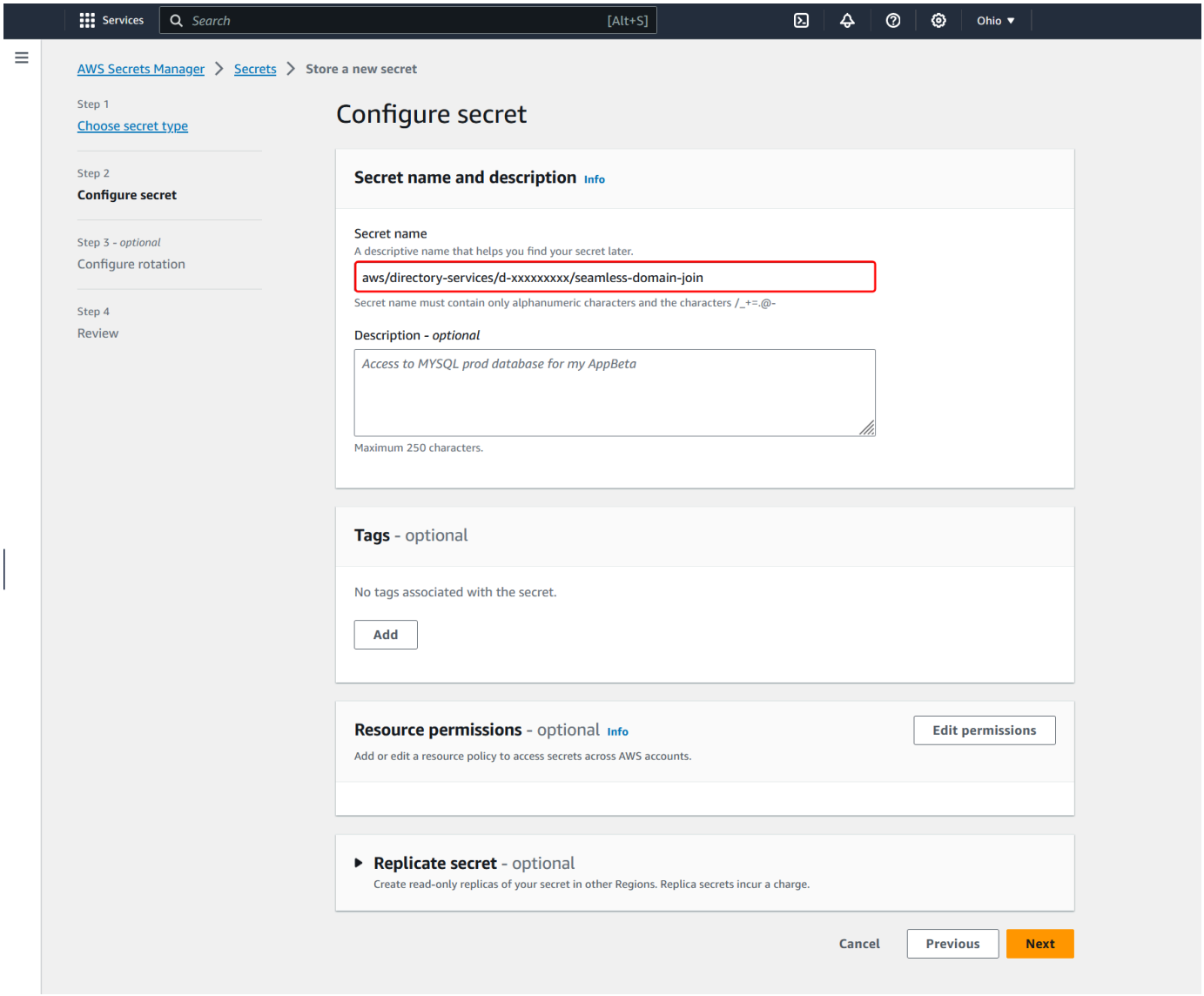
v. Escolha Próximo.

4. Em Nome secreto, insira um nome secreto que inclua sua ID de diretório usando o seguinte formato, substituindo *d-xxxxxxxxx* pela ID do diretório:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Ele será usado para recuperar segredos no aplicativo.

> **Note**
>
> Você deve inserir **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** exatamente como está, mas substituir *d-xxxxxxxxx* pelo ID do diretório. Certifique-se de que não haja espaços iniciais ou finais. Caso contrário, a associação ao domínio falhará.



5. Mantenha todo o resto definido como padrão e, em seguida, escolha Próximo.
6. Em Configurar rotação automática, mantenha a opção Desabilitar rotação automática selecionada e escolha Próximo.

   Você pode ativar a rotação desse segredo depois de armazená-lo.
7. Revise as configurações e escolha Armazenar para salvar as alterações. O console do Secrets Manager leva você de volta para a lista de segredos da sua conta com o novo segredo agora incluído na lista.
8. Escolha seu nome de segredo recém-criado na lista e anote o valor do ARN do segredo. Ele será necessário na próxima seção.

Ativar a rotação para o segredo da conta de serviço de domínio

Recomendamos que você alterne regularmente os segredos para melhorar sua postura de segurança.

Para ativar a rotação do segredo da conta de serviço de domínio

- Siga as instruções em Configurar a rotação automática para AWS Secrets Manager segredos no Guia do AWS Secrets Manager usuário.

  Para a Etapa 5, use o modelo de rotação das credenciais do Microsoft Active Directory no Guia do AWS Secrets Manager Usuário.

  Para obter ajuda, consulte Solucionar problemas AWS Secrets Manager de rotação no Guia do AWS Secrets Manager usuário.

Criar a política e o perfil do IAM necessários

Use as etapas de pré-requisito a seguir para criar uma política personalizada que permita acesso somente de leitura ao seu segredo de junção de domínio contínuo do Secrets Manager (que você criou anteriormente) e para criar uma nova função LinuxEC2 IAM. DomainJoin

Criar a política de leitura do IAM para o Secrets Manager

Você usa o console do IAM para criar uma política que concede acesso somente de leitura ao seu segredo do Secrets Manager.

Para criar a política de leitura do IAM para o Secrets Manager

1. Faça login no AWS Management Console como um usuário que tem permissão para criar políticas do IAM. Em seguida, abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, Gerenciamento de acesso, escolha Políticas.
3. Escolha Criar política.
4. Escolha a guia JSON e copie o texto do documento de política JSON a seguir. Em seguida, cole-o na caixa de texto JSON.

> **Note**
>
> Certifique-se de substituir o ARN da região e do recurso pela região e o ARN reais do segredo que você criou anteriormente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Quando terminar, escolha Próximo. O validador de política indica se há qualquer erro de sintaxe. Para obter mais informações, consulte Validar políticas do IAM.
6. Na página Revisar política, insira um nome de política, como **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Revise a seção Resumo para ver as permissões que são concedidas pela política. Em seguida, selecione Criar política para salvar suas alterações. A nova política aparece na lista de políticas gerenciadas e está pronta para ser anexada a uma identidade.

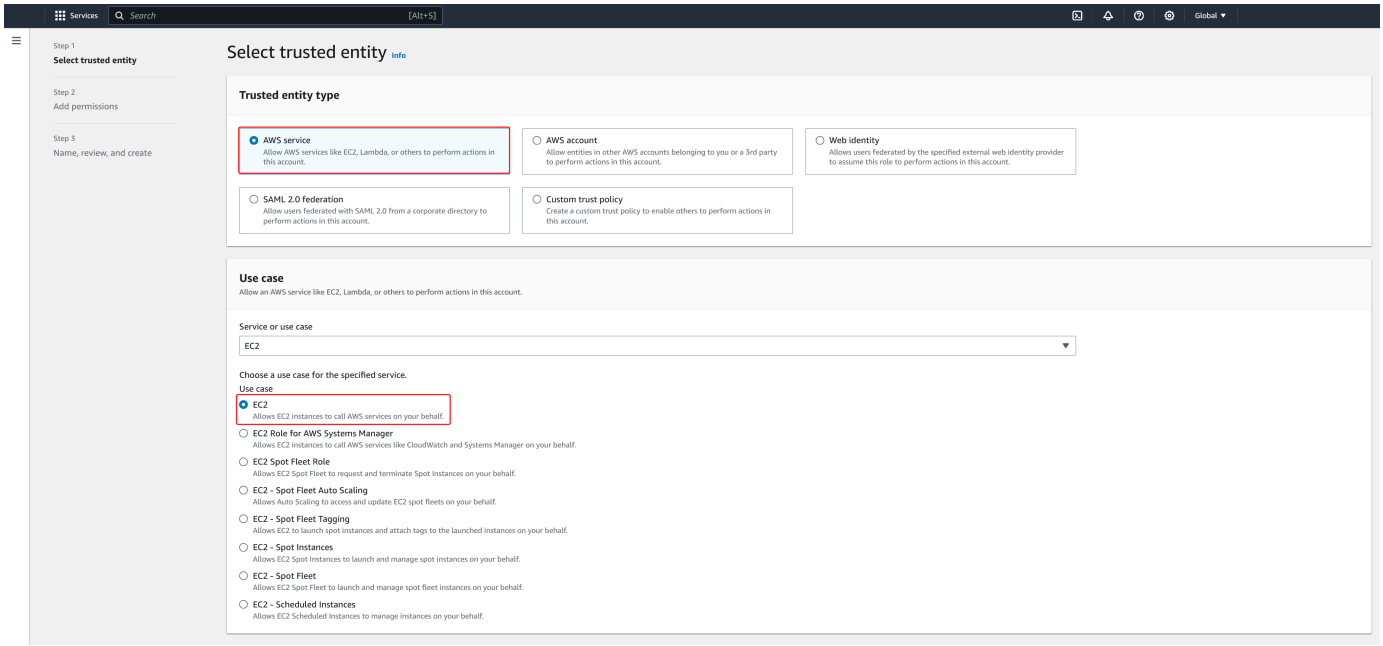
> **Note**
>
> Recomendamos criar uma política por segredo. Isso garante que as instâncias tenham acesso somente ao segredo apropriado e minimiza o impacto em caso de comprometimento de uma instância.

Crie a função LinuxEC2 DomainJoin

Você usa o console do IAM para criar o perfil que usará para associar sua instância do EC2 do Linux ao domínio.

Para criar a função LinuxEC2 DomainJoin

1. Faça login no AWS Management Console como um usuário que tem permissão para criar políticas do IAM. Em seguida, abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, em Gerenciamento de acesso, escolha Perfis.
3. No painel de conteúdo, escolha Criar perfil.
4. Em Select type of trusted entity (Selecionar o tipo de entidade confiável), escolha AWS service (serviço).
5. Em Caso de uso, escolha EC2 e, em seguida, escolha Avançar.



6. Em Políticas de filtro, faça o seguinte:

   a. Insira **`AmazonSSMManagedInstanceCore`**. Em seguida, marque a caixa de seleção para esse item na lista.

   b. Insira **`AmazonSSMDirectoryServiceAccess`**. Em seguida, marque a caixa de seleção para esse item na lista.

   c. Insira **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (ou o nome da política que você criou no procedimento anterior). Em seguida, marque a caixa de seleção para esse item na lista.

d. Depois de adicionar as três políticas listadas acima, selecione Criar função.

> **Note**
>
> O AmazonSSM DirectoryServiceAccess fornece as permissões para unir instâncias a uma Active Directory instância gerenciada por. AWS Directory Service O AmazonSSM ManagedInstanceCore fornece as permissões mínimas necessárias para usar o serviço. AWS Systems Manager Para obter mais informações sobre a criação de um perfil com essas permissões e sobre outras permissões e políticas que você pode atribuir ao seu perfil do IAM, consulte Criar um perfil de instância do IAM para Systems Manager no Guia do usuário do AWS Systems Manager .

7. Insira um nome para sua nova função, como **`LinuxEC2DomainJoin`** ou outro nome de sua preferência no campo Nome da função.
8. (Opcional) Em Role description (Descrição da função), insira uma descrição.
9. (Opcional) Escolha Adicionar nova tag na Etapa 3: Adicionar tags para adicionar tags. Os pares de chave-valor de tag são usados para organizar, rastrear ou controlar o acesso a essa função.
10. Selecione Criar função.

Associe perfeitamente uma instância Linux ao seu Simple AD Active Directory

Agora que você configurou todas as tarefas de pré-requisito, você pode usar o procedimento a seguir para unir perfeitamente sua instância do EC2 Linux.

Para unir perfeitamente sua instância Linux

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No seletor de região na barra de navegação, escolha o mesmo Região da AWS que o diretório existente.
3. No Painel do EC2, na seção Iniciar instância, escolha Iniciar instância.
4. Na página Iniciar uma instância, na seção Nome e tags, insira o nome que você gostaria de usar para sua instância Linux EC2.
5. (Opcional) Escolha Adicionar tags extras para um ou mais pares chave-valor de tag para organizar, monitorar ou controlar o acesso para esta instância do EC2.

6. Na seção Imagem do aplicativo e do sistema operacional (Amazon Machine Image), escolha uma AMI Linux que você deseja iniciar.

> **Note**
>
> A AMI usada deve ter AWS Systems Manager (SSM Agent) versão 2.3.1644.0 ou superior. Para verificar a versão do SSM Agent instalada em sua AMI iniciando uma instância por essa AMI, consulte Obter a versão do SSM Agent instalada. Se você precisar atualizar o SSM Agent, consulte Instalar e configurar o SSM Agent em instâncias do EC2 para Linux.
> O SSM usa o `aws:domainJoin` plug-in ao unir uma instância Linux a um Active Directory domínio. *`O plug-in altera o nome do host das instâncias Linux para o formato EC2AMAZ- XXXXXXX.`* Para obter mais informações sobre`aws:domainJoin`, consulte a referência do plug-in do documento de AWS Systems Manager comando no Guia AWS Systems Manager do usuário.

7. Na seção Tipo de instância, escolha o tipo de instância que você gostaria de usar na lista suspensa Tipo de instância.
8. Na seção Par de chaves: login, é possível optar por criar um novo par de chaves ou escolher um par de chaves existente. Para criar um novo par de chaves, escolha Criar par de chaves. Insira um nome para o par de chaves e selecione uma opção para Tipo de par de chaves e Formato do arquivo de chave privada. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha .pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha .ppk. Escolha Criar par de chaves. O arquivo de chave privada é baixado automaticamente pelo navegador. Salve o arquivo de chave privada em um lugar seguro.

> **Important**
>
> Esta é a única chance de você salvar o arquivo de chave privada.

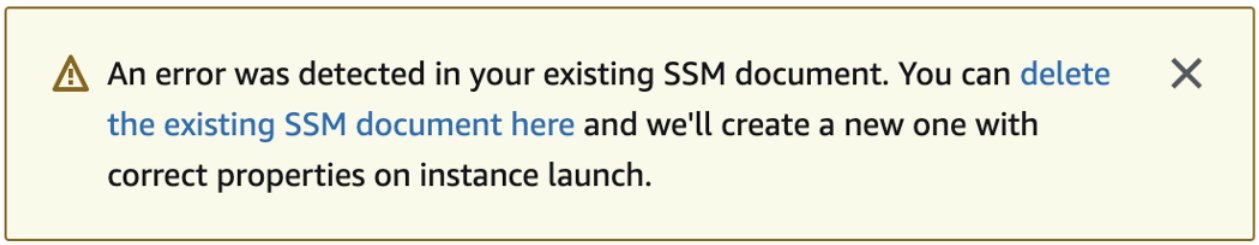
9. Na página Iniciar uma instância, na seção Configurações de rede, escolha Editar. Escolha a VPC na qual seu diretório foi criado na lista suspensa VPC: obrigatório.
10. Escolha uma das sub-redes públicas em sua VPC na lista suspensa Sub-rede. A sub-rede escolhida deve ter todo o tráfego externo ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.

Para obter mais informações sobre como conectar a um gateway da Internet, consulte Conectar à Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.

11. Em Atribuir IP público automaticamente, escolha Habilitar.

    Para obter mais informações sobre endereçamento IP público e privado, consulte Endereçamento IP de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.

12. Para configurações de Firewall (grupos de segurança), é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
13. Para opções de Configurar armazenamento, é possível usar as configurações padrão ou fazer alterações para atender às suas necessidades.
14. Selecione a seção Detalhes avançados, escolha seu domínio na lista suspensa Diretório de associação ao domínio.

> **Note**
>
> Depois de escolher o diretório de ingresso no domínio, você poderá ver:
>
> 
>
>
> Esse erro ocorre se o assistente de inicialização do EC2 identificar um documento SSM existente com propriedades inesperadas. Você pode executar uma das seguintes ações:
>
> - Se você editou anteriormente o documento SSM e as propriedades são esperadas, escolha fechar e continue a executar a instância do EC2 sem alterações.
> - Selecione o link excluir o documento SSM existente aqui para excluir o documento SSM. Isso permitirá a criação de um documento SSM com as propriedades corretas. O documento SSM será criado automaticamente quando você iniciar a instância do EC2.

15. Para o perfil da instância do IAM, escolha a função do IAM que você criou anteriormente na seção de pré-requisitos Etapa 2: Criar a função LinuxEC2. DomainJoin
16. Escolha Iniciar instância.

> **Note**
>
> Se você estiver realizando uma associação direta a domínio com o SUSE Linux, uma reinicialização será necessária antes que as autenticações funcionem. Para reinicializar o SUSE via terminal Linux, digite sudo reboot.

Associe manualmente uma instância Linux do Amazon EC2 ao seu Simple AD Active Directory

Além das instâncias Windows do Amazon EC2, você também pode unir determinadas instâncias Linux do Amazon EC2 ao seu Simple AD Active Directory. As seguintes distribuições e versões de instância do Linux são suportadas:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI do Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Outras distribuições e versões do Linux podem funcionar, mas não foram testadas.

Pré-requisitos

Antes de associar uma instância do Amazon Linux, CentOS, Red Hat ou Ubuntu ao seu diretório, a instância deve primeiro ser iniciada conforme especificado em Associe perfeitamente uma instância Linux do Amazon EC2 ao seu Simple AD Active Directory.

> **Important**
>
> Alguns dos procedimentos a seguir, se não forem executados corretamente, podem tornar sua instância inacessível ou não utilizável. Portanto, nós sugerimos enfaticamente

que você faça um backup ou tire um snapshot da sua instância antes de executar esses procedimentos.

Para associar uma instância do Linux ao seu diretório

Siga as etapas para a sua instância do Linux específica usando uma das seguintes guias:

Amazon Linux

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Verifique se sua instância do Amazon Linux de 64 bits está atualizada.

```
sudo yum -y update
```

4. Instale os pacotes do Amazon Linux necessários em sua instância do Linux.

> **Note**
>
> Alguns desses pacotes já podem estar instalados.
> Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração.
> Você geralmente pode deixar os campos nessas telas em branco.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Para obter ajuda para determinar a versão do Amazon Linux que você está usando, consulte Como identificar imagens do Amazon Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

5. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Uma conta no domínio *example.com* com privilégios de associação a domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

6. Ajuste o serviço SSH para permitir autenticação de senha.
   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

   b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

   c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

7. Após a instância reiniciar, conecte-a com qualquer cliente SSH e adicione o grupo de administradores de domínio à lista de sudoers executando as seguintes etapas:

   a. Abra o arquivo `sudoers` com o seguinte comando:

   ```
   sudo visudo
   ```

   b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

CentOS

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Verifique se sua instância do CentOS 7 está atualizada.

   ```
   sudo yum -y update
   ```

4. Instale os pacotes do CentOS 7 necessários na sua instância do Linux.

   > **Note**
   >
   > Alguns desses pacotes já podem estar instalados.

Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração. Você geralmente pode deixar os campos nessas telas em branco.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Uma conta no domínio *example.com* com privilégios de associação a domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

6. Ajuste o serviço SSH para permitir autenticação de senha.
   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

   b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

   c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

7. Após a instância reiniciar, conecte-a com qualquer cliente SSH e adicione o grupo de administradores de domínio à lista de sudoers executando as seguintes etapas:

   a. Abra o arquivo `sudoers` com o seguinte comando:

   ```
   sudo visudo
   ```

   b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

Red hat

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Certifique-se de que a instância do Red Hat - 64 bits está atualizada.

   ```
   sudo yum -y update
   ```

4. Instale os pacotes do Red Hat necessários na sua instância do Linux.

   > **Note**
   >
   > Alguns desses pacotes já podem estar instalados.

Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração. Você geralmente pode deixar os campos nessas telas em branco.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

O SaM AccountName para uma conta no domínio *example.com* que tem privilégios de associação de domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

6. Ajuste o serviço SSH para permitir autenticação de senha.
   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

   b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

   c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

7. Após a instância reiniciar, conecte-a com qualquer cliente SSH e adicione o grupo de administradores de domínio à lista de sudoers executando as seguintes etapas:

   a. Abra o arquivo `sudoers` com o seguinte comando:

   ```
   sudo visudo
   ```

   b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

Ubuntu

1. Conecte-se à instância usando qualquer cliente SSH.
2. Configure a instância Linux para usar os endereços IP do servidor DNS dos AWS Directory Service servidores DNS fornecidos. Você pode fazer isso configurando-o nas opções de DHCP conectadas à VPC ou configurando-o manualmente na instância. Se desejar defini-lo manualmente, consulte Como faço para atribuir um servidor DNS estático a uma instância privada do Amazon EC2 no Centro de Conhecimentos da AWS para obter orientação sobre a definição do servidor de DNS persistente para sua distribuição e versão específicas do Linux.
3. Certifique-se de que a instância do Ubuntu - 64 bits está atualizada.

   ```
   sudo apt-get update
   sudo apt-get -y upgrade
   ```

4. Instale os pacotes do Ubuntu necessários na sua instância do Linux.

   > **Note**
   >
   > Alguns desses pacotes já podem estar instalados.

Enquanto você instala os pacotes, você pode ver várias telas pop-up de configuração. Você geralmente pode deixar os campos nessas telas em branco.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Desabilite a resolução de DNS reverso e defina o realm padrão para o FQDN do domínio. Instâncias do Ubuntu devem ser capazes de fazer a resolução inversa no DNS para que um realm possa funcionar. Caso contrário, você precisa desabilitar DNS reverso no /etc/krb5.conf, como a seguir:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Junte a instância ao diretório com o comando a seguir.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

O SaM AccountName para uma conta no domínio *example.com* que tem privilégios de associação de domínio. Digite a senha da conta quando solicitado. Para obter mais informações sobre como delegar esses privilégios, consulte Delegar privilégios de associação ao diretório do AWS Managed Microsoft AD.

example.com

O nome de DNS totalmente qualificado do seu diretório.

```
...
 * Successfully enrolled machine in realm
```

7. Ajuste o serviço SSH para permitir autenticação de senha.

   a. Abra o arquivo `/etc/ssh/sshd_config` em um editor de textos.

```
sudo vi /etc/ssh/sshd_config
```

b. Defina a configuração `PasswordAuthentication` como `yes`.

```
PasswordAuthentication yes
```

c. Reinicie o serviço SSH.

```
sudo systemctl restart sshd.service
```

Alternativa:

```
sudo service sshd restart
```

8. Após a instância reiniciar, conecte-a com qualquer cliente SSH e adicione o grupo de administradores de domínio à lista de sudoers executando as seguintes etapas:

a. Abra o arquivo `sudoers` com o seguinte comando:

```
sudo visudo
```

b. Adicione o seguinte ao final do arquivo `sudoers` e salve-o.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(O exemplo acima usa "\<space>" para criar o caractere de espaço do Linux.)

> **Note**
>
> Ao usar o Simple AD, se você criar uma conta de usuário em uma instância do Linux com a opção "Forçar usuário a alterar a senha no primeiro login", esse usuário não poderá alterar inicialmente sua senha usando o comando kpasswd. Para alterar a senha pela primeira vez, um administrador de domínio deverá atualizar a senha de usuário usando as ferramentas de gerenciamento do Active Directory.

Gerenciar contas de uma instância do Linux

Para gerenciar contas no Simple AD de uma instância do Linux, você deve atualizar arquivos de configuração específicos na sua instância do Linux da seguinte maneira:

1. Defina krb5_use_kdcinfo como False (Falso) no arquivo /etc/sssd/sssd.conf. Por exemplo: .

   ```
   [domain/example.com]
       krb5_use_kdcinfo = False
   ```

2. Para que a configuração seja aplicada, você precisa reiniciar o serviço sssd:

   ```
   $ sudo systemctl restart sssd.service
   ```

   Você também poderia usar o:

   ```
   $ sudo service sssd start
   ```

3. Se você pretende gerenciar usuários de uma instância do CentOS Linux, também deverá editar o arquivo /etc/smb.conf para incluir:

   ```
   [global]
     workgroup = EXAMPLE.COM
     realm = EXAMPLE.COM
     netbios name = EXAMPLE
     security = ads
   ```

Restringir o acesso de login da conta

Como todas as contas estão definidas no Active Directory, por padrão, todos os usuários no diretório podem fazer login na instância. Você pode permitir que somente usuários específicos façam login na instância com ad_access_filter em sssd.conf. Por exemplo: .

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica que os usuários só podem ter acesso à instância se participarem de um grupo específico.

cn

O nome comum do grupo que deve ter acesso. Neste exemplo, o nome do grupo é *admins*.

ou

Essa é a unidade organizacional na qual o grupo acima está localizado. Neste exemplo, a UO é *Testou*.

dc

Este é o componente de domínio do seu domínio. Neste exemplo, *example*.

dc

Este é um componente adicional de domínio. Neste exemplo, *com*.

Você deve adicionar manualmente ad_access_filter ao /etc/sssd/sssd.conf.

Abra o arquivo /etc/sssd/sssd.conf em um editor de textos.

```
sudo vi /etc/sssd/sssd.conf
```

Depois disso, seu sssd.conf pode ficar da seguinte forma:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Para que a configuração entre em vigor, é necessário reiniciar o serviço sssd:

```
sudo systemctl restart sssd.service
```

Você também poderia usar o:

```
sudo service sssd restart
```

Mapeamento de ID

O mapeamento de ID pode ser realizado por dois métodos para manter uma experiência unificada entre as identidades Unix/Linux User Identifier (UID) e Group Identifier (GID) e Windows e Active Directory Security Identifier (SID).

1. Centralizado
2. Distribuído

> **Note**
>
> O mapeamento centralizado da identidade do usuário Active Directory requer uma interface de sistema operacional portátil ou POSIX.

Mapeamento centralizado da identidade do usuário

Active Directoryou outro serviço do Lightweight Directory Access Protocol (LDAP) fornece UID e GID aos usuários do Linux. EmActive Directory, esses identificadores são armazenados nos atributos dos usuários:

- UID - O nome de usuário do Linux (String)
- Número UID - O número de ID do usuário Linux (inteiro)
- Número GID - O número de ID do grupo Linux (inteiro)

Para configurar uma instância Linux para usar o UID e o GID deActive Directory, defina `ldap_id_mapping = False` no arquivo sssd.conf. Antes de definir esse valor, verifique se você adicionou um UID, um número UID e um número GID aos usuários e grupos em. Active Directory

Mapeamento distribuído de identidade de usuário

Se Active Directory não tiver a extensão POSIX ou se você optar por não gerenciar centralmente o mapeamento de identidade, o Linux poderá calcular os valores de UID e GID. O Linux usa o Identificador de Segurança (SID) exclusivo do usuário para manter a consistência.

Para configurar o mapeamento distribuído de ID de usuário, defina `ldap_id_mapping = True` no arquivo sssd.conf.

Conecte-se à instância Linux

Quando um usuário se conectar à instância usando um cliente SSH, será solicitado seu nome de usuário. O usuário pode informar o nome de usuário no formato `username@example.com` ou `EXAMPLE\username`. A resposta será semelhante à seguinte, dependendo da distribuição Linux que você estiver usando:

Amazon Linux, Red Hat Enterprise Linux e CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
```

```
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Delegar privilégios de associação a diretório para o Simple AD

Para fazer com que um computador passe a integrar seu diretório, você precisa de uma conta com privilégios para integrar computadores ao diretório.

Com o Simple AD os membros do grupo Administradores de Domínio têm privilégios suficientes para associar computadores ao diretório.

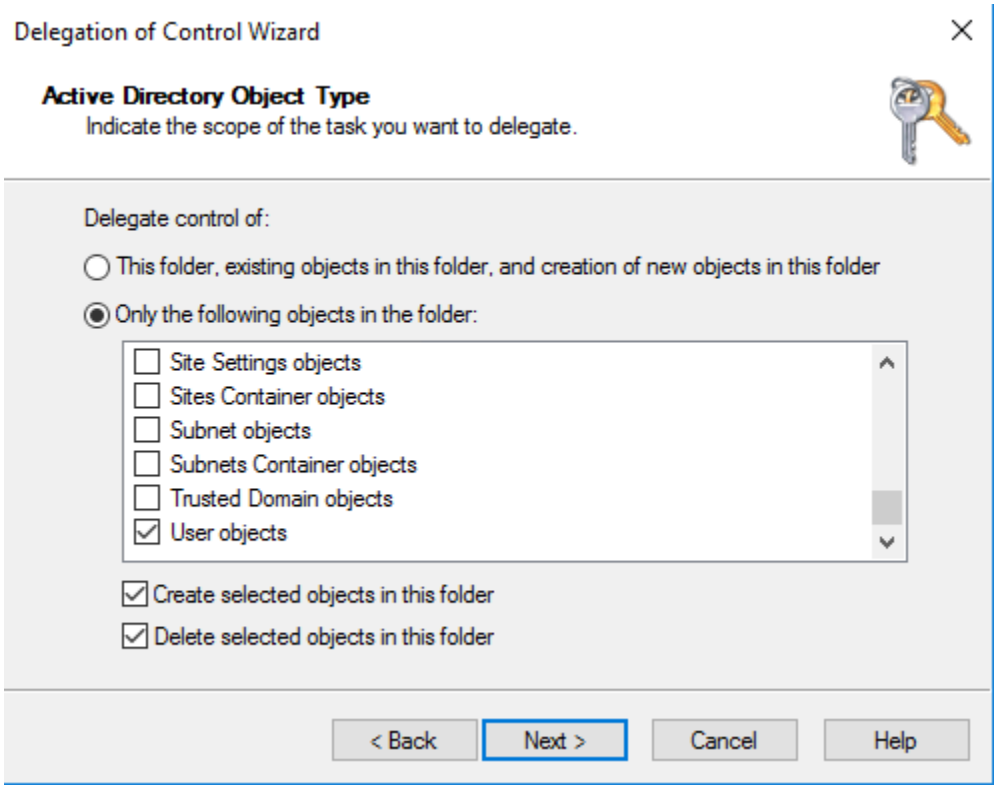
No entanto, a prática recomendada é que você deve usar uma conta que tenha apenas os privilégios mínimos necessários. O procedimento a seguir demonstra como criar um novo grupo chamado `Joiners` e delegar a ele os privilégios necessários para integrar computadores ao diretório.

Execute este procedimento em um computador que esteja integrado ao seu diretório e possua o snap-in do MMC Usuário e Computadores do Active Directory) instalado. Você também deve estar conectado como administrador de domínio.

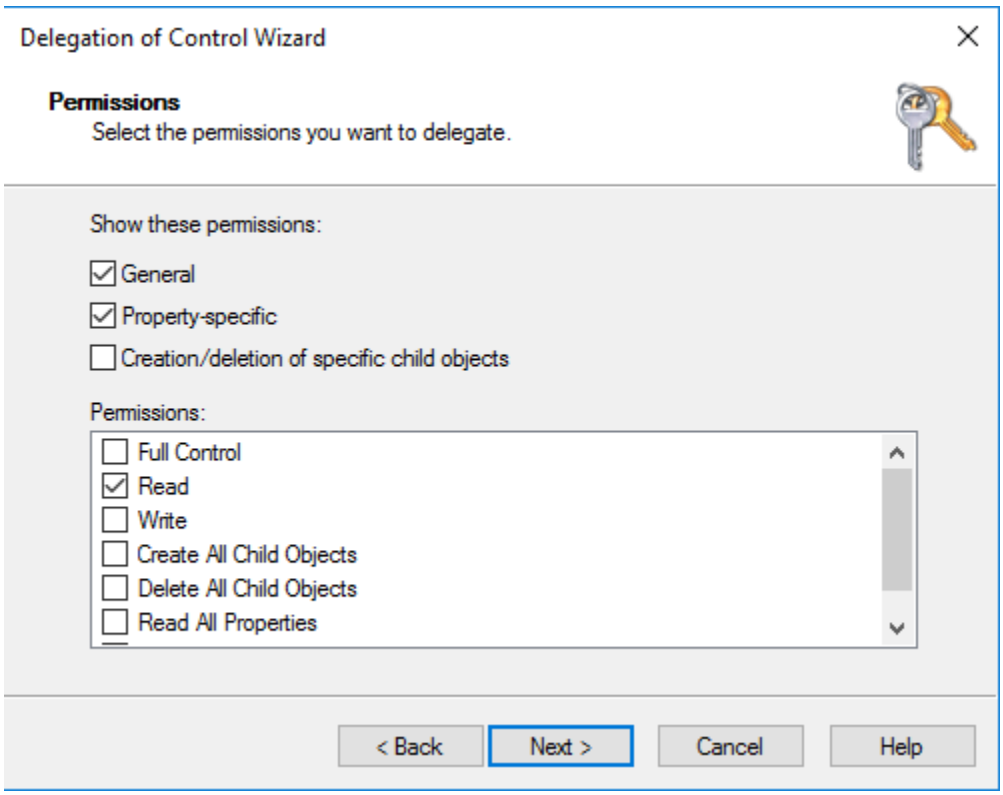
Para delegar privilégios de associação para o Simple AD

1. Abra Active Directory User and Computers (Usuário e computadores do Active Directory) e selecione a raiz do domínio na árvore de navegação.
2. Na árvore de navegação à esquerda, abra o menu de contexto (clique com o botão direito do mouse) em Users (Usuários), selecione New (Novo) e selecione Group (Grupo).
3. Na caixa New Object - Group, digite o seguinte, e escolha OK.
   - Em Group name (Nome do grupo), digite **`Joiners`**.
   - Em Group scope, escolha Global.
   - Em Group type, escolha Security.
4. Na árvore de navegação, selecione a raiz do seu domínio. No menu Action, escolha Delegate Control.
5. Na página Delegation of Control Wizard, escolha Next e escolha Add.

6. Na caixa Select Users, Computers, or Groups (Selecionar usuários, computadores ou grupos), digite `Joiners` e escolha OK. Se mais de um objeto for encontrado, selecione o grupo `Joiners` criado acima. Escolha Próximo.
7. Na página Tasks to Delegate, selecione Create a custom task to delegate e escolha Next.
8. Selecione Only the following objects in the folder e selecione Computer objects.
9. Selecione Create selected objects in this folder e Delete selected objects in this folder. Em seguida, escolha Próximo.



10. Selecione Read e Write e escolha Next.



11. Verifique as informações da página Completing the Delegation of Control Wizard e escolha Finish.
12. Crie um usuário com uma senha forte e adicione-o ao grupo `Joiners`. O usuário então terá privilégios suficientes para se conectar AWS Directory Service ao diretório.

Criar um conjunto de opções de DHCP

AWS recomenda que você crie um conjunto de opções de DHCP para seu AWS Directory Service diretório e atribua o conjunto de opções de DHCP à VPC em que seu diretório está. Dessa maneira, todas as instâncias nessa VPC podem apontar para o domínio especificado e os servidores DNS para resolver seus nomes de domínio.

Para obter mais informações sobre os conjuntos de opções de DHCP, consulte Conjuntos de opções de DHCP no Guia do usuário do Amazon VPC.

Para criar um conjunto de opções de DHCP para o seu diretório

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Conjuntos de opções DHCP e, então, selecione Criar conjuntos de opções DHCP.

3. Na página Criar conjunto de opções de DHCP, forneça os seguintes valores para o seu diretório:

   Nome

   Um tag opcional para o conjunto de opções.

   Domain name

   O nome totalmente qualificado do diretório, como `corp.example.com`.

   Servidores de nomes de domínio

   Os endereços IP dos AWS servidores DNS do seu diretório fornecido.

   > **Note**
   >
   > Para encontrar esses endereços, vá para o painel de navegação do console do AWS Directory Service, selecione Diretórios e escolha o ID do diretório correto.

   Servidores NTP

   Deixe esse campo em branco.

   Servidores de nomes NetBIOS

   Deixe esse campo em branco.

   Tipo de nó NetBIOS

   Deixe esse campo em branco.

4. Escolha Create DHCP Options set. O novo conjunto de opções DHCP aparece na sua lista de opções DHCP.
5. Anote o ID do novo conjunto de opções DHCP (dopt-*xxxxxxxx*). Você precisará usá-lo para associar o novo conjunto de opções à sua VPC.

Para alterar o conjunto de opções DHCP associado a uma VPC

Depois de criar um conjunto de opções DHCP, você não pode modificá-las. Se você quiser que sua VPC use um conjunto diferente de opções DHCP, será necessário criar um novo conjunto e associá-lo a sua VPC. Você também pode configurar sua VPC para não usar nenhuma opção DHCP.

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione a VPC e, em seguida, escolha Ações, Editar configurações de VPC.
4. Em Conjunto de opções DHCP, selecione um conjunto de opções ou escolha Nenhum conjunto de opções de DHCP e escolha Salvar.

Para alterar o conjunto de opções de DHCP associado a uma VPC usando a linha de comando, consulte o seguinte:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Manter seu diretório do Simple AD

Esta seção descreve como manter tarefas administrativas comuns para o seu ambiente do Simple AD.

Tópicos

- Excluir seu Simple AD
- Criar um snapshot ou restaurar seu diretório
- Visualizar informações do diretório

Excluir seu Simple AD

Quando um Simple AD é excluído, todos os dados e instantâneos do diretório são excluídos e não podem ser recuperados. Após a exclusão do diretório, todas as instâncias agregadas ao diretório permanecem intactas. No entanto, você não pode usar as credenciais do diretório para fazer login nessas instâncias. Em tais instâncias, você deve fazer login com uma conta de usuário local para a instância.

Como excluir um diretório

1. No painel de navegação do console do AWS Directory Service selecione Diretórios. Certifique-se de que você está no Região da AWS local onde o seu Active Directory está implantado. Para obter mais informações, consulte Escolha de uma região.

2. Certifique-se de que nenhum AWS aplicativo esteja habilitado para o diretório que você pretende excluir. AWS Os aplicativos habilitados impedirão que você exclua seu AWS Managed Microsoft AD ou Simple AD.

   a. Na página Directories (Diretórios), escolha o ID do diretório.

   b. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos). Na seção AWS aplicativos e serviços, você vê quais AWS aplicativos estão habilitados para o seu diretório.

      - Desative AWS Management Console o acesso. Para ter mais informações, consulte Desabilitar o acesso ao AWS Management Console.
      - Para desativar a Amazon WorkSpaces, você deve cancelar o registro do serviço no diretório no WorkSpaces console. Para obter mais informações, consulte Cancelamento do registro de um diretório no Amazon WorkSpaces Administration Guide.
      - Para desativar a Amazon WorkDocs, você deve excluir o WorkDocs site da Amazon no WorkDocs console da Amazon. Para obter mais informações, consulte Excluir um site no Guia de WorkDocs Administração da Amazon.
      - Para desativar a Amazon WorkMail, você deve remover a WorkMail organização da Amazon no WorkMail console da Amazon. Para obter mais informações, consulte Remover uma organização no Amazon WorkMail Administrator Guide.
      - Para desabilitar o Amazon FSx para Windows File Server, é necessário remover o sistema de arquivos Amazon FSx do domínio. Para obter mais informações, consulte Trabalhando com Active Directory o FSx for Windows File Server no Guia do usuário do Amazon FSx for Windows File Server.
      - Para desabilitar o Amazon Relational Database Service, é necessário remover a instância do Amazon RDS do domínio. Para obter mais informações, consulte Gerenciar uma instância de banco de dados em um domínio no Guia do usuário do Amazon RDS.
      - Para desativar o AWS Client VPN serviço, você deve remover o serviço de diretório do Client VPN Endpoint. Para obter mais informações, consulte Active DirectoryAutenticação no Guia AWS Client VPN do Administrador.
      - Para desabilitar o Amazon Connect, exclua a instância do Amazon Connect. Para obter mais informações, consulte Excluir uma instância do Amazon Connect no Guia de administração do Amazon Connect.

- Para desativar a Amazon QuickSight, você deve cancelar a assinatura da Amazon QuickSight. Para obter mais informações, consulte Fechar sua Amazon QuickSight conta no Guia QuickSight do usuário da Amazon.

> **Note**
>
> Se você o estiver usando AWS IAM Identity Center e já o tiver conectado ao diretório AWS gerenciado do Microsoft AD que planeja excluir, primeiro altere a fonte de identidade antes de excluí-la. Para obter mais informações, consulte Alterar sua fonte de identidade no Guia do usuário do Centro de Identidade do IAM.

3. No painel de navegação, selecionar Diretórios.
4. Selecione somente o diretório a ser excluído e clique em Excluir. A exclusão do diretório demora vários minutos. Quando o diretório for excluído, ele será removido da sua lista de diretórios.

Criar um snapshot ou restaurar seu diretório

AWS Directory Service fornece a capacidade de tirar instantâneos manuais dos dados para seu diretório Simple AD. Esses instantâneos podem ser usados para realizar uma point-in-time restauração em seu diretório. Não é possível criar snapshots de diretórios do AD Connector.

Tópicos

- Criar um snapshot do diretório
- Restaurar o diretório de um snapshot
- Excluir um snapshot

Criar um snapshot do diretório

Um snapshot pode ser usado para restaurar o diretório para o que ele era no momento em que o snapshot foi criado. Para criar um snapshot manual de seu diretório, execute as seguintes etapas.

> **Note**
>
> Há um limite de 5 snapshots manuais para cada diretório. Se já tiver atingido esse limite, deverá excluir um dos snapshots manuais existentes para poder criar outros.

Para criar um snapshot manual

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Maintenance (Manutenção).
4. Na seção Snapshots, escolha Ações e, em seguida, selecione Criar snapshot.
5. Na caixa de diálogo Criar snapshot do diretório, forneça uma descrição do snapshot, se desejado. Quando estiver pronto, escolha Criar.

Dependendo do tamanho do diretório, vários minutos podem ser necessários para que o snapshot seja criado. Quando o snapshot estiver pronto, o valor do Status é alterado para `Completed`.

Restaurar o diretório de um snapshot

Restaurar um diretório a partir de um snapshot é equivalente a mover o diretório de volta no tempo. Cada snapshot de diretório é exclusivo do diretório do qual ele foi criado. Um snapshot só pode ser restaurado para o diretório do qual ele foi criado. Além disso, a idade máxima aceita para um snapshot manual é 180 dias. Para obter mais informações, consulte Prazo de validade útil de um backup de estado do sistema do Active Directory no site da Microsoft.

> **Warning**
>
> Recomendamos entrar em contato com o AWS Support Center antes de qualquer restauração de snapshot; talvez possamos ajudar a evitar a necessidade de fazer uma restauração de snapshot. Todas as restaurações de um snapshot podem causar perda de dados, pois elas são de um momento em específico. É importante compreender que todos os servidores de DCs e DNS associados ao diretório ficarão offline até que a operação de restauração seja concluída.

Para restaurar o diretório a partir de um snapshot, execute as seguintes etapas.

Para restaurar um diretório a partir de um snapshot

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Maintenance (Manutenção).

4. Na seção Snapshots, selecione um snapshot na lista, escolha Ações e, em seguida, selecione Restaurar snapshot.
5. Analise as informações na caixa de diálogo Restaurar snapsho de diretório e escolha Restaurar.

Em um diretório do Simple AD, vários minutos poderão ser necessários para que o diretório seja restaurado. Quando a restauração for concluída com êxito, o valor de Status do diretório será alterado para `Active`. Todas as alterações feitas no diretório depois da data do snapshot serão sobrescritas.

Excluir um snapshot

Para excluir um snapshot

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Maintenance (Manutenção).
4. Na seção Snapshots, escolha Ações e, em seguida, selecione Excluir snapshot.
5. Verifique se você deseja excluir o snapshot e escolha Excluir.

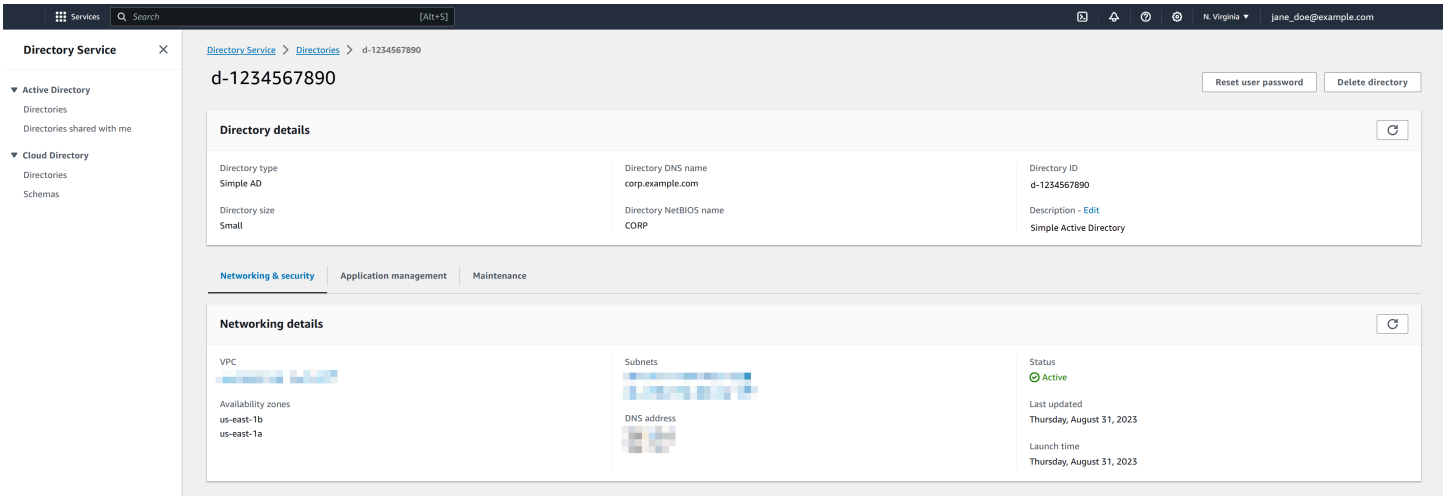
Visualizar informações do diretório

É possível visualizar informações detalhadas sobre um diretório.

Para visualizar informações detalhadas do diretório

1. No painel de navegação do AWS Directory Service console, em Active Directory, selecione Diretórios.
2. Clique no link de ID de seu diretório. As informações sobre o diretório são exibidas na página Detalhes do diretório.

Para obter mais informações sobre o campo Status, consulte Noções básicas sobre o status do diretório.



Permita o acesso a AWS aplicativos e serviços

Os usuários podem autorizar o Simple AD a fornecer a AWS aplicativos e serviços, como a Amazon WorkSpaces, acesso ao seuActive Directory. Os AWS aplicativos e serviços a seguir podem ser ativados ou desativados para funcionar com o Simple AD.

AWS aplicativo/serviço	Mais informações...
Amazon Chime	Para obter mais informações, consulte o Guia de administração do Amazon Chime.
Amazon WorkDocs	Para obter mais informações, consulte o Guia de WorkDocs administração da Amazon
Amazon WorkMail	Para obter mais informações, consulte o Amazon WorkMail Administrator Guide.
Amazon WorkSpaces	Você pode criar um Simple AD, AWS Managed Microsoft AD ou AD Connector diretamente do WorkSpaces. Basta iniciar o Advanced Setup ao criar seu Workspace. Para obter mais informações, consulte o Guia de WorkSpaces administração da Amazon.

AWS aplicativo/serviço	Mais informações...
AWS Management Console	Para ter mais informações, consulte Habilitar acesso ao AWS Management Console com as credenciais do AD.

Após habilitado, você controla o acesso aos diretórios no console da aplicação ou do serviço ao qual deseja fornecer acesso ao diretório. Para encontrar os links de AWS aplicativos e serviços descritos acima no AWS Directory Service console, execute as etapas a seguir.

Para exibir os aplicativos e serviços para um diretório

1. No painel de navegação do console doAWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Revise a lista na seção de Aplicações e serviços daAWS .

Para obter mais informações sobre como autorizar ou desautorizar o uso AWS Directory Servicede AWS aplicativos e serviços, consulte. Autorização para AWS aplicativos e serviços usando AWS Directory Service

Tópicos

- Criar um URL de acesso
- Autenticação única

Criar um URL de acesso

Um URL de acesso é usado com aplicações e serviços da AWS, como o Amazon WorkDocs, para acessar uma página de login associada a seu diretório. O URL deve ser globalmente exclusivo. Você pode criar uma URL de acesso para o diretório executando as seguintes etapas.

> **Warning**
>
> Depois de criar um URL de acesso ao aplicativo para esse diretório, ele não poderá ser alterado. Após o URL ser criado, ele não poderá ser usada por terceiros. Se você excluir o

diretório, a URL de acesso também será excluída e poderá ser usada por qualquer outra conta.

Para criar uma URL de acesso

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Na seção Application access URL (URL de acesso ao aplicativo), se um URL de acesso não tiver sido atribuído ao diretório, o botão Create (Criar) será exibido. Digite um alias do diretório e escolha Create (Criar). Se o erro A entidade já existe for retornado, o alias do diretório especificado já foi alocado. Escolha outro alias e repita esse procedimento.

   Seu URL de acesso é exibido no formato *<alias>*.awsapps.com.

Autenticação única

AWS Directory Service fornece a capacidade de permitir que seus usuários acessem a Amazon WorkDocs a partir de um computador associado ao diretório sem precisar inserir suas credenciais separadamente.

Antes de habilitar a autenticação única, é necessário executar etapas adicionais para permitir que os navegadores da Web dos usuários ofereçam suporte à autenticação única. Os usuários podem precisar modificar suas configurações de navegador da Web para habilitar a autenticação única.

> **Note**
>
> O logon único só funciona quando usado em um computador ingressado no diretório do AWS Directory Service . Não pode ser usado em computadores que não estão ingressados no diretório.

Se o diretório for um diretório do AD Connector e a conta de serviço do AD Connector não tiver a permissão para adicionar ou remover o atributo do nome da entidade principal de serviço, você terá duas opções para as etapas 5 e 6 abaixo:

1. Você poderá continuar e será solicitado o nome de usuário e a senha de um usuário do diretório que tenha essa permissão para adicionar ou remover o atributo do nome principal de serviço na conta de serviço do AD Connector. Essas credenciais são usadas apenas para habilitar a autenticação única e não são armazenadas pelo serviço. As permissões da conta de serviço do AD Connector não são alteradas.
2. Você pode delegar permissões para permitir que a conta de serviço do AD Connector adicione ou remova o atributo do nome principal do serviço em si mesma. Você pode executar os PowerShell comandos abaixo em um computador associado ao domínio usando uma conta que tenha permissões para modificar as permissões na conta de serviço do AD Connector. O comando abaixo permitirá que a conta de serviço do AD Connector adicione e remova um atributo de nome de entidade principal de serviço somente na própria conta.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Para ativar ou desativar o login único com a Amazon WorkDocs

1. No painel de navegação do console do AWS Directory Service selecione Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.

3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Na seção URL de acesso ao aplicativo, escolha Habilitar para habilitar o login único para a Amazon. WorkDocs

   Se você não vir o botão Habilitar, talvez seja necessário criar primeiro um URL de acesso para que essa opção seja exibida. Para obter mais informações sobre como criar uma URL de acesso, consulte Criar um URL de acesso.
5. Na caixa de diálogo Habilitar autenticação única para este diretório, escolha Habilitar. O logon único é habilitado para o diretório.
6. Se mais tarde você quiser desativar o login único com a Amazon WorkDocs, escolha Desativar e, na caixa de diálogo Desativar login único para este diretório, escolha Desativar novamente.

Tópicos

- Autenticação única para IE e Chrome
- Autenticação única para o Firefox

Autenticação única para IE e Chrome

Para permitir que os navegadores Microsoft Internet Explorer (IE) e o Google Chrome ofereçam suporte à autenticação única, as seguintes tarefas devem ser executadas no computador cliente:

- Adicione o URL de acesso (por exemplo, https://*<alias>*.awsapps.com) à lista de sites aprovados para autenticação única.
- Ative o script ativo (JavaScript).
- Permita o login automático.
- Habilitar a autenticação integrada.

Você ou seus usuários podem executar essas tarefas manualmente, ou você pode alterar essas configurações usando as configurações da Política de grupo.

Tópicos

- Atualização manual para autenticação única no Windows
- Atualização manual para autenticação única no OS X
- Configurações da política de grupo para autenticação única

Atualização manual para autenticação única no Windows

Para habilitar manualmente a autenticação única em um computador Windows, execute as seguintes etapas no computador cliente. Algumas dessas configurações já podem estar definidas corretamente.

Para habilitar manualmente o logon único para o Internet Explorer e o Chrome no Windows

1. Para abrir a caixa de diálogo Internet Properties, feche o menu Start, digite `Internet Options` na caixa de pesquisa e escolha Internet Options.
2. Adicione a URL de acesso à lista de sites aprovados para logon único executando as etapas a seguir:
    a. Na caixa de diálogo Internet Properties, selecione a guia Security.
    b. Selecione Local intranet e escolha Sites.
    c. Na caixa de diálogo Local intranet, escolha Advanced.
    d. Adicione a URL de acesso à lista de sites e escolha Close.
    e. Na caixa de diálogo Local intranet, escolha OK.
3. Para habilitar scripts ativos, execute as seguintes etapas:
    a. Na guia Security da caixa de diálogo Internet Properties, escolha Custom level.
    b. Na caixa de diálogo Security Settings - Local Intranet Zone, role para baixo até Scripting e selecione Enable em Active scripting.
    c. Na caixa de diálogo Security Settings - Local Intranet Zone, escolha OK.
4. Para habilitar o login automático, execute as seguintes etapas:
    a. Na guia Security da caixa de diálogo Internet Properties, escolha Custom level.
    b. Na caixa de diálogo Security Settings - Local Intranet Zone, role para baixo até User Authentication e selecione Automatic logon only in Intranet zone em Logon.
    c. Na caixa de diálogo Security Settings - Local Intranet Zone, escolha OK.
    d. Na caixa de diálogo Security Settings - Local Intranet Zone, escolha OK.
5. Para habilitar a autenticação integrada, execute as seguintes etapas:
    a. Na caixa de diálogo Internet Properties, selecione a guia Advanced.
    b. Role para baixo até Security e selecione Enable Integrated Windows Authentication.
    c. Na caixa de diálogo Internet Properties, escolha OK.

6. Feche e abra seu navegador novamente para que essas alterações entrem em vigor.

Atualização manual para autenticação única no OS X

Para habilitar manualmente a autenticação única para o Chrome no OS X, execute as seguintes etapas no computador cliente. Você precisará ter direitos de administrador no computador para concluir estas etapas.

Para habilitar manualmente logon único para o Chrome no OS X

1. Adicione seu URL de acesso à AuthServerAllowlistpolítica executando o seguinte comando:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Abra System Preferences, vá para o painel Profiles e exclua o perfil `Chrome Kerberos Configuration`.
3. Reinicie o Chrome e abra chrome://policy no Chrome para confirmar se as configurações estão implantadas.

Configurações da política de grupo para autenticação única

O administrador do domínio pode implementar as configurações da Política de grupo para fazer as alterações de logon único em computadores cliente ingressados no domínio.

> **Note**
>
> Se você gerencia os navegadores da Web Chrome nos computadores do seu domínio com as políticas do Chrome, você deve adicionar seu URL de acesso à AuthServerAllowlistpolítica. Para obter mais informações sobre como definir políticas do Chrome, acesse Configurações de políticas no Chrome.

Para habilitar o logon único manualmente para o Internet Explorer e o Chrome usando as configurações de Política de grupo

1. Crie um novo objeto de Política de grupo executando as seguintes etapas:

   a. Abra a ferramenta de gerenciamento de políticas de grupo, navegue até seu domínio e selecione Group Policy Objects.

b. No menu principal, escolha Action e selecione New.

c. Na caixa de diálogo Novo GPO, digite um nome descritivo para o objeto de política de grupo, como `IAM Identity Center Policy` e mantenha GPO iniciador de origem definido como (nenhum). Clique em OK.

2. Adicione a URL de acesso à lista de sites aprovados para logon único executando as etapas a seguir:

a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Objetos de política de grupo, abra o menu de contexto (clique com o botão direito do mouse) da sua política do Centro de Identidade do IAM e escolha Editar.

b. Na árvore de políticas, navegue para User Configuration > Preferences > Windows Settings.

c. Na lista Windows Settings, abra o menu de contexto (clique com o botão direito do mouse) de Registry e escolha New registry item.

d. Na caixa de diálogo New Registry Properties, insira as configurações a seguir e escolha OK:

Ação

`Update`

Hive

`HKEY_CURRENT_USER`

Path

`Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\`*`<alias>`*

O valor de *`<alias>`* é derivado do URL de acesso. Se sua URL de acesso for `https://examplecorp.awsapps.com`, o alias será `examplecorp`, e a chave do registro será `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Value name

`https`

Tipo de valor

`REG_DWORD`

Value data

1

3. Para habilitar scripts ativos, execute as seguintes etapas:

   a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Objetos de política de grupo, abra o menu de contexto (clique com o botão direito do mouse) da sua política do Centro de Identidade do IAM e escolha Editar.

   b. Na árvore de políticas, navegue para Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

   c. Na lista Intranet Zone, abra o menu de contexto (clique com o botão direito do mouse) de Allow active scripting e escolha Edit.

   d. Na caixa de diálogo Allow active scripting, insira as configurações a seguir e escolha OK:

      - Selecione o botão de opção Enabled.
      - Em Options, defina Allow active scripting como Enable.

4. Para habilitar o login automático, execute as seguintes etapas:

   a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Group Policy Objects, abra o menu de contexto (clique com o botão direito do mouse) de sua política de SSO e escolha Edit.

   b. Na árvore de políticas, navegue para Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

   c. Na lista Intranet Zone, abra o menu de contexto (clique com o botão direito do mouse) de Logon options e escolha Edit.

   d. Na caixa de diálogo Logon options, insira as configurações a seguir e escolha OK:

      - Selecione o botão de opção Enabled.
      - Em Options defina Logon options como Automatic logon only in Intranet zone.

5. Para habilitar a autenticação integrada, execute as seguintes etapas:

   a. Na ferramenta de gerenciamento de políticas de grupo, navegue para seu domínio, selecione Objetos de política de grupo, abra o menu de contexto (clique com o botão direito do mouse) da sua política do Centro de Identidade do IAM e escolha Editar.

b. Na árvore de políticas, navegue para User Configuration > Preferences > Windows Settings.

c. Na lista Windows Settings, abra o menu de contexto (clique com o botão direito do mouse) de Registry e escolha New registry item.

d. Na caixa de diálogo New Registry Properties, insira as configurações a seguir e escolha OK:

   Ação

   ```
   Update
   ```

   Hive

   ```
   HKEY_CURRENT_USER
   ```

   Path

   ```
   Software\Microsoft\Windows\CurrentVersion\Internet Settings
   ```

   Value name

   ```
   EnableNegotiate
   ```

   Tipo de valor

   ```
   REG_DWORD
   ```

   Value data

   ```
   1
   ```

6. Feche a janela Group Policy Management Editor se ainda estiver aberta.

7. Atribua a nova política a seu domínio seguindo estas etapas:

   a. Na árvore de gerenciamento de políticas de grupo, abra o menu contexto (clique com o botão direito do mouse) de seu domínio e escolha Link an Existing GPO.

   b. Na lista Objetos da política de grupo, selecione sua política do Centro de Identidade do IAM e escolha OK.

Essas alterações entrarão em vigor depois da próxima atualização de Política de grupo no cliente, ou na próxima vez que o usuário fizer login.

Autenticação única para o Firefox

Para permitir que o navegador Mozilla Firefox ofereça suporte à autenticação única, adicione o URL de acesso (por exemplo, https://*<alias>*.awsapps.com) à lista de sites aprovados para autenticação única. Isso pode ser feito manualmente ou ser automatizado com um script.

Tópicos

- Atualização manual para autenticação única
- Atualização automática para autenticação única

Atualização manual para autenticação única

Para adicionar a URL de acesso manualmente à lista de sites aprovados no Firefox, execute as seguintes etapas no computador cliente.

Para adicionar manualmente a URL de acesso à lista de sites aprovados no Firefox

1. Abra o Firefox e abra a página `about:config`.
2. Abra a preferência `network.negotiate-auth.trusted-uris` e adicione seu URL de acesso à lista de sites. Use uma vírgula (,) para separar várias entradas.

Atualização automática para autenticação única

Como um administrador de domínio, você pode usar um script para adicionar o URL de acesso à preferência de usuário `network.negotiate-auth.trusted-uris` do Firefox a todos os computadores na rede. Para obter mais informações, acesse https://support.mozilla.org/en-US/questions/939037.

Habilitar acesso ao AWS Management Console com as credenciais do AD

O AWS Directory Service permite que você conceda acesso ao AWS Management Console aos membros de seu diretório. Por padrão, os membros do diretório não têm acesso a nenhum recurso da AWS. Você atribui perfis do IAM aos membros do diretório para conceder a eles acesso a vários serviços e recursos da AWS. O perfil do IAM define os serviços, os recursos e o nível de acesso dos membros do seu diretório.

Para que seja possível conceder acesso ao console aos membros do diretório, o diretório deve ter um URL de acesso. Para obter mais informações sobre como visualizar detalhes do diretório e obter

seu URL de acesso, consulte Visualizar informações do diretório. Para obter mais informações sobre como criar uma URL de acesso, consulte Criar um URL de acesso.

Para obter mais informações sobre como criar e atribuir perfis do IAM aos membros do diretório, consulte Conceder a usuários e grupos acesso aos recursos da AWS.

Tópicos

- Habilitar acesso ao AWS Management Console
- Desabilitar o acesso ao AWS Management Console
- Definir a duração da sessão de login

Artigo relacionado do blog de segurança da AWS

- Como acessar o AWS Management Console usando o AWS Managed Microsoft AD e suas credenciais on-premises

Habilitar acesso ao AWS Management Console

Por padrão, o acesso ao console não é habilitado para nenhum diretório. Para habilitar o acesso ao console para os usuários e grupos de seu diretório, execute as seguintes etapas:

Para habilitar acesso ao console

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Na seção AWS Management Console, escolha Habilitar. O acesso ao console agora está habilitado para o diretório.

   Antes que os usuários possam entrar no console com seu URL de acesso, primeiro é necessário adicionar seus usuários ao perfil. Para obter mais informações sobre a atribuição de usuários a recursos do IAM, consulte Atribuir usuários ou grupos a um perfil existente. Depois que os perfis do IAM forem atribuídos, os usuários poderão acessar o console usando seu URL de acesso. Por exemplo, se o URL de acesso do diretório for example-corp.awsapps.com, o URL para acessar o console será https://example-corp.awsapps.com/console/.

Desabilitar o acesso ao AWS Management Console

Para desabilitar o acesso ao console para os usuários e grupos de seu diretório, execute as seguintes etapas:

Para desabilitar o acesso ao console

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Na seção AWS Management Console, escolha Desabilitar. O acesso ao console agora está desabilitado para o diretório.
5. Se algum perfil do IAM tiver sido atribuído a usuários ou grupos no diretório, o botão Desabilitar poderá não estar disponível. Nesse caso, será necessário remover todas as atribuições de perfis do IAM para o diretório antes de continuar, incluindo atribuições para usuários ou grupos no diretório que foram excluídos, os quais serão mostrados em Usuário excluído ou Grupo excluído.

   Após a remoção de todas as atribuições de perfis do IAM repita as etapas acima.

Definir a duração da sessão de login

Por padrão, os usuários têm 1 hora para usar sua sessão após terem feito login com êxito no console antes de serem desconectados. Depois disso, os usuários deverão fazer login novamente para iniciar a próxima sessão de 1 hora antes de serem desconectados novamente. Você pode usar o procedimento a seguir para alterar a duração para até 12 horas por sessão.

Para definir a duração da sessão de login

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios.
2. Na página Directories (Diretórios), escolha o ID do diretório.
3. Na página Directory details (Detalhes do diretório), selecione a guia Application management (Gerenciamento de aplicativos).
4. Na seção Aplicações e serviços da AWS, escolha Console de Gerenciamento da AWS.
5. Na caixa de diálogo Gerenciar acesso a recurso da AWS, escolha Continuar.
6. Na página Assign users and groups to IAM roles, em Set login session length, edite o valor numerado e escolha Save.

Tutorial: Criar um Simple AD Active Directory

O tutorial a seguir mostra todas as etapas necessárias para configurar um Simple AD Active Directory. O objetivo é que você comece a usar o Simple AD de Active Directory forma rápida e fácil, mas não deve ser usado em um ambiente de produção em grande escala.

Pré-requisitos do tutorial

Este tutorial assume o seguinte:

- Você tem um ativo Conta da AWS.
- Sua conta não atingiu o limite de Amazon VPCs para a região na qual você deseja usar o Simple AD. Para obter mais informações sobre a VPC, consulte O que é a Amazon VPC? e sub-redes em sua VPC no Guia do usuário da Amazon VPC.
- Você não tem uma VPC existente na região com um CIDR de. `10.0.0.0/16`

Para ter mais informações, consulte Pré-requisitos do Simple AD.

Etapa 1: Crie e configure sua Amazon VPC para Simple AD Active Directory

Crie e configure uma Amazon VPC para uso com o Simple AD. Antes de iniciar este procedimento, verifique se você concluiu os Pré-requisitos do tutorial.

Crie uma VPC para seu Simple AD Active Directory

Crie uma VPC com duas sub-redes públicas. AWS Directory Service requer duas sub-redes em sua VPC, e cada sub-rede deve estar em uma zona de disponibilidade diferente.

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No Painel da VPC, escolha Criar VPC.
3. Em Configurações da VPC, escolha VPC e mais.
4. Preencha estes campos da seguinte forma:
    - Mantenha a Geração automática selecionada em Geração automática da tag de nome. Altere um projeto para `ADS VPC`.
    - O Bloco CIDR IPv4 deveria ser `10.0.0.0/16`.
    - Mantenha a opção Sem bloco CIDR IPv6 selecionada.

- A Locação deve permanecer como Padrão.
- Selecione 2 para o Número de zonas de disponibilidade (AZ).
- Selecione 2 em Número de sub-redes públicas. O número de sub-redes privadas pode ser alterado para 0.
- Escolha Personalizar blocos CIDR de sub-rede para configurar o intervalo de endereços IP da sub-rede pública. Os blocos CIDR da sub-rede pública devem ser `10.0.0.0/20` e `10.0.16.0/20`.

5. Escolha Criar VPC. A criação da VPC leva alguns minutos.

Etapa 2: Crie seu Simple AD Active Directory

Para criar um novo Simple AD Active Directory, execute as etapas a seguir. Antes de iniciar esse procedimento, certifique-se de ter concluído os pré-requisitos identificados na Etapa 1: Crie Pré-requisitos do tutorial e configure sua Amazon VPC para Simple AD. Active Directory

Para criar um Simple AD Active Directory

1. No painel de navegação do console do AWS Directory Service, escolha Diretórios e escolha Configurar diretório.
2. Na página Selecionar tipo do diretório, escolha Simple AD e, em seguida, escolha Próximo.
3. Na página Enter directory information (Inserir informações do diretório), forneça as seguintes informações:

   Tamanho do diretório

   Selecione a opção de tamanho Small (Pequeno) ou Large (Grande). Para obter mais informações sobre os tamanhos, consulte Simple AD.

   Nome da organização

   Um nome de organização exclusivo para seu diretório que será usado para registrar dispositivos clientes.

   Esse campo só estará disponível se você estiver criando seu diretório como parte do lançamento WorkSpaces.

   Nome do DNS do diretório

   O nome completo do diretório, como `corp.example.com`.

Nome de NetBIOS do diretório

O nome curto do diretório, como `CORP`.

Senha do administrador

A senha do administrador do diretório. O processo de criação do diretório cria uma conta de administrador com o nome de usuário `Administrator` e essa senha.

A senha do administrador do diretório diferencia maiúsculas de minúsculas e deve ter de 8 a 64 caracteres, inclusive. Ela também precisa conter pelo menos um caractere de três das quatro categorias a seguir:

- Letras minúsculas (a-z)
- Letras maiúsculas (A-Z)
- Números (0-9)
- Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Confirmar senha

Digite a senha do administrador novamente.

Descrição do diretório

Uma descrição opcional do diretório.

4. Na página Choose VPC and subnets (Selecionar VPC e sub-redes), forneça as seguintes informações e selecione Next (Próximo).

   VPC

   A VPC do diretório.

   Subredes

   Selecione as sub-redes para os controladores de domínio. As duas sub-redes deve estar em diferentes zonas de disponibilidade.

5. Na página Review & create (Revisar e criar), analise as informações do diretório e faça as alterações necessárias. Quando as informações estiverem corretas, escolha Create directory (Criar diretório). A criação do diretório leva vários minutos. Depois de criado, o valor de Status é alterado para Ativo.

Práticas recomendadas para o Simple AD

Aqui estão algumas sugestões e diretrizes que você deve considerar para evitar problemas e tirar o máximo proveito do Simple AD.

Configuração: pré-requisitos

Considere essas diretrizes antes de criar seu diretório.

Verifique se você tem o tipo de diretório correto

AWS Directory Service fornece várias maneiras de usar Microsoft Active Directory com outros AWS serviços. Você pode escolher o serviço de diretório com os recursos necessários a um custo que caiba em seu orçamento:

- AWS O Directory Service for Microsoft Active Directory é um serviço gerenciado rico em recursos Microsoft Active Directory hospedado na AWS nuvem. AWS O Microsoft AD gerenciado é sua melhor opção se você tiver mais de 5.000 usuários e precisar de uma relação de confiança configurada entre um diretório AWS hospedado e seus diretórios locais.
- O AD Connector simplesmente conecta seu local existente Active Directory a. AWS O AD Connector é a melhor opção quando você deseja usar seu diretório on-premises existente com os serviços da AWS .
- Simple AD é um diretório de baixa escala e baixo custo com compatibilidade básicaActive Directory. Ele oferece suporte a até 5.000 usuários, aplicações compatíveis com Samba 4 e compatibilidade com LDAP para aplicações compatíveis com LDAP.

Para uma comparação mais detalhada das AWS Directory Service opções, consulteQual escolher.

Verificar se suas VPCs e instâncias estão configuradas corretamente

Para se conectar, gerenciar e usar seus diretórios, é necessário configurar corretamente as VPCs às quais seus diretórios estão associados. Consulte AWS Pré-requisitos gerenciados do Microsoft AD, Pré-requisitos do AD Connector ou Pré-requisitos do Simple AD para obter informações sobre os requisitos de segurança e de rede da VPC.

Se estiver adicionando uma instância a seu domínio, verifique se você tem conectividade e acesso remoto à sua instância, conforme descrito em Associe uma instância do Amazon EC2 ao seu AWS Microsoft AD gerenciado Active Directory.

Conhecer seus limites

Saiba mais sobre os vários limites do seu tipo de diretório específico. O armazenamento disponível e o tamanho agregado dos seus objetos são as únicas limitações no número de objetos que você pode armazenar em seu diretório. Consulte AWS Cotas gerenciadas do Microsoft AD, Cotas do AD Connector ou Cotas do Simple AD para obter detalhes sobre o diretório escolhido.

Entenda a configuração e o uso do grupo de AWS segurança do seu diretório

AWS cria um grupo de segurança e o anexa às interfaces de rede elástica do controlador de domínio do seu diretório. AWS configura o grupo de segurança para bloquear tráfego desnecessário para o diretório e permite o tráfego necessário.

Modificar o grupo de segurança do diretório

Se você deseja modificar a segurança dos grupos de segurança de seus diretórios, você pode fazê-lo. Faça essas alterações apenas se você compreender totalmente como funciona a filtragem do grupo de segurança. Para obter mais informações, consulte Grupos de segurança do Amazon EC2 para instâncias do Linux no Guia do usuário do Amazon EC2. Alterações impróprias podem resultar na perda de comunicações com os computadores e instâncias pretendidos. AWS recomenda que você não tente abrir portas adicionais para seu diretório, pois isso diminui a segurança do seu diretório. Reveja cuidadosamente o Modelo de responsabilidade compartilhada da AWS.

> **Warning**
>
> Tecnicamente, é possível associar os grupos de segurança do diretório a outras instâncias do EC2 que você criar. No entanto, não AWS recomenda essa prática. AWS pode ter motivos para modificar o grupo de segurança sem aviso prévio para atender às necessidades funcionais ou de segurança do diretório gerenciado. Essas alterações afetam as instâncias às quais você associa o grupo de segurança do diretório e podem interromper a operação das instâncias associadas. Além disso, a associação do grupo de segurança do diretório às suas instâncias do EC2 cria um possível risco de segurança para essas instâncias do EC2.

Use o Microsoft AD AWS gerenciado se forem necessárias relações de confiança

O Simple AD não oferece suporte a relações de confiança. Se precisar estabelecer uma relação de confiança entre seu AWS Directory Service diretório e outro diretório, use o AWS Directory Service for Microsoft Active Directory.

Configuração: criar seu diretório

Estas são algumas sugestões a serem consideradas ao criar seu diretório.

Lembre-se de seu ID e senha de administrador

Ao configurar o diretório, você fornece uma senha para a conta de administrador. O ID de conta é Administrator para o Simple AD. Lembre-se da senha criada para essa conta. Caso contrário, você não poderá adicionar objetos a seu diretório.

Entenda as restrições de nome de usuário para AWS aplicativos

AWS Directory Service fornece suporte para a maioria dos formatos de caracteres que podem ser usados na construção de nomes de usuário. No entanto, existem restrições de caracteres impostas aos nomes de usuário que serão usados para fazer login em AWS aplicativos, como WorkSpaces Amazon WorkMail, WorkDocs Amazon ou Amazon. QuickSight Essas restrições exigem que os seguintes caracteres não sejam usados:

- Espaços
- Caracteres multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> O símbolo@é permitido, desde que ele preceda um sufixo UPN.

Programar suas aplicações

Antes de programar seus aplicativos, considere o seguinte:

Use o serviço de localização de DCs do Windows

Ao desenvolver aplicativos, use o serviço localizador de DC do Windows ou use o serviço DNS dinâmico (DDNS) do seu AWS Microsoft AD gerenciado para localizar controladores de domínio (DCs). Não codifique aplicativos com o endereço de um DC. O serviço de localização de DC ajuda a garantir que a carga do diretório seja distribuída e permite que você aproveite a escalabilidade horizontal, adicionando controladores de domínio à implantação. Se você vincular o aplicativo a um DC fixo, e o DC passar por patches ou recuperação, seu aplicativo perderá acesso ao DC, em vez de usar um dos DCs restantes. Além disso, a codificação do DC pode resultar na criação de um ponto de acesso de um único DC. Em casos graves, a criação do ponto de acesso pode fazer com que o DC não responda. Esses casos também podem fazer com que a automação do AWS diretório sinalize o diretório como prejudicado e desencadeie processos de recuperação que substituam o DC que não responde.

Faça um teste de carga antes de implantar no ambiente de produção

Faça testes laboratoriais com objetos e solicitações que representam sua workload de produção para confirmar se o diretório é dimensionado conforme a carga da aplicação. Se você precisar de capacidade adicional, use o AWS Directory Service Microsoft Active Directory, que permite adicionar controladores de domínio para obter alto desempenho. Para ter mais informações, consulte Implantar controladores de domínio adicionais.

Use consultas LDAP eficientes

Muitas consultas LDAP para um controlador de domínio em milhares de objetos podem consumir ciclos de CPU significativos em um único DC, resultando em pontos de acesso. Isso pode afetar aplicativos que compartilham o mesmo DC durante a consulta.

Cotas do Simple AD

Geralmente, você não deve adicionar mais de 500 usuários a um diretório pequeno do Simple AD e não mais que 5.000 usuários a um diretório grande do Simple AD. Para obter opções de escalamento mais flexíveis e recursos adicionais do Active Directory, considere usar o AWS Directory Service for Microsoft Active Directory (Standard Edition ou Enterprise Edition).

A seguir estão as cotas padrão para o Simple AD. A menos que especificado de outra forma, cada cota é aplicada por região.

Cotas do Simple AD

Recurso	Cota padrão
Diretórios do Simple AD	10
Snapshots manuais*	5 por Simple AD

* A cota de snapshots manuais não pode ser alterada.

> **Note**
>
> Não é possível anexar um endereço IP público à sua interface de rede elástica (ENI) da AWS.

Política de compatibilidade de aplicativos do Simple AD

O Simple AD é uma implementação do Samba que fornece muitos dos recursos básicos do Active Directory. Em razão da enorme quantidade de aplicações personalizadas e comerciais prontas para uso que utilizam o Active Directory, a AWS não pode executar a verificação formal ou ampla da compatibilidade de aplicações de terceiros com o Simple AD. Embora a AWS trabalhe com os clientes na tentativa de superar possíveis desafios que possam surgir na instalação de aplicações, não podemos garantir que todas elas sejam ou continuem sendo compatíveis com o Simple AD.

As seguintes aplicações de terceiros são compatíveis com o Simple AD:

- Microsoft Internet Information Services (IIS) nas seguintes plataformas:
  - Windows Server 2003 R2
  - Windows Server 2008 R1
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Microsoft SQL Server:
  - SQL Server 2005 R2 (Express Edition, Web Edition e Standard Edition)
  - SQL Server 2008 R2 (Express Edition, Web Edition e Standard Edition)

  - SQL Server 2012 (Express Edition, Web Edition e Standard Edition)
  - SQL Server 2014 (Express Edition, Web Edition e Standard Edition)
- Microsoft SharePoint:
  - SharePoint 2010 Foundation
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

Os clientes podem optar por usar o AWS Directory Service for Microsoft Active Directory (AWS Microsoft AD gerenciado) para atingir um nível mais alto de compatibilidade com base no Active Directory real.

Solução de problemas do Simple AD

Os tópicos a seguir podem ajudá-lo a solucionar alguns problemas comuns que podem ser encontrados ao criar ou usar o diretório.

Tópicos

Recuperação de senha

Se um usuário esquecer uma senha ou estiver tendo problemas para entrar no diretório Simple AD ou AWS Managed Microsoft AD, você poderá redefinir a senha usando o AWS Management Console, Windows PowerShell ou o. AWS CLI

Para ter mais informações, consulte Redefinir uma senha de usuário do Simple AD.

Recebi um erro "O KDC não pode atender a opção solicitada" ao adicionar um usuário ao Simple AD

Isso pode ocorrer quando o cliente do Samba CLI não envia corretamente os comandos "net" para todos os controladores de domínio. Se receber essa mensagem de erro ao usar o comando "net ads" para adicionar um usuário ao diretório do Simple AD, use o argumento -S e especifique o endereço IP de um de seus controladores de domínio. Se ainda receber o erro, tente o outro controlador de domínio. Também é possível usar as ferramentas de administração do Active Directory para adicionar usuários ao seu diretório. Para ter mais informações, consulte Instale as ferramentas de administração do Active Directory para Simple AD.

Não posso atualizar o nome do DNS ou o endereço IP de uma instância associada ao meu domínio (atualização dinâmica do DNS)

As atualizações dinâmicas de DNS não são compatíveis com domínios do Simple AD. Você pode fazer alterações conectando-se diretamente ao seu diretório usando o Gerenciador DNS em uma instância que integrada em seu domínio.

Não posso fazer login no SQL Server usando uma conta do SQL Server

Você poderá receber um erro se tentar usar o SQL Server Management Studio (SSMS) com uma conta do SQL Server para fazer login no SQL Server em execução em uma instância do EC2 no Windows 2012 R2. O problema ocorre quando o SSMS é executado como um usuário de domínio e pode resultar no erro "Falha no login do usuário" mesmo quando credenciais válidas são fornecidas. Esse é um problema conhecido e AWS está trabalhando ativamente para resolvê-lo.

Como solução alternativa para o problema, você pode fazer login no SQL Server com a autenticação do Windows em vez da autenticação SQL. Ou iniciar o SSMS como um usuário local em vez de um usuário de domínio do Simple AD.

Meu diretório está travado no estado "Solicitado"

Se você tiver um diretório que está no estado “solicitado” por mais de cinco minutos, tente excluir o diretório e recriá-lo. Se o problema persistir, entre em contato com o AWS Support Center.

Recebo um erro de "AZ restrita" quando crio um diretório

Algumas AWS contas criadas antes de 2012 podem ter acesso às zonas de disponibilidade na região Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Norte da Califórnia) ou Ásia-Pacífico (Tóquio) que não oferecem suporte a AWS Directory Service diretórios. Se você receber um erro como esse ao criar um diretório, escolha uma sub-rede em outra zona de disponibilidade e tente criar o diretório novamente.

Alguns dos meus usuários não podem se autenticar com meu diretório

Suas contas de usuário devem ter a pré-autenticação Kerberos habilitada. Essa é a configuração padrão para novas contas de usuário e não deve ser alterada. Para obter mais informações sobre essa configuração, acesse Pré-autenticação na Microsoft TechNet.

Recursos adicionais do

Os recursos a seguir podem ajudá-lo a solucionar problemas à medida que você trabalha com AWS.

- AWS Centro de conhecimento — encontre perguntas frequentes e links para outros recursos para ajudá-lo a solucionar problemas.
- AWS Support Center — Obtenha suporte técnico.
- AWS Premium Support Center — Obtenha suporte técnico premium.

Tópicos

Motivos para status de diretórios do Simple AD

Quando um diretório está danificado ou inoperável, a mensagem de status do diretório contém informações adicionais. A mensagem de status é exibida no console do AWS Directory Service ou retornada no membro `DirectoryDescription.StageReason` pela API `DescribeDirectories`. Para obter mais informações sobre o status de diretório, consulte Noções básicas sobre o status do diretório.

As mensagens de status para um diretório do Simple AD são:

Tópicos

A interface de rede elástica do serviço de diretório não está conectada

Descrição

A interface de rede elástica (ENI) crítica que foi criada em seu nome durante a criação do diretório para estabelecer a conectividade de rede com sua VPC não está conectada à instância do diretório. As aplicações da AWS baseadas nesse diretório não funcionarão. Seu diretório não pode se conectar à sua rede on-premises.

Solução de problemas

Se a ENI estiver desconectada, mas ainda existir, entre em contato com o AWS Support. Se a ENI for excluída, não será possível resolver o problema e seu diretório ficará permanentemente inutilizável. Nesse caso, você deverá excluir o diretório e criar um novo.

Problemas detectados por instância

Descrição

Um erro interno foi detectado pela instância. Isso geralmente significa que o serviço de monitoramento está ativamente tentando recuperar as instâncias danificadas.

Solução de problemas

Na maioria dos casos, esse é um problema transitório e, eventualmente, o diretório retornará ao estado Ativo. Se o problema persistir, entre em contato com o AWS Support para obter assistência.

O usuário reservado crítico do AWS Directory Service está ausente no diretório

Descrição

Quando um Simple AD é criado, o AWS Directory Service cria uma conta de serviço no diretório com o nome `AWSAdmin`*`D-xxxxxxxxx`*. Este erro é recebido quando essa conta de serviço não pode ser encontrada. Sem essa conta, o AWS Directory Service não pode executar funções administrativas no diretório, tornando-o inutilizável.

Solução de problemas

Para corrigir esse problema, restaure o diretório para um snapshot anterior que tenha sido criado antes da exclusão da conta de serviço. Snapshots automáticos são capturados do diretório do Simple AD uma vez por dia. Se essa conta tiver sido excluída há mais de cinco dias, talvez não seja possível restaurar o diretório para um estado em que essa conta exista. Se você não conseguir restaurar o diretório de um snapshot onde essa conta existe, o diretório pode se tornar permanentemente inutilizável. Nesse caso, você deve excluir o diretório e criar um novo.

O usuário reservado crítico do AWS Directory Service precisa pertencer ao grupo Administradores de Domínio.

Descrição

Quando um Simple AD é criado, o AWS Directory Service cria uma conta de serviço no diretório com o nome `AWSAdmin`*`D-xxxxxxxxx`*. Este erro é recebido quando esta conta de serviço não é membro do grupo `Domain Admins`. A associação neste grupo é necessária para conceder ao AWS Directory Service os privilégios necessários para ele realizar operações de manutenção e recuperação, como a transferência de funções de FSMO, a união de domínios de novos controladores de diretório e a restauração de snapshots.

Solução de problemas

Use a ferramenta Active Directory Users and Computers (Usuários e computadores do Active Directory) para adicionar novamente a conta de serviço ao grupo `Domain Admins`.

O usuário reservado crítico do AWS Directory Service está desabilitado

Descrição

Quando um Simple AD é criado, o AWS Directory Service cria uma conta de serviço no diretório com o nome `AWSAdmin`*`D-xxxxxxxxx`*. Este erro é recebido quando esta conta de serviço está desabilitada. Esta conta deve ser habilitada para que o AWS Directory Service possa realizar as operações de manutenção e recuperação no diretório.

Solução de problemas

Use a ferramenta Active Directory Users and Computers (Usuários e computadores do Active Directory) para habilitar novamente a conta de serviço.

O controlador de domínio principal não possui todas as funções de FSMO

Descrição

Nem todas as funções de FSMO pertencem ao controlador do diretório do Simple AD. O AWS Directory Service não poderá assegurar determinados comportamentos e funcionalidades se as funções de FSMO não pertencerem ao controlador do diretório do Simple AD correto.

Solução de problemas

Use as ferramentas do Active Directory para mover as funções de FSMO de volta para o controlador de diretório de trabalho original. Para obter mais informações sobre como mover as funções do FSMO, acesse https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds. Se isso não corrigir o problema, entre em contato com o AWS Support para obter assistência adicional.

Falhas na replicação do controlador de domínio

Descrição

Os controladores do diretório do Simple AD não estão replicando entre si. Isso pode ter como causa um dos problemas a seguir:

- Os grupos de segurança dos controladores de diretório não estão com as portas corretas abertas.
- Os network ACLs são muito restritivos.

- A tabela de rotas da VPC não está roteando o tráfego de rede entre os controladores de diretório corretamente.
- Uma outra instância foi promovida a controlador de domínio no diretório.

Solução de problemas

Para obter mais informações sobre os requisitos de rede da VPC, consulte AWS Pré-requisitos gerenciados do Microsoft AD do AWS Managed Microsoft AD, Pré-requisitos do AD Connector do AD Connector ou Pré-requisitos do Simple AD do Simple AD. Se houver um controlador de domínio desconhecido no seu diretório, você deverá rebaixá-lo. Se sua configuração de rede da VPC está correta, mas o erro persiste, entre em contato com o AWS Support para obter assistência adicional.

Segurança em AWS Directory Service

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS Directory Service, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Directory Service. Os tópicos a seguir mostram como configurar para atender AWS Directory Service aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Directory Service recursos.

Tópicos de segurança

Os seguintes tópicos de segurança podem ser encontrados nesta seção:

- Gerenciamento de identidade e acesso para AWS Directory Service
- Registro e monitoramento em AWS Directory Service
- Validação de conformidade para AWS Directory Service
- Resiliência em AWS Directory Service
- Segurança da infraestrutura em AWS Directory Service

Tópicos de segurança adicionais

Os seguintes tópicos de segurança adicionais podem ser encontrados neste guia:

Contas, relações fiduciárias e acesso a AWS recursos

- Permissões para a conta de administrador
- Contas de serviço gerenciadas pelo grupo
- Criar uma relação de confiança
- Delegação restrita de Kerberos
- Conceder a usuários e grupos acesso aos recursos da AWS
- Autorização para AWS aplicativos e serviços usando AWS Directory Service

Proteção do diretório

- Proteger seu diretório do AWS Managed Microsoft AD
- Proteger seu diretório do AD Connector

Registro e monitoramento

- Monitorar seu AWS Managed Microsoft AD
- Monitore seu diretório do AD Connector

Resiliência

- Patches e manutenção do AWS Managed Microsoft AD

Gerenciamento de identidade e acesso para AWS Directory Service

O acesso a AWS Directory Service requer credenciais que AWS possam ser usadas para autenticar suas solicitações. Essas credenciais devem ter permissões para acessar AWS recursos, como um AWS Directory Service diretório. As seções a seguir fornecem detalhes sobre como você pode usar o AWS Identity and Access Management (IAM) e como ajudar AWS Directory Service a proteger seus recursos controlando quem pode acessá-los:

- Autenticação

- Controle de acesso

Autenticação

Saiba como acessar AWS usando identidades do IAM.

Controle de acesso

Você pode ter credenciais válidas para autenticar suas solicitações, mas, a menos que tenha permissões, não poderá criar ou acessar AWS Directory Service recursos. Por exemplo, você deve ter permissões para criar um AWS Directory Service diretório ou criar um instantâneo do diretório.

As seções a seguir descrevem como gerenciar permissões para AWS Directory Service. Recomendamos que você leia a visão geral primeiro.

- Visão geral do gerenciamento de permissões de acesso aos seus AWS Directory Service recursos
- Usando políticas baseadas em identidade (políticas do IAM) para AWS Directory Service
- AWS Directory Service Permissões de API: referência de ações, recursos e condições

Visão geral do gerenciamento de permissões de acesso aos seus AWS Directory Service recursos

Cada AWS recurso pertence a uma AWS conta, e as permissões para criar ou acessar os recursos são regidas por políticas de permissões. Um administrador da conta pode anexar políticas de permissões às identidades do IAM (ou seja, usuários, grupos e funções), e alguns serviços (como AWS Lambda) também oferecem suporte para anexar políticas de permissões aos recursos.

> **Note**
>
> Um administrador da conta (ou usuário administrador) é um usuário com privilégios de administrador. Para obter mais informações, consulte Melhores práticas do IAM no IAM User Guide.

Tópicos

- AWS Directory Service recursos e operações
- Informações sobre propriedade de recursos
- Gerenciamento de acesso aos recursos
- Especificar elementos da política: ações, efeitos, recursos e entidades principais
- Especificar condições em uma política

AWS Directory Service recursos e operações

Em AWS Directory Service, o recurso principal é um diretório. AWS Directory Service também oferece suporte a recursos de instantâneo de diretórios. No entanto, você pode criar snapshots apenas no contexto de um diretório existente. Portanto, um snapshot é conhecido como um sub-recurso.

Esses recursos têm nomes de recurso da Amazon (ARNs) exclusivos associados, conforme mostrado na tabela a seguir.

Tipo de recurso	Formato de Nome de região da Amazon (ARN)
Diretório	`arn:aws:ds: region:account-id :directory/ external-directory-id`
Snapshot	`arn:aws:ds: region:account-id :snapshot/ external-snapshot-id`

AWS Directory Service fornece um conjunto de operações para trabalhar com os recursos apropriados. Para obter uma lista das operações disponíveis, consulte Ações do Directory Service.

Informações sobre propriedade de recursos

O proprietário do recurso é a AWS conta que criou um recurso. Ou seja, o proprietário do recurso é a AWS conta da entidade principal (a conta raiz, um usuário do IAM ou uma função do IAM) que autentica a solicitação que cria o recurso. Os seguintes exemplos mostram como isso funciona:

- Se você usar as credenciais da conta raiz da sua AWS conta para criar um AWS Directory Service recurso, como um diretório, sua AWS conta é a proprietária desse recurso.

- Se você criar um usuário do IAM em sua AWS conta e conceder permissões para criar AWS Directory Service recursos para esse usuário, o usuário também poderá criar AWS Directory Service recursos. No entanto, sua AWS conta, à qual o usuário pertence, possui os recursos.
- Se você criar uma função do IAM em sua AWS conta com permissões para criar AWS Directory Service recursos, qualquer pessoa que possa assumir a função poderá criar AWS Directory Service recursos. Sua AWS conta, à qual a função pertence, é proprietária dos AWS Directory Service recursos.

Gerenciamento de acesso aos recursos

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação das políticas de permissões.

> **Note**
>
> Esta seção discute o uso do IAM no contexto de AWS Directory Service. Não são fornecidas informações detalhadas sobre o serviço IAM. Para ver a documentação completa do IAM, consulte O que é o IAM? no Guia do usuário do IAM. Para obter informações sobre a sintaxe e as descrições da política do IAM, consulte a Referência da política JSON do IAM no Guia do usuário do IAM.

As políticas anexadas a uma identidade do IAM são chamadas de políticas baseadas em identidade (políticas do IAM) e as políticas anexadas a um recurso são chamadas de políticas baseadas em recursos. AWS Directory Service suporta somente políticas baseadas em identidade (políticas do IAM).

Tópicos

- Políticas baseadas em identidade (políticas do IAM)
- Políticas baseadas em recursos

Políticas baseadas em identidade (políticas do IAM)

Você pode anexar políticas a identidades do IAM. Por exemplo, você pode fazer o seguinte:

- Anexe uma política de permissões a um usuário ou grupo em sua conta — Um administrador da conta pode usar uma política de permissões associada a um usuário específico para conceder

permissões para que esse usuário crie um AWS Directory Service recurso, como um novo diretório.

- Anexar uma política de permissões a uma função: você pode anexar uma política de permissões baseada em identidade a um perfil do IAM para conceder permissões entre contas.

  Para obter mais informações sobre o uso do IAM para delegar permissões, consulte Access management no IAM User Guide.

A seguinte política de permissões concede permissões a um usuário para executar todas as ações que começam com `Describe`. Essas ações mostram informações sobre um AWS Directory Service recurso, como um diretório ou um instantâneo. Observe que o caractere curinga (*) no `Resource` elemento indica que as ações são permitidas para todos os AWS Directory Service recursos pertencentes à conta.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Para obter mais informações sobre o uso de políticas baseadas em identidade com AWS Directory Service, consulte. Usando políticas baseadas em identidade (políticas do IAM) para AWS Directory Service Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identities (users, groups, and roles) no Guia do usuário do IAM.

Políticas baseadas em recursos

Outros serviços, como o Amazon S3, também aceitam políticas de permissões baseadas em recurso. Por exemplo, você pode anexar uma política a um bucket do S3 para gerenciar as permissões de acesso a esse bucket. AWS Directory Service não oferece suporte a políticas baseadas em recursos.

Especificar elementos da política: ações, efeitos, recursos e entidades principais

Para cada AWS Directory Service recurso, o serviço define um conjunto de operações de API. Para ter mais informações, consulte AWS Directory Service recursos e operações. Para obter uma lista das operações de API, consulte Ações do Directory Service.

Para conceder permissões para essas operações de API, AWS Directory Service defina um conjunto de ações que você pode especificar em uma política. Observe que a execução de uma operação de API pode exigir permissões para mais de uma ação.

Estes são os elementos de política básicos:

- Recurso: em uma política, você usa um Amazon Resource Name (ARN – Nome de recurso da Amazon) para identificar o recurso a que a política se aplica. Para AWS Directory Service recursos, você sempre usa o caractere curinga (*) nas políticas do IAM. Para ter mais informações, consulte AWS Directory Service recursos e operações.
- Ação: você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar. Por exemplo, a permissão `ds:DescribeDirectories` permite que o usuário execute a operação AWS Directory Service `DescribeDirectories`.
- Efeito: você especifica o efeito quando o usuário solicita a ação específica. E pode ser permitir ou negar. Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, para ter certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é a entidade principal implícita. Para políticas baseadas em recursos, você especifica o usuário, a conta, o serviço ou outra entidade que deseja receber permissões (aplica-se somente às políticas baseadas em recursos). AWS Directory Service não oferece suporte a políticas baseadas em recursos.

Para saber mais sobre a sintaxe e as descrições de políticas do IAM, consulte a Referência da política JSON do IAM no Guia do usuário do IAM.

Para ver uma tabela mostrando todas as ações da AWS Directory Service API e os recursos aos quais elas se aplicam, consulteAWS Directory Service Permissões de API: referência de ações, recursos e condições.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política de acesso para especificar as condições quando uma política deve entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte Condition no Guia do usuário do IAM.

Para expressar condições, você usa chaves de condição predefinidas. Não existem chaves de condição específicas do AWS Directory Service. No entanto, existem chaves de AWS condição que você pode usar conforme apropriado. Para obter uma lista completa das AWS chaves, consulte Chaves de condição globais disponíveis no Guia do usuário do IAM.

Usando políticas baseadas em identidade (políticas do IAM) para AWS Directory Service

Este tópico fornece exemplos de políticas baseadas em identidade em que um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e funções).

> **Important**
>
> Recomendamos que você primeiro analise os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para gerenciar o acesso aos seus AWS Directory Service recursos. Para ter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos seus AWS Directory Service recursos.

As seções neste tópico abrangem o seguinte:

- Permissões necessárias para usar o AWS Directory Service console
- AWS políticas gerenciadas (predefinidas) para AWS Directory Service
- Exemplos de política gerenciada pelo cliente
- Utilização de tags com políticas do IAM

A seguir, um exemplo de uma política de permissões.

```
{
```

```
{
 "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "AllowDsEc2IamGetRole",
          "Effect": "Allow",
          "Action": [
              "ds:CreateDirectory",
              "ec2:RevokeSecurityGroupIngress",
              "ec2:CreateNetworkInterface",
              "ec2:AuthorizeSecurityGroupEgress",
              "ec2:AuthorizeSecurityGroupIngress",
              "ec2:DescribeNetworkInterfaces",
              "ec2:DescribeVpcs",
              "ec2:CreateSecurityGroup",
              "ec2:RevokeSecurityGroupEgress",
              "ec2:DeleteSecurityGroup",
              "ec2:DeleteNetworkInterface",
              "ec2:DescribeSubnets",
              "iam:GetRole"
          ],
          "Resource": "*"
      },
      {
          "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
          "Effect": "Allow",
          "Action": [
              "iam:CreateRole",
              "iam:PutRolePolicy"
          ],
          "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
      },
      {
          "Sid": "AllowPassRole",
          "Effect": "Allow",
          "Action": "iam:PassRole",
          "Resource": "*",
          "Condition": {
              "StringEquals": {
                  "iam:PassedToService": "cloudwatch.amazonaws.com"
              }
          }
      }
  ]
```

```
}
```

A política inclui o seguinte:

- A primeira declaração concede permissão para criar um AWS Directory Service diretório. AWS Directory Service não oferece suporte a permissões para essa ação específica no nível do recurso. Portanto, a política especifica um caractere curinga (*) como valor do `Resource`.
- A segunda instrução concede permissões a determinadas ações do IAM. O acesso às ações do IAM é necessário para que AWS Directory Service você possa ler e criar funções do IAM em seu nome. O caractere curinga (*) no final do valor de `Resource` significa que a instrução fornece permissões para as ações do IAM em qualquer função do IAM. Para limitar essa permissão a uma função específica, substitua o caractere curinga (*) no ARN do recurso pelo nome da função específica. Para obter mais informações, consulte Ações do IAM.
- A terceira declaração concede permissões a um conjunto específico de recursos do Amazon EC2 que são necessários AWS Directory Service para permitir a criação, configuração e destruição de seus diretórios. O caractere curinga (*) no final do valor de `Resource` significa que a instrução fornece permissões para as ações do EC2 em qualquer recurso ou sub-recurso do EC2. Para limitar essa permissão a uma função específica, substitua o caractere curinga (*) no ARN do recurso pelo recurso ou sub-recurso específico. Para obter mais informações, consulte Ações do Amazon EC2.

A política não especifica o elemento `Principal` porque, em uma política baseada em identidade, a entidade principal que obtém as permissões não é especificada. Quando você anexar uma política um usuário, o usuário será a entidade principal implícita. Quando você anexa uma política de permissão a um perfil do IAM, a entidade principal identificada na política de confiança do perfil obtém as permissões.

Para ver uma tabela mostrando todas as ações da AWS Directory Service API e os recursos aos quais elas se aplicam, consulteAWS Directory Service Permissões de API: referência de ações, recursos e condições.

Permissões necessárias para usar o AWS Directory Service console

Para que um usuário trabalhe com o AWS Directory Service console, esse usuário deve ter as permissões listadas na política anterior ou as permissões concedidas pela função Directory Service Full Access Role ou Directory Service Read Only, descrita emAWS políticas gerenciadas (predefinidas) para AWS Directory Service.

Se você criar uma política do IAM que seja mais restritiva que as permissões mínimas necessárias, o console do não funcionará como pretendido para os usuários com essa política do IAM.

AWS políticas gerenciadas (predefinidas) para AWS Directory Service

AWS aborda muitos casos de uso comuns fornecendo políticas autônomas do IAM que são criadas e administradas pela AWS. As políticas gerenciadas concedem permissões necessárias para casos de uso comuns, de maneira que você possa evitar a necessidade de investigar quais permissões são necessárias. Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

As seguintes políticas AWS gerenciadas, que você pode anexar aos usuários em sua conta, são específicas para AWS Directory Service:

- AWSDirectoryServiceReadOnlyAccess— Concede a um usuário ou grupo acesso somente de leitura a todos os AWS Directory Service recursos, sub-redes EC2, interfaces de rede EC2 e tópicos e assinaturas do Amazon Simple Notification Service (Amazon SNS) para a conta raiz. AWS Para ter mais informações, consulte Usar as políticas gerenciadas da AWS com o AWS Directory Service.
- AWSDirectoryServiceFullAccess: concede a um usuário ou grupo o seguinte:
  - Acesso total ao AWS Directory Service
  - Acesso aos principais serviços do Amazon EC2 necessários para uso AWS Directory Service
  - Capacidade de listar tópicos do Amazon SNS
  - Capacidade de criar, gerenciar e excluir tópicos do Amazon SNS com um nome começando com “” DirectoryMonitoring

  Para ter mais informações, consulte Usar as políticas gerenciadas da AWS com o AWS Directory Service.

Além disso, há outras políticas AWS gerenciadas que são adequadas para uso com outras funções do IAM. Essas políticas são atribuídas às funções associadas aos usuários em seu AWS Directory Service diretório. Essas políticas são necessárias para que esses usuários tenham acesso a outros AWS recursos, como o Amazon EC2. Para ter mais informações, consulte Conceder a usuários e grupos acesso aos recursos da AWS.

Você também pode criar políticas personalizadas do IAM que permitem que os usuários acessem os recursos e as ações necessários da API do . Você pode anexar essas políticas personalizadas a usuários ou grupos do IAM que exijam essas permissões.

Exemplos de política gerenciada pelo cliente

Nesta seção, você pode encontrar exemplos de políticas de usuário que concedem permissões para várias AWS Directory Service ações.

> **Note**
>
> Todos os exemplos usam a Região do Oeste dos EUA (Oregon) (`us-west-2`) e contêm IDs de conta fictícios.

Exemplos

- Exemplo 1: permitir que um usuário execute qualquer ação de descrição em qualquer AWS Directory Service recurso
- Exemplo 2: permitir que um usuário crie um diretório

Exemplo 1: permitir que um usuário execute qualquer ação de descrição em qualquer AWS Directory Service recurso

A seguinte política de permissões concede permissões a um usuário para executar todas as ações que começam com `Describe`. Essas ações mostram informações sobre um AWS Directory Service recurso, como um diretório ou um instantâneo. Observe que o caractere curinga (*) no `Resource` elemento indica que as ações são permitidas para todos os AWS Directory Service recursos pertencentes à conta.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Exemplo 2: permitir que um usuário crie um diretório

A política de permissões a seguir concede permissões para permitir que um usuário crie um diretório e todos os outros recursos relacionados, como snapshots e confianças. Para fazer isso, permissões para determinados serviços do Amazon EC2 também são necessárias.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "ds:Create*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
                  ],
         "Resource":"*"
         ]
      }
   ]
}
```

Utilização de tags com políticas do IAM

Você pode aplicar permissões em nível de recurso com base em tags nas políticas do IAM que você usa para a maioria das ações de API. AWS Directory Service Isso oferece a você mais controle sobre quais recursos um usuário pode criar, modificar ou usar. Você pode usar o elemento `Condition` (também chamado bloco `Condition`) juntamente com os seguintes valores e chaves de contexto de condição em uma política do IAM para controlar o acesso do usuário (permissões) baseado em tags de um recurso:

- Use `aws:ResourceTag/`**`tag-key`**`: `**`tag-value`** para permitir ou negar ações do usuário em recursos com tags específicas.

- Use `aws:ResourceTag/`**`tag-key`**: **`tag-value`** para exigir que uma tag específica seja (ou não seja) usada ao fazer uma solicitação de API para criar ou modificar um recurso que permita tags.
- Use `aws:TagKeys`: [**`tag-key`**, ...] para exigir que um conjunto específico de chaves de tag seja (ou não seja) usado ao fazer uma solicitação de API para criar ou modificar um recurso que permita tags.

> **Note**
>
> Os valores e as chaves de contexto de condição em uma política do IAM se aplicam somente às ações do AWS Directory Service em que um identificador de um recurso que pode ser marcado com tags é um parâmetro obrigatório.

Controlar o acesso usando tags no Guia do usuário do IAM tem informações adicionais sobre o uso de tags. A seção Referência de política JSON do IAM desse guia detalhou a sintaxe, as descrições e os exemplos dos elementos, variáveis e lógica de avaliação das políticas JSON no IAM.

O seguinte exemplo de política de tags permite todas as chamadas de `ds`, desde que ela contenha o par de valor da tag "`fooKey`" ou "`fooValue`".

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
```

```
         ],
         "Resource":"*"
      }
   ]
}
```

O seguinte exemplo de política permite todas as chamadas `ds`, contanto que o recurso contenha o ID do diretório "`d-1234567890`".

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Para obter mais informações sobre ARNs, consulte Amazon Resource Names (ARNs) e AWS Service Namespaces.

A lista de operações de AWS Directory Service API a seguir oferece suporte a permissões em nível de recurso baseadas em tags:

- AcceptSharedDirectory
- AddIpRoutes
- AddTagsToResource
- CancelSchemaExtension
- CreateAlias

- CreateComputer
- CreateConditionalForwarder
- CreateSnapshot
- CreateLogSubscription
- CreateTrust
- DeleteConditionalForwarder
- DeleteDirectory
- DeleteLogSubscription
- DeleteSnapshot
- DeleteTrust
- DeregisterEventTopic
- DescribeConditionalForwarders
- DescribeDomainControllers
- DescribeEventTopics
- DescribeSharedDirectories
- DescribeSnapshots
- DescribeTrusts
- DisableRadius
- DisableSso
- EnableRadius
- EnableSso
- GetSnapshotLimits
- ListIpRoutes
- ListSchemaExtensions
- ListTagsForResource
- RegisterEventTopic
- RejectSharedDirectory
- RemoveIpRoutes

- RemoveTagsFromResource
- ResetUserPassword
- RestoreFromSnapshot
- ShareDirectory
- StartSchemaExtension
- UnshareDirectory
- UpdateConditionalForwarder
- UpdateNumberOfDomainControllers
- UpdateRadius
- UpdateTrust
- VerifyTrust

AWS Directory Service Permissões de API: referência de ações, recursos e condições

Ao configurar o Controle de acesso e escrever políticas de permissões que podem ser anexadas a uma identidade do IAM (políticas baseadas em identidade), você pode usar a tabela AWS Directory Service Permissões de API: referência de ações, recursos e condições como referência. Cada entrada de API na inclui o seguinte:

- Nome da operação AWS Directory Service da API
- As ações correspondentes para as quais você pode conceder permissões para executar a ação
- O AWS recurso para o qual você pode conceder as permissões

Especifique as ações no campo `Action` da política e o valor do recurso no campo `Resource` da política. Para especificar uma ação, use o prefixo `ds:` seguido do nome da operação da API (por exemplo, `ds:CreateDirectory`). Alguns AWS aplicativos podem exigir o uso de operações de AWS Directory Service API não públicas`ds:AuthorizeApplication`, como`ds:CheckAlias`,`ds:CreateIdentityPoolDirectory`,`ds:GetAuthorizedApplicationDetai` e `ds:UnauthorizeApplication` em suas políticas.

Algumas AWS Directory Service APIs só podem ser chamadas por meio do AWS Management Console. Elas não são APIs públicas, no sentido de que não podem ser chamadas

programaticamente e não são fornecidas por nenhum SDK. Eles aceitam as credenciais do usuário. Essas operações de API incluem `ds:DisableRoleAccessds:EnableRoleAccess`, `ds:UpdateDirectory` e.

Você pode usar chaves de condição AWS globais em suas AWS Directory Service políticas para expressar condições. Para obter uma lista completa das AWS chaves, consulte Chaves de condição globais disponíveis no Guia do usuário do IAM.

Related Topics

- Controle de acesso

Autorização para AWS aplicativos e serviços usando AWS Directory Service

Autorizando um AWS aplicativo em um Active Directory

AWS Directory Service concede permissões específicas para que os aplicativos selecionados se integrem perfeitamente ao seu Active Directory quando você autoriza um AWS aplicativo. AWS os aplicativos recebem apenas o acesso necessário para seu caso de uso. O conjunto de permissões internas concedidas a aplicações e administradores de aplicações após a autorização é fornecido abaixo:

> **Note**
>
> A `ds:AuthorizationApplication` permissão é necessária para autorizar um novo AWS aplicativo no Active Directory. As permissões para essa ação só devem ser fornecidas aos administradores que configuram integrações com o Directory Service.

- Leia o acesso aos dados de usuário, grupo, unidade organizacional, computador ou autoridade de certificação do Active Directory em todas as Unidades Organizacionais (UO) dos diretórios AWS Managed Microsoft AD, Simple AD, AD Connector, bem como domínios confiáveis do Managed AWS Microsoft AD, se permitido por uma relação de confiança.
- Grave acesso a usuários, grupos, membros de grupos, computadores ou dados da autoridade de certificação em sua unidade organizacional do AWS Managed Microsoft AD. Acesso de gravação a todas as UOs do Simple AD.

- Autenticação e gerenciamento de sessões de usuários do Active Directory para todos os tipos de diretório.

Alguns aplicativos AWS gerenciados do Microsoft AD, como Amazon RDS e Amazon FSx, se integram por meio de conexão de rede direta ao seu Active Directory. Nesse caso, as interações do diretório usam protocolos nativos do Active Directory, como LDAP e Kerberos. As permissões desses AWS aplicativos são controladas por uma conta de usuário do diretório criada na Unidade Organizacional AWS Reservada (OU) durante a autorização do aplicativo, que inclui gerenciamento de DNS e acesso total a uma OU personalizada criada para o aplicativo. Para usar esta conta, a aplicação exige permissões para a ação `ds:GetAuthorizedApplicationDetails` por meio das credenciais do chamador ou de um perfil do IAM.

Para obter mais informações sobre permissões de AWS Directory Service API, consulteAWS Directory Service Permissões de API: referência de ações, recursos e condições.

Para obter mais informações sobre como habilitar AWS aplicativos e serviços para o AWS Managed Microsoft AD, consultePermita o acesso a AWS aplicativos e serviços. Para obter mais informações sobre como habilitar AWS aplicativos e serviços para o AD Connector, consultePermita o acesso a AWS aplicativos e serviços. Para obter mais informações sobre como habilitar AWS aplicativos e serviços para o Simple AD, consultePermita o acesso a AWS aplicativos e serviços.

Desautorizando um AWS aplicativo em um Active Directory

Para remover as permissões de um AWS aplicativo acessar o Active Directory, a `ds:UnauthorizedApplication` permissão é necessária. Siga as etapas fornecidas pela aplicação para desativá-la.

Registro e monitoramento em AWS Directory Service

Como prática recomendada, monitore a sua organização para garantir que as alterações sejam registradas. Isso ajuda você a garantir que qualquer alteração inesperada possa ser investigada e que alterações indesejadas possam ser revertidas. AWS Directory Service atualmente oferece suporte aos dois AWS serviços a seguir para que você possa monitorar sua organização e a atividade que acontece dentro dela.

- Amazon CloudWatch - Você pode usar CloudWatch Eventos com o tipo de diretório AWS Managed Microsoft AD. Para ter mais informações, consulte Habilitar o encaminhamento de logs. Além disso, você pode usar CloudWatch métricas para monitorar o desempenho do controlador

de domínio. Para ter mais informações, consulte Determine quando adicionar controladores de domínio com métricas CloudWatch .

- AWS CloudTrail - Você pode usar CloudTrail com todos os tipos de AWS Directory Service diretórios. Para obter mais informações, consulte Logging AWS Directory Service API call with CloudTrail.

Validação de conformidade para AWS Directory Service

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o

Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).

- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Directory Service

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as Zonas de Disponibilidade, é possível projetar e operar aplicações e bancos de dados que executem o failover automaticamente entre as Zonas de Disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte infraestrutura AWS global.

Além da infraestrutura AWS global, AWS Directory Service oferece a capacidade de tirar instantâneos manuais dos dados a qualquer momento para ajudar a suportar suas necessidades de resiliência e backup de dados. Para ter mais informações, consulte Criar um snapshot ou restaurar seu diretório.

Segurança da infraestrutura em AWS Directory Service

Como serviço gerenciado, AWS Directory Service é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa chamadas de API AWS publicadas para acessar AWS Directory Service pela rede. Os clientes devem suportar o Transport Layer Security (TLS). Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter compatibilidade com conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece compatibilidade com esses modos.

Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount`global `aws:SourceArn`e as chaves de contexto nas políticas de recursos para limitar as permissões que

o AWS Directory Service for Microsoft Active Directory concede a outro serviço ao recurso. Se o valor de `aws:SourceArn` não contém ID da conta, como um ARN do bucket do Amazon S3, você deve usar ambas as chaves de contexto de condição global para limitar as permissões. Se você usa ambas as chaves de contexto de condição global, e o valor `aws:SourceArn` contém o ID da conta, o valor `aws:SourceAccount` e a conta no valor `aws:SourceArn` deverão utilizar a mesma ID de conta quando na mesma declaração de política. Use `aws:SourceArn` se quiser apenas um recurso associado a acessibilidade de serviço. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

Para o exemplo a seguir, o valor de `aws:SourceArn` deve ser um grupo de CloudWatch registros.

A maneira mais eficaz de se proteger do problema 'confused deputy' é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto no Microsoft AD AWS gerenciado para evitar o confuso problema auxiliar.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
    "Resource": [
      "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/YOUR_LOG_GROUP:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
```

```
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

No exemplo a seguir, o valor de `aws:SourceArn` deve ser um tópico do SNS em sua conta. Por exemplo, você pode usar algo como “ap-southeast-1” é sua região, “123456789012" é seu ID de cliente e" _d-966739499f” é o nome do tópico do Amazon SNS `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` que você criou. DirectoryMonitoring

A maneira mais eficaz de se proteger do problema ‘confused deputy’ é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto no Microsoft AD AWS gerenciado para evitar o confuso problema auxiliar.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": ["SNS:GetTopicAttributes",
     "SNS:SetTopicAttributes",
        "SNS:AddPermission",
     "SNS:RemovePermission",
     "SNS:DeleteTopic",
     "SNS:Subscribe",
     "SNS:ListSubscriptionsByTopic",
     "SNS:Publish"],
    "Resource": [
```

```
      "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

O exemplo a seguir mostra uma política de confiança do IAM para um perfil ao qual acesso ao console foi delegado. O valor de `aws:SourceArn` deve ser um recurso de diretório em sua conta. Para obter mais informações, consulte Tipos de recursos definidos por AWS Directory Service. Por exemplo, você pode usar `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890`, onde `123456789012` é seu ID de cliente e `d-1234567890` é o ID do diretório.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "sts:AssumeRole"
            ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

AWS Directory Service API e interface de endpoints Amazon VPC usando AWS PrivateLink

Você pode estabelecer uma conexão privada entre seus endpoints Amazon VPC e AWS Directory Service API criando uma interface VPC endpoint. Os endpoints de interface são desenvolvidos pelo AWS PrivateLink.

AWS PrivateLink permite que você acesse de forma privada as operações AWS Directory Service da API sem um gateway de internet, dispositivo NAT, conexão VPN ou AWS Direct Connect conexão. Tráfego entre sua VPC e o tráfego AWS Directory Service que não sai da AWS rede.

Cada endpoint de interface é representado por uma ou mais interfaces de rede elástica nas sub-redes. Para obter mais informações sobre a interface de rede elástica, consulte Interface de rede elástica no Guia do usuário do Amazon EC2.

Para obter mais informações sobre VPC endpoints, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia do usuário da Amazon VPC. Para obter mais informações sobre operações de AWS Directory Service API, consulte Referência de AWS Directory Service API.

Considerações sobre VPC endpoints

Antes de configurar uma interface VPC endpoint para endpoints de AWS Directory Service API, certifique-se de revisar Access and using AWS service (Serviço da AWS) an interface VPC endpoint no Guia.AWS PrivateLink

Todas as operações de AWS Directory Service API relevantes para o gerenciamento AWS Directory Service de recursos estão disponíveis em sua VPC usando. AWS PrivateLink

As políticas de endpoint VPC são compatíveis com endpoints da API Directory Service. Por padrão, o acesso total às operações da API do Directory Service é permitido por meio do endpoint. Para obter mais informações, consulte Controle o acesso aos endpoints da VPC usando políticas de endpoint no Guia do usuário da Amazon VPC.

Disponibilidade

AWS Directory Service oferece suporte a endpoints de VPC no seguinte: Regiões da AWS

Região da AWS disponibilidade

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- África (Cidade do Cabo)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Osaka)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Oeste do Canadá (Calgary)
- China (Pequim e Ningxia)
- Ásia-Pacífico (Hong Kong)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milão)
- Europe (Paris)
- Europa (Espanha)
- Europa (Estocolmo)
- Europa (Zurique)
- Israel (Tel Aviv)

- Oriente Médio (Barém)
- Oriente Médio (Emirados Árabes Unidos)
- América do Sul (São Paulo)
- AWS GovCloud (Leste dos EUA)
- AWS GovCloud (Oeste dos EUA)

Criação de um endpoint de interface para API AWS Directory Service

Você pode criar um endpoint de interface VPC para a AWS Directory Service API usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Create a VPC endpoint (Criar um endpoint da VPC) no Guia do AWS PrivateLink .

Crie um endpoint de interface para AWS Directory Service API usando o seguinte nome de serviço: `com.amazonaws.region.ds`

Exceto Regiões da AWS na China, se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API com AWS Directory Service o VPC endpoint usando seu nome DNS padrão para o, por exemplo. Região da AWS`ds.us-east-1.amazonaws.com` Para a China (Pequim e Ningxia) Regiões da AWS, você pode fazer solicitações de API com o VPC endpoint `ds-api.cn-north-1.amazonaws.com.cn` usando `ds-api.cn-northwest-1.amazonaws.com.cn` e, respectivamente.

Para obter mais informações, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia do usuário da Amazon VPC.

Criar uma política de VPC endpoint para a API AWS Directory Service

É possível anexar uma política de endpoint ao VPC endpoint que controla o acesso à API AWS Directory Service Essa política especifica as seguintes informações:

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

Para obter mais informações, consulte Controle o acesso aos endpoints da VPC usando políticas de endpoint no Guia do usuário da Amazon VPC.

Exemplo: política de VPC endpoint para ações de API AWS Directory Service

Veja a seguir um exemplo de uma política de endpoint para AWS Directory Service API. Quando você anexa essa política ao seu endpoint de interface, ela concede acesso às ações de AWS Directory Service API listadas para todos os diretores em todos os recursos.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:DescribeDirectories",
            "ds:DescribeCertificate",
         ],
         "Resource":"*"
      }
   ]
}
```

Exemplo: política de VPC endpoint que nega todo o acesso de um determinado endpoint Conta da AWS

A política de VPC endpoint a seguir nega a Conta da AWS *123456789012* todo o acesso aos recursos usando o endpoint. A política permite todas as ações de outras contas.

```
{
   "Statement": [
      {
         "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal:" "*"
      },
      {
        "Action": "*",
        "Effect": "Deny",
        "Resource": "*",
        "Principal": {
            "AWS": [
               "123456789012"
            ]
```

```
            }
        ]
}
```

Acordo de nível de serviço do AWS Directory Service

O AWS Directory Service é um serviço altamente disponível e é criado em uma infraestrutura gerenciada pela AWS. Ele tem o apoio de um Acordo de Nível de Serviço que define nossa política de disponibilidade do serviço.

Para obter mais informações, consulte o Acordo de nível de serviço do AWS Directory Service.

Disponibilidade da região para AWS Directory Service

A tabela a seguir fornece uma lista que descreve os endpoints específicos da região que são compatíveis com o tipo de diretório.

Nome da região	Região	Endpoint	Protocolo	AWS Microsoft AD gerenciado	AD Connector	Simple AD
Leste dos EUA (Norte da Virgínia)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 Sim	 Sim	 Sim
Leste dos EUA (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Oeste dos EUA (N. da Califórnia)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Oeste dos EUA (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 Sim	 Sim	 Sim

Nome da região	Região	Endpoint	Protocolo	AWS Microsoft AD gerenciado	AD Connector	Simple AD
África (Cidade do Cabo)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Ásia-Pacífico (Hong Kong)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Ásia-Pacífico (Hyderabad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Ásia-Pacífico (Jacarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Ásia-Pacífico (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Ásia-Pacífico (Mumbai	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 Sim	 Sim	 Não

Nome da região	Região	Endpoint	Protocolo	AWS Microsoft AD gerenciado	AD Connector	Simple AD
Ásia-Pacífico (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Ásia-Pacífico (Seul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 Sim	 Sim	 Não
Ásia-Pacífico (Singapura)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 Sim	 Sim	 Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 Sim	 Sim	 Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 Sim	 Sim	 Sim
Canadá (Central)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 Sim	 Sim	 Não

Nome da região	Região	Endpoint	Protocolo	AWS Microsoft AD gerenciado	AD Connector	Simple AD
Oeste do Canadá (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	Sim	Sim	Não
China (Pequim)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	Sim	Sim	Não
China (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	Sim	Sim	Não
Europa (Frankfurt)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	Sim	Sim	Não
Europa (Irlanda)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	Sim	Sim	Sim
Europa (Londres)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	Sim	Sim	Não
Europa (Milão)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	Sim	Sim	Não
Europa (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	Sim	Sim	Não

Nome da região	Região	Endpoint	Protocolo	AWS Microsoft AD gerenciado	AD Connector	Simple AD
Europa (Espanha)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	Sim	Sim	Não
Europa (Estocolmo)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	Sim	Sim	Não
Europa (Zurique)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	Sim	Sim	Não
Israel (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	Sim	Sim	Não
Oriente Médio (Barém)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	Sim	Sim	Não
Oriente Médio (Emirados Árabes Unidos)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	Sim	Sim	Não
América do Sul (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	Sim	Sim	Não

Nome da região	Região	Endpoint	Protocolo	AWS Microsoft AD gerenciado	AD Connector	Simple AD
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	anúncios. us-gov-west-1.amazonaws.com	HTTPS	 S	 S	 Não
AWS GovCloud (Leste dos EUA)	us-gov-east-1	anúncios. us-gov-east-1.amazonaws.com	HTTPS	 S	 S	 Não

Para obter informações sobre o uso AWS Directory Service na região AWS GovCloud (Oeste dos EUA) e na região AWS GovCloud (Leste dos EUA), consulte Endpoints de serviço.

Para obter informações sobre o uso AWS Directory Service nas regiões de Pequim e Ningxia, consulte Endpoints e ARNs para Amazon Web Services na China.

Compatibilidade do navegador

AWS aplicativos e serviços como Amazon WorkSpaces, Amazon Connect WorkMail, Amazon Chime, Amazon e AWS IAM Identity Center todos exigem credenciais de login válidas de um navegador compatível antes que você possa acessá-los. WorkDocs A tabela a seguir descreve apenas os navegadores e versões do navegador que são compatíveis para logins.

Navegador	Version (Versão)	Compatibilidade
Microsoft Edge	Últimas 3 versões	Compatível
Mozilla Firefox	Últimas 3 versões	Compatível
Google Chrome	Últimas 3 versões	Compatível
Apple Safari	Últimas 3 versões	Compatível

Agora que você verificou que está usando uma versão compatível do navegador, recomendamos que você também analise a seção a seguir para verificar se seu navegador foi configurado para usar a configuração do Transport Layer Security (TLS) exigida pela AWS.

O que é o TLS?

O TLS é um protocolo que navegadores da web e outros aplicativos usam para trocar dados com segurança por uma rede. O TLS garante que uma conexão com um endpoint remoto seja o endpoint pretendido por meio de criptografia e verificação de identidade de endpoint. As versões do TLS, até o momento, são TLS 1.0, 1.1, 1.2 e 1.3.

Quais versões do TLS são compatíveis com o Centro de Identidade do IAM

AWS aplicativos e serviços oferecem suporte a TLS 1.1, 1.2 e 1.3 para logins seguros. A partir de 30 de outubro de 2019, o TLS 1.0 não é mais compatível, por isso, é importante que todos os navegadores sejam configurados para oferecer suporte a TLS 1.1 ou superior. Isso significa que não será possível fazer login em aplicativos e serviços da AWS se você acessá-los enquanto o TLS 1.0 estiver habilitado. Para obter assistência fazer essa mudança, entre em contato com o administrador.

Como habilitar o suporte para versões do TLS em meu navegador

Depende do navegador. Geralmente, você pode encontrar essa configuração na área de configurações avançadas nas configurações do navegador. Por exemplo, no Internet Explorer, você encontrará várias opções de TLS em Propriedades da Internet, na guia Avançado e na seção Segurança. Verifique o site de ajuda do fabricante do navegador para obter instruções específicas.

Histórico do documento

A tabela a seguir descreve as alterações importantes feitas desde a última versão do Guia do Administrador do AWS Directory Service .

Alteração	Descrição	Data
Configurações da autenticação baseada em certificado	Conteúdo adicionado sobre duas novas configurações de segurança para o AWS Managed Microsoft AD.	11 de abril de 2023
AWS PrivateLink	Adição de conteúdo sobre AWS PrivateLink.	31 de março de 2023
Endpoints da VPC do Simple AD	Adição de conteúdo sobre quais endpoints da VPC não devem ser configurados.	25 de agosto de 2021
Endpoints da VPC do AD Connector	Adição de conteúdo sobre quais endpoints da VPC não devem ser configurados.	25 de agosto de 2021
Suporte ao cartão inteligente	Conteúdo adicionado sobre suporte para cartões inteligentes e Amazon WorkSpaces Application Manager na região AWS GovCloud (Oeste dos EUA)	1º de dezembro de 2020
Redefinição de senhas	Conteúdo adicionado sobre como redefinir senhas de usuário usando o AWS Management Console, Windows PowerShell AWS CLI e.	2 de janeiro de 2019

Compartilhamento de diretórios	Conteúdo adicionado sobre como usar o compartilhamento de diretórios com o AWS Managed Microsoft AD.	25 de setembro de 2018
Conteúdo migrado para o novo Guia do desenvolvedor do Amazon Cloud Directory	Conteúdo do Amazon Cloud Directory movido deste guia para o novo Guia do desenvolvedor do Amazon Cloud Directory.	21 de junho de 2018
Reformulação completa do sumário do guia de administração	Conteúdo reorganizado para abordar às necessidades do cliente de forma mais direta. Adição de novo conteúdo onde necessário.	5 de abril de 2018
AWS grupos delegados	Foi adicionada uma lista de grupos AWS delegados que podem ser atribuídos a usuários locais.	8 de março de 2018
Políticas de senha detalhadas	Adição de conteúdo sobre novas políticas de senhas.	5 de julho de 2017
Controladores de domínio adicionais	Conteúdo adicionado sobre como adicionar mais controladores de domínio ao seu diretório no AWS Managed Microsoft AD.	30 de junho de 2017
Tutoriais	Foram adicionados novos tutoriais para testar um ambiente de laboratório gerenciado do AWS Microsoft AD.	21 de junho de 2017

MFA com AWS Microsoft AD gerenciado	Conteúdo adicionado sobre o uso da MFA com o AWS Microsoft AD gerenciado.	13 de fevereiro de 2017
Amazon Cloud Directory	Adição de conteúdo sobre um novo tipo de diretório.	26 de janeiro de 2017
Extensões de esquema	Conteúdo adicionado sobre extensões de esquema com o AWS Directory Service for Microsoft Active Directory.	14 de novembro de 2016
Grande reorganização do Guia do AWS Directory Service Administrador	Conteúdo reorganizado para abordar às necessidades do cliente de forma mais direta.	14 de novembro de 2016
Notificações do SNS	Adição de conteúdo sobre notificações do SNS.	25 de fevereiro de 2016
Autorização e autenticação	Conteúdo adicionado sobre como usar o IAM com AWS Directory Service o.	25 de fevereiro de 2016
AWS Microsoft AD gerenciado	Conteúdo adicionado sobre o AWS Managed Microsoft AD e guias combinados em um único guia.	17 de novembro de 2015
Permitir que instâncias do Linux se associem a um diretório do Simple AD	Adição de conteúdo sobre como associar uma instância do Linux a um diretório do Simple AD.	23 de julho de 2015
Separação do guia	Divisão do Guia de administração do AWS Directory Service em guias separados.	14 de julho de 2015
Suporte à autenticação única	Adição de conteúdo sobre suporte à autenticação única.	31 de março de 2015

Novo guia	Esta é a primeira versão do Guia de administração do AWS Directory Service .	21 de outubro de 2014

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.