Guía de administración

AWS Directory Service

Version 1.0

AWS Directory Service: Guía de administración

Table of Contents

¿Qué es AWS Directory Service?

AWS Directory Service proporciona varias formas de usar Microsoft Active Directory (AD) con otros AWS servicios. Los directorios almacenan información sobre los usuarios, grupos y dispositivos, y los administradores los utilizan para administrar el acceso a la información y los recursos. AWS Directory Service ofrece varias opciones de directorio para los clientes que desean utilizar aplicaciones en la nube compatibles con Microsoft AD o el Protocolo ligero de acceso a directorios (LDAP) existentes. También ofrece las mismas opciones para los desarrolladores que necesiten un directorio para administrar usuarios, grupos, dispositivos y accesos.

¿Cuál debe elegir?

Puede elegir servicios de directorio con las características y la escalabilidad que mejor se adapten a sus necesidades. Utilice la siguiente tabla como ayuda para determinar qué opción de AWS Directory Service directorio funciona mejor para su organización.

¿Qué necesita hacer?	AWS Directory Service Opciones recomendadas
Necesito Active Directory o LDAP para mis aplicaciones en la nube	Utilice AWS Directory Service para Microsoft Active Directory (Standard Edition o Enterprise Edition) si necesita una versión real Microsoft Active Directory en la AWS nube que admita cargas Active Directory de trabajo compatibles o AWS aplicaciones y servicios como Amazon y WorkSpaces Amazon QuickSight, o si necesita compatibilidad con LDAP para aplicaciones Linux. Usa AD Connector si solo necesitas permitir que los usuarios locales inicien sesión en AWS las aplicaciones y los servicios con sus Active Directory credenciales. También puede usar AD Connector para unir las instancia s de Amazon EC2 a su dominio existenteActive Directory. Utilice Simple AD si necesita un directorio de bajo coste y escala con Active Directory compatibilidad básica que admita aplicaciones compatibles con Samba 4, o

¿Qué necesita hacer?	AWS Directory Service Opciones recomendadas
	si necesita compatibilidad con LDAP para aplicaciones compatibles con LDAP.
Desarrollo aplicaciones SaaS	Utilice Amazon Cognito si desarrolla aplicaciones SaaS a gran escala y necesita un directorio escalable para administrar y autenticar a sus suscriptores que funcione con identidades de redes sociales.

Para obtener más información sobre las opciones de AWS Directory Service directorio, consulte Cómo elegir soluciones en. Active DirectoryAWS

AWS Directory Service opciones

AWS Directory Service incluye varios tipos de directorios entre los que elegir. Para obtener más información, seleccione una de las siguientes pestañas:

AWS Directory Service for Microsoft Active Directory

También conocido como Microsoft AD AWS administrado, AWS Directory Service para Microsoft Active Directory funciona con un Microsoft Windows Server Active Directory (AD) real, administrado AWS en la AWS nube. Le permite migrar a la nube una amplia gama de aplicaciones compatibles con Active Directory. AWS AWS Microsoft AD administrado funciona con Microsoft SharePoint grupos de disponibilidad Microsoft SQL Server Always On y con muchas aplicaciones.NET. También es compatible con aplicaciones y servicios AWS gestionados, como Amazon WorkSpaces, Amazon WorkDocs QuickSight, Amazon Chime, Amazon Connect y Amazon Relational Database Service para (Amazon RDS paraSQL Server, Microsoft SQL Server Amazon RDS para y Amazon RDS Oracle para PostgreSQL).

AWS Managed Microsoft AD está aprobado para aplicaciones en la AWS nube que están sujetas al cumplimiento de la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) de EE. UU. o al Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) cuando habilita la conformidad para su directorio.

Todas las aplicaciones compatibles funcionan con las credenciales de usuario que usted almacena en Microsoft AD AWS administrado, o puede conectarse a su infraestructura de AD

existente con una confianza y utilizar las credenciales de un Active Directory entorno local o en EC2 Windows. Si une las instancias de EC2 a su Microsoft AD AWS administrado, sus usuarios pueden acceder a las cargas de trabajo de Windows en la AWS nube con la misma experiencia de inicio de sesión único (SSO) de Windows que cuando acceden a las cargas de trabajo de su red local.

AWS Microsoft AD administrado también admite casos de uso federados mediante Active Directory credenciales. Por sí solo, AWS Managed Microsoft AD le permite iniciar sesión en AWS Management Console. Con AWS IAM Identity Center, también puede obtener credenciales a corto plazo para usarlas con el AWS SDK y la CLI, y usar integraciones SAML preconfiguradas para iniciar sesión en muchas aplicaciones en la nube. Al agregar Microsoft Entra Connect (antes conocido comoAzure Active Directory Connect) y, opcionalmente, el Servicio de Active Directory federación (AD FS), puede iniciar sesión en Microsoft Office 365 y en otras aplicaciones en la nube con las credenciales almacenadas en AWS Managed Microsoft AD.

El servicio incluye características clave que le permiten ampliar el esquema, administrar políticas de contraseñas y habilitar las comunicaciones de LDAP seguro a través de capa de conexión segura (SSL)/Transport Layer Security (TLS). También puede habilitar la autenticación multifactor (MFA) para Microsoft AD AWS administrado a fin de proporcionar un nivel de seguridad adicional cuando los usuarios AWS accedan a las aplicaciones desde Internet. Como Active Directory es un directorio LDAP, también puede usar la autenticación gestionada de AWS Microsoft AD para Linux Secure Shell (SSH) y para otras aplicaciones habilitadas para LDAP.

AWS proporciona supervisión, instantáneas diarias y recuperación como parte del servicio: se agregan usuarios y grupos a AWS Microsoft AD administrado y se administra la política de grupo mediante Active Directory herramientas conocidas que se ejecutan en un Windows equipo unido al dominio de AWS Microsoft AD administrado. También puede escalar el directorio mediante la implementación de controladores de dominio adicionales y ayudar a mejorar el desempeño de las aplicaciones distribuyendo solicitudes a través de un gran número de controladores de dominio.

AWS Managed Microsoft AD está disponible en dos ediciones: Standard y Enterprise.

- Standard Edition: AWS Managed Microsoft AD (Standard Edition) está optimizado para servir como directorio principal para compañías pequeñas y medianas con hasta 5000 empleados. Le facilita suficiente capacidad de almacenamiento como para dar cabida a 30 000* objetos de directorio, como usuarios, grupos y equipos.
- Enterprise Edition: AWS Managed Microsoft AD (Enterprise Edition) está diseñado para su uso en grandes organizaciones y compañías con hasta 500 000* objetos de directorio.

* Los límites superiores son aproximaciones. Su directorio podría admitir más o menos objetos de directorio en función del tamaño de los mismos, y el comportamiento y las necesidades de rendimiento de sus aplicaciones.

Cuándo se debe usar

AWS Managed Microsoft AD es su mejor opción si necesita Active Directory funciones reales para soportar AWS aplicaciones o Windows cargas de trabajo, incluida Amazon Relational Database Service para. Microsoft SQL Server También es la mejor opción si quieres una versión independiente Active Directory en la AWS nube que sea compatible con Office 365 o si necesitas un directorio LDAP que dé soporte a tus aplicaciones de Linux. Para obtener más información, consulte AWS Microsoft AD gestionado.

AD Connector

AD Connector es un servicio de proxy que proporciona una forma sencilla de conectar AWS aplicaciones compatibles, como Amazon WorkSpaces QuickSight, Amazon y Amazon EC2 para las Windows Server instancias, a su entorno local existente. Microsoft Active Directory Con AD Connector, simplemente puede agregar una cuenta de servicio a suActive Directory. Conector AD también elimina la necesidad de sincronización de directorios y los costos y dificultades que conlleva alojar una infraestructura de federación.

Cuando añades usuarios a AWS aplicaciones como Amazon QuickSight, AD Connector lee los existentes Active Directory para crear listas de usuarios y grupos entre los que elegir. Cuando los usuarios inician sesión en las AWS aplicaciones, AD Connector reenvía las solicitudes de inicio de sesión a los controladores de Active Directory dominio locales para su autenticación. AD Connector funciona con muchas AWS aplicaciones y servicios WorkSpaces, como Amazon WorkDocs, Amazon QuickSight, Amazon, Amazon Chime, Amazon Connect y Amazon. WorkMail También puede unir sus Windows instancias EC2 a su Active Directory dominio local a través de AD Connector mediante una unión de dominio perfecta. AD Connector también permite a los usuarios acceder a los AWS recursos AWS Management Console y administrarlos iniciando sesión con sus Active Directory credenciales existentes. Conector AD no es compatible con RDS SQL Server.

También puede usar AD Connector para habilitar la autenticación multifactor (MFA) para los usuarios de AWS su aplicación conectándola a su infraestructura de MFA existente basada en RADIUS. Esto proporciona una capa adicional de seguridad cuando los usuarios obtienen acceso a las aplicaciones de AWS .

Con AD Connector, seguirás gestionando tu Active Directory negocio como lo haces ahora. Por ejemplo, puede añadir nuevos usuarios y grupos y actualizar las contraseñas mediante herramientas de Active Directory administración estándar en su entorno localActive Directory. Esto le ayuda a aplicar de forma coherente sus políticas de seguridad, como la caducidad de las contraseñas, el historial de contraseñas y los bloqueos de cuentas, independientemente de si los usuarios acceden a los recursos de forma local o en la AWS nube.

Cuándo se debe usar

AD Connector es la mejor opción si desea utilizar su directorio local existente con AWS servicios compatibles. Para obtener más información, consulte Conector de AD.

Simple AD

Simple AD es un Microsoft Active Directory directorio compatible AWS Directory Service que funciona con Samba 4. Simple AD admite Active Directory funciones básicas como cuentas de usuario, pertenencia a grupos, unirse a un dominio Linux o instancias EC2 Windows basadas en Linux, SSO basado en Kerberos y políticas de grupo. AWS proporciona supervisión, instantáneas diarias y recuperación como parte del servicio.

Simple AD es un directorio independiente en la nube que permite crear y administrar identidades de usuarios y administrar el acceso a las aplicaciones. Puede utilizar muchas aplicaciones y Active Directory herramientas conocidas que requieren funciones básicas. Active Directory Simple AD es compatible con las siguientes AWS aplicaciones: Amazon WorkSpaces WorkDocs, Amazon QuickSight, Amazon y Amazon WorkMail. También puede iniciar sesión en las cuentas AWS Management Console de usuario de Simple AD y administrar AWS los recursos.

Simple AD no admite la autenticación multifactorial (MFA), las relaciones de confianza, la actualización dinámica de DNS, las extensiones de esquema, la comunicación a través de LDAPS PowerShell , los cmdlets de AD ni la transferencia de funciones FSMO. Simple AD no es compatible con RDS SQL Server. Los clientes que necesiten las funciones de un directorio real Microsoft Active Directory o que tengan previsto utilizar su directorio con RDS SQL Server deberían utilizar AWS Microsoft AD administrado en su lugar. Compruebe que las aplicaciones que necesita sean totalmente compatibles con Samba 4 antes de usar Simple AD. Para obtener más información, visite https://www.samba.org.

Cuándo se debe usar

Puede usar Simple AD como un directorio independiente en la nube para admitir Windows cargas de trabajo que necesitan Active Directory funciones básicas, AWS aplicaciones compatibles

o para admitir cargas de trabajo de Linux que necesitan el servicio LDAP. Para obtener más información, consulte AD sencillo.

Amazon Cognito

Amazon Cognito es un directorio de usuarios que agrega inscripciones e inicios de sesión a su aplicación móvil o aplicación web utilizando grupos de usuarios de Amazon Cognito.

Cuándo se debe usar

También puede utilizar Amazon Cognito si necesita crear campos de registro personalizados y almacenar los metadatos en su directorio de usuarios. Este servicio totalmente administrado puede adaptarse para admitir cientos de millones de usuarios. Para obtener más información, consulte Grupos de usuarios de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.

Consulte Disponibilidad regional para AWS Directory Service para obtener una lista de los tipos de directorio admitidos por región.

Uso de Amazon EC2

Un conocimiento básico de Amazon EC2 es esencial para utilizar AWS Directory Service. Le recomendamos que empiece leyendo los siguientes temas:

- ¿Qué es Amazon EC2? en la Guía del usuario de Amazon EC2.
- Lanzamiento de instancias EC2 en la Guía del usuario de Amazon EC2.
- Grupos de seguridad en la Guía del usuario de Amazon EC2.
- ¿Qué es Amazon VPC? en la Guía del usuario de Amazon VPC.
- Adición de una puerta de enlace privada virtual de hardware a su VPC en la Guía del usuario de Amazon VPC.

Empezar con AWS Directory Service

Si aún no lo has hecho, también tendrás que crear una AWS cuenta y usar el AWS Identity and Access Management servicio para controlar el acceso.

Para trabajar con AWS Directory Service ellos, debe cumplir los requisitos previos de AWS Directory Service para Microsoft Active Directory, AD Connector o Simple AD. Para obtener más información, consulte AWS Requisitos previos de Microsoft AD gestionado, Requisitos previos de Conector AD, o Requisitos previos para Simple AD.

Inscríbase en un Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente al usuario root para realizar tareas que requieran dicho acceso.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Crea un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree uno para que no utilice el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Cree un usuario con acceso administrativo

1. Activar IAM Identity Center

   Consulte las instrucciones en Enabling AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En el Centro de identidades de IAM, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicie sesión como el usuario con acceso administrativo

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Asigne el acceso a usuarios adicionales

1. En el Centro de identidades de IAM, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos con privilegios mínimos.

Para obtener instrucciones, consulte Crear un conjunto de permisos en la Guía del usuario.AWS IAM Identity Center

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para obtener instrucciones, consulte Añadir grupos en la Guía del AWS IAM Identity Center usuario.

Más información

- Para obtener más información sobre cómo iniciar sesión AWS Management Console como usuario del Centro de Identidad de IAM, consulte Iniciar sesión en el portal de acceso al Centro de Identidad de IAM.
- Para obtener más información sobre cómo iniciar sesión AWS Management Console como usuario de IAM, consulte Iniciar sesión AWS Management Console como usuario de IAM.
- Para obtener más información sobre el uso de las políticas de IAM para controlar el acceso a sus AWS Directory Service recursos, consulte. Uso de políticas basadas en la identidad (políticas de IAM) para AWS Directory Service

AWS Microsoft AD gestionado

AWS Directory Service le permite ejecutar Microsoft Active Directory (AD) como un servicio gestionado. AWS Directory Service for Microsoft Active Directory, también conocido como AWS Managed Microsoft AD, funciona con Windows Server 2019. Al seleccionar e iniciar este tipo de directorio, se crea como un par de controladores de dominio de alta disponibilidad conectados a su nube privada virtual (Amazon VPC). Los controladores de dominio se ejecutan en distintas zonas de disponibilidad en una región de su elección. La supervisión y recuperación del host, la replicación de datos, las instantáneas y las actualizaciones de software se configuran y administran automáticamente.

Con Microsoft AD AWS administrado, puede ejecutar cargas de trabajo compatibles con directorios en la AWS nube, incluidas aplicaciones personalizadas basadas en .NET Microsoft SharePoint y SQL Server. También puede configurar una relación de confianza entre Microsoft AD AWS administrado en la AWS nube y su entorno local existente MicrosoftActive Directory, proporcionando a los usuarios y grupos acceso a los recursos de cualquiera de los dominios, mediante AWS IAM Identity Center.

AWS Directory Service facilita la configuración y la ejecución de directorios en la AWS nube o la conexión de sus AWS recursos con un entorno local Microsoft Active Directory existente. Una vez creado el directorio, puede usarlo para una diversas tareas:

- Administrar usuarios y grupos
- Proporcionar inicio de sesión único para aplicaciones y servicios
- Crear y aplicar políticas de grupo
- Simplifique la implementación y la administración de Linux y Microsoft Windows cargas de trabajo basadas en la nube
- Puede usar Microsoft AD AWS administrado para habilitar la autenticación multifactorial integrándola con su infraestructura de MFA existente basada en RADIUS para proporcionar una capa adicional de seguridad cuando los usuarios accedan a las aplicaciones. AWS
- Conéctese de forma segura a Amazon EC2, Linux e instancias Windows

> **Note**
>
> AWS gestiona las licencias de sus instancias de Windows servidor por usted; lo único que tiene que hacer es pagar las instancias que utilice. Tampoco es necesario comprar licencias

de acceso de cliente (CAL) adicionales de Windows Server, ya que el acceso está incluido en el precio. Cada instancia incluye dos conexiones remotas únicamente con fines de administración. Si necesita más de dos conexiones o si las necesita para fines distintos de la administración, es posible que tenga que incorporar licencias CAL adicionales de los Servicios de Escritorio remoto para usarlas en AWS.

Lee los temas de esta sección para empezar a crear un directorio AWS administrado de Microsoft AD, crear una relación de confianza entre Microsoft AD AWS administrado y tus directorios locales y ampliar tu esquema de Microsoft AD AWS administrado.

Temas

Artículos del blog AWS de seguridad relacionados

- Cómo delegar la administración del directorio AWS administrado de Microsoft AD a los usuarios de Active Directory locales
- Cómo configurar políticas de contraseñas aún más sólidas para ayudar a cumplir sus estándares de seguridad mediante el uso AWS Directory Service de Microsoft AD AWS administrado
- Cómo aumentar la redundancia y el rendimiento de su AWS Directory Service Microsoft AD AWS administrado mediante la adición de controladores de dominio
- Cómo habilitar el uso de escritorios remotos mediante la implementación del administrador de licencias de escritorio remoto de Microsoft en Microsoft AWS AD administrado
- Cómo acceder AWS Management Console mediante Microsoft AD AWS administrado y sus credenciales locales

- Cómo habilitar la autenticación multifactor para AWS los servicios mediante Microsoft AD AWS administrado y credenciales locales
- Cómo iniciar sesión fácilmente en los AWS servicios mediante el Active Directory local

Introducción a AWS Managed Microsoft AD

AWS Managed Microsoft AD crea un servidor 2019 totalmente administrado, Microsoft Active Directory Nube de AWS integrado y funciona con Windows Server 2019 y funciona en los niveles funcionales de bosque y dominio R2 de 2012. Cuando crea un directorio con Microsoft AD AWS administrado, AWS Directory Service crea dos controladores de dominio y agrega el servicio DNS en su nombre. Los controladores de dominio se crean en diferentes subredes de una Amazon VPC. Esta redundancia ayuda a garantizar que el directorio permanezca accesible incluso si se produce un error. Si necesita más controladores de dominio, puede añadirlos posteriormente. Para obtener más información, consulte Implementación de controladores de dominio adicionales.

Temas

AWS Requisitos previos de Microsoft AD gestionado

Para crear un Microsoft AD AWS gestionadoActive Directory, necesitas una Amazon VPC con lo siguiente:

- Dos subredes como mínimo. Cada una de las subredes debe estar en una zona de disponibilidad diferente.
- La VPC debe disponer de tenencia de hardware predeterminada.
- No puede crear un Microsoft AD AWS administrado en una VPC con direcciones del espacio de direcciones 198.18.0.0/15.

Si necesita integrar su dominio de Microsoft AD AWS administrado con un Active Directory dominio local existente, debe tener los niveles funcionales de bosque y dominio de su dominio local configurados en Windows Server 2003 o superior.

AWS Directory Service utiliza una estructura de dos VPC. Las instancias EC2 que componen su directorio se ejecutan fuera de su AWS cuenta y son administradas por. AWS Contienen dos adaptadores de red, `ETH0` y `ETH1`. `ETH0` es el adaptador de administración y se encuentra fuera de su cuenta. `ETH1` se crea dentro de su cuenta.

El rango IP de administración de la red ETH0 de su directorio es 198.18.0.0/15.

AWS IAM Identity Center requisitos previos

Si planea usar el Centro de identidades de IAM con Microsoft AD AWS administrado, debe asegurarse de que se cumpla lo siguiente:

- El directorio de Microsoft AD AWS administrado está configurado en la cuenta de administración de la AWS organización.
- Su instancia de IAM Identity Center se encuentra en la misma región en la que está configurado su directorio AWS gestionado de Microsoft AD.

Para obtener más información, consulte los requisitos previos del Centro de identidad de IAM en la Guía del AWS IAM Identity Center usuario.

Requisitos previos de la autenticación multifactor

Para admitir la autenticación multifactorial con su directorio de Microsoft AD AWS administrado, debe configurar su servidor de servicio de usuario telefónico de autenticación remota (RADIUS) local o basado en la nube de la siguiente manera para que pueda aceptar solicitudes de su directorio de AWS Microsoft AD administrado en. AWS

1. En su servidor RADIUS, cree dos clientes RADIUS para representar los dos controladores de dominio (DC) AWS administrados de Microsoft AD. AWS Debe configurar ambos clientes utilizando los siguientes parámetros comunes (su servidor RADIUS puede variar):
   - Dirección (DNS o IP): es la dirección DNS de uno de los DC AWS administrados de Microsoft AD. Ambas direcciones DNS se encuentran en la consola de AWS Directory Service, en la página de detalles del directorio AWS administrado de Microsoft AD en el que planea usar MFA. Las direcciones DNS que se muestran representan las direcciones IP de los dos DC AWS administrados de Microsoft AD que utilizan. AWS

> **Note**
>
> Si su servidor RADIUS es compatible con direcciones DNS, deberá crear una única configuración de cliente RADIUS. De lo contrario, deberá crear una configuración de cliente de RADIUS para cada controlador de dominio de AWS Managed Microsoft AD.

- Port number: configure el número de puerto donde su servidor RADIUS acepta conexiones de clientes RADIUS. El puerto para RADIUS estándar es 1812.
- Shared secret (Secreto compartido): escriba o genere el secreto compartido que el servidor RADIUS utilizará para conectar con los clientes de RADIUS.
- Protocolo: es posible que deba configurar el protocolo de autenticación entre los DC de Microsoft AD AWS administrados y el servidor RADIUS. Los protocolos admitidos son PAP, CHAP, MS-CHAPv1 y MS-CHAPv2. Se recomienda utilizar MS-CHAPv2, ya que es el que ofrece la mayor seguridad de las tres opciones.
- Application name: puede ser opcional en algunos servidores RADIUS y normalmente identifica la aplicación en los mensajes o en los informes.

2. Configure su red existente para permitir el tráfico entrante desde los clientes RADIUS (direcciones DNS de Microsoft AD DC AWS administradas, consulte el paso 1) al puerto de su servidor RADIUS.
3. Añada una regla al grupo de seguridad Amazon EC2 de su dominio gestionado de AWS Microsoft AD que permita el tráfico entrante desde la dirección DNS y el número de puerto del servidor RADIUS definidos anteriormente. Para obtener más información, consulte Agregar reglas a un grupo de seguridad en la Guía del usuario de EC2.

Para obtener más información sobre el uso de Microsoft AD AWS administrado con MFA, consulte. Habilite la autenticación multifactorial para Microsoft AWS AD administrado

Cree su Microsoft AD AWS administrado

Para crear un nuevo directorio, siga estos pasos. Antes de comenzar este procedimiento, asegúrese de haber completado los requisitos previos que se indican en AWS Requisitos previos de Microsoft AD gestionado.

Para crear un directorio de Microsoft AD AWS administrado

1. En el panel de navegación de la consola de AWS Directory Service, elija Directorios y, a continuación, elija Configurar directorio.
2. En la página Seleccionar tipo de directorio, elija AWS Managed Microsoft AD y, a continuación, elija Siguiente.
3. En la página Enter directory information (Especifique la información del directorio), facilite la siguiente información:

   Edición

   Elija entre la edición estándar o la edición empresarial de AWS Managed Microsoft AD. Para obtener más información acerca de las ediciones, consulte AWS Directory Service para Microsoft Active Directory.

   Nombre de DNS del directorio

   El nombre completo del directorio, como por ejemplo `corp.example.com`.

   > **Note**
   > Si planea usar Amazon Route 53 para DNS, el nombre de dominio de su Microsoft AD AWS administrado debe ser diferente al nombre de dominio de Route 53. Se pueden producir problemas de resolución de DNS si Route 53 y AWS Managed Microsoft AD comparten el mismo nombre de dominio.

   Nombre NetBIOS del directorio

   El nombre abreviado del directorio, como `CORP`.

   Descripción del directorio

   Descripción opcional del directorio.

   Contraseña de administrador

   Contraseña del administrador del directorio. Al crear el directorio, se crea también una cuenta de administrador con el nombre de usuario `Admin` y esta contraseña.

   La contraseña no puede incluir la palabra “admin”.

La contraseña del administrador del directorio distingue entre mayúsculas y minúsculas y debe tener 8 caracteres como mínimo y 64 como máximo. También debe contener al menos un carácter de tres de las siguientes categorías:

- Letras minúsculas (a-z)
- Letras mayúsculas (A-Z)
- Números (0-9)
- Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmar contraseña

Vuelva a escribir la contraseña de administrador.

4. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la siguiente información y, a continuación, elija Next (Siguiente).

   VPC

   VPC del directorio.

   Subredes

   Elija las subredes de los controladores de dominio. Las dos subredes deben estar en diferentes zonas de disponibilidad.

5. En la página Review & create (Revisar y crear), revise la información del directorio y haga los cambios que sean necesarios. Cuando la información sea correcta, seleccione Create directory (Crear directorio). Se tarda entre 20 y 40 minutos en crear el directorio. Una vez creado, el valor Status cambia a Active.

Qué se crea con su Active Directory AWS administrado de Microsoft AD

Al crear un Active Directory con Microsoft AD AWS administrado, AWS Directory Service realiza las siguientes tareas en su nombre:

- Crea y asocia automáticamente una interfaz de red elástica (ENI) a cada uno de sus controladores de dominio. Cada uno de estos ENI es esencial para la conectividad entre la VPC AWS Directory Service y los controladores de dominio y nunca debe eliminarse. Puede identificar todas las interfaces de red reservadas para su uso AWS Directory Service mediante la descripción: «interfaz de red AWS creada para el identificador del directorio». Para obtener más información, consulte Elastic Network Interfaces en la Guía del usuario de Amazon EC2. El servidor DNS

predeterminado del Microsoft AD AWS administrado Active Directory es el servidor DNS de la VPC en el enrutamiento entre dominios sin clase (CIDR) +2. Para obtener más información, consulte el servidor DNS de Amazon en la Guía del usuario de Amazon VPC.

> **Note**
>
> De forma predeterminada, los controladores de dominio se implementan en dos zonas de disponibilidad de una región y se conectan a su Amazon VPC (VPC). Las copias de seguridad se realizan automáticamente una vez al día y los volúmenes de Amazon EBS (EBS) se cifran para garantizar la seguridad de los datos en reposo. Los controladores de dominio que tienen errores se sustituyen automáticamente en la misma zona de disponibilidad con la misma dirección IP y se puede llevar a cabo una recuperación de desastres completa con la última copia de seguridad.

- Aprovisiona Active Directory dentro de la VPC mediante dos controladores de dominio para tolerancia a errores y alta disponibilidad. Se pueden aprovisionar más controladores de dominio para mayor resiliencia y rendimiento después de que el directorio se haya creado correctamente y esté activo. Para obtener más información, consulte Implementación de controladores de dominio adicionales.

> **Note**
>
> AWS no permite la instalación de agentes de supervisión en los controladores de dominio AWS gestionados de Microsoft AD.

- Crea un grupo de seguridad de AWS que establece reglas de red para el tráfico entrante y saliente de los controladores de dominio. La regla de salida predeterminada permite todas las ENI o instancias de tráfico asociadas al grupo de AWS seguridad creado. Las reglas de entrada predeterminadas solo permiten el tráfico a través de puertos requeridos por Active Directory desde cualquier origen (0.0.0.0/0). Las reglas 0.0.0.0/0 no introducen vulnerabilidades de seguridad, ya que el tráfico a los controladores de dominio se limita al tráfico procedente de su VPC, de otras VPC interconectadas o de redes a las que se haya conectado mediante Transit AWS Direct Connect Gateway AWS o Virtual Private Network. Para mayor seguridad, las ENI que se crean no tienen direcciones IP elásticas conectadas a ellas y el usuario no tiene permiso para asociar una IP elástica a esas ENI. Por lo tanto, el único tráfico entrante que puede comunicarse con su Microsoft AD AWS administrado es el tráfico de VPC local y enrutado por VPC. Tenga mucho cuidado al intentar cambiar estas reglas, ya que podría perder la capacidad de comunicarse con

los controladores de dominio. Para obtener más información, consulte Mejores prácticas para Microsoft AD AWS administrado. De forma predeterminada, se crean las siguientes reglas del grupo de AWS seguridad:

Reglas entrantes

Protocolo	Intervalo de puertos	Origen	Tipo de tráfico	Uso de Active Directory
ICMP	N/A	0.0.0.0/0	Ping	LDAP Keep Alive, DFS
TCP y UDP	53	0.0.0.0/0	DNS	Autenticación de usuarios y equipos, resolución de nombres, relaciones de confianza
TCP y UDP	88	0.0.0.0/0	Kerberos	Autenticación de usuarios y equipos, relaciones de confianza de nivel de bosque
TCP y UDP	389	0.0.0.0/0	LDAP	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza

Protocolo	Intervalo de puertos	Origen	Tipo de tráfico	Uso de Active Directory
TCP y UDP	445	0.0.0.0/0	SMB/CIFS	Replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza
TCP y UDP	464	0.0.0.0/0	Cambiar/e stablecer contraseña de Kerberos	Replicación, autenticación de usuarios y equipos, relaciones de confianza
TCP	135	0.0.0.0/0	Replicación	RPC, EPM
TCP	636	0.0.0.0/0	LDAP SSL	Directorio, replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza
TCP	1024 - 65535	0.0.0.0/0	RPC	Replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza

Protocolo	Intervalo de puertos	Origen	Tipo de tráfico	Uso de Active Directory
TCP	3268 - 3269	0.0.0.0/0	LDAP GC y LDAP GC SSL	Directorio, replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza
UDP	123	0.0.0.0/0	Hora de Windows	Hora de Windows, relaciones de confianza
UDP	138	0.0.0.0/0	DFSN & NetLogon	DFS, política de grupo
Todos	Todos	sg-###### ############	All Traffic	

Reglas salientes

Protocolo	Rango de puerto	Destino	Tipo de tráfico	Uso de Active Directory
Todos	Todos	sg-###### ############	All Traffic	

- Para obtener más información acerca de los puertos y protocolos que utiliza Active Directory, consulte Información general del servicio y requisitos de puertos de red para Windows en la documentación de Microsoft.
- Crea una cuenta de administrador para el directorio con el nombre de usuario Admin y la contraseña especificada. Esta cuenta se encuentra en la unidad organizativa Users (por ejemplo,

Corp > Users). Utiliza esta cuenta para administrar su directorio en la AWS nube. Para obtener más información, consulte Permisos para la cuenta de administrador.

> **Important**
>
> Asegúrese de guardar esta contraseña. AWS Directory Service no almacena esta contraseña y no se puede recuperar. Sin embargo, puede restablecer una contraseña desde la AWS Directory Service consola o mediante la ResetUserPasswordAPI.

- Crea las tres unidades organizativas (OU) siguientes en la raíz del dominio:

Nombre de OU	Descripción
AWS Grupos delegados	Almacena todos los grupos que puede usar para delegar permisos AWS específicos a sus usuarios.
AWS Reservado	Almacena todas las cuentas específicas de AWS administración.

<su-nombre-de-dominio>	El nombre de esta OU se basa en el nombre NetBIOS que escribió cuando creó el directori o. Si no especificó un nombre NetBIOS, este será de forma predeterminada la primera parte del nombre de DNS del directorio (por ejemplo, en el caso de corp.example.com, el nombre NetBIOS sería corp). Esta OU es propiedad de todos sus objetos de directorio AWS relacionados AWS y los contiene, sobre los que tiene el control total. Esta OU contiene dos unidades organizativas secundarias de forma predeterminada: Computers (Equipos) y Users (Usuarios). Por ejemplo:
	• Corp
	  • Computers
	  • Usuarios

- Crea los siguientes grupos en la OU de grupos AWS delegados:

Nombre del grupo	Descripción
AWS Operadores de cuentas delegadas	Los miembros de este grupo de seguridad tienen una capacidad de administración de cuentas limitada, por ejemplo, a restablecer contraseñas
AWS Administradores de activación delegados basados en Active Directory	Los miembros de este grupo de seguridad pueden crear objetos de activación de licencias por volumen de Active Directory, lo que permite a las empresas activar equipos mediante una conexión con sus dominios.
AWS Agregar estaciones de trabajo a los usuarios del dominio por delegación	Los miembros de este grupo de seguridad puede unir 10 equipos a un dominio.
AWS Administradores delegados	Los miembros de este grupo de seguridad pueden administrar Microsoft AD AWS administrado, tener el control total de todos los objetos de la unidad organizativa y administrar los grupos contenidos en la unidad organizativa de grupos AWS delegados.
AWS La persona delegada puede autenticar objetos	Los miembros de este grupo de seguridad tienen la posibilidad de autenticarse en los recursos informáticos de la unidad organizat iva AWS reservada (solo es necesaria para los objetos locales con confianza habilitada para la autenticación selectiva).

Nombre del grupo	Descripción
AWS La persona delegada puede autentica rse en los controladores de dominio	Los miembros de este grupo de seguridad tienen la capacidad de autenticarse en los recursos del equipo en la unidad organizat iva de controladores de dominio (solo se necesitan para objetos locales con relacione s de confianza habilitadas para autenticación selectiva).
AWS Administradores delegados de por vida de los objetos eliminados	Los miembros de este grupo de seguridad pueden modificar el DeletedObjectLifetime objeto MSDS, que define cuánto tiempo estará disponible un objeto eliminado para su recuperación en la papelera de reciclaje de AD.
AWS Administradores delegados de sistemas de archivos distribuidos	Los miembros de este grupo de seguridad pueden agregar y eliminar espacios de nombres FRS, DFS-R y DFS.
AWS Administradores de sistemas de nombres de dominio delegados	Los miembros de este grupo de seguridad pueden administrar el DNS integrado de Active Directory.
AWS Administradores delegados del protocolo de configuración dinámica de host	Los miembros de este grupo de seguridad pueden autorizar los servidores DHCP de Windows en la compañía.
AWS Administradores de autoridades de certificación empresariales delegadas	Los miembros de este grupo de seguridad pueden implementar y administrar la infraestr uctura de la entidad de certificación de empresa de Microsoft.
AWS Administradores delegados de políticas de contraseñas detalladas	Los miembros de este grupo de seguridad pueden modificar las políticas de contraseñas específicas creadas previamente.

Nombre del grupo	Descripción
AWS Administradores de FSx delegados	Los miembros de este grupo de seguridad tienen la capacidad de administrar los recursos de Amazon FSx.
AWS Administradores de políticas de grupo delegados	Los miembros de este grupo de seguridad pueden realizar tareas de administración de las políticas de grupo (crear, editar, eliminar, vincular, etc.).
AWS Administradores delegados de la delegación de Kerberos	Los miembros de este grupo de seguridad pueden habilitar la delegación en los objetos de equipos y cuentas de usuario.
AWS Administradores de cuentas de servicios gestionados delegados	Los miembros de este grupo de seguridad pueden crear y eliminar cuentas de servicio administradas.
AWS Dispositivos delegados que no cumplen con la normativa MS-NPRC	Los miembros de este grupo de seguridad no podrán exigir comunicaciones por canales seguros con los controladores de dominio. Este grupo es para cuentas de equipos.
AWS Administradores del servicio de acceso remoto delegado	Los miembros de este grupo de seguridad pueden agregar y eliminar servidores RAS del grupo de servidores RAS e IAS.
AWS Delegated Replicate Directory cambia de administrador	Los miembros de este grupo de seguridad pueden sincronizar la información del perfil de Active Directory con SharePoint el servidor.
AWS Administradores de servidores delegados	Los miembros de este grupo de seguridad se incluyen en el grupo de administradores locales en todos los equipos unidos al dominio.

Nombre del grupo	Descripción
AWS Administradores de sitios y servicios delegados	Los miembros de este grupo de seguridad pueden cambiar el nombre del objeto Default-First-Site-Name en los sitios y servicios de Active Directory.
AWS Administradores de administración de sistemas delegados	Los miembros de este grupo de seguridad pueden crear y administrar objetos en el contenedor de administración del sistema.
AWS Administradores de licencias delegados de Terminal Server	Los miembros de este grupo de seguridad pueden agregar y eliminar servidores de licencias de Terminal Server del grupo de servidores de licencias de Terminal Server.
AWS Administradores de sufijos de nombre principal de usuario delegado	Los miembros de este grupo de seguridad pueden agregar y eliminar sufijos de nombre principal de usuario.

- Crea y aplica los siguientes objetos de política de grupo (GPO):

> **Note**
>
> No tiene permiso para eliminar, modificar o desvincular estos GPO. Esto se debe a su diseño, ya que están reservados para su AWS uso. Si es necesario, puede vincularlos a las unidades organizativas que controle.

Nombre de política de grupo	Aplica a	Descripción
Política de dominio predeterminada	Dominio	Incluye la contraseña de dominio y las políticas Kerberos.
ServerAdmins	Todas las cuentas de equipo que no sean controladores de dominios	Añade los «administradores de servidores AWS delegados» como miembros

Nombre de política de grupo	Aplica a	Descripción
		del grupo BUILTIN\ Administrators.
AWS Política reservada: usuario	AWS Cuentas de usuario reservadas	Establece la configuración de seguridad recomendada en todas las cuentas de usuario de la unidad organizativa AWS reservada.
AWS Política de Active Directory administrada	Todos los controladores de dominio	Establece la configuración de seguridad recomendada en todos los controladores de dominio.
TimePolicyNT5DS	Todos los controladores de dominio que no sean PDCe	Establece todas las políticas de tiempo de controladores de dominio que no sean PDCe para utilizar la hora de Windows (NT5DS).
TimePolicyPDC	El controlador de dominio PDCe	Establece la política de tiempo del controlador de dominio PDCe para utilizar el protocolo de tiempo de red (NTP).
Política predeterminada de controladores de dominio	No se utiliza	Aprovisionada durante la creación del dominio, se utiliza en su lugar la política de Active Directory AWS administrada.

Si desea ver la configuración de cada GPO, puede hacerlo desde una instancia de Windows unida a un dominio con la Consola de administración de políticas de grupo (GPMC) habilitada.

Permisos para la cuenta de administrador

Al crear un AWS directorio de Directory Service para Microsoft Active Directory, AWS crea una unidad organizativa (OU) para almacenar todos los grupos y cuentas AWS relacionados. Para obtener más información acerca de esta unidad organizativa, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD. Esto incluye la cuenta Admin. La cuenta Admin tiene permisos para llevar a cabo las siguientes actividades administrativas comunes en la unidad organizativa:

- Agregar, actualizar o eliminar usuarios, grupos y equipos. Para obtener más información, consulte Administración de usuarios y grupos en AWS Managed Microsoft AD.
- Añadir recursos a su dominio, como servidores de archivos o de impresión y, a continuación, asignar permisos para esos recursos a usuarios y grupos dentro de la unidad organizativa.
- Crear unidades organizativas y contenedores adicionales.
- Delegar la autoridad de unidades organizativas y contenedores adicionales. Para obtener más información, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.
- Crear y enlazar políticas de grupo.
- Restaurar objetos eliminados de la papelera de reciclaje de Active Directory.
- Ejecute los Windows PowerShell módulos de Active Directory y DNS en el servicio web de Active Directory.
- Crear y configurar cuentas de servicio administradas por grupos. Para obtener más información, consulte Cuentas de servicio administradas por grupos.
- Configurar una delegación limitada por Kerberos. Para obtener más información, consulte Delegación limitada de Kerberos.

La cuenta Admin también tiene derechos para realizar las siguientes actividades en todo el dominio:

- Administrar configuraciones DNS (agregar, quitar o actualizar registros, zonas y programas de envío).
- Ver logs de eventos DNS
- Ver logs de eventos de seguridad

Solo las acciones que se indican aquí se pueden realizar en la cuenta Admin. La cuenta Admin también carece de permisos para cualquier acción relacionada con el directorio fuera de su unidad organizativa específica, como en la unidad organizativa principal.

> **Important**
>
> AWS Los administradores de dominio tienen acceso administrativo completo a todos los dominios en los que están alojados AWS. Consulte su acuerdo AWS y las preguntas frecuentes sobre protección de AWS datos para obtener más información sobre cómo AWS gestiona el contenido, incluida la información de los directorios, que almacena en AWS los sistemas.

> **Note**
>
> Le recomendamos que no elimine ni cambie el nombre de esta cuenta. Si ya no desea utilizar la cuenta, le recomendamos que establezca una contraseña larga (64 caracteres aleatorios, como máximo) y, a continuación, deshabilite la cuenta.

Cuentas con privilegios de administrador de la empresa y administrador del dominio

AWS cambia automáticamente la contraseña de administrador integrada por una contraseña aleatoria cada 90 días. Cada vez que se solicita la contraseña de administrador integrada para uso humano, se crea un AWS ticket y se registra en el AWS Directory Service equipo. Las credenciales de la cuenta se cifran y se gestionan a través de canales seguros. Además, las credenciales de la cuenta de administrador solo las puede solicitar el equipo AWS Directory Service de administración.

Para realizar la gestión operativa de su directorio, AWS tiene el control exclusivo de las cuentas con privilegios de administrador empresarial y administrador de dominio. Esto incluye el control exclusivo de la cuenta de administrador de Active Directory. AWS protege esta cuenta automatizando la administración de contraseñas mediante el uso de una bóveda de contraseñas. Durante la rotación automática de la contraseña de administrador, AWS crea una cuenta de usuario temporal y le otorga privilegios de administrador de dominio. Esta cuenta temporal se usa como respaldo en caso de que se produzca un error de rotación en la cuenta del administrador. Tras rotar AWS correctamente la contraseña de administrador, AWS elimina la cuenta de administrador temporal.

Normalmente, el directorio AWS funciona completamente mediante la automatización. En el caso de que un proceso de automatización no pueda resolver un problema operativo, es AWS posible que necesite que un ingeniero de soporte inicie sesión en su controlador de dominio (DC) para realizar el diagnóstico. En estos raros casos, AWS implementa un sistema de solicitudes/notificaciones para conceder el acceso. En este proceso, la AWS automatización crea una cuenta de usuario de tiempo limitado en el directorio que tiene permisos de administrador de dominio. AWS asocia la cuenta de usuario al ingeniero asignado para trabajar en su directorio. AWS registra esta asociación en nuestro sistema de registro y proporciona al ingeniero las credenciales que debe utilizar. Todas las acciones realizadas por el ingeniero se registran en los registros de eventos de Windows. Cuando transcurre el tiempo asignado, la automatización elimina la cuenta de usuario.

Puede monitorizar las acciones administrativas de la cuenta mediante la característica de reenvío de registros del directorio. Esta función le permite reenviar los eventos de AD Security a su CloudWatch sistema, donde puede implementar soluciones de monitoreo. Para obtener más información, consulte Habilitación del reenvío de registros.

Todos los ID de eventos de seguridad 4624, 4672 y 4648 se registran cuando alguien inicia sesión en un centro de distribución de forma interactiva. Puede ver el registro de eventos de seguridad de Windows de cada controlador de dominio mediante el Visor de eventos de Microsoft Management Console (MMC) desde un equipo Windows unido a un dominio. También puede Habilitación del reenvío de registros enviar todos los registros de eventos de seguridad a CloudWatch los registros de su cuenta.

Es posible que, de vez en cuando, veas usuarios creados y eliminados en la OU AWS reservada. AWS es responsable de la administración y la seguridad de todos los objetos de esta unidad organizativa y de cualquier otra unidad organizativa o contenedor en los que no hayamos delegado permisos de acceso y administración. Es posible que vea las creaciones y eliminaciones en esa unidad organizativa. Esto se debe a que AWS Directory Service utiliza la automatización para cambiar la contraseña del administrador del dominio de forma regular. Cuando se rota la contraseña, se crea una copia de seguridad en caso de que se produzca un error en la rotación. Una vez que la rotación se lleva a cabo correctamente, la cuenta de respaldo se elimina automáticamente. Además, en el raro caso de que se necesite un acceso interactivo a los centros de distribución para solucionar problemas, se crea una cuenta de usuario temporal para que la utilice un AWS Directory Service ingeniero. Cuando el ingeniero complete su trabajo, se eliminará la cuenta de usuario temporal. Tenga en cuenta que cada vez que se solicitan credenciales interactivas para un directorio, se notifica al equipo AWS Directory Service de administración.

Conceptos clave de AWS Managed Microsoft AD

Sacará el máximo partido de AWS Managed Microsoft AD si se familiariza con los siguientes conceptos clave.

Temas

Esquema de Active Directory

Un esquema es la definición de atributos y clases que forman parte de un directorio distribuido y es similar a los campos y las tablas de una base de datos. Los esquemas incluyen un conjunto de reglas que determinan el tipo y el formato de los datos que se pueden añadir o incluir en la base de datos. La clase User es un ejemplo de un valor class que se almacena en la base de datos. Algunos ejemplos de atributos de la clase User pueden incluir el nombre, apellidos, número de teléfono, etc.

Elementos del esquema

Los atributos, las clases y los objetos son los elementos básicos utilizados para crear definiciones de objetos en el esquema. A continuación se ofrece información detallada sobre los elementos de esquema que es importante que conozca antes de empezar el proceso de ampliación del esquema de AWS Managed Microsoft AD.

Atributos

Cada atributo de esquema, que es similar a un campo en una base de datos, tiene varias propiedades que definen las características del atributo. Por ejemplo, la propiedad LDAP que utilizan los clientes para leer y escribir el atributo es `LDAPDisplayName`. La propiedad `LDAPDisplayName` debe ser única en todos los atributos y clases. Para obtener una lista completa de las características de atributos, consulte Characteristics of Attributes en el sitio web de MSDN. Si desea obtener instrucciones adicionales sobre cómo crear un atributo, consulte Defining a New Attribute en el sitio web de MSDN.

Clases

Las clases se parecen a las tablas de una base de datos, y también tienen varias propiedades que es necesario definir. Por ejemplo, `objectClassCategory` define la categoría de clase. Para obtener una lista completa de las características de clase, consulte Characteristics of Object Classes en el sitio web de MSDN. Para obtener más información sobre cómo crear una nueva clase, consulte Defining a New Class en el sitio web de MSDN.

Identificador de objeto (OID)

Cada clase y atributo deben tener un OID exclusivo para todos los objetos. Los proveedores de software deben obtener su propio OID para garantizar la unicidad. La unicidad evita conflictos en el supuesto de que se utilice el mismo atributo en más de una solicitud para finalidades diferentes. Para garantizar la originalidad, puede obtener un OID raíz de una autoridad de registro de nombres de ISO. También puede obtener un OID básico de Microsoft. Para obtener más información sobre los OID y cómo obtenerlos, consulte Identificadores de objetos en el sitio web de MSDN.

Atributos vinculados a esquemas

Algunos atributos están vinculados a dos clases, con vínculos de paso y retroceso. Un excelente ejemplo de ello son los grupos. Si mira un grupo, verá los miembros de ese grupo; si echa un vistazo a un usuario, verá a qué grupos pertenece. Cuando añada un usuario a un grupo, Active Directory creará un vínculo al grupo y después Active Directory añadirá un vínculo para volver del grupo al usuario. Se debe generar un identificador de vínculo único al crear un atributo que se vinculará. Para obtener más información, consulte Linked Attributes en el sitio web de MSDN.

Temas relacionados

- Cuándo debería ampliar su esquema de AWS Managed Microsoft AD
- Tutorial: Ampliación del esquema de Microsoft AD AWS administrado

Aplicación de parches y mantenimiento de AWS Managed Microsoft AD

AWS Directory Service para Microsoft Active Directory, también conocido como AWS DS para AWS Managed Microsoft AD, en realidad es Microsoft Active Directory Domain Services (AD DS), entregado como un servicio administrado. El sistema utiliza Microsoft Windows Server 2019 para los controladores de dominio (DC) y AWS les agrega software para administrar servicios. AWS actualiza (aplica parches) a los DC para agregar nuevas funcionalidades y mantener el software de Microsoft

Windows Server al día. Durante el proceso de aplicación de parches, el directorio continúa disponible para su uso.

Asegurar la disponibilidad

De forma predeterminada, cada directorio consta de dos DC, cada uno de ellos instalado en una zona de disponibilidad diferente. Si lo desea, puede agregar DC para aumentar aún más la disponibilidad. Para los entornos críticos que necesitan alta disponibilidad y tolerancia a errores, recomendamos implementar centros de distribución adicionales. AWSparchea los DC de forma secuencial, tiempo durante el cual el DC que AWS está parcheando activamente no está disponible. En caso de que uno o más de sus DC esté fuera de servicio temporalmente, AWS retrasa la aplicación de parches hasta que haya al menos dos DC operativos en el directorio. Esta función le permite utilizar el resto de los DC en funcionamiento durante el proceso de aplicación de parches, que suele tardar entre 30 y 45 minutos por cada DC, aunque puede variar. Para garantizar que las aplicaciones puedan obtener acceso a un DC en funcionamiento en caso de que uno o varios DC no estén disponibles por cualquier motivo, incluida la aplicación de parches, estas deberían utilizar el servicio de localización de DC de Windows y no utilizar direcciones de DC estáticas.

Cómo funciona la programación de aplicación de parches

Para mantener el software de Microsoft Windows Server actualizado en los DC, AWS utiliza actualizaciones de Microsoft. Como cada mes Microsoft ofrece paquetes acumulativos de parches para Windows Server, AWS hace todo lo posible para probar y aplicar dichos paquetes a todos los DC de los clientes en el plazo de tres semanas naturales. Además, AWS revisa las actualizaciones que Microsoft publica fuera del paquete mensual acumulativo en función de su aplicabilidad a los DC y su urgencia. En el caso de los parches de seguridad que Microsoft clasifica como críticos o importantes, y que son relevantes para los DC, AWS hace todo lo posible para probarlos e implementarlos en un plazo de cinco días.

Cuentas de servicio administradas por grupos

Con Windows Server 2012, Microsoft introdujo un nuevo método que los administradores pueden utilizar para administrar cuentas de servicio llamado “cuentas de servicio administradas por grupos (gMSA)”. Con las gMSA, los administradores de servicios ya no tienen que administrar manualmente la sincronización de contraseñas entre las instancias de servicio. En cambio, un administrador podría simplemente crear una gMSA en Active Directory y, a continuación, configurar varias instancias de servicio para utilizar esa única gMSA.

Para conceder permisos de tal forma que los usuarios de AWS Managed Microsoft AD puedan crear una gMSA, debe agregar sus cuentas como miembro del grupo de seguridad Administradores delegados de AWS para cuentas de servicio administradas. De forma predeterminada, la cuenta de administrador es miembro de este grupo. Para obtener más información sobre las GMSA, consulte Descripción general de las cuentas de servicio gestionadas por grupos en el sitio web de Microsoft TechNet .

Artículo relacionado del blog de AWS sobre seguridad

- Cómo Microsoft AD administrado por AWS contribuye a simplificar la implementación y a mejorar la seguridad de aplicaciones .NET integradas en Active Directory

Delegación limitada de Kerberos

La delegación limitada de Kerberos es una característica de Windows Server. Esta característica otorga a los administradores del servicio la capacidad de especificar y aplicar límites de confianza en una aplicación limitando el alcance hasta el que pueden actuar los servicios de esta última en representación de un usuario. Esto puede resultar útil cuando es preciso configurar qué cuentas del servicio de frontend pueden delegar en sus servicios de backend. La delegación limitada de Kerberos también evita que la gMSA se conecte a cualquier servicio en nombre de sus usuarios de Active Directory, con lo que se evita la posibilidad de abusos por parte de un desarrollador deshonesto.

Por ejemplo, supongamos que el usuario jsmith inicia sesión en una aplicación de recursos humanos. Quiere que SQL Server aplique los permisos de base de datos de jsmith. Sin embargo, de forma predeterminada, SQL Server abre la conexión a la base de datos con las credenciales de la cuenta de servicio que aplican hr-app-service los permisos en lugar de los permisos configurados por jsmith. Debe permitir que la aplicación de pago de nóminas de recursos humanos obtenga acceso a la base de datos de SQL Server con las credenciales de jsmith. Para ello, habilita la delegación restringida de Kerberos para la cuenta de hr-app-service servicio en el directorio de AWS Microsoft AD administrado en. AWS Cuando jsmith inicie sesión, Active Directory facilitará un ticket de Kerberos que Windows utilizará automáticamente cuando jsmith intente obtener acceso a otros servicios en la red. La delegación de Kerberos permite a la hr-app-service cuenta reutilizar el vale Kerberos de jsmith al acceder a la base de datos y, por lo tanto, aplicar los permisos específicos de jsmith al abrir la conexión a la base de datos.

Para conceder permisos que permitan a los usuarios de AWS Managed Microsoft AD configurar la delegación limitada de Kerberos, debe agregar sus cuentas como miembro del grupo de seguridad

Administradores delegados de AWS para la delegación Kerberos. De forma predeterminada, la cuenta de administrador es miembro de este grupo. Para obtener más información sobre la delegación restringida de Kerberos, consulte Descripción general de la delegación restringida de Kerberos en el sitio web de Microsoft. TechNet

La delegación restringida basada en recursos se introdujo con Windows Server 2012. Proporciona al administrador del servicio backend la capacidad de configurar la delegación restringida para el servicio.

Mejores prácticas para Microsoft AD AWS administrado

Estas son algunas sugerencias y pautas que debe tener en cuenta para evitar problemas y aprovechar al máximo Microsoft AD AWS administrado.

Configuración: requisitos previos

Plantéese estas directrices antes de crear el directorio.

Compruebe que tena el tipo de directorio correcto

AWS Directory Service proporciona varias formas de usarlo Microsoft Active Directory con otros AWS servicios. Puede elegir el servicio de directorio con las características que necesita con un costo que se adapte a su presupuesto:

- AWS Directory Service para Microsoft Active Directory es un servicio gestionado y Microsoft Active Directory alojado en la AWS nube con muchas funciones. AWS Microsoft AD administrado es la mejor opción si tiene más de 5000 usuarios y necesita establecer una relación de confianza entre un directorio AWS hospedado y sus directorios locales.
- AD Connector simplemente conecta su entorno local existente Active Directory a AWS. Conector AD es la mejor opción si desea utilizar su directorio en las instalaciones con los servicios de AWS .
- Simple AD es un directorio de bajo coste y escala con Active Directory compatibilidad básica. Admite 5000 usuarios o menos, aplicaciones compatibles con Samba 4 y compatibilidad LDAP para aplicaciones compatibles con LDAP.

Para obtener una comparación más detallada de AWS Directory Service las opciones, consulte¿Cuál debe elegir?.

Asegúrese de que sus VPC y sus instancias se hayan configurado correctamente

Para gestionar y utilizar sus directorios, así como conectarse a ellos, debe configurar correctamente las VPC a las que están asociados los directorios. Consulte AWS Requisitos previos de Microsoft AD gestionado, Requisitos previos de Conector AD o Requisitos previos para Simple AD para obtener información sobre la seguridad de VPC y los requisitos de red.

Si está añadiendo una instancia a su dominio, asegúrese de que dispone de conectividad y acceso remoto a la instancia, tal y como se describe en Unir una instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory.

Sea consciente de sus límites

Obtenga información sobre los distintos límites de su tipo de directorio específico. El almacenamiento disponible y el tamaño total de los objetos son las únicas limitaciones en cuanto al número de objetos que puede almacenar en el directorio. Consulte cualquiera de las opciones AWS Cuotas administradas de Microsoft AD, Cuotas de Conector AD o Cuotas de Simple AD para obtener más información sobre el directorio que ha elegido.

Comprenda la configuración y el uso de los grupos de AWS seguridad de su directorio

AWS crea un grupo de seguridad y lo adjunta a las interfaces de red elásticas del controlador de dominio de su directorio. Este grupo de seguridad bloquea el tráfico innecesario al controlador de dominio, pero permite el necesario para las comunicaciones de Active Directory. AWS configura el grupo de seguridad para abrir solo los puertos necesarios para las comunicaciones de Active Directory. En la configuración predeterminada, el grupo de seguridad acepta el tráfico a estos puertos desde cualquier dirección IP. AWS adjunta el grupo de seguridad a las interfaces de los controladores de dominio a las que se puede acceder desde las VPC emparejadas o redimensionadas. A estas interfaces no se puede acceder desde Internet aunque modifique las tablas de enrutamiento, cambie las conexiones de red a la VPC y configure el servicio NAT Gateway. Como tal, solo las instancias y los equipos que tengan una ruta de red en la VPC pueden acceder al directorio. Esto simplifica la configuración, eliminando el requisito de configurar rangos de direcciones específicos. En su lugar, se configuran rutas y grupos de seguridad en la VPC que permiten el tráfico únicamente a partir de instancias y equipos de confianza.

Modificación del grupo de seguridad del directorio

Si desea aumentar la seguridad de los grupos de seguridad de sus directorios, puede modificarlos para que acepten tráfico de una lista más restrictiva de direcciones IP. Por ejemplo, puede cambiar

las direcciones aceptadas desde 0.0.0.0/0 hasta un rango de CIDR que sea específico de una sola subred o un solo equipo. De forma similar, podría optar por restringir las direcciones de destino con las que puedan comunicarse sus controladores de dominio. Realice esos cambios únicamente si comprende completamente cómo funcionan los filtros de los grupos de seguridad. Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias de Linux en la Guía del usuario de Amazon EC2. Los cambios incorrectos pueden provocar la pérdida de comunicación con los ordenadores e instancias previstos. AWS recomienda no intentar abrir puertos adicionales al controlador de dominio, ya que esto reduce la seguridad del directorio. Lea detenidamente el Modelo de responsabilidad compartida de AWS.

> **Warning**
>
> Técnicamente, puede asociar los grupos de seguridad que utiliza el directorio a otras instancias EC2 que cree. Sin embargo, no AWS recomienda esta práctica. AWS puede tener motivos para modificar el grupo de seguridad sin previo aviso para satisfacer las necesidades funcionales o de seguridad del directorio gestionado. Estos cambios afectan a cualquier instancia a la que asocie el grupo de seguridad del directorio. Además, al asociar el grupo de seguridad del directorio a sus instancias EC2 se crea un posible riesgo de seguridad para sus instancias EC2. El grupo de seguridad del directorio acepta tráfico en los puertos necesarios de Active Directory desde cualquier dirección IP. Si asocia este grupo de seguridad a una instancia EC2 con una dirección IP pública conectada a Internet, cualquier equipo en Internet puede comunicarse con su instancia EC2 en los puertos abiertos.

Configuración: creación del directorio

A continuación se indican algunas sugerencias que debe tener en cuenta en el momento de crear su directorio.

Recuerde su ID de administrador y su contraseña

Cuando se configura el directorio, se proporciona la contraseña de la cuenta de administrador. Ese ID de cuenta es Admin de AWS Managed Microsoft AD. Recuerde la contraseña que cree para esta cuenta; de lo contrario, no podrá añadir objetos a su directorio.

Crear un conjunto de opciones de DHCP

Le recomendamos que cree un conjunto de opciones de DHCP para su AWS Directory Service directorio y que asigne el conjunto de opciones de DHCP a la VPC en la que se encuentra su

directorio. De esta forma, las instancias de la VPC pueden apuntar al dominio especificado y los servidores DNS pueden resolver sus nombres de dominio.

Para obtener más información sobre las opciones de DHCP, consulte Crear o cambiar un conjunto de opciones de DHCP.

Habilite la configuración del reenviador condicional

La siguiente configuración de reenvío condicional Guarde este reenviador condicional en Active Directory y replique de la siguiente manera: debe estar habilitado. Al habilitar esta configuración, se evitará que la configuración del reenviador condicional desaparezca cuando se sustituya un nodo debido a un fallo de infraestructura o a un fallo por sobrecarga.

Implementación de controladores de dominio adicionales

De forma predeterminada, AWS crea dos controladores de dominio que existen en zonas de disponibilidad independientes. Esto proporciona resistencia a errores durante la aplicación de parches de software y otros eventos que pueden provocar que no se pueda obtener acceso a un controlador de dominio o no esté disponible. Le recomendamos que implemente controladores de dominio adicionales para aumentar aún más la resiliencia y garantizar el rendimiento de escalado ascendente en caso de que se produzca un evento a largo plazo que afecte al acceso a un controlador de dominio o a una zona de disponibilidad.

Para obtener más información, consulte Utilice el servicio de localización de DC de Windows.

Comprender restricciones de nombre de usuario para aplicaciones de AWS

AWS Directory Service es compatible con la mayoría de los formatos de caracteres que se pueden utilizar en la construcción de nombres de usuario. Sin embargo, hay restricciones de caracteres que se aplican a los nombres de usuario que se utilizarán para iniciar sesión en AWS aplicaciones, como WorkSpaces Amazon WorkMail, WorkDocs Amazon o Amazon. QuickSight Estas restricciones requieren que no se utilicen los siguientes caracteres:

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

> **Note**
>
> El símbolo @ se permite siempre que preceda a un sufijo UPN.

Uso del directorio

Estas son algunas sugerencias que tener en cuenta al utilizar su directorio.

No modificar los usuarios, los grupos, ni las unidades organizativas predefinidos

Al AWS Directory Service lanzar un directorio, AWS crea una unidad organizativa (OU) que contiene todos los objetos del directorio. Esta unidad organizativa, que tiene el nombre de NetBIOS que escribió al crear el directorio, se encuentra en la raíz del dominio. La raíz del dominio es propiedad de y está gestionada por AWS. También se crean varios grupos y un usuario administrativo.

No mueva, elimine ni modifique de ningún otro modo estos objetos predefinidos. Si lo hace, puede hacer que su directorio sea inaccesible tanto para usted como para. AWS Para obtener más información, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD.

Unirse a dominios de manera automática

Al lanzar una instancia de Windows que va a formar parte de un AWS Directory Service dominio, suele ser más fácil unirse al dominio como parte del proceso de creación de la instancia en lugar de añadirla manualmente más adelante. Para unirse automáticamente a un dominio, solo tiene que seleccionar el directorio correcto para Domain join directory al lanzar una nueva instancia. Puede encontrar detalles en Unir sin problemas una instancia de Amazon EC2 para Windows a su AWS Microsoft AD gestionado Active Directory.

Configurar relaciones de confianza correctamente

Al configurar una relación de confianza entre el directorio AWS administrado de Microsoft AD y otro directorio, tenga en cuenta estas pautas:

- El tipo de relación de confianza debe coincidir en ambos lados (bosque o externo)
- Asegúrese de que la dirección de la relación de confianza esté configurada correctamente si se utiliza una relación de confianza unidireccional (saliente en el dominio origen de la confianza, entrante en el dominio destino de la confianza)

- Los nombres de dominio completos (FQDN) y los nombres NetBIOS deben ser únicos entre bosques/dominios

Para más información e instrucciones específicas sobre cómo configurar una relación de confianza, consulte Creación de una relación de confianza.

Administración del directorio

Tenga en cuenta estas sugerencias para gestionar su directorio.

Seguimiento del rendimiento de su controlador de dominio

Para ayudar a optimizar las decisiones de escalado y mejorar la resiliencia y el rendimiento de los directorios, le recomendamos que utilice CloudWatch métricas. Para obtener más información, consulte Supervisión de sus controladores de dominio con métricas de rendimiento.

Para obtener instrucciones sobre cómo configurar las métricas del controlador de dominio mediante la CloudWatch consola, consulte Cómo automatizar el escalado AWS administrado de Microsoft AD en función de las métricas de uso en el blog AWS de seguridad.

Planifique cuidadosamente las extensiones del esquema

Debe aplicar cuidadosamente las extensiones del esquema para indexar el directorio para las consultas importantes y frecuentes. Tenga cuidado de no sobreindexar el directorio, ya que los índices consumen espacio en el directorio y los valores indexados que cambian rápidamente pueden provocar problemas de desempeño. Para añadir índices, debe crear un archivo de formato ligero de intercambio de directorios (LDIF) del protocolo ligero de acceso a directorios (LDAP) y extender el cambio de esquema. Para obtener más información, consulte Ampliar el esquema.

Acerca de los equilibradores de carga

No utilices un balanceador de carga delante de los puntos finales de Microsoft AD AWS administrados. Microsoft diseñó Active Directory (AD) para su uso con un algoritmo de detección de controladores de dominio (DC) que encuentra el DC operativo con mayor capacidad de respuesta sin balanceo de carga externo. Los balanceadores de carga de red externos detectan incorrectamente los DC activos y pueden hacer que la aplicación se envíe a un DC que se está iniciando, pero que no está listo para su uso. Para obtener más información, consulte Equilibradores de carga y Active Directory en Microsoft, TechNet donde se recomienda corregir las aplicaciones para que usen Active Directory correctamente en lugar de implementar balanceadores de carga externos.

Haga una copia de seguridad de la instancia

Si decide añadir manualmente una instancia a un AWS Directory Service dominio existente, primero haga una copia de seguridad o tome una instantánea de esa instancia. Esto es especialmente importante a la hora de unirse a una instancia de Linux. Algunos de los procedimientos utilizados para agregar una instancia, si no se realizan correctamente, pueden hacer que la instancia resulte inaccesible o inservible. Para obtener más información, consulte Creación de una instantánea o restauración del directorio.

Configuración de la mensajería SNS

Con Amazon Simple Notification Service (Amazon SNS), puede recibir mensajes de correo electrónico o de texto (SMS) cuando cambie el estado del directorio. Se le notificará si el directorio pasa de un estado Activo a Deteriorado o Inoperable. También recibirá una notificación cuando el directorio vuelva a estar en estado activo.

Recuerde también que si tiene un tema de SNS del que recibe mensajes AWS Directory Service, antes de eliminarlo de la consola de Amazon SNS, debe asociar su directorio a un tema de SNS diferente. En caso contrario, se arriesga a perder importantes mensajes de estado del directorio. Para obtener información sobre cómo configurar Amazon SNS, consulte Configurar las notificaciones de estado del directorio con Amazon SNS.

Aplicación de la configuración del servicio de directorio

AWS Microsoft AD administrado le permite personalizar su configuración de seguridad para cumplir con sus requisitos de cumplimiento y seguridad. AWS Microsoft AD administrado implementa y mantiene la configuración en todos los controladores de dominio de su directorio, incluso al agregar nuevas regiones o controladores de dominio adicionales. Puede configurar y aplicar estas opciones de seguridad a todos los directorios nuevos y existentes. Puede hacerlo en la consola siguiendo los pasos de la UpdateSettings API Editar la configuración de seguridad del directorio o a través de ella.

Para obtener más información, consulte Establecimiento de la configuración de seguridad del directorio.

Elimine las aplicaciones de Amazon Enterprise antes de eliminar un directorio

Antes de eliminar un directorio asociado a una o más aplicaciones empresariales de Amazon, WorkSpaces como Amazon WorkSpaces Application Manager, Amazon WorkDocs, Amazon o Amazon WorkMail Relational Database Service (Amazon RDS), primero debe eliminar cada

aplicación. AWS Management Console Para obtener más información sobre cómo eliminar estas aplicaciones, consulte Elimine su Microsoft AD AWS administrado.

Utilizar clientes SMB 2.x al acceder a los recursos compartidos SYSVOL y NETLOGON

Los ordenadores cliente utilizan el bloque de mensajes del servidor (SMB) para acceder a los recursos compartidos SYSVOL y NETLOGON en los controladores de dominio gestionados de AWS Microsoft AD para la política de grupo, los scripts de inicio de sesión y otros archivos. AWS Managed Microsoft AD solo es compatible con SMB versión 2.0 (SMBv2) y versiones posteriores.

Los protocolos SMBv2 y versiones más recientes agregan una serie de características que mejoran el rendimiento del cliente y aumentan la seguridad de los controladores de dominio y los clientes. Este cambio sigue las recomendaciones del United Stated Computer Emergency Readiness Team y Microsoft para deshabilitar SMBv1.

> **Important**
>
> Si actualmente utiliza clientes SMBv1 para tener acceso a los recursos compartidos SYSVOL y NETLOGON de su controlador de dominio, debe actualizar esos clientes para utilizar SMBv2 o versiones posteriores. Su directorio funcionará correctamente, pero sus clientes SMBv1 no podrán conectarse a los recursos compartidos SYSVOL y NETLOGON de sus controladores de dominio gestionados de AWS Microsoft AD y tampoco podrán procesar la política de grupo.

Los clientes SMBv1 funcionarán con cualquier otro servidor de archivos compatible con SMBv1 que tenga. Sin embargo, le AWS recomienda que actualice todos sus servidores y clientes SMB a SMBv2 o a una versión más reciente. Para obtener más información sobre cómo deshabilitar SMBv1 y actualizarlo a las versiones SMB más recientes en sus sistemas, consulte estas publicaciones en Microsoft y en la documentación. TechNet Microsoft

Seguimiento de conexiones remotas SMBv1

Puede revisar el registro de eventos de Microsoft-Windows-SMBServer/Audit Windows conectándose de forma remota al controlador de dominio administrado de AWS Microsoft AD; cualquier evento de este registro indica conexiones SMBv1. A continuación se muestra un ejemplo de la información que puede ver en uno de estos registros:

Acceso SMB1

Dirección del cliente: ###.###.###.###

Directrices:

Este evento indica que un cliente intentó acceder al servidor mediante SMB1. Para dejar de auditar el acceso a SMB1, utilice el cmdlet Set-. Windows PowerShell SmbServerConfiguration

Programación de las aplicaciones

Antes de programar sus aplicaciones, tenga en cuenta lo siguiente:

Utilice el servicio de localización de DC de Windows

Al desarrollar aplicaciones, utilice el servicio de localización de Windows DC o el servicio DNS dinámico (DDNS) de su AWS Microsoft AD administrado para localizar los controladores de dominio (DC). No incluya la dirección de un DC en el código de las aplicaciones. El servicio de localización de DC ayuda a garantizar la distribución de la carga de directorios y le permite aprovechar el escalado horizontal añadiendo controladores de dominio a su implementación. Si vincula la aplicación a un DC fijo y se somete a una operación de aplicación de parches o de recuperación a dicho DC, la aplicación perderá el acceso al DC en lugar de utilizar uno de los DC restantes. Además, la inclusión de un DC en el código de la aplicación puede provocar que dicho DC se sobrecargue. En casos graves, esto puede hacer que el DC deje de responder. En estos casos, la automatización de AWS directorios también puede marcar el directorio como dañado y desencadenar procesos de recuperación que sustituyan al DC que no responde.

Pruebas de carga antes de la puesta en producción

Asegúrese de hacer pruebas de laboratorio con objetos y solicitudes que sean representativos de su carga de trabajo de producción para confirmar que el directorio puede adaptarse a la carga de su aplicación. Si necesita capacidad adicional, pruebe con DC adicionales para que las solicitudes se distribuyan entre los DC disponibles. Para obtener más información, consulte Implementación de controladores de dominio adicionales.

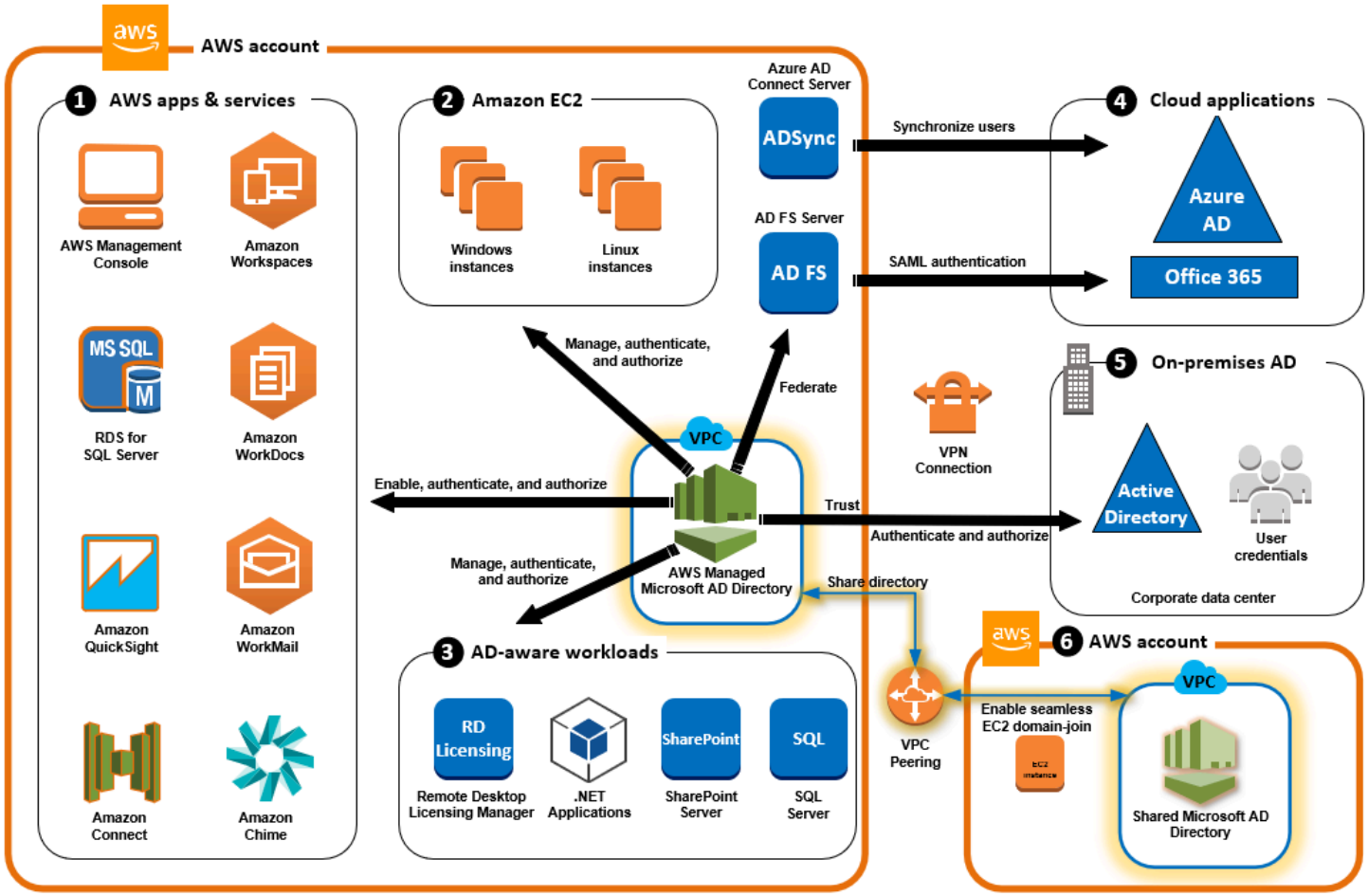
Uso de consultas LDAP eficientes

Las consultas amplias de LDAP a un controlador de dominio con decenas de miles de objetos pueden consumir un número importante de ciclos de CPU en un único DC, lo que se traduce en una sobrecarga. Esto podría afectar a las aplicaciones que comparten el mismo DC durante la consulta.

Casos de uso de Microsoft AD AWS administrado

Con Microsoft AD AWS administrado, puede compartir un único directorio para varios casos de uso. Por ejemplo, puede compartir un directorio para autenticar y autorizar el acceso de las aplicaciones .NET, Amazon RDS para SQL Server con la autenticación de Windows habilitada y Amazon Chime para mensajería y videoconferencias.

En el siguiente diagrama se muestran algunos de los casos de uso del directorio AWS administrado de Microsoft AD. Estos incluyen la posibilidad de conceder a sus usuarios acceso a aplicaciones en la nube externas y permitir que los usuarios de Active Directory locales administren los recursos de la AWS nube y tengan acceso a ellos.



Utilice Microsoft AD AWS administrado para cualquiera de los siguientes casos de uso empresarial.

Temas

- Caso de uso 1: inicie sesión en AWS aplicaciones y servicios con credenciales de Active Directory
- Caso de uso 2: Administración de instancias de Amazon EC2

- Caso de uso 3: proporcione servicios de directorio a sus cargas de trabajo compatibles con Active Directory
- Caso de uso 4: para Office 365 y otras aplicaciones AWS IAM Identity Center en la nube
- Caso de uso 5: extienda su Active Directory local a la nube AWS
- Caso de uso 6: comparta su directorio para unir sin problemas las instancias de Amazon EC2 a un dominio de todas las cuentas AWS

Caso de uso 1: inicie sesión en AWS aplicaciones y servicios con credenciales de Active Directory

Puede habilitar varias AWS aplicaciones y servicios AWS Client VPN, como Amazon Chime AWS Management ConsoleAWS IAM Identity Center, Amazon Connect, Amazon FSx, Amazon, Amazon RDS for SQL Server, QuickSightAmazon, Amazon, WorkDocs WorkMailAmazon WorkSpaces, y utilizar AWS su directorio gestionado de Microsoft AD. Al habilitar una AWS aplicación o un servicio en su directorio, los usuarios pueden acceder a la aplicación o el servicio con sus credenciales de Active Directory.

Por ejemplo, puede permitir que los usuarios inicien sesión en él AWS Management Console con sus credenciales de Active Directory. Para ello, habilite la aplicación AWS Management Console as en su directorio y, a continuación, asigne los usuarios y grupos de Active Directory a las funciones de IAM. Cuando los usuarios inician sesión en AWS Management Console, asumen una función de IAM para administrar AWS los recursos. Esto facilita la concesión de acceso a sus usuarios a la AWS Management Console sin necesidad de configurar y administrar una infraestructura de SAML independiente.

Para mejorar aún más la experiencia del usuario final, puedes habilitar las funciones de inicio de sesión único para Amazon WorkDocs, que ofrecen a tus usuarios la posibilidad de acceder a Amazon WorkDocs desde un ordenador conectado al directorio sin tener que introducir sus credenciales por separado.

Puedes conceder acceso a las cuentas de usuario de tu directorio o de tu Active Directory local para que puedan iniciar sesión en él AWS Management Console o AWS CLI utilizar sus credenciales y permisos existentes para gestionar los AWS recursos mediante la asignación de funciones de IAM directamente a las cuentas de usuario existentes.

Integración de FSx for Windows File Server AWS con Managed Microsoft AD

La integración de FSx for Windows File Server AWS con Microsoft AD administrado proporciona un sistema de archivos de protocolo de bloque de mensajes de servidor (SMB) nativo totalmente administrado y basado en Microsoft Windows que le permite mover fácilmente sus aplicaciones y clientes basados en Windows (que utilizan almacenamiento de archivos compartido) a. AWS Aunque FSx para Windows File Server se puede integrar con una instancia de Microsoft Active Directory autogestionado, no analizaremos este escenario aquí.

Casos de uso y recursos comunes de Amazon FSx

En esta sección se proporciona una referencia a los recursos sobre las integraciones habituales de FSx for Windows File Server con casos de uso de AWS Managed Microsoft AD. Cada uno de los casos de uso de esta sección comienza con una configuración básica de AWS Managed Microsoft AD y FSx para Windows File Server. Para obtener más información acerca de cómo crear y configurar el rol, consulte:

- Introducción a AWS Managed Microsoft AD
- Introducción a Amazon FSx

FSx para Windows File Server como almacenamiento persistente en contenedores de Windows

Amazon Elastic Container Service (ECS) ya admite los contenedores de Windows en las instancias de contenedor que se lanzan desde la AMI de Windows Server optimizada para Amazon ECS. Las instancias de contenedor de Windows utilizan su propia versión del agente de contenedor de Amazon ECS. En la AMI de Windows Server optimizada para Amazon ECS, el agente de contenedor de Amazon ECS se ejecuta como un servicio en el host.

Amazon ECS admite la autenticación de Active Directory para contenedores de Windows a través de un tipo especial de cuenta de servicio denominada cuenta de servicio administrada de grupo (gMSA). Dado que los contenedores de Windows no se pueden unir a un dominio, debe configurar un contenedor de Windows para que se ejecute con gMSA.

Elementos relacionados

- Uso de FSx para Windows File Server como almacenamiento persistente en contenedores de Windows
- Cuentas de servicio administradas por grupos

Soporte para Amazon AppStream 2.0

Amazon AppStream 2.0 es un servicio de streaming de aplicaciones totalmente gestionado. Proporciona una gama de soluciones para que los usuarios guarden datos y accedan a ellos a través de sus aplicaciones. Amazon FSx con AppStream 2.0 proporciona una unidad de almacenamiento persistente personal mediante Amazon FSx y se puede configurar para proporcionar una carpeta compartida para acceder a archivos comunes.

Elementos relacionados

- Tutorial 4: Uso de Amazon FSx con Amazon 2.0 AppStream
- Uso de Amazon FSx con Amazon 2.0 AppStream
- Uso de Active Directory con 2.0 AppStream

Compatibilidad con Microsoft SQL Server

FSx para Windows File Server se puede utilizar como opción de almacenamiento para Microsoft SQL Server 2012 (a partir de la versión 11.x de 2012) y las bases de datos del sistema más recientes (incluidas Master, Model, MSDB y TempDB), así como para las bases de datos de usuarios de Database Engine.

Elementos relacionados

- Instalación de SQL Server con almacenamiento compartido de archivos SMB
- Simplificación de las implementaciones de alta disponibilidad de Microsoft SQL Server mediante FSx para Windows File Server
- Cuentas de servicio administradas por grupos

Compatibilidad con carpetas de inicio y perfiles de usuario itinerantes

FSx para Windows File Server se puede utilizar para almacenar datos de las carpetas principales de los usuarios de Active Directory y de Mis documentos en una ubicación central. FSx para Windows File Server también se puede utilizar para almacenar datos de perfiles de usuario itinerantes.

Elementos relacionados

- Los directorios principales de Windows se simplifican con Amazon FSx
- Implementación de perfiles de usuario itinerantes

- Uso de FSx for Windows File Server con WorkSpaces

Compatibilidad con el uso compartido de archivos en red

Los recursos compartidos de archivos en red de FSx para Windows File Server proporcionan una solución de uso compartido de archivos gestionada y escalable. Un caso de uso son las unidades asignadas para clientes que se pueden crear manualmente o mediante una política de grupo.

Elementos relacionados

- Tutorial 6: escalado horizontal del rendimiento con particiones
- Asignación de unidades
- Uso de FSx for Windows File Server con WorkSpaces

Compatibilidad con la instalación de software de políticas grupales

Como el tamaño y el rendimiento de la carpeta SYSVOL son limitados, se recomienda evitar almacenar datos como los archivos de instalación de software en esa carpeta. Como posible solución a esto, FSx para Windows File Server se puede configurar para almacenar todos los archivos de software que se instalan mediante la política de grupo.

Elementos relacionados

- Utilice la política de grupo para instalar software de forma remota

Compatibilidad de destino de Windows Server Backup

FSx para Windows File Server se puede configurar como unidad de destino en Windows Server Backup mediante el recurso compartido de archivos UNC. En este caso, debe especificar la ruta UNC a su FSx para Windows File Server en lugar de al volumen EBS adjunto.

Elementos relacionados

- Recuperación del estado del sistema del servidor

Amazon FSx también admite el uso compartido de directorios gestionado de AWS Microsoft AD. Para obtener más información, consulte:

- Compartir el directorio

- Uso de Amazon FSx con AWS Microsoft AD gestionado en una VPC o cuenta diferente

Integración de Amazon RDS con Microsoft AWS AD administrado

Amazon RDS admite la autenticación externa de usuarios de bases de datos que usan Kerberos con Microsoft Active Directory. Kerberos es un protocolo de autenticación de red que usa tickets y criptografía de clave simétrica para eliminar la necesidad de transmitir contraseñas a través de la red. La compatibilidad de Amazon RDS con Kerberos y Active Directory ofrece beneficios de inicio de sesión único y autenticación centralizada de usuarios de bases de datos, por lo que puede mantener sus credenciales de usuario de Active Directory.

Para empezar con este caso de uso, primero tendrá que configurar una configuración básica de AWS Managed Microsoft AD y Amazon RDS.

- Introducción a AWS Managed Microsoft AD
- Introducción a Amazon RDS

Todos los casos de uso a los que se hace referencia a continuación comenzarán con una base de Microsoft AD y Amazon RDS AWS gestionados y tratarán sobre cómo integrar Amazon RDS con AWS Microsoft AD gestionado.

- Uso de la autenticación de Windows con una instancia de base de datos de Amazon RDS para SQL Server
- Uso de la autenticación de Kerberos para MySQL
- Uso de la autenticación de Kerberos con Amazon RDS para Oracle
- Uso de la autenticación de Kerberos con Amazon RDS para PostgreSQL

Amazon RDS también admite la compartición de directorios AWS gestionada de Microsoft AD. Para obtener más información, consulte:

- Compartir el directorio
- Unión de las instancias de base de datos de Amazon RDS en distintas cuentas a un único dominio compartido

Para obtener más información sobre cómo unir Amazon RDS para SQL Server a Active Directory, consulte Unión de Amazon RDS para SQL Server a su Active Directory autogestionado.

Aplicación .NET que utiliza Amazon RDS para SQL Server con cuentas de servicio administradas de grupo

Puede integrar Amazon RDS para SQL Server con una aplicación.NET básica y cuentas de servicio administradas por grupos (gMSA). Para obtener más información, consulte Cómo Microsoft AD AWS administrado ayuda a simplificar la implementación y mejorar la seguridad de las aplicaciones.NET integradas en Active Directory

Caso de uso 2: Administración de instancias de Amazon EC2

Con las conocidas herramientas de administración de Active Directory, puede aplicar objetos de política de grupo (GPO) de Active Directory para administrar de forma centralizada sus instancias de Amazon EC2 para Windows o Linux uniendo las instancias a su dominio AWS administrado de Microsoft AD.

Además, sus usuarios pueden iniciar sesión en sus instancias con sus credenciales de Active Directory. Esto elimina la necesidad de utilizar credenciales de instancias individuales o distribuir archivos de clave privada (PEM). Esto le facilita conceder o revocar el acceso a los usuarios al instante mediante las herramientas de administración de usuarios de Active Directory que ya utiliza.

Caso de uso 3: proporcione servicios de directorio a sus cargas de trabajo compatibles con Active Directory

AWS Managed Microsoft AD es un auténtico Active Directory de Microsoft que le permite ejecutar cargas de trabajo tradicionales compatibles con Active Directory, como Remote Desktop Licensing Manager y Microsoft y SharePoint Microsoft SQL Server Always On in the Cloud. AWS AWS Microsoft AD administrado también le ayuda a simplificar y mejorar la seguridad de las aplicaciones.NET integradas en Active Directory mediante el uso de cuentas de servicios administradas grupales (GMSA) y la delegación restringida de Kerberos (KCD).

Caso de uso 4: para Office 365 y otras aplicaciones AWS IAM Identity Center en la nube

Puede usar Microsoft AD AWS administrado AWS IAM Identity Center para proporcionar aplicaciones en la nube. Puede usar Microsoft Entra Connect (antes conocido comoAzure Active Directory Connect) para sincronizar sus usuarios en Microsoft Entra (anteriormente conocido como Azure Active Directory (AzureAD)) y, después, usar los Servicios de federación de Active Directory (AD FS) para que sus usuarios puedan acceder a Microsoft Office 365 y a otras aplicaciones en la nube de SAML 2.0 mediante sus credenciales de Active Directory.

La integración de Microsoft AD AWS administrado con IAM Identity Center añade capacidades de SAML a su AWS Microsoft AD administrado y/o a sus dominios de confianza locales. Una vez integrados, sus usuarios pueden utilizar el Centro de Identidad de IAM con servicios compatibles con el SAML, incluidas las aplicaciones en la nube AWS Management Console y de terceros, como Office 365, Concur y Salesforce, sin tener que configurar una infraestructura de SAML. Para ver una demostración del proceso que permite a los usuarios locales utilizar el IAM Identity Center, consulte el siguiente vídeo. YouTube

> **Note**
>
> AWS Se cambió el nombre de Single Sign-On por el de IAM Identity Center.

Caso de uso 5: extienda su Active Directory local a la nube AWS

Si ya tiene una infraestructura de Active Directory y quiere usarla al migrar cargas de trabajo compatibles con Active Directory a la nube AWS , Managed AWS Microsoft AD puede ayudarlo. Puede usar las confianzas de Active Directory para conectar Microsoft AD AWS administrado a su Active Directory existente. Esto significa que sus usuarios pueden acceder a AWS aplicaciones y aplicaciones compatibles con Active Directory con sus credenciales de Active Directory locales, sin necesidad de sincronizar usuarios, grupos o contraseñas.

Por ejemplo, sus usuarios pueden iniciar sesión en Amazon AWS Management Console y en Amazon WorkSpaces con sus nombres de usuario y contraseñas de Active Directory existentes. Además, cuando utiliza aplicaciones compatibles SharePoint con Active Directory, como AWS Microsoft AD administrado, los usuarios de Windows que hayan iniciado sesión pueden acceder a estas aplicaciones sin necesidad de volver a introducir las credenciales.

También puede migrar su dominio de Active Directory local AWS para liberarse de la carga operativa de su infraestructura de Active Directory mediante el kit de herramientas de migración de Active Directory (ADMT) y el servicio de exportación de contraseñas (PES) para realizar la migración.

Caso de uso 6: comparta su directorio para unir sin problemas las instancias de Amazon EC2 a un dominio de todas las cuentas AWS

Compartir su directorio entre varias AWS cuentas le permite administrar AWS servicios como Amazon EC2 fácilmente sin necesidad de operar un directorio para cada cuenta y cada VPC. Puede

utilizar su directorio desde cualquier cuenta de AWS y desde cualquier Amazon VPC dentro de una región de AWS . Esta capacidad hace que sea más fácil y rentable administrar cargas de trabajo compatibles con el directorio con un único directorio entre cuentas y VPC. Por ejemplo, ahora puede administrar sus cargas de trabajo de Windows implementadas en instancias de EC2 en varias cuentas y las VPC fácilmente mediante un único directorio de AWS Managed Microsoft AD.

Cuando comparte su directorio de Microsoft AD AWS gestionado con otra AWS cuenta, puede utilizar la consola Amazon EC2 o AWS Systems Managerunir sus instancias sin problemas desde cualquier Amazon VPC de la cuenta y la región. AWS Puede implementar rápidamente las cargas de trabajo compatibles con un directorio en instancias EC2 al eliminar la necesidad de unir manualmente las instancias a un dominio o de implementar directorios en cada cuenta y VPC. Para obtener más información, consulte Compartir el directorio.

Cómo administrar Microsoft AD AWS administrado

En esta sección se enumeran todos los procedimientos para operar y mantener un entorno Microsoft AD AWS administrado.

Temas

Protección del directorio de AWS Managed Microsoft AD

En esta sección, se describen las consideraciones para proteger su entorno de AWS Managed Microsoft AD.

Temas

Administrar las políticas de contraseñas para AWS Managed Microsoft AD

AWS Microsoft AD administrado le permite definir y asignar diferentes políticas de bloqueo de cuentas y contraseñas (también denominadas políticas de contraseñas específicas) para los grupos de usuarios que administra en su dominio de AWS Microsoft AD administrado. Al crear un directorio de Microsoft AD AWS administrado, se crea una política de dominio predeterminada y se aplica aActive Directory. Esta política incluye las siguientes opciones:

Política	Opción
Aplicar el historial de contraseñas	Se recuerdan 24 contraseñas
Antigüedad máxima de la contraseña	42 días *
Antigüedad mínima de la contraseña	1 día
Longitud mínima de la contraseña	7 caracteres
La contraseña debe cumplir los requisitos de complejidad	Habilitado
Almacenamiento de contraseña mediante cifrado reversible	Deshabilitad

* Nota: el valor de 42 días de la antigüedad máxima de la contraseña también se aplica a la contraseña del administrador.

Por ejemplo, puede asignar una configuración de las políticas menos estricta para aquellos empleados con acceso solo a información de baja confidencialidad. Para los administradores sénior que obtienen acceso con frecuencia a información confidencial, puede aplicar una configuración más estricta.

Los siguientes son recursos para obtener más información sobre las políticas Microsoft Active Directory de contraseñas y las políticas de seguridad detalladas:

- Configure los ajustes de la política de seguridad
- Requisitos de complejidad de las contraseñas
- Consideraciones de seguridad sobre la complejidad de las

AWS proporciona un conjunto de políticas de contraseñas detalladas en AWS Microsoft AD administrado que puede configurar y asignar a sus grupos. Para configurar las políticas, puede utilizar herramientas de Microsoft políticas estándar, como Active Directory el Centro de administración. Para empezar a utilizar las herramientas Microsoft de políticas, consulteInstalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado.

Cómo se aplican las políticas de contraseñas

Existen diferencias en la forma en que se aplican las políticas de contraseñas detalladas en función de si la contraseña se restableció o se cambió. Los usuarios del dominio pueden cambiar su propia contraseña. Un Active Directory administrador o un usuario con los permisos necesarios puede restablecer las contraseñas de los usuarios. Consulte la siguiente tabla para obtener más información.

Política	Restablecimiento de contraseña	Cambio de contraseña
Aplicar el historial de contraseñas	No	Sí

Política	Restablecimiento de contraseña	Cambio de contraseña
Antigüedad máxima de la contraseña	Sí	Sí
Antigüedad mínima de la contraseña	No	Sí
Longitud mínima de la contraseña	Sí	Sí
La contraseña debe cumplir los requisitos de complejidad	Sí	Sí

Estas diferencias tienen implicaciones de seguridad. Por ejemplo, cada vez que se restablece la contraseña de un usuario, no se aplican las políticas sobre el historial de contraseñas y la antigüedad mínima de las contraseñas. Para obtener más información, consulte la documentación de Microsoft sobre las consideraciones de seguridad relacionadas con la aplicación del historial de contraseñas y las políticas de antigüedad mínima de las contraseñas.

Temas

- Configuración de políticas admitida
- Delegar quién puede administrar sus políticas de contraseñas
- Asignar políticas de contraseñas a sus usuarios

Artículo AWS de blog sobre seguridad relacionado

- Cómo configurar políticas de contraseñas aún más sólidas para ayudar a cumplir sus estándares de seguridad mediante el uso AWS Directory Service de Microsoft AD AWS administrado

Configuración de políticas admitida

AWS Microsoft AD administrado incluye cinco políticas detalladas con un valor de prioridad no editable. Las políticas tienen una serie de propiedades que puede configurar para forzar la seguridad de las contraseñas y acciones de bloqueo de cuentas en caso de producirse errores de inicio de sesión. Puede asignar las políticas a cero o más grupos de Active Directory. Si un usuario final es miembro de varios grupos y recibe más de una política de contraseñas, Active Directory fuerza la política con el valor de prioridad más bajo.

AWS políticas de contraseñas predefinidas

En la siguiente tabla se enumeran las cinco políticas incluidas en el directorio de Microsoft AD AWS administrado y su valor de prioridad asignado. Para obtener más información, consulte Prioridad.

Nombre de la política	Prioridad
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

Propiedades de las políticas de contraseñas

Puede editar las siguientes propiedades en sus políticas de contraseñas para ajustarlas a los estándares de conformidad que satisfagan las necesidades de su negocio.

- Nombre de la política
- Aplicar el historial de contraseñas
- Longitud mínima de la contraseña
- Antigüedad mínima de la contraseña

- Antigüedad máxima de la contraseña
- Almacenamiento de contraseña mediante cifrado reversible
- La contraseña debe cumplir los requisitos de complejidad

No puede modificar los valores de prioridad de estas políticas. Para obtener más información sobre cómo afectan estas configuraciones a la aplicación de contraseñas, consulte AD DS: políticas de contraseñas detalladas en el sitio web de Microsoft. TechNet Para obtener información general acerca de estas políticas, consulte la Política de contraseñas en el TechNet sitio web de Microsoft.

Políticas de bloqueo de cuentas

También puede modificar las siguientes propiedades de sus políticas de contraseñas para especificar si Active Directory debería bloquear una cuenta tras producirse errores de inicio de sesión y cómo hacerlo:

- Número de intentos de inicio de sesión con error permitidos
- Duración de bloqueo de cuentas
- Restablecimiento de intentos de inicio de sesión con error tras una duración determinada

Para obtener información general acerca de estas políticas, consulte la Política de bloqueo de cuentas en el sitio TechNet web de Microsoft.

Prioridad

Las políticas con un valor de prioridad más bajo tienen mayor prioridad. Puede asignar políticas de contraseñas a grupos de seguridad de Active Directory. Aunque debe aplicar una sola política a un grupo de seguridad, un solo usuario puede recibir más de una política de contraseñas. Por ejemplo, supongamos que `jsmith` es miembro del grupo HR y también del grupo MANAGERS. Si asigna CustomerPSO-05 (que tiene una prioridad de 50) al grupo HR y CustomerPSO-04 (que tiene una prioridad de 40) a MANAGERS, CustomerPSO-04 tiene la prioridad más alta y Active Directory aplica esa política a `jsmith`.

Si asigna varias políticas a un usuario o grupo, Active Directory determina la política obtenida del modo siguiente:

1. Se aplica una política que asigna directamente al objeto de usuario.

2. Si no se asigna ninguna política directamente al objeto de usuario, se aplica la política con el valor de prioridad más bajo de todas las políticas recibidas por el usuario como resultado de la pertenencia a un grupo.

Para obtener más información, consulte AD DS: políticas de contraseñas detalladas en el sitio web de Microsoft. TechNet

Delegar quién puede administrar sus políticas de contraseñas

Puede delegar permisos para administrar las políticas de contraseñas en cuentas de usuario específicas que haya creado en su Microsoft AD AWS administrado agregando las cuentas al grupo de seguridad de administradores de políticas de contraseñas específicas AWS delegadas. Cuando una cuenta pasa a ser un miembro de este grupo, la cuenta tiene permisos para editar y configurar cualquiera de las políticas de contraseñas indicadas anteriormente.

Para delegar quién puede administrar políticas de contraseñas

1. Inicie el centro de administración de Active Directory (ADAC) desde cualquier instancia de EC2 administrada que haya unido a su dominio de AWS Microsoft AD administrado.
2. Cambie a la Vista de árbol y vaya a la unidad organizativa AWS Delegated Groups. Para obtener más información acerca de esta unidad organizativa, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD.
3. Busque el grupo de usuarios AWS Delegated Fine Grained Password Policy Administrators. Añada cualquier usuario o grupo de su dominio a este grupo.

Asignar políticas de contraseñas a sus usuarios

Las cuentas de usuario que son miembros del grupo de seguridad AWS Delegated Fine Grained Password Policy Administrators pueden utilizar el siguiente procedimiento para asignar políticas a usuarios y grupos de seguridad.

Para asignar políticas de contraseñas a sus usuarios

1. Inicie el centro de administración de Active Directory (ADAC) desde cualquier instancia de EC2 administrada que haya unido a su dominio de AWS Microsoft AD administrado.
2. Cambie a vista de árbol y vaya a System\Password Settings Container.
3. Haga doble clic en la política detallada que desee editar. Haga clic en Add (Agregar) para editar las propiedades de las políticas y añada usuarios o grupos de seguridad a la política. Para

obtener más información acerca de las políticas detalladas predeterminadas proporcionadas con AWS Managed Microsoft AD, consulte AWS políticas de contraseñas predefinidas.

4. Para comprobar que se ha aplicado la política de contraseñas, ejecute el siguiente comando: PowerShell

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

> **Note**
>
> Evite utilizar el comando `net user`, ya que los resultados que obtenga podrían ser inexactos.

Si no configura ninguna de las cinco políticas de contraseñas del directorio AWS administrado de Microsoft AD, Active Directory utilizará la política de grupo de dominios predeterminada. Para obtener detalles adicionales acerca del uso del contenedor de configuraciones de contraseña, consulte esta entrada de blog de Microsoft.

Habilite la autenticación multifactorial para Microsoft AWS AD administrado

Puede habilitar la autenticación multifactor (MFA) en su directorio AWS administrado de Microsoft AD para aumentar la seguridad cuando los usuarios especifican sus credenciales de AD para acceder. Aplicaciones empresariales de Amazon admitidas Cuando se habilita la autenticación MFA, los usuarios deben introducir su nombre de usuario y su contraseña (el primer factor) como de costumbre, pero además deben introducir un código de autenticación (el segundo factor), proporcionado por la solución de MFA virtual o de hardware. La combinación de estos factores proporciona seguridad adicional, ya que impiden el acceso a las aplicaciones empresariales de Amazon, a menos que se proporcionen credenciales de usuario válidas y un código de MFA válido.

Para habilitar la MFA, debe tener una solución de MFA compuesta por un servidor Remote Authentication Dial-In User Service (RADIUS), o disponer de un complemento de MFA para un servidor RADIUS que ya tenga implementado en su infraestructura en las instalaciones. La solución de MFA debería implementar claves de acceso de un solo uso (OTP) que los usuarios obtienen de un dispositivo de hardware o de un software que se ejecuta en un dispositivo como un teléfono móvil.

RADIUS es un protocolo cliente/servidor estándar en el sector que proporciona administración de autenticación, autorización y contabilidad para que los usuarios puedan conectarse a servicios

de red. AWS Microsoft AD administrado incluye un cliente RADIUS que se conecta al servidor RADIUS en el que ha implementado la solución de MFA. El servidor RADIUS valida el nombre de usuario y el código de OTP. Si el servidor RADIUS valida correctamente al usuario, AWS Managed Microsoft AD autentica al usuario en Active Directory. Tras la autenticación correcta de Active Directory, los usuarios pueden acceder a la AWS aplicación. La comunicación entre el cliente RADIUS AWS administrado de Microsoft AD y el servidor RADIUS requiere que configure grupos de AWS seguridad que permitan la comunicación a través del puerto 1812.

Puede habilitar la autenticación multifactor para su directorio AWS administrado de Microsoft AD mediante el siguiente procedimiento. Para obtener más información acerca de cómo configurar su servidor RADIUS para que funcione con AWS Directory Service y MFA, consulte Requisitos previos de la autenticación multifactor.

Consideraciones

Las siguientes son algunas consideraciones para la autenticación multifactor para su Microsoft AD AWS administrado:

- La autenticación multifactor no puede usarse con Simple AD. Sin embargo, la MFA se puede habilitar para su directorio de Conector AD. Para obtener más información, consulte Habilitación de la autenticación multifactor para Conector AD.
- La MFA es una función regional de Managed AWS Microsoft AD. Si utiliza Replicación multirregional, los siguientes procedimientos se deberán aplicar por separado en cada región. Para obtener más información, consulte Características globales frente a las regionales.
- Si piensa utilizar Microsoft AD AWS administrado para las comunicaciones externas, le recomendamos que configure una puerta de enlace de Internet con traducción de direcciones de red (NAT) o una puerta de enlace de Internet fuera de la AWS red para estas comunicaciones.
  - Si desea admitir las comunicaciones externas entre su Microsoft AD AWS administrado y su servidor RADIUS alojado en la AWS red, póngase en contacto con AWS Support.

Habilite la autenticación multifactorial para Microsoft AWS AD administrado

El siguiente procedimiento muestra cómo habilitar la autenticación multifactor para Microsoft AD AWS administrado.

1. Identifique la dirección IP de su servidor MFA RADIUS y de su directorio administrado de AWS Microsoft AD.

2. Edite los grupos de seguridad de Virtual Private Cloud (VPC) para habilitar las comunicaciones a través del puerto 1812 entre los puntos finales IP gestionados de AWS Microsoft AD y su servidor de MFA RADIUS.
3. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
4. Elija el enlace de ID de directorio para su directorio AWS administrado de Microsoft AD.
5. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación de varias regiones, seleccione la región en la que quiere habilitar MFA y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
6. En la sección Multi-factor authentication (Autenticación multifactor), elija Actions (Acciones) y, a continuación, seleccione Enable (Habilitar).
7. En la página Enable multi-factor authentication (MFA) (Habilitar la autenticación multifactor (MFA)), proporcione los valores siguientes:

   Display label (Mostrar etiqueta)

   Proporcione un nombre de etiqueta.

   RADIUS server DNS name or IP addresses (Nombre de DNS o direcciones IP del servidor RADIUS)

   Direcciones IP de los puntos de enlace del servidor RADIUS o dirección IP del balanceador de carga del servidor RADIUS. Puede especificar varias direcciones IP separándolas mediante comas (por ejemplo, `192.0.0.0,192.0.0.12`).

   > **Note**
   >
   > El MFA RADIUS solo se aplica para autenticar el acceso a las AWS Management Console aplicaciones y servicios empresariales de Amazon, como Amazon o WorkSpaces Amazon QuickSight Chime. No proporciona MFA a las cargas de trabajo de Windows que se ejecutan en instancias EC2 ni para iniciar sesión en una instancia EC2. AWS Directory Service no admite la autenticación RADIUS Challenge/Response.
   > En el momento en que los usuarios especifiquen el nombre de usuario y la contraseña, deben disponer de un código MFA. Como alternativa, debe usar una

solución que realice MFA, out-of-band como la verificación de texto por SMS para el usuario. En las soluciones de out-of-band MFA, debe asegurarse de establecer el valor de tiempo de espera RADIUS de forma adecuada para su solución. Al utilizar una solución de out-of-band MFA, la página de inicio de sesión solicitará al usuario un código de MFA. En ese caso, los usuarios deben escribir su contraseña en el campo de contraseña y en el campo de MFA.

Puerto

Puerto que utiliza el servidor RADIUS para las comunicaciones. La red local debe permitir el tráfico entrante desde los servidores a través del puerto de servidor RADIUS predeterminado (UDP:1812). AWS Directory Service

Código secreto compartido

Código de secreto compartido que se especificó cuando se crearon los puntos de enlace de RADIUS.

Confirm shared secret code (Confirmar código secreto compartido)

Confirme el código secreto compartido para los puntos de enlace de RADIUS.

Protocolo

Seleccione el protocolo que se especificó cuando se crearon los puntos de enlace de RADIUS.

Tiempo de espera del servidor (en segundos)

Tiempo, en segundos, que hay que esperar a que el servidor RADIUS responda. Este valor debe estar entre 1 y 50.

> **Note**
>
> Recomendamos configurar el tiempo de espera del servidor RADIUS en 20 segundos o menos. Si el tiempo de espera supera los 20 segundos, el sistema no podrá volver a intentarlo con otro servidor RADIUS y podría producirse un error en el tiempo de espera.

Número máximo de reintentos de solicitud RADIUS

Número de veces que se intenta la comunicación con el servidor RADIUS. Este valor debe estar entre 0 y 10.

La autenticación multifactor está disponible cuando RADIUS Status cambia a Habilitado.

8. Seleccione Habilitar.

Aplicaciones empresariales de Amazon admitidas

Todas las aplicaciones de TI empresariales de Amazon WorkSpaces WorkDocs, incluidas Amazon WorkMail QuickSight, Amazon y Access to AWS Managed Microsoft AD AWS IAM Identity Center y AD Connector con MFA, AWS Management Console son compatibles con ellos.

Para obtener información sobre cómo configurar el acceso básico de los usuarios a las aplicaciones de Amazon Enterprise, el inicio de sesión AWS único y el AWS Management Console uso AWS Directory Service, consulte Habilite el acceso a AWS aplicaciones y servicios y. Habilitación del acceso a la AWS Management Console con credenciales de AD

Artículo de blog sobre AWS seguridad relacionado

- Cómo habilitar la autenticación multifactor para AWS los servicios mediante Microsoft AD AWS administrado y credenciales locales

Habilite LDAP o LDAPS seguros

El protocolo ligero de acceso a directorios (LDAP) es un protocolo de comunicación estándar que se utiliza para leer y escribir datos en y desde Active Directory. Algunas aplicaciones utilizan LDAP para añadir, quitar o buscar usuarios y grupos de Active Directory o para transportar credenciales para autenticar a los usuarios en Active Directory. Cada comunicación LDAP incluye un cliente (como una aplicación) y un servidor (como Active Directory).

De forma predeterminada, las comunicaciones a través de LDAP no están cifradas. Esto permite a un usuario malintencionado utilizar el software de monitorización de red para ver los paquetes de datos que pasan por la red. Esta es la razón por la que en muchas políticas de seguridad corporativas se requiere que las organizaciones cifren todas las comunicaciones LDAP.

Para mitigar esta forma de exposición de datos, AWS Managed Microsoft AD ofrece una opción: puede habilitar LDAP a través de Secure Sockets Layer (SSL) /Transport Layer Security (TLS), también conocido como LDAPS. Con LDAPS, puede mejorar la seguridad de las conexiones. También puede cumplir con los requisitos de conformidad cifrando todas las comunicaciones entre sus aplicaciones habilitadas para LDAP y Managed AWS Microsoft AD.

AWS Managed Microsoft AD proporciona soporte para LDAPS en los siguientes escenarios de implementación:

- El LDAPS del lado del servidor cifra las comunicaciones LDAP entre sus aplicaciones comerciales o locales compatibles con LDAP (que actúan como clientes LDAP) y Managed Microsoft AD (que actúa como servidor LDAP). AWS Para obtener más información, consulte Habilite el LDAPS del lado del servidor mediante Microsoft AD administrado AWS.
- El LDAPS del lado del cliente cifra las comunicaciones LDAP entre AWS aplicaciones (que actúan como clientes LDAP) y su Active Directory autogestionado (local) (que actúa como WorkSpaces servidor LDAP). Para obtener más información, consulte Habilite el LDAPS del lado del cliente mediante Microsoft AD administrado AWS.

Temas

Habilite el LDAPS del lado del servidor mediante Microsoft AD administrado AWS

La compatibilidad con el protocolo ligero de acceso a directorios Secure Sockets Layer Layer Layer (SSL) /Transport Layer Security (TLS) (LDAPS) del lado del servidor cifra las comunicaciones LDAP entre sus aplicaciones comerciales o locales compatibles con LDAP y su directorio administrado de Microsoft AD. AWS Esto ayuda a mejorar la seguridad de todas las conexiones y a cumplir los requisitos de cumplimiento mediante el protocolo criptográfico SSL (Capa de conexión segura).

Habilitación de LDAPS del servidor

Para obtener instrucciones detalladas sobre cómo configurar y configurar el LDAPS del lado del servidor y el servidor de la entidad de certificación (CA), consulte Cómo habilitar el LDAPS del lado del servidor para su directorio AWS administrado de Microsoft AD en el blog de seguridad. AWS

La mayor parte de la configuración se debe llevar a cabo desde la instancia de Amazon EC2 que se utiliza para administrar los controladores de dominio de AWS Managed Microsoft AD. Los siguientes pasos le guiarán para habilitar el LDAPS para su dominio en la nube. AWS

Si desea utilizar la automatización para configurar su infraestructura de PKI, puede utilizar Microsoft Public Key Infrastructure on AWS QuickStart Guide. En concreto, querrá seguir las instrucciones de la guía para cargar la plantilla para Implementar Microsoft PKI en una VPC existente de AWS. Una vez que cargue la plantilla, asegúrese de elegir **`AWSManaged`** cuando llegue la opción Tipo de servicios de dominio de Active Directory. Si ha utilizado la QuickStart guía, puede ir directamente aPaso 3: creación de una plantilla de certificado.

Temas

Paso 1: delegación de quién puede habilitar LDAPS

Para habilitar el LDAPS del lado del servidor, debe ser miembro del grupo Administradores o Administradores de Autoridades de Certificación Empresariales AWS Delegadas en su directorio de Microsoft AD administrado AWS . También puede ser el usuario administrativo predeterminado (cuenta de administrador). Si lo prefiere, puede tener un usuario distinto del administrador para la cuenta de LDAPS. En ese caso, añada ese usuario al grupo Administradores o Administradores de Autoridades de Certificación Empresariales AWS Delegadas en su directorio de AWS Microsoft AD administrado.

Paso 2: configuración de su entidad de certificación

Para poder habilitar LDAPS del lado del servidor, debe crear un certificado. Este certificado debe emitirlo un servidor de CA empresarial de Microsoft que esté unido a su dominio de Microsoft AD AWS administrado. Una vez creado, el certificado debe instalarse en cada uno de los controladores de dominio de ese dominio. Este certificado permite que el servicio LDAP de los controladores de dominio reciba y acepte automáticamente las conexiones SSL de clientes LDAP.

> **Note**
>
> El LDAPS del lado del servidor con AWS Microsoft AD administrado no admite los certificados emitidos por una CA independiente. Tampoco se admiten los certificados emitidos por una entidad de certificación de terceros.

Dependiendo de sus necesidades empresariales, dispone de las siguientes opciones para configurar o conectarse a una entidad de certificación en su dominio:

- Crear una CA empresarial subordinada: (recomendada) Con esta opción, puede implementar un servidor de CA empresarial subordinado de Microsoft en la AWS nube. El servidor puede utilizar Amazon EC2 para que funcione con la CA raíz de Microsoft existente. Para obtener más información acerca de cómo configurar una CA empresarial subordinada de Microsoft, consulte el paso 4: Agregar una CA empresarial de Microsoft al directorio de AWS Microsoft AD en Cómo habilitar el LDAPS del lado del servidor para su directorio de AWS Microsoft AD administrado.
- Crear una CA empresarial raíz de Microsoft: con esta opción, puede crear una CA empresarial raíz de Microsoft en la AWS nube mediante Amazon EC2 y unirla a su dominio de AWS Microsoft AD administrado. Esta entidad de certificación raíz puede emitir el certificado para los controladores de dominio. Para obtener más información sobre la configuración de una nueva CA raíz, consulte el paso 3: Instalar y configurar una CA sin conexión en Cómo habilitar el LDAPS del lado del servidor para su directorio administrado de AWS Microsoft AD.

Para obtener más información acerca de cómo unir la instancia EC2 al dominio, consulte Unir una instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory.

Paso 3: creación de una plantilla de certificado

Una vez configurada la CA de empresa, puede configurar la plantilla de certificado de autenticación Kerberos.

Creación de una plantilla de certificado

1. Inicie Microsoft Windows Server Manager. Seleccione Herramientas > Autoridad de certificación.
2. En la ventana Entidad de certificación, expanda el árbol Entidad de certificación en el panel izquierdo. Haga clic con el botón derecho en Plantillas de certificado y luego elija Administrar.
3. En la ventana de Consola de plantillas de certificado de, haga clic con el botón derecho en Autenticación Kerberos y luego elija Plantilla duplicada.

4. Aparecerá la ventana Propiedades de la nueva plantilla.
5. En la ventana Propiedades de la nueva plantilla, vaya a la pestaña Compatibilidad y, a continuación, haga lo siguiente:
   a. Cambie la autoridad de certificación por el sistema operativo que coincida con su CA.
   b. Si aparece una ventana Cambios resultantes, seleccione Aceptar.
   c. Cambie el destinatario de la certificación a Windows 10/Windows Server 2016.

      > **Note**
      > AWS Managed Microsoft AD funciona con Windows Server 2019.

   d. Si aparecen ventanas de cambios resultantes, seleccione Aceptar.
6. Haga clic en la pestaña General y cambie el nombre para mostrar de la plantilla a LDAPOVERSSL o cualquier otro nombre que prefiera.
7. Haga clic en la pestaña Seguridad y elija Controladores de dominio en la sección Nombres de usuarios o grupo. En la sección Permisos para controladores de dominio, compruebe que las casillas de verificación Permitir para Leer, Inscribir e Inscribir automáticamente estén activadas.
8. Haga clic en Aceptar para crear la plantilla del certificado LDAPOVERSSL (o el nombre que especificó anteriormente). Cierre la ventana de la Consola de plantillas de certificados.
9. En la ventana Entidad de certificación, haga clic con el botón derecho en Plantillas de certificado y elija Nuevo > Plantilla de certificado que se va a emitir.
10. En la ventana Habilitar plantillas de certificados, elija LDAPOVERSSL (o el nombre que especificó anteriormente) y, a continuación, elija Aceptar.

Paso 4: adición de reglas de grupos de seguridad

En el paso final, debe abrir la consola de Amazon EC2 y agregar reglas del grupo de seguridad. Estas reglas permiten que los controladores de dominio se conecten a la CA empresarial para solicitar un certificado. Para ello, tiene que añadir reglas de entrada para que su entidad de certificación empresarial pueda aceptar el tráfico entrante desde los controladores de dominio. A continuación, añada reglas de salida para permitir el tráfico desde los controladores de dominio a la entidad de certificación empresarial.

Una vez que ambas reglas se han configurado, los controladores de dominio solicitan automáticamente un certificado de su entidad de certificación empresarial y habilitan LDAPS para su

directorio. El servicio de LDAP en los controladores de dominio ya está listo para aceptar conexiones LDAPS.

Configuración de reglas de grupos de seguridad

1. Vaya a la consola de Amazon EC2 en https://console.aws.amazon.com/ec2 e inicie sesión con las credenciales de administrador.
2. En el panel izquierdo, elija Security Groups en Network & Security.
3. En el panel principal, elija el grupo AWS de seguridad de su CA.
4. Elija la pestaña Inbound (Entrada) y, a continuación, elija Edit (Editar).
5. En el cuadro de diálogo Edit inbound rules, haga lo siguiente:
   - Seleccione Add Rule (Agregar regla).
   - Elija All traffic en Type y Custom en Source.
   - Introduzca el grupo de AWS seguridad de su directorio (por ejemplo, sg-123456789) en el cuadro situado junto a Fuente.
   - Seleccione Guardar.
6. Ahora elija el grupo de AWS seguridad de su directorio AWS administrado de Microsoft AD. Elija la pestaña Outbound y, a continuación, elija Edit.
7. En el cuadro de diálogo Edit outbound rules, haga lo siguiente:
   - Seleccione Add Rule (Agregar regla).
   - Elija All traffic en Type y Custom en Destination.
   - Escriba el grupo de AWS seguridad de su entidad emisora de certificados en el cuadro situado junto a Destino.
   - Seleccione Guardar.

Puede probar la conexión LDAPS al directorio AWS administrado de Microsoft AD mediante la herramienta LDP. La herramienta LDP viene con las herramientas de administración de Active Directory. Para obtener más información, consulte Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado.

> **Note**
>
> Antes de probar la conexión LDAPS, debe esperar hasta 30 minutos a que la entidad de certificación subordinada emita un certificado para los controladores de dominio.

Para obtener más información sobre el LDAPS del lado del servidor y ver un ejemplo de caso de uso sobre cómo configurarlo, consulte Cómo habilitar el LDAPS del lado del servidor para su directorio AWS administrado de Microsoft AD en el blog de seguridad. AWS

Habilite el LDAPS del lado del cliente mediante Microsoft AD administrado AWS

La compatibilidad con el protocolo ligero de acceso a directorios Secure Sockets Layer (SSL) / Transport Layer Security (TLS) (LDAPS) del lado del cliente en AWS Microsoft AD administrado cifra las comunicaciones entre Microsoft Active Directory (AD) autogestionado (local) y las aplicaciones. AWS Algunos ejemplos de dichas aplicaciones incluyen WorkSpaces Amazon QuickSight y Amazon Chime. AWS IAM Identity Center Este cifrado le ayuda a proteger mejor los datos de identidad de su organización y a cumplir sus requisitos de seguridad.

Requisitos previos

Antes de habilitar LDAPS del lado del cliente, debe cumplir los siguientes requisitos.

Temas

- Cree una relación de confianza entre su Microsoft AD AWS administrado y el autogestionado Microsoft Active Directory
- Implementar certificados de servidor en Active Directory
- Requisitos de certificación de la autoridad de certificación
- Requisitos de red

Cree una relación de confianza entre su Microsoft AD AWS administrado y el autogestionado Microsoft Active Directory

En primer lugar, debe establecer una relación de confianza entre su Microsoft AD administrado y el AWS autogestionado Microsoft Active Directory para habilitar el LDAPS del lado del cliente. Para obtener más información, consulte the section called “Creación de una relación de confianza”.

Implementar certificados de servidor en Active Directory

Para habilitar LDAPS en el lado del cliente, debe obtener e instalar certificados de servidor para cada controlador de dominio en Active Directory. Estos certificados los utilizará el servicio LDAP para escuchar y aceptar automáticamente conexiones SSL de clientes LDAP. Puede utilizar certificados SSL emitidos por una implementación interna de Active Directory Certificate Services (ADCS) o adquiridos a un emisor comercial. Para obtener más información acerca de los requisitos de certificados de servidor de Active Directory, consulte Certificado LDAP a través de SSL (LDAPS) en el sitio web de Microsoft.

Requisitos de certificación de la autoridad de certificación

Se requiere un certificado de CA (entidad de certificación) que represente al emisor de los certificados de servidor para la operación LDAPS del lado del cliente. Los certificados de entidad de certificación coinciden con los certificados de servidor que presentan los controladores de dominio de Active Directory para cifrar las comunicaciones LDAP. Tenga en cuenta los siguientes requisitos de los certificados de CA:

- Se requiere una autoridad de certificación empresarial (CA) para habilitar el LDAPS del lado del cliente. Puede utilizar el Servicio de Active Directory Certificación, una autoridad de certificación comercial externa o. AWS Certificate Manager Para obtener más información sobre la autoridad de certificación Microsoft empresarial, consulte Microsoftla documentación.
- Para registrar un certificado, deben quedar más de 90 días para que caduque.
- Los certificados deben estar en formato PEM (Privacy-Enhanced Mail). Si exporta certificados de CA desde Active Directory, elija X.509 (.CER) codificado en base64 como formato de archivo de exportación.
- Se puede almacenar un máximo de cinco (5) certificados de CA por directorio AWS administrado de Microsoft AD.
- No se admiten los certificados que utilizan el algoritmo de firma RSASSA-PSS.
- Los certificados de CA que se encadenan a cada certificado de servidor de cada dominio de confianza deben estar registrados.

Requisitos de red

AWS el tráfico LDAP de la aplicación se ejecutará exclusivamente en el puerto TCP 636, sin recurrir al puerto LDAP 389. Sin embargo, las comunicaciones LDAP de Windows que admiten la replicación, relaciones de confianza y otras características seguirán utilizando el puerto LDAP 389

con la seguridad nativa de Windows. Configure grupos de AWS seguridad y firewalls de red para permitir las comunicaciones TCP en el puerto 636 en AWS Microsoft AD administrado (saliente) y Active Directory autoadministrado (entrante). Deje abierto el puerto LDAP 389 entre AWS Managed Microsoft AD y la instancia de Active Directory autoadministrada.

Habilitación de LDAPS del cliente

Para habilitar LDAPS del cliente, importe el certificado de la entidad de certificación (CA) en AWS Managed Microsoft AD y, a continuación, habilite LDAPS en el directorio. Tras la habilitación, todo el tráfico LDAP entre las aplicaciones de AWS y su instancia de Active Directory autoadministrada se realizará con el cifrado de canal SSL (Capa de conexión segura).

Puede utilizar dos métodos diferentes para habilitar LDAPS en el lado del cliente para su directorio. Puede usar el método o el AWS Management Console método. AWS CLI

> **Note**
>
> El LDAPS del lado del cliente es una función regional de Managed AWS Microsoft AD. Si utiliza Replicación multirregional, los siguientes procedimientos se deberán aplicar por separado en cada región. Para obtener más información, consulte Características globales frente a las regionales.

Temas

Paso 1: Registrar un certificado en AWS Directory Service

Utilice uno de los siguientes métodos para registrar un certificado AWS Directory Service.

Método 1: para registrar el certificado en AWS Directory Service (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.

3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiere habilitar el certificado y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Client-side LDAPS (LDAPS del lado del cliente), seleccione el menú Actions (Acciones) y, a continuación, seleccione Register certificate (Registrar certificado).
5. En el cuadro de diálogo Register a CA certificate (Registrar un certificado de entidad de certificación), seleccione Browse (Examinar) y, a continuación, seleccione el certificado y elija Open (Abrir).
6. Elija Register certificate (Registrar certificado).

Método 2: Para registrar su certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando de la . Para los datos del certificado, elija la ubicación del archivo de certificado de CA. Se proporcionará un ID de certificado en la respuesta.

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

Paso 2: comprobación del estado del registro

Para ver el estado del registro de un certificado o una lista de certificados registrados, utilice uno de los métodos siguientes.

Método 1: comprobar el estado de registro del certificado en AWS Directory Service (AWS Management Console)

1. Vaya a la sección Client-side LDAPS (LDAPS del lado del cliente) de la página Directory details (Detalles del directorio).
2. Revise el estado actual del registro de certificado que se muestra en la columna Registration status (Estado del registro). Cuando el valor de estado de registro cambia a Registered (Registrado), el certificado se ha registrado correctamente.

Método 2: comprobar el estado de registro del certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando de la . Si el valor de estado devuelve `Registered`, el certificado se ha registrado correctamente.

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

Paso 3: habilitación de LDAPS del cliente

Utilice uno de los siguientes métodos para habilitar la entrada del LDAPS del lado del cliente. AWS Directory Service

> **Note**
>
> Debe haber registrado correctamente al menos un certificado para poder habilitar LDAPS en el lado del cliente.

Método 1: Para habilitar el LDAPS del lado del cliente en () AWS Directory ServiceAWS Management Console

1. Vaya a la sección Client-side LDAPS (LDAPS del lado del cliente) de la página Directory details (Detalles del directorio).
2. Seleccione Habilitar. Si esta opción no está disponible, compruebe que se ha registrado correctamente un certificado válido y vuelva a intentarlo.
3. En el cuadro de diálogo Enable client-side LDAPS (Habilitar LDAPS del lado del cliente), elija Enable (Habilitar).

Método 2: Para habilitar el LDAPS del lado del cliente en () AWS Directory ServiceAWS CLI

- Ejecute el siguiente comando de la .

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

Paso 4: comprobación del estado de LDAPS

Utilice uno de los siguientes métodos para comprobar el estado del LDAPS. AWS Directory Service

Método 1: Para comprobar el estado del LDAPS en AWS Directory Service ()AWS Management Console

1. Vaya a la sección Client-side LDAPS (LDAPS del lado del cliente) de la página Directory details (Detalles del directorio).
2. Si el valor de estado se muestra como Enabled (Habilitado), LDAPS se ha configurado correctamente.

Método 2: Para comprobar el estado del LDAPS en AWS Directory Service ()AWS CLI

- Ejecute el siguiente comando de la . Si el valor de estado devuelve `Enabled`, LDAPS se ha configurado correctamente.

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

Administración de LDAPS del cliente

Utilice estos comandos para administrar la configuración de LDAPS.

Puede utilizar dos métodos distintos para administrar la configuración de LDAPS del lado del cliente. Puede utilizar el AWS Management Console método o el AWS CLI método.

Ver detalles del certificado

Utilice cualquiera de los métodos siguientes para ver cuándo está establecida la caducidad de un certificado.

Método 1: para ver los detalles del certificado en AWS Directory Service (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiera ver el certificado y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.

- Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.

4. En la sección Client-side LDAPS (LDAPS del lado del cliente), en CA certificates (Certificados de entidad de certificación), se mostrará la información del certificado.

Método 2: ver los detalles del certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando de la . Para obtener el ID de certificado, utilice el identificador devuelto por `register-certificate` o `list-certificates`.

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

Anular el registro de un certificado

Utilice cualquiera de los métodos siguientes para anular el registro de un certificado.

> **Note**
>
> Si sólo se registra un certificado, primero debe deshabilitar LDAPS antes de anular el registro del certificado.

Método 1: anular el registro de un certificado en AWS Directory Service ()AWS Management Console

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiere anular el registro del certificado y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Client-side LDAPS (LDAPS del lado del cliente), elija Actions (Acciones) y, a continuación, elija Deregister certificate (Anular registro del certificado).

5. En el cuadro de diálogo Deregister a CA certificate (Anular el registro del certificado de entidad de certificación), elija Deregister (Anular registro).

Método 2: anular el registro de un certificado en () AWS Directory ServiceAWS CLI

- Ejecute el siguiente comando de la . Para obtener el ID de certificado, utilice el identificador devuelto por `register-certificate` o `list-certificates`.

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

Deshabilitación de LDAPS del cliente

Utilice cualquiera de los métodos siguientes para deshabilitar LDAPS del lado del cliente.

Método 1: deshabilitar el LDAPS del lado del cliente en () AWS Directory ServiceAWS Management Console

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiera deshabilitar LDAPS del cliente y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Client-side LDAPS (LDAPS del lado del cliente), elija Disable (Deshabilitar).
5. En el cuadro de diálogo Disable client-side LDAPS (Deshabilitar LDAPS del lado del cliente), elija Disable (Deshabilitar).

Método 2: Para deshabilitar el LDAPS del lado del cliente en () AWS Directory ServiceAWS CLI

- Ejecute el siguiente comando de la .

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

Problemas con la inscripción de certificados

El proceso de inscripción de los controladores de dominio AWS gestionados de Microsoft AD con los certificados de CA puede tardar hasta 30 minutos. Si tiene problemas con la inscripción del certificado y desea reiniciar sus controladores de dominio AWS gestionados de Microsoft AD, puede ponerse en contacto con AWS Support. Para crear un caso de soporte, consulte Creación de casos de soporte y administración de casos.

Gestione el cumplimiento de AWS Managed Microsoft AD

Puede usar Microsoft AD AWS administrado para respaldar sus aplicaciones compatibles con Active Directory, en la AWS nube, que están sujetas a los siguientes requisitos de conformidad. Sin embargo, sus aplicaciones no se atendrán a los requisitos de conformidad si utiliza Simple AD o Conector de AD.

Estándares de conformidad admitidos

AWS Managed Microsoft AD se ha sometido a una auditoría para cumplir con los siguientes estándares y es apto para su uso como parte de soluciones para las que necesita obtener una certificación de conformidad.

FedRAMP	AWS Managed Microsoft AD cumple con los requisito s de seguridad del Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) y ha recibido una Autoridad Provisional para Operar (P-ATO) de la Junta de Autorización Conjunta (JAB) de FedRAMP en los niveles de referencia Moderado y Alto. Para obtener más información acerca de FedRAMP, consulte Conformidad con FedRAMP.
PCI Security Standards Council PARTICIPATING ORGANIZATION™	AWS Managed Microsoft AD cuenta con un certificado de conformidad con la versión 3.2 del Estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI) en el nivel 1 de proveedor de servicios. Los clientes que utilizan AWS productos y servicios para almacenar,

	procesar o transmitir datos de titulares de tarjetas pueden utilizar AWS Managed Microsoft AD para gestionar su propia certificación de conformidad con PCI DSS. Para obtener más información sobre PCI DSS, incluida la forma de solicitar una copia del PCI AWS Complianc e Package, consulte PCI DSS nivel 1. Lo que es más importante, debe configurar políticas de contraseñas detalladas en Managed AWS Microsoft AD para que sean coherentes con los estándares PCI DSS versión 3.2. Para obtener más información sobre las políticas que se deben aplicar, consulte la sección siguiente titulada Habilitar la conformidad con PCI para su directorio AWS administrado de Microsoft AD.
	AWS ha ampliado su programa de cumplimiento de la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) para incluir Managed AWS Microsoft AD como un servicio que cumple con los requisitos de la HIPAA. Si ha firmado un acuerdo de asociació n comercial (BAA) con usted AWS, puede usar AWS Managed Microsoft AD para ayudarlo a crear sus aplicacio nes compatibles con la HIPAA. AWS ofrece un documento técnico centrado en la HIPAA para los clientes que estén interesados en obtener más información sobre cómo pueden aprovechar AWS el procesamiento y el almacenamiento de la información de salud. Para obtener más información, consulte Conformid ad con HIPAA.

Responsabilidad compartida

La seguridad, incluida la conformidad con FedRAMP, HIPAA y PCI, es una responsabilidad compartida. Es importante entender que el estado de conformidad con Microsoft AD AWS administrado no se aplica automáticamente a las aplicaciones que se ejecutan en la AWS nube. Debe asegurarse de que el uso de los AWS servicios cumpla con los estándares.

Para obtener una lista completa de los distintos programas de AWS conformidad compatibles con AWS Managed Microsoft AD, consulta AWS los servicios incluidos en el ámbito de aplicación por programa de conformidad.

Habilite el cumplimiento de PCI para su directorio AWS administrado de Microsoft AD

Para habilitar la conformidad con PCI en su directorio AWS administrado de Microsoft AD, debe configurar políticas de contraseñas detalladas tal como se especifica en el documento de certificación de conformidad (AOC) y resumen de responsabilidad de PCI DSS proporcionado por. AWS Artifact

Para obtener más información acerca del uso de políticas de contraseñas detalladas, consulte Administrar las políticas de contraseñas para AWS Managed Microsoft AD.

Mejorar la configuración de seguridad de la red de AWS Managed Microsoft AD

El grupo de seguridad de AWS que se aprovisiona para el directorio de AWS Managed Microsoft AD se configura con los puertos de red entrantes mínimos necesarios para admitir todos los casos de uso conocidos del directorio de AWS Managed Microsoft AD. Para obtener más información sobre el grupo de seguridad de AWS aprovisionado, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD.

Para mejorar aún más la seguridad de red de su directorio de AWS Managed Microsoft AD puede modificar el grupo de seguridad de AWS en función de los escenarios comunes que se muestran a continuación.

Temas

Compatibilidad solo con aplicaciones de AWS

Todas las cuentas de usuario se aprovisionan solo en AWS Managed Microsoft AD para utilizarse con aplicaciones de AWS compatibles, como las siguientes:

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

Puede utilizar la siguiente configuración de grupo de seguridad de AWS para bloquear todo el tráfico no esencial a los controladores de dominio de AWS Managed Microsoft AD.

> **Note**
>
> - Lo que se muestra a continuación no es compatible con la configuración de este grupo de seguridad de AWS:
> - Instancias de Amazon EC2
> - Amazon FSx
> - Amazon RDS para MySQL
> - Amazon RDS para Oracle
> - Amazon RDS para PostgreSQL
> - Amazon RDS para SQL Server
> - WorkSpaces
> - Relaciones de confianza de Active Directory
> - Clientes o servidores unidos al dominio

Reglas entrantes

Ninguno.

Reglas salientes

Ninguno.

Solo aplicaciones de AWS con compatibilidad con relaciones de confianza

Todas las cuentas de usuario se aprovisionan en AWS Managed Microsoft AD o Active Directory de confianza para utilizarlas con aplicaciones de AWS compatibles, como las siguientes:

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

Puede modificar la configuración del grupo de seguridad de AWS aprovisionado para bloquear todo el tráfico no esencial en los controladores de dominio de AWS Managed Microsoft AD.

> **Note**
>
> - Lo que se muestra a continuación no es compatible con la configuración de este grupo de seguridad de AWS:
> - Instancias de Amazon EC2
> - Amazon FSx
> - Amazon RDS para MySQL
> - Amazon RDS para Oracle
> - Amazon RDS para PostgreSQL
> - Amazon RDS para SQL Server
> - WorkSpaces
> - Relaciones de confianza de Active Directory
> - Clientes o servidores unidos al dominio
> - Esta configuración requiere que se asegure de que la red “CIDR en las instalaciones” sea segura.

- TCP 445 se utiliza solo para la creación de relaciones de confianza y se puede eliminar una vez establecida la relación de confianza.
- TCP 636 solo se requiere cuando LDAP a través de SSL está en uso.

Reglas entrantes

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP y UDP	53	CIDR en las instalaciones	DNS	Autenticación de usuarios y equipos, resolución de nombres, relaciones de confianza
TCP y UDP	88	CIDR en las instalaciones	Kerberos	Autenticación de usuarios y equipos, relaciones de confianza de nivel de bosque
TCP y UDP	389	CIDR en las instalaciones	LDAP	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza
TCP y UDP	464	CIDR en las instalaciones	Cambiar/e stablecer	Replicación, autenticación de usuarios

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
			contraseña de Kerberos	y equipos, relaciones de confianza
TCP	445	CIDR en las instalaciones	SMB/CIFS	Replicación, autenticación de usuarios y equipos, relaciones de confianza de políticas de grupo
TCP	135	CIDR en las instalaciones	Replicación	RPC, EPM
TCP	636	CIDR en las instalaciones	LDAP SSL	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza
TCP	49152 - 65535	CIDR en las instalaciones	RPC	Replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP	3268 - 3269	CIDR en las instalaciones	LDAP GC y LDAP GC SSL	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza
UDP	123	CIDR en las instalaciones	Hora de Windows	Hora de Windows, relaciones de confianza

Reglas salientes

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
Todos	Todos	CIDR en las instalaciones	Todo el tráfico	

Compatibilidad de cargas de trabajo de Active Directory nativas y de aplicaciones de AWS

Las cuentas de usuario se aprovisionan solo en AWS Managed Microsoft AD para utilizarse con aplicaciones de AWS compatibles, como las siguientes:

- Amazon Chime
- Amazon Connect
- Instancias de 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

Puede modificar la configuración del grupo de seguridad de AWS aprovisionado para bloquear todo el tráfico no esencial en los controladores de dominio de AWS Managed Microsoft AD.

> **Note**
>
> - Las relaciones de confianza de Active Directory no se pueden crear ni mantener entre el directorio de AWS Managed Microsoft AD y el dominio en las instalaciones.
> - Requiere asegurarse de que la red "CIDR cliente" es segura.
> - TCP 636 solo se requiere cuando LDAP a través de SSL está en uso.
> - Si desea utilizar una CA empresarial con esta configuración, deberá crear una regla de salida "TCP, 443, CA CIDR".

Reglas entrantes

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP y UDP	53	CIDR cliente	DNS	Autenticación de usuarios y equipos, resolución de nombres,

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
				relaciones de confianza
TCP y UDP	88	CIDR cliente	Kerberos	Autenticación de usuarios y equipos, relaciones de confianza de nivel de bosque
TCP y UDP	389	CIDR cliente	LDAP	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza
TCP y UDP	445	CIDR cliente	SMB/CIFS	Replicación, autenticación de usuarios y equipos, relaciones de confianza de políticas de grupo
TCP y UDP	464	CIDR cliente	Cambiar/e stablecer contraseña de Kerberos	Replicación, autenticación de usuarios y equipos, relaciones de confianza

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP	135	CIDR cliente	Replicación	RPC, EPM
TCP	636	CIDR cliente	LDAP SSL	Política de grupo de autenticación de directorios, replicación, usuarios y equipos, relaciones de confianza
TCP	49152 - 65535	CIDR cliente	RPC	Replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza
TCP	3268 - 3269	CIDR cliente	LDAP GC y LDAP GC SSL	Política de grupo de autenticación de directorios, replicación, usuarios y equipos, relaciones de confianza
TCP	9389	CIDR cliente	SOAP	Servicios web de AD DS
UDP	123	CIDR cliente	Hora de Windows	Hora de Windows, relaciones de confianza

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
UDP	138	CIDR cliente	DFSN & NetLogon	DFS, política de grupo

Reglas salientes

Ninguno.

Compatibilidad de cargas de trabajo de Active Directory nativas y de aplicaciones de AWS que admiten relaciones de confianza

Todas las cuentas de usuario se aprovisionan en AWS Managed Microsoft AD o Active Directory de confianza para utilizarlas con aplicaciones de AWS compatibles, como las siguientes:

- Amazon Chime
- Amazon Connect
- Instancias de 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

Puede modificar la configuración del grupo de seguridad de AWS aprovisionado para bloquear todo el tráfico no esencial en los controladores de dominio de AWS Managed Microsoft AD.

> **Note**
>
> - Requiere que se asegure de que las redes “CIDR en las instalaciones” y “CIDR cliente” sean seguras.
> - TCP 445 con “CIDR en las instalaciones” se utiliza solo para la creación de relaciones de confianza y se puede eliminar después de que se haya establecido la relación de confianza.
> - TCP 445 con "CIDR cliente" debe dejarse abierto ya que es necesario para el procesamiento de la política de grupo.
> - TCP 636 solo se requiere cuando LDAP a través de SSL está en uso.
> - Si desea utilizar una CA empresarial con esta configuración, deberá crear una regla de salida "TCP, 443, CA CIDR".

Reglas entrantes

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP y UDP	53	CIDR en las instalaciones	DNS	Autenticación de usuarios y equipos, resolución de nombres, relaciones de confianza
TCP y UDP	88	CIDR en las instalaciones	Kerberos	Autenticación de usuarios y equipos, relaciones de confianza de nivel de bosque
TCP y UDP	389	CIDR en las instalaciones	LDAP	Política de grupo de autentica

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
				ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza
TCP y UDP	464	CIDR en las instalaciones	Cambiar/e stablecer contraseña de Kerberos	Replicación, autenticación de usuarios y equipos, relaciones de confianza
TCP	445	CIDR en las instalaciones	SMB/CIFS	Replicación, autenticación de usuarios y equipos, relaciones de confianza de políticas de grupo
TCP	135	CIDR en las instalaciones	Replicación	RPC, EPM
TCP	636	CIDR en las instalaciones	LDAP SSL	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP	49152 - 65535	CIDR en las instalaciones	RPC	Replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza
TCP	3268 - 3269	CIDR en las instalaciones	LDAP GC y LDAP GC SSL	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza
UDP	123	CIDR en las instalaciones	Hora de Windows	Hora de Windows, relaciones de confianza
TCP y UDP	53	CIDR cliente	DNS	Autenticación de usuarios y equipos, resolución de nombres, relaciones de confianza

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP y UDP	88	CIDR cliente	Kerberos	Autenticación de usuarios y equipos, relaciones de confianza de nivel de bosque
TCP y UDP	389	CIDR cliente	LDAP	Política de grupo de autentica ción de directori os, replicaci ón, usuarios y equipos, relaciones de confianza
TCP y UDP	445	CIDR cliente	SMB/CIFS	Replicación, autenticación de usuarios y equipos, relaciones de confianza de políticas de grupo
TCP y UDP	464	CIDR cliente	Cambiar/e stablecer contraseña de Kerberos	Replicación, autenticación de usuarios y equipos, relaciones de confianza
TCP	135	CIDR cliente	Replicación	RPC, EPM

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
TCP	636	CIDR cliente	LDAP SSL	Política de grupo de autenticación de directorios, replicación, usuarios y equipos, relaciones de confianza
TCP	49152 - 65535	CIDR cliente	RPC	Replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza
TCP	3268 - 3269	CIDR cliente	LDAP GC y LDAP GC SSL	Política de grupo de autenticación de directorios, replicación, usuarios y equipos, relaciones de confianza
TCP	9389	CIDR cliente	SOAP	Servicios web de AD DS
UDP	123	CIDR cliente	Hora de Windows	Hora de Windows, relaciones de confianza

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
UDP	138	CIDR cliente	DFSN & NetLogon	DFS, política de grupo

Reglas salientes

Protocolo	Rango de puerto	Origen	Tipo de tráfico	Uso de Active Directory
Todos	Todos	CIDR en las instalaciones	Todo el tráfico	

Establecimiento de la configuración de seguridad del directorio

Puede configurar ajustes de directorio detallados para AWS Managed Microsoft AD a fin de cumplir con los requisitos de conformidad y seguridad sin aumentar la carga de trabajo operativa. En la configuración del directorio, puede actualizar la configuración del canal seguro para los protocolos y cifrados utilizados en él. Por ejemplo, tiene la flexibilidad de deshabilitar los cifrados heredados individuales, como RC4 o DES, y los protocolos, como SSL 2.0/3.0 y TLS 1.0/1.1. AWS Luego, Managed Microsoft AD implementa la configuración en todos los controladores de dominio del directorio, administra los reinicios de los controladores de dominio y mantiene esta configuración a medida que escala horizontalmente o implementa más Regiones de AWS. Para más información sobre la configuración disponible, consulte Lista de la configuración de seguridad del directorio.

Editar la configuración de seguridad del directorio

Puede configurar y editar los ajustes de cualquiera de los directorios.

Para editar la configuración del directorio

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Directory Service en https://console.aws.amazon.com/directoryservicev2/.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En Redes y seguridad, busque Configuración del directorio y, a continuación, seleccione Editar configuración.

4. En Editar configuración, cambie el valor de la configuración que quiera editar. Al editar una configuración, su estado cambia de Predeterminado a Listo para actualizarse. Si ha editado la configuración anteriormente, su estado cambia de Actualizado a Preparado para actualizarse. A continuación, seleccione Revisar.
5. En Revisar y actualizar la configuración, consulte Configuración del directorio y asegúrese de que todos los nuevos valores sean correctos. Si quiere hacer cualquier otro cambio en la configuración, seleccione Editar configuración. Cuando esté satisfecho con los cambios y esté listo para implementar los nuevos valores, seleccione Actualizar configuración. A continuación, volverá a la página del ID del directorio.

> **Note**
>
> En Configuración del directorio, puede ver el estado de la configuración actualizada. Mientras se implementa la configuración, el estado muestra Actualización. No puede editar otros ajustes mientras uno muestre Actualización en Estado. El estado muestra Actualizado si la configuración se actualiza correctamente con su edición. El estado muestra Error si la configuración no se actualiza con la edición.

Configuración de seguridad del directorio con errores

Si se produce un error durante una actualización de la configuración, el estado se muestra como Con errores. En caso de error, la configuración no se actualiza a los nuevos valores y los valores originales permanecen implementados. Puede volver a intentar actualizar esta configuración o revertirla a sus valores anteriores.

Para resolver un error en la configuración actualizada

- En Configuración del directorio, seleccione Resolver la configuración con errores. A continuación, lleve a cabo alguna de las operaciones siguientes:
  - Para restablecer la configuración a su valor original antes del estado de error, seleccione Revertir la configuración con errores. A continuación, selecciona Revertir en el modal emergente.
  - Para volver a intentar actualizar la configuración del directorio, seleccione Reintentar la configuración con errores. Si quiere hacer cambios adicionales en la configuración del directorio antes de volver a intentar las actualizaciones con errores, seleccione Continuar

editando. En Revisar y volver a intentar las actualizaciones con errores, seleccione Actualizar configuración.

Lista de la configuración de seguridad del directorio

La siguiente lista muestra el tipo, el nombre de la configuración, el nombre de la API, los valores potenciales y la descripción de todas las configuraciones de seguridad del directorio disponibles.

TLS 1.2 y AES 256/256 son las configuraciones de seguridad del directorio predeterminadas si todas las demás configuraciones de seguridad están deshabilitadas. No es posible deshabilitarlas.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
Autenticación basada en certificados	Compensación por retroactividad del certificado	CERTIFICATE_BACKDATING_COMPENSATION	Años: 0 a 50 Meses: 0 a 11 Días: 0 a 30 Horario: 0 a 23 Minutos: 0 a 59 Segundos: 0 a 59	Especifique un valor para indicar el tiempo durante el que un certificado puede ser anterior a un usuario de Active Directory y seguir utilizándose para la autenticación en Active Directory. El valor predeterminado es 10 minutos. Puede

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
				configurar este valor desde 1 segundo hasta 50 años. Para configurar este ajuste, debe seleccionar el tipo de compatibilidad para un cumplimiento estricto de la vinculación de certificados. Para obtener más información, consulte KB5014754: cambios en la autenticación basada en certificados en los controladores de dominio de Windows en la documentación de Microsoft Support.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	Cumplimiento estricto del certificado	CERTIFICATE_STRONG_ENFORCEMENT	Compatibilidad, cumplimiento total	Especifique cualquiera de los siguientes tipos de cumplimiento: • Compatibilidad (predeterminada): se permite la autenticación si un certificado no se puede asignar de forma segura a un usuario. Si el certificado es anterior a la cuenta de usuario de Active Directory, también debe configurar la compensación por retroactividad del

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
				certificado o se producirá un error en la autenticación. • Cumplimiento total: no se permite la autenticación si un certificado no se puede asignar de forma estricta a un usuario. Si elige este tipo de cumplimiento, no se puede configurar la compensación por retroactividad del certificado. Para obtener más información, consulte

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
				KB5014754: cambios en la autenticación basada en certificados en los controladores de dominio de Windows en la documentación de Microsoft Support.
Canal seguro: cifrado	AES 128/128	AES_128_128	Habilitar, deshabilitar	Active o desactive el cifrado AES 128/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	DES 56/56	DES_56_56	Habilitar, deshabilitar	Active o desactive el cifrado DES 56/56 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.
	RC2 40/128	RC2_40_128	Habilitar, deshabilitar	Active o desactive el cifrado RC2 40/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	RC2 56/128	RC2_56_128	Habilitar, deshabilitar	Active o desactive el cifrado RC2 56/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.
	RC2 128/128	RC2_128_128	Habilitar, deshabilitar	Active o desactive el cifrado RC2 128/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	RC4 40/128	RC4_40_128	Habilitar, deshabilitar	Active o desactive el cifrado RC4 40/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.
	RC4 56/128	RC4_56_128	Habilitar, deshabilitar	Active o desactive el cifrado RC4 56/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	RC4 64/128	RC4_64_128	Habilitar, deshabilitar	Active o desactive el cifrado RC4 64/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.
	RC4 128/128	RC4_128_128	Habilitar, deshabilitar	Active o desactive el cifrado RC4 128/128 para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	DES 168/168 triple	3DES_168_168	Habilitar, deshabilitar	Active o desactive el cifrado DES 168/168 triple para garantizar la seguridad de las comunicaciones entre los controladores de dominio de su directorio.
Canal seguro: protocolo	PCT 1.0	PCT_1_0	Habilitar, deshabilitar	Active o desactive el protocolo PCT 1.0 para las comunicaciones de canal seguro (servidor y cliente) en los controladores de dominio de su directorio.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	SSL 2.0	SSL_2_0	Habilitar, deshabilitar	Active o desactive el protocolo SSL 2.0 para las comunicaciones de canal seguro (servidor y cliente) en los controladores de dominio de su directorio.
	SSL 3.0	SSL_3_0	Habilitar, deshabilitar	Active o desactive el protocolo SSL 3.0 para las comunicaciones de canal seguro (servidor y cliente) en los controladores de dominio de su directorio.

Tipo	Nombre de la configuración	Nombre de API	Valores potenciales	Descripción de la configuración
	TLS 1.0	TLS_1_0	Habilitar, deshabilitar	Active o desactive el protocolo TLS 1.0 para las comunicaciones de canal seguro (servidor y cliente) en los controladores de dominio de su directorio.
	TLS 1.1	TLS_1_1	Habilitar, deshabilitar	Active o desactive el protocolo TLS 1.1 para las comunicaciones de canal seguro (servidor y cliente) en los controladores de dominio de su directorio.

Configurar el AWS Private CA conector para AD

Puede integrar su Microsoft AD AWS administrado con AWS Private Certificate Authority (CA) para emitir y administrar certificados para los usuarios, grupos y máquinas unidos al dominio de Active Directory. AWS Private CA Connector for Active Directory le permite utilizar un sustituto AWS Private

CA directo y totalmente gestionado para sus CA empresariales autogestionadas sin necesidad de implementar, aplicar parches o actualizar agentes locales o servidores proxy.

> **Note**
>
> No se admite la inscripción de certificados LDAPS del lado del servidor para controladores de dominio AWS Microsoft AD administrados con AWS Private CA Connector for Active Directory. Para habilitar el LDAPS del lado del servidor para su directorio, consulte Cómo habilitar el LDAPS del lado del servidor para su AWS directorio administrado de Microsoft AD.

Puede configurar la AWS Private CA integración con su directorio a través de la consola Directory Service, la consola AWS Private CA Connector for Active Directory o llamando a la `CreateTemplate`API. Para configurar la integración de una CA privada a través de la consola de AWS Private CA Connector for Active Directory, consulte Creación de una plantilla de conector. Consulte a continuación los pasos para configurar esta integración desde la AWS Directory Service consola.

Para configurar AWS Private CA Connector para AD

1. Inicie sesión en AWS Management Console y abra la AWS Directory Service consola enhttps://console.aws.amazon.com/directoryservicev2/.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la pestaña Red y seguridad, en AWS Private CA Conector para AD, selecciona Configurar AWS Private CA conector para AD. Active DirectoryAparece la página Crear un certificado de CA privado para. Siga los pasos de la consola para crear su CA privada para que el Active Directory conector se inscriba en su CA privada. Para obtener más información, consulte Creación de un conector.
4. Después de crear el conector, siga los pasos que se indican a continuación para ver los detalles, incluido el estado del conector y el estado de la entidad de certificación (CA) privada asociada.

Para ver AWS Private CA Connector for AD

1. Inicie sesión en AWS Management Console y abra la AWS Directory Service consola enhttps://console.aws.amazon.com/directoryservicev2/.

2. En la página Directories (Directorios), elija el ID del directorio.
3. En Redes y seguridad, en Conector para AD deAWS Private CA , puede ver sus tanto sus conectores de entidad de certificación (CA) privados como las entidades de certificación (CA) asociadas. De forma predeterminada, verá los siguientes campos:
   a. AWS Private CA ID de conector: el identificador único de un AWS Private CA conector. Al hacer clic en él, se accede a la página de detalles de ese AWS Private CA conector.
   b. AWS Private CA asunto: información sobre el nombre distintivo de la CA. Al hacer clic en él, se accede a la página de detalles de AWS Private CA.
   c. Estado: basado en una verificación de estado del AWS Private CA conector y del AWS Private CA. Si se aprueban ambas comprobaciones, aparecerá Activo. Si una de las comprobaciones falla, aparece 1/2 comprobaciones con errores. Si ambas comprobaciones fallan, aparece Error. Para obtener más información sobre un estado fallido, coloque el puntero del ratón sobre el hipervínculo para saber qué comprobación tuvo errores. Siga las instrucciones de la consola para solucionarlo.
   d. Fecha de creación: el día en que se creó el AWS Private CA conector.

Para obtener más información, consulte View connector details.

Supervisión de su AWS Managed Microsoft AD

Puede supervisar su directorio de AWS Managed Microsoft AD con los siguientes métodos:

Temas

Descripción del estado del directorio

Estos son los diferentes estados de un directorio.

Activo

El directorio funciona con normalidad. AWS Directory Service no ha detectado problemas en su directorio.

Creando

El directorio se está creando en estos momentos. Los directorios suelen tardar entre 20 y 45 minutos en crearse, pero esto depende de la carga del sistema.

Eliminado

El directorio se ha eliminado. Se han liberado todos los recursos para el directorio. Una vez que un directorio entra en este estado, no se puede recuperar.

Eliminando

El directorio se está eliminando. El directorio permanecerá en este estado hasta que se haya eliminado por completo. Una vez que un directorio entra en este estado, la operación de eliminación no se puede cancelar y el directorio no se puede recuperar.

Con error

No se pudo crear el directorio. Elimine este directorio. Si este problema sigue sin resolverse, contacte con el Centro de AWS Support.

Deteriorado

El directorio se está ejecutando en estado degradado. Se han detectado uno o varios problemas y no todas las operaciones de directorios pueden funcionar con plena capacidad operativa. Hay muchas razones posibles para que el directorio se encuentre en este estado. Entre ellas se incluyen las actividades normales de mantenimiento operativo, como la aplicación de parches o la rotación de instancias de EC2, la sobrecarga provocada por una aplicación en uno de los controladores de dominio o los cambios que haga en la red que interrumpan de forma inadvertida las comunicaciones del directorio. Para obtener más información, consulte Solución de problemas de Microsoft AD AWS administrado, Solución de problemas de Conector AD y Solución de problemas de Simple AD. En el caso de problemas normales relacionados con el mantenimiento, los AWS resuelve en 40 minutos. Si después de revisar el tema de solución de problemas, su directorio sigue dañado durante más de 40 minutos, le recomendamos que contacte con el Centro de AWS Support.

> **Important**
>
> No restaure una instantánea mientras el directorio esté deteriorado. Es poco frecuente que la restauración de las instantáneas sea necesaria para resolver los problemas. Para obtener más información, consulte Creación de una instantánea o restauración del directorio.

Solicitada

Actualmente hay pendiente una solicitud para crear su directorio.

RestoreFailed

Error al restaurar el directorio a partir de una instantánea. Vuelva a intentar restaurarlo. Si el problema continúa, use otra instantánea o contacte con el Centro de AWS Support.

Restauración

El directorio se está restaurando actualmente a partir de una instantánea automática o manual. La restauración a partir de una instantánea suele tardar unos minutos, en función del tamaño del directorio de datos en la instantánea.

Configurar las notificaciones de estado del directorio con Amazon SNS

Mediante Amazon Simple Notification Service (Amazon SNS), puede recibir mensajes de correo electrónico o de texto (SMS) cuando cambie el estado del directorio. Recibirá una notificación si su directorio pasa de un estado activo a uno deteriorado. También recibirá una notificación cuando el directorio vuelva a estar en estado activo.

Cómo funciona

Amazon SNS utiliza “temas” para recopilar y distribuir mensajes. Cada tema cuenta con uno o varios suscriptores que reciben los mensajes que se han publicado en dicho tema. Si sigue los pasos que se indican a continuación, puede añadir AWS Directory Service un editor a un tema de Amazon SNS. Cuando AWS Directory Service detecta un cambio en el estado de su directorio, publica un mensaje sobre ese tema, que luego se envía a los suscriptores del tema.

Puede asociar varios directorios como publicadores a un único tema. También puede agregar mensajes de estado del directorio a los temas que ha creado anteriormente en Amazon SNS. Tiene

un control detallado sobre quién puede publicar un tema y suscribirse a él. Para obtener información completa sobre Amazon SNS, consulte ¿Qué es Amazon SNS?.

> **Note**
>
> Las notificaciones de estado del directorio son una función regional de AWS Managed Microsoft AD. Si utiliza Replicación multirregional, los siguientes procedimientos se deberán aplicar por separado en cada región. Para obtener más información, consulte Características globales frente a las regionales.

Habilitación de la mensajería SNS para su directorio

1. Inicie sesión en la AWS Directory Service consola AWS Management Console y ábrala.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiere habilitar la mensajería SNS y, a continuación, elija la pestaña Mantenimiento. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, elija la pestaña Mantenimiento.
4. En la sección Supervisión de directorios, elija Acciones y, a continuación, seleccione Crear notificación.
5. En la página Crear notificación, seleccione Elegir un tipo de notificación y, a continuación, Crear una nueva notificación. También, si ya dispone de un tema de SNS, puede seleccionar Asociar un tema de SNS existente para enviar mensajes de estado desde este directorio a ese tema.

   > **Note**
   >
   > Si elige Crear una nueva notificación, pero, a continuación, utiliza el mismo nombre para un tema de SNS que ya existe, Amazon SNS no creará un nuevo tema, sino que tan solo agregará la información de la nueva suscripción al existente.
   > Si selecciona Asociar tema de SNS existentes, solo podrá elegir un tema de SNS que se encuentre en la misma región que el directorio.

6. Elija una opción en Tipo de destinatario e ingrese la información del contacto en Destinatario. Si escribe un número de teléfono para SMS, utilice solo números. No incluya guiones, espacios o paréntesis.
7. (Opcional) Proporcione un nombre para su tema y un nombre de visualización de SNS. El nombre de visualización es una abreviatura de hasta 10 caracteres que se incluye en todos los mensajes SMS de este tema. Cuando se utiliza la opción de SMS, es necesario el nombre de visualización.

> **Note**
>
> Si ha iniciado sesión con un usuario o rol de IAM que solo tiene la política DirectoryServiceFullAccessadministrada, el nombre del tema debe empezar por «DirectoryMonitoring». Si desea personalizar aún más su nombre de tema necesitará privilegios adicionales de SNS.

8. Seleccione Crear.

Si desea designar suscriptores de SNS adicionales, como una dirección de correo electrónico adicional, colas de Amazon SQS, AWS Lambda o puede hacerlo desde la consola de Amazon SNS.

Habilitación de mensajes de estado del directorio de un tema

1. Inicie sesión en la consola AWS Management Console y ábrala.AWS Directory Service
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que desee eliminar los mensajes de estado y, a continuación, seleccione la pestaña Mantenimiento. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, elija la pestaña Mantenimiento.
4. En la sección Supervisión de directorios, seleccione un nombre de tema de SNS de la lista, elija Acciones y, a continuación, seleccione Eliminar.
5. Elija Eliminar.

Así eliminará su directorio como publicador en el tema de SNS seleccionado. Si quieres eliminar todo el tema, puedes hacerlo desde la consola de Amazon SNS.

> **Note**
>
> Antes de eliminar un tema de Amazon SNS mediante la consola de SNS, debe asegurarse de que un directorio no está enviando mensajes de estado a dicho tema.
> Si elimina un tema de Amazon SNS mediante la consola de SNS, este cambio no se reflejará inmediatamente en la consola de Directory Services. Solo se le informaría la próxima vez que un directorio publique una notificación en el tema eliminado, en cuyo caso vería un estado actualizado en la pestaña Monitoring del directorio que indica que no se ha encontrado el tema.
> Por lo tanto, para evitar perder mensajes importantes sobre el estado del directorio, antes de eliminar cualquier tema del que reciba mensajes AWS Directory Service, asocie su directorio a un tema diferente de Amazon SNS.

Revisión de los logs de su directorio de AWS Managed Microsoft AD

Los registros de seguridad de las instancias del controlador de dominios de AWS Managed Microsoft AD se archivan durante un año. También puede configurar su directorio de AWS Managed Microsoft AD para que reenvíe los registros del controlador de dominio a Registros de Amazon CloudWatch casi en tiempo real. Para obtener más información, consulte Habilitación del reenvío de registros.

AWS registra los siguientes eventos relacionados con cuestiones de conformidad.

Categoría de monitorización	Configuración de la política	Estado de la auditoría
Inicio de sesión de la cuenta	Auditar validación de credenciales	Correcto o error
	Auditar otros eventos de inicio de sesión de la cuenta	Correcto o error
Administración de cuentas	Auditar administración de cuentas de equipo	Correcto o error

Categoría de monitorización	Configuración de la política	Estado de la auditoría
	Auditar otros eventos de administración de cuentas	Correcto o error
	Auditar administración de grupos de seguridad	Correcto o error
	Auditar administración de cuentas de usuario	Correcto o error
Seguimiento detallado	Auditar la actividad DPAPI	Correcto o error
	Auditar la actividad PNP	Correcto
	Auditar creación de procesos	Correcto o error
Acceso DS	Auditar el acceso del servicio de directorio	Correcto o error
	Auditar cambios de servicio de directorio	Correcto o error
Inicio/cierre de sesión	Auditar el bloqueo de cuentas	Correcto o error
	Auditar cierre de sesión	Correcto
	Auditar inicio de sesión	Correcto o error
	Auditar otros eventos de inicio de sesión o cierre de sesión	Correcto o error
	Auditar inicio de sesión especial	Correcto o error
Acceso de objetos	Auditar otros eventos de acceso a objetos	Correcto o error
	Auditar almacenamiento extraíble	Correcto o error

Categoría de monitorización	Configuración de la política	Estado de la auditoría
	Auditar almacenamiento provisional de directiva de acceso central	Correcto o error
Cambio de políticas	Auditar el cambio de políticas	Correcto o error
	Auditar cambio de política de autenticación	Correcto o error
	Auditar cambio de política de autorización	Correcto o error
	Auditar el cambio de política de nivel de regla de MPSSVC	Correcto
	Auditar otros eventos de cambio de política	Error
Uso de privilegios	Auditar uso de privilegios confidenciales	Correcto o error
System (Sistema)	Auditoría controlador IPsec	Correcto o error
	Auditar otros eventos del sistema	Correcto o error
	Auditar cambio de estado de seguridad	Correcto o error
	Auditar extensión del sistema de seguridad	Correcto o error
	Auditar integridad del sistema	Correcto o error

Habilitación del reenvío de registros

Puede utilizar la consola o las API de AWS Directory Service para reenviar registros de eventos de seguridad del controlador de dominio a Registros de Amazon CloudWatch. Esto le permite cumplir sus requisitos de políticas de retención de registros, auditorías y monitorización de seguridad proporcionando transparencia a los eventos de seguridad del directorio.

Registros de CloudWatch también puede reenviar estos eventos a otras cuentas de AWS, servicios de AWS y a aplicaciones de terceros. Esto facilita la monitorización y la configuración centralizadas de las alertas para detectar actividades anormales casi en tiempo real y responder a ellas de manera proactiva.

Una vez habilitado el reenvío de registros, puede utilizar la consola de Registros de CloudWatch para recuperar los datos del grupo de registro que especificó al habilitar el servicio. Este grupo de registros contiene los registros de seguridad de sus controladores de dominio.

Para obtener más información sobre los grupos de registros y cómo leer sus datos, consulte Trabajo con grupos y flujos de registro en la Guía del usuario de Registros de Amazon CloudWatch.

> **Note**
>
> El reenvío de registros es una característica regional de AWS Managed Microsoft AD. Si utiliza Replicación multirregional, los siguientes procedimientos se deberán aplicar por separado en cada región. Para obtener más información, consulte Características globales frente a las regionales.

Para habilitar el reenvío de registros

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. Elija el ID de directorio del directorio de AWS Managed Microsoft AD que desea compartir.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiera habilitar el reenvío de registros y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.

4. En la sección Log forwarding (Reenvío de registros), elija Enable (Habilitar).
5. En el cuadro de diálogo Enable log forwarding to CloudWatch (Habilitar el reenvío de registros a CloudWatch), elija una de las siguientes opciones:
   a. Seleccione Crear un nuevo grupo de registro de CloudWatch y, en Nombre del grupo de registro, especifique un nombre al que puede hacer referencia en Registros de CloudWatch.
   b. Seleccione Choose an existing CloudWatch log group (Elija un grupo de registros de CloudWatch) y en Existing CloudWatch log groups (Grupos de registros de CloudWatch existentes), seleccione un grupo de registro en el menú.
6. Revise el enlace y la información sobre los precios y, a continuación, elija Enable (Habilitar).

Para deshabilitar el reenvío de registros

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. Elija el ID de directorio del directorio de AWS Managed Microsoft AD que desea compartir.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiera deshabilitar el reenvío de registros y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Log forwarding (Reenvío de registros), elija Disable (Deshabilitar).
5. Una vez que haya leído la información del cuadro de diálogo Disable log forwarding (Deshabilitar reenvío de registros), elija Disable (Deshabilitar).

Uso de la CLI para habilitar el reenvío de registros

Para poder utilizar el comando `ds create-log-subscription`, primero debe crear un grupo de registro de Amazon CloudWatch y, a continuación, crear una política de recursos de IAM que concederá los permisos necesarios a ese grupo. Para habilitar el reenvío de registros mediante la CLI, realice todos los pasos que se indican a continuación.

Paso 1: crear un grupo de registro en Registros de CloudWatch

Cree un grupo de registros que se utilizará para recibir los registros de seguridad de los controladores de dominio. Recomendamos que el nombre vaya precedido de `/aws/directoryservice/`, pero esto no es obligatorio. Por ejemplo:

EJEMPLO DE COMANDO DE LA CLI

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

EJEMPLO DE COMANDO DE POWERSHELL

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

Para obtener información acerca de cómo crear un grupo de registros, consulte Crear un grupo de registro en Registros de CloudWatch en la Guía del usuario de Registros de Amazon CloudWatch.

Paso 2: crear una política de recursos de Registros de CloudWatch en IAM

Cree una política de recursos de Registros de CloudWatch que conceda derechos a AWS Directory Service para agregar registros al grupo de registros nuevo creado en el paso 1. Puede especificar el ARN exacto del grupo de registros para limitar el acceso de AWS Directory Service a otros grupos de registros o utilizar un comodín para incluir todos los grupos de registros. La siguiente política de ejemplo utiliza el método del comodín para indicar que se incluirán todos los grupos de registros que empiecen por `/aws/directoryservice/` pertenecientes a la cuenta de AWS donde reside el directorio.

```
{
    "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/*"
        }
```

```
    ]
}
```

Tendrá que guardar esta política en un archivo de texto (por ejemplo, DSPolicy.json) en la estación de trabajo local, ya que deberá ejecutarla desde la CLI. Por ejemplo:

EJEMPLO DE COMANDO DE LA CLI

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

EJEMPLO DE COMANDO DE POWERSHELL

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

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

Paso 3: crear una suscripción de registro de AWS Directory Service

En este último paso, ya puede proceder a habilitar el reenvío de registros mediante la creación de la suscripción de registro. Por ejemplo:

EJEMPLO DE COMANDO DE LA CLI

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

EJEMPLO DE COMANDO DE POWERSHELL

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

Supervisión de sus controladores de dominio con métricas de rendimiento

AWS Directory Service se integra con Amazon CloudWatch para ayudarte a proporcionarte importantes métricas de rendimiento para cada controlador de dominio de tuActive Directory. Esto significa que puede supervisar los contadores de rendimiento de los controladores de dominio, como el uso de la CPU y la memoria. También puede configurar alarmas e iniciar acciones automatizadas para responder a los períodos de uso elevado. Por ejemplo, puede configurar una alarma para un uso de la CPU del controlador de dominio superior al 70 % y crear un tema de SNS que le notifique cuando esto ocurra. Puedes usar este tema de SNS para iniciar la automatización, como AWS

Lambda las funciones, a fin de aumentar el número de controladores de dominio para tu Active Directory empresa.

Para obtener más información sobre la supervisión de los controladores de dominio, consulte Determine cuándo agregar controladores de dominio con CloudWatch métricas.

Hay tarifas asociadas a Amazon CloudWatch. Para obtener más información, consulta CloudWatchfacturación y coste.

> **Important**
>
> Las métricas de rendimiento de los CloudWatch controladores de dominio no están disponibles en la región Canadá Oeste (Calgary).

Encuentre las métricas de rendimiento de los controladores de dominio en CloudWatch

En la CloudWatch consola de Amazon, las métricas de un servicio determinado se agrupan primero por el espacio de nombres del servicio. Puede agregar filtros de métricas que estén subordinados a ese espacio de nombres. Utilice el siguiente procedimiento para localizar el espacio de nombres y la métrica subordinada correctos que se requieren para configurar las métricas del controlador de dominio de AWS Microsoft AD administrado en. CloudWatch

Para buscar las métricas del controlador de dominio en la consola CloudWatch

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. En la lista de métricas, seleccione el espacio de nombres llamado Servicio de directorio y, a continuación, en la lista, seleccione la métrica AWS Managed Microsoft AD.

Para obtener instrucciones sobre cómo configurar las métricas del controlador de dominio mediante la CloudWatch consola, consulte Cómo automatizar el escalado AWS administrado de Microsoft AD en función de las métricas de uso en el blog AWS de seguridad.

Determine cuándo agregar controladores de dominio con CloudWatch métricas

El equilibrio de carga entre todos los controladores de dominio es importante para garantizar la resiliencia y el rendimiento de los mismosActive Directory. Para ayudarlo a optimizar el rendimiento

de sus controladores de dominio en Microsoft AD AWS administrado, le recomendamos que primero supervise las métricas importantes CloudWatch para formar una línea de base. Durante este proceso, analizas tu uso a Active Directory lo largo del tiempo para identificar tu uso promedio y Active Directory máximo. Tras determinar tu punto de referencia, puedes supervisar estas métricas de forma regular para ayudarte a determinar cuándo añadir un controlador de dominio a tu empresaActive Directory.

Es importante supervisar las siguientes métricas de forma periódica. Para obtener una lista completa de las métricas de los controladores de dominio disponibles en CloudWatch, consulteAWS Contadores de rendimiento gestionados de Microsoft AD.

- Métricas específicas del controlador de dominio, como:
  - Procesador
  - Memoria
  - Disco lógico
  - Interfaz de red
- AWS Métricas administradas específicas del directorio de Microsoft AD, como:
  - Búsquedas de LDAP
  - Enlaces
  - Consultas de DNS
  - Lecturas del directorio
  - Escrituras del directorio

Para obtener instrucciones sobre cómo configurar las métricas del controlador de dominio mediante la CloudWatch consola, consulte Cómo automatizar el escalado AWS administrado de Microsoft AD en función de las métricas de uso en el blog AWS de seguridad. Para obtener información general sobre las métricas en CloudWatch, consulta Uso de CloudWatch las métricas de Amazon en la Guía del CloudWatch usuario de Amazon.

Para obtener información general sobre la planificación de controladores de dominio, consulte Planificación de la capacidad de los servicios de Active Directory dominio en el sitio web de Microsoft.

AWS Contadores de rendimiento gestionados de Microsoft AD

En la siguiente tabla se enumeran todos los contadores de rendimiento disponibles en Amazon CloudWatch para realizar un seguimiento del rendimiento del controlador de dominio y del directorio en AWS Managed Microsoft AD.

Categoría métrica	Nombre de métrica
Base de datos ==> Instancias (NTDSA)	% de aciertos de la caché de la base de datos
	Latencia media de lecturas de la base de datos de E/S
	Lecturas de la base de datos de E/S por segundo
	Latencia media de escrituras de registros de E/S
DirectoryServices (NTDS)	Tiempo de enlace de LDAP
	Operaciones de replicación pendientes de DRA
	Sincronizaciones de replicación pendientes de DRA
DNS	Consultas recursivas por segundo
	Error de consulta recursiva por segundo
	Consultas de TCP recibidas por segundo
	Consultas totales recibidas por segundo
	Respuestas totales enviadas por segundo
	Consultas de UDP recibidas por segundo
LogicalDisk	Prom. Longitud de la cola de disco
	% de espacio libre

Categoría métrica	Nombre de métrica
Memoria	% de bytes confirmados en uso
	Tiempo de conservación medio de la caché en espera a largo plazo (s)
Interfaz de red	Bytes enviados por segundo
	Bytes recibidos por segundo
	Ancho de banda actual
NTDS	Retraso de cola estimado de ATQ
	Latencia de solicitudes de ATQ
	Lecturas del directorio DS por segundo
	Búsquedas en el directorio DS por segundo
	Escrituras en el directorio DS por segundo
	Sesiones de clientes LDAP
	Búsquedas LDAP por segundo
	Enlaces LDAP correctos por segundo
Procesador	% de tiempo de procesador
Estadísticas de seguridad para todo el sistema	Autenticaciones de Kerberos
	Autenticaciones de NTLM

Replicación multirregional

La replicación multirregional se puede utilizar para replicar automáticamente los datos del directorio AWS administrado de Microsoft AD en varios Regiones de AWSdirectorios. Esta replicación puede mejorar el rendimiento de los usuarios y las aplicaciones en ubicaciones geográficas dispersas. AWS

Microsoft AD administrado utiliza la replicación nativa de Active Directory para replicar los datos del directorio de forma segura en la nueva región.

La replicación multirregional solo se admite en la edición Enterprise de AWS Managed Microsoft AD.

Puede utilizar la replicación multirregional automatizada en la mayoría de las regiones en las que esté disponible AWS Managed Microsoft AD.

> **Important**
>
> La replicación multirregional no está disponible en las siguientes regiones opcionales:
>
> - África (Ciudad del Cabo) (af-south-1)
> - Asia-Pacífico (Hong Kong) ap-east-1
> - Asia Pacífico (Hyderabad): ap-south-2
> - Asia-Pacífico (Yakarta): ap-southeast-3
> - Asia Pacífico (Melbourne): ap-southeast-4
> - Canadá Oeste (Calgary) ca-west-1
> - UE (Milán) (eu-south-1)
> - Europa (España): eu-south-2
> - Europa (Zúrich): eu-central-2
> - Israel (Tel Aviv) il-central-1
> - Medio Oriente (Baréin) me-south-1
> - Medio Oriente (EAU): me-central-1
>
> Para obtener más información sobre las regiones de suscripción voluntaria y cómo habilitarlas, consulte Especificar qué regiones puede usar Regiones de AWS su cuenta en la Guía.AWS Account Management

Ventajas

Con la replicación multirregional en Microsoft AD AWS administrado, las aplicaciones compatibles con Active Directory utilizan el directorio de forma local para lograr un alto rendimiento y la función multirregión para aumentar la resiliencia. Puede utilizar la replicación multirregional con aplicaciones compatibles con Active Directory, como SQL Server SharePoint Always On, así como con AWS

servicios como Amazon RDS for SQL Server y fSx for Windows File Server. Los siguientes son beneficios adicionales de la replicación de varias regiones.

- Le permite implementar una única instancia de Microsoft AD AWS administrada de forma global y rápida, y elimina la ardua tarea de autoadministrar una infraestructura global de Active Directory.
- Hace que sea más fácil y rentable implementar y administrar las cargas de trabajo de Windows y Linux en varias AWS regiones. La replicación automatizada en varias regiones permite un rendimiento óptimo en sus aplicaciones globales compatibles con Active Directory. Todas las aplicaciones implementadas en instancias de Windows o Linux utilizan Microsoft AD AWS administrado de forma local en la región, lo que permite responder a las solicitudes de los usuarios desde la región más cercana posible.
- Proporciona resiliencia multirregional. Implementado en la infraestructura AWS administrada de alta disponibilidad, AWS Managed Microsoft AD gestiona las actualizaciones de software automatizadas, la supervisión, la recuperación y la seguridad de la infraestructura de Active Directory subyacente en todas las regiones. Esto le permite centrarse en compilar sus aplicaciones.

Temas

Características globales frente a las regionales

Cuando agrega una AWS región a su directorio mediante la replicación multirregional, AWS Directory Service mejora el alcance de todas las funciones para que se adapten a las regiones. Estas características aparecen en varias pestañas de la página de detalles que aparece al elegir el ID de un directorio en la consola de AWS Directory Service . Esto significa que todas las características están habilitadas, configuradas o administradas en función de la región que seleccione en la sección replicación multirregional de la consola. Los cambios que haga en las características de cada región se aplican de forma global o por región.

La replicación multirregional solo se admite en la edición Enterprise de AWS Managed Microsoft AD.

Características globales

Todos los cambios que haga en las características globales mientras esté seleccionado Región principal se aplicarán en todas las regiones.

Puede identificar las características que se utilizan de manera global en la página Detalles del directorio, ya que junto a ellas aparece Se ha aplicado a todas las regiones replicadas. Como alternativa, si ha seleccionado otra región de la lista que no sea la región principal, puede identificar las características utilizadas a nivel mundial porque muestran Heredados de la región principal.

Características regionales

Los cambios que haga en una característica de Región adicional se aplicarán únicamente a esa región.

Puede identificar las características que son regionales en la página Detalles del directorio, ya que junto a ellas no aparece Aplicadas a todas las regiones replicadas o Heredadas de la región principal.

Regiones principales frente a las adicionales

Con la replicación multirregional, AWS Managed Microsoft AD utiliza los dos tipos de regiones siguientes para diferenciar la forma en que se deben aplicar las características globales o regionales en todo el directorio.

Región principal

La región inicial en la que creó el directorio por primera vez se denomina región principal. Solo puede hacer operaciones a nivel de directorio global, como crear relaciones de confianza de Active Directory y actualizar el esquema de AD desde la región principal.

La región principal siempre se puede identificar como la primera región que aparece en la parte superior de la lista de la sección de Replicación multirregional y termina con : principal. Por ejemplo, Este de EE. UU. (Norte de Virginia): principal.

Todos los cambios que haga en Características globales mientras esté seleccionada la región principal se aplicarán en todas las regiones.

Solo puede agregar regiones mientras la región principal esté seleccionada. Para obtener más información, consulte Agregar una región replicada.

Región adicional

Todas las regiones que haya agregado a su directorio se denominan regiones adicionales.

Si bien algunas características se pueden administrar de forma global para todas las regiones, otras se administran de forma individual por región. Para administrar una característica de una región adicional (región no principal), primero debe seleccionar la región adicional de la lista de la sección de Replicación multirregional de la página Detalles del directorio. A continuación, puede proceder a administrar la característica.

Cualquier cambio que haga a Características regionales mientras esté seleccionada una región adicional se aplicará solo a esa región.

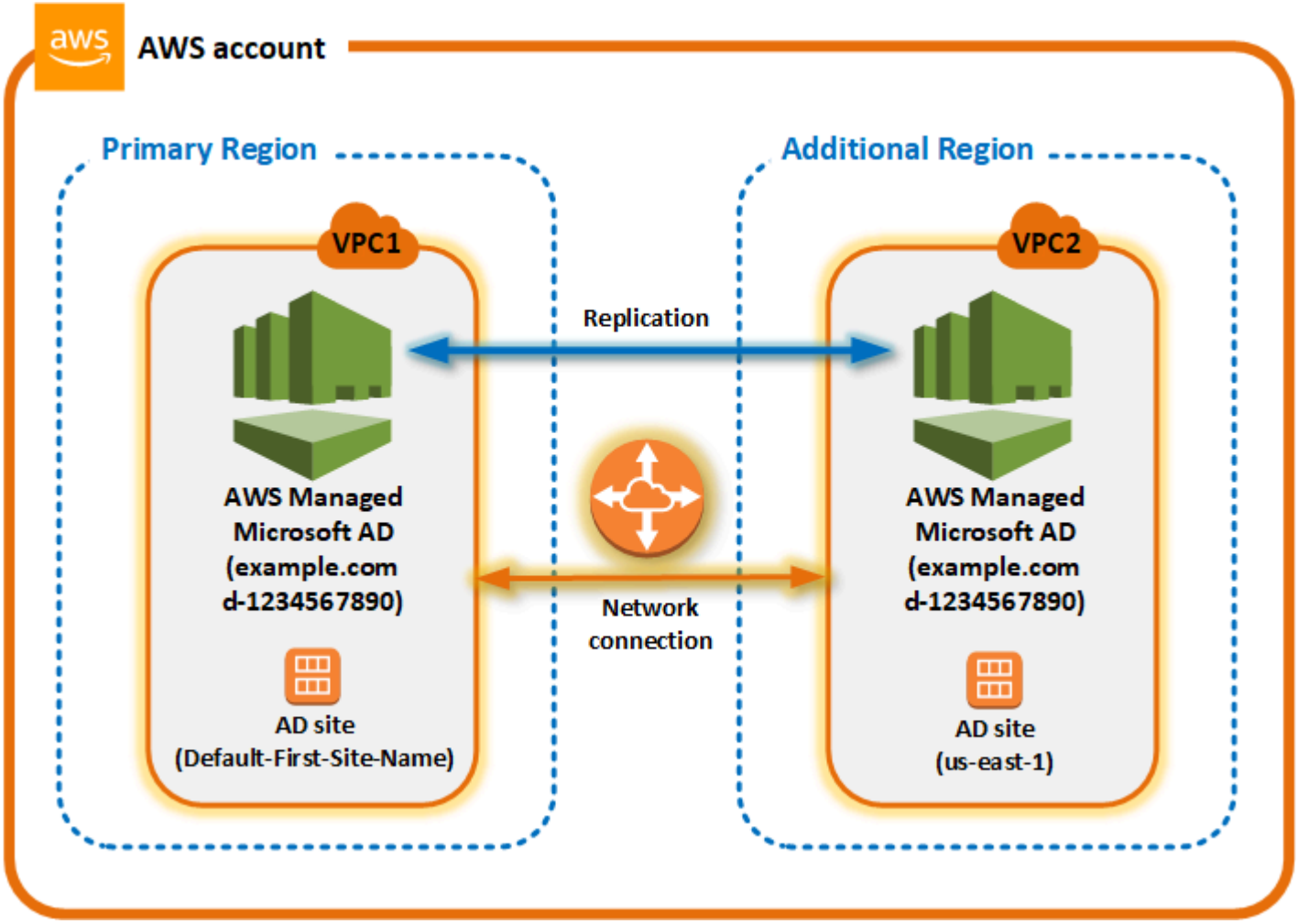
Funcionamiento de la replicación multirregional

Con la función de replicación multirregional, AWS Managed Microsoft AD elimina el trabajo pesado e indiferenciado de administrar una infraestructura global de Active Directory. Cuando se configura, AWS replica todos los datos del directorio de clientes, incluidos los usuarios, los grupos, las políticas de grupo y el esquema, en varias regiones. AWS

Una vez que se ha agregado una nueva región, se llevan a cabo automáticamente las siguientes operaciones, como se muestra en la ilustración:

- AWS Microsoft AD administrado crea dos controladores de dominio en la VPC seleccionada y los implementa en la nueva región de la misma cuenta. AWS El identificador de directorio (`directory_id`) sigue siendo el mismo en todas las regiones. Puede agregar controladores de dominio adicionales más adelante, si lo desea.
- AWS Microsoft AD administrado configura la conexión de red entre la región principal y la nueva región.
- AWS Microsoft AD administrado crea un nuevo sitio de Active Directory y le asigna el mismo nombre que la región, como us-east-1. También puede cambiarle el nombre más adelante con la herramienta Sitios y servicios de Active Directory.
- AWS Microsoft AD administrado replica todos los objetos y configuraciones de Active Directory en la nueva región, incluidos los usuarios, los grupos, las políticas de grupo, las confianzas de Active Directory, las unidades organizativas y el esquema de Active Directory. Los enlaces a sitios de Active Directory están configurados para usar Notificación de cambios. Si la notificación de cambios entre sitios está habilitada, los cambios se propagan al sitio remoto con la misma frecuencia con la que se propagan dentro del sitio de origen, incluidos los cambios que requieren una replicación urgente.

- Si es la primera región que agregas, AWS Managed Microsoft AD hace que todas las funciones sean compatibles con múltiples regiones. Para obtener más información, consulte Características globales frente a las regionales.



Sitios de Active Directory

La replicación multirregional admite varios sitios de Active Directory (un sitio de Active Directory por región). Cuando se agrega una región nueva, se le da el mismo nombre que a la región (por ejemplo, us-east-1). También puede cambiarle el nombre más adelante con Sitios y servicios de Active Directory.

AWS servicios

AWS servicios como Amazon RDS for SQL Server y Amazon FSx se conectan a las instancias locales del directorio global. Esto permite a los usuarios iniciar sesión una vez en las aplicaciones compatibles con Active Directory que se ejecutan, así AWS como en AWS servicios como Amazon

RDS for SQL Server, en cualquier región. AWS Para ello, los usuarios necesitan credenciales de Microsoft AD AWS administrado o de Active Directory local cuando tengan una confianza en su Microsoft AD AWS administrado.

Puede usar los siguientes AWS servicios con la función de replicación 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

Conmutación por error

En caso de que todos los controladores de dominio de una región estén inactivos, AWS Managed Microsoft AD recupera los controladores de dominio y replica los datos del directorio automáticamente. Mientras tanto, los controladores de dominio de otras regiones seguirán en funcionamiento.

Agregar una región replicada

Al añadir una región mediante la Replicación multirregional función, AWS Managed Microsoft AD crea dos controladores de dominio en la AWS región seleccionada, Amazon Virtual Private Cloud (VPC) y la subred. AWS Managed Microsoft AD también crea los grupos de seguridad relacionados que permiten que las cargas de trabajo de Windows se conecten al directorio de la nueva región. También crea estos recursos con la misma AWS cuenta en la que ya está implementado el directorio. Para ello, debe elegir la región, especificar la VPC y proporcionar las configuraciones para la nueva región.

La replicación multirregional solo se admite en la edición Enterprise de AWS Managed Microsoft AD.

Requisitos previos

Antes de continuar con los pasos de adición de una nueva región de replicación, lo recomendamos revisar las siguientes tareas de requisitos previos.

- Compruebe que tiene los permisos AWS Identity and Access Management (IAM) necesarios, la configuración de Amazon VPC y la configuración de subred en la nueva región en la que quiere replicar el directorio.
- Si quiere usar sus credenciales de Active Directory locales existentes para acceder a las cargas de trabajo compatibles con Active Directory y administrarlas AWS, debe crear una confianza de Active Directory entre AWS Microsoft AD administrado y su infraestructura de AD local. Para obtener más información acerca de las relaciones de confianza, consulte Conéctese a su infraestructura de Active Directory existente.
- Si ya tiene una relación de confianza entre su Active Directory local y desea añadir una región replicada, debe comprobar que dispone de la configuración de subred y VPC de Amazon necesaria en la nueva región en la que quiere replicar el directorio.

Adición de una región

Utilice el siguiente procedimiento para agregar una región replicada al directorio AWS administrado de Microsoft AD.

Para agregar una región replicada

1. En el panel de navegación de la consola deAWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, en Replicación multirregional, elija la región principal de la lista y, a continuación, elija Agregar región.

   > **Note**
   >
   > Solo puede agregar regiones mientras la región principal esté seleccionada. Para obtener más información, consulte Región principal .

4. En la página Agregar región, en Región, elija la región que quiera agregar de la lista.
5. En VPC, elija la VPC que quiera usar en esta región.

> **Note**
>
> Esta VPC no debe tener un enrutamiento entre dominios sin clases (CIDR) que se superponga con una VPC utilizada por este directorio en otra región.

6. En Subredes, elija la subred que quiera usar en esta región.
7. Revise la información en Precios y, a continuación, seleccione Agregar..
8. Cuando AWS Managed Microsoft AD complete el proceso de implementación del controlador de dominio, la región mostrará el estado Activa. Ahora puede hacer actualizaciones en esta región según sea necesario.

Siguientes pasos

Después de agregar una nueva región, se recomiendan los siguientes pasos:

- Implemente controladores de dominio adicionales (hasta 20) en la nueva región según sea necesario. De forma predeterminada, el número de controladores de dominio al agregar una nueva región es 2, que es el mínimo requerido por motivos de tolerancia a errores y alta disponibilidad. Para obtener más información, consulte Agregar o quitar controladores de dominio adicionales.
- Comparta su directorio con más AWS cuentas por región. Las configuraciones de uso compartido de directorios no se replican automáticamente desde la región principal. Para obtener más información, consulte Compartir el directorio.
- Activa el reenvío de registros para recuperar los registros de seguridad de tu directorio mediante Amazon CloudWatch Logs de la nueva región. Al habilitar el reenvío de registros, debe proporcionar un nombre del grupo de registros en cada región en la que haya replicado el directorio. Para obtener más información, consulte Habilitación del reenvío de registros.
- Active la supervisión de Amazon Simple Notification Service (Amazon SNS) de la nueva región para hacer un seguimiento del estado del directorio por región. Para obtener más información, consulte Configurar las notificaciones de estado del directorio con Amazon SNS.

Delegar una región replicada

Utilice el siguiente procedimiento para eliminar una región del directorio AWS administrado de Microsoft AD. Antes de eliminar una región, asegúrese de que no tenga ninguno de los siguientes elementos:

- Aplicaciones autorizadas adjuntas a ella.
- Directorios compartidos asociados a ella.

Eliminación de una región replicada

1. En el panel de navegación de la consola deAWS Directory Service, elija Directories (Directorios).
2. En la barra de navegación, seleccione el selector Regiones y, a continuación, seleccione la región en la que está almacenado el directorio.
3. En la página Directories (Directorios), elija el ID del directorio.
4. En la página Detalles del directorio, en Replicación multirregional, elija Eliminar región.
5. En el cuadro de diálogo Eliminar región, revise la información y, a continuación, ingrese el nombre de la región para confirmar. A continuación, elija Eliminar.

> **Note**
>
> No puede hacer actualizaciones en la región mientras se está eliminando.

Compartir el directorio

AWS Managed Microsoft AD se integra sin problemas con AWS Organizations para permitir el uso compartido sencillo de varias cuentas de AWS. Puede compartir un directorio único con otras cuentas de AWS de confianza dentro de la misma organización o compartir el directorio con otras cuentas de AWS que están fuera de su organización. También puede compartir su directorio cuando su cuenta de AWS no es actualmente miembro de una organización.

> **Note**
>
> AWS cobra un cargo adicional por el uso compartido del directorio. Para obtener más información, consulte la página Precios en el sitio web de AWS Directory Service.

El uso compartido del directorio hace que AWS Managed Microsoft AD sea una forma más rentable de integración con Amazon EC2 en varias cuentas y VPC. El uso compartido de directorios está disponible en todas las regiones de AWS donde se ofrece AWS Managed Microsoft AD.

> **Note**
>
> En la región de AWS China (Ningxia), esta característica solo está disponible cuando se utiliza AWS Systems Manager (SSM) para unir fácilmente sus instancias de Amazon EC2.

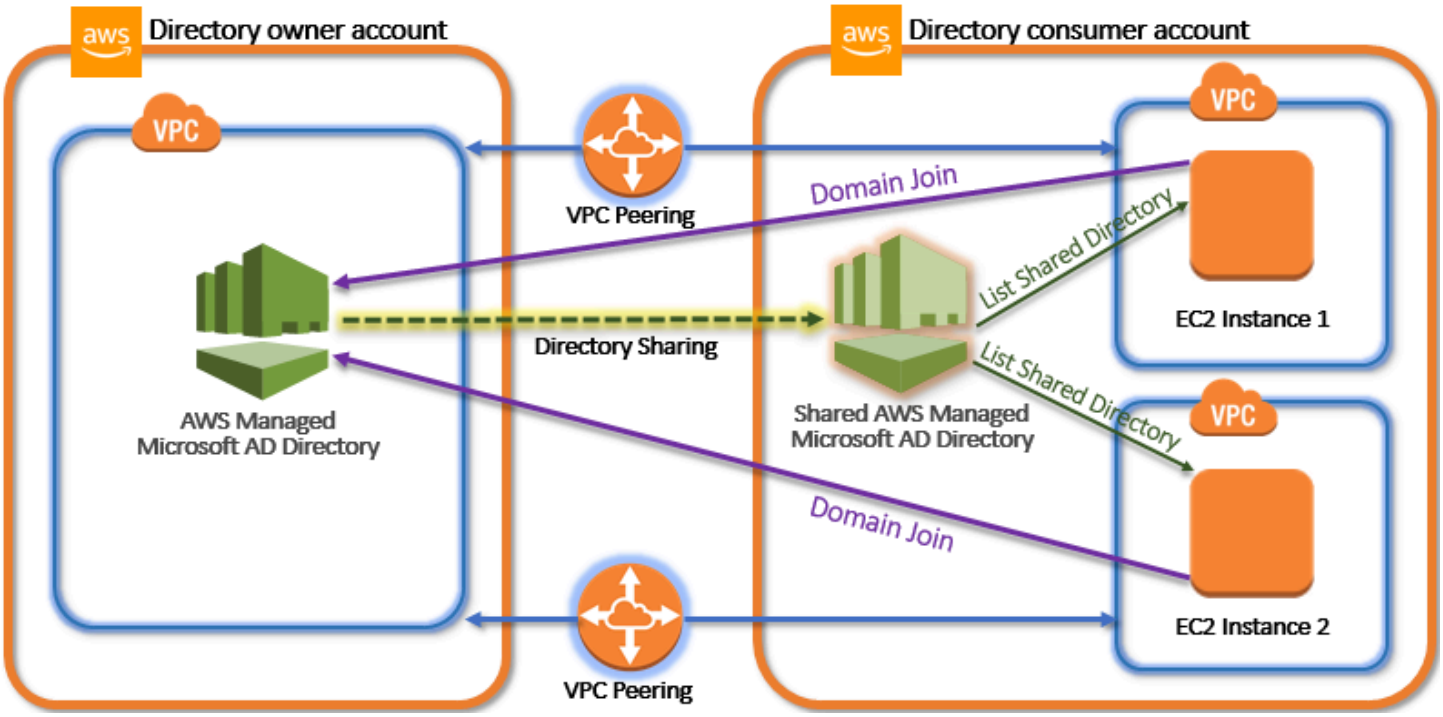
Para obtener más información acerca del uso compartido de directorios y cómo ampliar el alcance de su directorio de AWS Managed Microsoft AD más allá de los límites de una cuenta de AWS, consulte los siguientes temas.

Temas

- Conceptos clave de uso compartido de directorios
- Tutorial: Cómo compartir su directorio AWS gestionado de Microsoft AD para unirse a dominios EC2 sin problemas
- Dejar de compartir el directorio

Conceptos clave de uso compartido de directorios

Sacará el máximo partido de la característica de uso compartido de directorio si se familiariza con los siguientes conceptos clave.



Cuenta del propietario de directorio

Un propietario de directorio es el titular de la Cuenta de AWS que posee el directorio de origen en la relación de directorio compartido. Un administrador de esta cuenta inicia el flujo de trabajo de uso compartido de directorio especificando las Cuentas de AWS con las que compartir su directorio. Los propietarios del directorio pueden ver con quién han compartido un directorio utilizando la pestaña Scale & Share (Escalar y compartir) para un directorio determinado en la consola de AWS Directory Service.

Cuenta del consumidor de directorio

En una relación de directorio compartido, un consumidor de directorio representa la Cuenta de AWS con la que el propietario del directorio ha compartido el directorio. En función del método de uso compartido utilizado, es posible que un administrador de esta cuenta tenga que aceptar la invitación enviada por el propietario del directorio antes de que pueda comenzar a utilizar el directorio compartido.

El proceso de uso compartido del directorio crea un directorio compartido en la cuenta del consumidor de directorio. Este directorio compartido contiene los metadatos que permiten a la instancia EC2 unirse fácilmente al dominio, que localiza el directorio de origen en la cuenta del propietario del directorio. Cada directorio compartido en la cuenta del consumidor de directorio tiene un identificador único (Shared directory ID [ID de directorio compartido]).

Métodos de uso compartido

AWS Managed Microsoft AD proporciona los dos métodos de uso compartido de directorio siguientes:

- AWS Organizations: este método facilita compartir el directorio en su organización ya que puede examinar y validar las cuentas del consumidor de directorio. Para utilizar esta opción, la organización debe tener habilitada Todas las características y el directorio debe estar en la cuenta de administración de la organización. Este método de uso compartido simplifica la configuración, ya que no se requiere que las cuentas de consumidor del directorio acepten su solicitud de uso compartido del directorio. En la consola, este método se denomina Compartir este directorio con otras Cuentas de AWS de la organización.
- Protocolo de enlace: este método permite compartir directorios cuando no utiliza AWS Organizations. El método de protocolo de enlace requiere que la cuenta del consumidor del directorio acepte la solicitud de uso compartido del directorio. En la consola, este método se denomina Compartir este directorio con otras Cuentas de AWS.

La conectividad de red

La conectividad de red es un requisito previo para utilizar una relación de uso compartido de directorios entre Cuentas de AWS. AWS admite muchas soluciones para conectar sus VPC, algunas de las cuales incluyen interconexión con la VPC, Transit Gateway y VPN. Para empezar, consulte Tutorial: Cómo compartir su directorio AWS gestionado de Microsoft AD para unirse a dominios EC2 sin problemas.

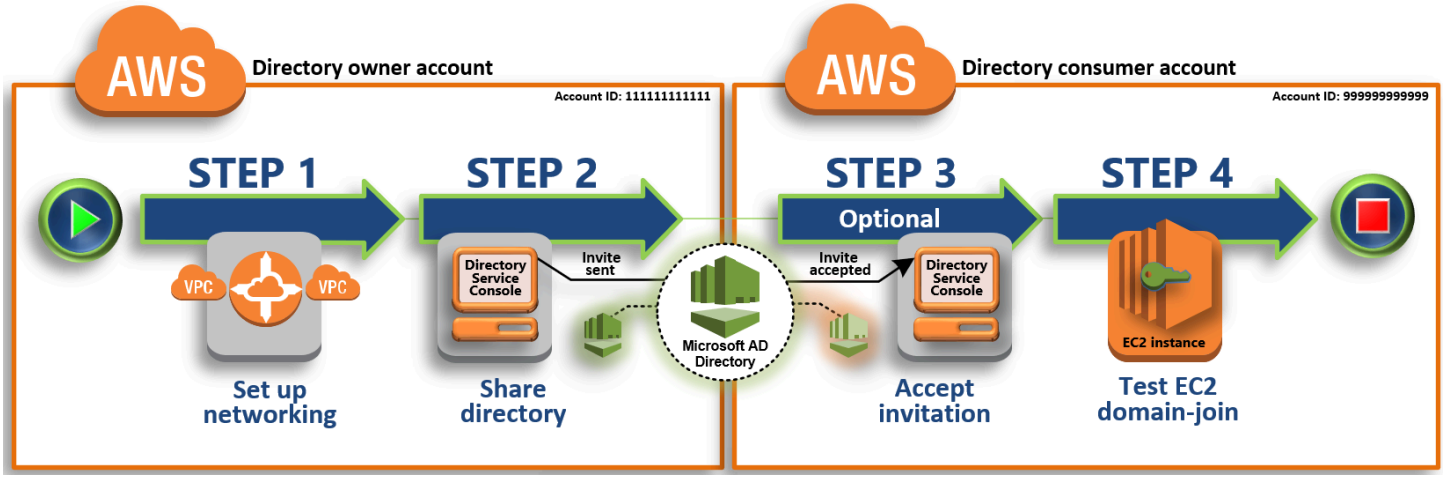
Tutorial: Cómo compartir su directorio AWS gestionado de Microsoft AD para unirse a dominios EC2 sin problemas

Este tutorial le muestra cómo compartir su directorio AWS administrado de Microsoft AD (la cuenta del propietario del directorio) con otro Cuenta de AWS (la cuenta del consumidor del directorio). Una vez cumplidos los requisitos de red, compartirás un directorio entre dos Cuentas de AWS. A continuación, aprenderá a unir de forma fluida una instancia EC2 a un dominio en la cuenta del consumidor de directorio.

Le recomendamos que revise primero los conceptos clave de uso compartido de directorios y utilice el contenido de caso de uso antes de comenzar a trabajar con este tutorial. Para obtener más información, consulte Conceptos clave de uso compartido de directorios.

El proceso para compartir el directorio varía en función de si se comparte el directorio con otra Cuenta de AWS persona de la misma AWS organización o con una cuenta ajena a la AWS organización. Para obtener más información sobre cómo funciona el uso compartido, consulte Métodos de uso compartido.

Este flujo de trabajo incluye cuatro pasos básicos.



Paso 1: configuración del entorno de red

En la cuenta del propietario de directorio, configure todos los requisitos previos de red necesarios para el proceso de uso compartido de directorio.

Paso 2: uso compartido el directorio

Cuando haya iniciado sesión con credenciales de administrador de propietario del directorio, abra la consola de AWS Directory Service y comience el flujo de trabajo de uso compartido de directorio, que envía una invitación a la cuenta del consumidor de directorio.

Paso 3: Aceptar la invitación a un directorio compartido (opcional)

Al iniciar sesión con las credenciales de administrador consumidor del directorio, debe abrir la AWS Directory Service consola y aceptar la invitación para compartir el directorio.

Paso 4: prueba de la unión fluida de una instancia de EC2 para Windows Server a un dominio

Por último, como administrador de consumidor de directorio, intente unir una instancia EC2 a su dominio y verifique que funciona.

Recursos adicionales

- Caso de uso: compartir su directorio para unir sin problemas instancias de Amazon EC2 a un dominio a través de Cuentas de AWS
- AWS Artículo del blog de seguridad: Cómo unir instancias de Amazon EC2 de varias cuentas y VPC a un único directorio administrado de AWS Microsoft AD

Paso 1: configuración del entorno de red

Antes de comenzar los pasos de este tutorial, debe hacer lo siguiente:

- Cree dos nuevas Cuentas de AWS para realizar pruebas en la misma región. Al crear una Cuenta de AWS, se crea automáticamente una nube privada virtual (VPC) dedicada en cada cuenta. Tome nota del ID de VPC en cada cuenta. Necesitará este valor más adelante.
- Cree una interconexión con VPC entre las dos VPC en cada cuenta utilizando los procedimientos que se indican en este paso.

> **Note**
>
> Aunque hay muchas maneras de conectar las VPC de la cuenta del propietario de directorio y del consumidor de directorio, este tutorial utilizará el método de interconexión con la VPC. Para ver otras opciones de conectividad con la VPC, consulte La conectividad de red.

Configuración de una conexión de emparejamiento de VPC entre la cuenta del propietario de directorio y la del consumidor de directorio

La interconexión de VPC que creará es entre las VPC del consumidor de directorio y del propietario de directorio. Siga estos pasos para configurar una interconexión con VPC para conectividad con la cuenta del consumidor de directorio. Con esta conexión puede dirigir el tráfico entre ambas VPC mediante direcciones IP privadas.

Creación de una conexión de emparejamiento de VPC entre la cuenta del propietario de directorio y la del consumidor de directorio

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. Asegúrese de iniciar sesión como usuario con credenciales de administrador en la cuenta del propietario de directorio.
2. En el panel de navegación, elija Peering Connections. A continuación, elija Create Peering Connection (Crear interconexión).
3. Configure la información siguiente:
   - Peering connection name tag (Etiqueta de nombre de interconexión): Proporcione un nombre que identifique claramente esta conexión con la VPC en la cuenta del consumidor de directorio.
   - VPC (Requester) [VPC (Solicitante)]: Seleccione el ID de VPC para la cuenta del propietario de directorio.
   - En Select another VPC to peer with (Seleccionar otra VPC para interconexión), asegúrese de que My account (Mi cuenta) y This region (Esta región) estén seleccionados.
   - VPC (Accepter) [VPC (Receptora)]: Seleccione el ID de VPC para la cuenta del consumidor de directorio.

4. Elija Create Peering Connection (Crear interconexión). En el cuadro de diálogo de confirmación, elija OK.

Dado que ambas VPC se encuentran en la misma región, el administrador de la cuenta del propietario de directorio que envió la solicitud de interconexión de VPC también puede aceptar la solicitud de interconexión en nombre de la cuenta del consumidor de directorio.

Aceptación de la solicitud de interconexión en nombre de la cuenta del consumidor de directorio

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Peering Connections.
3. Seleccione la interconexión de VPC pendiente. (Su estado es Pendiente de aceptación). Elija Actions (Acciones), Accept Request (Aceptar solicitud).
4. En el cuadro de diálogo de confirmación, elija Yes, Accept. En el siguiente cuadro de diálogo de confirmación, elija Modify my route tables now (Modificar mis tablas de ruteo ahora) para ir directamente a la página de tablas de ruteo.

Ahora que su interconexión de VPC está activa, deberá añadir una entrada en la tabla de ruteo de su VPC en la cuenta del propietario de directorio. De esta forma, permite el direccionamiento del tráfico a la VPC en la cuenta del consumidor de directorio.

Adición de una entrada a la tabla de ruteo de VPC en la cuenta del propietario de directorio

1. Mientras esté en la sección Tablas de enrutamiento de la consola de Amazon VPC, seleccione la tabla de enrutamiento para la VPC de propietario de directorio.
2. En la pestaña Rutas, elija Editar rutas y, a continuación, Agregar ruta.
3. En la columna Destination (Destino), escriba el bloque de CIDR de la VPC de consumidor de directorio.
4. En la columna Target (Objetivo), escriba el ID de interconexión de VPC (por ejemplo, **`pcx-123456789abcde000`**) para la interconexión que creó anteriormente en la cuenta del propietario de directorio.
5. Elija Guardar cambios.

Adición de una entrada a la tabla de ruteo de VPC en la cuenta del consumidor de directorio

1. Mientras esté en la sección Tablas de enrutamiento de la consola de Amazon VPC, seleccione la tabla de enrutamiento para la VPC de consumidor de directorio.
2. En la pestaña Rutas, elija Editar rutas y, a continuación, Agregar ruta.
3. En la columna Destination (Destino), escriba el bloque de CIDR de la VPC de propietario de directorio.
4. En la columna Target (Objetivo), escriba el ID de interconexión de VPC (por ejemplo, **`pcx-123456789abcde001`**) para la interconexión que creó anteriormente en la cuenta del consumidor de directorio.
5. Elija Guardar cambios.

Asegúrese de configurar el grupo de seguridad de las VPC de consumidor de directorio para habilitar el tráfico saliente añadiendo los puertos y protocolos de Active Directory a la tabla de reglas salientes. Para obtener más información, consulte Grupos de seguridad para su VPC y Requisitos previos de AWS Managed Microsoft AD.

Paso siguiente

Paso 2: uso compartido el directorio

Paso 2: uso compartido el directorio

Utilice los siguientes procedimientos para iniciar el flujo de trabajo de uso compartido del directorio desde la cuenta del propietario de directorio.

> **Note**
>
> El uso compartido de directorios es una función regional de AWS Managed Microsoft AD. Si utiliza Replicación multirregional, los siguientes procedimientos se deberán aplicar por separado en cada región. Para obtener más información, consulte Características globales frente a las regionales.

Uso compartido de su directorio desde la cuenta del propietario de directorio

1. Inicie sesión AWS Management Console con las credenciales de administrador de la cuenta del propietario del directorio y abra la AWS Directory Service consola en https://console.aws.amazon.com/directoryservicev2/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija el ID de directorio del directorio AWS administrado de Microsoft AD que desee compartir.
4. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiera compartir el directorio y, a continuación, seleccione la pestaña Escalar y compartir. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Escalar y compartir.
5. En la sección Shared directories (Directorios compartidos), seleccione Actions (Acciones) y, a continuación, elija Create new shared directory (Crear nuevo directorio compartido).
6. En la página Elige con Cuentas de AWS quién quieres compartir, elige uno de los siguientes métodos de uso compartido en función de las necesidades de tu empresa:
   a. Comparta este directorio con Cuentas de AWS miembros de su organización: con esta opción, puede seleccionar el directorio con el Cuentas de AWS que desea compartir el directorio de una lista que muestra todo el contenido Cuentas de AWS interno de su AWS organización. Debe habilitar el acceso de confianza AWS Directory Service antes de compartir un directorio. Para obtener más información, consulte Cómo habilitar o deshabilitar el acceso de confianza.

      > **Note**
      > Para utilizar esta opción, la organización debe tener habilitada Todas las características y el directorio debe estar en la cuenta de administración de la organización.

      i. Cuentas de AWS En su organización, seleccione la carpeta con la Cuentas de AWS que desee compartir el directorio y haga clic en Agregar.
      ii. Revise la información sobre precios y luego seleccione Share (Compartir).

iii. Continúe en el Paso 4 de esta guía. Como todos Cuentas de AWS pertenecen a la misma organización, no es necesario que siga el paso 3.

b. Compartir este directorio con otros Cuentas de AWS: con esta opción, puede compartir un directorio con cuentas de dentro o fuera de su AWS organización. También puede usar esta opción cuando su directorio no sea miembro de una AWS organización y desee compartirlo con otra Cuenta de AWS.

   i. En ID de Cuenta de AWS , escriba todos los ID de Cuenta de AWS con los que desea compartir el directorio y, a continuación, haga clic en Agregar.

   ii. En Enviar una nota, escriba un mensaje al administrador en la otra Cuenta de AWS.

   iii. Revise la información sobre precios y luego seleccione Share (Compartir).

   iv. Continúe con el paso 3.

Paso siguiente

Paso 3: Aceptar la invitación a un directorio compartido (opcional)

Paso 3: Aceptar la invitación a un directorio compartido (opcional)

Si eligió la opción Compartir este directorio con otras Cuentas de AWS (método de protocolo de enlace) en el procedimiento anterior, debería utilizar este procedimiento para finalizar el flujo de trabajo de directorio compartido. Si eligió la opción Compartir este directorio con miembros Cuentas de AWS de su organización, omita este paso y continúe con el paso 4.

Acpetación de la invitación al directorio compartido

1. Inicie sesión AWS Management Console con las credenciales de administrador de la cuenta de consumidor del directorio y abra la AWS Directory Service consola en https://console.aws.amazon.com/directoryservicev2/.
2. En el panel de navegación, elija Directories shared with me (Directorios compartidos conmigo).
3. En la columna Shared directory ID (ID de directorio compartido), elija el ID de directorio que tiene el estado Pending acceptance (Pendiente de aceptación).
4. En la página Shared directory details (Detalles de directorio compartido), elija Review (Revisar).
5. En el cuadro de diálogo Pending shared directory invitation (Invitación a directorio compartido pendiente), revise la nota, detalles de propietario de directorio e información acerca del precio. Si está de acuerdo, seleccione Accept (Aceptar) para empezar a utilizar el directorio.

Paso siguiente

Paso 4: prueba de la unión fluida de una instancia de EC2 para Windows Server a un dominio

Paso 4: prueba de la unión fluida de una instancia de EC2 para Windows Server a un dominio

Puede utilizar uno de los dos métodos siguientes para probar la unión fluida de una instancia de EC2 a un dominio.

Método 1: prueba de la unión del dominio a través de la consola de Amazon EC2

Siga estos pasos en la cuenta del consumidor de directorio.

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, elija el Región de AWS mismo directorio que el existente.
3. En el panel de control de EC2, en la sección Lanzar instancia, elija Lanzar instancia.
4. En la página Lanzar una instancia, en la sección Nombre y etiquetas, ingrese el nombre que desee utilizar para la instancia de EC2 de Windows.
5. (Opcional) Elija Agregar etiquetas adicionales para agregar uno o varios pares clave-valor de etiqueta para organizar o controlar el acceso a esta instancia de EC2 o hacer su seguimiento.
6. En la sección Imagen de aplicación y sistema operativo (Imagen de máquina de Amazon), elija Windows en el panel Inicio rápido. Puede cambiar la imagen de máquina de Amazon (AMI) de Windows desde la lista desplegable Imagen de máquina de Amazon (AMI).
7. En la sección Tipo de instancia, elija el tipo de instancia que desee usar en la lista desplegable Tipo de instancia.
8. En la sección Par de claves (inicio de sesión), puede elegir entre crear un nuevo par de claves o elegir un par de claves existente.

    a. Para crear un nuevo par de claves, elija Crear nuevo par de claves.
    b. Ingrese un nombre para el par de claves y seleccione una opción en Tipo de par de claves y Formato de archivo de clave privada.
    c. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija .pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija .ppk.
    d. Elija Crear par de claves.
    e. Su navegador descargará el archivo de clave privada automáticamente. Guarde el archivo de clave privada en un lugar seguro.

> **Important**
>
> Esta es la única oportunidad para guardar el archivo de clave privada.

9. En la página Lanzar una instancia, en la sección Configuración de red, elija Editar. Elija la VPC en la que se creó el directorio en la lista desplegable VPC: obligatoria.
10. Elija una de las subredes públicas de su VPC en la lista desplegable Subred. La subred que elija debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.

    Para obtener más información sobre cómo conectar una puerta de enlace de Internet, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.
11. En Autoasignar IP pública, elija Habilitar.

    Para obtener más información sobre el direccionamiento IP público y privado, consulte el direccionamiento IP de las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.
12. En la configuración Firewall (grupos de seguridad), puede usar la configuración predeterminada o hacer cambios para adaptarla a sus necesidades.
13. En la configuración Configurar almacenamiento, puede utilizar los ajustes predeterminados o hacer los cambios necesarios para adaptarlos a sus necesidades.
14. Seleccione la sección Detalles avanzados y elija su dominio en la lista desplegable Directorio de unión de dominios.

> **Note**
>
> Tras elegir el directorio de unión de dominios, es posible que vea lo siguiente:
>
> > An error was detected in your existing SSM document. You can delete the existing SSM document here and we'll create a new one with correct properties on instance launch.
>
> Este error se produce si el asistente de lanzamiento de EC2 identifica un documento SSM existente con propiedades inesperadas. Puede elegir una de las opciones siguientes:

- Si ya ha editado el documento SSM y las propiedades son las esperadas, seleccione cerrar y proceda a lanzar la instancia de EC2 sin cambios.
- Seleccione el enlace para eliminar el documento SSM existente aquí para eliminar el documento SSM. Esto permitirá crear un documento SSM con las propiedades correctas. El documento SSM se creará automáticamente al lanzar la instancia EC2.

15. En Perfil de instancia de IAM, puede seleccionar un perfil de instancia de IAM existente o crear uno nuevo. Seleccione un perfil de instancia de IAM que tenga DirectoryServiceAccess adjuntas las políticas AWS administradas AmazonSSM ManagedInstanceCore y AmazonSSM en la lista desplegable de perfiles de instancias de IAM. Para crear uno nuevo, elija el enlace Crear un nuevo perfil de IAM y, a continuación, haga lo siguiente:

    1. Elija Crear rol.
    2. En Seleccionar tipo de entidad de confianza, elija Servicio de AWS .
    3. En Caso de uso, elija EC2.
    4. En Añadir permisos, en la lista de políticas, seleccione las políticas de AmazonSSM ManagedInstanceCore y AmazonSSM. DirectoryServiceAccess Para filtrar la lista, escriba **`SSM`** en el cuadro de búsqueda. Elija Siguiente.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess proporciona los permisos para unir instancias a una instancia gestionada por. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore proporciona los permisos mínimos necesarios para usar el servicio. AWS Systems Manager Para obtener más información sobre la creación de un rol con estos permisos y para obtener información sobre otros permisos y políticas que puede asignar a su rol de IAM, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

    5. En la página Asignar un nombre, revisar, crear, ingrese un Nombre de rol. Necesitará este nombre de rol para asociarlo a la instancia de EC2.
    6. (Opcional) Puede proporcionar una descripción del perfil de instancia de IAM en el campo Descripción.
    7. Elija Crear rol.

8. Vuelva a la página Lanzar una instancia y elija el icono de actualización situado junto al perfil de instancia de IAM. El nuevo perfil de instancia de IAM debería estar visible en la lista desplegable Perfil de instancia de IAM. Elija el nuevo perfil y deje el resto de la configuración con sus valores predeterminados.

16. Seleccione Iniciar instancia.

Método 2: pruebe la unión de dominios mediante AWS Systems Manager

Siga estos pasos en la cuenta del consumidor de directorio. Para completar este procedimiento, necesitará información sobre la cuenta del propietario de directorio, como el ID del directorio, el nombre del directorio y las direcciones IP de DNS.

Requisitos previos

- Configuración AWS Systems Manager.
  - Para obtener más información acerca de Systems Manager, consulte Configuración general de AWS Systems Manager.
- Las instancias a las que desee unirse al dominio AWS administrado de Microsoft Active Directory deben tener una función de IAM asociada que contenga las políticas administradas de AmazonSSM ManagedInstanceCore y DirectoryServiceAccessAmazonSSM.
  - Para obtener más información acerca de estas políticas administradas y otras políticas que puede asociar a un perfil de instancia de IAM de Systems Manager, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager . Para obtener más información sobre las políticas administradas, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Para obtener más información sobre el uso de Systems Manager para unir instancias EC2 a un dominio AWS administrado de Microsoft Active Directory, consulte ¿Cómo se une una instancia EC2 de Windows en ejecución a mi dominio de AWS Directory Service? AWS Systems Manager .

1. Abre la AWS Systems Manager consola enhttps://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, en Administración de nodos, elija Ejecutar comando.
3. Elija Run command (Ejecutar comando).
4. En la página Ejecutar un comando, busque `AWS-JoinDirectoryServiceDomain`. Cuando se muestre en los resultados de búsqueda, seleccione la opción `AWS-JoinDirectoryServiceDomain`.

5. Desplácese hasta la sección Command parameters (Parámetros del comando). Debe proporcionar los siguientes parámetros:

> **Note**
>
> Para localizar el ID del directorio, el nombre del directorio y las direcciones IP del DNS, vuelva a la AWS Directory Service consola, seleccione Directorios compartidos conmigo y seleccione su directorio. Encontrará el ID del directorio en la sección Detalles del directorio compartido. Puede encontrar los valores de Nombre del directorio y Direcciones IP de DNS en la sección de Detalles del directorio propietario.

   - Para el identificador de directorio, introduzca el nombre del Microsoft Active Directory AWS administrado.
   - En Nombre del directorio, escriba el nombre del directorio de AWS Managed Microsoft Active (de la cuenta del propietario de directorio).
   - Para las direcciones IP DNS, introduzca las direcciones IP de los servidores DNS en el Microsoft Active Directory AWS administrado (para la cuenta del propietario del directorio).
6. En Destinos, seleccione Elegir instancias manualmente y, a continuación, seleccione las instancias que quiere que se unan al dominio.
7. Deje el resto del formulario con los valores predeterminados, desplácese hacia abajo en la página y, a continuación, elija Run (Ejecutar).
8. El estado del comando cambiará de Pendiente a Correcto una vez que las instancias se hayan unido correctamente al dominio. Para ver el resultado del comando, seleccione el ID de instancia de la instancia que se unió al dominio y Ver el resultado.

Después de completar cualquiera de estos pasos, debería poder unir la instancia EC2 al dominio. Una vez hecho esto, podrá iniciar sesión en la instancia mediante un cliente de Protocolo de escritorio remoto (RDP) con las credenciales de su cuenta de usuario de Microsoft AD AWS administrada.

Dejar de compartir el directorio

Utilice el siguiente procedimiento para dejar de compartir un directorio de AWS Managed Microsoft AD.

Para dejar de compartir el directorio

1. En el panel de navegación de la consola de AWS Directory Service, en Active Directory, seleccione Directorios.
2. Elija el ID de directorio del directorio de AWS Managed Microsoft AD que desea dejar de compartir.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que quiera dejar de compartir el directorio y, a continuación, seleccione la pestaña Escalar y compartir. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Escalar y compartir.
4. En la sección Shared directories (Directorios compartidos), seleccione el directorio compartido que desea dejar de compartir, elija Actions (Acciones) y, a continuación, elija Unshare (Dejar de compartir).
5. En el cuadro de diálogo Unshare directory (Dejar de compartir directorio), elija Unshare (Dejar de compartir).

Recursos adicionales

- Caso de uso: compartir el directorio para unir de forma sencilla instancias de Amazon EC2 a un dominio a través de cuentas de AWS
- Artículo del blog de seguridad de AWS: How to Join Amazon EC2 Instances From Multiple Accounts and VPCs to a directorio individual de AWS Managed Microsoft AD
- Unión de las instancias de base de datos de Amazon RDS en distintas cuentas a un único dominio compartido

Unir una instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory

Puede unir sin problemas una instancia de Amazon EC2 a su Active Directory dominio cuando se lance la instancia. Para obtener más información, consulte Unir sin problemas una instancia de Amazon EC2 para Windows a su AWS Microsoft AD gestionado Active Directory. También puede

lanzar una instancia EC2 y unirla a un Active Directory dominio directamente desde la AWS Directory Service consola con AWS Systems Manager Automation.

Si necesita unir manualmente una instancia EC2 a su Active Directory dominio, debe lanzar la instancia en la región y el grupo de seguridad o la subred adecuados y, a continuación, unir la instancia al dominio.

Para poder conectarse de forma remota a estas instancias, debe disponer de conectividad IP a las instancias desde la red en la que se está conectando. En la mayoría de los casos, esto requiere conectar una puerta de enlace de Internet a su VPC y que la instancia tenga una dirección IP pública.

Temas

Inicie una instancia de administración de directorios en su Microsoft AD AWS administrado Active Directory

Este procedimiento lanza una Windows instancia de administración de directorios de Amazon EC2 en el AWS Management Console uso de AWS Systems Manager Automation para administrar sus directorios. También puede lograrlo ejecutando directamente el comando automation AWS-CreateDS ManagementInstance en la AWS Systems Manager consola de automatización.

Requisitos previos

Para lanzar una instancia de EC2 de administración de directorios desde la consola, debe tener los siguientes permisos habilitados en la cuenta.

- `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 lanzar una instancia EC2 de administración de directorios en AWS Management Console

1. Inicie sesión en la consola de AWS Directory Service.
2. En Active Directory, elija Directorios.
3. Elija el ID de directorio del directorio en el que desee lanzar una instancia EC2 de administración de directorios.
4. En la página del directorio, en la esquina superior derecha, elija Acciones.
5. En la lista desplegable Acciones, seleccione Iniciar la instancia EC2 de administración de directorios.
6. En la página Iniciar la instancia de EC2 de administración de directorios, en Parámetros de entrada, complete los campos.

   a. (Opcional) Puedes proporcionar un key pair para la instancia. En la lista desplegable Nombre del par de claves: opcional, seleccione un par de claves.

   b. (Opcional) Seleccione AWS CLI el comando Ver para ver un ejemplo que utilice AWS CLI para ejecutar esta automatización.
7. Seleccione Submit (Enviar).

8. Volverá a la página del directorio. Aparece una barra flash verde en la parte superior de la pantalla para indicar que el lanzamiento se inició correctamente.

Para ver la instancia EC2 de administración de directorios

Si no ha lanzado ninguna instancia de EC2 para un directorio, aparece un guion (-) en Instancia de EC2 de administración de directorios.

1. En Active Directory, elija Directorios y seleccione el directorio que quiera ver.
2. En Detalles del directorio, en Instancia de EC2 de administración de directorios, elija una o todas las instancias que quiera ver.
3. Al elegir una instancia, se le redirige a la página Conectarse a la instancia de EC2 para conectar un escritorio remoto a la instancia.

Unir sin problemas una instancia de Amazon EC2 para Windows a su AWS Microsoft AD gestionado Active Directory

Este procedimiento une sin problemas una Windows instancia de Amazon EC2 a su AWS Microsoft AD administrado. Si necesita realizar una unión de dominios entre varios dominios sin problemas Cuentas de AWS, consulteTutorial: Cómo compartir su directorio AWS gestionado de Microsoft AD para unirse a dominios EC2 sin problemas. Para obtener información completa sobre Amazon EC2, consulte ¿Qué es Amazon EC2?.

Para unirse sin problemas a una instancia de Amazon EC2 Windows

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, elija el Región de AWS mismo directorio que el existente.
3. En el panel de control de EC2, en la sección Lanzar instancia, elija Lanzar instancia.
4. En la página Lanzar una instancia, en la sección Nombre y etiquetas, ingrese el nombre que desee utilizar para la instancia de EC2 de Windows.
5. (Opcional) Elija Agregar etiquetas adicionales para agregar uno o varios pares clave-valor de etiqueta para organizar o controlar el acceso a esta instancia de EC2 o hacer su seguimiento.
6. En la sección Imagen de aplicación y sistema operativo (Imagen de máquina de Amazon), elija Windows en el panel Inicio rápido. Puede cambiar la imagen de máquina de Amazon (AMI) de Windows desde la lista desplegable Imagen de máquina de Amazon (AMI).

7. En la sección Tipo de instancia, elija el tipo de instancia que desee usar en la lista desplegable Tipo de instancia.
8. En la sección Par de claves (inicio de sesión), puede elegir entre crear un nuevo par de claves o elegir un par de claves existente.
   a. Para crear un nuevo par de claves, elija Crear nuevo par de claves.
   b. Ingrese un nombre para el par de claves y seleccione una opción en Tipo de par de claves y Formato de archivo de clave privada.
   c. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija .pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija .ppk.
   d. Elija Crear par de claves.
   e. Su navegador descargará el archivo de clave privada automáticamente. Guarde el archivo de clave privada en un lugar seguro.

   > **Important**
   >
   > Esta es la única oportunidad para guardar el archivo de clave privada.

9. En la página Lanzar una instancia, en la sección Configuración de red, elija Editar. Elija la VPC en la que se creó el directorio en la lista desplegable VPC: obligatoria.
10. Elija una de las subredes públicas de su VPC en la lista desplegable Subred. La subred que elija debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.

    Para obtener más información sobre cómo conectar una puerta de enlace de Internet, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.
11. En Autoasignar IP pública, elija Habilitar.

    Para obtener más información sobre el direccionamiento IP público y privado, consulte el direccionamiento IP de las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.
12. En la configuración Firewall (grupos de seguridad), puede usar la configuración predeterminada o hacer cambios para adaptarla a sus necesidades.
13. En la configuración Configurar almacenamiento, puede utilizar los ajustes predeterminados o hacer los cambios necesarios para adaptarlos a sus necesidades.

14. Seleccione la sección Detalles avanzados y elija su dominio en la lista desplegable Directorio de unión de dominios.

> **Note**
>
> Tras elegir el directorio de unión de dominios, es posible que vea lo siguiente:
>
> > An error was detected in your existing SSM document. You can delete the existing SSM document here and we'll create a new one with correct properties on instance launch.
>
> Este error se produce si el asistente de lanzamiento de EC2 identifica un documento SSM existente con propiedades inesperadas. Puede elegir una de las opciones siguientes:
>
> - Si ya ha editado el documento SSM y las propiedades son las esperadas, seleccione cerrar y proceda a lanzar la instancia de EC2 sin cambios.
> - Seleccione el enlace para eliminar el documento SSM existente aquí para eliminar el documento SSM. Esto permitirá crear un documento SSM con las propiedades correctas. El documento SSM se creará automáticamente al lanzar la instancia EC2.

15. En Perfil de instancia de IAM, puede seleccionar un perfil de instancia de IAM existente o crear uno nuevo. Seleccione un perfil de instancia de IAM que tenga DirectoryServiceAccess adjuntas las políticas AWS administradas AmazonSSM ManagedInstanceCore y AmazonSSM en la lista desplegable de perfiles de instancias de IAM. Para crear uno nuevo, elija el enlace Crear un nuevo perfil de IAM y, a continuación, haga lo siguiente:

    1. Elija Crear rol.
    2. En Seleccionar tipo de entidad de confianza, elija Servicio de AWS .
    3. En Caso de uso, elija EC2.
    4. En Añadir permisos, en la lista de políticas, seleccione las políticas de AmazonSSM ManagedInstanceCore y AmazonSSM. DirectoryServiceAccess Para filtrar la lista, escriba **`SSM`** en el cuadro de búsqueda. Elija Siguiente.

> **Note**
>
> AmazonSSM DirectoryServiceAccess proporciona los permisos para unir instancias a una instancia gestionada por. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore proporciona los permisos mínimos necesarios para usar el servicio. AWS Systems Manager Para obtener más información sobre la creación de un rol con estos permisos y para obtener información sobre otros permisos y políticas que puede asignar a su rol de IAM, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

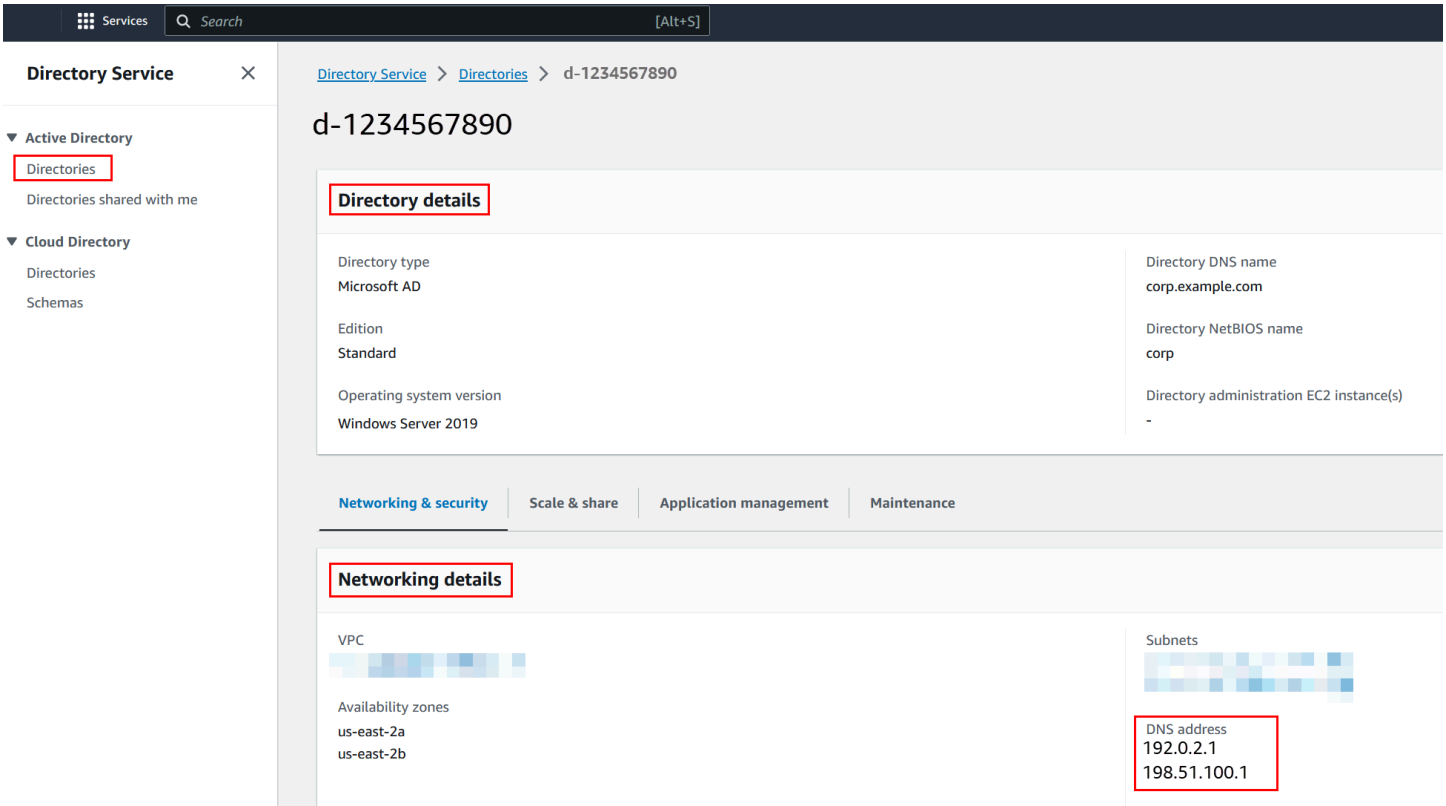
5. En la página Asignar un nombre, revisar, crear, ingrese un Nombre de rol. Necesitará este nombre de rol para asociarlo a la instancia de EC2.
6. (Opcional) Puede proporcionar una descripción del perfil de instancia de IAM en el campo Descripción.
7. Elija Crear rol.
8. Vuelva a la página Lanzar una instancia y elija el icono de actualización situado junto al perfil de instancia de IAM. El nuevo perfil de instancia de IAM debería estar visible en la lista desplegable Perfil de instancia de IAM. Elija el nuevo perfil y deje el resto de la configuración con sus valores predeterminados.

16. Seleccione Iniciar instancia.

Unir manualmente una Windows instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory

Para unir manualmente una Windows instancia Amazon EC2 existente a un AWS Microsoft AD gestionadoActive Directory, la instancia debe lanzarse con los parámetros que se especifican en. Unir sin problemas una instancia de Amazon EC2 para Windows a su AWS Microsoft AD gestionado Active Directory

Necesitará las direcciones IP de los servidores DNS AWS administrados de Microsoft AD. Puede encontrar esta información en las secciones Servicios de directorio > Directorios > el enlace del ID de directorio de su directorio > Detalles del directorio y Redes y seguridad.



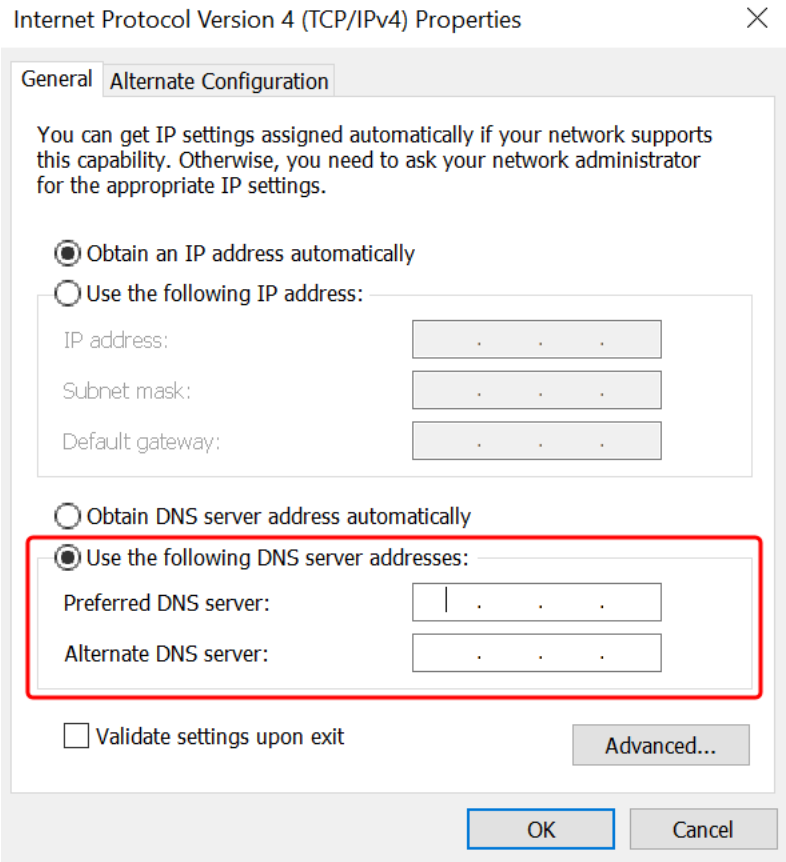
Para unir una instancia de Windows a un Microsoft AD AWS administrado Active Directory

1. Conéctese a la instancia mediante un cliente de Protocolo de escritorio remoto.
2. Abra el cuadro de diálogo de propiedades TCP/IPv4 en la instancia.
   a. Abra Conexiones de red.

      > **Tip**
      >
      > Puede abrir Conexiones de red directamente ejecutando lo siguiente en un símbolo del sistema en la instancia.
      >
      > ```
      > %SystemRoot%\system32\control.exe ncpa.cpl
      > ```

   b. Abra el menú contextual (haga clic con el botón) de cualquier conexión de red habilitada y elija Propiedades.
   c. En el cuadro de diálogo de propiedades de conexión, abra (doble clic) Protocolo de Internet versión 4.

3. Seleccione Usar las siguientes direcciones de servidor DNS, cambie las direcciones del servidor DNS preferido y del servidor DNS alternativo por las direcciones IP de los servidores DNS AWS gestionados proporcionados por Microsoft AD y pulse Aceptar.



4. Abra el cuadro de diálogo Propiedades del sistema de la instancia, seleccione la pestaña Nombre de equipo y elija Cambiar.

> **Tip**
>
> Puede abrir el cuadro de diálogo Propiedades del sistema directamente en un símbolo del sistema en la instancia.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. En el campo Miembro de, seleccione Dominio, introduzca el nombre completo de su Active Directory AWS administrado de Microsoft AD y pulse Aceptar.
6. Cuando se le pida el nombre y la contraseña del administrador del dominio, introduzca el nombre de usuario y la contraseña de una cuenta que tenga privilegios de unión a un dominio.

Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

> **Note**
>
> Puede introducir el nombre completo del dominio o el nombre de NetBIOS, seguido de una barra invertida (\) y, a continuación, el nombre de usuario. El nombre de usuario sería Admin. Por ejemplo, **`corp.example.com\admin`** o **`corp\admin`**.

7. Cuando reciba el mensaje de bienvenida al dominio, reinicie la instancia para que se apliquen los cambios.

Ahora que la instancia se ha unido al dominio de Active Directory AWS administrado de Microsoft AD, puede iniciar sesión en esa instancia de forma remota e instalar utilidades para administrar el directorio, como agregar usuarios y grupos. Las herramientas de administración de Active Directory se pueden utilizar para crear usuarios y grupos. Para obtener más información, consulte Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado.

> **Note**
>
> También puede usar Amazon Route 53 para procesar consultas de DNS en lugar de cambiar manualmente las direcciones DNS de las instancias de Amazon EC2. Para obtener más información, consulte Integrar la resolución de DNS del servicio de directorio Amazon Route 53 Resolver y reenviar las consultas DNS salientes a la red.

Unir sin problemas una instancia de Amazon EC2 Linux a su Active Directory AWS gestionado de Microsoft AD

Este procedimiento une sin problemas una instancia Linux de Amazon EC2 a su Active Directory administrado de AWS Microsoft AD. Si necesita realizar una unión de dominios sin problemas en varias AWS cuentas, puede optar por habilitar el uso compartido de directorios.

Son compatibles las siguientes distribuciones y versiones de instancias de Linux:

- 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 y Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Las distribuciones anteriores a Ubuntu 14 y Red Hat Enterprise Linux 7 no admiten la característica de unión fluida de dominios.

Para ver una demostración del proceso de unir sin problemas una instancia de Linux a su Active Directory AWS administrado de Microsoft AD, consulte el siguiente YouTube vídeo.

Demostración de la unión a la dominio AD de Amazon EC2 para Linux

Requisitos previos

Para poder configurar una unión de dominio perfecta a una instancia de Linux, debes completar los procedimientos de esta sección.

Selección de la cuenta de servicio de unión de dominios fluida

Puede unir sin problemas ordenadores Linux a su dominio de Active Directory AWS administrado de Microsoft AD. Para ello, debe usar una cuenta de usuario con permisos de creación de cuentas de equipos para unir las máquinas al dominio. Si bien es posible que los miembros de los administradores delegados de AWS u otros grupos tengan privilegios suficientes para unir los equipos al dominio, no lo recomendamos. Como práctica recomendada, le recomendamos que utilice una cuenta de servicio que tenga los privilegios mínimos necesarios para unir los equipos al dominio.

Para delegar una cuenta con los privilegios mínimos necesarios para unir los equipos al dominio, puede ejecutar los siguientes PowerShell comandos. Debe ejecutar estos comandos desde un equipo Windows unido a un dominio con Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado instalado. Además, debe utilizar una cuenta que tenga permiso para modificar los permisos de la unidad organizativa o el contenedor del equipo. El PowerShell comando establece los permisos que permiten a la cuenta de servicio crear objetos de ordenador en el contenedor de ordenadores predeterminado del dominio.

```
$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"
```

Si prefiere utilizar una interfaz de usuario gráfica (GUI), puede utilizar el proceso manual que se describe en Privilegios delegados a su cuenta de servicio.

Creación de secretos para almacenar la cuenta de servicio de dominio

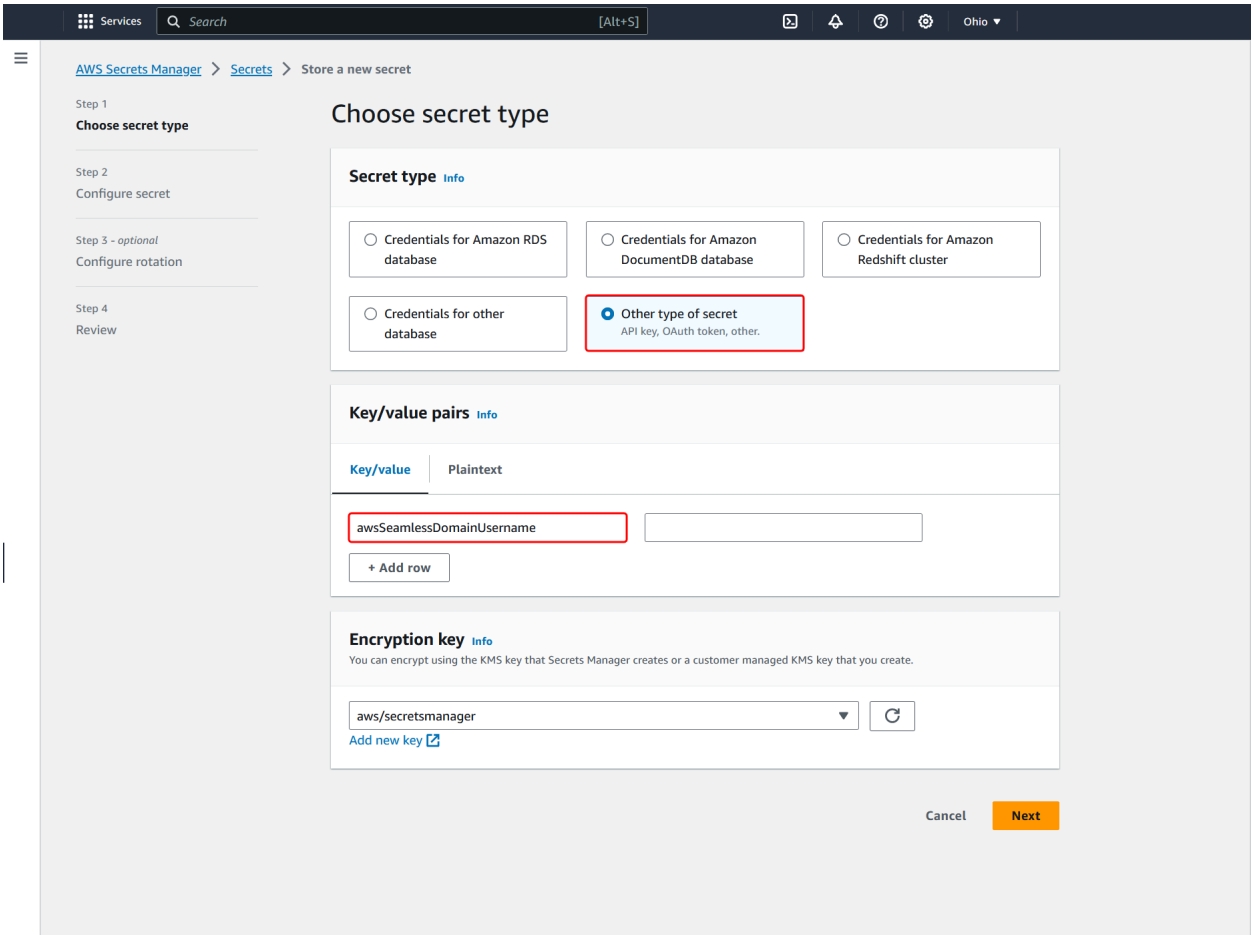
Puede utilizarlos AWS Secrets Manager para almacenar la cuenta de servicio del dominio.

Creación de secretos y almacenamiento de la información de la cuenta de servicio de dominio

1. Inicie sesión en la AWS Secrets Manager consola AWS Management Console y ábrala en https://console.aws.amazon.com/secretsmanager/.
2. Elija Almacenar un secreto nuevo.
3. En la página Store a new secret (Almacenar un nuevo secreto), haga lo siguiente:
   a. En Tipo de secreto, seleccione Otro tipo de secretos.
   b. En Pares clave/valor, haga lo siguiente:
      i. En el cuadro de filtro, escriba **`awsSeamlessDomainUsername`**. En la misma fila, en el cuadro siguiente, introduce el nombre de usuario de tu cuenta de servicio. Por ejemplo,

si utilizó el PowerShell comando anteriormente, el nombre de la cuenta de servicio sería**`awsSeamlessDomain`**.

> **Note**
>
> Debe ingresar **`awsSeamlessDomainUsername`** exactamente como está. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.



ii. Seleccione Agregar regla.

iii. En la nueva fila, en el primer cuadro, ingrese **`awsSeamlessDomainPassword`**. En la misma fila, en el cuadro siguiente, ingrese la contraseña de su cuenta de servicio.

> **Note**
>
> Debe ingresar **`awsSeamlessDomainPassword`** exactamente como está. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.

iv. En Clave de cifrado, deje el valor predeterminado`aws/secretsmanager`. AWS Secrets Manager siempre cifra el secreto al elegir esta opción. También puede elegir una clave que haya creado.

> **Note**
>
> Hay tarifas asociadas AWS Secrets Manager, según el secreto que utilices. Para obtener la lista de precios completa, consulte Precios de AWS Secrets Manager.
> Puedes usar la clave AWS gestionada `aws/secretsmanager` que crea Secrets Manager para cifrar tus secretos de forma gratuita. Si crea sus propias claves de KMS para cifrar sus secretos, se le AWS cobrará la tarifa actual AWS KMS . Para obtener más información, consulte AWS Key Management Service Precios.

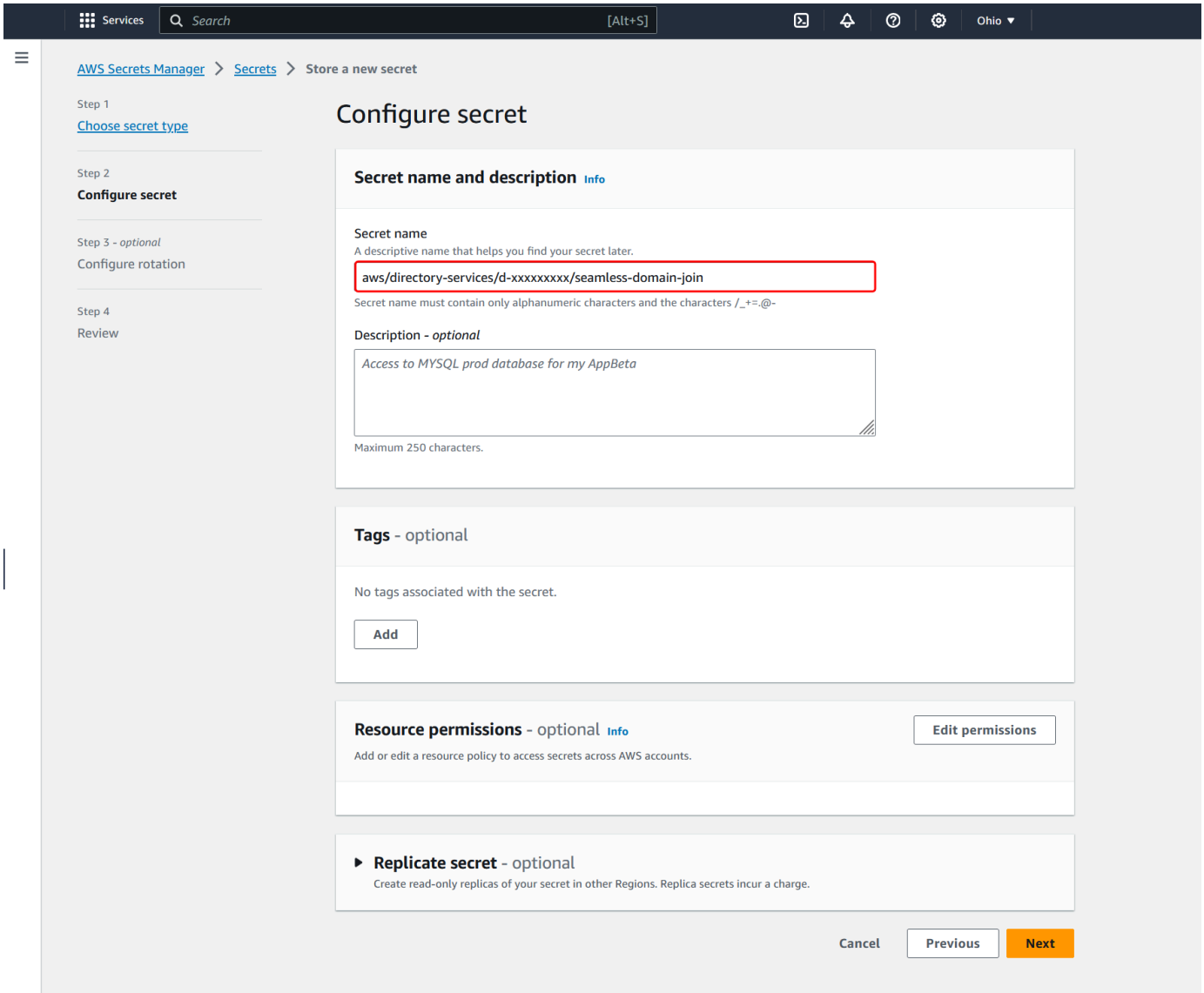
v. Elija Siguiente.

4. En Nombre secreto, introduzca un nombre secreto que incluya su ID de directorio con el siguiente formato y sustituya *`d-xxxxxxxxx`* por su ID de directorio:

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

Se usará para recuperar los secretos de la aplicación.

> **Note**
>
> Debe escribir **`aws/directory-services/`*`d-xxxxxxxxx`*`/seamless-domain-join`** exactamente como está, pero sustituya *`d-xxxxxxxxxx`* por su ID de directorio. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.



5. Deje todo lo demás con los valores predeterminados y, a continuación, elija Siguiente.
6. En Configurar rotación automática, elija Deshabilitar rotación automática y, a continuación, Siguiente.

   Puedes activar la rotación de este secreto después de guardarlo.
7. Revise la configuración y, a continuación, elija Almacenar para guardar los cambios. La consola de Secrets Manager vuelve a la lista de secretos de su cuenta con el nuevo secreto ahora incluido en la lista.
8. Elija el nombre del secreto recién creado de la lista y tome nota del valor del ARN del secreto. Lo necesitará en la sección siguiente.

Activa la rotación del secreto de la cuenta del servicio de dominio

Te recomendamos que cambies los secretos con regularidad para mejorar tu postura de seguridad.

Para activar la rotación del secreto de la cuenta del servicio de dominio

- Sigue las instrucciones de la Guía del AWS Secrets Manager usuario sobre cómo configurar la rotación automática de datos AWS Secrets Manager secretos.

  Para el paso 5, utilice la plantilla de rotación de credenciales de Microsoft Active Directory en la Guía del AWS Secrets Manager usuario.

  Para obtener ayuda, consulte Solucionar problemas de AWS Secrets Manager rotación en la Guía del AWS Secrets Manager usuario.

Creación del rol y la política de IAM obligatorios

Siga los siguientes pasos previos para crear una política personalizada que permita el acceso de solo lectura a su secreto de unión a dominios integrada de Secrets Manager (que creó anteriormente) y para crear un nuevo rol de IAM de DomainJoin LinuxEC2.

Creación de la política de lectura de IAM de Secrets Manager

Utilizará la consola de IAM para crear una política que concede acceso de solo lectura a su secreto de Secrets Manager.

Creación de la política de lectura de IAM de Secrets Manager

1. Inicie sesión AWS Management Console como usuario con permiso para crear políticas de IAM. A continuación, abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, Administración de acceso, selecciona Políticas.
3. Elija Crear política.
4. Seleccione la pestaña JSON y copie el texto del siguiente documento de política JSON. A continuación, péguelo en el cuadro de texto JSON.

> **Note**
>
> Asegúrate de reemplazar el ARN de región y recurso por el ARN y la región reales del secreto que creaste 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. Cuando haya terminado, elija Next. El validador de políticas notifica los errores de sintaxis. Para obtener más información, consulte Validación de políticas de IAM.
6. En la página Revisar política, ingrese un nombre para la política, como **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Revise el Resumen de la política para ver los permisos concedidos por su política. Seleccione Crear política para guardar los cambios. La nueva política aparece en la lista de las políticas administradas y está lista para asociar a una identidad.

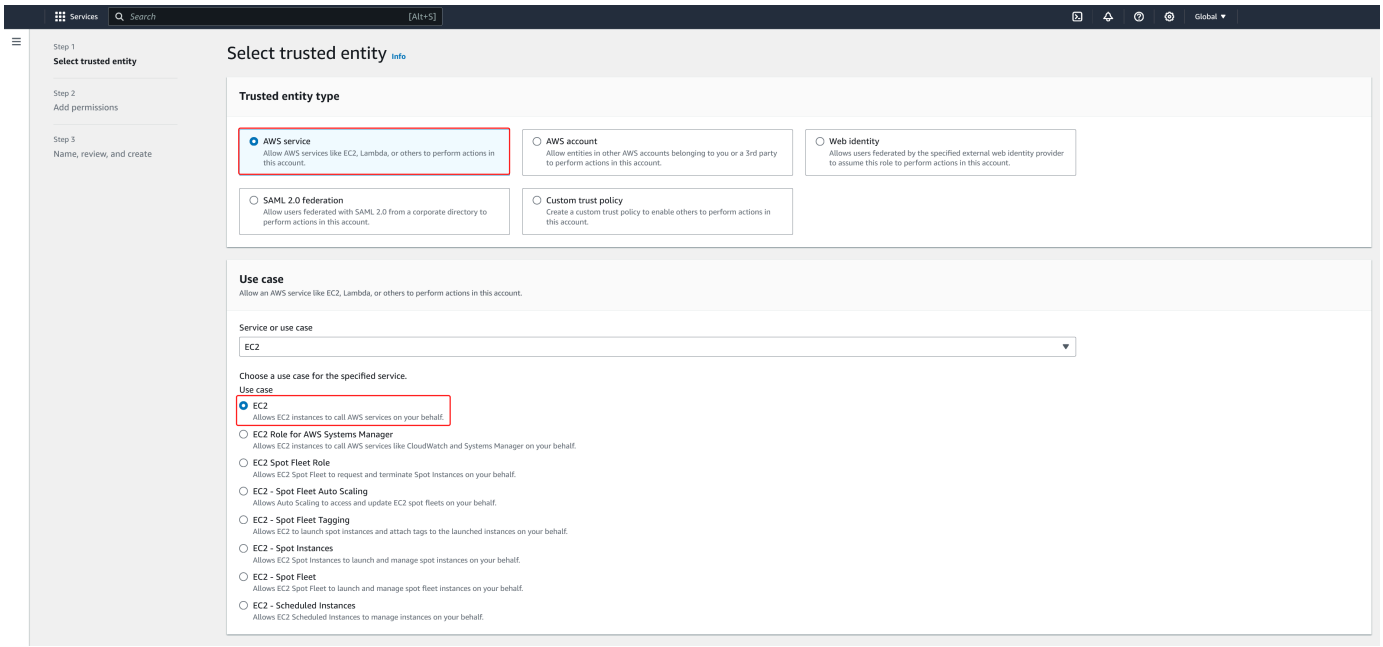
> **Note**
>
> Le recomendamos que cree una política por secreto. De este modo, se garantiza que las instancias solo tengan acceso al secreto adecuado y se minimiza el impacto en caso de que una instancia se vea comprometida.

Cree el rol LinuxEC2 DomainJoin

Utilice la consola de IAM para crear el rol que utilizará para unirse al dominio de su instancia de EC2 de Linux.

Para crear el rol LinuxEC2 DomainJoin

1. Inicie sesión AWS Management Console como usuario con permiso para crear políticas de IAM. A continuación, abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, en Administración del acceso, elija Roles.
3. En el panel de contenido, elija Crear rol.
4. En Seleccionar tipo de entidad de confianza, seleccione Servicio de AWS .
5. En Caso de uso, elija EC2 y, a continuación, elija Siguiente.



6. En Políticas de filtro, haga lo siguiente:
   a. Escriba **`AmazonSSMManagedInstanceCore`**. A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   b. Escriba **`AmazonSSMDirectoryServiceAccess`**. A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   c. Ingrese **`SM-Secret-Linux-DJ-`***`d-xxxxxxxxxx`***`-Read`** (o el nombre de la política creada en el procedimiento anterior). A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   d. Tras añadir las tres políticas enumeradas anteriormente, seleccione Crear función.

> **Note**
>
> AmazonSSM DirectoryServiceAccess proporciona los permisos para unir instancias a una instancia Active Directory gestionada por. AWS Directory Service AmazonSSM ManagedInstanceCore proporciona los permisos mínimos necesarios para usar el servicio. AWS Systems Manager Para obtener más información sobre la creación de un rol con estos permisos y para obtener información sobre otros permisos y políticas que puede asignar a su rol de IAM, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

7. Introduzca un nombre para su nueva función, por ejemplo, **`LinuxEC2DomainJoin`** u otro nombre que prefiera en el campo Nombre de la función.
8. (Opcional) En Role description (Descripción del rol), escriba una descripción.
9. (Opcional) Selecciona Añadir nueva etiqueta en el paso 3: Añadir etiquetas para añadir etiquetas. Los pares clave-valor de etiquetas se utilizan para organizar, rastrear o controlar el acceso de este rol.
10. Elija Crear rol.

Únase a su instancia de Linux sin problemas

Ahora que ha configurado todas las tareas previas, puede utilizar el siguiente procedimiento para unirse sin problemas a su instancia EC2 de Linux.

Para unirse sin problemas a su instancia de Linux

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En el selector de regiones de la barra de navegación, elija el Región de AWS mismo directorio que el existente.
3. En el panel de control de EC2, en la sección Lanzar instancia, elija Lanzar instancia.
4. En la página Lanzar una instancia, en la sección Nombre y etiquetas, introduce el nombre que te gustaría usar para tu instancia EC2 de Linux.
5. (Opcional) Elija Agregar etiquetas adicionales para agregar uno o varios pares clave-valor de etiqueta para organizar o controlar el acceso a esta instancia de EC2 o hacer su seguimiento.

6. En la sección Imagen de aplicación e sistema operativo (Amazon Machine Image), elija la AMI de Linux que desee lanzar.

> **Note**
>
> La AMI utilizada debe tener AWS Systems Manager (SSM Agent) la versión 2.3.1644.0 o superior. Para comprobar la versión de SSM Agent instalada en la AMI mediante el lanzamiento de una instancia desde esa AMI, consulte Obtener la versión de SSM Agent instalada actualmente. Si necesita actualizar SSM Agent, consulte Instalación y configuración de SSM Agent en instancias de EC2 para Linux.
> SSM usa el `aws:domainJoin` complemento al unir una instancia de Linux a un dominio. Active Directory *El complemento cambia el nombre de host de las instancias de Linux al formato EC2AMAZ-XXXXXXX.* Para obtener más información al respecto*`aws:domainJoin`*, consulte la referencia del complemento del documento de AWS Systems Manager comandos en la Guía del usuario.AWS Systems Manager

7. En la sección Tipo de instancia, elija el tipo de instancia que desee usar en la lista desplegable Tipo de instancia.
8. En la sección Par de claves (inicio de sesión), puede elegir entre crear un nuevo par de claves o elegir un par de claves existente. Para crear un nuevo par de claves, elija Crear nuevo par de claves. Ingrese un nombre para el par de claves y seleccione una opción en Tipo de par de claves y Formato de archivo de clave privada. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija .pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija .ppk. Elija Crear par de claves. Su navegador descargará el archivo de clave privada automáticamente. Guarde el archivo de clave privada en un lugar seguro.

> **Important**
>
> Esta es la única oportunidad para guardar el archivo de clave privada.

9. En la página Lanzar una instancia, en la sección Configuración de red, elija Editar. Elija la VPC en la que se creó el directorio en la lista desplegable VPC: obligatoria.
10. Elija una de las subredes públicas de su VPC en la lista desplegable Subred. La subred que elija debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.

Para obtener más información sobre cómo conectar una puerta de enlace de Internet, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.

11. En Autoasignar IP pública, elija Habilitar.

    Para obtener más información sobre el direccionamiento IP público y privado, consulte el direccionamiento IP de las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

12. En la configuración Firewall (grupos de seguridad), puede usar la configuración predeterminada o hacer cambios para adaptarla a sus necesidades.
13. En la configuración Configurar almacenamiento, puede utilizar los ajustes predeterminados o hacer los cambios necesarios para adaptarlos a sus necesidades.
14. Seleccione la sección Detalles avanzados y elija su dominio en la lista desplegable Directorio de unión de dominios.

> **Note**
>
> Tras elegir el directorio de unión de dominios, es posible que vea lo siguiente:
>
> ⚠ An error was detected in your existing SSM document. You can delete the existing SSM document here and we'll create a new one with correct properties on instance launch. ✕
>
> Este error se produce si el asistente de lanzamiento de EC2 identifica un documento SSM existente con propiedades inesperadas. Puede elegir una de las opciones siguientes:
>
> - Si ya ha editado el documento SSM y las propiedades son las esperadas, seleccione cerrar y proceda a lanzar la instancia de EC2 sin cambios.
> - Seleccione el enlace para eliminar el documento SSM existente aquí para eliminar el documento SSM. Esto permitirá crear un documento SSM con las propiedades correctas. El documento SSM se creará automáticamente al lanzar la instancia EC2.

15. Para el perfil de instancia de IAM, elija el rol de IAM que creó anteriormente en la sección de requisitos previos. Paso 2: Crear el rol LinuxEC2. DomainJoin
16. Seleccione Iniciar instancia.

> **Note**
>
> Si va a llevar a cabo una unión de dominio fluida con SUSE Linux, es necesario reiniciarla para que las autenticaciones funcionen. Para reiniciar SUSE desde el terminal Linux, escriba sudo reboot.

Unir manualmente una instancia de Amazon EC2 Linux a su Active Directory AWS administrado de Microsoft AD

Además de las instancias Windows de Amazon EC2, también puede unir determinadas instancias de Amazon EC2 Linux a su Active Directory AWS administrado de Microsoft AD. Son compatibles las siguientes distribuciones y versiones de instancias de Linux:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI de Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS y Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Puede que funcionen otras versiones y distribuciones de Linux, pero no se han probado.

Unir una instancia de Linux a su Microsoft AD AWS administrado

Antes de poder unir una instancia de Amazon Linux, CentOS, Red Hat o Ubuntu a su directorio, la instancia debe lanzarse primero como se especifica en Únase a su instancia de Linux sin problemas.

> **Important**
>
> Algunos de los siguientes procedimientos, si no se siguen correctamente, pueden hacer que la instancia resulte inaccesible o inservible. Por lo tanto, recomendamos encarecidamente

que realice una copia de seguridad o una instantánea de la instancia antes de realizar estos procedimientos.

Para unir una instancia de Linux al directorio

Siga los pasos para su instancia de Linux específica mediante una de las siguientes pestañas:

Amazon Linux

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para que utilice las direcciones IP del servidor DNS AWS Directory Service de los servidores DNS proporcionados. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de 64 bits de Amazon Linux esté actualizada.

   ```
   sudo yum -y update
   ```

4. Instale los paquetes necesarios de Amazon Linux en la instancia de Linux.

   > **Note**
   > Algunos de estos paquetes pueden estar ya instalados.
   > Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

   Amazon Linux

   ```
   sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
    krb5-workstation
   ```

> **Note**
>
> Si necesita ayuda para determinar la versión de Amazon Linux que está utilizando, consulte Identificación de imágenes de Amazon Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.

5. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Una cuenta en el dominio *example.com* con privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

6. Configure el servicio SSH para permitir autenticación de contraseñas.

   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Establezca la opción `PasswordAuthentication` en `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Reinicie el servicio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Otra opción:

```
sudo service sshd restart
```

7. Una vez reiniciada la instancia, conéctate a ella con cualquier cliente SSH y añade el grupo de administradores AWS delegados a la lista de sudoers siguiendo estos pasos:

   a. Abra el archivo `sudoers` con el siguiente comando:

   ```
   sudo visudo
   ```

   b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

CentOS

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configura la instancia de Linux para que utilice las direcciones IP del servidor DNS de los servidores DNS proporcionados. AWS Directory Service Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de CentOS 7 esté actualizada.

   ```
   sudo yum -y update
   ```

4. Instale los paquetes necesarios de CentOS 7 en la instancia de Linux.

   > **Note**
   >
   > Algunos de estos paquetes pueden estar ya instalados.

Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Una cuenta en el dominio *example.com* con privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

6. Configure el servicio SSH para permitir autenticación de contraseñas.
   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Establezca la opción `PasswordAuthentication` en `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Reinicie el servicio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Otra opción:

```
sudo service sshd restart
```

7. Una vez reiniciada la instancia, conéctate a ella con cualquier cliente SSH y añade el grupo de administradores AWS delegados a la lista de sudoers siguiendo estos pasos:

   a. Abra el archivo `sudoers` con el siguiente comando:

   ```
   sudo visudo
   ```

   b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

Red Hat

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configura la instancia de Linux para que utilice las direcciones IP del servidor DNS de los servidores DNS proporcionados. AWS Directory Service Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de 64 bits de Red Hat esté actualizada.

   ```
   sudo yum -y update
   ```

4. Instale los paquetes necesarios de Red Hat en la instancia de Linux.

   > **Note**
   >
   > Algunos de estos paquetes pueden estar ya instalados.

Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

El SaM AccountName de una cuenta del dominio *example.com* que tiene privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

6. Configure el servicio SSH para permitir autenticación de contraseñas.
   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Establezca la opción `PasswordAuthentication` en `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Reinicie el servicio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Otra opción:

```
sudo service sshd restart
```

7. Una vez reiniciada la instancia, conéctate a ella con cualquier cliente SSH y añade el grupo de administradores AWS delegados a la lista de sudoers siguiendo estos pasos:

   a. Abra el archivo `sudoers` con el siguiente comando:

   ```
   sudo visudo
   ```

   b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

SUSE

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para utilizar las direcciones IP de los servidores DNS proporcionados por AWS Directory Service. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que su instancia de SUSE Linux 15 esté actualizada.

   a. Conecte el repositorio de paquetes.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Actualice SUSE.

   ```
   sudo zypper update -y
   ```

4. Instale los paquetes SUSE Linux 15 necesarios en su instancia de Linux.

> **Note**
>
> Algunos de estos paquetes pueden estar ya instalados.
> Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-
client
```

5. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -U join_account example.com --verbose
```

join_account

El SaM del dominio AccountName *example.com* que tiene privilegios de unión a un dominio. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Tenga en cuenta que se esperan las dos devoluciones siguientes.

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Habilite manualmente SSSD en PAM.

```
sudo pam-config --add --sss
```

7. Edite nsswitch.conf para habilitar SSSD en nsswitch.conf

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. Agregue la siguiente línea a /etc/pam.d/common-session para crear automáticamente un directorio de inicio en el inicio de sesión inicial

```
sudo vi /etc/pam.d/common-session
```

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Reinicie la instancia para completar el proceso unido al dominio.

```
sudo reboot
```

10. Vuelva a conectarse a la instancia mediante cualquier cliente SSH para verificar que la unión al dominio se ha completado correctamente y finalice los pasos adicionales.

    a. Para confirmar que la instancia se ha inscrito en el dominio

    ```
    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. Visualización del estado del daemon de 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. Para permitir el acceso de un usuario a través de SSH y la consola

```
sudo realm permit join_account@example.com
```

Para permitir el acceso de un grupo de dominio a través de SSH y la consola

```
sudo realm permit -g 'AWS Delegated Administrators'
```

O para permitir el acceso de todos los usuarios

```
sudo realm permit --all
```

12. Configure el servicio SSH para permitir autenticación de contraseñas.
    a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Establezca la opción `PasswordAuthentication` en `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Reinicie el servicio SSH.

    ```
    sudo systemctl restart sshd.service
    ```

Otra opción:

```
sudo service sshd restart
```

13.13. Una vez reiniciada la instancia, conéctate a ella con cualquier cliente SSH y añade el grupo de administradores AWS delegados a la lista de sudoers siguiendo estos pasos:

a. Abra el archivo sudoers con el siguiente comando:

```
sudo visudo
```

b. Agregue lo siguiente a la parte inferior del archivo sudoers y guárdelo.

```
## Add the "Domain Admins" group from the awsad.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configura la instancia de Linux para que utilice las direcciones IP del servidor DNS de los servidores DNS proporcionados. AWS Directory Service Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de 64 bits de Ubuntu esté actualizada.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Instale los paquetes necesarios de Ubuntu en la instancia de Linux.

> **Note**
>
> Algunos de estos paquetes pueden estar ya instalados.

Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Deshabilite la resolución inversa de DNS y establezca el dominio predeterminado en el FQDN de su dominio. Las instancias de Ubuntu deben poder resolverse de forma inversa en el DNS para que el dominio funcione. De lo contrario, tiene que deshabilitar el DNS inverso en /etc/krb5.conf de la manera siguiente:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

El SaM AccountName de una cuenta del dominio *example.com* que tiene privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

7. Configure el servicio SSH para permitir autenticación de contraseñas.

   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

```
sudo vi /etc/ssh/sshd_config
```

b. Establezca la opción `PasswordAuthentication` en `yes`.

```
PasswordAuthentication yes
```

c. Reinicie el servicio SSH.

```
sudo systemctl restart sshd.service
```

Otra opción:

```
sudo service sshd restart
```

8. Una vez reiniciada la instancia, conéctate a ella con cualquier cliente SSH y añade el grupo de administradores AWS delegados a la lista de sudoers siguiendo estos pasos:

a. Abra el archivo `sudoers` con el siguiente comando:

```
sudo visudo
```

b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

Restricción de acceso de inicio de sesión de cuenta

Como todas las cuentas están definidas en Active Directory, todos los usuarios del directorio pueden iniciar sesión en la instancia de forma predeterminada. Puede permitir que solo unos usuarios específicos inicien sesión en la instancia con ad_access_filter en sssd.conf. Por ejemplo:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

`memberOf`

Indica que solo debe permitirse el acceso a la instancia a los usuarios si son miembros de un grupo específico.

cn

El nombre común del grupo que debería tener acceso. En este ejemplo, el nombre del grupo es *admins*.

ou

Esta es la unidad organizativa en la que se encuentra el grupo anterior. En este ejemplo, el valor de OU es *Testou*.

dc

Este es el componente de dominio de su dominio. En este ejemplo, *example*.

dc

Este es un componente de dominio adicional. En este ejemplo, *com*.

Debe agregar manualmente ad_access_filter a su /etc/sssd/sssd.conf.

Abra el archivo /etc/sssd/sssd.conf en un editor de texto.

```
sudo vi /etc/sssd/sssd.conf
```

Después de hacerlo, su sssd.conf podrá tener este aspecto:

```
[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 se aplique la configuración, debe reiniciar el servicio sssd:

```
sudo systemctl restart sssd.service
```

También puede usar:

```
sudo service sssd restart
```

Como todas las cuentas están definidas en Active Directory, todos los usuarios del directorio pueden iniciar sesión en la instancia de forma predeterminada. Puede permitir que solo unos usuarios específicos inicien sesión en la instancia con ad_access_filter en sssd.conf.

Por ejemplo:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica que solo debe permitirse el acceso a la instancia a los usuarios si son miembros de un grupo específico.

cn

El nombre común del grupo que debería tener acceso. En este ejemplo, el nombre del grupo es *admins*.

ou

Esta es la unidad organizativa en la que se encuentra el grupo anterior. En este ejemplo, el valor de OU es *Testou*.

dc

Este es el componente de dominio de su dominio. En este ejemplo, *example*.

dc

Este es un componente de dominio adicional. En este ejemplo, *com*.

Debe agregar manualmente ad_access_filter a su /etc/sssd/sssd.conf.

1. Abra el archivo /etc/sssd/sssd.conf en un editor de texto.

```
sudo vi /etc/sssd/sssd.conf
```

2. Después de hacerlo, su sssd.conf podrá tener este aspecto:

```
[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 se aplique la configuración, debe reiniciar el servicio sssd:

```
sudo systemctl restart sssd.service
```

También puede usar:

```
sudo service sssd restart
```

Mapeo de ID

El mapeo de ID se puede realizar mediante dos métodos para mantener una experiencia unificada entre las identidades del identificador de usuario (UID) y el identificador de grupo (GID) de UNIX/Linux y las identidades del identificador de Active Directory seguridad (SID).

1. Centralizado
2. Distribuido

> **Note**
>
> El mapeo centralizado de la identidad de los usuarios Active Directory requiere una interfaz de sistema operativo portátil o POSIX.

Mapeo centralizado de identidades de usuarios

Active Directoryu otro servicio de Protocolo ligero de acceso a directorios (LDAP) proporciona UID y GID a los usuarios de Linux. EnActive Directory, estos identificadores se almacenan en los atributos de los usuarios:

- UID: el nombre de usuario de Linux (cadena)
- Número de UID: el número de ID de usuario de Linux (entero)
- Número GID: el número de ID del grupo de Linux (entero)

Para configurar una instancia de Linux para usar el UID y el GID de origenActive Directory, configúrelo `ldap_id_mapping = False` en el archivo sssd.conf. Antes de establecer este valor, compruebe que ha agregado un UID, un número UID y un número GID a los usuarios y grupos que contiene. Active Directory

Mapeo distribuido de identidades de usuarios

Si Active Directory no tiene la extensión POSIX o si decide no gestionar de forma centralizada el mapeo de identidades, Linux puede calcular los valores de UID y GID. Linux utiliza el identificador de seguridad (SID) único del usuario para mantener la coherencia.

Para configurar el mapeo de ID de usuario distribuido, configúrelo `ldap_id_mapping = True` en el archivo sssd.conf.

Conéctese a la instancia de Linux

Cuando un usuario se conecta a la instancia mediante un cliente SSH, se le solicita que indique su nombre de usuario. El usuario puede introducir el nombre de usuario en formato `username@example.com` o `EXAMPLE\username`. La respuesta tendrá un aspecto similar al siguiente, en función de la distribución de Linux que utilice:

Amazon Linux, Red Hat Enterprise Linux y 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%
```

Unir manualmente una instancia de Amazon EC2 Linux a su Active Directory administrado de AWS Microsoft AD mediante Winbind

Puede usar el servicio Winbind para unir manualmente sus instancias Linux de Amazon EC2 a un dominio AWS administrado de Microsoft AD Active Directory. Esto permite a los usuarios de Active Directory locales actuales utilizar sus credenciales de Active Directory al acceder a las instancias

de Linux unidas a su Active Directory AWS administrado de Microsoft AD. Son compatibles las siguientes distribuciones y versiones de instancias de Linux:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI de Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS y Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
> Puede que funcionen otras versiones y distribuciones de Linux, pero no se han probado.

Unir una instancia de Linux a su Active Directory AWS administrado de Microsoft AD

> **Important**
> Algunos de los siguientes procedimientos, si no se siguen correctamente, pueden hacer que la instancia resulte inaccesible o inservible. Por lo tanto, recomendamos encarecidamente que realice una copia de seguridad o una instantánea de la instancia antes de realizar estos procedimientos.

Para unir una instancia de Linux al directorio

Siga los pasos para su instancia de Linux específica mediante una de las siguientes pestañas:

Amazon Linux/CENTOS/REDHAT

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para utilizar las direcciones IP de los servidores DNS proporcionados por AWS Directory Service. Puede hacerlo configurándolo en el conjunto de

opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.

3. Asegúrese de que su instancia de Linux esté actualizada.

```
sudo yum -y update
```

4. Instale los paquetes necesarios de Samba o Winbind en la instancia de Linux.

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-
clients
```

5. Haga una copia de seguridad del archivo `smb.conf` principal para poder volver a él en caso de que se produzca un error:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Abra el archivo de configuración original [`/etc/samba/smb.conf`] en un editor de texto.

```
sudo vim /etc/samba/smb.conf
```

Complete la información del entorno de dominio de Active Directory como se muestra en el siguiente ejemplo:

```
[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 el archivo de host [`/etc/hosts`] en un editor de texto.

```
sudo vim /etc/hosts
```

Agregue la dirección IP privada de su instancia de Linux de la siguiente manera:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Si no especificó la dirección IP en el archivo `/etc/hosts`, es posible que reciba el siguiente error de DNS al unir la instancia al dominio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Este error significa que la unión se hizo correctamente, pero el comando [net ads] no pudo registrar el registro DNS en DNS.

8. Una la instancia de Linux a Active Directory mediante la utilidad net.

```
sudo net ads join -U join_account@example.com
```

`join_account@example.com`

Una cuenta en el dominio *`example.com`* con privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

`example.com`

El nombre de DNS completo del directorio.

```
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 el archivo de configuración PAM. Utilice el siguiente comando para agregar las entradas necesarias para la autenticación de winbind:

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10. Configure el servicio SSH para permitir autenticación de contraseñas al editar el archivo `/etc/ssh/sshd_config`.
    a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Establezca la opción `PasswordAuthentication` en `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Reinicie el servicio SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    Otra opción:

    ```
    sudo service sshd restart
    ```

11. Una vez que la instancia se haya reiniciado, siga estos pasos para conectarse a ella con cualquier cliente SSH y agregue privilegios raíz para el grupo o usuario del dominio a la lista de sudoers:
    a. Abra el archivo `sudoers` con el siguiente comando:

    ```
    sudo visudo
    ```

    b. Agregue los grupos o usuarios necesarios de su dominio de confianza de la siguiente manera y, a continuación, guárdelos.

    ```
    ## 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
    ```

    (En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

SUSE

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para utilizar las direcciones IP de los servidores DNS proporcionados por AWS Directory Service. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que su instancia de SUSE Linux 15 esté actualizada.
   a. Conecte el repositorio de paquetes.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Actualice SUSE.

   ```
   sudo zypper update -y
   ```

4. Instale los paquetes necesarios de Samba o Winbind en la instancia de Linux.

   ```
   sudo zypper in -y samba samba-winbind
   ```

5. Haga una copia de seguridad del archivo `smb.conf` principal para poder volver a él en caso de que se produzca un error:

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. Abra el archivo de configuración original [`/etc/samba/smb.conf`] en un editor de texto.

   ```
   sudo vim /etc/samba/smb.conf
   ```

   Complete la información del entorno de dominio de Active Directory como se muestra en el siguiente ejemplo:

   ```
   [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 el archivo de host [`/etc/hosts`] en un editor de texto.

```
sudo vim /etc/hosts
```

Agregue la dirección IP privada de su instancia de Linux de la siguiente manera:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Si no especificó la dirección IP en el archivo `/etc/hosts`, es posible que reciba el siguiente error de DNS al unir la instancia al dominio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Este error significa que la unión se hizo correctamente, pero el comando [net ads] no pudo registrar el registro DNS en DNS.

8. Una la instancia de Linux al directorio con el siguiente comando.

```
sudo net ads join -U join_account@example.com
```

`join_account`

El SaM AccountName del dominio *`example.com`* que tiene privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

`example.com`

El nombre de DNS completo del directorio.

```
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 el archivo de configuración PAM. Utilice el siguiente comando para agregar las entradas necesarias para la autenticación de Winbind:

```
sudo pam-config --add --winbind --mkhomedir
```

10. Abra el archivo de configuración de Name Service Switch [`/etc/nsswitch.conf`] en un editor de texto.

```
vim /etc/nsswitch.conf
```

Agregue la directiva de Winbind como se muestra a continuación.

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11. Configure el servicio SSH para permitir autenticación de contraseñas al editar el archivo `/etc/ssh/sshd_config`.

a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

```
sudo vim /etc/ssh/sshd_config
```

b. Establezca la opción `PasswordAuthentication` en `yes`.

```
PasswordAuthentication yes
```

c. Reinicie el servicio SSH.

```
sudo systemctl restart sshd.service
```

Otra opción:

```
sudo service sshd restart
```

12. Una vez que la instancia se haya reiniciado, siga estos pasos para conectarse a ella con cualquier cliente SSH y agregue privilegios raíz para el grupo o usuario del dominio a la lista de sudoers:

a. Abra el archivo `sudoers` con el siguiente comando:

```
sudo visudo
```

b. Agregue los grupos o usuarios necesarios de su dominio de confianza de la siguiente manera y, a continuación, guárdelos.

```
## 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
```

(En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

Ubuntu

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para utilizar las direcciones IP de los servidores DNS proporcionados por AWS Directory Service. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea configurarlo manualmente, consulte Cómo asignar un servidor DNS estático a una instancia privada de Amazon EC2 en el AWS Knowledge Center para obtener orientación sobre cómo configurar el servidor DNS persistente para su distribución y versión de Linux en particular.
3. Asegúrese de que su instancia de Linux esté actualizada.

```
sudo yum -y update
```

```
sudo apt-get -y upgrade
```

4. Instale los paquetes necesarios de Samba o Winbind en la instancia de Linux.

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. Haga una copia de seguridad del archivo `smb.conf` principal para poder volver a él en caso de que se produzca un error.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Abra el archivo de configuración original [`/etc/samba/smb.conf`] en un editor de texto.

```
sudo vim /etc/samba/smb.conf
```

Complete la información del entorno de dominio de Active Directory como se muestra en el siguiente ejemplo:

```
[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 el archivo de host [`/etc/hosts`] en un editor de texto.

```
sudo vim /etc/hosts
```

Agregue la dirección IP privada de su instancia de Linux de la siguiente manera:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Si no especificó la dirección IP en el archivo `/etc/hosts`, es posible que reciba el siguiente error de DNS al unir la instancia al dominio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Este error significa que la unión se hizo correctamente, pero el comando [net ads] no pudo registrar el registro DNS en DNS.

8. Una la instancia de Linux a Active Directory mediante la utilidad net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Una cuenta en el dominio *example.com* con privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
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 el archivo de configuración PAM. Utilice el siguiente comando para agregar las entradas necesarias para la autenticación de Winbind:

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Abra el archivo de configuración de Name Service Switch [`/etc/nsswitch.conf`] en un editor de texto.

```
vim /etc/nsswitch.conf
```

Agregue la directiva de Winbind como se muestra a continuación.

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. Configure el servicio SSH para permitir autenticación de contraseñas al editar el archivo `/etc/ssh/sshd_config`.

a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

```
sudo vim /etc/ssh/sshd_config
```

b. Establezca la opción `PasswordAuthentication` en `yes`.

```
PasswordAuthentication yes
```

c. Reinicie el servicio SSH.

```
sudo systemctl restart sshd.service
```

Otra opción:

```
sudo service sshd restart
```

12. Una vez que la instancia se haya reiniciado, siga estos pasos para conectarse a ella con cualquier cliente SSH y agregue privilegios raíz para el grupo o usuario del dominio a la lista de sudoers:

a. Abra el archivo `sudoers` con el siguiente comando:

```
sudo visudo
```

b. Agregue los grupos o usuarios necesarios de su dominio de confianza de la siguiente manera y, a continuación, guárdelos.

```
## 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
```

(En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

Conéctese a la instancia de Linux

Cuando un usuario se conecta a la instancia mediante un cliente SSH, se le solicita que indique su nombre de usuario. El usuario puede introducir el nombre de usuario en formato `username@example.com` o `EXAMPLE\username`. La respuesta tendrá un aspecto similar al siguiente, en función de la distribución de Linux que utilice:

Amazon Linux, Red Hat Enterprise Linux y 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%
```

Unir manualmente una instancia Mac de Amazon EC2 a su Active Directory AWS administrado de Microsoft AD

Este procedimiento une manualmente una instancia Mac de Amazon EC2 a su Active Directory administrado de AWS Microsoft AD.

Requisitos previos

- Las instancias Mac de Amazon EC2 requieren hosts dedicados de Amazon EC2. Debe asignar un host dedicado y lanzar una instancia en el host. Para obtener más información, consulte Lanzar una instancia de Mac en la Guía del usuario de Amazon EC2.
- Se recomienda crear un conjunto de opciones de DHCP para su Active Directory AWS administrado de Microsoft AD. Esto permitirá que cualquier instancia de tu Amazon VPC apunte al dominio y a los servidores DNS especificados para resolver sus nombres de dominio. Para obtener más información, consulte Crear o cambiar un conjunto de opciones de DHCP.

> **Note**
>
> El precio del alojamiento dedicado varía según la opción de pago que selecciones. Para obtener más información, consulte la Guía del usuario sobre precios y facturación en Amazon EC2.

Para unirse manualmente a una instancia de Mac

1. Usa el siguiente comando SSH para conectarte a tu instancia de Mac. Para obtener más información sobre la conexión a la instancia de Mac, consulta Conectarse a la instancia de Mac.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
   ```

2. Tras conectarte a la instancia de Mac, crea una contraseña para la cuenta *ec2-user* mediante el siguiente comando:

   ```
   sudo passwd ec2-user
   ```

3. Cuando se te pida en la línea de comandos, introduce una contraseña para la cuenta *ec2-user*. Puede actualizar el sistema operativo y el software siguiendo el procedimiento de la Guía del usuario de Amazon EC2 para actualizar el sistema operativo y el software.
4. Usa el siguiente comando *dsconfigad* para unir tu instancia de Mac al dominio administrado de AWS Microsoft AD Active Directory. Asegúrese de reemplazar el nombre de dominio, el nombre del equipo y la unidad organizativa por la información de dominio de Active Directory AWS administrado de Microsoft AD. Para obtener más información, consulta el sitio web de Apple sobre cómo configurar el acceso al dominio en la Utilidad de Directorios en Mac.

> **Warning**
>
> El nombre del equipo no debe contener un guión. Los guiones pueden impedir el enlace al Active Directory administrado de AWS Microsoft AD.

```
sudo dsconfigad -add domainName -computer computerName -username Username -
ou "Your-AWS-Delegated-Organizational-Unit"
```

En el siguiente ejemplo, se muestra el aspecto que debe tener el comando al unirse a un usuario administrativo en una instancia de Mac con el nombre **`myec2mac01`** del **`example.com`** dominio:

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. Usa el siguiente comando para añadir los administradores AWS delegados al usuario administrativo de tu instancia de Mac:

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators
```

6. Utilice el siguiente comando para confirmar que la unión al dominio AWS administrado de Microsoft AD Active Directory se ha realizado correctamente:

```
dsconfigad -show
```

Ha unido correctamente su instancia de Mac a su Active Directory AWS administrado de Microsoft AD. Ahora puedes iniciar sesión en tu instancia de Mac con tus credenciales de Active Directory AWS administrado de Microsoft AD.

La primera vez que inicies sesión en tu instancia de Mac, tendrás la opción de iniciar sesión como el «Otro» usuario. En este punto, puedes usar tus credenciales de dominio de Active Directory para iniciar sesión en la instancia de Mac. Si no aparece la palabra «Otros» en la pantalla de inicio de sesión después de completar estos pasos, inicie sesión como ec2-user y, a continuación, cierre la sesión.

Para iniciar sesión mediante la interfaz gráfica de usuario con un usuario de dominio, siga los pasos de la Guía del usuario de Amazon EC2 para Conectarse a la interfaz gráfica de usuario (GUI) de la instancia.

Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD

Para unir un equipo al directorio, necesita una cuenta con privilegios para unir equipos al directorio.

Con AWS Directory Service para Microsoft Active Directory, los miembros de los grupos Admins y AWS Delegated Server Administrators tienen estos privilegios.

No obstante, la práctica recomendada es que use una cuenta que tenga solo los privilegios mínimos necesarios. En el procedimiento siguiente se explica cómo crear un nuevo grupo denominado `Joiners` y cómo delegar en este grupo los privilegios necesarios para unir equipos al directorio.

Debe llevar a cabo este procedimiento en un equipo que esté unido al directorio y que tenga instalado el complemento de MMC Usuarios y equipos de Active Directory. Además, es necesario la sesión se inicie como administrador del dominio.

Para delegar los privilegios de unión a AWS Managed Microsoft AD

1. Abra Usuarios y equipos de Active Directory y seleccione la unidad organizativa (OU) que tiene su nombre de NetBIOS en el árbol de navegación; a continuación, seleccione la unidad organizativa Usuarios.

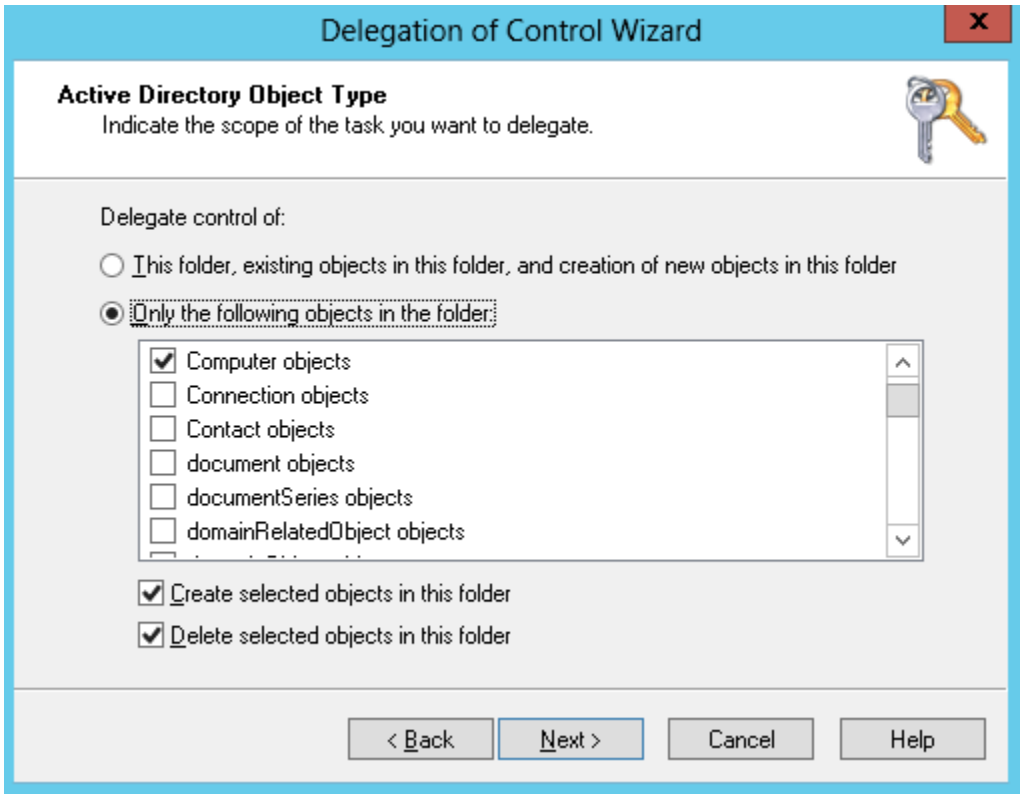
   > **Important**
   >
   > Al iniciar un AWS Directory Service para Microsoft Active Directory, AWS crea una unidad organizativa (OU) que contiene todos los objetos del directorio. Esta unidad organizativa, que tiene el nombre de NetBIOS que escribió al crear el directorio, se encuentra en la raíz del dominio. La raíz del dominio es propiedad de y está administrada por AWS. No puede realizar cambios en el dominio raíz en sí, por lo que deberá crear el grupo **`Joiners`** dentro de la unidad organizativa de su nombre de NetBIOS.

2. Abra el menú contextual (clic con el botón derecho) para Usuarios, seleccione Nuevo y después seleccione Grupo.
3. En el cuadro Nuevo objeto - Grupo, escriba lo siguiente y haga clic en Aceptar.

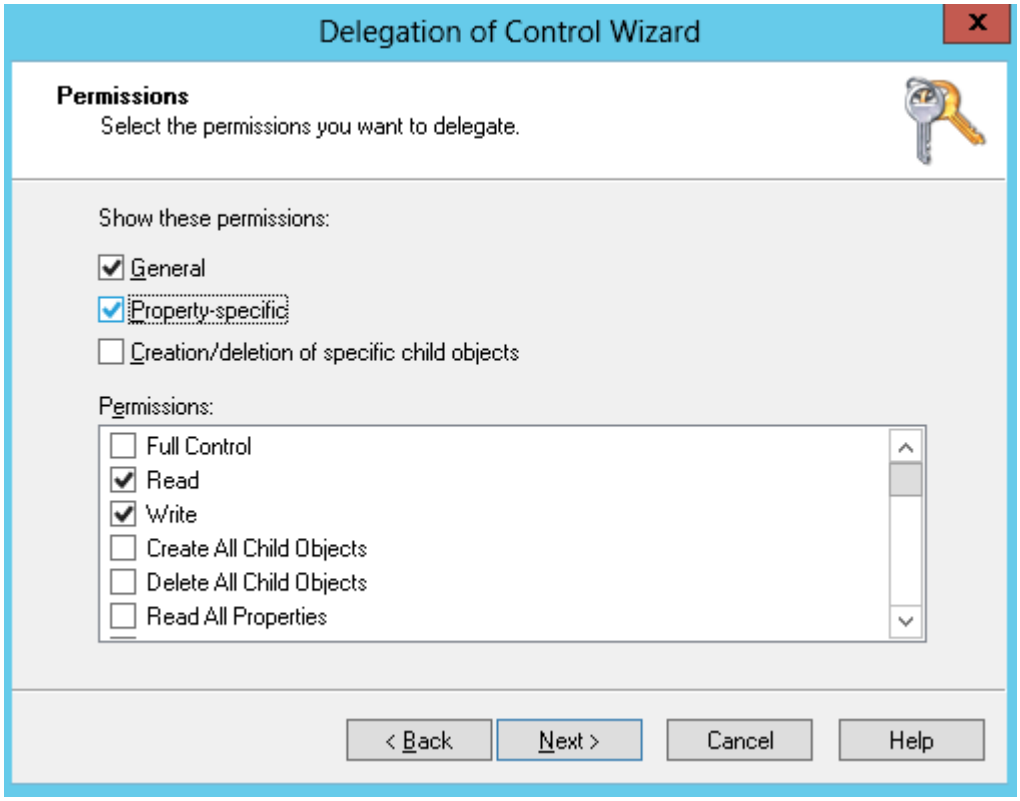
   - En Group Name (Nombre de grupo), escriba **`Joiners`**.

- En Ámbito de grupo, escriba Global.
- En Tipo de grupo, seleccione Seguridad.

4. En el árbol de navegación, seleccione el contenedor Equipos bajo su nombre de NetBIOS. En el menú Acción, elija Delegar control.
5. En la página Asistente para delegación de control, elija Siguiente y después seleccione Agregar.
6. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, escriba `Joiners` y haga clic en Aceptar. Si se encuentran varios objetos, seleccione el grupo `Joiners` que creó anteriormente. Elija Siguiente.
7. En la página Tareas que se delegarán, seleccione Crear una tarea personalizada para delegar y luego elija Siguiente.
8. Seleccione Sólo los siguientes objetos en la carpeta y, a continuación, seleccione Objetos de equipo.
9. Seleccione Crear los objetos seleccionados en esta carpeta y Eliminar los objetos seleccionados en esta carpeta. A continuación, elija Next.



10. Seleccione Lectura y Escritura y luego elija Siguiente.



11. Compruebe la información en la página Finalización del Asistente para delegación de control y seleccione Finalizar.
12. Cree un usuario con una contraseña segura y añádalo al grupo `Joiners`. Este usuario debe estar en el contenedor Usuarios que bajo su nombre de NetBIOS. El usuario tendrá entonces privilegios suficientes para conectar instancias al directorio.

Crear o cambiar un conjunto de opciones de DHCP

AWS recomienda crear un conjunto de opciones de DHCP para el AWS Directory Service directorio y asignar el conjunto de opciones de DHCP a la VPC en la que se encuentra el directorio. De este modo, las instancias de la VPC apuntarán al dominio y a los servidores DNS especificados para resolver los nombres de dominio.

Para obtener más información sobre los conjuntos de opciones de DHCP, consulte Conjuntos de opciones de DHCP en la Guía del usuario de Amazon VPC.

Creación de un conjunto de opciones de DHCP para un directorio

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, elija DHCP Options Sets y, a continuación, elija Create DHCP options set.
3. En la página Crear conjunto de opciones de DHCP, facilite los siguientes valores para el directorio:

   Nombre

   Etiqueta opcional para el conjunto de opciones.

   Nombre del dominio

   El nombre completo del directorio, por ejemplo `corp.example.com`.

   Domain name servers

   Las direcciones IP de los servidores DNS del directorio AWS proporcionado por el usuario.

   > **Note**
   > Para encontrarlas, en el panel de navegación de la consola de AWS Directory Service seleccione Directorios y elija el identificador de directorio correspondiente.

   NTP servers

   Deje este campo en blanco.

   NetBIOS name servers

   Deje este campo en blanco.

   NetBIOS node type

   Deje este campo en blanco.
4. Luego, Create DHCP options set (Crear conjunto de opciones de DHCP). El nuevo conjunto de opciones de DHCP aparecerá en la lista de opciones de DHCP.
5. Anote el ID del nuevo conjunto de opciones de DHCP (dopt-*xxxxxxxx*). Lo necesitará para asociar dicho conjunto a su VPC.

Para cambiar el conjunto de opciones de DHCP asociado a una VPC

Los conjuntos de opciones de DHCP no se pueden modificar una vez creados. Si quiere que su VPC utilice un conjunto de opciones de DHCP distinto, tendrá que crear uno nuevo y asociarlo a la VPC. También puede configurar la VPC para que no utilice opciones de DHCP.

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione la VPC y, a continuación, elija Acciones, Editar la configuración de la VPC.
4. En Conjunto de opciones de DHCP, seleccione un conjunto de opciones o elija Sin conjunto de opciones de DHCP y, a continuación, elija Guardar.

Para cambiar el conjunto de opciones de DHCP asociado a una VPC mediante la línea de comandos, consulte lo siguiente:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Administración de usuarios y grupos en AWS Managed Microsoft AD

Los usuarios representan a las personas físicas o entidades que tienen acceso al directorio. Los grupos resultan muy útiles para conceder o denegar privilegios a un conjunto de usuarios en lugar de asignar esos privilegios a cada usuario por separado. Si un usuario se va a otra organización, basta con cambiarlo a un grupo diferente y automáticamente recibirá los privilegios necesarios para la nueva organización.

Para crear usuarios y grupos en un directorio de AWS Directory Service, debe usar cualquier instancia (ya sea en las instalaciones o EC2) que se haya unido a su directorio de AWS Directory Service y haber iniciado sesión como usuario con privilegios para crear usuarios y grupos. También es necesario instalar las herramientas de Active Directory en su instancia de EC2 para que pueda agregar sus usuarios y grupos con el complemento Usuarios y equipo de Active Directory.

Puede implementar una instancia de EC2 preconfigurada con las herramientas administrativas de Active Directory preinstaladas desde la consola de administración de AWS Directory Service. Para obtener más información, consulte Inicie una instancia de administración de directorios en su Microsoft AD AWS administrado Active Directory.

Si necesita implementar una instancia de EC2 autoadministrada con herramientas administrativas e instalar las herramientas necesarias, consulte Paso 3: Implemente una instancia de Amazon EC2 para gestionar su Active Directory gestionado de AWS Microsoft AD.

> **Note**
>
> Las cuentas de usuario deben tener habilitada la autenticación previa de Kerberos. Es la configuración predeterminada para cuentas de usuario nuevas y no debe modificarse. Para obtener más información acerca de esta configuración, vaya a Preauthentication en Microsoft TechNet.

En los temas siguientes se incluyen instrucciones sobre cómo crear y administrar usuarios y grupos.

Temas

Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado

Para gestionarla Active Directory desde una instancia de Windows Server de Amazon EC2, debe instalarla Active Directory Domain Services and Active Directory Lightweight Directory Services Tools en la instancia. Utilice el siguiente procedimiento para instalar estas herramientas en una instancia EC2 de Windows Server.

Requisitos previos

Antes de comenzar este procedimiento, complete lo siguiente:

1. Cree un Microsoft AD AWS administradoActive Directory. Para obtener más información, consulte Cree su Microsoft AD AWS administrado.

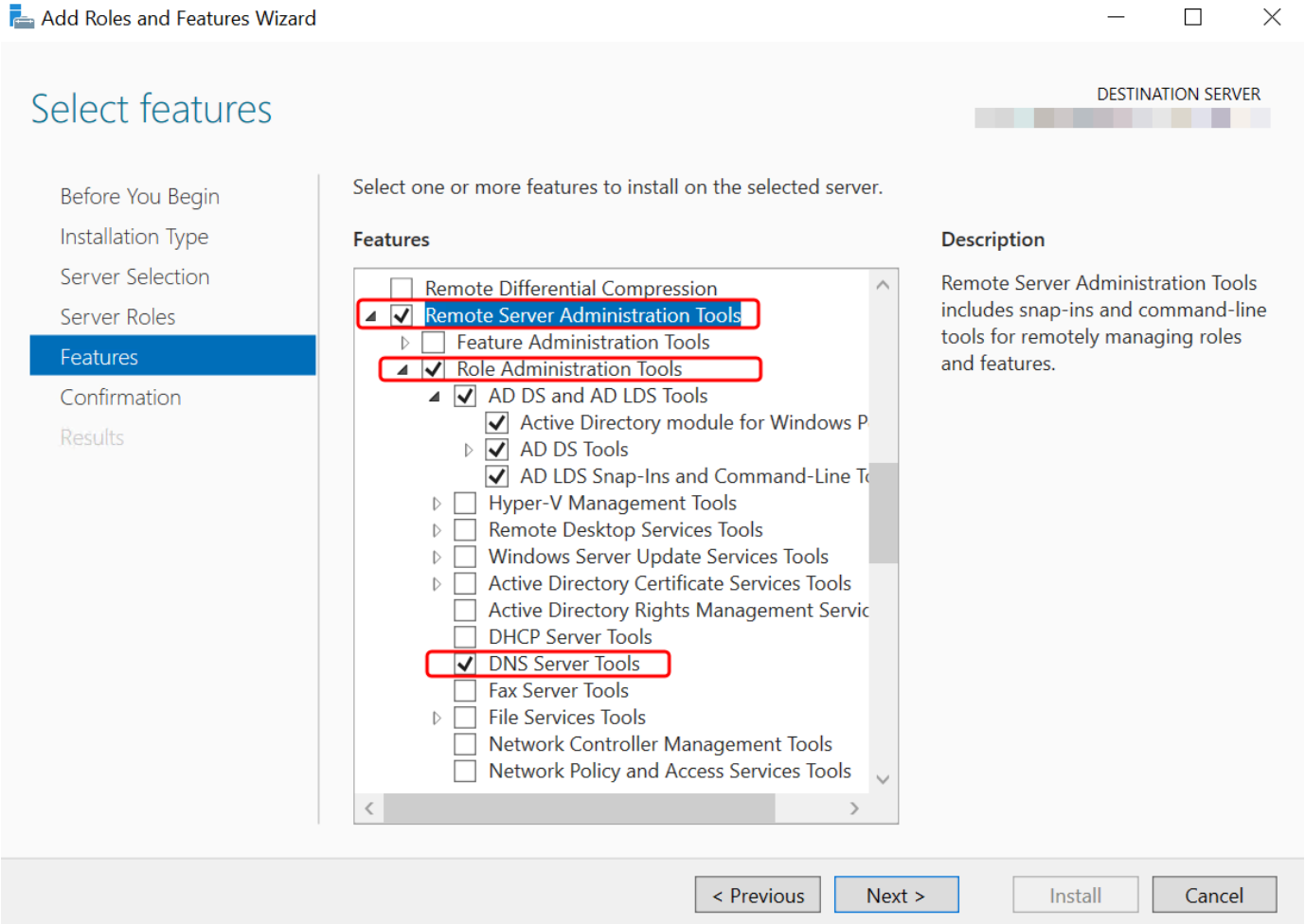
2. Inicie y únase a una instancia EC2 de Windows Server a su Active Directory AWS administrado de Microsoft AD. La instancia EC2 necesita las siguientes políticas para crear usuarios y grupos: **`AWSSSMManagedInstanceCore`** y. **`AmazonSSMDirectoryServiceAccess`** Para obtener más información, consulte Inicie una instancia de administración de directorios en su Microsoft AD AWS administrado Active Directory y Unir sin problemas una instancia de Amazon EC2 para Windows a su AWS Microsoft AD gestionado Active Directory.
3. Necesitará las credenciales del administrador de su Active Directory dominio. Estas credenciales se crearon cuando se creó el Microsoft AD AWS administrado. Si ha seguido el procedimiento indicado enCree su Microsoft AD AWS administrado, su nombre de usuario de administrador incluye su nombre de NetBIOS,. **`corp\admin`**

Instale las herramientas de administración de Active Directory en la instancia EC2 de Windows Server

Para instalar las herramientas de administración de Active Directory en la instancia EC2 de Windows Server

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la consola de Amazon EC2, elija Instancias, seleccione la instancia de Windows Server y, a continuación, elija Conectarse.
3. En la página Conectarse a la instancia, elija Cliente RDP.
4. En la pestaña Cliente RDP, elija Descargar archivo de Escritorio remoto y, a continuación, seleccione Obtener contraseña para recuperar la contraseña.
5. En la sección Obtener contraseña de Windows, seleccione Cargar archivo de clave privada. Elija el archivo de clave privada .pem asociado a la instancia de Windows Server. Tras cargar el archivo de clave privada, seleccione Descifrar contraseña.
6. En el cuadro de diálogo de seguridad de Windows, copie las credenciales de administrador local del equipo Windows Server para iniciar sesión. El nombre de usuario puede tener los siguientes formatos: ***`NetBIOS-Name`***`\admin` o***`DNS-Name`***`\admin`. Por ejemplo, **`corp\admin`** sería el nombre de usuario si hubiera seguido el procedimiento indicado enCree su Microsoft AD AWS administrado.
7. Una vez que haya iniciado sesión en la instancia de Windows Server, abra el Administrador del servidor desde el menú Inicio seleccionando el Administrador del servidor.
8. En el panel de Server Manager, elija Agregar roles y características.

9. En Asistente para agregar roles y características, elija Tipo de instalación, seleccione Instalación basada en características o en roles y luego Siguiente.
10. En Selección de servidor, asegúrese de que el servidor local está seleccionado y elija Características en el panel de navegación izquierdo.
11. En el árbol Características, seleccione y abra Herramientas de administración remota del servidor, Herramientas de administración de roles y Herramientas de AD DS y AD LDS. Con las herramientas de AD DS y AD LDS seleccionadas, se selecciona el Active Directorymódulo para Windows PowerShell, las herramientas de AD DS y los complementos y herramientas de línea de comandos de AD LDS. Desplácese hacia abajo y seleccione Herramientas del servidor DNS y, a continuación, elija Siguiente.



12. Revise la información y elija Instalar. Cuando termine de instalarse la característica, las herramientas Active Directory Domain Services y Active Directory Lightweight Directory Services estarán disponibles en el menú de inicio, en la carpeta Herramientas administrativas.

Métodos alternativos para instalar las herramientas de administración de Active Directory en una instancia EC2 de Windows Server

- Estos son algunos otros métodos para instalar las herramientas de administración de Active Directory:
  - Si lo desea, puede optar por instalar las herramientas de administración de Active Directory medianteWindows PowerShell. Por ejemplo, puede instalar las herramientas de administración remota de Active Directory desde una PowerShell ventana de comandos utilizando`Install-WindowsFeature RSAT-ADDS`. Para obtener más información, consulte Instalar-WindowsFeature en el sitio web de Microsoft.
  - También puede iniciar una instancia EC2 de administración de directorios en la AWS Management Console que ya tenga instaladas las herramientas Active Directory Domain Services y Active Directory Lightweight Directory Services siguiendo los procedimientos descritos enInicie una instancia de administración de directorios en su Microsoft AD AWS administrado Active Directory.

Creación de un usuario

Utilice el siguiente procedimiento para crear un usuario con una instancia de EC2 unida al directorio de AWS Managed Microsoft AD. Antes de poder crear usuarios, debe completar los procedimientos de Instalación de las herramientas de administración de Active Directory.

Puede utilizar cualquiera de los métodos siguientes para crear un usuario:

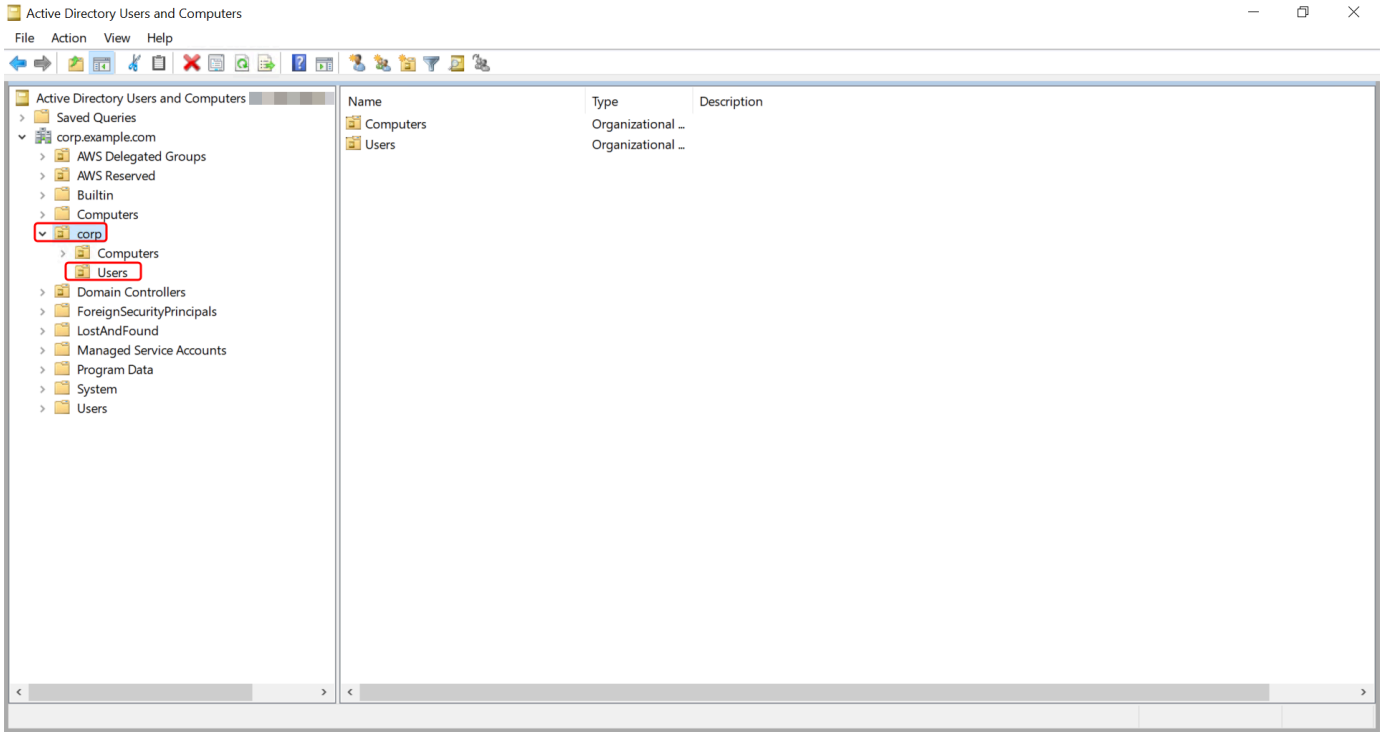
- Active DirectoryHerramientas de administración
- Windows PowerShell

Cree un usuario con las herramientas Active Directory de administración

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.
2. Abra la herramienta Usuarios y equipos de Active Directory desde el menú Inicio de Windows. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas de Windows.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. En el árbol de directorios, seleccione una unidad organizativa con el nombre de NetBIOS de su directorio (OU) en la que desee almacenar el usuario (por ejemplo,**`corp\Users`**). Para obtener más información sobre la estructura de unidades organizativas que utilizan los directorios AWS, consulteQué se crea con su Active Directory AWS administrado de Microsoft AD.



4. En el menú Acción, haga clic en Nuevo y, a continuación, haga clic en Usuario para abrir el asistente de nuevo usuario.
5. En la primera página del asistente, introduzca los valores de los siguientes campos y, a continuación, elija Siguiente.
   - First name (Nombre)
   - Last name (Apellidos)
   - Nombre de inicio de sesión de usuario

6. En la segunda página del asistente, especifique una contraseña temporal en Contraseña y Confirmar contraseña. Asegúrese de que está seleccionada la opción El usuario debe cambiar la contraseña en el próximo inicio de sesión. No debe estar seleccionada ninguna otra opción. Elija Siguiente.
7. En la tercera página del asistente, compruebe que la información de este es correcta y elija Finalizar. El nuevo usuario aparecerá en la carpeta Users.

Cree un usuario en Windows PowerShell

1. Conéctese a la instancia unida a su Active Directory dominio como Active Directory administrador.
2. Abra Windows PowerShell.
3. Escribe el siguiente comando sustituyendo el nombre **`jane.doe`** de usuario por el nombre de usuario que quieres crear. Se le pedirá Windows PowerShell que proporcione una contraseña para el nuevo usuario. Para obtener más información sobre los requisitos de complejidad de las Active Directory contraseñas, consulte Microsoftla documentación. Para obtener más información sobre el comando New-ADUser, consulte la documentación. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Eliminación de un usuario

Utilice el siguiente procedimiento para eliminar un usuario que esté unido a su Microsoft AD AWS administradoActive Directory.

Puede utilizar cualquiera de los métodos siguientes para eliminar un usuario:

- Active DirectoryHerramientas de administración
- Windows PowerShell

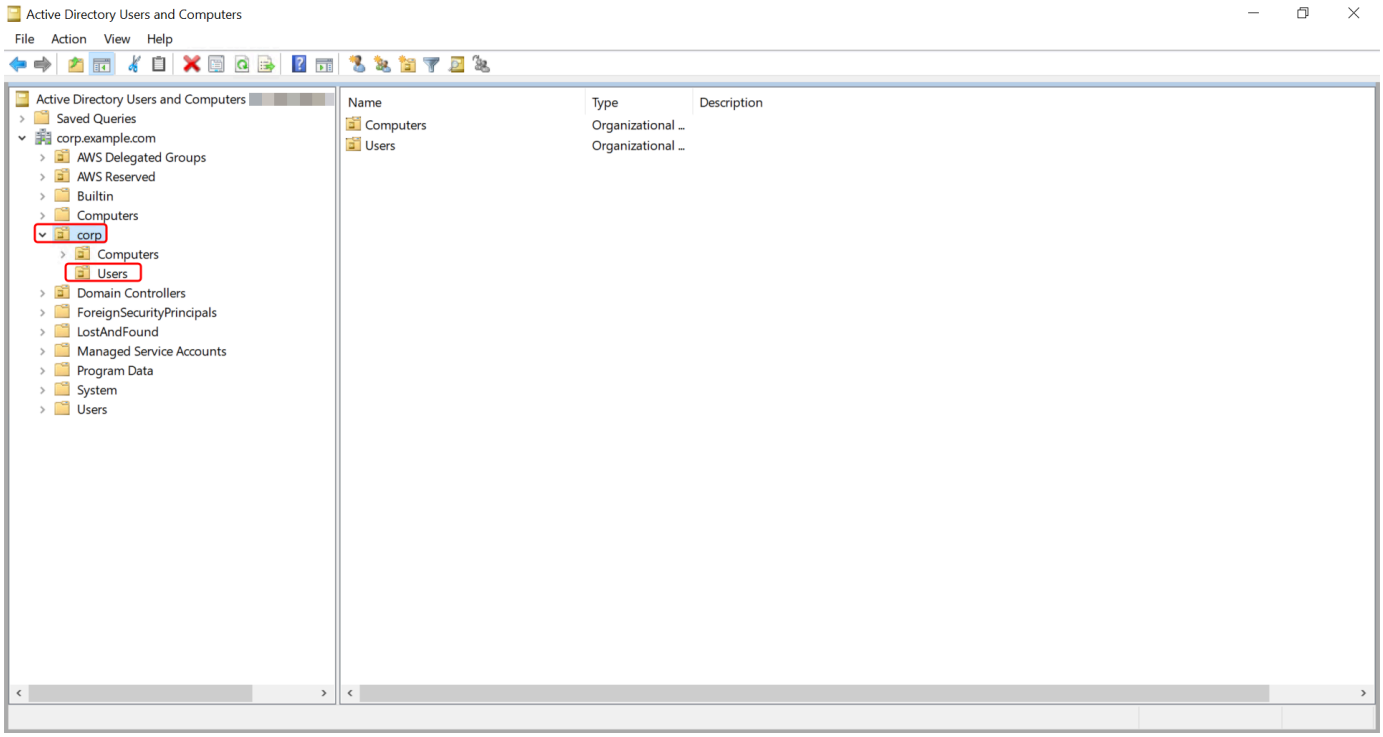
Eliminar un usuario con las herramientas Active Directory de administración

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.

2. Abra la herramienta Usuarios y equipos de Active Directory desde el menú Inicio de Windows. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas de Windows.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. En el árbol de directorios, seleccione la unidad organizativa que contiene el usuario que desea eliminar (por ejemplo,**`corp\Users`**).



4. Seleccione el usuario que desee eliminar. En el menú Acciones, elija Eliminar.

5. Aparecerá un cuadro de diálogo en el que se le solicitará que confirme que desea eliminar el usuario. Seleccione Sí para eliminar el usuario. Esto elimina permanentemente el usuario seleccionado.

Elimine un usuario en Windows PowerShell

1. Conéctese a la instancia unida a su Active Directory dominio como Active Directory administrador.
2. Abra Windows PowerShell.
3. Escribe el siguiente comando para reemplazar el nombre **`jane.doe`** de usuario por el nombre del usuario que deseas eliminar. Para obtener más información sobre el comando Remove-ADUser, consulte la documentación. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Consideraciones sobre la papelera de reciclaje AD

Los usuarios eliminados se almacenan temporalmente en la papelera de reciclaje de AD. Para obtener más información sobre la papelera de reciclaje de AD, consulte La papelera de reciclaje de AD: comprensión, implementación, mejores prácticas y solución Microsoft de problemas en el blog Pregúntele al equipo de servicios de directorio.

Restablecimiento de la contraseña de un usuario

Los usuarios deben cumplir con las políticas de contraseñas tal como se definen en laActive Directory. A veces, esto puede afectar a los usuarios, incluido el Active Directory administrador, y estos olvidan su contraseña. Cuando esto sucede, puede restablecer rápidamente la contraseña del usuario AWS Directory Service si el usuario reside en AWS Managed Microsoft AD.

Debe iniciar sesión como usuario con los permisos necesarios para restablecer las contraseñas. Para obtener más información sobre los permisos, consulte Descripción general de la administración de los permisos de acceso a sus AWS Directory Service recursos.

Puede restablecer la contraseña de cualquier usuario suyo, Active Directory con las siguientes excepciones:

- Puede restablecer la contraseña de cualquier usuario de la unidad organizativa (OU) que se base en el nombre de NetBIOS que utilizó al crear su. Active Directory Por ejemplo, si ha seguido el procedimiento indicado en Cree su Microsoft AD AWS administrado su NetBIOS, el nombre sería CORP y las contraseñas de los usuarios que podría restablecer serían miembros de Corp/Users OU.

- No puede restablecer la contraseña de ningún usuario ajeno a la OU que se base en el nombre de NetBIOS que utilizó al crear su. Active Directory Por ejemplo, no puede restablecer la contraseña de un usuario de una unidad organizativa AWS reservada. Para obtener más información acerca de la estructura de unidades organizativas de Microsoft AD AWS administrado, consulteQué se crea con su Active Directory AWS administrado de Microsoft AD.

Para obtener más información sobre cómo se aplican las políticas de contraseñas cuando se restablece una contraseña en Microsoft AD AWS administrado, consulteCómo se aplican las políticas de contraseñas.

Puede utilizar cualquiera de los métodos siguientes para restablecer la contraseña de un usuario:

- AWS Management Console
- AWS CLI
- Windows PowerShell

Restablezca una contraseña de usuario en AWS Management Console

1. En el panel de navegación de la AWS Directory Service consola, en Active Directory, elija Directorios y, a continuación, seleccione el elemento de la lista Active Directory en el que desee restablecer la contraseña de usuario.
2. En la página Detalles del directorio, seleccione Acciones, y elija Restablecer contraseña.
3. En el cuadro de diálogo Restablecer la contraseña de usuario, en Nombre de usuario escriba el nombre de usuario cuya contraseña debe cambiar.
4. Escriba una contraseña en Nueva contraseña y Confirmar contraseña y, a continuación, seleccione Restablecer contraseña.

Restablezca la contraseña de un usuario en AWS CLI

1. Para instalar el AWS CLI, consulte Instalar o actualizar la última versión del AWS CLI.
2. Abre el AWS CLI.
3. Escriba el siguiente comando y sustituya el ID del directorio, el nombre de usuario **`jane.doe`** y la contraseña **`P@ssw0rd`** por el ID del Active Directory directorio y las credenciales deseadas. Consulte reset-user-passwordla Referencia de AWS CLI comandos para obtener más información.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Restablezca una contraseña de usuario en Windows PowerShell

1. Conéctese a la instancia unida a su Active Directory dominio como Active Directory administrador.
2. Abra Windows PowerShell.
3. Escribe el siguiente comando para sustituir el nombre de usuario**`jane.doe`**, el ID del directorio y la contraseña **`P@ssw0rd`** por el ID del Active Directory directorio y las credenciales que desees. Consulte el UserPassword cmdlet Reset-DS para obtener más información.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Creación de un grupo

Utilice el siguiente procedimiento para crear un grupo de seguridad con una instancia EC2 que esté unida al directorio de Microsoft AD AWS administrado. Antes de poder crear grupos de seguridad, debe completar los procedimientos de Instalación de las herramientas de administración de Active Directory.

También puede usar Windows PowerShell comandos para crear grupos. Para obtener más información, consulte New-ADGroup en la documentación de Windows Server 2022. PowerShell

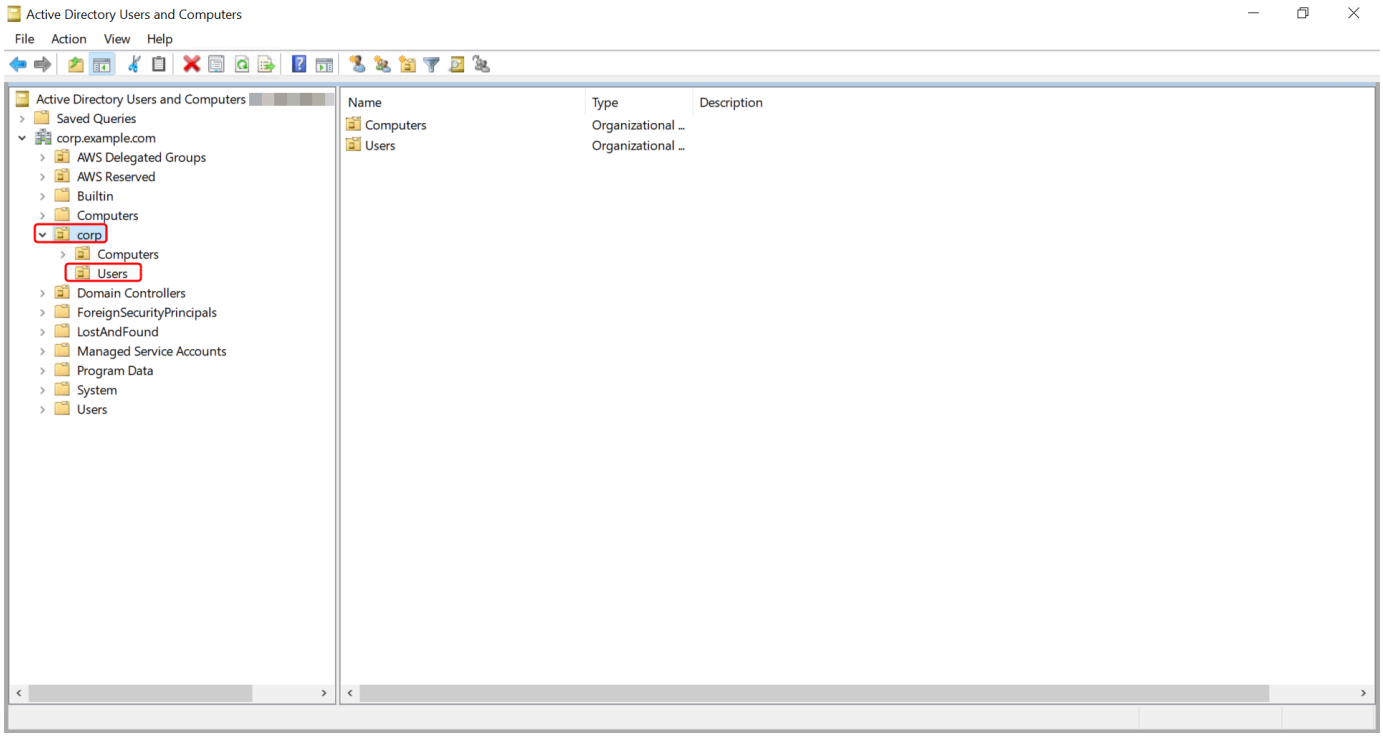
Creación de un grupo

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.
2. Abra la herramienta Usuarios y equipos de Active Directory. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. En el árbol del directorio, seleccione una unidad organizativa (OU) bajo el nombre de NetBIOS de su directorio en la que desee almacenar el grupo (por ejemplo, Corp\Users). Para obtener más información sobre la estructura de unidades organizativas que utilizan los directorios en AWS, consulte. Qué se crea con su Active Directory AWS administrado de Microsoft AD



4. En el menú Action, haga clic en New y, a continuación, haga clic en Group para abrir el asistente de nuevo grupo.
5. Escriba un nombre para el grupo en Nombre del grupo, seleccione un Ámbito del grupo que se adapte a sus necesidades y seleccione Seguridad para el Tipo de grupo. Para obtener más información sobre el ámbito de los grupos y los grupos de seguridad de Active Directory, consulte los Grupos de seguridad de Active Directory en la documentación de Microsoft Windows Server.
6. Haga clic en OK (Aceptar). El nuevo grupo de seguridad aparecerá en la carpeta Usuarios.

Adición de un usuario a un grupo

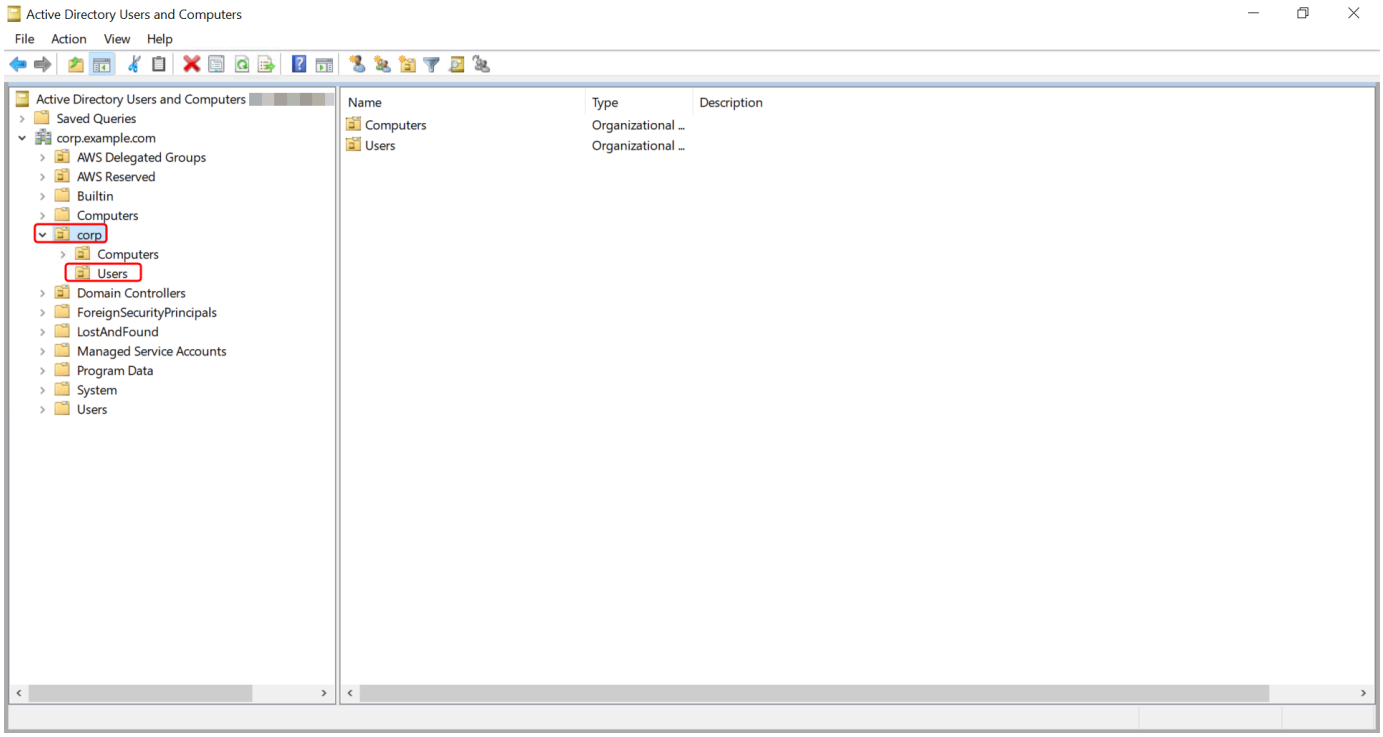
Utilice el siguiente procedimiento para agregar un usuario a un grupo de seguridad con una instancia de EC2 unida al directorio de AWS Managed Microsoft AD.

Para añadir un usuario a un grupo

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.
2. Abra la herramienta Usuarios y equipos de Active Directory. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. En el árbol del directorio, seleccione la unidad organizativa (OU) situada bajo el nombre de NetBIOS en la que ha almacenado el grupo y seleccione el grupo al que desea agregar un usuario como miembro.



4. En el menú Acción, haga clic en Propiedades para abrir el cuadro de diálogo de propiedades del grupo.
5. Seleccione la pestaña Miembros y haga clic en Agregar.

6. En Introduzca los nombres de los objetos que desea seleccionar, escriba el nombre de usuario que desee añadir y haga clic en Aceptar. El nombre aparecerá en la lista de Miembros. Haga clic en OK de nuevo para actualizar la pertenencia a grupos.
7. Para comprobar que el usuario es ahora miembro del grupo, selecciónelo en la carpeta Usuarios y haga clic en Propiedades en el menú Acción para abrir el cuadro de diálogo de propiedades. Seleccione la pestaña Miembro de. Debería ver el nombre del grupo en la lista de grupos a los que pertenece el usuario.

Conéctese a su infraestructura de Active Directory existente

En esta sección se describe cómo configurar las relaciones de confianza entre Microsoft AD AWS administrado y la infraestructura de Active Directory existente.

Temas

Creación de una relación de confianza

Puede configurar relaciones de confianza externas y forestales unidireccionales y bidireccionales entre su AWS Directory Service para Microsoft Active Directory y los directorios autogestionados (locales), así como entre varios directorios gestionados de AWS Microsoft AD en la nube. AWS AWS Microsoft AD administrado admite las tres direcciones de relación de confianza: entrante, saliente y bidireccional (bidireccional).

Para obtener más información sobre la relación de confianza, consulte Todo lo que desea saber sobre las confianzas con Microsoft AD AWS administrado.

> **Note**
>
> Al configurar relaciones de confianza, debe asegurarse de que su directorio autogestionado sea y siga siendo compatible con AWS Directory Service s. Para obtener más información acerca de sus responsabilidades, consulte nuestro modelo de responsabilidad compartida.

AWS Microsoft AD administrado admite confianzas tanto externas como forestales. Para ver un caso de ejemplo donde se muestra cómo crear una relación de confianza entre bosques, consulte Tutorial: Creación de una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio de Active Directory autogestionado.

Se requiere una confianza bidireccional para aplicaciones AWS empresariales como Amazon Chime, Amazon Connect, QuickSight Amazon AWS IAM Identity Center, Amazon WorkDocs, Amazon WorkMail, WorkSpaces Amazon y. AWS Management Console AWS Microsoft AD administrado debe poder consultar a los usuarios y grupos de su cuenta autogestionadaActive Directory.

Amazon EC2, Amazon RDS y Amazon FSx funcionarán con una confianza unidireccional o bidireccional.

Requisitos previos

Para crear una relación de confianza solo son necesarios unos pasos, pero primero debe completar otros pasos previos antes de configurarla.

> **Note**
>
> AWS Microsoft AD administrado no admite la confianza con los dominios de etiqueta única.

Conéctese a VPC

Si va a crear una relación de confianza con su directorio autogestionado, primero debe conectar su red autogestionada a la Amazon VPC que contiene su Microsoft AD gestionado AWS . El firewall de las redes Microsoft AD AWS autoadministradas y administradas debe tener abiertos los puertos de red que aparecen en la Microsoft documentación de WindowsServer 2008 y versiones posteriores.

Para usar su nombre NetBIOS en lugar de su nombre de dominio completo para la autenticación con AWS aplicaciones como Amazon o WorkDocs Amazon QuickSight, debe permitir el puerto

9389. Para obtener más información sobre los puertos y protocolos de Active Directory, consulte la documentación sobre la descripción general del servicio y los requisitos de los puertos de Windows red. Microsoft

Estos son los puertos mínimos necesarios para poder conectarse al directorio. La configuración específica podría requerir abrir puertos adicionales.

Configure la VPC

La VPC que contiene su AWS Microsoft AD administrado debe tener las reglas de entrada y salida adecuadas.

Configuración de las reglas de salida de la VPC

1. En la AWS Directory Service consola, en la página Detalles del directorio, anota tu ID de directorio AWS administrado de Microsoft AD.
2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
3. Seleccione Security Groups.
4. Busca tu ID de directorio AWS administrado de Microsoft AD. En los resultados de la búsqueda, seleccione el elemento con la descripción «grupo de seguridad AWS creado para los controladores de directorio con ID de directorio».

   > **Note**
   >
   > El grupo de seguridad seleccionado es un grupo de seguridad que se crea automáticamente en el momento de crearse el directorio.

5. Vaya a la pestaña Outbound Rules de ese grupo de seguridad. Seleccione Edit y después Add another rule. Para la nueva regla, escriba los siguientes valores:

   - Type: All Traffic
   - Protocol: All
   - Destination determina el tráfico que puede salir de sus controladores de dominio y a dónde puede ir en su red autogestionada. Especifique una única dirección IP o un rango de direcciones IP en notación CIDR (por ejemplo, 203.0.113.5/32). También puede especificar el nombre o el ID de otro grupo de seguridad en la misma región. Para obtener más información, consulte Comprenda la configuración y el uso de los grupos de AWS seguridad de su directorio.

6. Seleccione Guardar.

Habilitación de la autenticación previa de Kerberos

Sus cuentas de usuario deben tener habilitada la autenticación previa de Kerberos. Para obtener más información acerca de esta configuración, consulte Autenticación previa en Microsoft TechNet.

Configuración de programas de envío condicionales DNS en su dominio autogestionado

Debe configurar programas de envío condicionales DNS en su dominio autogestionado. Consulte Asignar un reenviador condicional a un nombre de dominio en Microsoft TechNet para obtener más información sobre los reenviadores condicionales.

Para seguir estos pasos, debe tener acceso a las herramientas de Windows Server enumeradas a continuación para su dominio autogestionado:

- AD DS y AD LDS Tools
- DNS

Configuración de reenviadores condicionales DNS en su dominio autogestionado

1. En primer lugar, debe obtener información sobre su Microsoft AD AWS administrado. Inicie sesión en la AWS Management Console y abra la consola de AWS Directory Service.
2. En el panel de navegación, seleccione Directories.
3. Elija el ID de directorio de su Microsoft AD AWS administrado.
4. Tome nota del nombre de dominio completo (FQDN) y las direcciones de DNS de su directorio.
5. Ahora, vuelva a su controlador de dominio autogestionado. Abra el Administrador del servidor.
6. En el menú Herramientas, elija DNS.
7. En el árbol de la consola, amplíe el servidor DNS del dominio para el cual esté configurando la relación de confianza.
8. En el árbol de la consola, seleccione Reenviadores condicionales.
9. En el menú Acción, elija Nuevo reenviador condicional.
10. En el dominio DNS, escriba el nombre de dominio completo (FQDN) de su Microsoft AD AWS administrado, que indicó anteriormente.
11. Elija las direcciones IP de los servidores principales y escriba las direcciones DNS de su directorio AWS administrado de Microsoft AD, que indicó anteriormente.

Después de escribir las direcciones de DNS, es posible que aparezca un error que indique que se ha agotado el tiempo de espera o que no se pudo resolver la operación. Por lo general, puede ignorar estos errores.

12. Active la casilla Almacenar este reenviador condicional en Active Directory y replicarlo como sigue: Todos los servidores DNS en este dominio. Seleccione Aceptar.

Contraseña de relación de confianza

Si crea una relación de confianza con un dominio existente, configure la relación de confianza en ese dominio con las herramientas de administración de Windows Server. Al hacerlo, indique su contraseña de confianza. Deberá usar esta misma contraseña al configurar la relación de confianza en el Microsoft AD AWS administrado. Para obtener más información, consulte Administración de confianzas en Microsoft TechNet.

Ahora está listo para crear la relación de confianza en su Microsoft AD AWS administrado.

NetBIOS y nombres de dominio

Los nombres de dominio y NetBIOS deben ser únicos y no pueden ser los mismos para establecer una relación de confianza.

Crear, verificar o eliminar una relación de confianza

> **Note**
>
> Las relaciones de confianza son una característica global de AWS Managed Microsoft AD. Si está utilizando Replicación multirregional, se deben seguir estos procedimientos en Región principal . Los cambios se aplicarán automáticamente en todas las regiones replicadas. Para obtener más información, consulte Características globales frente a las regionales.

Para crear una relación de confianza con su Microsoft AD AWS administrado

1. Abra la consola de AWS Directory Service.
2. En la página Directorios, elige tu ID de Microsoft AD AWS administrado.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:

- Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
- Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.

4. En la sección Trust relationships (Relaciones de confianza), elija Actions (Acciones) y, a continuación, seleccione Add trust relationship (Añadir relación de confianza).
5. En la página Add a trust relationship (Añadir una relación de confianza), proporcione la información necesaria, incluidos el tipo de confianza, el nombre de dominio completo (FQDN) del dominio de confianza, la contraseña de confianza y la dirección de confianza.
6. (Opcional) Si desea permitir que solo los usuarios autorizados accedan a los recursos de su directorio AWS administrado de Microsoft AD, puede seleccionar opcionalmente la casilla de verificación Autenticación selectiva. Para obtener información general sobre la autenticación selectiva, consulte Consideraciones de seguridad para Trusts on Microsoft TechNet.
7. En Reenviador condicional, escriba la dirección IP del servidor DNS autogestionado. Si ha creado anteriormente reenviadores condicionales, puede escribir el FQDN de su dominio autogestionado en lugar de una dirección IP de DNS.
8. (Opcional) Elija Agregar otra dirección IP y escriba la dirección IP de un servidor DNS autogestionado adicional. Puede repetir este paso para cada dirección de servidor DNS aplicable, con un máximo de cuatro direcciones.
9. Elija Añadir.
10. Si el servidor DNS o la red de su dominio autogestionado usa un espacio de direcciones IP público (no RFC 1918), vaya a la sección Direccionamiento IP, elija Acciones y, a continuación, elija Agregar ruta. Escriba el bloque de direcciones IP del servidor DNS o su red autogestionada en formato CIDR, por ejemplo 203.0.113.0/24. Este paso no es necesario si su servidor DNS y su red autogestionada están utilizando espacios de direcciones IP RFC 1918.

    > **Note**
    >
    > Cuando se utiliza un espacio de direcciones IP públicas, asegúrese de no utilizar ninguno de los rangos de direcciones IP de AWS dado que no se pueden utilizar.

11. (Opcional) Le recomendamos que mientras se encuentra en la página Add routes (Añadir rutas) también seleccione Add routes to the security group for this directory's VPC (Añadir rutas al grupo de seguridad de la VPC de este directorio). De este modo se configurarán los grupos

de seguridad según se detalla anteriormente, en “Configuración de la VPC”. Estas reglas de seguridad afectan a una interfaz de red interna no expuesta públicamente. Si esta opción no está disponible, verá un mensaje en su lugar en el que se indica que ya ha personalizado sus grupos de seguridad.

Debe configurar la relación de confianza en ambos dominios. Las relaciones deben ser complementarias. Por ejemplo, si crea una relación de confianza saliente en un dominio, debe crear una relación de confianza entrante en el otro.

Si crea una relación de confianza con un dominio existente, configure la relación de confianza en ese dominio con las herramientas de administración de Windows Server.

Puede crear varias confianzas entre su Microsoft AD AWS administrado y varios dominios de Active Directory. No obstante, solo puede existir una relación de confianza por par a la vez. Por ejemplo, si existe una relación de confianza unidireccional en la “dirección entrante” y desea configurar otra relación de confianza en la “dirección saliente”, deberá eliminar la relación de confianza existente y crear una nueva relación de confianza bidireccional.

Verificación de una relación de confianza saliente

1. Abra la consola de AWS Directory Service.
2. En la página Directorios, elige tu ID de Microsoft AD AWS administrado.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Trust relationships (Relaciones de confianza), seleccione la confianza que desea verificar, elija Actions (Acciones) y, a continuación, seleccione Verify trust relationship (Verificar relación de confianza).

Este proceso verifica solo la dirección de salida de una confianza bidireccional. AWS no admite la verificación de un fideicomiso entrante. Para obtener más información sobre cómo comprobar la confianza hacia o desde su Active Directory autoadministrado, consulte Verificar una confianza en Microsoft TechNet.

Eliminación de una relación de confianza existente

1. Abra la consola de AWS Directory Service.
2. En la página Directorios, elige tu ID de Microsoft AD AWS administrado.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Trust relationships (Relaciones de confianza), seleccione la confianza que desea eliminar, elija Actions (Acciones) y, a continuación, seleccione Delete trust relationship (Eliminar relación de confianza).
5. Elija Eliminar.

Agregar rutas IP al utilizar direcciones IP públicas

Puede utilizar AWS Directory Service para Microsoft Active Directory para aprovechar muchas características eficaces de Active Directory, incluido el establecimiento de confianzas con otros directorios. Sin embargo, si los servidores DNS para las redes de los demás directorios utilizan direcciones IP públicas (no RFC 1918), debe especificar dichas direcciones IP como parte de la configuración de la confianza. Las instrucciones para hacerlo pueden encontrarse en Creación de una relación de confianza.

Del mismo modo, también debe escribir la información de la dirección IP cuando dirija el tráfico desde su AWS Managed Microsoft AD en AWS a una VPC de AWS interconectada, si la VPC utiliza rangos de IP públicas.

Al añadir las direcciones IP tal y como se describe en Creación de una relación de confianza, tiene la opción de seleccionar Add routes to the security group for this directory's VPC. Esta opción se debe seleccionar a menos que haya personalizado anteriormente el grupo de seguridad para permitir el tráfico necesario, tal y como se muestra a continuación. Para obtener más información, consulte Comprenda la configuración y el uso de los grupos de AWS seguridad de su directorio.

Tutorial: Creación de una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio de Active Directory autogestionado

En este tutorial, se explican todos los pasos necesarios para configurar una relación de confianza entre AWS Directory Service para Microsoft Active Directory y su directorio de Microsoft Active Directory (en las instalaciones) autogestionado. Crear la relación de confianza solo requiere unos cuantos pasos, pero antes se deben haber satisfecho los requisitos previos siguientes.

Temas

Véase también

Creación de una relación de confianza

Requisitos previos

Este tutorial parte de la base de que ya se dispone de lo siguiente:

> **Note**
>
> AWS Managed Microsoft AD no admite la confianza con dominios de etiqueta única.

- Se ha creado un directorio de AWS Managed Microsoft AD en AWS. Si necesita ayuda para hacerlo, consulte Introducción a AWS Managed Microsoft AD.
- Se ha agregado una instancia de EC2 que ejecuta Windows a ese directorio de AWS Managed Microsoft AD. Si necesita ayuda para hacerlo, consulte Unir manualmente una Windows instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory.

> **Important**
>
> La cuenta de administrador de su directorio de AWS Managed Microsoft AD debe tener acceso administrativo a esta instancia.

- Las siguientes herramientas de Windows Server instaladas en la instancia:
  - AD DS y AD LDS Tools
  - DNS

  Si necesita ayuda para hacerlo, consulte Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado.
- Un directorio de Microsoft Active Directory (en las instalaciones) autogestionado

  Debe disponer de acceso administrativo a ese directorio. Las herramientas de Windows Server antes indicadas también deben estar disponibles para este directorio.
- Una conexión activa entre la red autogestionada y la VPC que contiene el directorio de AWS Managed Microsoft AD. Si necesita ayuda para hacerlo, consulte Amazon Virtual Private Cloud Connectivity Options.
- Una política de seguridad local configurada correctamente. Compruebe `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` y asegúrese de que contenga al menos las siguientes tres canalizaciones mencionadas a continuación:
  - netlogon
  - samr
  - lsarpc
- Los nombres de dominio y NetBIOS deben ser únicos y no pueden ser los mismos para establecer una relación de confianza

Para obtener más información acerca de los requisitos previos para crear una relación de confianza, consulte Creación de una relación de confianza.

Configuración del tutorial

Para este tutorial, ya hemos creado un directorio de AWS Managed Microsoft AD y un dominio autogestionado. La red autogestionada está conectada a la VPC de AWS Managed Microsoft AD. Estas son las propiedades de ambos directorios:

AWS Managed Microsoft AD que se ejecuta en AWS

- Nombre de dominio (FQDN): MyManagedAD.example.com
- Nombre NetBIOS: MyManagedAD

- Direcciones de DNS: 10.0.10.246, 10.0.20.121
- CIDR de VPC: 10.0.0.0/16

AWS Managed Microsoft AD reside en el identificador de la VPC: vpc-12345678.

Dominio de AWS Managed Microsoft AD o autogestionado

- Nombre de dominio (FQDN): corp.example.com
- Nombre NetBIOS: CORP
- Direcciones de DNS: 172.16.10.153
- CIDR autogestionado: 172.16.0.0/16

Paso siguiente

Paso 1: preparación del dominio de AD autogestionado

Paso 1: preparación del dominio de AD autogestionado

En primer lugar, es necesario completar varios pasos previos obligatorios en su dominio autogestionado (en las instalaciones).

Configuración de un firewall autogestionado

Debe configurar el firewall autoadministrado para que los siguientes puertos estén abiertos a los CIDR de todas las subredes utilizadas por la VPC que contiene su Microsoft AD administrado. AWS En este tutorial, permitimos el tráfico entrante y saliente desde 10.0.0.0/16 (el bloque CIDR de nuestra VPC gestionada de AWS Microsoft AD) en los siguientes puertos:

- TCP/UDP 53: DNS
- TCP/UDP 88: autenticación de Kerberos
- TCP/UDP 389: protocolo ligero de acceso a directorios (LDAP)
- TCP 445: bloque de mensajes del servidor (SMB)
- TCP 9389: Servicios web de Active Directory (ADWS) (opcional: este puerto debe estar abierto si desea utilizar su nombre de NetBIOS en lugar del nombre de dominio completo para la autenticación con aplicaciones AWS como Amazon o WorkDocs Amazon). QuickSight

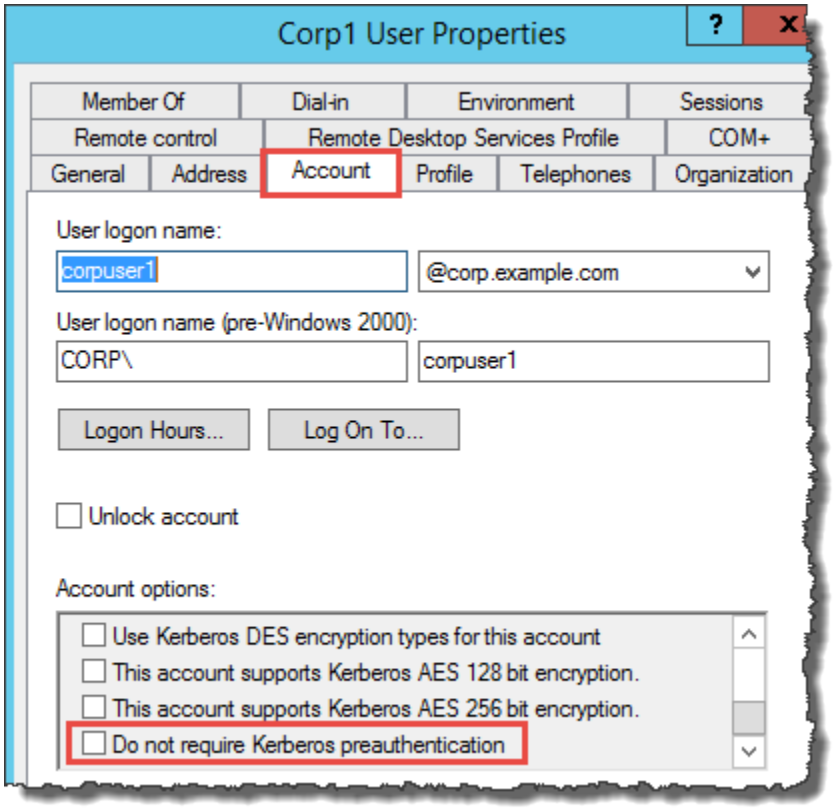
> **Note**
>
> SMBv1 ya no es compatible.
> Estos son los puertos mínimos necesarios para conectar la VPC y al directorio autogestionado. La configuración específica podría requerir abrir puertos adicionales.

Asegúrese de que la autenticación previa de Kerberos esté habilitada

Las cuentas de usuario en ambos directorios deben tener habilitada la autenticación previa de Kerberos. Esta es la configuración predeterminada, pero vamos a comprobar las propiedades de cualquier usuario aleatorio para asegurarnos de que no haya cambiado nada.

Para ver la configuración de Kerberos del usuario

1. En el controlador de dominio autogestionado, abra Server Manager.
2. En el menú Herramientas, elija Usuarios y equipos de Active Directory.
3. Elija la carpeta Users (Usuarios) y abra el menú contextual (haga clic con el botón derecho del ratón). Seleccione cualquiera de las cuentas de usuario que se muestran en el panel de la derecha. Seleccione Propiedades.
4. Elija la pestaña Cuenta. En la lista Opciones de cuenta, desplácese hacia abajo y asegúrese de que No pedir la autenticación Kerberos previa no esté seleccionado.



Configuración de reenviadores condicionales DNS en su dominio autogestionado

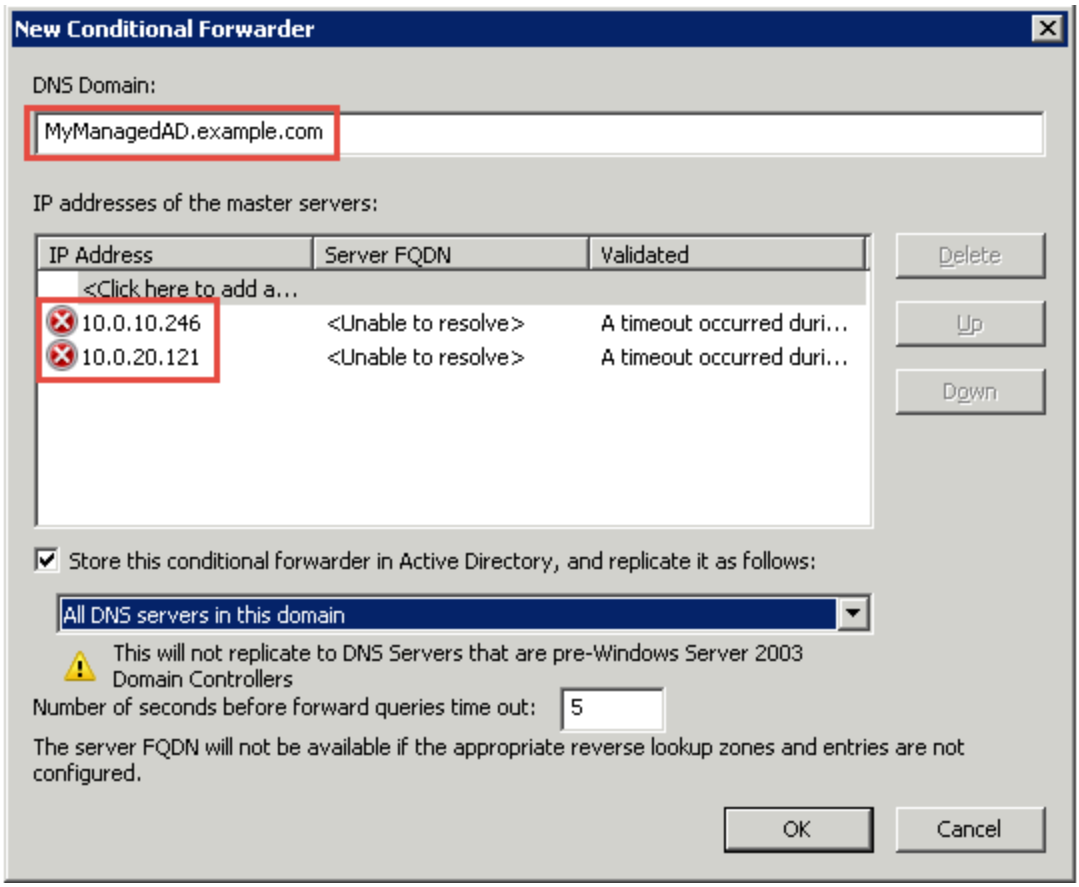
Debe configurar programas de envío condicionales DNS en cada dominio. Antes de hacerlo en tu dominio autogestionado, primero obtendrás información sobre tu Microsoft AD AWS gestionado.

Configuración de reenviadores condicionales DNS en su dominio autogestionado

1. Inicia sesión en la AWS Directory Service consola AWS Management Console y ábrela.
2. En el panel de navegación, seleccione Directories.
3. Elija el ID de directorio de su Microsoft AD AWS administrado.
4. En la página Details (Detalles), anote los valores de Directory name (Nombre de directorio) y DNS address (Dirección DNS) del directorio.
5. Ahora, vuelva a su controlador de dominio autogestionado. Abra el Administrador del servidor.
6. En el menú Herramientas, elija DNS.
7. En el árbol de la consola, amplíe el servidor DNS del dominio para el cual esté configurando la relación de confianza. Nuestro servidor es WIN-5V70CN7VJ0.corp.example.com.
8. En el árbol de la consola, seleccione Reenviadores condicionales.

9. En el menú Acción, elija Nuevo reenviador condicional.
10. En el dominio DNS, escriba el nombre de dominio completo (FQDN) de su Microsoft AD AWS administrado, que indicó anteriormente. En este ejemplo, el FQDN es MyManaged AD.example.com.
11. Elija las direcciones IP de los servidores principales y escriba las direcciones DNS de su directorio AWS administrado de Microsoft AD, que indicó anteriormente. En este ejemplo son: 10.0.10.246 y 10.0.20.121

    Después de escribir las direcciones de DNS, es posible que aparezca un error que indique que se ha agotado el tiempo de espera o que no se pudo resolver la operación. Por lo general, puede ignorar estos errores.



12. Active la casilla Almacenar este reenviador condicional en Active Directory y replicarlo como sigue.
13. Seleccione Todos los servidores DNS en este dominio y después haga clic en Aceptar.

Paso siguiente

Paso 2: preparación de su AWS Managed Microsoft AD

Paso 2: preparación de su AWS Managed Microsoft AD

Ahora preparemos su Microsoft AD AWS administrado para la relación de confianza. Muchos de los pasos siguientes son casi idénticos a los que acaba de completar para su dominio autogestionado. Sin embargo, esta vez está trabajando con su Microsoft AD AWS administrado.

Configuración de las subredes de VPC y los grupos de seguridad

Debe permitir el tráfico de su red autogestionada a la VPC que contiene su Microsoft AD AWS gestionado. Para ello, tendrá que asegurarse de que las ACL asociadas a las subredes utilizadas para implementar su AWS Microsoft AD administrado y las reglas de los grupos de seguridad configuradas en los controladores de dominio permiten el tráfico necesario para respaldar las confianzas.

Los requisitos de puertos varían en función de la versión de Windows Server que utilizan los controladores de dominio y de los servicios o las aplicaciones que van a utilizar la relación de confianza. Para este tutorial, tendrá que abrir los siguientes puertos:

Entrada

- TCP/UDP 53: DNS
- TCP/UDP 88: autenticación de Kerberos
- UDP 123: NTP
- TCP 135: RPC
- TCP/UDP 389: LDAP
- TCP/UDP 445: SMB
- TCP/UDP 464: autenticación Kerberos
- TCP 636: LDAPS (LDAP a través de TLS/SSL)
- TCP 3268-3269: catálogo global
- TCP/UDP 49152-65535: puertos efímeros de RPC

> **Note**
>
> SMBv1 ya no es compatible.

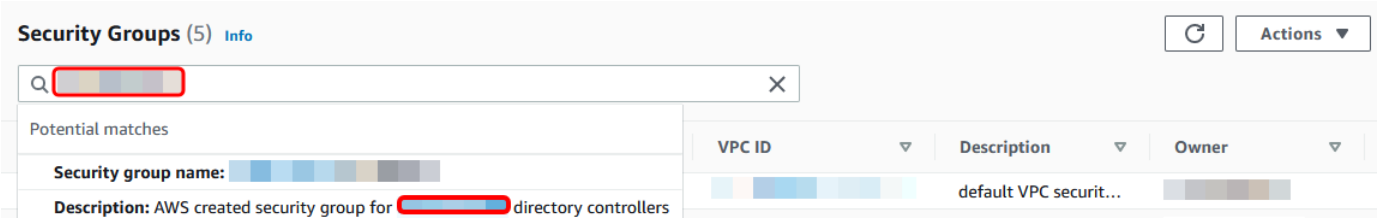
Salida

- ALL

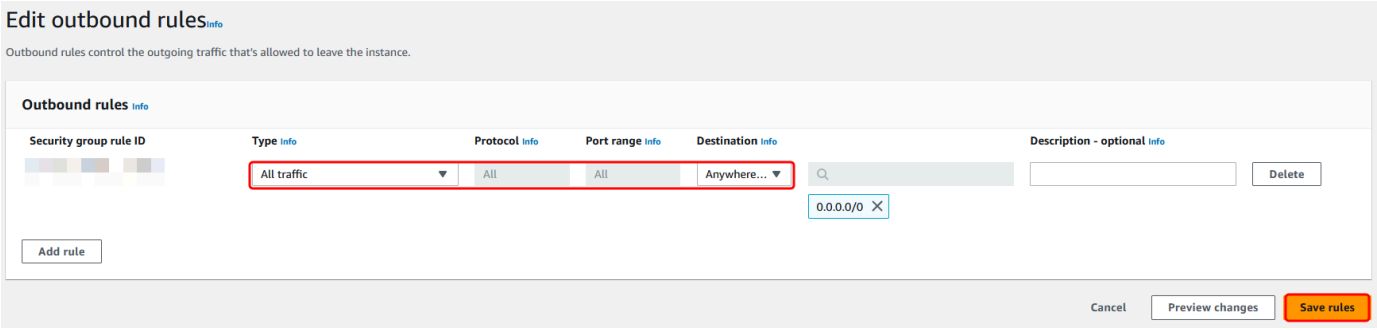
> **Note**
>
> Estos son los puertos mínimos necesarios para poder conectar la VPC y el directorio autogestionado. La configuración específica podría requerir abrir puertos adicionales.

Para configurar las reglas de entrada y salida del controlador de dominio AWS administrado de Microsoft AD

1. Vuelva a la consola de AWS Directory Service. En la lista de directorios, anote el identificador de directorio de su directorio AWS administrado de Microsoft AD.
2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
3. En el panel de navegación, elija Security Groups (Grupos de seguridad).
4. Usa el cuadro de búsqueda para buscar tu ID de directorio de Microsoft AD AWS administrado. En los resultados de la búsqueda, seleccione el grupo de seguridad con la descripción**`AWS created security group for yourdirectoryID directory controllers`**.



5. Vaya a la pestaña Outbound Rules en ese grupo de seguridad. Elija Editar reglas y, a continuación, Agregar regla. Para la nueva regla, escriba los siguientes valores:
   - Type (Tipo): ALL Traffic (Todo el tráfico)
   - Protocol (Protocolo): ALL (Todos)
   - Destination (Destino) determina el tráfico que puede salir de sus controladores de dominio y a dónde puede ir. Especifique una única dirección IP o un rango de direcciones IP en notación CIDR (por ejemplo, 203.0.113.5/32). También puede especificar el nombre o el ID de otro grupo de seguridad en la misma región. Para obtener más información, consulte Comprenda la configuración y el uso de los grupos de AWS seguridad de su directorio.
6. Seleccione Guardar regla.

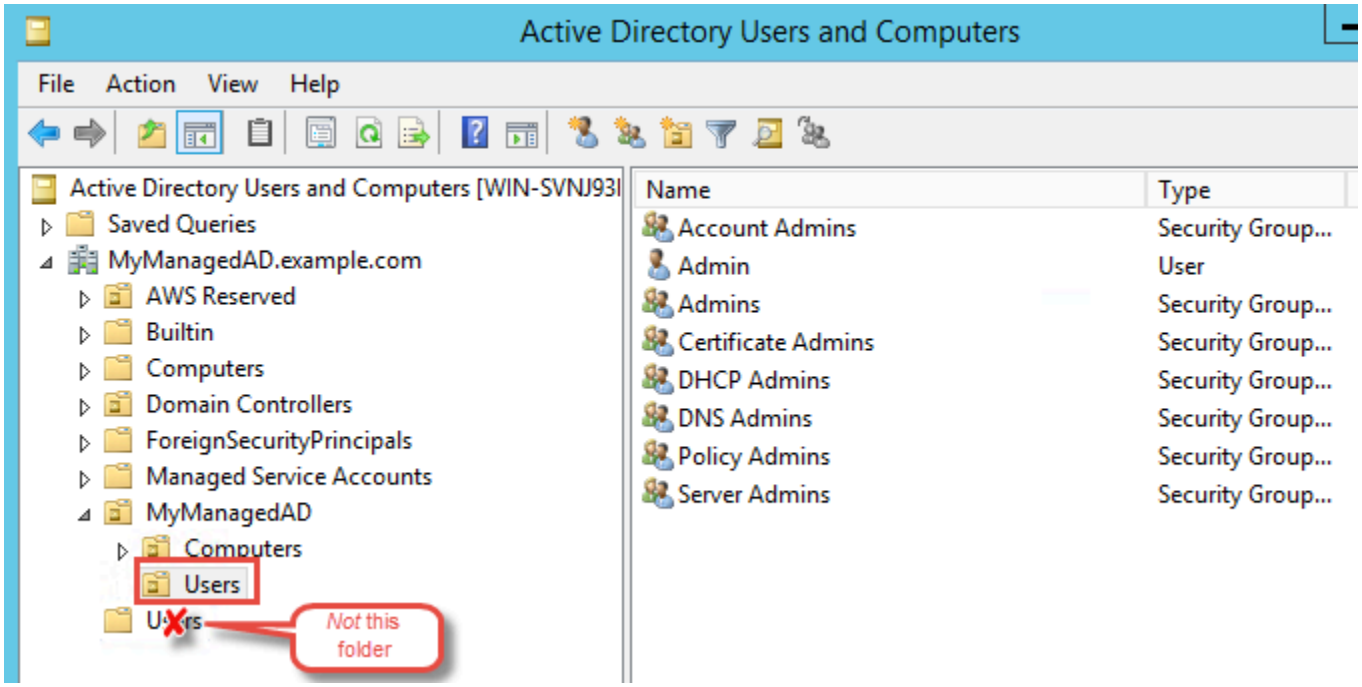


Asegúrese de que la autenticación previa de Kerberos esté habilitada

Ahora quiere confirmar que los usuarios de su Microsoft AD AWS administrado también tienen habilitada la autenticación previa de Kerberos. Este es el mismo proceso que ha completado para su directorio autogestionado. Esta es la configuración predeterminada, pero vamos a comprobar que no haya cambiado nada.

Visualización de la configuración de Kerberos del usuario

1. Inicie sesión en una instancia que sea miembro de su directorio AWS administrado de Microsoft AD mediante el Permisos para la cuenta de administrador dominio o una cuenta a la que se le hayan delegado permisos para administrar los usuarios del dominio.
2. Si no están instaladas todavía, instale la herramienta Usuarios y equipos de Active Directory y la herramienta de DNS. Obtenga información sobre cómo instalar estas herramientas en Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado.
3. Abra el Administrador del servidor. En el menú Herramientas, elija Usuarios y equipos de Active Directory.
4. Seleccione la carpeta Usuarios en su dominio. Tenga en cuenta que esta es la carpeta Users (Usuarios) situada bajo el nombre de NetBIOS, no la carpeta Users (Usuarios) situada bajo el nombre de dominio completo (FQDN).



5. En la lista de usuarios, haga clic con el botón derecho en un usuario y seleccione Properties (Propiedades).
6. Elija la pestaña Cuenta. En la lista Opciones de cuenta, desplácese hacia abajo y asegúrese de que No pedir la autenticación Kerberos previa no esté activado.

Paso siguiente

Paso 3: creación de la relación de confianza

Paso 3: creación de la relación de confianza

Ahora que ha finalizado el trabajo de preparación, los pasos finales se centran en crear las relaciones de confianza. Primero deberá crear la relación de confianza en el dominio autogestionado y, después, por último, en su directorio de AWS Managed Microsoft AD. Si se presenta algún problema durante el proceso de creación de relaciones de confianza, consulte Motivos de los estados al crear relaciones de confianza para obtener ayuda.

Configuración de la relación de confianza en el directorio de Active Directory autogestionado

En este tutorial, va a configurar una relación de confianza bidireccional. No obstante, si crea una relación de confianza entre bosques unidireccional, tenga en cuenta que la dirección de la relación de confianza de cada uno de los dominios debe ser complementaria. Por ejemplo, si crea una

relación de confianza unidireccional saliente en su dominio autogestionado, debe crear una relación de confianza entrante unidireccional en su directorio de AWS Managed Microsoft AD.

> **Note**
>
> AWS Managed Microsoft AD también admite relaciones de confianza externas. Sin embargo, para este tutorial, creará una relación de confianza bidireccional entre bosques.

Para configurar la confianza en su Active Directory autoadministrado

1. Abra el Administrador del servidor y, en el menú Herramientas, elija Dominios y confianzas de Active Directory.
2. Abra el menú contextual (con el botón derecho) de su dominio y elija Propiedades.
3. Elija la pestaña Confianzas y luego Nueva confianza. Escriba el nombre de su AWS Managed Microsoft AD y elija Siguiente.
4. Elija Confianza de bosque. Elija Siguiente.
5. Elija Bidireccional. Elija Siguiente.
6. Elija Solo este dominio. Elija Siguiente.
7. Elija Autenticación en todo el bosque. Elija Siguiente.
8. Escriba un valor en Contraseña de la confianza. Asegúrese de que podrá recordar esta contraseña, ya que la necesitará al configurar la relación de confianza para su AWS Managed Microsoft AD.
9. En el siguiente cuadro de diálogo, confirme la configuración y elija Siguiente. Confirme que la confianza se haya creado correctamente y vuelva a seleccionar Siguiente.
10. Elija No, no confirmar la confianza saliente. Elija Siguiente.
11. Elija No, no confirmar la confianza entrante. Elija Siguiente.

Configuración de la relación de confianza en su directorio de AWS Managed Microsoft AD

Por último, tendrá que configurar la relación de confianza entre bosques con el directorio de AWS Managed Microsoft AD. Como ha creado una relación de confianza bidireccional entre bosques en el dominio autogestionado, también tiene que crear una relación de confianza bidireccional utilizando el directorio de AWS Managed Microsoft AD.

> **Note**
>
> Las relaciones de confianza son una característica global de AWS Managed Microsoft AD. Si está utilizando Replicación multirregional, se deben seguir estos procedimientos en Región principal . Los cambios se aplicarán automáticamente en todas las regiones replicadas. Para obtener más información, consulte Características globales frente a las regionales.

Configuración de la relación de confianza en su directorio de AWS Managed Microsoft AD

1. Vuelva a la consola de AWS Directory Service.
2. En la página Directorios, elija el ID de AWS Managed Microsoft AD.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Trust relationships (Relaciones de confianza), elija Actions (Acciones) y, a continuación, seleccione Add trust relationship (Añadir relación de confianza).
5. En la página Agregar una relación de confianza, especifique el tipo de confianza. En este caso, elegimos Relación de confianza entre bosques. Escriba el FQDN de su dominio autogestionado (en este tutorial, **`corp.example.com`**). Escriba la misma contraseña de confianza que usó al crear la relación de confianza en su dominio autogestionado. Especifique la dirección. En este caso, elegimos Bidireccional.
6. En el campo Reenviador condicional, ingrese la dirección IP del servidor DNS autogestionado. En este ejemplo, escriba 172.16.10.153.
7. (Opcional) Elija Agregar otra dirección IP y escriba una segunda dirección IP para el servidor DNS autogestionado. Puede especificar hasta un total de cuatro servidores DNS.
8. Seleccione Añadir.

Enhorabuena. Ahora tienes una relación de confianza entre tu dominio autogestionado (corp.example.com) y tu AWS Microsoft AD gestionado (AD.example.com). MyManaged Solo se puede configurar una relación entre estos dos dominios. Si, por ejemplo, desea cambiar la dirección

de confianza por una unidireccional, primero tendría que eliminar esta relación de confianza y crear una nueva.

Para obtener más información, incluidas instrucciones acerca de cómo verificar o eliminar relaciones de confianza, consulte Creación de una relación de confianza.

Tutorial: Creación de una relación de confianza entre dos dominios de AWS Managed Microsoft AD

En este tutorial, se explican todos los pasos necesarios para configurar una relación de confianza entre dos dominios de AWS Directory Service para Microsoft Active Directory.

Temas

Véase también

Creación de una relación de confianza

Paso 1: preparación de su AWS Managed Microsoft AD

En esta sección, preparará su Microsoft AD AWS administrado para la relación de confianza con otro Microsoft AD AWS administrado. Muchos de los pasos siguientes son casi idénticos a los que acaba de completar en Tutorial: Creación de una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio de Active Directory autogestionado. Sin embargo, esta vez está configurando sus entornos AWS gestionados de Microsoft AD para que funcionen entre sí.

Configuración de las subredes de VPC y los grupos de seguridad

Debe permitir el tráfico de una red de Microsoft AD AWS administrada a la VPC que contiene el otro AWS Microsoft AD administrado. Para ello, tendrá que asegurarse de que las ACL asociadas a las subredes utilizadas para implementar su AWS Microsoft AD administrado y las reglas de los grupos de seguridad configuradas en los controladores de dominio permiten el tráfico necesario para respaldar las confianzas.

Los requisitos de puertos varían en función de la versión de Windows Server que utilizan los controladores de dominio y de los servicios o las aplicaciones que van a utilizar la relación de confianza. Para este tutorial, tendrá que abrir los siguientes puertos:

Entrada

- TCP/UDP 53: DNS
- TCP/UDP 88: autenticación de Kerberos
- UDP 123: NTP
- TCP 135: RPC
- TCP/UDP 389: LDAP
- TCP/UDP 445: SMB

> **Note**
>
> SMBv1 ya no es compatible.

- TCP/UDP 464: autenticación Kerberos
- TCP 636: LDAPS (LDAP a través de TLS/SSL)
- TCP 3268-3269: catálogo global
- TCP/UDP 1024-65535: puertos efímeros de RPC

Salida

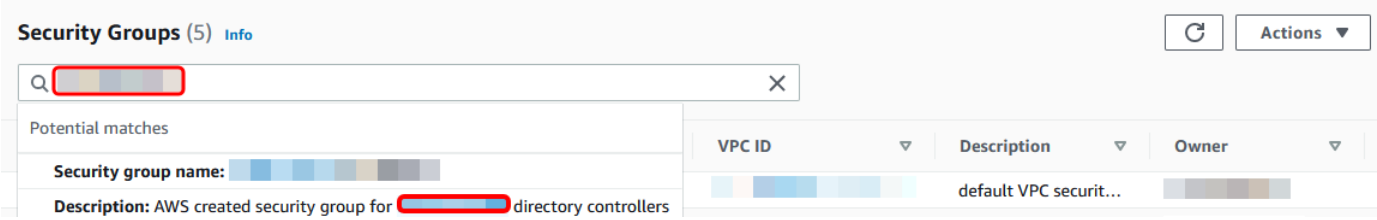
- ALL

> **Note**
>
> Estos son los puertos mínimos que se necesitan para poder conectar las VPC desde ambos AWS Managed Microsoft AD. La configuración específica podría requerir abrir puertos adicionales. Para obtener más información, consulte How to configure a firewall for Active Directory domains and trusts en el sitio web de Microsoft.

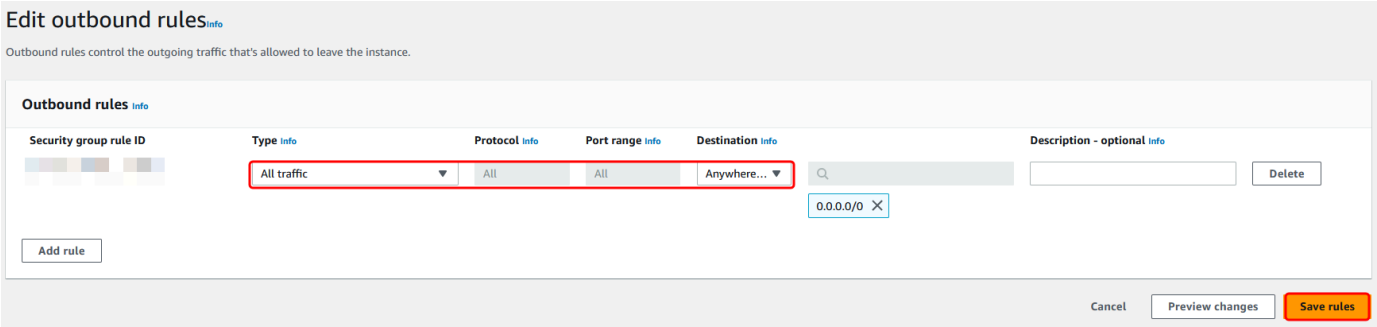
Para configurar las reglas de salida del controlador de dominio AWS administrado de Microsoft AD

> **Note**
>
> Repita los pasos del 1 al 6 que aparecen a continuación para cada directorio.

1. Vaya a la consola de AWS Directory Service. En la lista de directorios, anote el identificador de directorio de su directorio AWS administrado de Microsoft AD.
2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
3. En el panel de navegación, elija Security Groups (Grupos de seguridad).
4. Usa el cuadro de búsqueda para buscar tu ID de directorio de Microsoft AD AWS administrado. En los resultados de búsqueda, seleccione el elemento con la descripción **`AWS created security group for yourdirectoryID directory controllers`**.



5. Vaya a la pestaña Outbound Rules en ese grupo de seguridad. Elija Edit y después Add another rule. Para la nueva regla, escriba los siguientes valores:
   - Type (Tipo): ALL Traffic (Todo el tráfico)
   - Protocol (Protocolo): ALL (Todos)
   - Destination (Destino) determina el tráfico que puede salir de sus controladores de dominio y a dónde puede ir. Especifique una única dirección IP o un rango de direcciones IP en notación CIDR (por ejemplo, 203.0.113.5/32). También puede especificar el nombre o el ID de otro grupo de seguridad en la misma región. Para obtener más información, consulte Comprenda la configuración y el uso de los grupos de AWS seguridad de su directorio.
6. Seleccione Guardar.



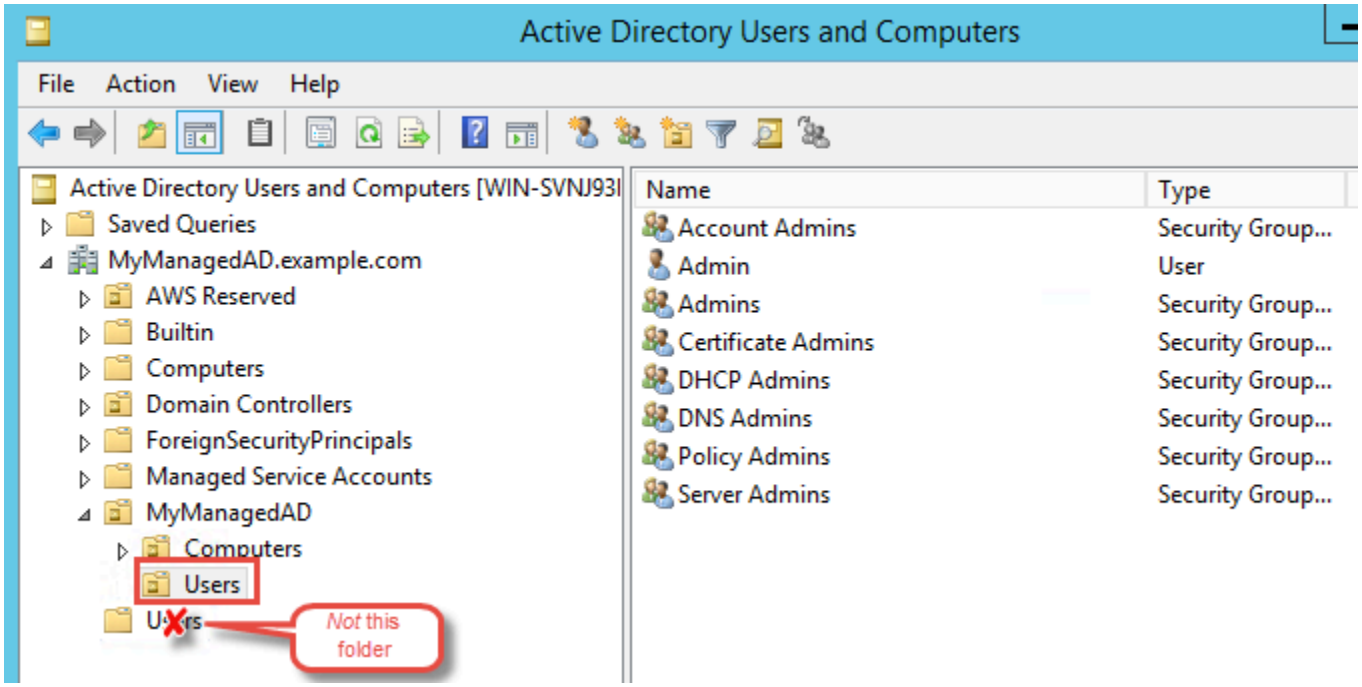
Asegúrese de que la autenticación previa de Kerberos esté habilitada

Ahora quiere confirmar que los usuarios de su Microsoft AD AWS administrado también tienen habilitada la autenticación previa de Kerberos. Este es el mismo proceso que ha completado para

su directorio local. Esta es la configuración predeterminada, pero vamos a comprobar que no haya cambiado nada.

Visualización de la configuración de Kerberos del usuario

1. Inicie sesión en una instancia que sea miembro de su directorio AWS administrado de Microsoft AD mediante el Permisos para la cuenta de administrador dominio o una cuenta a la que se le hayan delegado permisos para administrar los usuarios del dominio.
2. Si no están instaladas todavía, instale la herramienta Usuarios y equipos de Active Directory y la herramienta de DNS. Obtenga información sobre cómo instalar estas herramientas en Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado.
3. Abra el Administrador del servidor. En el menú Herramientas, elija Usuarios y equipos de Active Directory.
4. Seleccione la carpeta Usuarios en su dominio. Tenga en cuenta que esta es la carpeta Users (Usuarios) situada bajo el nombre de NetBIOS, no la carpeta Users (Usuarios) situada bajo el nombre de dominio completo (FQDN).



5. En la lista de usuarios, haga clic con el botón derecho en un usuario y seleccione Properties (Propiedades).
6. Elija la pestaña Cuenta. En la lista Opciones de cuenta, desplácese hacia abajo y asegúrese de que No pedir la autenticación Kerberos previa no esté activado.

Paso siguiente

Paso 2: crear la relación de confianza con otro dominio de AWS Managed Microsoft AD

Paso 2: crear la relación de confianza con otro dominio de AWS Managed Microsoft AD

Ahora que ha finalizado el trabajo de preparación, los pasos finales se centran en crear las relaciones de confianza entre los dos dominios de AWS Managed Microsoft AD. Si se presenta algún problema durante el proceso de creación de relaciones de confianza, consulte Motivos de los estados al crear relaciones de confianza para obtener ayuda.

Configuración de la relación de confianza en su primer dominio de AWS Managed Microsoft AD

En este tutorial, va a configurar una relación de confianza bidireccional. No obstante, si crea una relación de confianza entre bosques unidireccional, tenga en cuenta que la dirección de la relación de confianza de cada uno de los dominios debe ser complementaria. Por ejemplo, si crea una relación de confianza unidireccional saliente en su primer dominio, debe crear una relación de confianza entrante unidireccional en su dominio de AWS Managed Microsoft AD.

> **Note**
>
> AWS Managed Microsoft AD también admite relaciones de confianza externas. Sin embargo, para este tutorial, creará una relación de confianza bidireccional entre bosques.

Para configurar la relación de confianza en su primer dominio de AWS Managed Microsoft AD

1. Abra la consola de AWS Directory Service.
2. En la página Directorios, elija el primer ID de AWS Managed Microsoft AD.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Trust relationships (Relaciones de confianza), elija Actions (Acciones) y, a continuación, seleccione Add trust relationship (Añadir relación de confianza).

5. En la página Agregar una relación de confianza, escriba el FQDN del segundo dominio de AWS Managed Microsoft AD. Asegúrese de que podrá recordar esta contraseña, ya que la necesitará al configurar la relación de confianza para el segundo domino de AWS Managed Microsoft AD. Especifique la dirección. En este caso, elija Bidireccional.
6. En el campo Reenviador condicional, escriba la dirección IP del servidor DNS del segundo dominio de AWS Managed Microsoft AD.
7. (Opcional) Elija Agregar otra dirección IP y escriba una segunda dirección IP para el servidor DNS del segundo dominio de AWS Managed Microsoft AD. Puede especificar hasta un total de cuatro servidores DNS.
8. Elija Add (Agregar). La relación de confianza fallará en este punto, como es de esperar, hasta que creemos la otra parte de la relación de confianza.

Configuración de la relación de confianza en su segundo dominio de AWS Managed Microsoft AD

Ahora, configure la relación de confianza entre bosques con el segundo directorio de AWS Managed Microsoft AD. Como ha creado una relación de confianza bidireccional entre bosques en el primer dominio de AWS Managed Microsoft AD, también tiene que crear una relación de confianza bidireccional utilizando este domino de AWS Managed Microsoft AD.

Para configurar la relación de confianza en su segundo dominio de AWS Managed Microsoft AD

1. Vuelva a la consola de AWS Directory Service.
2. En la página Directorios, elija el ID del segundo dominio de AWS Managed Microsoft AD.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Trust relationships (Relaciones de confianza), elija Actions (Acciones) y, a continuación, seleccione Add trust relationship (Añadir relación de confianza).
5. En la página Agregar una relación de confianza, escriba el FQDN del primer dominio de AWS Managed Microsoft AD. Escriba la misma contraseña de confianza que usó al crear la relación de confianza en su dominio local. Especifique la dirección. En este caso, elija Bidireccional.

6. En el campo Reenviador condicional, escriba la dirección IP del servidor DNS del primer dominio de AWS Managed Microsoft AD.
7. (Opcional) Elija Agregar otra dirección IP y escriba una segunda dirección IP para el servidor DNS del primer dominio de AWS Managed Microsoft AD. Puede especificar hasta un total de cuatro servidores DNS.
8. Elija Add (Agregar). La relación de confianza debe verificarse poco después.
9. Ahora, vuelva a la relación de confianza que creó en el primer dominio y vuelve a verificar la relación de confianza.

Enhorabuena. Ahora tiene una relación de confianza entre sus dos dominios de AWS Managed Microsoft AD. Solo se puede configurar una relación entre estos dos dominios. Si, por ejemplo, desea cambiar la dirección de confianza por una unidireccional, primero tendría que eliminar esta relación de confianza y crear una nueva.

Conecta tu Microsoft AD AWS administrado a Microsoft Entra Connect Sync

En este tutorial, se explican los pasos necesarios para realizar la instalación Microsoft Entra Connect Syncy Microsoft Entra IDsincronizarla con su Microsoft AD AWS administrado.

En este tutorial, aprenderá a hacer lo siguiente:

1. Cree un usuario de dominio de Microsoft AD AWS administrado.
2. Descargue Entra Connect Sync.
3. Se utiliza Windows PowerShell para ejecutar un script con el fin de proporcionar los permisos adecuados al usuario recién creado.
4. Instale Entra Connect Sync.

Requisitos previos

Necesitará lo siguiente para completar este tutorial:

- Un Microsoft AD AWS gestionado. Para obtener más información, consulte the section called “Cree su Microsoft AD AWS administrado”.
- Una instancia de Amazon EC2 Windows Server unida a su AWS Microsoft AD administrado. Para obtener más información, consulte Únase sin problemas a una instancia de Windows.

- Un Windows servidor EC2 Active Directory Administration Tools instalado para administrar su Microsoft AD AWS administrado. Para obtener más información, consulte the section called “Instale las herramientas de administración de AD para Microsoft AD AWS administrado”.

Paso 1: Crear un usuario de Active Directory dominio

En este tutorial se da por sentado que ya tiene Active Directory Administration Tools instalada una instancia de Microsoft AD AWS gestionada y una instancia de EC2 Windows Server. Para obtener más información, consulte the section called “Instale las herramientas de administración de AD para Microsoft AD AWS administrado”.

1. Conéctese a la instancia en la que Active Directory Administration Tools se instalaron.
2. Cree un usuario de dominio de Microsoft AD AWS administrado. Este usuario se convertirá en Active Directory Directory Service (AD DS) Connector account el formularioEntra Connect Sync. Para ver los pasos detallados de este proceso, consultethe section called “Creación de un usuario”.

Paso 2: Descargar Entra Connect Sync

- Descargue Entra Connect Sync desde el Microsoftsitio web a la instancia EC2 que es el administrador de AWS Managed Microsoft AD.

> **Warning**
>
> No la abra ni ejecute Entra Connect Sync en este momento. Los siguientes pasos proporcionarán los permisos necesarios para el usuario de dominio creado en el paso 1.

Paso 3: Ejecute el Windows PowerShell script

- PowerShellÁbralo como administrador y ejecute el siguiente script. Mientras se ejecuta el script, se le pedirá que introduzca el SaM del AccountName usuario de dominio recién creado en el paso 1.

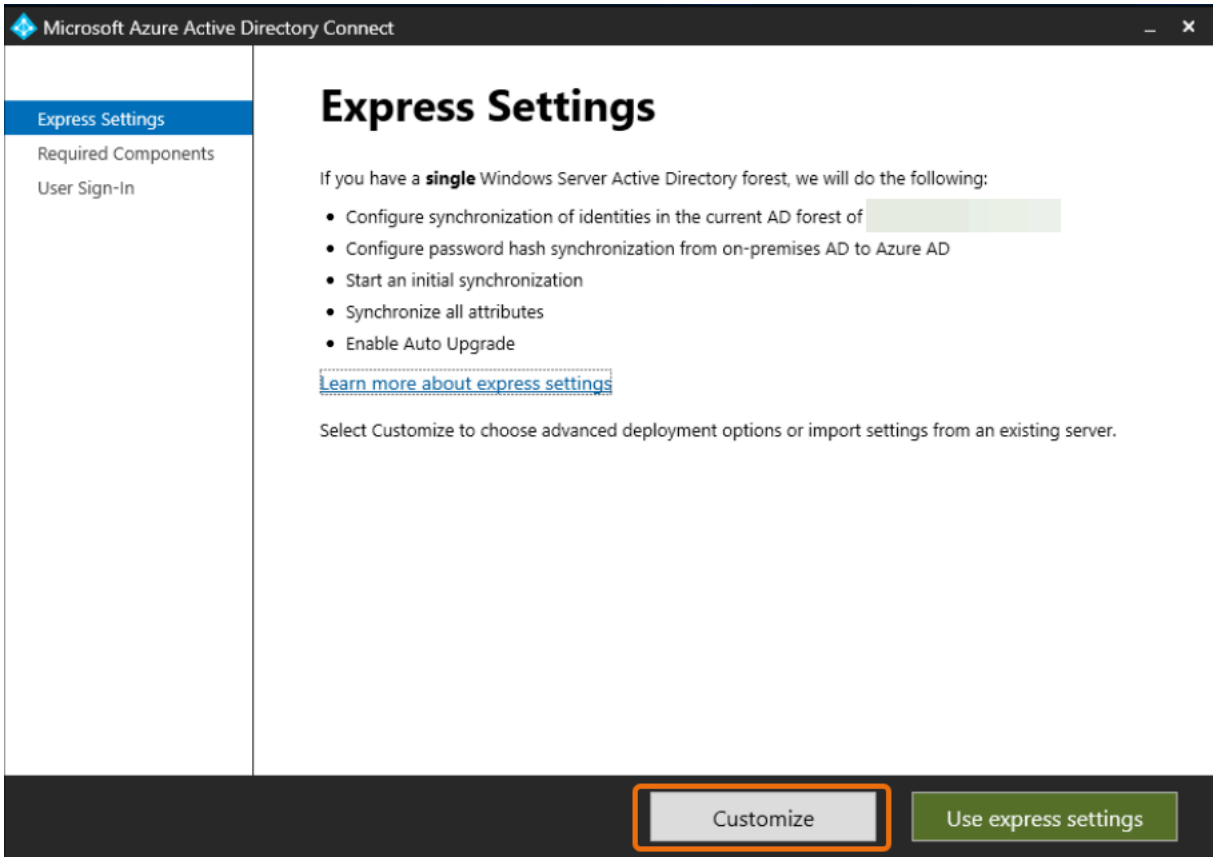
```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"
```

```
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 $_"
    }
```

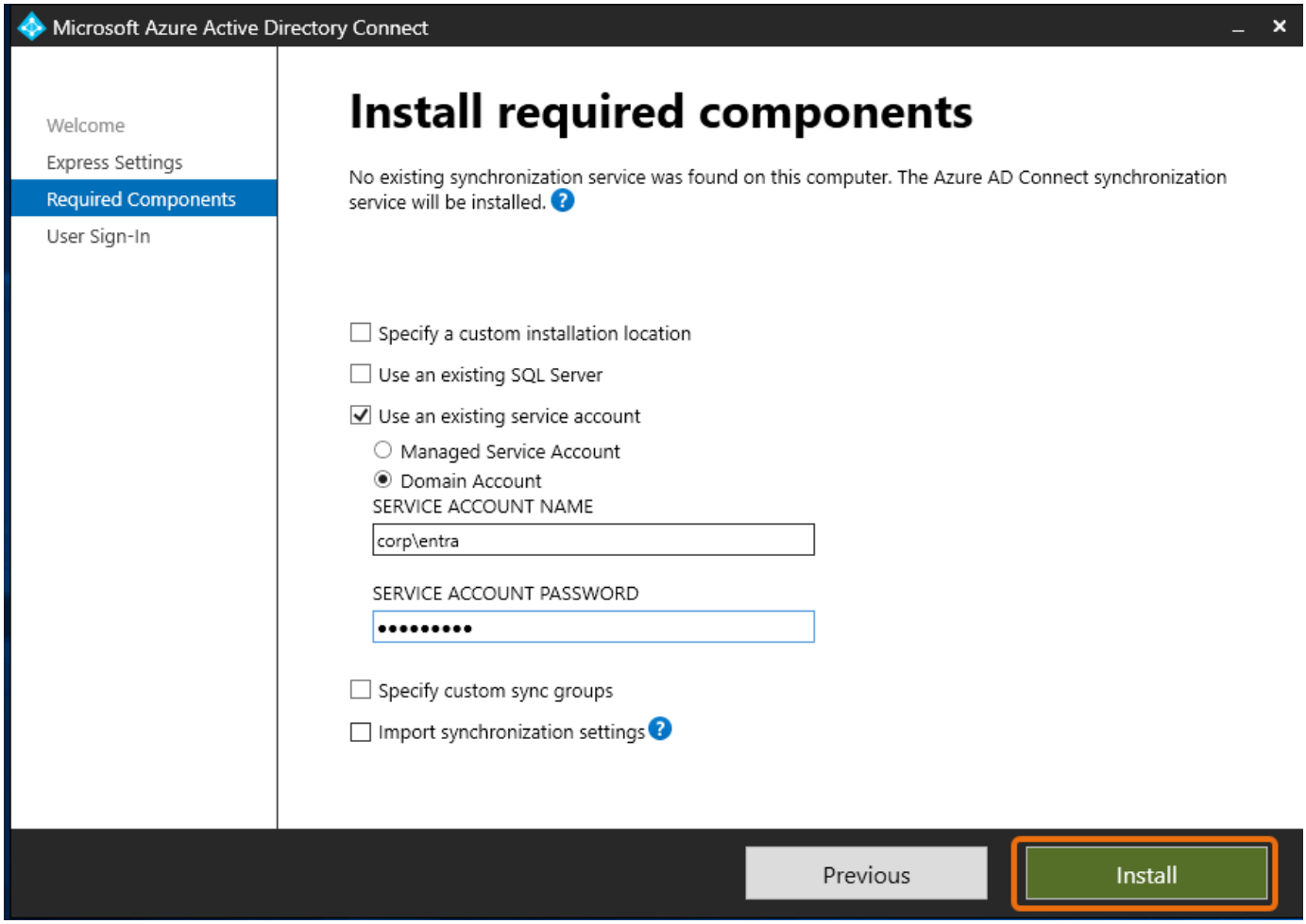
```
    Foreach ($OU in $OUs) {
        try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
 $ADConnectorAccountDN -ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        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 : $_"
    }
    }
}
```

Paso 4: Instalar Entra Connect Sync

1. Una vez que se haya completado el script, puede ejecutar el archivo de configuración descargado Microsoft Entra Connect (antes conocido comoAzure Active Directory Connect).
2. Tras ejecutar el archivo de configuración del paso anterior, se abre una Microsoft Azure Active Directory Connect ventana. En la ventana Configuración rápida, seleccione Personalizar.



3. En la ventana Instalar los componentes necesarios, active la casilla Usar una cuenta de servicio existente. En NOMBRE DE LA CUENTA DE SERVICIO y CONTRASEÑA DE LA CUENTA DE SERVICIO, introduzca el AD DS Connector account nombre y la contraseña del usuario que creó en el paso 1. Por ejemplo, si su AD DS Connector account nombre es`entra`, el nombre de la cuenta sería`corp\entra`. A continuación, selecciona Instalar.



4. En la ventana de inicio de sesión del usuario, seleccione una de las siguientes opciones:

   a. Autenticación transferida: esta opción le permite iniciar sesión en su cuenta Active Directory con su nombre de usuario y contraseña.

   b. No configurar: esto le permite utilizar el inicio de sesión federado con Microsoft Entra (antes conocido como Azure Active Directory (AzureAD)) o. Office 365

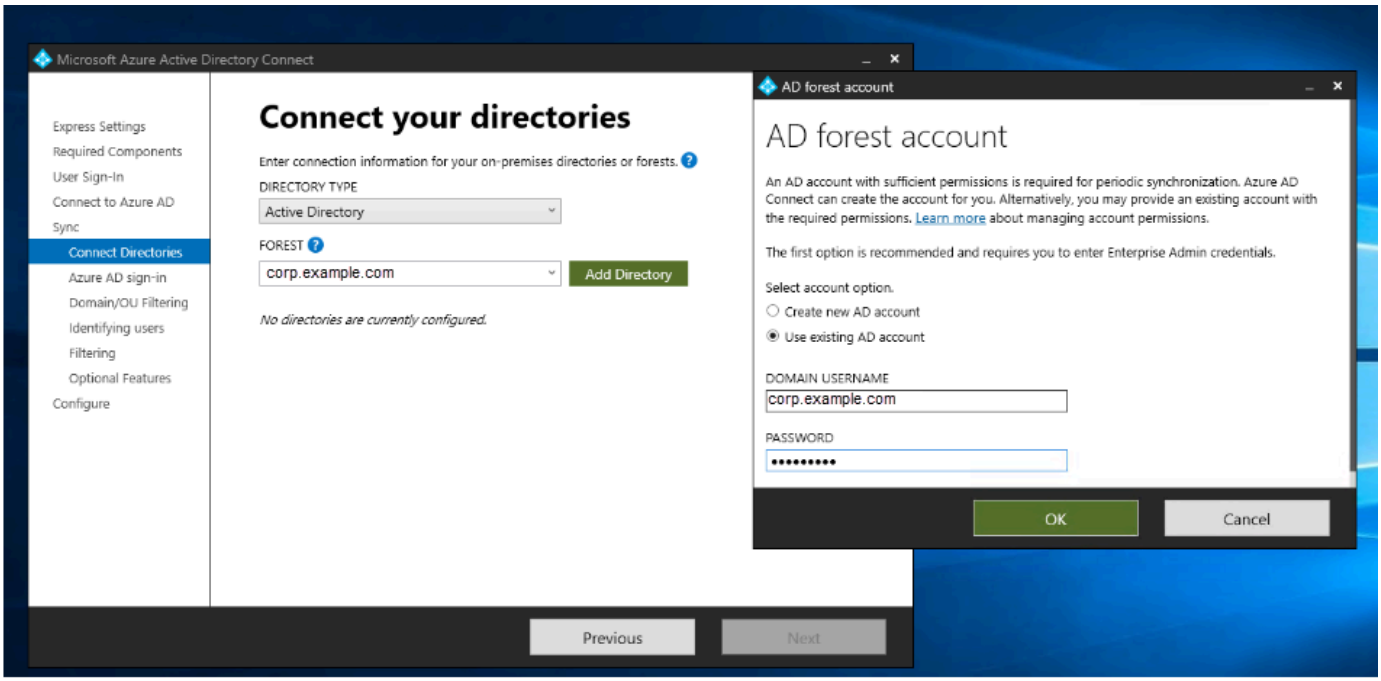
   A continuación, seleccione Siguiente.

5. En la Azure ventana Conectar a, introduzca su nombre de usuario y contraseña de administrador global Entra ID y seleccione Siguiente.

6. En la ventana Conecta tus directorios, selecciona TIPO Active DirectoryDE DIRECTORIO. Elija el bosque para su Microsoft AD for FOREST AWS administrado. A continuación, seleccione Agregar directorio.

7. Aparece un cuadro emergente en el que se solicitan las opciones de su cuenta. Selecciona Usar una cuenta de AD existente. Introduce el AD DS Connector account nombre de usuario

y la contraseña creados en el paso 1 y, a continuación, selecciona Aceptar. A continuación, seleccione Siguiente.



8. En la ventana de Azure ADinicio de sesión, selecciona Continuar sin hacer coincidir todos los sufijos UPN con los dominios verificados, solo si no has añadido un dominio personalizado verificado. Entra ID A continuación, seleccione Siguiente.
9. En la ventana de filtrado de dominios o unidades organizativas, selecciona las opciones que mejor se adapten a tus necesidades. Para obtener más información, consulte Entra Connect Sync: Configurar el filtrado en Microsoft la documentación. A continuación, seleccione Siguiente.
10. En la ventana Identificación de usuarios, filtrado y funciones opcionales, mantenga los valores predeterminados y seleccione Siguiente.
11. En la ventana Configurar, revise los ajustes de configuración y seleccione Configurar. La instalación Entra Connect Sync finalizará y los usuarios comenzarán a sincronizarse con. Microsoft Entra ID

Ampliar el esquema

AWS Managed Microsoft AD utiliza esquemas para organizar y forzar el modo de almacenamiento de los datos del directorio. El proceso para añadir definiciones al esquema se denomina "ampliar el esquema". Las ampliaciones de los esquemas le permiten modificar el esquema de su directorio de AWS Managed Microsoft AD mediante un archivo LDAP Data Interchange Format (LDIF) válido. Para

obtener más información acerca de los esquemas de AD y cómo ampliar su esquema, consulte los temas que se indican a continuación.

Temas

- Cuándo debería ampliar su esquema de AWS Managed Microsoft AD
- Tutorial: Ampliación del esquema de Microsoft AD AWS administrado

Cuándo debería ampliar su esquema de AWS Managed Microsoft AD

Para ampliar el esquema de AWS Managed Microsoft AD, puede agregar más clases de objetos y atributos. Podría hacerlo, por ejemplo, si tuviera una aplicación que requiriera cambios en el esquema para permitir el inicio de sesión único.

También puede utilizar las extensiones de esquema para habilitar aplicaciones que dependen de clases de objetos y atributos específicos de Active Directory. Esto puede ser especialmente útil si tiene que migrar aplicaciones de empresa que dependen de AWS Managed Microsoft AD a la nube de AWS.

Cada atributo o clase que se añada a un esquema de Active Directory debe estar definido por un identificador único. De esta forma, cuando las empresas añadan extensiones al esquema, tendrán la certeza de que son únicas y no entran en conflicto con otras. Estos identificadores reciben el nombre de identificadores de objetos (OID) y se almacenan en AWS Managed Microsoft AD.

Para empezar, consulte Tutorial: Ampliación del esquema de Microsoft AD AWS administrado.

Temas relacionados

- Ampliar el esquema
- Elementos del esquema

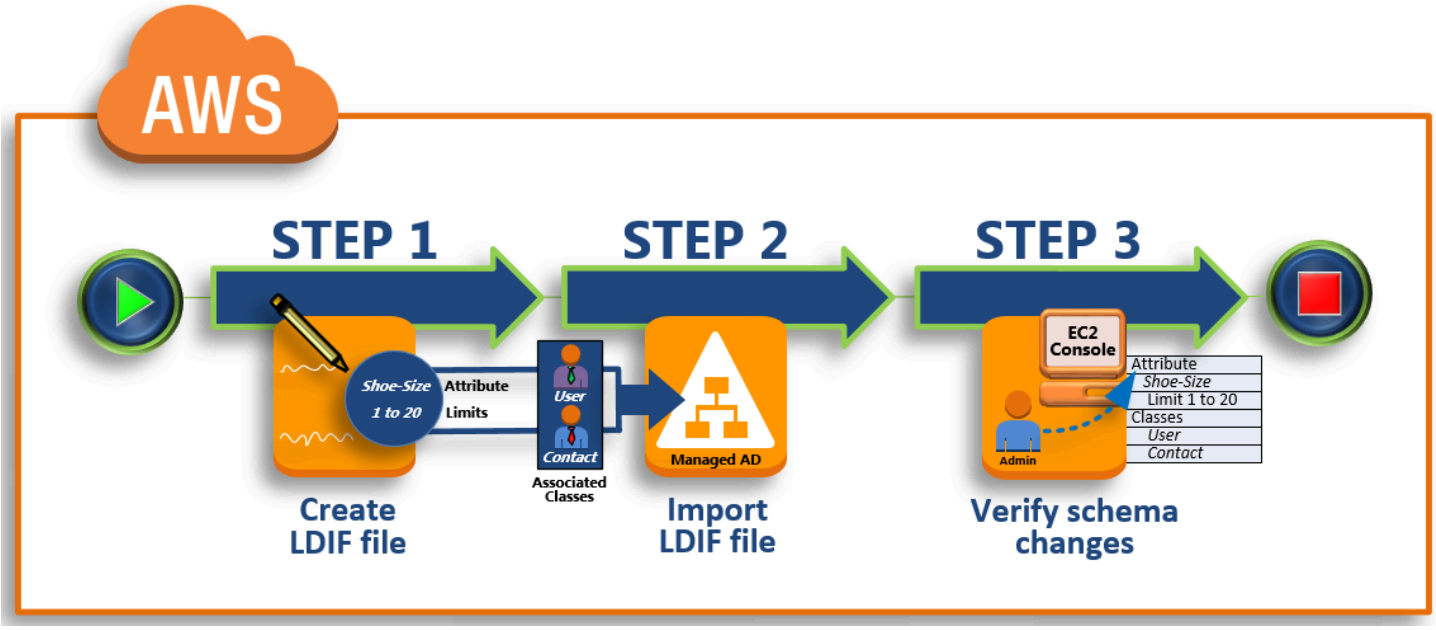
Tutorial: Ampliación del esquema de Microsoft AD AWS administrado

En este tutorial, aprenderá a ampliar el esquema de su AWS directorio de Directory Service for Microsoft Active Directory, también conocido como Microsoft AD AWS administrado, agregando atributos y clases únicos que cumplan con sus requisitos específicos. AWS Las extensiones de esquema de Microsoft AD administradas solo se pueden cargar y aplicar mediante un archivo de script LDIF (Lightweight Directory Interchange Format) válido.

Los atributos (attributeSchema) definen los campos de la base de datos, mientras que las clases (classSchema) definen las tablas de la base de datos. Por ejemplo, todos los objetos de usuario de Active Directory se definen mediante la clase de esquema User, mientras que las propiedades individuales de un usuario, como, por ejemplo, su dirección de correo electrónico o un número de teléfono, se definen mediante un atributo.

Si desea añadir una propiedad nueva, como Shoe-Size, deberá definir un nuevo atributo, de tipo integer. También puede definir límites inferior y superior, como de 1 a 20. Una vez creado el objeto attributeSchema Shoe-Size (talla de zapato), a continuación, tendrá que modificar el objeto classSchema User de modo que contenga dicho atributo. los atributos Se pueden enlazar con varias clases. También podría añadir Shoe-Size a la clase Contacto, por ejemplo. Para obtener más información acerca de los esquemas de Active Directory, consulte Cuándo debería ampliar su esquema de AWS Managed Microsoft AD.

Este flujo de trabajo incluye tres pasos básicos.



Paso 1: creación del archivo LDIF

En primer lugar, se crea un archivo LDIF y se definen los nuevos atributos y cualquier clase a la que los atributos deban añadirse. Puede utilizar este archivo para la siguiente fase del flujo de trabajo.

Paso 2: importación del archivo LDIF

En este paso, utilizará la AWS Directory Service consola para importar el archivo LDIF a su entorno de Microsoft Active Directory.

Paso 3: comprobación de si la ampliación del esquema ha funcionado

Por último, como administrador, utilizará una instancia EC2 para comprobar si las nuevas extensiones aparecen en el complemento de esquemas de Active Directory.

Paso 1: creación del archivo LDIF

Los archivos LDIF son archivos estándar con formato de intercambio de datos sencillo que representan contenido de directorios LDAP (protocolo ligero de acceso a directorios) y solicitudes de actualización. LDIF transmite el contenido de directorio como un conjunto de registros, un registro por cada objeto (o entrada). También representa las solicitudes de actualización, como adición, modificación, eliminación y cambio de nombre, como un conjunto de registros, un registro por cada solicitud de actualización.

AWS Directory Service Importa el archivo LDIF con los cambios de esquema ejecutando la `ldifde.exe` aplicación en el directorio administrado de AWS Microsoft AD. Por lo tanto, le resultará útil para comprender la sintaxis del script LDIF. Para obtener más información, consulte LDIF Scripts.

Hay varias herramientas LDIF de terceros para extraer, limpiar y actualizar las actualizaciones de los esquemas. Independientemente de la herramienta que utilice, es importante comprender que todos los identificadores utilizados en su archivo LDIF deben ser únicos.

Se recomienda encarecidamente leer los siguientes conceptos y consejos antes de crear el archivo LDIF.

- Elementos de los esquemas: lea información sobre los elementos de los esquemas, como, por ejemplo, atributos, clases, ID de objetos y atributos vinculados. Para obtener más información, consulte Elementos del esquema.

- Secuencia de los elementos: asegúrese de que el orden en que se disponen los elementos dentro del archivo LDIF siga el diseño de árbol de información de directorios (DIT) de arriba abajo. Estas son las normas generales de orden de secuencia en los archivos LDIF:

  - Separar los elementos con una línea en blanco.
  - Enumerar los elementos secundarios después de sus primarios.
  - Asegurarse de que existan en el esquema elementos como atributos o clases de objetos. En caso de no estar presentes, deberá añadirlos al esquema para poder usarlos. Por ejemplo, para poder asignar un atributo a una clase, debe crearse el atributo.

- Formato del nombre distintivo: para cada nueva instrucción dentro del archivo LDIF, defina el nombre distintivo (DN) como la primera línea de la instrucción. El DN identifica un objeto de Active Directory dentro del árbol del objeto de Active Directory, y debe contener los componentes de dominio de su directorio. Por ejemplo, los componentes de dominio del directorio en este tutorial son `DC=example,DC=com`.

  El DN también debe contener el nombre común (CN) del objeto de Active Directory. La primera entrada CN es el nombre de clase o el atributo. A continuación, debe utilizar `CN=Schema,CN=Configuration`. Este CN le garantiza que puede ampliar el esquema de Active Directory. Como ya se mencionó antes, no se puede añadir ni modificar el contenido de los objetos de Active Directory. Este es el formato general de un DN.

  ```
  dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
  ```

  En este tutorial, el DN del nuevo atributo Shoe-Size sería así:

  ```
  dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
  ```

- Advertencias: lea las siguientes advertencias antes de ampliar su esquema.
  - Antes de ampliar el esquema de Active Directory, es importante leer las advertencias que hace Microsoft sobre las repercusiones de esta operación. Para obtener más información, consulte What You Must Know Before Extending the Schema.
  - No se pueden eliminar las clases o los atributos de esquema. Por lo tanto, si comete un error y no desea restaurar a partir de una copia de seguridad, solo podrá deshabilitar el objeto. Para obtener más información, consulte Disabling Existing Classes and Attributes.
  - No defaultSecurityDescriptor se admiten cambios en.

Para obtener más información sobre cómo se crean los archivos LDIF y ver un ejemplo de archivo LDIF que se puede usar para probar las extensiones de esquema de AWS Microsoft AD administradas, consulte el artículo Cómo extender su esquema de directorio administrado de AWS Microsoft AD en el blog de seguridad. AWS

Paso siguiente

Paso 2: importación del archivo LDIF

Paso 2: importación del archivo LDIF

Puede ampliar el esquema importando un archivo LDIF desde la AWS Directory Service consola o mediante la API. Para obtener más información acerca de cómo hacerlo con las API de ampliación del esquema, consulte la Referencia de la API de AWS Directory Service . En este momento, AWS no permite utilizar aplicaciones externas, como Microsoft Exchange, para actualizar esquemas directamente.

> **Important**
>
> Al actualizar el esquema de directorios AWS gestionados de Microsoft AD, la operación no es reversible. En otras palabras, cuando crea una clase nueva o un atributo nuevo, Active Directory no le permite eliminarlo. No obstante, sí puede deshabilitarlo.
> Si debe eliminar los cambios aplicados en un esquema, una opción es restaurar el directorio a partir de una instantánea anterior. Restaurar una instantánea devuelve tanto el esquema como los datos del directorio a un punto anterior, no solo el esquema. Tenga en cuenta que la antigüedad máxima admitida de una instantánea es de 180 días. Para obtener más información, consulte Tiempo de conservación de una copia de seguridad de estado del sistema de Active Directory en el sitio web de Microsoft.

Antes de que comience el proceso de actualización, AWS Managed Microsoft AD toma una instantánea para conservar el estado actual del directorio.

> **Note**
>
> Las extensiones de esquema son una función global de AWS Managed Microsoft AD. Si está utilizando Replicación multirregional, se deben seguir estos procedimientos en Región principal . Los cambios se aplicarán automáticamente en todas las regiones replicadas. Para obtener más información, consulte Características globales frente a las regionales.

Importación del archivo LDIF

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:

- Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Mantenimiento. Para obtener más información, consulte Regiones principales frente a las adicionales.
- Si no aparece ninguna región en la sección Replicación multirregional, elija la pestaña Mantenimiento.

4. En la sección Schema extensions (Ampliaciones del esquema), elija Actions (Acciones) y, a continuación, seleccione Upload and update schema (Cargar y actualizar el esquema).
5. En el cuadro de diálogo, haga clic en Browse, seleccione un archivo LDIF válido, escriba una descripción y, a continuación, elija Update Schema.

> **Important**
>
> Ampliar el esquema es una operación fundamental. No actualice ningún esquema en el entorno de producción sin antes probar la actualización con su aplicación en un entorno de desarrollo o de prueba.

Aplicación del archivo LDIF

Una vez cargado el archivo LDIF, Managed AWS Microsoft AD toma medidas para proteger el directorio contra errores, ya que aplica los cambios en el siguiente orden.

1. Se valida el archivo LDIF. Como los scripts de LDIF pueden manipular cualquier objeto del dominio, Managed AWS Microsoft AD realiza comprobaciones inmediatamente después de la carga para garantizar que la operación de importación no falle. Estas comprobaciones sirven para garantizar lo siguiente:
   - Que los objetos que se van a actualizar solo estén en el contenedor de esquemas.
   - Que la parte de DC (controladores de dominio) coincida con el nombre del dominio en el que se esté ejecutando el script LDIF.
2. Se toma una instantánea del directorio. Puede utilizar esta instantánea para restaurar su directorio en caso de tener algún problema con la aplicación después de actualizar el esquema.
3. Aplica los cambios a un único DC. AWS El Microsoft AD administrado aísla uno de sus DC y aplica las actualizaciones del archivo LDIF al DC aislado. A continuación, selecciona uno de sus DC como esquema principal, lo elimina de la replicación de directorios y aplica el archivo LDIF mediante. `Ldifde.exe`

4. La replicación se produce en todos los DC. AWS Microsoft AD administrado vuelve a agregar el DC aislado a la replicación para completar la actualización. Mientras sucede todo esto, el directorio sigue suministrando sin interrupción el servicio de Active Directory a sus aplicaciones.

Paso siguiente

Paso 3: comprobación de si la ampliación del esquema ha funcionado

Paso 3: comprobación de si la ampliación del esquema ha funcionado

Tras terminar el proceso de importación, es importante comprobar si se aplicaron las actualizaciones de esquema al directorio. Esto es especialmente clave antes de migrar o actualizar cualquier aplicación que se base en la actualización del esquema. Puede hacerlo usando varias herramientas LDAP diferentes o escribiendo una herramienta de pruebas que ejecute los comandos LDAP adecuados.

Este procedimiento utiliza el complemento del esquema de Active Directory o PowerShell para comprobar que se han aplicado las actualizaciones del esquema. Debe ejecutar estas herramientas desde un equipo que sea un dominio unido a su Microsoft AD AWS administrado. Puede ser un servidor de Windows que se ejecute en la red local con acceso a la nube virtual privada (VPC) o a través de una conexión de red privada virtual (VPN). También puede ejecutar estas herramientas en una instancia de Amazon EC2 de Windows (consulte Cómo lanzar una nueva instancia de EC2 con la unión de dominios fluida).

Verificación con el complemento de esquema de Active Directory

1. Instale el complemento Active Directory Schema siguiendo las instrucciones del TechNetsitio web.
2. Abra Microsoft Management Console (MMC) y amplíe el árbol AD Schema correspondiente a su directorio.
3. Recorra las carpetas Classes y Attributes hasta encontrar los cambios de esquema que efectuó antes.

Para verificar mediante PowerShell

1. Abre una PowerShell ventana.
2. Utilice el cmdlet `Get-ADObject` tal y como se muestra a continuación para verificar el cambio del esquema. Por ejemplo:

```
get-adobject -Identity 'CN=Shoe-
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

Paso opcional

Añadir un valor al nuevo atributo: opcional

Añadir un valor al nuevo atributo: opcional

Utilice este paso opcional cuando haya creado un atributo nuevo y desee añadir un nuevo valor al atributo en el directorio de Microsoft AD AWS administrado.

Adición de un valor a un atributo

1. Abre la utilidad de línea de Windows PowerShell comandos y establece el nuevo atributo con el siguiente comando. En este ejemplo, añadiremos un nuevo valor EC2InstanceID al atributo para un equipo específico.

   ```
   PS C:\> set-adcomputer -Identity computer name -add @{example-
   EC2InstanceID = 'EC2 instance ID'}
   ```

2. Puede validar que se haya agregado el valor EC2InstanceID al objeto del equipo ejecutando el siguiente comando:

   ```
   PS C:\> get-adcomputer -Identity computer name –Property example-
   EC2InstanceID
   ```

Recursos relacionados

En el sitio web de Microsoft encontrará los siguientes enlaces a recursos, con información relacionada.

- Extending the Schema (Windows)
- Active Directory Schema (Windows)
- Active Directory Schema
- Administración de Windows: Ampliación del esquema de Active Directory
- Restrictions on Schema Extension (Windows)
- Ldifde

Mantenga su directorio AWS administrado de Microsoft AD

En esta sección se describe cómo mantener las tareas administrativas comunes para su entorno Microsoft AD AWS administrado.

Temas

Adición de sufijos UPN alternativos

Puede simplificar la administración de los nombres de inicio de sesión de Active Directory (AD) y mejorar la experiencia de inicio de sesión de los usuarios mediante la adición de sufijos de nombre principal de usuario (UPN) alternativos a su directorio de AWS Managed Microsoft AD. Para ello, debe haber iniciado sesión en la cuenta de administrador o en una cuenta que pertenezca al grupo Administradores delegados para sufijos de nombre principal de usuario de AWS. Para obtener más información sobre este grupo, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD.

Para añadir sufijos UPN alternativos

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Localice una instancia de Amazon EC2 que se haya unido a su directorio de AWS Managed Microsoft AD. Seleccione la instancia y, a continuación, elija Connect (Conectar).
3. En la ventana Administrador del servidor, elija Herramientas. A continuación, elija Dominios y confianzas de Active Directory.
4. En el panel izquierdo, haga clic con el botón derecho en Dominios y confianza de Active Directory y, a continuación, elija Propiedades.
5. En la pestaña Sufijos UPN, escriba un sufijo UPN alternativo (como, por ejemplo, **`sales.example.com`**). Elija Agregar y, a continuación, elija Aplicar.

6. Si necesita añadir sufijos UPN alternativos adicionales, repita el paso 5 hasta que tenga los sufijos UPN que necesite.

Elimine su Microsoft AD AWS administrado

Cuando se elimina un Microsoft AD AWS administrado, se eliminan todos los datos del directorio y las instantáneas y no se pueden recuperar. Una vez que se elimina el directorio, todas las instancias que están unidas a él permanecen intactas. No se puede, sin embargo, utilizar las credenciales del directorio para iniciar sesión en estas instancias. Es necesario iniciar sesión en estas instancias con una cuenta de usuario que sea local para la instancia.

Eliminación de un directorio

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios. Asegúrese de estar en el Región de AWS lugar donde Active Directory está desplegado el suyo. Para obtener más información, consulte Elegir una región.
2. Asegúrese de que no haya ninguna AWS aplicación habilitada en el directorio que desea eliminar. AWS Las aplicaciones habilitadas le impedirán eliminar su Microsoft AD AWS administrado o su AD Simple.
   a. En la página Directories (Directorios), elija el ID del directorio.
   b. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones). En la sección de AWS aplicaciones y servicios, verá qué AWS aplicaciones están habilitadas para su directorio.
      - Deshabilita AWS Management Console el acceso. Para obtener más información, consulte Deshabilitación del acceso a la AWS Management Console.
      - Para deshabilitar Amazon WorkSpaces, debes anular el registro del servicio en el directorio de la consola. WorkSpaces Para obtener más información, consulta Cómo anular el registro de un directorio en la Guía de WorkSpaces administración de Amazon.
      - Para deshabilitar Amazon WorkDocs, debes eliminar el WorkDocs sitio de Amazon en la WorkDocs consola de Amazon. Para obtener más información, consulta Eliminar un sitio en la Guía de WorkDocs administración de Amazon.
      - Para deshabilitar Amazon WorkMail, debes eliminar la WorkMail organización de Amazon en la WorkMail consola de Amazon. Para obtener más información, consulta Eliminar una organización en la Guía del WorkMail administrador de Amazon.

- Para deshabilitar Amazon FSx para Windows File Server, debe eliminar el sistema de archivos de Amazon FSx del dominio. Para obtener más información, consulte Cómo trabajar con Active Directory fSx for Windows File Server en la Guía del usuario de Amazon FSx for Windows File Server.
- Para deshabilitar Amazon Relational Database Service, debe eliminar la instancia de Amazon RDS del dominio. Para obtener más información, consulte Administración de una instancia de base de datos en un dominio en la Guía del usuario de Amazon RDS.
- Para deshabilitar el AWS Client VPN servicio, debe eliminar el servicio de directorio del punto final Client VPN. Para obtener más información, consulte Active DirectoryAutenticación en la Guía AWS Client VPN del administrador.
- Para deshabilitar Amazon Connect, debe eliminar la instancia de Amazon Connect. Para obtener más información, consulte Eliminación de una instancia de Amazon Connect en la Guía de administración de Amazon Connect.
- Para deshabilitar Amazon QuickSight, debes darte de baja de Amazon QuickSight. Para obtener más información, consulta Cómo cerrar tu Amazon QuickSight cuenta en la Guía del QuickSight usuario de Amazon.

> **Note**
>
> Si lo está utilizando AWS IAM Identity Center y ya lo ha conectado anteriormente al directorio AWS administrado de Microsoft AD que planea eliminar, primero debe cambiar la fuente de identidad antes de poder eliminarlo. Para obtener más información, consulte Cambio del origen de identidad en la Guía del usuario de IAM Identity Center.

3. En el panel de navegación, elija Directories (Directorios).
4. Seleccione únicamente el directorio que se va a eliminar y haga clic en Eliminar. La eliminación del directorio tarda varios minutos. Cuando el directorio se haya eliminado, se eliminará de la lista de directorios.

Cambio del nombre del sitio de su directorio

Puede cambiar el nombre del sitio predeterminado de su directorio de AWS Managed Microsoft AD para que coincida con los nombres de sitio de Microsoft Active Directory (AD) existentes. De este modo, AWS Managed Microsoft AD podrá buscar y autenticar más rápidamente los usuarios de AD

existentes en su directorio en las instalaciones. El resultado es una mejor experiencia cuando los usuarios inician sesión en recursos de AWS como las instancias de Amazon EC2 y Amazon RDS para SQL Server que ha unido a su directorio de AWS Managed Microsoft AD.

Para ello, debe haber iniciado sesión en la cuenta Admin o en una cuenta que pertenezca al grupo AWS Delegated Sites and Services Administrators. Para obtener más información sobre este grupo, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD.

Para obtener beneficios adicionales al cambiar el nombre del sitio en relación con las relaciones de confianza, consulte Localizador de dominios en una relación de confianza de bosque en el sitio web de Microsoft.

Para cambiar el nombre del sitio de AWS Managed Microsoft AD

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Localice una instancia de Amazon EC2 que se haya unido a su directorio de AWS Managed Microsoft AD. Seleccione la instancia y, a continuación, elija Connect (Conectar).
3. En la ventana Administrador del servidor, elija Herramientas. A continuación, elija Sitios y servicios de Active Directory.
4. En el panel izquierdo, expanda la carpeta Sitios, haga clic con el botón derecho del ratón en el nombre del sitio (el nombre predeterminado es Default-Site-Name) y, a continuación, elija Cambiar nombre.
5. Escribe el nuevo nombre del sitio y pulse Intro.

Creación de una instantánea o restauración del directorio

AWS Directory Service proporciona instantáneas diarias automatizadas y la posibilidad de realizar instantáneas manuales de los datos para su Active Directory administrado de AWS Microsoft AD. Estas instantáneas se pueden usar para realizar una point-in-time restauración de su Active Directory. Está limitado a cinco instantáneas manuales por cada Active Directory AWS administrado de Microsoft AD. Si ya ha alcanzado este límite, para poder crear otra instantánea tendrá que eliminar una instantánea creada manualmente. No puede tomar instantáneas de directorios de Conector AD.

> **Note**
>
> La instantánea es una función global de AWS Managed Microsoft AD. Si está utilizando Replicación multirregional, se deben seguir estos procedimientos en Región principal . Los

cambios se aplicarán automáticamente en todas las regiones replicadas. Para obtener más información, consulte Características globales frente a las regionales.

Temas

Creación de una instantánea del directorio

Se puede usar una instantánea para restaurar el directorio al estado en el que se encontraba cuando se hizo la instantánea. Para crear una instantánea del directorio manualmente, siga estos pasos:

> **Note**
>
> Solo se pueden crear 5 instantáneas manualmente por directorio. Si ya ha alcanzado este límite, para poder crear otra instantánea tendrá que eliminar una instantánea creada manualmente.

Creación de una instantánea manual

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, seleccione la pestaña Mantenimiento.
4. En la sección Instantáneas, elija Acciones y, a continuación, seleccione Crear instantánea.
5. En el cuadro de diálogo Crear una instantánea del directorio, proporcione una descripción de la instantánea, si lo desea. Cuando esté todo listo, seleccione Crear.

En función del tamaño del directorio, puede que transcurran varios minutos hasta que se cree la instantánea. Cuando la instantánea esté lista, el valor Status cambia a `Completed`.

Restauración de un directorio a partir de una instantánea

Restaurar un directorio a partir de una instantánea equivale a hacer que el directorio retroceda en el tiempo. Las instantáneas del directorio son exclusivas del directorio desde el que se crearon. Una

instantánea solo se puede restaurar en el directorio a partir del cual se creó. Además, la antigüedad máxima admitida de una instantánea manual es de 180 días. Para obtener más información, consulte Tiempo de conservación de una copia de seguridad de estado del sistema de Active Directory en el sitio web de Microsoft.

> **Warning**
>
> Le recomendamos que contacte con el Centro de AWS Support antes de llevar a cabo cualquier restauración de una instantánea; tal vez podamos ayudarle a evitar la necesidad de restaurar instantáneas. Cualquier restauración a partir de una instantánea puede provocar la pérdida de datos, ya que las instantáneas reflejan el estado del directorio en un momento determinado. Es importante que entienda que los servidores DNS y controladores de dominio asociados al directorio funcionarán sin conexión hasta que finalice la restauración.

Para restaurar el directorio a partir de una instantánea, siga estos pasos:

Para restaurar un directorio a partir de una instantánea

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, seleccione la pestaña Mantenimiento.
4. En la sección Instantáneas, seleccione una instantánea de la lista, elija Acciones y, a continuación, seleccione Restaurar instantánea.
5. Lea la información del cuadro de diálogo Restaurar instantánea del directorio y elija Restaurar.

En el caso de un directorio AWS administrado de Microsoft AD, la restauración del directorio puede tardar de dos a tres horas. Cuando la restauración se haya llevado a cabo correctamente, el valor de Estado del directorio cambia a `Active`. Los cambios efectuados en el directorio después de la fecha de instantánea se sobrescriben.

Eliminación de una instantánea

Eliminación de una instantánea

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.

3. En la página Detalles del directorio, seleccione la pestaña Mantenimiento.
4. En la sección Instantáneas, elija Acciones y, a continuación, seleccione Eliminar instantánea.
5. Confirme que desea eliminar la instantánea y elija Eliminar.

Actualice su Microsoft AD AWS administrado

Puede actualizar su edición Standard Edition AWS Managed Microsoft AD Active Directory a la edición Enterprise poniéndose en contacto con AWS Support. Para obtener más información, consulte Creación de casos de soporte y administración de casos en la Guía AWS Support del usuario.

> **Note**
>
> La replicación multirregional solo está disponible en la edición AWS Managed Microsoft AD Enterprise para las siguientes regiones:
>
> - US East (Ohio)
> - Este de EE. UU. (Norte de Virginia)
> - Oeste de EE. UU. (Norte de California)
> - Oeste de EE. UU. (Oregón)
> - África (Ciudad del Cabo)
> - Asia-Pacífico (Hong Kong)
> - Asia-Pacífico (Mumbai)
> - Asia-Pacífico (Hyderabad)
> - Asia-Pacífico (Osaka)
> - Asia-Pacífico (Seúl)
> - Asia-Pacífico (Singapur)
> - Asia-Pacífico (Sídney)
> - Asia-Pacífico (Yakarta)
> - Asia-Pacífico (Melbourne)
> - Asia-Pacífico (Tokio)
> - Canadá (centro)
> - Oeste de Canadá (Calgary

- China (Pekín)
- China (Ningxia)
- Europa (Fráncfort)
- Europa (Zúrich)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- Europa (Milán)
- Europa (España)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)
- América del Sur (São Paulo)
- AWS GovCloud (EE. UU.-Oeste)
- AWS GovCloud (EE. UU.-Este)

Hay algunas limitaciones que debe tener en cuenta al actualizar su Microsoft AD AWS administrado. Son los siguientes:

- La actualización conllevará un coste adicional. Para obtener más información, consulte Precios de AWS Directory Service.
- Una vez que se actualice su Active Directory, no podrá volver a su edición anterior.
- Las instantáneas anteriores no se pueden usar para restaurar una Active Directory vez que se haya actualizado.
- Las actualizaciones se realizan en una fecha y hora programadas y acordadas AWS Support. Las mejoras se realizan de lunes a viernes, de 9:00 a 17:00, hora estándar del Pacífico.
- El proceso de actualización requiere de cuatro a cinco horas.
- Durante el proceso de actualización, los controladores de dominio de su Microsoft AD AWS administrado se actualizan de uno en uno. Esto puede afectar negativamente al rendimiento y provocar un tiempo de inactividad durante el período de mantenimiento.

- Si sus aplicaciones utilizan los nombres de host o las direcciones IP de los controladores de dominio en lugar del nombre de dominio de Active Directory, estas aplicaciones deberán actualizarse.
- Si utiliza LDAPS (Protocolo ligero de acceso a directorios sobre SSL), los controladores de dominio necesitarán certificados nuevos.

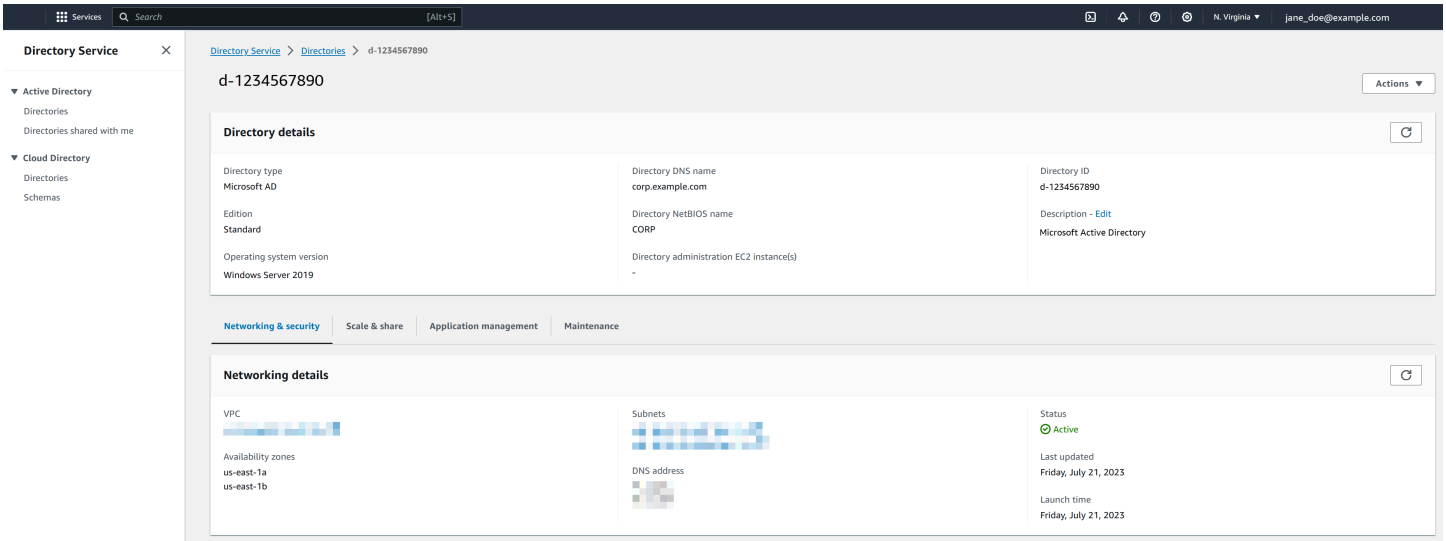
Ver información del directorio

Puede ver información detallada sobre un directorio.

Visualización de información detallada del directorio

1. En el panel de navegación de la AWS Directory Service consola, en Active Directory, selecciona Directorios.
2. Haga clic en el enlace del identificador de directorio correspondiente al directorio. La información acerca del directorio se muestra en la sección Detalles del directorio.

Para obtener más información acerca del campo Status, consulte Descripción del estado del directorio.



Otorgar acceso a los recursos de AWS a usuarios y grupos

AWS Directory Service ofrece la posibilidad de dar a los usuarios y grupos del directorio acceso a AWS servicios y recursos, como el acceso a la consola Amazon EC2. De forma similar a conceder a los usuarios de IAM acceso para gestionar directoriosPolíticas basadas en identidades (políticas

de IAM), tal como se describe en, para que los usuarios de su directorio tengan acceso a otros AWS recursos, como Amazon EC2, debe asignar funciones y políticas de IAM a esos usuarios y grupos. Para obtener más información, consulte Roles de IAM en la Guía del usuario de IAM.

Para obtener información sobre cómo conceder a los usuarios acceso al AWS Management Console, consulte. Habilitación del acceso a la AWS Management Console con credenciales de AD

Temas

Creación de un rol nuevo

Si necesita crear un nuevo rol de IAM para usarlo con él AWS Directory Service, debe crearlo mediante la consola de IAM. Una vez creado el rol, debe establecer una relación de confianza con ese rol antes de poder verlo en la AWS Directory Service consola. Para obtener más información, consulte Edición de la relación de confianza para una función existente.

> **Note**
>
> El usuario que haga esta tarea debe tener permiso para ejecutar las siguientes acciones de IAM. Para obtener más información, consulte Políticas basadas en identidades (políticas de IAM).
>
> - Nombre: PassRole
> - objetivo: GetRole
> - objetivo: CreateRole
> - objetivo: PutRolePolicy

Creación de un nuevo rol en la consola de IAM

1. En el panel de navegación de la consola de IAM, elija Roles. Para obtener más información, consulte Creación de un rol (AWS Management Console) en Guía del usuario de IAM.
2. Seleccione Crear rol.
3. En Choose the service that will use this role (Elija el servicio que utilizará este rol), seleccione Directory Service (Servicio de directorio) y Next (Siguiente).
4. Seleccione la casilla de verificación situada junto a la política (por ejemplo, AmazonEC2 FullAccess) que desee aplicar a los usuarios del directorio y, a continuación, seleccione Siguiente.
5. Si es necesario, añada una etiqueta al rol y, a continuación, seleccione Next (Siguiente).
6. Escriba un nombre en Role name (Nombre del rol) y una descripción opcional en Description (Descripción) y, a continuación, elija Create role (Crear rol).

Ejemplo: Creación de un rol para habilitar el acceso a la AWS Management Console

En la siguiente lista de comprobación, se ofrece un ejemplo de las tareas que debe llevar a cabo para crear un nuevo rol que otorgue a usuarios específicos del directorio acceso a la consola de Amazon EC2.

1. Cree un rol con la consola de IAM utilizando el procedimiento anterior. Cuando se le solicite una política, elija AmazonEC2. FullAccess
2. Utilice los pasos que se indican en Edición de la relación de confianza para una función existente para editar el rol que acaba de crear y, a continuación, añada la información de relación de confianza necesaria al documento de política. Este paso es necesario para que el rol esté visible inmediatamente después de habilitar el acceso al rol AWS Management Console en el siguiente paso.
3. Siga los pasos que se indican en Habilitación del acceso a la AWS Management Console con credenciales de AD para configurar el acceso general a la AWS Management Console.
4. Siga los pasos que se indican en Asignación de usuarios o grupos a una función existente para asignar el nuevo rol a los usuarios que necesitan acceso completo a los recursos de EC2.

Edición de la relación de confianza para una función existente

Puede asignar las funciones de IAM existentes a sus AWS Directory Service usuarios y grupos. Sin embargo, para ello, el rol debe tener una relación de confianza con AWS Directory Service. Al AWS

Directory Service crear un rol mediante el procedimiento indicado enCreación de un rol nuevo, esta relación de confianza se establece automáticamente. Solo tiene que establecer esta relación de confianza para las roles de IAM que no haya creado AWS Directory Service.

Para establecer una relación de confianza para un rol existente con AWS Directory Service

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, en Administración de accesos, elija Roles.

   La consola muestra los roles asociados a su cuenta.
3. Elija el nombre del rol que desea modificar y, una vez que esté en la página que corresponda al rol deseado, seleccione la pestaña Relaciones de confianza.
4. Elija Editar la política de confianza.
5. En Documento de política, pegue lo siguiente y, a continuación, seleccione Actualizar política de confianza.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

También puede actualizar este documento de política mediante AWS CLI. Para obtener más información, consulte update-trust en la Referencia de comandos de la AWS CLI .

Asignación de usuarios o grupos a una función existente

Puede asignar una función de IAM existente a un AWS Directory Service usuario o grupo. Para ello, asegúrese de haber completado lo siguiente.

Requisitos previos

- Cree un Microsoft AD AWS administrado.
- Cree un usuario o cree un grupo.
- Cree un rol con el que tenga una relación de confianza AWS Directory Service. Puede editar la relación de confianza de un rol existente.

> **Note**
>
> No se permite el acceso al directorio a los usuarios en grupos anidados. Los miembros del grupo principal tienen acceso a la consola, pero los miembros de los grupos secundarios no.

Para asignar usuarios o grupos a una función existente de IAM

1. En el panel de navegación de la consola de AWS Directory Service, en Active Directory, elija Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si no aparece ninguna región en la sección Replicación de varias regiones, seleccione la pestaña Administración de aplicaciones.
   - Si tiene varias regiones en la sección Replicación de varias regiones, seleccione la región en la que desee hacer las asignaciones, a continuación, elija la pestaña Administración de aplicaciones. Para obtener más información, consulte Regiones principales frente a las adicionales.
4. Desplázate hacia abajo hasta la AWS Management Consolesección, selecciona Acciones y Activar.
5. En la sección Acceso delegado a la consola, elija el nombre de la función de IAM para la función de IAM existente a la que desee asignar usuarios.
6. En la página Selected role (Rol seleccionado), en Manage users and groups for this role (Administrar usuarios y grupos para este rol), elija Add (Añadir).
7. En la página Agregar usuarios y grupos al rol, junto a Seleccionar bosque de Active Directory, elija el bosque de AWS Managed Microsoft AD (este bosque) o el bosque en las instalaciones (bosque de confianza), el que contenga la ubicación de las cuentas que necesitan obtener

acceso a la AWS Management Console. Para obtener más información sobre cómo configurar un bosque de confianza, consulte Tutorial: Creación de una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio de Active Directory autogestionado.

8. En Specify which users or groups to add (Especificar usuarios y grupos a añadir), seleccione Find by user (Buscar por usuario) o Find by group (Buscar por grupo) y, a continuación, escriba el nombre del usuario o grupo. En la lista de posibles coincidencias, elija el usuario o el grupo que desee añadir.
9. Seleccione Add para terminar de asignar usuarios y grupos al rol.

Visualización de los usuarios y los grupos asignados a una función

Para ver los usuarios y grupos asignados a una función, siga estos pasos.

Requisitos previos

- Asigne sus usuarios o grupos a un rol existente.

Visualización de los usuarios y grupos asignados a una función

1. En el panel de navegación de la consola de AWS Directory Service, en Active Directory, elija Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación de varias regiones, seleccione la región en la que desee ver las asignaciones, a continuación, elija la pestaña Administración de aplicaciones. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación de varias regiones, seleccione la pestaña Administración de aplicaciones.
4. En la sección Acceso delegado a la consola, elija el rol de IAM que desee ver.
5. En la página Rol seleccionado, en Administrar los usuarios y grupos para este rol, puede ver los usuarios y grupos asignados al rol.

Eliminación de un usuario o un grupo de un rol

Para eliminar un usuario o un grupo de una función, siga estos pasos.

Para eliminar un usuario o un grupo de una función

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación de varias regiones, seleccione la región en la que desee eliminar las asignaciones, a continuación, elija la pestaña Administración de aplicaciones. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación de varias regiones, seleccione la pestaña Administración de aplicaciones.
4. En la sección AWS Management Console, elija el rol que desea ver.
5. En la página Selected role (Rol seleccionado), en Manage users and groups for this role (Administrar usuarios y grupos para este rol), seleccione los usuarios o grupos de los que desea eliminar el rol y elija Remove (Eliminar). La función se elimina de los usuarios y los grupos especificados, pero no de su cuenta.

Uso de políticas administradas de AWS con AWS Directory Service

AWS Directory Service ofrece las siguientes políticas administradas de AWS para dar acceso a los usuarios y los grupos a servicios y recursos de AWS. Por ejemplo, acceso a la consola de Amazon EC2. Debe iniciar sesión en la AWS Management Console para poder ver estas políticas.

- Acceso de solo lectura
- Acceso de usuario avanzado
- Acceso completo a AWS Directory Service
- Acceso de solo lectura a AWS Directory Service
- Acceso completo a Amazon Cloud Directory
- Acceso de solo lectura a Amazon Cloud Directory
- Acceso completo a Amazon EC2

- Acceso de solo lectura a Amazon EC2
- Acceso completo a Amazon VPC
- Acceso de solo lectura a Amazon VPC
- Acceso completo a Amazon RDS
- Acceso de solo lectura a Amazon RDS
- Acceso completo a Amazon DynamoDB
- Acceso de solo lectura a Amazon DynamoDB
- Acceso completo a Amazon S3
- Acceso de solo lectura a Amazon S3
- Acceso completo a AWS CloudTrail
- Acceso de solo lectura a AWS CloudTrail
- Acceso completo a Amazon CloudWatch
- Acceso de solo lectura a Amazon CloudWatch
- Acceso completo a Registros de Amazon CloudWatch
- Acceso de solo lectura a Registros de Amazon CloudWatch

Para obtener más información acerca de cómo crear sus propias políticas, consulte Ejemplos de políticas para administrar recursos de AWS en la Guía de usuario de IAM.

Habilite el acceso a AWS aplicaciones y servicios

Los usuarios pueden autorizar a AWS Managed Microsoft AD a que dé acceso a sus AWS aplicaciones y servicios WorkSpaces, como AmazonActive Directory. Las siguientes AWS aplicaciones y servicios se pueden habilitar o deshabilitar para que funcionen con Microsoft AD AWS administrado.

AWS aplicación/servicio	Más información…
Amazon Chime	Para obtener más información, consulte la Guía de administración de Amazon Chime.
Amazon Connect	Para obtener más información, consulte la Guía de administración de Amazon Connect.

AWS aplicación/servicio	Más información…
Amazon FSx para Windows File Server	Para obtener más información, consulte Uso de Amazon FSx con AWS Directory Service para Microsoft Active Directory.
Amazon QuickSight	Para obtener más información, consulta la Guía del QuickSight usuario de Amazon.
Amazon Relational Database Service	Para obtener más información, consulte la Amazon RDS User Guide.
Amazon WorkDocs	Para obtener más información, consulta la Guía de WorkDocs administración de Amazon.
Amazon WorkMail	Para obtener más información, consulta la Guía del WorkMail administrador de Amazon.
Amazon WorkSpaces	Puede crear un AD Simple, un AD AWS administrado de Microsoft o un AD Connector directamente desde WorkSpaces. Solo tiene que lanzar Advanced Setup al crear su espacio de Workspace. Para obtener más información, consulta la Guía de WorkSpaces administración de Amazon.
AWS Client VPN	Para más información, consulte la Guía del usuario de AWS Client VPN.
AWS IAM Identity Center	Para más información, consulte la Guía del usuario de AWS IAM Identity Center.
AWS License Manager	Para obtener más información, consulte la Guía del usuario de License Manager.
AWS Management Console	Para obtener más información, consulte Habilitación del acceso a la AWS Management Console con credenciales de AD.

AWS aplicación/servicio	Más información…
AWS Private Certificate Authority	Para obtener más información, consulte AWS Private CA Connector for Active Directory.
AWS Transfer Family	Para más información, consulte la Guía del usuario de AWS Transfer Family.

Una vez habilitado, el acceso a los directorios se gestiona en la consola de la aplicación o del servicio al que desea otorgar acceso a su directorio. Para encontrar los enlaces de AWS aplicaciones y servicios descritos anteriormente en la AWS Directory Service consola, lleve a cabo los siguientes pasos.

Para mostrar las aplicaciones y los servicios para un directorio

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. Consulte la lista en la sección de Aplicaciones y servicios de AWS .

Para obtener más información sobre cómo autorizar o desautorizar el uso de AWS aplicaciones y servicios AWS Directory Service, consulteAutorización para AWS aplicaciones y servicios que utilizan AWS Directory Service.

Temas

- Creación de una URL de acceso
- Inicio de sesión único

Creación de una URL de acceso

La URL de acceso se usa con las aplicaciones y los servicios de AWS, como Amazon WorkDocs, para llegar a una página de inicio de sesión asociada a su directorio. La dirección URL debe ser única en todo el mundo. Estos son los pasos para crear una URL de acceso para el directorio.

> **Warning**
>
> Cuando se crea una URL de acceso de aplicaciones para este directorio, no se puede modificar. Una vez creada la URL de acceso, nadie más podrá usarla. Si elimina el directorio, se eliminará también la URL de acceso. A partir de ese momento, cualquier otra cuenta podrá usarla.

> **Note**
>
> La URL de acceso solo se puede configurar desde la región principal cuando se utilizan directorios en varias regiones.

Para crear una URL de acceso

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Administración de aplicaciones. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación de varias regiones, seleccione la pestaña Administración de aplicaciones.
4. En la sección Application access URL (URL de acceso a aplicaciones), si no se ha asignado una URL de acceso al directorio, se mostrará el botón Create (Crear). Escriba un alias de directorio y elija Create (Crear). Si se devuelve un error La entidad ya existe, eso significa que ya se ha asignado el alias de directorio especificado. Elija otro alias y repita el procedimiento.

   La URL de acceso se muestra en el formato `<alias>`.awsapps.com. De forma predeterminada, esta URL lo llevará a la página de inicio de sesión de Amazon WorkDocs.

Inicio de sesión único

AWS Directory Service ofrece la posibilidad de permitir a los usuarios acceder a Amazon WorkDocs desde un ordenador unido al directorio sin tener que introducir sus credenciales por separado.

Antes de habilitar el inicio de sesión único, debe tomar determinadas medidas adicionales para permitir que los navegadores web de los usuarios admitan la función de inicio de sesión único. Los usuarios pueden necesitar modificar la configuración de su navegador web para permitir el inicio de sesión único.

> **Note**
>
> La función de inicio de sesión único solo funciona en equipos que se hayan unido al directorio de AWS Directory Service . No puede aplicarse en equipos que no estén vinculados al directorio.

Si el directorio es un directorio de AD Connector y la cuenta de servicio de AD Connector no tiene permiso para agregar o eliminar el atributo de nombre de la entidad principal del servicio, en los pasos 5 y 6 siguientes, tiene dos opciones:

1. Puede continuar y se le pedirá el nombre de usuario y la contraseña de un usuario de directorio que tenga este permiso para agregar o eliminar el atributo del nombre de la entidad principal del servicio en la cuenta de servicio de AD Connector. Estas credenciales solo se usan para permitir el inicio de sesión único; el servicio no las guarda. Los permisos de la cuenta del servicio AD Connector no se cambian.
2. Puede delegar permisos para permitir que la cuenta de servicio de AD Connector añada o elimine el atributo de nombre principal del servicio por sí misma. Puede ejecutar los siguientes PowerShell comandos desde un equipo unido a un dominio mediante una cuenta que tenga permisos para modificar los permisos de la cuenta de servicio de AD Connector. El siguiente comando le dará a la cuenta del servicio de AD Connector la capacidad de agregar y eliminar un atributo de nombre de la entidad principal del servicio solo para ella misma.

```
$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 activar o desactivar el inicio de sesión único con Amazon WorkDocs

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. En la sección URL de acceso a la aplicación, selecciona Habilitar para habilitar el inicio de sesión único en Amazon. WorkDocs

   Si no ve el botón Habilitar, puede que tenga que crear primero una URL de acceso antes de que se muestre esta opción. Para obtener más información sobre cómo crear una URL de acceso, consulte Creación de una URL de acceso.
5. En el cuadro de diálogo Habilitar el inicio de sesión único para este directorio, elija Habilitar. El inicio de sesión único está habilitado para el directorio.
6. Si más adelante quieres deshabilitar el inicio de sesión único con Amazon WorkDocs, selecciona Inhabilitar y, a continuación, en el cuadro de diálogo Inhabilitar el inicio de sesión único para este directorio, selecciona Inhabilitar de nuevo.

Temas

Inicio de sesión único en IE y Chrome

Para permitir que los navegadores Microsoft Internet Explorer (IE) y Google Chrome admitan la función de inicio de sesión único, deberá hacer lo siguiente en el equipo cliente:

- Agregue su URL de acceso (por ejemplo, https://*<alias>*.awsapps.com) a la lista de sitios aprobados para inicio de sesión único.
- Habilita las secuencias de comandos activas (). JavaScript
- Permita el inicio de sesión automático.
- Habilite la autenticación integrada.

Usted o sus usuarios pueden realizar estas tareas manualmente, o bien pueden cambiar estos ajustes mediante la configuración de la política de grupo.

Temas

Actualización manual para inicio de sesión único en Windows

Para habilitar manualmente la función de inicio de sesión único en un equipo Windows, siga estos pasos en el equipo cliente. Es posible que algunos de estos ajustes estén ya establecidos correctamente.

Habilitación manual de la función de inicio de sesión único en Internet Explorer y Chrome en Windows

1. Para abrir el cuadro de diálogo Internet Properties, elija el menú Start, escriba `Internet Options` en el cuadro de búsqueda y elija Internet Options.
2. Añada su URL de acceso a la lista de sitios aprobados para inicio de sesión único siguiendo estos pasos:
   a. En el cuadro de diálogo Internet Properties, seleccione la pestaña Security.
   b. Seleccione Local intranet y elija Sites.
   c. En el cuadro de diálogo Local intranet, elija Advanced.

   d. Añada su URL de acceso a la lista de sitios web y elija Close.
   e. En el cuadro de diálogo Local intranet, elija OK.
3. Para habilitar el scripting activo, siga estos pasos:
   a. En la pestaña Security del cuadro de diálogo Internet Properties, elija Custom level.
   b. En el cuadro de diálogo Security Settings - Local Intranet Zone, desplácese hasta Scripting y seleccione Enable en Active scripting.
   c. En el cuadro de diálogo Security Settings - Local Intranet Zone, elija OK.
4. Para habilitar el inicio de sesión automático, siga estos pasos:
   a. En la pestaña Security del cuadro de diálogo Internet Properties, elija Custom level.
   b. En el cuadro de diálogo Security Settings - Local Intranet Zone, desplácese hasta User Authentication y seleccione Automatic logon only in Intranet zone en Logon.
   c. En el cuadro de diálogo Security Settings - Local Intranet Zone, elija OK.
   d. En el cuadro de diálogo Security Settings - Local Intranet Zone, elija OK.
5. Para habilitar la autenticación integrada, siga estos pasos:
   a. En el cuadro de diálogo Internet Properties, seleccione la pestaña Advanced.
   b. Desplácese hasta Security y seleccione Enable Integrated Windows Authentication.
   c. En el cuadro de diálogo Internet Properties, seleccione OK.
6. Cierre el navegador y vuelva a abrirlo para que se apliquen los cambios.

Actualización manual para inicio de sesión único en OS X

Para habilitar manualmente el inicio de sesión único para Chrome en OS X, siga estos pasos en el equipo cliente. Necesitará derechos de administrador en su equipo para poder completar estos pasos.

Habilitación manual de la función de inicio de sesión único en Chrome en OS X

1. Añada su URL de acceso a la AuthServerAllowlistpolítica ejecutando el siguiente comando:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Abra System Preferences, vaya al panel Profiles y elimine el perfil `Chrome Kerberos Configuration`.

3. Reinicie Chrome y abra chrome://policy en Chrome para confirmar que se haya implementado la nueva configuración.

Configuración de la política de grupo para el inicio de sesión único

El administrador del dominio puede implementar una configuración de política de grupo para aplicar cambios en la configuración de inicio de sesión único en los equipos cliente vinculados al dominio.

> **Note**
>
> Si administras los navegadores web Chrome en los ordenadores de tu dominio con políticas de Chrome, debes añadir tu URL de acceso a la AuthServerAllowlistpolítica. Para obtener más información sobre la configuración de políticas de Chrome, vaya a Policy Settings in Chrome (en inglés).

Habilitación del inicio de sesión único para Internet Explorer y Chrome mediante la configuración de la política de grupo

1. Cree un nuevo objeto de política de grupo siguiendo estos pasos:
   a. Abra la herramienta de administración de directivas de grupo, navegue hasta su dominio y seleccione Group Policy Objects.
   b. En el menú principal, elija Action y seleccione New.
   c. En el cuadro de diálogo Nuevo GPO, escriba un nombre descriptivo para el objeto de políticas de grupo, como `IAM Identity Center Policy`, y deje GPO de inicio de origen establecido en (ninguno). Haga clic en OK (Aceptar).
2. Añada la URL de acceso a la lista de sitios aprobados para inicio de sesión único siguiendo estos pasos:
   a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Objetos de políticas de grupo, abra el menú contextual (clic con el botón derecho) de su política de IAM Identity Center y, a continuación, elija Editar.
   b. En el árbol de políticas, navegue a User Configuration > Preferences > Windows Settings.
   c. En la lista Windows Settings, abra el menú contextual (clic con el botón derecho) de Registry y elija New registry item.

d. En el cuadro de diálogo New Registry Properties, especifique las siguientes opciones y elija OK:

Action

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

Ruta

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\<alias>
```

El valor de *<alias>* se deriva de la URL de acceso. Si su URL de acceso es `https://examplecorp.awsapps.com`, el alias será `examplecorp`, y la clave de registro será `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Value name

```
https
```

Value type

```
REG_DWORD
```

Value data

```
1
```

3. Para habilitar el scripting activo, siga estos pasos:

a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Objetos de políticas de grupo, abra el menú contextual (clic con el botón derecho) de su política de IAM Identity Center y, a continuación, elija Editar.

b. En el árbol de políticas, navegue a Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

c. En la lista Intranet Zone, abra el menú contextual (clic con el botón derecho) para Allow active scripting y elija Edit.

d. En el cuadro de diálogo Allow active scripting, especifique las siguientes opciones y elija OK:

- Seleccione el botón de opción Enabled.
- En Options ajuste Allow active scripting en Enable.

4. Para habilitar el inicio de sesión automático, siga estos pasos:

a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Group Policy Objects, abra el menú contextual (clic con el botón derecho) de su política de inicio de sesión único y, a continuación, elija Edit.

b. En el árbol de políticas, navegue a Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

c. En la lista Intranet Zone, abra el menú contextual (clic con el botón derecho) para Logon options y elija Edit.

d. En el cuadro de diálogo Logon options, especifique las siguientes opciones y elija OK:

- Seleccione el botón de opción Enabled.
- En Options ajuste Logon options en Automatic logon only in Intranet zone.

5. Para habilitar la autenticación integrada, siga estos pasos:

a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Objetos de políticas de grupo, abra el menú contextual (clic con el botón derecho) de su política de IAM Identity Center y, a continuación, elija Editar.

b. En el árbol de políticas, navegue a User Configuration > Preferences > Windows Settings.

c. En la lista Windows Settings, abra el menú contextual (clic con el botón derecho) de Registry y elija New registry item.

d. En el cuadro de diálogo New Registry Properties, especifique las siguientes opciones y elija OK:

Action

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

Ruta

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

Value name

```
EnableNegotiate
```

Value type

```
REG_DWORD
```

Value data

```
1
```

6. Cierre la ventana de Group Policy Management Editor si aún está abierta.
7. Asigne la nueva política a su dominio siguiendo estos pasos:
   a. En el árbol de administración de la directiva de grupo, abra el menú contextual (clic con el botón derecho) de su dominio y elija Link an Existing GPO.
   b. En la lista Objetos de políticas de grupo, seleccione su política de IAM Identity Center y elija Aceptar.

Estos cambios se aplicarán tras la siguiente actualización de la política de grupo en el cliente o la siguiente vez que el usuario inicie sesión.

Inicio de sesión único en Firefox

Para permitir que el navegador Mozilla Firefox admita el inicio de sesión único, agregue su URL de acceso (por ejemplo, https://*<alias>*.awsapps.com) a la lista de sitios aprobados para inicio de sesión único. Esto puede hacerse manualmente o con un script automatizado.

Temas

- Actualización manual para inicio de sesión único
- Actualización automática para inicio de sesión único

Actualización manual para inicio de sesión único

Para añadir manualmente su URL de acceso a la lista de sitios aprobados en Firefox, siga estos pasos en el equipo cliente.

Para añadir manualmente su URL de acceso a la lista de sitios aprobados en Firefox

1. Abra Firefox y abra luego la página `about:config`.
2. Abra la preferencia `network.negotiate-auth.trusted-uris` y agregue su URL de acceso a la lista de sitios. Utilice una coma (,) para separar varias entradas.

Actualización automática para inicio de sesión único

Como administrador del dominio, puede utilizar un script para agregar su URL de acceso a la preferencia de usuario `network.negotiate-auth.trusted-uris` de Firefox en todos los equipos que haya en la red. Para obtener más información, consulte https://support.mozilla.org/es-es/questions/939037.

Habilitación del acceso a la AWS Management Console con credenciales de AD

AWS Directory Service le permite conceder acceso a AWS Management Console a los miembros de su directorio. De forma predeterminada, los miembros de su directorio no tienen acceso a los recursos de AWS. Asigne roles de IAM a los miembros de su directorio para darles acceso a los distintos servicios y recursos de AWS. El rol de IAM define los servicios, los recursos y el nivel de acceso que tienen los miembros de su directorio.

Para que los miembros de su directorio puedan tener acceso a la consola, es preciso que este cuente con una URL de acceso. Para obtener más información sobre cómo ver los detalles del directorio y obtener la URL de acceso, consulte Ver información del directorio. Para obtener más información sobre cómo crear una URL de acceso, consulte Creación de una URL de acceso.

Para obtener más información sobre cómo crear roles de IAM y asignarlos a los miembros del directorio, consulte Otorgar acceso a los recursos de AWS a usuarios y grupos.

Temas

Artículo relacionado del blog de seguridad de AWS

- Cómo acceder a la AWS Management Console con AWS Managed Microsoft AD y las credenciales en las instalaciones

> **Note**
>
> Acceder a AWS Management Console es una característica regional de AWS Managed Microsoft AD. Si utiliza Replicación multirregional, los siguientes procedimientos se deberán aplicar por separado en cada región. Para obtener más información, consulte Características globales frente a las regionales.

Habilitación del acceso a AWS Management Console

De forma predeterminada, el acceso a la consola no está habilitado para ningún directorio. Para que los grupos y usuarios de su directorio puedan tener acceso a la consola, siga estos pasos:

Para habilitar el acceso a la consola

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación de varias regiones, seleccione la región en la que desee habilitar el acceso a AWS Management Console, a continuación, elija la pestaña Administración de aplicaciones. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación de varias regiones, seleccione la pestaña Administración de aplicaciones.
4. En la sección de la AWS Management Console, elija Habilitar. El acceso a la consola estará habilitado para su directorio.

   Para que los usuarios puedan iniciar sesión en la consola con su URL de acceso, primero debe agregar sus usuarios al rol. Para obtener más información general sobre la asignación de usuarios a roles de IAM, consulte Asignación de usuarios o grupos a una función existente. Una vez asignados los roles de IAM, los usuarios pueden obtener acceso a la consola con su URL de

acceso. Por ejemplo, si su URL de acceso al directorio es example-corp.awsapps.com, la URL para obtener acceso a la consola es https://example-corp.awsapps.com/console/.

Deshabilitación del acceso a la AWS Management Console

Para deshabilitar el acceso de los grupos y usuarios de su directorio a la consola, siga estos pasos:

Para deshabilitar el acceso a la consola

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación de varias regiones, seleccione la región en la que desee deshabilitar el acceso a AWS Management Console, a continuación, elija la pestaña Administración de aplicaciones. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación de varias regiones, seleccione la pestaña Administración de aplicaciones.
4. En la sección de la AWS Management Console, elija Deshabilitar. El acceso a la consola estará deshabilitado para su directorio.
5. Si los roles de IAM se han asignado a usuarios o grupos del directorio, el botón Deshabilitar no estará disponible. En este caso, debe quitar todas las asignaciones del rol de IAM para el directorio antes de continuar, incluidas las asignaciones para los usuarios o grupos del directorio que se han eliminado, que aparecerán como Usuario eliminado o Grupo eliminado.

   Una vez eliminadas todas las asignaciones de rol de IAM, repita los pasos anteriores.

Establecimiento de la duración del inicio de sesión

De forma predeterminada, el tiempo que transcurre desde que los usuarios inician sesión en la consola hasta que se cierra la sesión es de una hora. Al cabo de esa hora, los usuarios deben volver a iniciar sesión, con lo que comienza la siguiente sesión de una hora de duración hasta que se cierre la sesión. Puede utilizar este procedimiento para ampliar el período de tiempo hasta un máximo de 12 horas por sesión.

Para establecer la duración del inicio de sesión

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación de varias regiones, seleccione la región en la que desee configurar la duración de la sesión de inicio de sesión y, a continuación, elija la pestaña Administración de aplicaciones. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación de varias regiones, seleccione la pestaña Administración de aplicaciones.
4. En la sección Aplicaciones y servicios de AWS, elija Consola de administración de AWS.
5. En el cuadro de diálogo Administrar el acceso a los recursos de AWS, elija Continuar.
6. En la página Assign users and groups to IAM roles, en Set login session length, edite el valor numerado y luego elija Save.

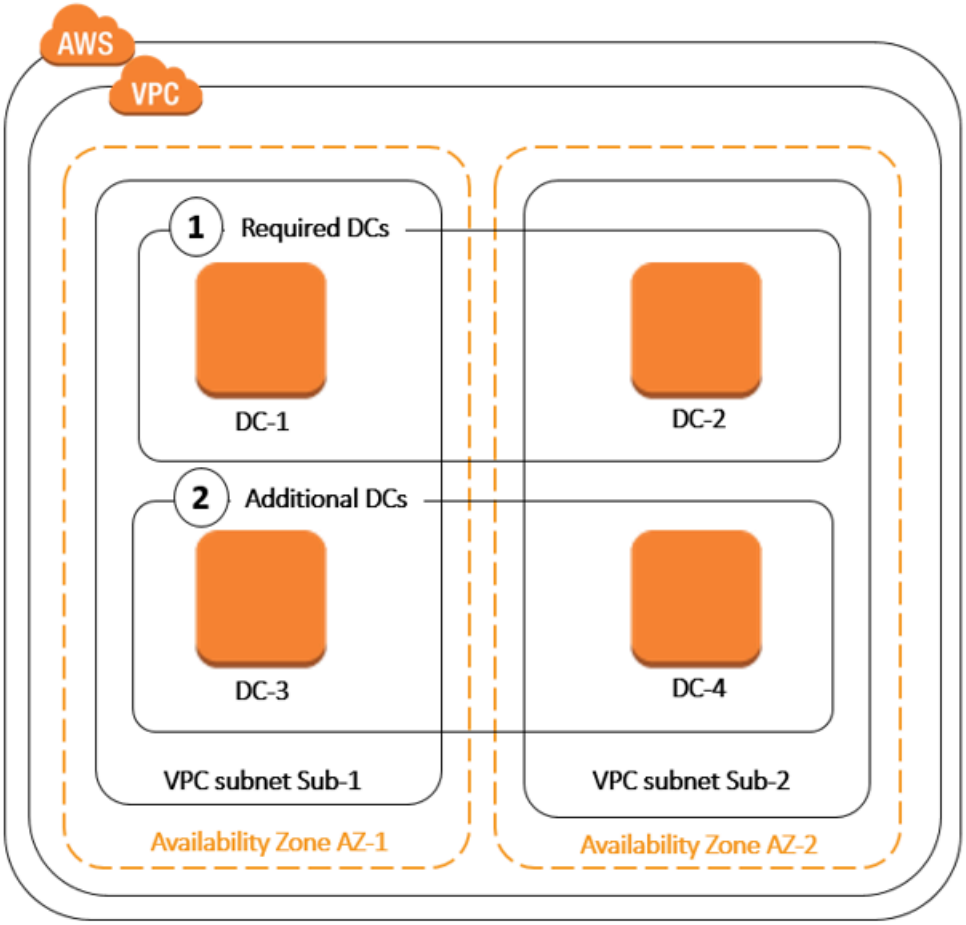
Implementación de controladores de dominio adicionales

La implementación de controladores de dominios adicionales aumenta la redundancia, lo que mejora aún más la resistencia y la disponibilidad. Esto también mejora el desempeño del directorio al poder utilizar un mayor número de solicitudes de Active Directory. Por ejemplo, ahora puede usar AWS Managed Microsoft AD para admitir varias aplicaciones.NET que se despliegan en grandes flotas de instancias de Amazon EC2 y Amazon RDS for SQL Server.

Al crear el directorio por primera vez, AWS Managed Microsoft AD implementa dos controladores de dominio en varias zonas de disponibilidad, lo cual es necesario para garantizar una alta disponibilidad. Más adelante, puede implementar fácilmente controladores de dominio adicionales a través de la AWS Directory Service consola simplemente especificando el número total de controladores de dominio que desea. AWS Microsoft AD administrado distribuye los controladores de dominio adicionales a las zonas de disponibilidad y las subredes de Amazon VPC en las que se ejecuta el directorio.

Por ejemplo, en la siguiente ilustración, DC-1 y DC-2 representan los dos controladores de dominio que se crearon originalmente con su directorio. La AWS Directory Service consola hace referencia

a estos controladores de dominio predeterminados como obligatorios. AWS El Microsoft AD administrado localiza intencionadamente cada uno de estos controladores de dominio en zonas de disponibilidad independientes durante el proceso de creación del directorio. Luego podrá optar por añadir dos controladores de dominio más para ayudar a distribuir la carga de autenticación en las horas pico de inicio de sesión. DC-3 y DC-4 representan los nuevos controladores de dominio, a los que ahora la consola considera Additional. Como antes, AWS Managed Microsoft AD vuelve a colocar automáticamente los nuevos controladores de dominio en diferentes zonas de disponibilidad para garantizar la alta disponibilidad de su dominio.



Este proceso evita tener que configurar manualmente la replicación de datos del directorio, las instantáneas diarias automatizadas o la monitorización de los controladores de dominio adicionales. También es más fácil migrar y ejecutar cargas de trabajo críticas integradas en Active Directory en la nube de AWS sin tener que implementar y mantener su propia infraestructura de Active Directory. También puedes implementar o quitar controladores de dominio adicionales para AWS Managed Microsoft AD mediante la UpdateNumberOfDomainControllersAPI.

> **Note**
>
> Los controladores de dominio adicionales son una función regional de AWS Managed Microsoft AD. Si utiliza Replicación multirregional, los siguientes procedimientos se deberán aplicar por separado en cada región. Para obtener más información, consulte Características globales frente a las regionales.

Agregar o quitar controladores de dominio adicionales

Antes de agregar o quitar controladores de dominio adicionales, aquí encontrará más información sobre los requisitos de los controladores de dominio:

- Después de la implementación de controladores de dominio adicionales, puede reducir el número de controladores de dominio a dos, que es el mínimo necesario para lograr tolerancia a errores y una alta disponibilidad.
- Los controladores de dominio eliminados se eliminarán de la lista de controladores de dominio adicionales. Los controladores de dominio principal y secundario son obligatorios y no se pueden eliminar.
- Si ha configurado su Microsoft AD AWS administrado para habilitar LDAPS, cualquier controlador de dominio adicional que agregue también tendrá LDAPS habilitado automáticamente. Para obtener más información, consulte Habilite LDAP o LDAPS seguros.

Utilice el siguiente procedimiento para implementar o quitar controladores de dominio adicionales en su directorio de AWS Managed Microsoft AD.

Para añadir o quitar controladores de dominio adicionales

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
    - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región en la que desee agregar o eliminar controladores de dominio y, a continuación, seleccione la pestaña Escalar y compartir. Para obtener más información, consulte Regiones principales frente a las adicionales.

- Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Escalar y compartir.

4. En la sección Domain controllers (Controladores de dominio), elija Edit (Editar).
5. Especifique el número de controladores de dominio que va a añadir o quitar del directorio y, a continuación, elija Modify (Modificar).
6. Cuando AWS Managed Microsoft AD finaliza el proceso de implementación, todos los controladores de dominio muestran el estado Activo y aparecen las subredes de Amazon VPC y de Zona de disponibilidad asignadas. Los nuevos controladores de dominio se distribuyen de manera equitativa entre las zonas de disponibilidad y subredes en las que el directorio ya está implementado.

Artículo de blog sobre AWS seguridad relacionado

- Cómo aumentar la redundancia y el rendimiento de su AWS Directory Service Microsoft AD AWS administrado mediante la adición de controladores de dominio

Migración de los usuarios de Active Directory a AWS Managed Microsoft AD

Puede usar el kit de herramientas de migración para Active Directory (ADMT) junto con el Servicio de exportación de contraseñas (PES) para migrar los usuarios del Active Directory autoadministrado al directorio administrado de AWS Microsoft AD. Esto le permite migrar los objetos de Active Directory y las contraseñas cifradas para sus usuarios con mayor facilidad.

Para obtener instrucciones detalladas, consulte How to migrate your on-premises domain to AWS Managed Microsoft AD using ADMT en el Blog de seguridad deAWS.

AWS Cuotas administradas de Microsoft AD

Las siguientes son las cuotas predeterminadas para AWS Managed Microsoft AD. A menos que se indique lo contrario, cada cuota es por cada región.

AWS Cuotas administradas de Microsoft AD

Recurso	Cuota predeterminada
AWS Directorios gestionados de Microsoft AD	20

Recurso	Cuota predeterminada
Instantáneas manuales *	5 por Microsoft AD AWS administrado
Antigüedad de las instantáneas manuales **	180 días
Número máximo de controladores de dominio por directorio	20
Dominios compartidos por Microsoft AD Standard ***	5
Dominios compartidos por Microsoft AD Enterprise ***	125
Número máximo de certificados de entidad de certificación (CA) registrados por directorio	5
Número máximo de AWS regiones totales en un único directorio AWS gestionado de Microsoft AD (Enterprise Edition) ****	5

*La cuota de instantáneas manuales no se puede cambiar.

** La antigüedad máxima admitida de una instantánea manual es de 180 días y no se puede cambiar. Esto es porque así lo estipula el atributo de tiempo de conservación-marcador de exclusión de objetos eliminados, que define el tiempo de conservación de una copia de seguridad de estado del sistema de Active Directory. No es posible realizar una restauración a partir de una instantánea que tiene una antigüedad de más de 180 días. Para obtener más información, consulte Tiempo de conservación de una copia de seguridad de estado del sistema de Active Directory en el sitio web de Microsoft.

*** La cuota predeterminada de dominios compartidos se refiere al número de cuentas con las que se puede compartir un directorio individual.

**** Esto incluye 1 región principal y hasta 4 adicionales. Para obtener más información, consulte Regiones principales frente a las adicionales.

> **Note**
>
> No puede adjuntar una dirección IP pública a la interface de red AWS elástica (ENI).

Para obtener más información sobre el diseño de aplicaciones y la distribución de la carga, consulte Programación de las aplicaciones.

Para obtener información sobre las cuotas de objetos y de almacenamiento, consulte la tabla comparativa en la página Precios de AWS Directory Service.

Compatibilidad de aplicaciones para Microsoft AD AWS administrado

AWS Directory Service for Microsoft Active Directory (Microsoft AD AWS administrado) es compatible con varios AWS servicios y aplicaciones de terceros.

La siguiente es una lista de AWS aplicaciones y servicios compatibles:

- Amazon Chime: para obtener instrucciones detalladas, consulte Conexión con Active Directory.
- Amazon Connect: para obtener más información, consulte Cómo funciona Amazon Connect.
- Amazon EC2: para obtener más información, consulte Unir una instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory.
- Amazon QuickSight : para obtener más información, consulte Administración de cuentas de usuario en Amazon QuickSight Enterprise Edition.
- Amazon RDS para MySQL: para obtener más información, consulte Uso de la autenticación de Kerberos para MySQL.
- Amazon RDS para Oracle: para obtener más información, consulte Uso de la autenticación Kerberos con Amazon RDS para Oracle.
- Amazon RDS para PostgreSQL: para obtener más información, consulte Uso de la autenticación Kerberos con Amazon RDS para PostgreSQL.
- Amazon RDS para SQL Server: para obtener más información, consulte Uso de la autenticación de Windows con una instancia de base de datos de Microsoft SQL Server.
- Amazon WorkDocs : para obtener instrucciones detalladas, consulte Conectarse a su directorio local con AWS Managed Microsoft AD.

- Amazon WorkMail : para obtener instrucciones detalladas, consulte Integrar Amazon WorkMail con un directorio existente (configuración estándar).
- AWS Client VPN - Para obtener instrucciones detalladas, consulte Autenticación y autorización del cliente.
- AWS IAM Identity Center - Para obtener instrucciones detalladas, consulte Conectar el centro de identidad de IAM a un Active Directory local.
- AWS License Manager - Para obtener más información, consulte Suscripciones basadas en usuarios en. AWS License Manager
- AWS Management Console — Para obtener más información, consulteHabilitación del acceso a la AWS Management Console con credenciales de AD.
- FSx para Windows File Server: para obtener más información, consulte ¿Qué es FSx para Windows File Server?.
- WorkSpaces - Para obtener instrucciones detalladas, consulte Iniciar una WorkSpace con Microsoft AD AWS administrado.

Debido a la magnitud de off-the-shelf las aplicaciones personalizadas y comerciales que utilizan Active Directory, AWS no realizan ni pueden realizar una verificación formal o amplia de la compatibilidad de las aplicaciones de terceros con AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Si bien AWS trabaja con los clientes para intentar superar los posibles problemas de instalación de aplicaciones que puedan surgir, no podemos garantizar que ninguna aplicación sea o siga siendo compatible con AWS Managed Microsoft AD.

Las siguientes aplicaciones de terceros son compatibles con AWS Managed Microsoft AD:

- Active Directory-Based Activation (ADBA)
- 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 conocido como Azure Active Directory (AzureAD))
- Microsoft Entra Connect(anteriormente conocido comoAzure Active Directory Connect)
- Distributed File System Replication (DFSR)
- Distributed File System Namespaces (DFSN)

- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(incluidos los grupos de disponibilidad Always On de SQL Server)
- Microsoft System Center Configuration Manager(SCCM): el usuario que implemente SCCM debe ser miembro del grupo de administradores de administración AWS delegada del sistema.
- Microsoft Windows and Windows Server OS
- Office 365

Tenga en cuenta que es posible que no todas las configuraciones de estas aplicaciones sean compatibles.

Directrices de compatibilidad

Aunque las aplicaciones pueden tener configuraciones que sean incompatibles, las configuraciones de implementación de las aplicaciones a menudo pueden superar la incompatibilidad. A continuación se describen los motivos más comunes para incompatibilidad de las aplicaciones. Los clientes pueden usar esta información para investigar las características de compatibilidad de una aplicación determinada e identificar los posibles cambios de implementación.

- Administrador del dominio u otros permisos privilegiados: algunas aplicaciones requieren su instalación como administrador del dominio. Como AWS debe conservar el control exclusivo de este nivel de permisos para poder ofrecer Active Directory como un servicio administrado, no puede actuar como administrador del dominio para instalar dichas aplicaciones. Sin embargo, a menudo puede instalar estas aplicaciones delegando permisos específicos, menos privilegiados y AWS compatibles a la persona que realiza la instalación. Para obtener más información sobre los permisos exactos que necesita la aplicación, pregunte al proveedor de la aplicación. Para obtener más información sobre los permisos que AWS le permiten delegar, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD.
- Acceso a Active Directory contenedores privilegiados: dentro de su directorio, AWS Managed Microsoft AD proporciona una unidad organizativa (OU) sobre la que tiene el control administrativo total. No tiene permisos de creación o de escritura, y puede que tenga permisos de lectura limitados a los contenedores situados en posiciones más elevadas en el árbol de Active Directory que la OU. Las aplicaciones que crean o tienen acceso a los contenedores para los que usted no tiene permisos podrían no funcionar. Sin embargo, este tipo de aplicaciones a menudo ofrecen la posibilidad alternativa de usar un contenedor que se crea dentro de su OU. Póngase en contacto con el proveedor de su aplicación para encontrar la forma de crear y utilizar un contenedor de

su OU como alternativa. Para obtener más información sobre cómo administrar su OU, consulte Cómo administrar Microsoft AD AWS administrado.

- Cambios de esquema durante el flujo de trabajo de instalación: algunas Active Directory aplicaciones requieren cambios en el esquema predeterminado de Active Directory y pueden intentar instalar esos cambios como parte del flujo de trabajo de instalación de la aplicación. Debido a la naturaleza privilegiada de las extensiones de esquema, AWS lo hace posible al importar archivos de formato ligero de intercambio de directorios (LDIF) únicamente a través de la consola AWS Directory Service , la CLI o el SDK. Estas aplicaciones suelen incluir un archivo LDIF que se puede aplicar al directorio mediante el proceso de actualización del esquema. AWS Directory Service Para obtener más información sobre cómo funciona el proceso de importación de archivos LDIF, consulte Tutorial: Ampliación del esquema de Microsoft AD AWS administrado. Puede instalar la aplicación de forma que omita la instalación del esquema durante el proceso de instalación.

Aplicaciones incompatibles conocidas

A continuación se enumeran las off-the-shelf aplicaciones comerciales más solicitadas para las que no hemos encontrado una configuración que funcione con AWS Managed Microsoft AD. AWS actualiza esta lista de vez en cuando, a su entera discreción, como cortesía para ayudarle a evitar esfuerzos improductivos. AWS proporcione esta información sin garantías ni reclamos con respecto a la compatibilidad actual o 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 Tutoriales de laboratorio de pruebas gestionadas de Microsoft AD

Esta sección proporciona una serie de tutoriales guiados que le ayudarán a establecer un entorno de laboratorio de pruebas AWS en el que pueda experimentar con Microsoft AD AWS administrado.

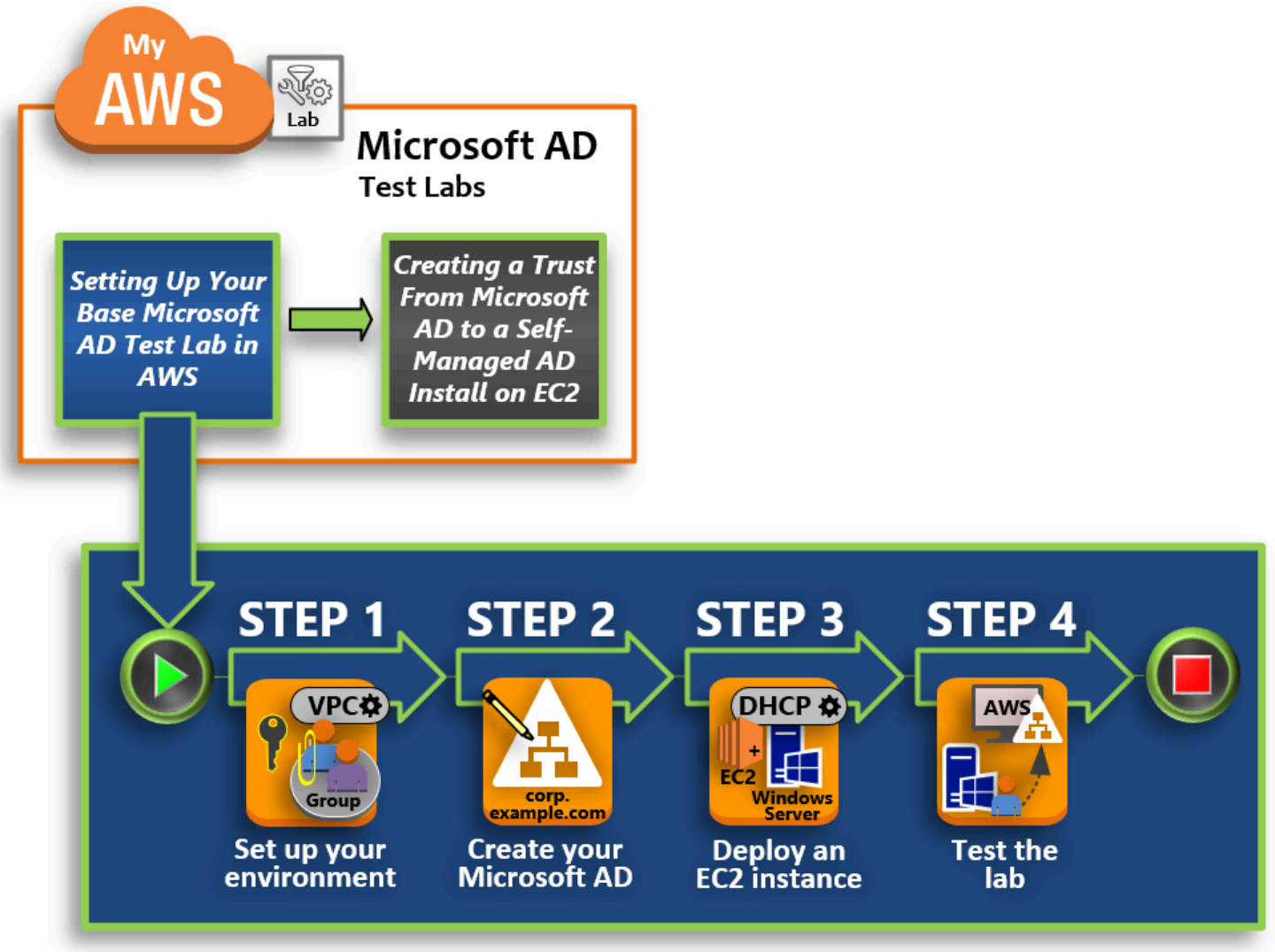
Temas

- Tutorial: Configuración de su laboratorio de pruebas base de Microsoft AD AWS administrado en AWS
- Tutorial: Creación de una confianza desde Microsoft AD AWS gestionado a una instalación autogestionada de Active Directory en Amazon EC2

Tutorial: Configuración de su laboratorio de pruebas base de Microsoft AD AWS administrado en AWS

Este tutorial le enseña cómo configurar su AWS entorno para prepararse para una nueva instalación AWS gestionada de Microsoft AD que utilice una nueva instancia de Amazon EC2 que ejecute Windows Server 2019. Luego, le enseña a usar las herramientas de administración típicas de Active Directory para administrar su entorno Microsoft AD AWS administrado desde su instancia EC2 de Windows. Cuando complete el tutorial, habrá establecido los requisitos previos de la red y habrá configurado un nuevo bosque AWS administrado de Microsoft AD.

Como se muestra en la siguiente ilustración, el laboratorio que cree a partir de este tutorial es el componente fundamental para el aprendizaje práctico sobre AWS Microsoft AD administrado. Posteriormente, podrá agregar tutoriales opcionales para una experiencia más práctica. Esta serie de tutoriales es ideal para cualquiera que se acerque por primera vez a AWS Managed Microsoft AD y quiera contar con un laboratorio de pruebas para evaluación. Para completar este tutorial se necesita aproximadamente 1 hora.



Paso 1: Configure su AWS entorno para Microsoft AD Active Directory AWS administrado

Una vez completadas las tareas previas, debe crear y configurar una Amazon VPC en su instancia EC2.

Paso 2: Cree su Microsoft AD Active Directory AWS administrado

En este paso, configuras Microsoft AD AWS administrado AWS por primera vez.

Paso 3: Implemente una instancia de Amazon EC2 para gestionar su Active Directory gestionado de AWS Microsoft AD

A continuación, veremos las distintas tareas posteriores a la implementación necesarias para que los equipos clientes se conecten a su nuevo dominio y para configurar un nuevo sistema de Windows Server en EC2.

Paso 4: verificación de que el laboratorio de pruebas base esté operativo

Por último, como administrador, debe verificar que pueda iniciar sesión y conectarse a AWS Managed Microsoft AD desde su sistema de Windows Server en EC2. Tras haber comprobado satisfactoriamente que el laboratorio es operativo, puede seguir agregando otros módulos guía del laboratorio de pruebas.

Requisitos previos

Si quiere utilizar solamente los pasos de la IU de este tutorial para crear su laboratorio de pruebas, puede omitir esta sección de requisitos previos y pasar al paso 1. Sin embargo, si planea usar AWS CLI comandos o AWS Tools for Windows PowerShell módulos para crear su entorno de laboratorio de pruebas, primero debe configurar lo siguiente:

- Usuario de IAM con la clave de acceso y la clave de acceso secreta: si desea utilizar los módulos AWS CLI o AWS Tools for Windows PowerShell , necesitará un usuario de IAM con una clave de acceso. Si no tiene una clave de acceso, consulte Creación, modificación y visualización de claves de acceso (AWS Management Console).
- AWS Command Line Interface (opcional): descárguelo e instálelo AWS CLI en Windows. Una vez instalado, abra la línea de comandos o Windows PowerShell la ventana y, a continuación, escriba`aws configure`. Tenga en cuenta que necesita la clave de acceso y la clave secreta para completar la configuración. Consulte el primer requisito previo para ver los pasos que indican cómo hacer esto. Se le solicitará que indique lo siguiente:
  - AWS ID de clave de acceso [Ninguno]: `AKIAIOSFODNN7EXAMPLE`
  - AWS clave de acceso secreta [Ninguna]: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - Nombre de la región predeterminada [Ninguna]: `us-west-2`
  - Default output format [None]: `json`
- AWS Tools for Windows PowerShell (opcional): descargue e instale la versión más reciente de AWS Tools for Windows PowerShell desde https://aws.amazon.com/powershell/ y ejecute el siguiente comando. Tenga en cuenta que necesita su clave de acceso y la clave secreta para completar la configuración. Consulte el primer requisito previo para ver los pasos que indican cómo hacerlo.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

Paso 1: Configure su AWS entorno para Microsoft AD Active Directory AWS administrado

Antes de poder crear Microsoft AD AWS administrado en su laboratorio de AWS pruebas, primero debe configurar el par de claves de Amazon EC2 para que todos los datos de inicio de sesión estén cifrados.

Crear un par de claves

Si ya tiene un par de claves, puede omitir este paso. Para obtener más información sobre los pares de claves de Amazon EC2, consulte Crear pares de claves.

Crear un par de claves

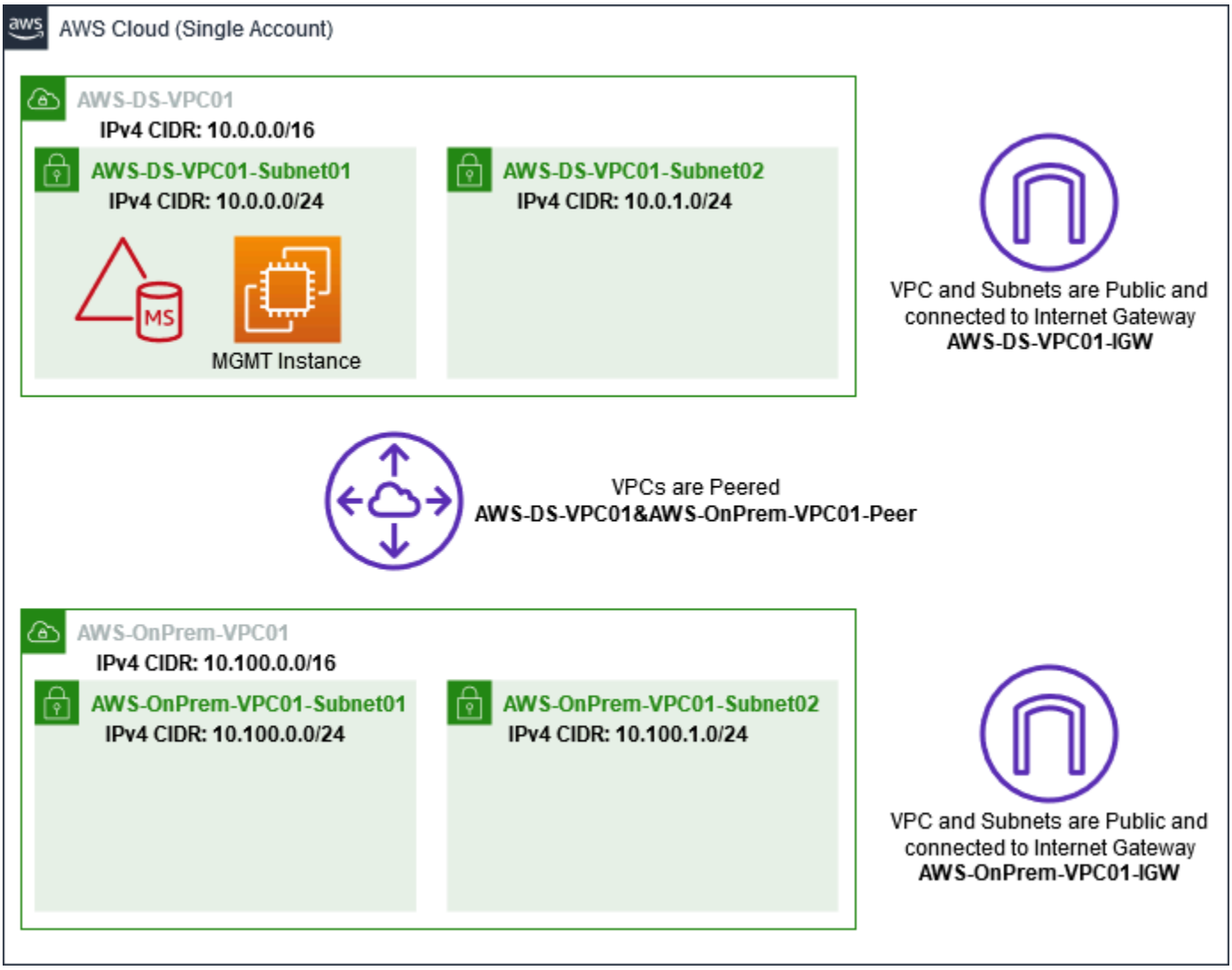
1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Network & Security, seleccione Key Pairs y después Create Key Pair.
3. En Key pair name (Nombre del par de claves), escriba **AWS-DS-KP**. En Key pair file format (Formato de archivo del par de claves), seleccione pem, y, a continuación, elija Create (Crear).
4. Su navegador descargará el archivo de clave privada automáticamente. El nombre del archivo es el nombre que indicó cuando creó el par de claves con la extensión `.pem`. Guarde el archivo de clave privada en un lugar seguro.

> **Important**
>
> Esta es la única oportunidad para guardar el archivo de clave privada. Deberá proporcionar el nombre de su par de claves al lanzar una instancia, y la clave privada correspondiente cada vez que descifre la contraseña de la instancia.

Cree, configure y empareja dos Amazon VPC

Como se muestra en la ilustración siguiente, cuando termine este proceso de varios pasos habrá creado y configurado dos VPC públicas, dos subredes públicas por VPC, una gateway de Internet por VPC y una interconexión de VPC entre las VPC. Elegimos utilizar VPC y subredes públicas con el propósito de simplificar y ahorrar costos. Para cargas de trabajo de producción, recomendamos

utilizar VPC privadas. Para obtener más información sobre cómo mejorar la seguridad de la VPC, consulte Seguridad en Amazon Virtual Private Cloud.



Todos los PowerShell ejemplos utilizan AWS CLI la información de VPC que se muestra a continuación y están integrados en us-west-2. Puede elegir cualquier región admitida para crear su entorno. Para obtener más información, consulte ¿Qué es Amazon VPC?.

Paso 1: Crear dos VPC

En este paso, debe crear dos VPC en la misma cuenta con los parámetros especificados en la siguiente tabla. AWS Microsoft AD administrado admite el uso de cuentas independientes con Compartir el directorio esta función. La primera VPC se utilizará para Managed AWS Microsoft AD. La segunda VPC se utilizará para los recursos que se pueden utilizar más adelante en Tutorial: Creación de una confianza desde Microsoft AD AWS gestionado a una instalación autogestionada de Active Directory en Amazon EC2.

Información sobre las VPC administradas de Active Directory	Información de la VPC en las instalaciones
Etiqueta de nombre: -DS-VPC01 AWS IPv4 CIDR block (Bloque de CIDR IPv4): 10.0.0.0/16 IPv6 CIDR block: No IPv6 CIDR Block Tenencia: predeterminada	Etiqueta de nombre: - -VPC01 AWS OnPrem Bloque de CIDR IPv4: 10.100.0.0/16 IPv6 CIDR block: No IPv6 CIDR Block Tenencia: predeterminada

Para obtener instrucciones detalladas, consulte Crear una VPC.

Paso 2: Crear dos subredes por VPC

Después de haber creado las VPC, deberá crear dos subredes por VPC utilizando los parámetros especificados en la tabla siguiente. En este laboratorio de pruebas cada subred será /24. Esto permitirá emitir hasta 256 direcciones por subred. Cada subred debe estar en una zona de disponibilidad distinta. Poner cada subred en una zona de disponibilidad distinta es uno de los AWS Requisitos previos de Microsoft AD gestionado.

Información de la subred AWS-DS-VPC01:	AWS- OnPrem -Información de subred del VPC01
Etiqueta de nombre: -DS-VPC01-Subnet01 AWS VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS Zona de disponibilidad: us-west-2a Bloque de CIDR IPv4: 10.0.0.0/24	Etiqueta de nombre: - -VPC01-Subnet01 AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem Zona de disponibilidad: us-west-2a Bloque de CIDR IPv4: 10.100.0.0/24
Etiqueta de nombre: -DS-VPC01-Subnet02 AWS VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS	Etiqueta de nombre: - -VPC01-Subnet02 AWS OnPrem

Información de la subred AWS-DS-VPC01:	AWS- OnPrem -Información de subred del VPC01
Zona de disponibilidad: us-west-2b Bloque de CIDR IPv4: 10.0.1.0/24	VPC: vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem Zona de disponibilidad: us-west-2b Bloque de CIDR IPv4: 10.100.1.0/24

Para obtener instrucciones detalladas, consulte Crear una subred en la VPC.

Paso 3: Crear y asociar una gateway de Internet a las VPC

Dado que estamos utilizando VPC públicas, tendrá que crear y asociar una gateway de Internet a las VPC utilizando los parámetros especificados en la siguiente tabla. Esto le permitirá conectarse y administrar sus instancias EC2.

Información de la puerta de enlace de Internet AWS-DS-VPC01	AWS- OnPrem -Información sobre la pasarela de Internet Gateway VPC01
Etiqueta de nombre: -DS-VPC01-IGW AWS VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS	Etiqueta de nombre: - -VPC01-IGW AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Para obtener instrucciones detalladas, consulte Gateways de Internet.

Paso 4: Configurar una conexión de emparejamiento de VPC entre AWS-DS-VPC01 y - -VPC01 AWS OnPrem

Dado que ya ha creado dos VPC anteriormente, deberá conectarlas en red usando una interconexión de VPC mediante los parámetros especificados en la tabla siguiente. Si bien hay muchas formas de conectar las VPC, en este tutorial se utilizará el peering de VPC. AWS Microsoft AD administrado admite muchas soluciones para conectar sus VPC, algunas de las cuales incluyen el emparejamiento de VPC, Transit Gateway y VPN.

Etiqueta de nombre de la conexión de emparejamiento: -DS-VPC01& - -VPC01-Peer AWSAWS OnPrem

VPC (solicitante): vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS

Cuenta: Mi Cuenta

Región: Esta región

VPC (aceptador): vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Para obtener instrucciones sobre cómo crear una interconexión de VPC con otra VPC desde su cuenta, consulte Crear una interconexión de VPC con otra VPC de su cuenta.

Paso 5: Agregar dos rutas a la tabla de enrutamiento principal de cada VPC

Para que la interconexión de VPC y las gateways de Internet creadas en los pasos anteriores funcionen, deberá actualizar la tabla de enrutamiento principal de ambas VPC utilizando los parámetros especificados en la tabla siguiente. Agregará dos rutas: 0.0.0.0/0 que enrutará a todos los destinos no conocidos explícitamente en la tabla de enrutamiento y 10.0.0.0/16 o 10.100.0.0/16 que enrutará a cada VPC a través de la interconexión de VPC establecida anteriormente.

Puede encontrar fácilmente la tabla de enrutamiento correcta para cada VPC filtrando la etiqueta de nombre de la VPC (AWS-DS-VPC01 o - -VPC01). AWS OnPrem

Información de la ruta 1 de AWS-DS-VPC01	Información de la ruta 2 de AWS-DS-VPC01	AWS- Información sobre la ruta 1 de la -VPC01 OnPrem	AWS- -Información sobre la ruta 2 OnPrem del VPC01
Destino: 0.0.0.0/0 Objetivo: igw-xxxxxxxxxxxxxx -DS-VPC01-IGW AWS	Destino: 10.100.0.0/16 Objetivo: pcx-xxxxxxxxxxxxxxxxx AWSAWS-DS-VPC01& - -VPC01-peer OnPrem	Destino: 0.0.0.0/0 Objetivo: igw-xxxxxxxxxxxxxx AWS-OnPrem-VPC01	Destino: 10.0.0.0/16 Objetivo: pcx-xxxxxxxxxxxxx -DS-VPC01& - AWS-VPC01-peer AWS OnPrem

Para obtener instrucciones sobre cómo agregar rutas a una tabla de enrutamiento de VPC, consulte Agregar y quitar rutas de una tabla de enrutamiento.

Creación de grupos de seguridad para instancias de Amazon EC2

De forma predeterminada, AWS Managed Microsoft AD crea un grupo de seguridad para administrar el tráfico entre sus controladores de dominio. En esta sección, deberá crear dos grupos de seguridad (uno para cada VPC) que se utilizarán para administrar el tráfico dentro de su VPC para las instancias EC2 mediante los parámetros especificados en las tablas siguientes. También agregará una regla que permite la entrada RDP (3389) desde cualquier lugar y para todos los tipos de tráfico entrante desde la VPC local. Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias de Windows.

Información del grupo de seguridad de AWS-DS-VPC01:
Nombre del grupo de seguridad: AWS DS Test Lab Security Group Descripción: Grupo de seguridad AWS DS Test Lab VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS

Reglas de entrada de grupos de seguridad para -DS-VPC01 AWS

Tipo	Protocolo	Rango de puerto	Origen	Tipo de tráfico
Regla TCP personalizada	TCP	3389	Mi dirección IP	Escritorio remoto
All Traffic	Todos	Todos	10.0.0.0/16	Todo el tráfico local de VPC

Reglas de salida del grupo de seguridad para -DS-VPC01 AWS

Tipo	Protocolo	Rango de puerto	Destino	Tipo de tráfico
All Traffic	Todos	Todos	0.0.0.0/0	Todo el tráfico

AWS- Información del grupo de seguridad -VPC01: OnPrem
Nombre del grupo de seguridad: AWS OnPrem Test Lab Security Group.
Descripción: Grupo de seguridad de AWS OnPrem Test Lab.
VPC: vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Reglas de entrada de grupos de seguridad para - AWS-VPC01 OnPrem

Tipo	Protocolo	Rango de puerto	Origen	Tipo de tráfico
Regla TCP personalizada	TCP	3389	Mi dirección IP	Escritorio remoto
Regla TCP personalizada	TCP	53	10.0.0.0/16	DNS
Regla TCP personalizada	TCP	88	10.0.0.0/16	Kerberos
Regla TCP personalizada	TCP	389	10.0.0.0/16	LDAP
Regla TCP personalizada	TCP	464	10.0.0.0/16	Cambiar/e stablecer contraseña de Kerberos
Regla TCP personalizada	TCP	445	10.0.0.0/16	SMB/CIFS
Regla TCP personalizada	TCP	135	10.0.0.0/16	Replicación
Regla TCP personalizada	TCP	636	10.0.0.0/16	LDAP SSL

Tipo	Protocolo	Rango de puerto	Origen	Tipo de tráfico
Regla TCP personalizada	TCP	49152 - 65535	10.0.0.0/16	RPC
Regla TCP personalizada	TCP	3268 - 3269	10.0.0.0/16	LDAP GC y LDAP GC SSL
Regla UDP personalizada	UDP	53	10.0.0.0/16	DNS
Regla UDP personalizada	UDP	88	10.0.0.0/16	Kerberos
Regla UDP personalizada	UDP	123	10.0.0.0/16	Hora de Windows
Regla UDP personalizada	UDP	389	10.0.0.0/16	LDAP
Regla UDP personalizada	UDP	464	10.0.0.0/16	Cambiar/e stablecer contraseña de Kerberos
All Traffic	Todos	Todos	10.100.0.0/16	Todo el tráfico local de VPC

Reglas de salida del grupo de seguridad para - -VPC01 AWS OnPrem

Tipo	Protocolo	Rango de puerto	Destino	Tipo de tráfico
All Traffic	Todos	Todos	0.0.0.0/0	Todo el tráfico

Para obtener instrucciones detalladas sobre cómo crear y agregar reglas a los grupos de seguridad, consulte Trabajar con grupos de seguridad.

Paso 2: Cree su Microsoft AD Active Directory AWS administrado

Puede utilizar tres métodos diferentes para crear su directorio. Puede usar el AWS Management Console procedimiento (recomendado para este tutorial) o puede usar los AWS Tools for Windows PowerShell procedimientos AWS CLI o para crear su directorio.

Método 1: para crear el directorio AWS administrado de Microsoft AD (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, elija Directorios y, a continuación, elija Configurar directorio.
2. En la página Seleccionar tipo de directorio, elija AWS Managed Microsoft AD y, a continuación, elija Siguiente.
3. En la página Enter directory information (Especifique la información del directorio), proporcione la información siguiente y, a continuación, elija Next (Siguiente).
   - En Edition (Edición), seleccione la edición Standard Edition o Enterprise Edition. Para obtener más información acerca de las ediciones, consulte AWS Directory Service para Microsoft Active Directory.
   - En Directory DNS name (Nombre de DNS del directorio), escriba **`corp.example.com`**.
   - En Directory NetBIOS name (Nombre NetBIOS del directorio), escriba **`corp`**.
   - En Directory description (Descripción del directorio), escriba **`AWS DS Managed`**.
   - En Admin password, escriba la contraseña que quiera usar para esta cuenta y escriba de nuevo la contraseña en Confirm password. Esta cuenta de Admin se crea automáticamente durante el proceso de creación del directorio. La contraseña no puede incluir la palabra admin. La contraseña del administrador del directorio distingue entre mayúsculas y minúsculas y debe tener 8 caracteres como mínimo y 64 como máximo. También debe contener al menos un carácter de tres de las siguientes categorías:
     - Letras minúsculas (a-z)
     - Letras mayúsculas (A-Z)
     - Números (0-9)
     - Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
4. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la siguiente información y, a continuación, elija Next (Siguiente).
   - En VPC, elija la opción que comienza por AWS-DS-VPC01 y termina con (10.0.0.0/16).
   - En Subnets (Subredes), elija las subredes públicas 10.0.0.0/24 y 10.0.1.0/24.

5. En la página Review & create (Revisar y crear), revise la información del directorio y haga los cambios que sean necesarios. Cuando la información sea correcta, seleccione Create directory (Crear directorio). Se tarda entre 20 y 40 minutos en crear el directorio. Una vez creado, el valor Status cambia a Active.

Método 2: Para crear su Microsoft AD AWS administrado (Windows PowerShell) (opcional)

1. Abra Windows PowerShell.
2. Escriba el siguiente comando. Asegúrese de utilizar los valores proporcionados en el paso 4 del AWS Management Console procedimiento 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 crear su Microsoft AD AWS administrado (AWS CLI) (opcional)

1. Abre el AWS CLI.
2. Escriba el siguiente comando. Asegúrese de utilizar los valores proporcionados en el paso 4 del AWS Management Console procedimiento 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
```

Paso 3: Implemente una instancia de Amazon EC2 para gestionar su Active Directory gestionado de AWS Microsoft AD

Para este laboratorio, utilizamos instancias de Amazon EC2 que tienen direcciones IP públicas para facilitar el acceso a la instancia de administración desde cualquier lugar. En un entorno de producción, puede usar instancias que estén en una VPC privada a la que solo se pueda acceder a través de una VPN o AWS Direct Connect un enlace. No es necesario que la instancia tenga una dirección IP pública.

En esta sección, veremos las distintas tareas posteriores a la implementación necesarias para que los equipos clientes se conecten a su dominio con el servidor Windows Server de su nueva instancia

EC2. Puede utilizar el servidor Windows Server en el siguiente paso para verificar que el laboratorio funcione.

Opcional: cree un conjunto de opciones de DHCP en AWS-DS-VPC01 para su directorio

En este procedimiento opcional, debe configurar un ámbito de opciones de DHCP para que las instancias EC2 de su VPC utilicen automáticamente su AWS Microsoft AD administrado para la resolución de DNS. Para obtener más información, consulte Conjuntos de opciones de DHCP.

Creación de un conjunto de opciones de DHCP para un directorio

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija DHCP Options Sets y, a continuación, elija Create DHCP options set.
3. En la página Create DHCP options set (Crear conjunto de opciones de DHCP), facilite los siguientes valores para el directorio:
   - En Name (Nombre), escriba **`AWS DS DHCP`**.
   - En Domain name (Nombre del dominio), escriba **`corp.example.com`**.
   - En Domain name servers (Servidores de nombres de dominio), introduzca las direcciones IP de los servidores DNS de su directorio de AWS proporcionado.

     > **Note**
     >
     > Para buscar estas direcciones, vaya a la página de AWS Directory Service directorios y, a continuación, elija el ID de directorio correspondiente. En la página Detalles, identifique y utilice las IP que aparecen en la dirección DNS.
     > Como alternativa, para buscar estas direcciones, vaya a la página Directorios de AWS Directory Service y, a continuación, elija el identificador de directorio correspondiente. A continuación, seleccione Escalar y compartir. En Controladores de dominio, identifique y use las IP que aparecen en Dirección IP.

   - Deje las opciones en blanco para NTP servers, NetBIOS name servers y NetBIOS node type.
4. Seleccione Create DHCP options set (Crear conjunto de opciones de DHCP) y, a continuación, elija Close (Cerrar). El nuevo conjunto de opciones de DHCP aparecerá en la lista de opciones de DHCP.
5. Anote el ID del nuevo conjunto de opciones de DHCP (dopt-***xxxxxxxx***). Debe usarlo al final de este procedimiento para asociar el nuevo conjunto de opciones a su VPC.

> **Note**
>
> La integración sencilla en un dominio funciona sin tener que configurar un conjunto de opciones DHCP.

6. En el panel de navegación, elija Your VPCs (Sus VPC).
7. En la lista de VPC, seleccione AWS DS VPC, elija Acciones y, a continuación, elija Editar conjunto de opciones de DHCP.
8. En la página Edit DHCP options set (Editar conjunto de opciones de DHCP), seleccione el conjunto de opciones registrado en el paso 5 y, a continuación, seleccione Save (Guardar).

Cree un rol para unir las instancias de Windows a su dominio de Microsoft AD AWS administrado

Utilice este procedimiento para configurar un rol que une una instancia de Amazon EC2 para Windows a un dominio. Para obtener más información, consulte Unir sin problemas una instancia de Amazon EC2 para Windows a su AWS Microsoft AD gestionado Active Directory.

Configuración de EC2 para unir instancias de Windows a su dominio

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, elija Crear rol.
3. En Seleccionar tipo de entidad de confianza, seleccione Servicio de AWS .
4. Justo debajo de Choose the service that will use this role (Elegir el servicio que utilizará este rol), elija EC2 y, a continuación, elija Next: Permissions (Siguiente: Permisos).
5. En la página Attached permissions policy (Asociar política de permisos), haga lo siguiente:
   - Seleccione la casilla situada junto a la política gestionada de AmazonSSM. ManagedInstanceCore Esta política proporciona los permisos mínimos necesarios para utilizar el servicio de Systems Manager.
   - Seleccione la casilla situada junto a la política gestionada de AmazonSSM DirectoryServiceAccess. La política proporciona los permisos para unir instancias a un Active Directory administrado por AWS Directory Service.

Para obtener información acerca de estas políticas administradas y otras políticas que puede asociar a un perfil de instancia de IAM de Systems Manager, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager . Para obtener más información sobre las políticas administradas, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

6. Elija Next: Tags (Siguiente: Etiquetas).
7. (Opcional) Añada uno o varios pares clave-valor de etiqueta para organizar, realizar un seguimiento o controlar el acceso a este rol y, a continuación, elija Next: Review (Siguiente: Revisar).
8. En Nombre del rol, introduzca un nombre para el rol que describa que se usa para unir instancias a un dominio, como EC2. DomainJoin
9. (Opcional) En Role description (Descripción del rol), escriba una descripción.
10. Elija Create role. El sistema le devuelve a la página Roles.

Cree una instancia de Amazon EC2 y únase automáticamente al directorio

En este procedimiento, configura un sistema Windows Server en una instancia EC2 que se puede utilizar más adelante para administrar usuarios, grupos y políticas en Active Directory.

Creación de una instancia EC2 y unión automática al directorio

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Iniciar instancia.
3. En la página Step 1 (Paso 1), junto a Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx*** elija Select (Seleccionar).
4. En la página Step 2 (Paso 2), seleccione t3.micro (tenga en cuenta que puede elegir un tipo de instancia más grande) y después elija Next: Configure Instance Details (Siguiente: Configurar detalles de instancia).
5. En la página Step 3, haga lo siguiente:
   - En Red, elija la VPC que termina con AWS-DS-VPC01 (por ejemplo, vpc-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01).

- En Subred elija Subred pública 1, que debería estar preconfigurada para su zona de disponibilidad preferida (por ejemplo, subnet-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01-Subnet01 | ***us-west-2a***).
- Para Auto-assign Public IP, elija Enable (si el ajuste de subred no está establecido como habilitado de forma predeterminada).
- Para Domain join directory, seleccione corp.example.com (d-***xxxxxxxxxx***).
- Para el rol de IAM, elija el nombre con el que asignó el rol de la instanciaCree un rol para unir las instancias de Windows a su dominio de Microsoft AD AWS administrado, como EC2. DomainJoin
- No cambie el resto de los valores predeterminados de los demás ajustes.
- Elija Siguiente: Agregar almacenamiento.

6. En la página Step 4, deje la configuración predeterminada y, a continuación, elija Next: Add Tags.
7. En la página Step 5, elija Add Tag. En Key (Clave), escriba **`corp.example.com-mgmt`** y, a continuación, elija Next: Configure Security Group (Siguiente: Configurar grupo de seguridad).
8. En la página Paso 6, elija Seleccionar un grupo de seguridad existente, seleccione Grupo de seguridad del laboratorio de pruebas de AWS DS (que configuró anteriormente en el Tutorial básico) y, a continuación, elija Revisar y lanzar para revisar la instancia.
9. En la página Step 7, revise la página y, a continuación, seleccione Launch.
10. En el cuadro de diálogo Select an existing key pair or create a new key pair, proceda del modo siguiente:
    - Elija Choose an existing key pair.
    - En Seleccionar un par de claves, elija AWS-DS-KP.
    - Active la casilla I acknowledge....
    - Elija Launch Instances.
11. Elija Ver instancias para volver a la consola de Amazon EC2 y ver el estado de la implementación.

Instalación de las herramientas de Active Directory en su instancia de EC2

Puede elegir entre dos métodos para instalar las herramientas de administración del dominio de Active Directory en su instancia EC2. Puedes usar la interfaz de usuario del administrador de servidores (recomendada para este tutorial) o. Windows PowerShell

Para instalar las herramientas de Active Directory en su instancia de EC2 (Server Manager)

1. En la consola de Amazon EC2, elija Instancias, seleccione la instancia que acaba de crear y, a continuación, elija Conectar.
2. En el cuadro de diálogo Connect To Your Instance (Conectar s su instancia), elija Get Password (Obtener contraseña) para recuperar la contraseña si no lo ha hecho aún y, a continuación, elija Download Remote Desktop File (Descargar archivo de escritorio remoto).
3. En el cuadro de diálogo Windows Security (Seguridad de Windows), escriba sus credenciales de administrador local para que el equipo con Windows Server inicie sesión (por ejemplo, **`administrator`**).
4. En el menú Inicio, elija Administrador del servidor.
5. En Panel, elija Agregar roles y características.
6. En Asistente para agregar roles y características, elija Siguiente.
7. En la página Seleccionar tipo de instalación, elija Instalación basada en características o en roles y, a continuación, elija Siguiente.
8. En la página Seleccionar servidor de destino, asegúrese de que se selecciona el servidor local y, a continuación, elija Siguiente.
9. En la página }Seleccionar roles de servidor, elija Siguiente.
10. En la página Seleccionar características, haga lo siguiente:
    - Active la casilla de verificación Administración de directivas de grupo.
    - Amplíe Herramientas de administración remota del servidor y, a continuación, expanda Herramientas de administración de roles.
    - Active la casilla de verificación Herramientas de AD DS y AD LDS.
    - Active la casilla de verificación de herramientas de servidor DNS.
    - Elija Siguiente.
11. En la página de Confirmar selecciones de instalación, revise la información y seleccione Instalar. Cuando haya terminado la instalación de la característica, las siguientes herramientas o

complementos estarán disponibles en la carpeta Herramientas administrativas de Windows en el menú Inicio.

- Centro de administración de Active Directory
- Dominios y relaciones de confianza de Active Directory
- Módulo Active Directory para Windows PowerShell
- Sitios y servicios de Active Directory
- Usuarios y equipos de Active Directory
- Edición ADSI
- DNS
- Administración de políticas de grupo

Para instalar las herramientas de Active Directory en su instancia EC2 (Windows PowerShell) (opcional)

1. Inicie Windows PowerShell.
2. Escriba el siguiente comando.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-
Tools,RSAT-DNS-Server
```

Paso 4: verificación de que el laboratorio de pruebas base esté operativo

Utilice el siguiente procedimiento para verificar que el laboratorio de pruebas se ha configurado correctamente antes de agregar módulos de guía adicionales del laboratorio de pruebas. Este procedimiento comprueba que Windows Server esté configurado correctamente, que se pueda conectar al dominio corp.example.com y que se utilice para administrar el bosque administrado de AWS Microsoft AD.

Verificación de que el laboratorio de pruebas esté operativo

1. Cierre sesión en la instancia EC2 en la que hubiera iniciado sesión como administrador local.
2. En la consola de Amazon EC2, elija Instancias en el panel de navegación. A continuación, seleccione la instancia que creó. Elija Conectar.
3. En el cuadro de diálogo Connect To Your Instance, elija Download Remote Desktop File.

4. En el cuadro de diálogo Windows Security (Seguridad de Windows), escriba sus credenciales de administrador para el dominio CORP para iniciar sesión (por ejemplo, **`corp\admin`**).
5. Una vez que haya iniciado sesión, en el menú Inicio, bajo Herramientas administrativas de Windows, seleccione Usuarios y equipos de Active Directory.
6. Debería poder ver corp.example.com con todas las unidades organizativas y cuentas predeterminadas asociadas a un nuevo dominio. En Controladores de dominio, observe los nombres de los controladores de dominio que se crearon automáticamente al crear su Microsoft AD AWS administrado en el paso 2 de este tutorial.

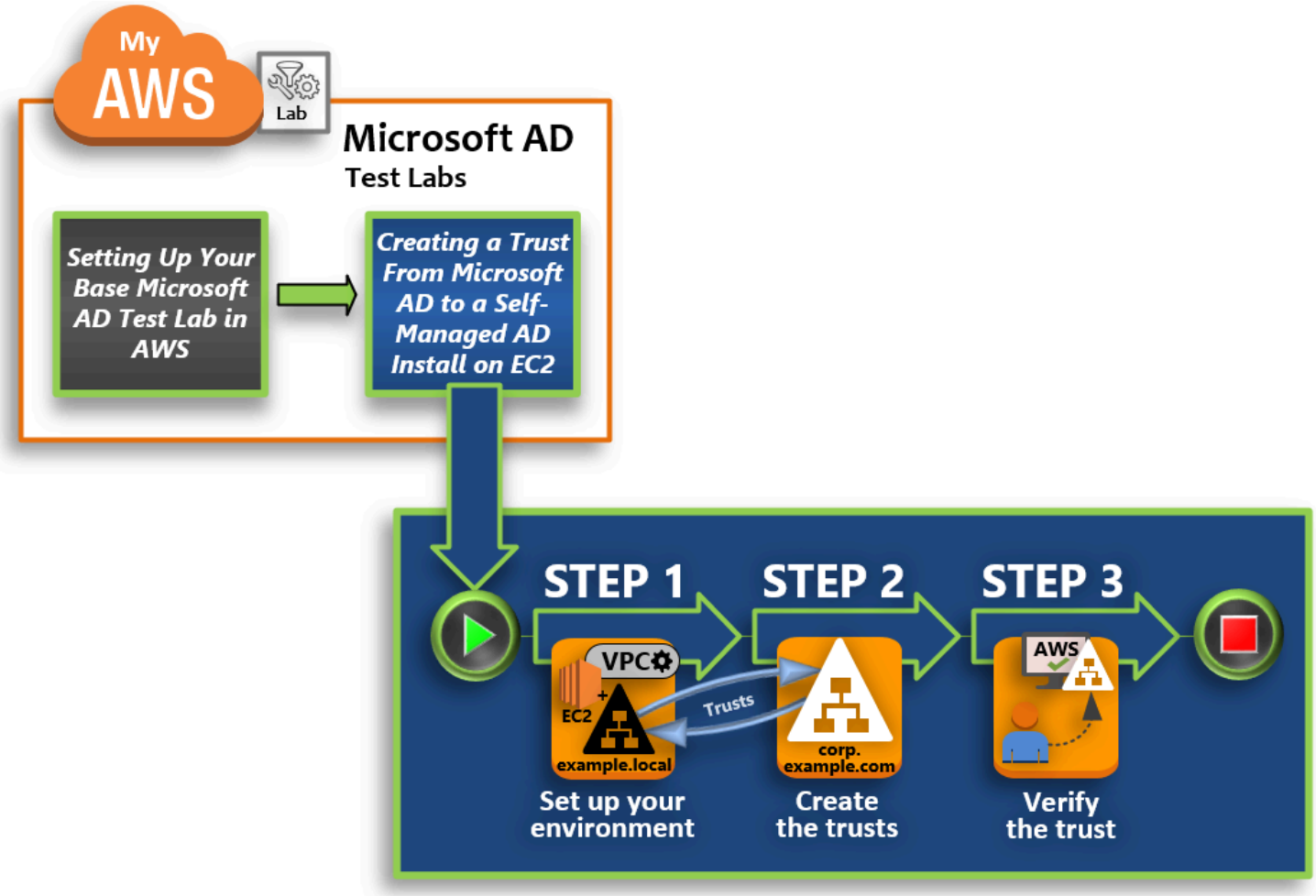
¡Enhorabuena! Ya se ha configurado su entorno de laboratorio de pruebas base AWS administrado de Microsoft AD. Está preparado para empezar a agregar el siguiente laboratorio de pruebas de la serie.

Siguiente tutorial: Tutorial: Creación de una confianza desde Microsoft AD AWS gestionado a una instalación autogestionada de Active Directory en Amazon EC2

Tutorial: Creación de una confianza desde Microsoft AD AWS gestionado a una instalación autogestionada de Active Directory en Amazon EC2

En este tutorial, aprenderá a crear una confianza entre el bosque de AWS Directory Service para Microsoft Active Directory que creó en el tutorial básico. También aprenderá a crear un nuevo bosque de Active Directory nativo en un servidor Windows Server en Amazon EC2. Como se muestra en la siguiente ilustración, el laboratorio que cree a partir de este tutorial es el segundo componente necesario para configurar un laboratorio de pruebas de Microsoft AD AWS administrado completo. Puede usar el laboratorio de pruebas para probar sus soluciones basadas exclusivamente en la nube o en la nube híbrida AWS .

Solo deberá crear este tutorial una vez. A continuación, podrá añadir tutoriales opcionales cuando sea necesario para conseguir más experiencia.



Paso 1: configuración del entorno para las relaciones de confianza

Antes de poder establecer relaciones de confianza entre un nuevo bosque de Active Directory y el bosque de AWS Managed Microsoft AD que creó en el Tutorial básico, tiene que preparar su entorno de Amazon EC2. Para ello, primero deberá crear un servidor Windows Server 2019, promocionar ese servidor a un controlador de dominio y, a continuación, configurar su VPC en consecuencia.

Paso 2: creación de las relaciones de confianza

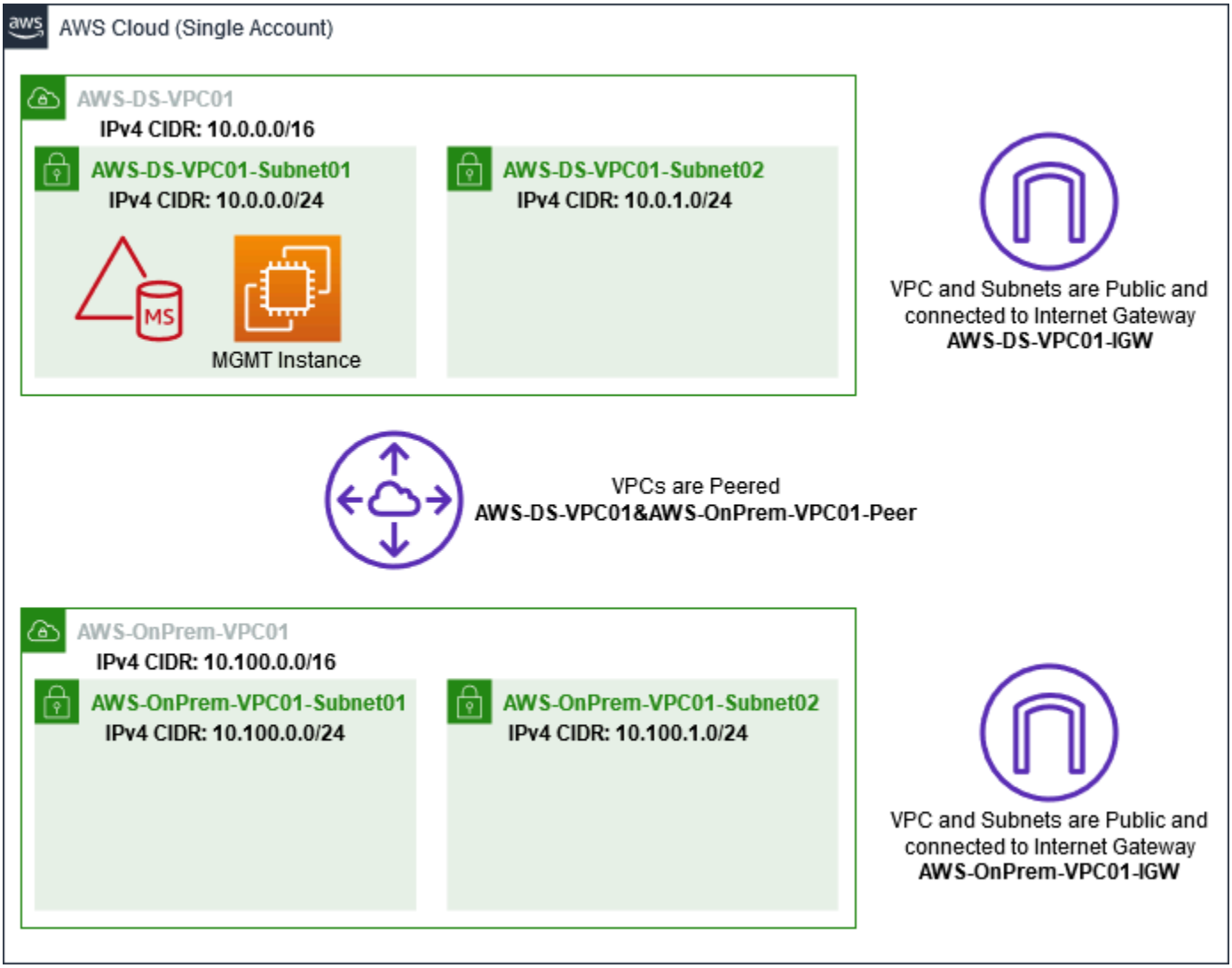
En este paso, creará una relación de confianza bidireccional entre el bosque de Active Directory recién creado alojado en Amazon EC2 y el bosque AWS gestionado de Microsoft AD en. AWS

Paso 3: comprobación de la relación de confianza

Por último, como administrador, utiliza la AWS Directory Service consola para comprobar que las nuevas confianzas están operativas.

Paso 1: configuración del entorno para las relaciones de confianza

En esta sección, configurará su entorno Amazon EC2, implementará su nuevo bosque y preparará su VPC para las confianzas. AWS



Creación de una instancia de EC2 de Windows Server 2019

Siga este procedimiento para crear un servidor miembro de Windows Server 2019 en Amazon EC2.

Creación de una instancia EC2 de Windows Server 2019

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la consola de Amazon EC2, elija Lanzar instancia.
3. En la página Step 1 (Paso 1), busque Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx*** en la lista. A continuación, elija Seleccionar.

4. En la página Step 2, seleccione t2.large y, a continuación, elija Next: Configure Instance Details.
5. En la página Step 3, haga lo siguiente:
   - Para Network, seleccione vpc- ***xxxxxxxxxxxxxxxxx*** AWS- OnPrem -VPC01 (que ya configuró en el tutorial básico).
   - *Para* ***Subnet, seleccione subnet- xxxxxxxxxxxxxxxxx | - -VPC01-Subnet01 | - -VPC01.*** AWS OnPrem AWS OnPrem
   - En la lista Auto-assign Public IP, elija Enable (si el ajuste de subred no está ajustado en Enable de forma predeterminada).
   - No cambie el resto de los valores predeterminados de los demás ajustes.
   - Elija Siguiente: Añadir almacenamiento.
6. En la página Step 4, deje la configuración predeterminada y, a continuación, elija Next: Add Tags.
7. En la página Step 5, elija Add Tag. En Key (Clave), escriba **`example.local-DC01`** y, a continuación, elija Next: Configure Security Group (Siguiente: Configurar grupo de seguridad).
8. En la página Paso 6, elija Seleccionar un grupo de seguridad existente, seleccione Grupo de seguridad del laboratorio de pruebas de AWS On-Prem (que configuró anteriormente en el Tutorial básico) y, a continuación, elija Revisar y lanzar para revisar la instancia.
9. En la página Step 7, revise la página y, a continuación, seleccione Launch.
10. En el cuadro de diálogo Select an existing key pair or create a new key pair, proceda del modo siguiente:
    - Elija Choose an existing key pair.
    - En Seleccionar un par de claves, elija AWS-DS-KP (que configuró anteriormente en el Tutorial básico).
    - Active la casilla I acknowledge....
    - Elija Launch Instances.
11. Elija Ver instancias para volver a la consola de Amazon EC2 y ver el estado de la implementación.

Promoción de su servidor a controlador de dominio

Antes de poder crear relaciones de confianza, debe crear e implementar el primer controlador de dominio para un nuevo bosque. Durante este proceso, puede configurar un nuevo bosque de Active

Directory, instalar DNS y establecer este servidor para usar el servidor DNS local para la resolución de nombres. Debe reiniciar el servidor al final de este procedimiento.

> **Note**
>
> Si desea crear un controlador de dominio que se AWS replique con su red local, primero debe unir manualmente la instancia EC2 a su dominio local. Hecho esto, podrá promocionar el servidor a un controlador de dominio.

Para promocionar su servidor a un controlador de dominio

1. En la consola de Amazon EC2, elija Instancias, seleccione la instancia que acaba de crear y, a continuación, elija Conectar.
2. En el cuadro de diálogo Connect To Your Instance, elija Download Remote Desktop File.
3. En el cuadro de diálogo Windows Security (Seguridad de Windows), escriba sus credenciales de administrador local para que el equipo con Windows Server inicie sesión (por ejemplo, **`administrator`**). Si aún no tiene la contraseña de administrador local, vuelva a la consola de Amazon EC2, haga clic con el botón derecho en la instancia y elija Obtener contraseña de Windows. Vaya a su archivo `AWS DS KP.pem` o a su clave personal `.pem` y, a continuación, elija Decrypt Password.
4. En el menú Inicio, elija Administrador del servidor.
5. En Panel, elija Agregar roles y características.
6. En Asistente para agregar roles y características, elija Siguiente.
7. En la página Seleccionar tipo de instalación, elija Instalación basada en características o en roles y, a continuación, elija Siguiente.
8. En la página Seleccionar servidor de destino, asegúrese de que se selecciona el servidor local y, a continuación, elija Siguiente.
9. En la página Seleccionar roles de servidor, seleccione Servicios de dominio de Active Directory. En el cuadro de diálogo Asistente para agregar roles y características, compruebe que se activa la casilla Incluir herramientas de administración (si es aplicable). Elija Agregar características y, luego, seleccione Siguiente.
10. En la página Seleccionar características, elija Siguiente.
11. En la página Servicios de dominio de Active Directory, elija Siguiente.
12. En la página Confirmar selecciones de instalación, elija Instalar.

13. Una vez instalados los binarios de Active Directory, elija Cerrar.
14. Al abrirse el administrador del servidor, busque una marca en la parte superior junto a la palabra Administrar. Cuando esta marca pase a color amarillo, el servidor estará listo para promocionarse.
15. Elija la marca amarilla y, a continuación, elija Promover este servidor a controlador de dominio.
16. En la página Configuración de implementación, elija Agregar un nuevo bosque. En Nombre del dominio raíz, escriba **`example.local`** y, a continuación, elija Siguiente.
17. En la página Opciones del controlador de dominio, haga lo siguiente:
    - Tanto en Nivel funcional de bosque como en Nivel funcional del dominio, elija Windows Server 2016.
    - En Especificar las capacidades del controlador de dominio, compruebe que estén seleccionados tanto el servidor DNS como el Catálogo global (GC).
    - Escriba y, a continuación, confirme una contraseña de Directory Services Restore Mode (DSRM). A continuación, elija Next.
18. En la página Opciones de DNS, ignore la advertencia sobre delegación y elija Siguiente.
19. En la página de opciones adicionales, asegúrese de que EXAMPLE aparezca como nombre de NetBios dominio.
20. En la página Rutas, deje los valores predeterminados y seleccione Siguiente.
21. En la página Revisar opciones, seleccione Siguiente. El servidor realiza ahora comprobaciones para asegurarse de que se cumplen todos los requisitos previos para el controlador de dominio. Si bien pueden aparecer algunas advertencias, puede ignorarlas de forma segura.
22. Elija Instalar. Una vez realizada la instalación, el servidor se reinicia y, a continuación, pasa a ser un controlador de dominio funcional.

Configure la VPC

Los tres procedimientos siguientes le guían a través de los pasos para configurar su VPC a fin de establecer conectividad con AWS.

Configuración de las reglas de salida de la VPC

1. En la AWS Directory Service consola, anote el ID del directorio AWS administrado de Microsoft AD para corp.example.com que creó anteriormente en el tutorial básico.
2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

3. En el panel de navegación, elija Security Groups (Grupos de seguridad).
4. Busca tu ID de directorio AWS administrado de Microsoft AD. En los resultados de búsqueda, seleccione el elemento que tiene la descripción Grupo de seguridad de AWS creado para los controladores de directorio d-***xxxxxx***.

> **Note**
>
> Este grupo de seguridad se creó automáticamente en el momento de crearse su directorio.

5. Elija la pestaña Outbound Rules en ese grupo de seguridad. Elija Edit y Add another rule y, a continuación, añada los siguientes valores:
   - En Type, seleccione All Traffic.
   - En Destination, escriba **`0.0.0.0/0`**.
   - No cambie el resto de los valores predeterminados de los demás ajustes.
   - Seleccione Guardar.

Para comprobar que la autenticación previa de Kerberos está habilitada

1. En el controlador de dominio example.local, abra Administrador del servidor.
2. En el menú Herramientas, elija Usuarios y equipos de Active Directory.
3. Vaya al directorio Usuarios, haga clic con el botón derecho en cualquier usuario y seleccione Propiedades y, a continuación, elija la pestaña Cuenta. En la lista Opciones de la cuenta, desplácese hacia abajo y asegúrese de que No pedir la autenticación Kerberos previa no esté seleccionado.
4. Siga los mismos pasos para el dominio corp.example.com en la instancia de corp.example.com-mgmt .

Configuración de programas de envío condicionales DNS

> **Note**
>
> Un reenviador condicional es un servidor DNS en una red que se utiliza para reenviar consultas DNS según el nombre de dominio DNS de la consulta. Por ejemplo, un servidor DNS puede configurarse para reenviar todas las consultas que recibe para los nombres que

terminan con widgets.example.com a la dirección IP de un servidor DNS específico o a las direcciones IP de varios servidores DNS.

1. Abra la consola de AWS Directory Service.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el ID de directorio de su Microsoft AD AWS administrado.
4. Tome nota del nombre de dominio completo (FQDN), corp.example.com, y las direcciones DNS de su directorio.
5. Ahora, vuelva a su controlador de dominio example.local y, a continuación, abra Administrador del servidor.
6. En el menú Herramientas, elija DNS.
7. En el árbol de la consola, amplíe el servidor DNS del dominio para el cual esté configurando la confianza y vaya a Reenviadores condicionales.
8. Haga clic con el botón derecho en Reenviadores condicionales y, a continuación, elija Nuevo reenviador condicional.
9. En Dominio DNS, escriba **`corp.example.com`**.
10. En Direcciones IP de los servidores principales, seleccione <Haga clic aquí para añadir... >, escriba la primera dirección DNS del directorio AWS administrado de Microsoft AD (que anotó en el procedimiento anterior) y, a continuación, presione Entrar. Haga lo mismo para la segunda dirección DNS. Después de escribir las direcciones DNS, es posible que aparezca un error que indique que se ha agotado el tiempo de espera o que no se pudo resolver la operación. Por lo general, puede ignorar estos errores.
11. Active la casilla Almacenar este reenviador condicional en Active Directory y replicarlo como sigue. En el menú desplegable, elija Todos los servidores DNS en este bosque y, a continuación, elija Aceptar.

Paso 2: creación de las relaciones de confianza

En esta sección creará dos relaciones de confianza entre bosques independientes. Una confianza se crea a partir del dominio de Active Directory de la instancia EC2 y la otra a partir de su Microsoft AD AWS administrado en AWS.

Para crear la confianza de su dominio EC2 a su Microsoft AWS AD administrado

1. Inicie sesión en example.local.
2. Abra Administrador del servidor y, en el árbol de la consola, elija DNS. Anote la dirección IPv4 que aparece para el servidor. La necesitará en el siguiente procedimiento cuando cree un programa de envío condicional a partir de corp.example.com para el directorio example.local.
3. En el menú Herramientas, elija Dominios y confianzas de Active Directory.
4. En el árbol de la consola, haga clic con el botón derecho en example.local y, a continuación, elija Propiedades.
5. En la pestaña Confianzas, elija Nueva confianza y, a continuación, elija Siguiente.
6. En la página Nombre de confianza, escriba **`corp.example.com`** y, a continuación, elija Siguiente.
7. En la página Tipo de confianza, elija Confianza de bosque y, a continuación, elija Siguiente.

> **Note**
>
> AWS Managed Microsoft AD también admite confianzas externas. Sin embargo, para este tutorial, creará una relación de confianza bidireccional entre bosques.

8. En la página Dirección de confianza, elija Bidireccional y, a continuación, elija Siguiente.

> **Note**
>
> Si decide más adelante probar esto con una relación de confianza unidireccional en su lugar, asegúrese de que las direcciones de la relación de confianza estén configuradas correctamente (salientes en el dominio origen de la confianza, entrantes en el dominio destino de la confianza). Para obtener información general, consulte Descripción de la dirección de la relación de confianza en el sitio web de Microsoft.

9. En la página Partes de la relación de confianza, elija Solo este dominio y, a continuación, elija Siguiente.
10. En la página Nivel de autenticación de confianza saliente, elija autenticación en todo el bosque y, a continuación, elija Siguiente.

> **Note**
>
> Aunque encuentre Selective authentication (Autenticación selectiva) como opción, por motivos de simplicidad, le recomendamos que no la habilite en este momento. Cuando se configura, restringe el acceso a través de una relación de confianza externa o de bosque solo a los usuarios de un dominio o bosque de confianza a los que se hayan concedido explícitamente permisos de autenticación a objetos de equipo (equipos de recursos) que residen en el dominio o bosque de confianza. Para obtener más información, consulte Configurar la autenticación selectiva.

11. En la página Contraseña de la confianza, escriba la contraseña de confianza dos veces y, a continuación, elija Siguiente. Usará esta misma contraseña en el siguiente procedimiento.
12. En la página Se ha completado la selección de confianzas, revise los resultados y, a continuación, elija Siguiente.
13. En la página Se ha completado la creación de confianzas, revise los resultados y, a continuación, elija Siguiente.
14. En la página Confirmar confianza saliente, elija No, no confirmar la confianza saliente. A continuación, elija Siguiente
15. En la página Confirmar confianza entrante, elija No, no confirmar la confianza entrante. A continuación, elija Siguiente
16. En la página Finalización del Asistente para nueva confianza, elija Finalizar.

> **Note**
>
> Las relaciones de confianza son una característica global de AWS Managed Microsoft AD. Si está utilizando Replicación multirregional, se deben seguir estos procedimientos en Región principal . Los cambios se aplicarán automáticamente en todas las regiones replicadas. Para obtener más información, consulte Características globales frente a las regionales.

Para crear la confianza de su Microsoft AD AWS administrado a su dominio EC2

1. Abra la consola de AWS Directory Service.
2. Elija el directorio corp.example.com.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.
4. En la sección Trust relationships (Relaciones de confianza), elija Actions (Acciones) y, a continuación, seleccione Add trust relationship (Añadir relación de confianza).
5. En el cuadro de diálogo Add a trust relationship, haga lo siguiente:
   - En Trust type (Tipo de relación de confianza) seleccione Forest trust (Confianza de bosque).

     > **Note**
     >
     > Asegúrese de que el tipo de confianza que elija aquí coincida con el mismo tipo de confianza configurado en el procedimiento anterior (para crear la confianza de su dominio EC2 en su Microsoft AD AWS administrado).

   - En Existing or new remote domain name (Nombre de dominio remoto existente o nuevo), escriba example.local.
   - En Trust password, escriba la misma contraseña que proporcionó en el procedimiento anterior.
   - En Trust direction (Dirección de confianza), seleccione Two-way (Bidireccional).

     > **Note**
     >
     > - Si decide más adelante probar esto con una relación de confianza unidireccional en su lugar, asegúrese de que las direcciones de la relación de confianza estén configuradas correctamente (salientes en el dominio origen de la confianza, entrantes en el dominio destino de la confianza). Para obtener información general, consulte Descripción de la dirección de la relación de confianza en el sitio web de Microsoft.

- Aunque encuentre Selective authentication (Autenticación selectiva) como opción, por motivos de simplicidad, le recomendamos que no la habilite en este momento. Cuando se configura, restringe el acceso a través de una relación de confianza externa o de bosque solo a los usuarios de un dominio o bosque de confianza a los que se hayan concedido explícitamente permisos de autenticación a objetos de equipo (equipos de recursos) que residen en el dominio o bosque de confianza. Para obtener más información, consulte Configurar la autenticación selectiva.

- En Conditional forwarder (Reenviador condicional), escriba la dirección IP de su servidor DNS en el bosque example.local (que anotó en el procedimiento anterior).

> **Note**
>
> Un reenviador condicional es un servidor DNS en una red que se utiliza para reenviar consultas DNS según el nombre de dominio DNS de la consulta. Por ejemplo, un servidor DNS puede configurarse para reenviar todas las consultas que recibe para los nombres que terminan con widgets.example.com a la dirección IP de un servidor DNS específico o a las direcciones IP de varios servidores DNS.

6. Elija Añadir.

Paso 3: comprobación de la relación de confianza

En esta sección probará si las relaciones de confianza se configuraron correctamente entre AWS y Active Directory en Amazon EC2.

Verificación de la confianza

1. Abra la consola de AWS Directory Service.
2. Elija el directorio corp.example.com.
3. En la página Detalles del directorio, lleve a cabo una de las siguientes operaciones:
   - Si tiene varias regiones en la sección Replicación multirregional, seleccione la región principal y, a continuación, elija la pestaña Redes y seguridad. Para obtener más información, consulte Regiones principales frente a las adicionales.
   - Si no aparece ninguna región en la sección Replicación multirregional, seleccione la pestaña Redes y seguridad.

4. En la sección Trust relationships (Relaciones de confianza), seleccione la relación de confianza que acaba de crear.
5. Elija Actions y, a continuación, elija Verify trust relationship.

Una vez completada la verificación, debería ver Verified bajo la columna Status.

¡Enhorabuena por completar este tutorial! Ahora tiene un entorno de Active Directory de bosques múltiples totalmente funcional a partir del cual puede empezar a probar diversos escenarios. Están previstos tutoriales del laboratorio de prueba adicionales en 2018, de modo que consulte de vez en cuando para ver las novedades.

Solución de problemas de Microsoft AD AWS administrado

La siguiente información puede ayudarle a solucionar algunos problemas comunes que podría encontrar a la hora de crear o utilizar el directorio.

Problemas con su Microsoft AD AWS administrado

Algunas tareas de solución de problemas solo se pueden completar con AWS Support. Estas son algunas de las tareas:

- Reiniciar los controladores de dominio AWS Directory Service proporcionados.
- Actualice su Microsoft AD AWS administrado.

Para crear un caso de soporte, consulte Creación de casos de soporte y administración de casos.

Problemas con el inicio de sesión en línea y las comunicaciones por canales seguros

Como medida de mitigación contra la CVE-2020-1472, Microsoft ha publicado un parche que modifica la forma en que los controladores de dominio procesan las comunicaciones del canal seguro de Netlogon. Desde la introducción de estos cambios de Netlogon seguro, es posible que su Microsoft AD administrado no acepte algunas conexiones de Netlogon (servidores, estaciones de trabajo y validaciones de confianza). AWS

Para comprobar si tu problema está relacionado con el inicio de sesión en la red o con las comunicaciones por canales seguros, busca en Amazon CloudWatch Logs los ID de evento

5827 (para problemas relacionados con la autenticación de dispositivos) o 5828 (para problemas relacionados con la validación de confianza de AD). Para obtener información sobre CloudWatch Microsoft AD AWS administrado, consulteHabilitación del reenvío de registros.

Para obtener más información sobre la mitigación de la CVE-2020-1472, consulte How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 en el sitio web de Microsoft.

Problemas con el restablecimiento de la contraseña del usuario

Al intentar restablecer la contraseña de un usuario, recibe un mensaje de error similar al siguiente:

```
Response Status: 400 Bad Request
```

Este problema puede producirse cuando hay objetos duplicados en la unidad organizativa (OU) AWS gestionada de Microsoft AD con nombres de inicio de sesión de usuario idénticos. Los nombres de inicio de sesión de los usuarios deben ser únicos. Consulte la sección Solución de problemas de datos de directorio en Microsoft la documentación para obtener más información.

Recuperación de contraseña

Si un usuario olvida una contraseña o tiene problemas para iniciar sesión en el directorio Simple AD o AWS Managed Microsoft AD, puede restablecer su contraseña mediante el AWS Management Console, Windows PowerShell o el AWS CLI.

Para obtener más información, consulte Restablecimiento de la contraseña de un usuario.

Recursos adicionales

Los siguientes recursos pueden ayudarle a solucionar problemas a medida que trabaja con él. AWS

- AWS Centro de conocimiento: encuentre preguntas frecuentes y enlaces a otros recursos que le ayudarán a solucionar problemas.
- AWS Support Center: obtenga asistencia técnica.
- AWS Centro de soporte premium: obtenga soporte técnico premium.

Los siguientes recursos pueden ayudarle a solucionar problemas comunesActive Directory.

- Documentación de Active Directory

- AD DSSolución de problemas

Temas

Supervisión del servidor DNS con Visor de eventos de Microsoft

Puede auditar los eventos de DNS de AWS Managed Microsoft AD, lo que facilita la identificación y solución de problemas de DNS. Por ejemplo, si falta un registro de DNS, puede utilizar el log de eventos de auditoría de DNS para ayudar a identificar la causa raíz y solucionar el problema. También puede utilizar los logs de eventos de auditoría de DNS para mejorar la seguridad mediante la detección y el bloqueo de solicitudes procedentes de direcciones IP sospechosas.

Para ello, debe haber iniciado sesión en la cuenta Admin o en una cuenta que pertenezca al grupo de Administradores delegados de AWS para DNS. Para obtener más información sobre este grupo, consulte Qué se crea con su Active Directory AWS administrado de Microsoft AD.

Para acceder a Visor de eventos para el DNS de AWS Managed Microsoft AD

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Instances.
3. Localice una instancia de Amazon EC2 que se haya unido a su directorio de AWS Managed Microsoft AD. Seleccione la instancia y, a continuación, elija Connect (Conectar).
4. Una vez conectado a la instancia de Amazon EC2, abra el menú Inicio y seleccione la carpeta Herramientas administrativas de Windows. En la carpeta Herramientas administrativas, seleccione Visor de eventos.
5. En la ventana Visor de eventos, elija Acción y, a continuación, elija Conectarse a otro equipo.
6. Seleccione Otro equipo, escriba el nombre o la dirección IP de uno de sus servidores DNS de AWS Managed Microsoft AD y, a continuación, elija Aceptar.
7. En el panel izquierdo, vaya a Registros de aplicaciones y servicios>Microsoft>Windows>Servidor DNS y, a continuación, seleccione Auditar.

Errores de unión de dominio en Linux

Lo siguiente puede ayudarle a solucionar algunos mensajes de error que pueden aparecer al unir una instancia EC2 Linux a su directorio administrado de AWS Microsoft AD.

Instancias de Linux que no pueden unirse a dominio o autenticar

Las instancias de Ubuntu 14.04, 16.04 y 18.04 deben poder resolverse de forma inversa en el DNS para que un dominio pueda funcionar con Microsoft Active Directory. De lo contrario, se podría encontrar con uno de estos dos escenarios:

Escenario 1: Instancias de Ubuntu que aún no se han unido a un dominio

Para las instancias de Ubuntu que intentan unirse a un dominio, el comando `sudo realm join` no puede proporcionar los permisos necesarios para unirse al dominio y podría aparecer el siguiente error:

! Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) adcli: couldn't connect to EXAMPLE.COM domain: Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) ! Insufficient permissions to join the domain realm: Couldn't join realm: Insufficient permissions to join the domain

Escenario 2: Instancias de Ubuntu que se han unido a un dominio

En el caso de las instancias de Ubuntu que ya están unidas a un dominio de Microsoft Active Directory, los intentos de establecer SSH en la instancia con las credenciales del dominio pueden fallar y provocar los siguientes errores:

$ ssh admin@EJEMPLO.COM@198.51.100

no existe esa identidad: /Users/username/.ssh/id_ed25519: No existe ese archivo o directorio

Contraseña de admin@EJEMPLO.COM@198.51.100:

Permiso denegado. Inténtelo de nuevo más tarde.

Contraseña de admin@EJEMPLO.COM@198.51.100:

Si inicia sesión en la instancia con una clave pública y comprueba `/var/log/auth.log`, es posible que aparezcan los siguientes errores sobre la imposibilidad de encontrar al usuario:

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_unix(sshd:auth): authentication failure; 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): authentication failure; 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): received for user admin@EXAMPLE.COM: 10 (User not known to the underlying authentication module)

May 12 01:02:14 ip-192-0-2-0 sshd[2251]: Failed password for invalid user admin@EXAMPLE.COM from 203.0.113.0 port 13344 ssh2

May 12 01:02:15 ip-192-0-2-0 sshd[2251]: Connection closed by 203.0.113.0 [preauth]

Sin embargo, el `kinit` del usuario sigue funcionando. Consulte este ejemplo:

ubuntu@ip-192-0-2-0:~$ kinit admin@EXAMPLE.COM Password for admin@EXAMPLE.COM: ubuntu@ip-192-0-2-0:~$ klist Ticket cache: FILE:/tmp/krb5cc_1000 Default principal: admin@EXAMPLE.COM

Solución

La solución que se recomienda actualmente para estos dos escenarios es desactivar DNS inverso en `/etc/krb5.conf` en la sección [libdefaults], tal y como se muestra a continuación:

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Problema de autenticación de relación de confianza unidireccional con la unión de dominios fluida

Si ha establecido una confianza de salida unidireccional entre su Microsoft AD AWS administrado y su Active Directory local, es posible que se produzca un problema de autenticación al intentar autenticarse en la instancia de Linux unida al dominio mediante sus credenciales de Active Directory de confianza con Winbind.

Errores

Jul 31 00:00:00 EC2AMAZ-LSMWqT sshd[23832]: Failed password for user@corp.example.com from xxx.xxx.xxx.xxx port 18309 ssh2

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): getting password (0x00000390)

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): pam_get_item returned a password

31 de julio 00:05:00 EC2AMAZ-LSMWqt sshd [23832]: pam_winbind (sshd:auth): solicitud wbcLogonUser fallida: WBC_ERR_AUTH_ERROR, error PAM: PAM_SYSTEM_ERR (4), NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**, el mensaje de error era: No se encuentra el nombre del objeto.

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): internal module error (retval = PAM_SYSTEM_ERR(4), user = 'CORP\user')

Solución

Para resolver este problema, tendrá que comentar o eliminar una directiva del archivo de configuración del módulo PAM (`/etc/security/pam_winbind.conf`) siguiendo estos pasos.

1. Abra el archivo `/etc/security/pam_winbind.conf` en un editor de texto.

```
sudo vim /etc/security/pam_winbind.conf
```

2. Comente o elimine la siguiente directiva krb5_auth = yes.

```
[global]

cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. Detenga el servicio Winbind y vuelva a iniciarlo.

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

Poco espacio de almacenamiento disponible en Active Directory

Si su Microsoft AD AWS administrado está dañado debido a que Active Directory tiene poco espacio de almacenamiento disponible, es necesario tomar medidas inmediatas para devolver el directorio a un estado activo. Las dos causas más frecuentes de este deterioro se tratan en las siguientes secciones:

1. La carpeta SYSVOL almacena algo más que objetos esenciales de políticas de grupo
2. La base de datos de Active Directory está llena

Para obtener información sobre los precios del almacenamiento AWS administrado de Microsoft AD, consulte AWS Directory Service Precios.

La carpeta SYSVOL almacena algo más que objetos esenciales de políticas de grupo

Una causa frecuente de este deterioro es el almacenamiento de archivos no esenciales para el procesamiento de políticas de grupo en la carpeta SYSVOL. Estos archivos no esenciales pueden ser EXE, MSI o cualquier otro archivo que no sea esencial para el procesamiento de la política de grupo. Los objetos esenciales para procesar políticas de grupo son los objetos de políticas de grupo, los scripts de inicio/cierre de sesión y elalmacén central de objetos de políticas de grupo. Todos los archivos no esenciales deben almacenarse en un servidor de archivos que no sean los controladores de dominio AWS gestionados de Microsoft AD.

Si se necesitan archivos para la instalación de software de políticas de grupo, debe utilizar un servidor de archivos para almacenar esos archivos de instalación. Si prefiere no autogestionar un servidor de archivos, AWS ofrece una opción de servidor de archivos gestionado, Amazon FSx.

Para eliminar cualquier archivo innecesario, puede acceder al recurso compartido SYSVOL a través de su ruta de convención de nomenclatura universal (UNC). Por ejemplo, si el nombre de dominio completo (FQDN) de su dominio es example.com, la ruta UNC de SYSVOL será “\\example.local\SYSVOL\example.local\”. Una vez que localice y elimine los objetos no esenciales para que la política de grupo procese el directorio, debería volver a un estado activo en 30 minutos. Si después de 30 minutos el directorio no está activo, póngase en contacto con AWS Support.

Al almacenar únicamente los archivos esenciales de políticas de grupo en su recurso compartido SYSVOL, no dañará su directorio por un sobredimensionamiento de SYSVOL.

La base de datos de Active Directory está llena

Una causa frecuente de este deterioro es que la base de datos de Active Directory está llena. Para ver si es el caso, puede comprobar la cantidad total de objetos que hay en su directorio. Resaltamos la palabra total en negrita para asegurarnos de que entienda que los objetos eliminados también se tienen en cuenta a la hora de calcular el número total de objetos que hay en un directorio.

De forma predeterminada, AWS Managed Microsoft AD guarda los artículos en la papelera de reciclaje de AD durante 180 días antes de que se conviertan en objetos reciclados. Cuando un objeto se convierte en un objeto reciclado (con marcador de exclusión), este se conserva durante otros 180 días antes de que se elimine definitivamente del directorio. Por lo tanto, cuando se elimina un objeto, este existe en la base de datos del directorio durante 360 días antes de su eliminación definitiva. Esta es la razón por la que se debe evaluar el número total de objetos.

Para obtener más información sobre los recuentos de objetos AWS gestionados compatibles con Microsoft AD, consulta AWS Directory Service los precios.

Para obtener el número total de objetos de un directorio que incluye los objetos eliminados, puedes ejecutar el siguiente PowerShell comando desde una instancia de Windows unida a un dominio. Para obtener información sobre los pasos para configurar una instancia de administración, consulte Administración de usuarios y grupos en AWS Managed Microsoft AD.

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
 Select-Object -Property 'Count'
```

A continuación se muestra un ejemplo de resultados del comando anterior:

```
Count
10000
```

Si la cantidad total es superior al número de objetos admitidos para el tamaño de su directorio, que figura en la nota anterior, ha superado la capacidad de su directorio.

A continuación se muestran las opciones para resolver este problema:

1. Limpieza de AD
   a. Eliminación de los objetos no deseados de AD.

b. Eliminación de los objetos no deseados de la papelera de reciclaje de AD. Tenga en cuenta que esta es una acción destructiva y que la única forma de recuperar esos objetos eliminados será realizar una restauración del directorio.

c. El siguiente comando eliminará todos los objetos eliminados de la papelera de reciclaje de AD.

> **Important**
>
> Utilice este comando con extrema precaución, ya que se trata de un comando destructivo y la única forma de recuperar esos objetos eliminados será realizar una restauración del directorio.

```
$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. Abre un caso con AWS Support para solicitar que se AWS Directory Service recupere el espacio libre.

2. Si el tipo de directorio es Standard Edition, abra un caso con AWS Support solicitando que su directorio se actualice a Enterprise Edition. Esto también aumentará el costo de su directorio. Para obtener información acerca de los precios, consulte Precios de AWS Directory Service.

En Microsoft AD AWS administrado, los miembros del grupo de administradores AWS delegados de por vida de objetos eliminados tienen la posibilidad de modificar el `msDS-DeletedObjectLifetime` atributo que establece el tiempo en días que los objetos eliminados se guardan en la papelera de reciclaje de AD antes de que se conviertan en objetos reciclados.

> **Note**
>
> Este es un tema avanzado. Si no se configura correctamente, puede provocar la pérdida de datos. Le recomendamos que revise primero La papelera de reciclaje de AD: comprensión,

implementación, prácticas recomendadas y solución de problemas para comprender mejor estos procesos.

La capacidad para cambiar el valor del atributo de `msDS-DeletedObjectLifetime` a un número inferior puede ayudar a garantizar que la cantidad de objetos no supere los niveles permitidos. El valor válido más bajo que se puede establecer para este atributo es de 2 días. Una vez superado ese valor, ya no podrá recuperar el objeto eliminado mediante la papelera de reciclaje de AD. Tendrá que restaurar su directorio a partir de una instantánea para recuperar los objetos. Para obtener más información, consulte Creación de una instantánea o restauración del directorio. Cualquier restauración a partir de una instantánea puede provocar la pérdida de datos, ya que las instantáneas reflejan el estado del directorio en un momento determinado.

Para cambiar el tiempo de conservación de los objetos eliminados en su directorio, ejecute el siguiente comando:

> **Note**
>
> Si ejecuta el comando tal cual, establecerá el valor del atributo de tiempo de conservación de los objetos eliminados en 30 días. Si desea que sea más largo o más corto, reemplace “30” con el número que prefiera. No obstante, le recomendamos que no supere el número predeterminado 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}
```

Errores de ampliación de esquema

Esto puede ayudarle a solucionar algunos mensajes de error que pueden aparecer al ampliar el esquema de su directorio de AWS Managed Microsoft AD.

Referencia

Error

Add error on entry starting on line 1: Referral The server side error is: 0x202b A referral was returned from the server. The extended server error is: 0000202B: RefErr: DSID-0310082F, data 0, 1 access points \tref 1: ‘example.com’ Number of Objects Modified: 0

Solución de problemas

Asegúrese de que todos los campos de nombre distinguido tengan el nombre de dominio correcto. En el ejemplo anterior, `DC=example,dc=com` debe sustituirse por el `DistinguishedName` que muestra el cmdlet `Get-ADDomain`.

No se puede leer el archivo de importación

Error

No se puede leer el archivo de importación. Número de objetos modificados: 0

Solución de problemas

El archivo LDIF importado está vacío (0 bytes). Asegúrese de que se ha cargado el archivo correcto.

Error de sintaxis

Error

Hay un error de sintaxis en el archivo de entrada Error en la línea 21. El último token empieza por "q". Número de objetos modificados: 0

Solución de problemas

El texto de la línea 21 no tiene el formato correcto. La primera letra del texto no válido `A`. Actualice la línea 21 con una sintaxis de LDIF válida. Para obtener más información acerca de cómo dar formato al archivo LDIF, consulte Paso 1: creación del archivo LDIF.

Existe el atributo o valor

Error

Add error on entry starting on line 1: Attribute Or Value Exists The server side error is: 0x2083 The specified value already exists. The extended server error is: 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0

Solución de problemas

El cambio de esquema ya se ha aplicado.

No existe ese atributo

Error

Add error on entry starting on line 1: No Such Attribute The server side error is: 0x2085 The attribute value cannot be removed because it is not present on the object. The extended server error is: 00002085: AtrErr: DSID-03152367, #1: \t0: 00002085: DSID-03152367, problem 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0

Solución de problemas

El archivo LDIF está intentando eliminar un atributo de una clase, pero dicho atributo no está adjunto a la clase. Es probable que ya se aplicara el cambio de esquema.

Error

Add error on entry starting on line 41: No Such Attribute 0x57 The parameter is incorrect. El error del servidor ampliado es: 0x208d No se ha encontrado el objeto del directorio. The extended server error is: "00000057: LdapErr: DSID-0C090D8A, comment: Error in attribute conversion operation, data 0, v2580" Number of Objects Modified: 0

Solución de problemas

El atributo que aparece en la línea 41 es incorrecto. Vuelva a comprobar la ortografía.

No existe ese objeto

Error

> Add error on entry starting on line 1: No Such Object The server side error is: 0x208d Directory object not found. The extended server error is: 0000208D: NameErr: DSID-03100238, problem 2001 (NO_OBJECT), data 0, best match of: ’CN=Schema,CN=Configuration,DC=example,DC=com’ Number of Objects Modified: 0

Solución de problemas

> El objeto al que hace referencia el nombre distinguido (DN) no existe.

Motivos de los estados al crear relaciones de confianza

Cuando falle la creación de una relación de confianza, el mensaje de estado contendrá información adicional. A continuación le ayudamos a comprender lo que significan esos mensajes.

Acceso denegado

Se ha rechazado el acceso al intentar crear la relación de confianza. O la contraseña de confianza es incorrecta o bien la configuración de seguridad del dominio remoto no permite configurar una relación de confianza. Para resolver este problema, pruebe lo siguiente:

- El Microsoft AD AWS administrado Active Directory y el autoadministrado con el Active Directory que desea crear una relación de confianza deben tener el mismo nombre de primer sitio. El nombre del primer sitio está establecido en. `Default-First-Site-Name` Si estos nombres varían de un dominio a otro, se produce un error de acceso denegado.
- Compruebe que está utilizando la misma contraseña de confianza que utilizó al crear la relación de confianza correspondiente en el dominio remoto.
- Compruebe también que la configuración de seguridad de su dominio permite crear relaciones de confianza.
- Compruebe que la política de seguridad local está configurada correctamente. Compruebe específicamente `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` y asegúrese de que contiene al menos las siguientes tres canalizaciones mencionadas a continuación:
  - netlogon
  - samr

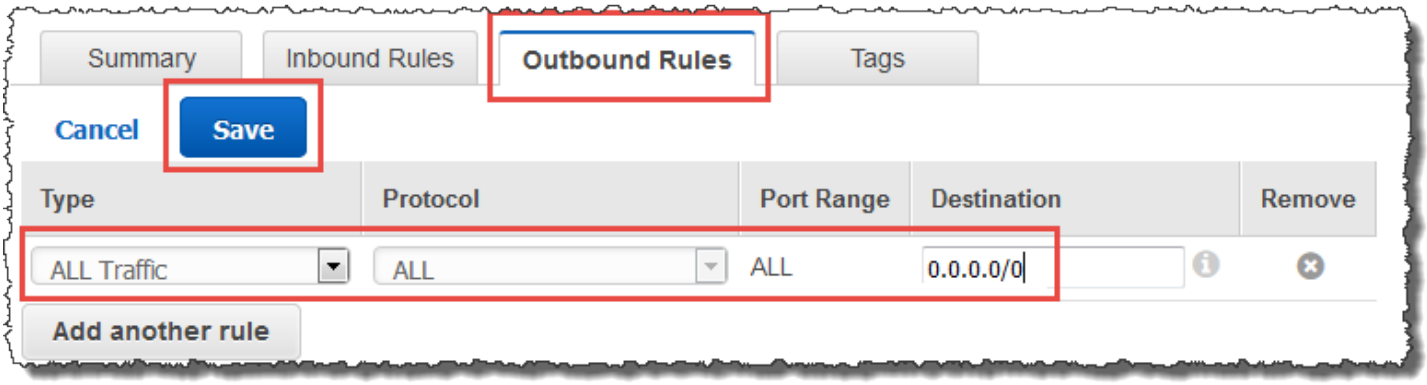
- lsarpc
- Compruebe que las canalizaciones mencionadas anteriormente existan como valores de la clave de NullSessionPipesregistro que se encuentra en la ruta de registro HKLM\ SYSTEM\\ services\ CurrentControlSetLanmanServer\ Parameters. Estos valores deben insertarse en filas separadas.

> **Note**
>
> `Network access: Named Pipes that can be accessed anonymously` no está configurado de forma predeterminada y se mostrará `Not Defined`. Esto es normal, ya que la configuración predeterminada efectiva del controlador de dominio de `Network access: Named Pipes that can be accessed anonymously` es `netlogon`, `samr`, `lsarpc`.

- Compruebe la siguiente configuración de firma del bloque de mensajes del servidor (SMB) en la política de controladores de dominio predeterminada. Estos ajustes se encuentran en Configuración del ordenador > Configuración de Windows > Configuración de seguridad > Políticas locales y opciones de seguridad. Deben coincidir con los siguientes ajustes:
  - Microsoftcliente de red: firme digitalmente las comunicaciones (siempre): predeterminado: activado
  - Microsoftcliente de red: firma digitalmente las comunicaciones (si el servidor lo acepta): predeterminado: activado
  - Microsoftservidor de red: firmar digitalmente las comunicaciones (siempre): activado
  - Microsoftservidor de red: firme digitalmente las comunicaciones (si el cliente está de acuerdo): predeterminado: habilitado

El nombre de dominio especificado no existe o no se pudo contactar con él

Para solucionar este problema, asegúrese de que la configuración de grupo de seguridad para su dominio y la lista de control de acceso (ACL) para la VPC sea correcta y que haya introducido correctamente la información del programa de envío condicional. AWS configura el grupo de seguridad para que abra solo los puertos que las comunicaciones de Active Directory necesiten. En la configuración predeterminada, el grupo de seguridad acepta el tráfico a estos puertos desde cualquier dirección IP. El tráfico saliente está restringido al grupo de seguridad. Deberá actualizar la regla de salida del grupo de seguridad para permitir el tráfico a su red en las instalaciones. Para obtener más información sobre los requisitos de seguridad, consulte Paso 2: preparación de su AWS Managed Microsoft AD.



Si los servidores DNS de las redes de los demás directorios utilizan direcciones IP públicas (distintas de la RFC 1918), tendrá que agregar una ruta IP en el directorio desde la consola de servicios de directorio hasta los servidores DNS. Para obtener más información, consulte Crear, verificar o eliminar una relación de confianza y Requisitos previos.

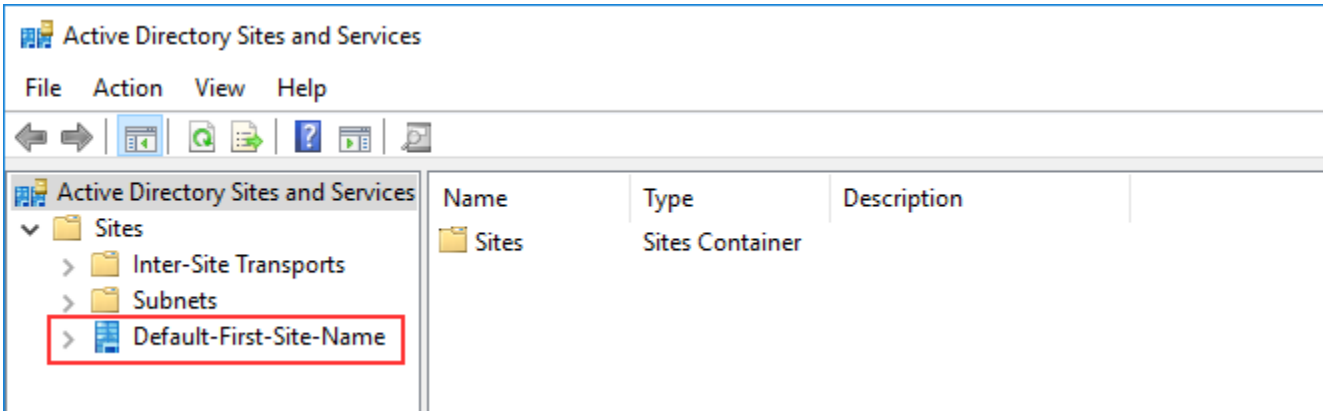
La Autoridad de Números Asignados en Internet (IANA) ha reservado los siguientes tres bloques del espacio de direcciones IP para redes de Internet privadas:

- 10.0.0.0 - 10.255.255.255 (prefijo 10/8)
- 172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)
- 192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

Para obtener más información, consulte https://tools.ietf.org/html/rfc1918.

Compruebe que el nombre del sitio de AD predeterminado para su Microsoft AD AWS administrado coincide con el nombre del sitio de AD predeterminado de su infraestructura local. El equipo determina el nombre del sitio mediante un dominio del que el equipo es miembro, no a partir del dominio del usuario. Si se cambia el nombre del sitio para que coincida con las instalaciones más cercanas, se garantiza que el localizador de centros de distribución utilizará un controlador de dominio del sitio más cercano. Si esto no resuelve el problema, es posible que se almacenara en caché la información desde un programa de envío condicional creado anteriormente que esté impidiendo crear una nueva relación de confianza. Espere unos minutos y, a continuación, vuelva a crear la relación de confianza y el programa de envío condicional.

Para obtener más información sobre cómo funciona, consulte Domain Locator Across a Forest Trust en el Microsoft sitio web.



No se pudo llevar a cabo la operación en este dominio

Para resolver este problema, asegúrese de que ambos dominios o directorios no tengan nombres NETBIOS superpuestos. Si los dominios o directorios tienen nombres NETBIOS superpuestos, vuelva a crear uno de ellos con un nombre NETBIOS diferente e inténtelo de nuevo.

La creación de relaciones de confianza no se puede llevar a cabo debido al error “Required and valid domain name”

Los nombres de DNS únicamente pueden contener caracteres alfabéticos (A-Z), caracteres numéricos (0-9), el signo menos (-) y un punto (.). El punto es un carácter que solo se permite cuando se utiliza para delimitar los componentes de los nombres de estilo de dominio. Tenga en cuenta las siguientes soluciones:

- AWS Microsoft AD administrado no admite confianzas con dominios de etiqueta única. Para obtener más información, consulte la Microsoftcompatibilidad con dominios de etiqueta única.
- Según el RFC 1123 (https://tools.ietf.org/html/rfc1123), los únicos caracteres que se pueden utilizar en las etiquetas DNS son de la “A” a la “Z”, de la “a” a la “z”, del “0” al “9” y un guion (“-”). También se utiliza el punto [.] en los nombres de DNS, pero solo entre las etiquetas de DNS y al final de un FQDN.
- Según el RFC 952 (https://tools.ietf.org/html/rfc952), un “nombre” (nombre de red, host, puerta de enlace o dominio) es una cadena de texto de hasta 24 caracteres extraída del alfabeto (A-Z), dígitos (0-9), signo menos (-) y punto (.). Tenga en cuenta que los puntos solo se permiten cuando sirven para delimitar los componentes de los “nombres de estilo de dominio”.

Para obtener más información, consulte Cumplir las restricciones de nombres para hosts y dominios en el sitio Microsoft web.

Herramientas generales de comprobación de confianza

Las siguientes son herramientas que se pueden utilizar para solucionar diversos problemas relacionados con la confianza.

AWS Herramienta de solución de problemas de automatización de Systems Manager

Los flujos de trabajo de Support Automation (SAW) utilizan AWS Systems Manager Automation para proporcionarle un manual predefinido para AWS Directory Service. La AWSSupport herramienta TroubleshootDirectoryTrust runbook le ayuda a diagnosticar problemas comunes de creación de confianza entre Microsoft AD AWS administrado y un entorno local MicrosoftActive Directory.

DirectoryServicePortTest herramienta

La herramienta de DirectoryServicePortTestpruebas puede resultar útil para solucionar problemas de creación de confianza entre Microsoft AD AWS administrado y Active Directory local. Para ver un ejemplo de cómo se puede utilizar la herramienta, consulte Probar el conector de AD.

Herramienta NETDOM y NLTEST

Los administradores pueden utilizar las herramientas de línea de comandos Netdom y Nltest para buscar, mostrar, crear, eliminar y gestionar las reacciones de confianza. Estas herramientas se comunican directamente con la autoridad de LSA a través de un controlador de dominio. Para ver un ejemplo de cómo utilizar estas herramientas, consulte Netdom y NLTEST en el sitio web. Microsoft

Herramienta de captura de paquetes

Puede utilizar el complemento de captura de paquetes de Windows integrado para investigar y solucionar un posible problema de red. Para obtener más información, consulte Capture a Network Trace without installing anything.

Conector de AD

AD Connector es una puerta de enlace de directorios con la que puedes redirigir las solicitudes de directorio a tu entorno local Microsoft Active Directory sin almacenar en caché ninguna información en la nube. Conector AD está disponible en dos tamaños: pequeño y grande. Un pequeño Conector AD está diseñado para organizaciones más pequeñas y para gestionar un número bajo de operaciones por segundo. Un Conector AD grande está diseñado para organizaciones más grandes y para gestionar un número entre moderado y alto de operaciones por segundo. Puede distribuir las cargas de la aplicación entre varios conectores de AD para satisfacer sus necesidades de rendimiento. No se aplica ningún límite de usuarios o conexiones.

AD Connector no admite las confianzas transitivas de Active Directory. Los conectores de AD y los dominios de Active Directory locales tienen una relación de 1 a 1. Es decir, para cada dominio local, incluidos los dominios secundarios de un bosque de Active Directory en los que desee autenticarse, debe crear un AD Connector único.

> **Note**
>
> AD Connector no se puede compartir con otras AWS cuentas. Si es un requisito, considere la posibilidad de utilizar Microsoft AD AWS administrado paraCompartir el directorio. AD Connector tampoco es compatible con varias VPC, lo que significa que AWS aplicaciones como WorkSpacesestas deben aprovisionarse en la misma VPC que el AD Connector.

Una vez configurado, Conector AD ofrece los siguientes beneficios:

- Los usuarios finales y los administradores de TI pueden usar sus credenciales corporativas actuales para iniciar sesión en AWS aplicaciones como WorkSpaces Amazon WorkDocs o Amazon WorkMail.
- Puede administrar AWS recursos como las instancias de Amazon EC2 o los buckets de Amazon S3 mediante el acceso basado en roles de IAM al. AWS Management Console
- Puede aplicar de forma coherente las políticas de seguridad existentes (como la caducidad de las contraseñas, el historial de contraseñas y los bloqueos de cuentas) tanto si los usuarios como los administradores de TI acceden a los recursos de su infraestructura local o de la nube. AWS
- Puede usar AD Connector para habilitar la autenticación multifactorial integrándola con su infraestructura de MFA basada en RADIUS existente para proporcionar una capa adicional de seguridad cuando los usuarios accedan a las aplicaciones. AWS

Siga leyendo los temas de esta sección para obtener información acerca de cómo conectarse a un directorio y sacar el máximo partido a las características de Conector AD.

Temas

Introducción a Conector AD

Con AD Connector, puede conectarse AWS Directory Service a su empresa actualActive Directory. Cuando te conectas a tu directorio existente, todos los datos del directorio permanecen en tus controladores de dominio. AWS Directory Service no replica ninguno de los datos del directorio.

Temas

Requisitos previos de Conector AD

Para conectarse a su directorio existente con Conector AD, necesita lo siguiente:

Amazon VPC

Configurar una VPC con lo siguiente:

- Dos subredes como mínimo. Cada una de las subredes debe estar en una zona de disponibilidad diferente.
- La VPC debe estar conectada a la red existente a través de una conexión de red privada virtual (VPN) o de AWS Direct Connect.
- La VPC debe disponer de tenencia de hardware predeterminada.

AWS Directory Service utiliza una estructura de dos VPC. Las instancias EC2 que componen su directorio se ejecutan fuera de su AWS cuenta y son administradas por. AWS Contienen dos adaptadores de red, `ETH0` y `ETH1`. `ETH0` es el adaptador de administración y se encuentra fuera de su cuenta. `ETH1` se crea dentro de su cuenta.

El rango de IP de administración de la red `ETH0` del directorio se elige mediante programación para garantizar que no entre en conflicto con la VPC en la que está implementado el directorio. Este rango de IP puede estar en cualquiera de los siguientes pares (ya que los directorios se ejecutan en dos subredes):

- 10.0.1.0/24 y 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 y 192.168.2.0/24

Para evitar conflictos, comprobamos el primer octeto del CIDR `ETH1`. Si comienza con un 10, entonces elegimos una VPC 192.168.0.0/16 con subredes 192.168.1.0/24 y 192.168.2.0/24. Si el primer octeto no es un 10, elegimos una VPC 10.0.0.0/16 con subredes 10.0.1.0/24 y 10.0.2.0/24.

El algoritmo de selección no incluye las rutas de la VPC. Por lo tanto, es posible que este escenario provoque un conflicto del enrutamiento IP.

Para obtener más información, consulte los siguientes temas en la Guía del usuario de Amazon VPC.

- ¿Qué es Amazon VPC?
- Subredes de la VPC
- Adición de una gateway privada virtual de hardware a la VPC

Para obtener más información al respecto AWS Direct Connect, consulte la Guía del AWS Direct Connect usuario.

Existente Active Directory

Deberás conectarte a una red existente con un Active Directory dominio.

> **Note**
>
> Conector AD no admite dominios de etiqueta única.

El nivel funcional de este Active Directory dominio debe ser igual `Windows Server 2003` o superior. Conector AD también admite la conexión a un dominio alojado en una instancia de Amazon EC2.

> **Note**
>
> Conector AD no admite controladores de dominio de solo lectura (RODC) cuando se utiliza en combinación con la característica de unión de dominios de Amazon EC2.

Cuenta de servicio

Debe disponer de las credenciales de una cuenta de servicio en el directorio existente con los siguientes privilegios delegados:

- Leer usuarios y grupos: obligatorio
- Unir ordenadores al dominio: solo es obligatorio cuando se utiliza Seamless Domain Join y WorkSpaces
- Crear objetos de ordenador: solo es necesario cuando se utiliza Seamless Domain Join y WorkSpaces
- La contraseña de la cuenta de servicio debe cumplir con los requisitos de AWS contraseña. AWS las contraseñas deben ser:
  - Entre 8 y 128 caracteres, ambos inclusive.
  - Contiene al menos un carácter de tres de las cuatro categorías siguientes:
    - Letras minúsculas (a-z)
    - Letras mayúsculas (A-Z)
    - Números (0-9)
    - Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Para obtener más información, consulte Privilegios delegados a su cuenta de servicio.

> **Note**
>
> Conector AD usa Kerberos para la autenticación y autorización de AWS aplicaciones. LDAP solo se usa para búsquedas de objetos de usuarios y grupos (operaciones de lectura). Con las transacciones LDAP, nada es mutable y las credenciales no se

transmiten en texto limpio. La autenticación la gestiona un servicio AWS interno, que utiliza los tickets de Kerberos para realizar operaciones de LDAP como usuario.

Permisos de usuario

Todos los usuarios de Active Directory deben tener permisos para leer sus propias atributos. En concreto los siguientes atributos:

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

De forma predeterminada, los usuarios de Active Directory tienen permisos de lectura para estos atributos. Sin embargo, los administradores pueden modificarlos con el paso del tiempo, por lo que conviene que compruebe que los usuarios tienen estos permisos de lectura antes de configurar Conector AD por primera vez.

Direcciones IP

Consiga las direcciones IP de dos servidores DNS o controladores de dominio de su directorio existente.

Conector AD obtiene los registros SRV `_ldap._tcp.<DnsDomainName>` y `_kerberos._tcp.<DnsDomainName>` de estos servidores al conectar a su directorio, de modo que estos servidores deben contener dichos registros SRV. Conector AD intenta encontrar un controlador de dominio común que proporcionará ambos servicios LDAP y Kerberos, de modo que estos registros SRV deben incluir al menos un controlador de dominio común. Para obtener más información acerca de los registros SRV, vaya a SRV Resource Records en Microsoft. TechNet

Puertos para subredes

Para que AD Connector redirija las solicitudes de directorio a sus controladores de Active Directory dominio existentes, el firewall de su red actual debe tener los siguientes puertos abiertos a los CIDR de ambas subredes de su Amazon VPC.

- TCP/UDP 53: DNS
- TCP/UDP 88: autenticación de Kerberos
- TCP/UDP 389: LDAP

Estos son los puertos mínimos necesarios antes de que Conector AD pueda conectarse al directorio. La configuración específica podría requerir abrir puertos adicionales.

Si quieres usar AD Connector y Amazon WorkSpaces, el atributo DisableVLVSupportLDAP debe estar establecido en 0 para tus controladores de dominio. Esta es la configuración predeterminada para los controladores de dominio. AD Connector no podrá consultar a los usuarios del directorio si el atributo DisableVLVSupportLDAP está habilitado. Esto impide que AD Connector funcione con Amazon WorkSpaces.

> **Note**
>
> Si los servidores DNS o los servidores del controlador de dominio de su Active Directory dominio existente están dentro de la VPC, los grupos de seguridad asociados a esos servidores deben tener los puertos anteriores abiertos a los CIDR de ambas subredes de la VPC.

Para conocer los requisitos de puertos adicionales, consulte los requisitos de puertos AD y AD DS en la documentación. Microsoft

Autenticación previa de Kerberos

Las cuentas de usuario deben tener habilitada la autenticación previa de Kerberos. Para obtener instrucciones detalladas sobre cómo habilitar este ajuste, consulte Asegúrese de que la autenticación previa de Kerberos esté habilitada. Para obtener información general sobre esta configuración, consulte Autenticación previa en Microsoft TechNet.

Tipos de cifrado

AD Connector admite los siguientes tipos de cifrado para la autenticación de los controladores de dominio de Active Directory a través de Kerberos:

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center requisitos previos

Si planea utilizar IAM Identity Center con Conector AD, debe asegurarse de que se cumpla lo siguiente:

- El AD Connector está configurado en la cuenta de administración de la AWS organización.
- Su instancia de IAM Identity Center debe estar en la misma región en la que se configuró su directorio del Conector AD.

Para obtener más información, consulte los requisitos previos del Centro de identidad de IAM en la Guía del AWS IAM Identity Center usuario.

Requisitos previos de la autenticación multifactor

Para admitir la autenticación multifactor con su directorio de Conector AD necesita lo siguiente:

- Un servidor Remote Authentication Dial In User Service (RADIUS) en la red existente que tenga dos puntos de enlace de cliente. Los puntos de enlace de cliente de RADIUS tienen que cumplir los siguientes requisitos:
  - Para crear los puntos de enlace, necesita las direcciones IP de los servidores de AWS Directory Service . Estas direcciones IP se pueden obtener en el campo Directory IP Address de los detalles del directorio.
  - Los dos puntos de enlace de RADIUS tienen que utilizar el mismo código secreto compartido.
- Su red actual debe permitir el tráfico entrante desde los servidores a través del puerto de servidor RADIUS predeterminado (1812). AWS Directory Service
- Los nombres de usuario deben ser idénticos en el servidor RADIUS y en el directorio existente.

Para obtener más información sobre cómo utilizar Conector AD con la MFA, consulte Habilitación de la autenticación multifactor para Conector AD.

Privilegios delegados a su cuenta de servicio

Para poder conectarse al directorio existente, debe disponer de las credenciales de su cuenta de servicio del Conector AD en el directorio existente que tiene determinados privilegios delegados. Aunque los miembros del grupo Domain Admins (Administradores del dominio) tengan suficientes privilegios para conectarse al directorio, es recomendable utilizar una cuenta de servicio que tenga únicamente los privilegios mínimos necesarios para conectarse al directorio. El siguiente

procedimiento muestra cómo crear un nuevo grupo llamado`Connectors`, delegar los privilegios necesarios para conectarse a este grupo y, AWS Directory Service a continuación, agregar una nueva cuenta de servicio a este grupo.

Este procedimiento debe realizarse en un equipo que esté unido al directorio y que tenga instalado el complemento de MMC Usuarios y equipos de Active Directory. Además, es necesario la sesión se inicie como administrador del dominio.

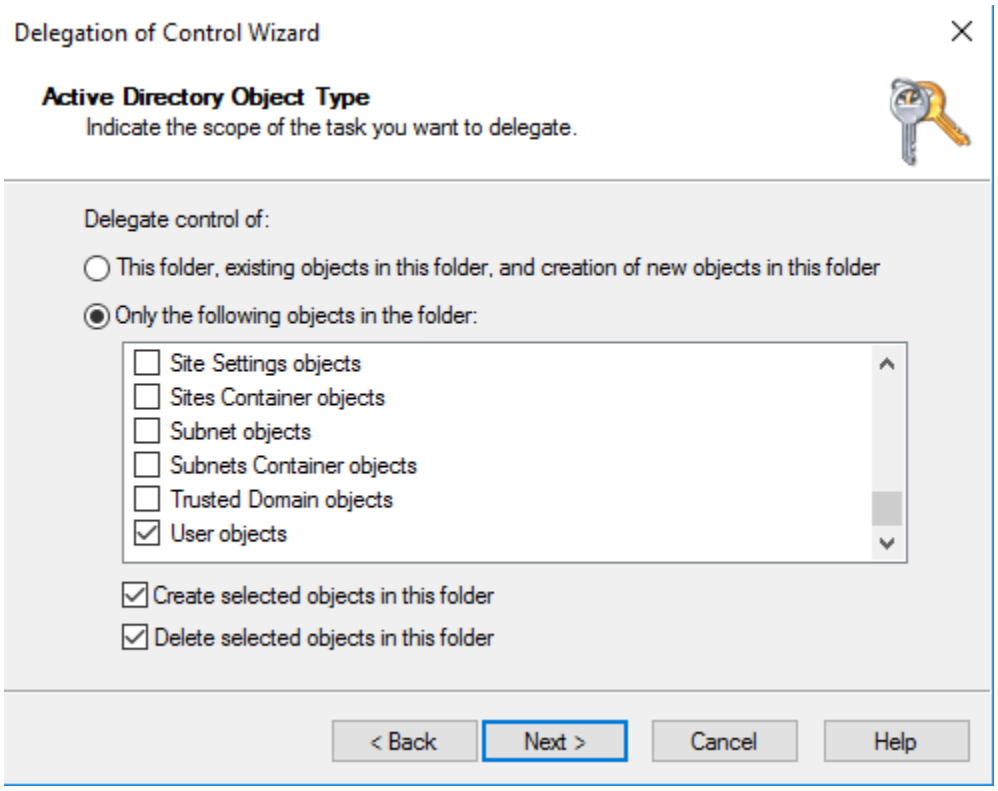
Para delegar privilegios a su cuenta de servicio

1. Abra Usuarios y equipos de Active Directory y seleccione la raíz del dominio en el árbol de navegación.
2. En la lista del panel izquierdo, haga clic con el botón derecho en Usuarios, seleccione Nuevo y, a continuación, seleccione Grupo.
3. En el cuadro Nuevo objeto - Grupo, escriba lo siguiente y haga clic en Aceptar.

Campo	Valor/Selección
Nombre del grupo	`Connectors`
Ámbito del grupo	Global
Tipo de grupo	Seguridad

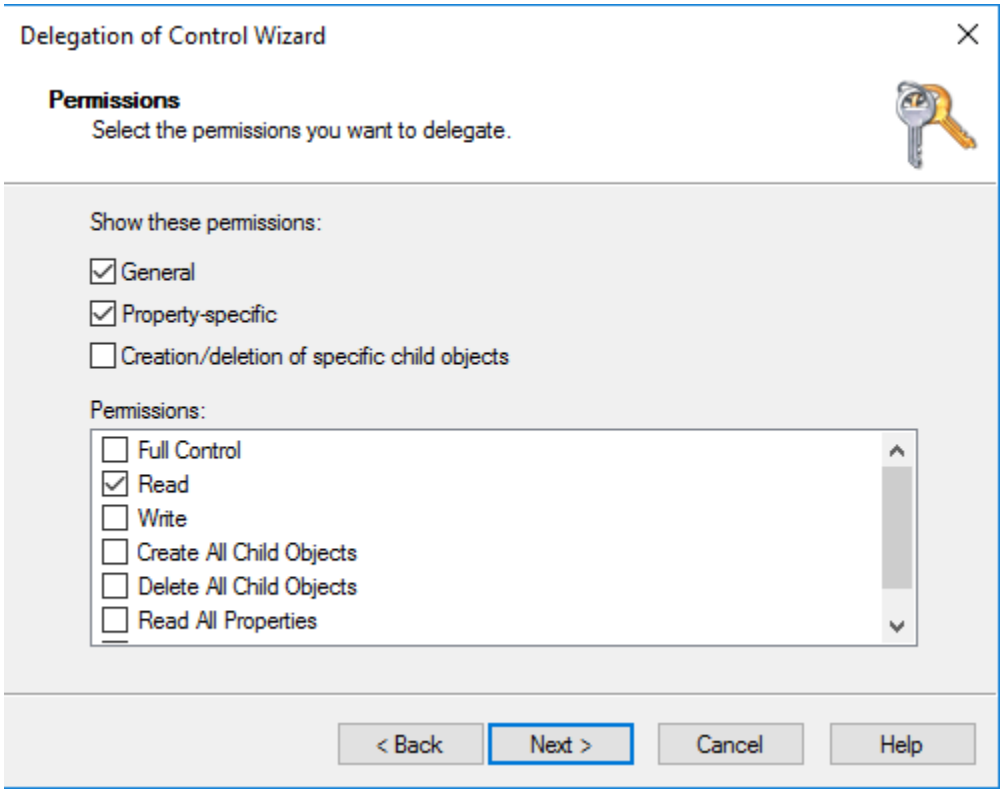
4. En el árbol de navegación Usuarios y equipos de Active Directory, seleccione la raíz del dominio. En el menú, seleccione Acción y luego Delegar control. Si su AD Connector está conectado a AWS Managed Microsoft AD, no tendrá acceso para delegar el control en el nivel raíz del dominio. En este caso, para delegar el control, seleccione la unidad organizativa situada en la unidad organizativa del directorio en la que se crearán los objetos del equipo.
5. En la página Asistente para delegación de control, haga clic en Siguiente y luego en Agregar.
6. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, escriba `Connectors` y haga clic en Aceptar. Si se encuentran varios objetos, seleccione el grupo `Connectors` que creó anteriormente. Haga clic en Next (Siguiente).
7. En la página Tareas que se delegarán, seleccione Crear una tarea personalizada para delegar y luego elija Siguiente.
8. Seleccione Sólo los siguientes objetos en la carpeta y, a continuación, seleccione Objetos de equipo y Objetos de usuario.

9. Seleccione Crear los objetos seleccionados en esta carpeta y Eliminar los objetos seleccionados en esta carpeta. A continuación, elija Next.



10. Seleccione Read (Lectura) y después elija Next (Siguiente).

> **Note**
>
> Si va a utilizar Seamless Domain Join o WorkSpaces, también debe habilitar los permisos de escritura para que Active Directory pueda crear objetos de ordenador.



11. Compruebe la información en la página Finalización del Asistente para delegación de control y haga clic en Finalizar.
12. Cree una cuenta de usuario con una contraseña segura y añada ese usuario al grupo `Connectors`. Este usuario se conocerá como su cuenta de servicio AD Connector y, dado que ahora es miembro del `Connectors` grupo, ahora tiene privilegios suficientes AWS Directory Service para conectarse al directorio.

Probar el conector de AD

Para que Conector AD pueda conectarse al directorio existente, el firewall de la red existente debe tener ciertos puertos abiertos para los CIDR de las dos subredes de la VPC. Para probar si estas condiciones se cumplen, siga estos pasos:

Para probar la conexión

1. Ejecute una instancia de Windows en la VPC y conéctese a ella a través de RDP. La instancia debe ser miembro del dominio existente. El resto de los pasos deben realizarse en esta instancia de VPC.

2. Descarga y descomprime la aplicación de DirectoryServicePortTestprueba. La aplicación de prueba contiene el código fuente y los archivos del proyecto de Visual Studio para que, si lo desea, pueda modificarla.

> **Note**
>
> Este script no es compatible con Windows Server 2003 o sistemas operativos antiguos.

3. Desde un símbolo del sistema de Windows, ejecute la aplicación de prueba DirectoryServicePortTest con las siguientes opciones:

> **Note**
>
> La aplicación de DirectoryServicePortTest prueba solo se puede usar cuando los niveles funcionales del dominio y del bosque están configurados en Windows Server 2012 R2 o versiones anteriores.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
 "53,88,389" -udp "53,88,389"
```

<nombre_dominio>

Nombre completo del dominio. Se utiliza para comprobar los niveles funcionales del bosque y el dominio. Si no incluye el nombre del dominio, no se comprobarán los niveles funcionales.

<dirección_IP_servidor>

Dirección IP de un controlador del dominio existente. Los puertos se comprobarán utilizando esta dirección IP. Si no incluye la dirección IP, no se comprobarán los puertos.

Esta aplicación de prueba determina si están abiertos los puertos necesarios desde la VPC a su dominio y también verifica los niveles funcionales mínimos del bosque y el dominio.

El resultado será similar al siguiente:

```
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
```

A continuación se muestra el código fuente de la aplicación 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;
        }
    }
}
```

Creación de un Conector AD

Para conectarse a su directorio existente con Conector AD, siga estos pasos. Antes de comenzar este procedimiento, asegúrese de haber completado los requisitos previos que se indican en Requisitos previos de Conector AD.

> **Note**
>
> No puede crear un Conector AD con una plantilla de Cloud Formation.

Para conectarse con Conector AD

1. En el panel de navegación de la consola de AWS Directory Service, elija Directorios y, a continuación, elija Configurar directorio.
2. En la página Seleccionar tipo de directorio, elija Conector AD y, a continuación, elija Siguiente.

3. En la página Enter AD Connector information (Especifique la información de AD Connector), facilite la siguiente información:

   Tamaño del directorio

   Elija entre la opción de tamaño Small (Pequeño) o Large (Grande). Para obtener más información acerca de los tamaños, consulte Conector de AD.

   Descripción del directorio

   Descripción opcional del directorio.

4. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la siguiente información y, a continuación, elija Next (Siguiente).

   VPC

   VPC del directorio.

   Subredes

   Elija las subredes de los controladores de dominio. Las dos subredes deben estar en diferentes zonas de disponibilidad.

5. En la página Connect to AD (Conectar a AD), proporcione la siguiente información:

   Nombre de DNS del directorio

   Nombre completo del directorio existente, por ejemplo `corp.example.com`.

   Nombre NetBIOS del directorio

   Nombre abreviado del directorio existente, por ejemplo `CORP`.

   Direcciones IP de DNS

   La dirección IP de al menos un servidor DNS del directorio existente. Estos servidores deben ser accesibles desde cada subred especificada en el paso 4. Estos servidores pueden estar ubicados fuera de AWS, siempre que haya conectividad de red entre las subredes especificadas y las direcciones IP del servidor DNS.

   Nombre de usuario de la cuenta de servicio

   El nombre de usuario de un usuario del directorio existente. Para obtener más información acerca de esta cuenta, consulte Requisitos previos de Conector AD.

Contraseña de la cuenta de servicio

La contraseña de la cuenta del usuario existente. Esta contraseña distingue entre mayúsculas y minúsculas y debe tener un mínimo de 8 caracteres y un máximo de 128. También debe contener al menos un carácter de tres de las siguientes categorías:

- Letras minúsculas (a-z)
- Letras mayúsculas (A-Z)
- Números (0-9)
- Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmar contraseña

Vuelva a escribir la contraseña de la cuenta del usuario existente.

6. En la página Review & create (Revisar y crear), revise la información del directorio y haga los cambios que sean necesarios. Cuando la información sea correcta, seleccione Create directory (Crear directorio). La creación del directorio tarda varios minutos. Una vez creado, el valor Status cambia a Active.

Qué se crea con tu AD Connector

Al crear un AD Connector, crea y asocia AWS Directory Service automáticamente una interfaz de red elástica (ENI) a cada una de las instancias de AD Connector. Cada uno de estos ENI es esencial para la conectividad entre la VPC y el AD AWS Directory Service Connector y nunca se debe eliminar. Puede identificar todas las interfaces de red reservadas para su uso AWS Directory Service mediante la descripción: «interfaz de red AWS creada para el identificador del directorio». Para obtener más información sobre ENI, consulte Interfaces de red elásticas en la Guía del usuario de Amazon EC2.

> **Note**
>
> Las instancias del Conector AD se implementan en dos zonas de disponibilidad de una región de forma predeterminada y se conectan a su Amazon Virtual Private Cloud (VPC). Las instancias del Conector AD que fallan se reemplazan automáticamente en la misma zona de disponibilidad con la misma dirección IP.

Al iniciar sesión en cualquier AWS aplicación o servicio integrado con un AD Connector (AWS IAM Identity Center incluido), la aplicación o el servicio reenvía la solicitud de autenticación a AD Connector, que luego la reenvía a un controlador de dominio de su Active Directory autogestionado para su autenticación. Si te has autenticado correctamente en tu Active Directory autogestionado, AD Connector devuelve un token de autenticación a la aplicación o al servicio (similar a un token de Kerberos). En este punto, ya puedes acceder a la AWS aplicación o al servicio.

Cómo administrar Conector AD

En esta sección, se presentan todos los procedimientos de uso y mantenimiento de un entorno de Conector AD.

Temas

Protección del directorio de Conector AD

Esta sección describe las consideraciones para proteger su entorno de Conector AD.

Temas

Actualización de las credenciales de su cuenta de servicio de Conector AD en AWS Directory Service

Las credenciales de Conector AD que proporciona en AWS Directory Service representan la cuenta de servicio que se utiliza para acceder a su directorio en las instalaciones existente. Puede modificar estas credenciales de la cuenta de servicio en AWS Directory Service siguiendo estos pasos.

> **Note**
>
> Si AWS IAM Identity Center está habilitado para el directorio, AWS Directory Service debe transferir el nombre principal del servicio (SPN) de la cuenta de servicio actual a la nueva cuenta de servicio. Si la cuenta de servicio actual no tiene permiso para eliminar el SPN o la nueva cuenta de servicio no tiene permiso para añadir el SPN, se le solicitarán las credenciales de una cuenta de directorio que tenga permiso para realizar ambas acciones. Estas credenciales solo se usarán para transferir el SPN. El servicio no las almacenará.

Para actualizar las credenciales de su cuenta de servicio de Conector AD en AWS Directory Service

1. En el panel de navegación de la consola de AWS Directory Service, en Active Directory, elija Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Detalles del directorio, desplácese hacia abajo hasta la sección Credenciales de la cuenta de servicio.
4. En la sección Credenciales de cuenta de servicio, elija Actualizar.
5. En el cuadro de diálogo Actualizar las credenciales de la cuenta de servicio, escriba el nombre de usuario y la contraseña de la cuenta de servicio. Vuelva a escribir la contraseña para confirmarla y, a continuación, seleccione Actualizar.

Habilitación de la autenticación multifactor para Conector AD

Puede habilitar la autenticación multifactor para Conector AD si tiene Active Directory ejecutándose en las instalaciones o en instancias de EC2. Para obtener más información acerca de cómo usar la autenticación multifactor con AWS Directory Service, consulte Requisitos previos de Conector AD.

> **Note**
>
> La autenticación multifactor no puede usarse con Simple AD. Sin embargo, la MFA se puede habilitar para su directorio de AWS Managed Microsoft AD. Para obtener más información, consulte Habilite la autenticación multifactorial para Microsoft AWS AD administrado.

Habilitación de la autenticación multifactor para Conector AD

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el vínculo del ID de su directorio del Conector AD.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Networking & security (Redes y seguridad).
4. En la sección Multi-factor authentication (Autenticación multifactor), elija Actions (Acciones) y, a continuación, seleccione Enable (Habilitar).
5. En la página Enable multi-factor authentication (MFA) (Habilitar la autenticación multifactor (MFA)), proporcione los valores siguientes:

   Display label (Mostrar etiqueta)

   Proporcione un nombre de etiqueta.

   RADIUS server DNS name or IP addresses (Nombre de DNS o direcciones IP del servidor RADIUS)

   Direcciones IP de los puntos de enlace del servidor RADIUS o dirección IP del balanceador de carga del servidor RADIUS. Puede especificar varias direcciones IP separándolas mediante comas (por ejemplo, `192.0.0.0,192.0.0.12`).

   > **Note**
   >
   > El MFA RADIUS solo se aplica para autenticar el acceso a las AWS Management Console aplicaciones y servicios empresariales de Amazon, como Amazon o WorkSpaces Amazon QuickSight Chime. No proporciona MFA a cargas de trabajo de Windows que se ejecutan en instancias EC2 o para iniciar sesión en una instancia EC2. AWS Directory Service no admite la autenticación de desafío/respuesta de RADIUS.

En el momento en que los usuarios especifiquen el nombre de usuario y la contraseña, deben disponer de un código MFA. Como alternativa, debe usar una solución que realice MFA, out-of-band como la verificación de texto por SMS para el usuario. En las soluciones de out-of-band MFA, debe asegurarse de establecer el valor de tiempo de espera RADIUS de forma adecuada para su solución. Al utilizar una solución de out-of-band MFA, la página de inicio de sesión solicitará al usuario un código de MFA. En ese caso, se recomienda a los usuarios que escriban su contraseña en el campo de contraseña y en el campo de MFA.

Puerto

Puerto que utiliza el servidor RADIUS para las comunicaciones. La red local debe permitir el tráfico entrante procedente del puerto de servidor RADIUS (UDP:1812) de los servidores AWS Directory Service.

Código secreto compartido

Código de secreto compartido que se especificó cuando se crearon los puntos de enlace de RADIUS.

Confirm shared secret code (Confirmar código secreto compartido)

Confirme el código secreto compartido para los puntos de enlace de RADIUS.

Protocolo

Seleccione el protocolo que se especificó cuando se crearon los puntos de enlace de RADIUS.

Tiempo de espera del servidor (en segundos)

Tiempo, en segundos, que hay que esperar a que el servidor RADIUS responda. Este valor debe estar entre 1 y 50.

Número máximo de reintentos de solicitud RADIUS

Número de veces que se intenta la comunicación con el servidor RADIUS. Este valor debe estar entre 0 y 10.

La autenticación multifactor está disponible cuando RADIUS Status cambia a Habilitado.

6. Elija Habilitar.

Habilitar LDAPS del cliente mediante Conector AD

La compatibilidad con LDAPS del cliente en Conector AD cifra las comunicaciones entre Microsoft Active Directory (AD) y las aplicaciones de AWS. Algunos ejemplos de estas aplicaciones son WorkSpaces, AWS IAM Identity Center, Amazon QuickSight y Amazon Chime. Este cifrado le ayuda a proteger mejor los datos de identidad de su organización y a cumplir sus requisitos de seguridad.

Temas

Requisitos previos

Antes de habilitar LDAPS del lado del cliente, debe cumplir los siguientes requisitos.

Temas

Implementar certificados de servidor en Active Directory

Para habilitar LDAPS en el lado del cliente, debe obtener e instalar certificados de servidor para cada controlador de dominio en Active Directory. Estos certificados los utilizará el servicio LDAP para escuchar y aceptar automáticamente conexiones SSL de clientes LDAP. Puede utilizar certificados SSL emitidos por una implementación interna de Active Directory Certificate Services (ADCS) o adquiridos a un emisor comercial. Para obtener más información acerca de los requisitos de certificados de servidor de Active Directory, consulte Certificado LDAP a través de SSL (LDAPS) en el sitio web de Microsoft.

Requisitos del certificado de CA

Se requiere un certificado de CA (entidad de certificación) que represente al emisor de los certificados de servidor para la operación LDAPS del lado del cliente. Los certificados de entidad de certificación coinciden con los certificados de servidor que presentan los controladores de dominio de

Active Directory para cifrar las comunicaciones LDAP. Tenga en cuenta los siguientes requisitos de los certificados de CA:

- Para registrar un certificado, deben quedar más de 90 días para que caduque.
- Los certificados deben estar en formato PEM (Privacy-Enhanced Mail). Si exporta certificados de CA desde Active Directory, elija X.509 (.CER) codificado en base64 como formato de archivo de exportación.
- Se puede almacenar un máximo de cinco (5) certificados de entidad de certificación por directorio de Conector AD.
- No se admiten los certificados que utilizan el algoritmo de firma RSASSA-PSS.

Requisitos de red

El tráfico LDAP de las aplicaciones de AWS se ejecutará exclusivamente en el puerto TCP 636, sin la posibilidad de utilizar el puerto LDAP 389 como segunda opción. Sin embargo, las comunicaciones LDAP de Windows que admiten la replicación, relaciones de confianza y otras características seguirán utilizando el puerto LDAP 389 con la seguridad nativa de Windows. Configure grupos de seguridad de AWS y firewalls de red para permitir las comunicaciones TCP en el puerto 636 en Conector AD (saliente) y en la instancia de Active Directory autoadministrada (entrante).

Habilitar LDAPS del cliente

Para habilitar LDAPS del cliente, importe el certificado de la entidad de certificación (CA) en Conector AD y, a continuación, habilite LDAPS en el directorio. Tras la habilitación, todo el tráfico LDAP entre las aplicaciones de AWS y su instancia de Active Directory autoadministrada se realizará con el cifrado de canal SSL (Capa de conexión segura).

Puede utilizar dos métodos diferentes para habilitar LDAPS en el lado del cliente para su directorio. Puede utilizar el método de la AWS Management Console o AWS CLI.

Temas

Paso 1: registrar el certificado en AWS Directory Service

Utilice cualquiera de los métodos siguientes para registrar un certificado en AWS Directory Service.

Método 1: para registrar su certificado en AWS Directory Service (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).
4. En la sección Client-side LDAPS (LDAPS del lado del cliente), seleccione el menú Actions (Acciones) y, a continuación, seleccione Register certificate (Registrar certificado).
5. En el cuadro de diálogo Register a CA certificate (Registrar un certificado de entidad de certificación), seleccione Browse (Examinar) y, a continuación, seleccione el certificado y elija Open (Abrir).
6. Elija Register certificate (Registrar certificado).

Método 2: para registrar su certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando. Para los datos del certificado, elija la ubicación del archivo de certificado de CA. Se proporcionará un ID de certificado en la respuesta.

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

Paso 2: comprobar el estado del registro

Para ver el estado del registro de un certificado o una lista de certificados registrados, utilice uno de los métodos siguientes.

Método 1: para comprobar el estado del registro del certificado en AWS Directory Service (AWS Management Console)

1. Vaya a la sección Client-side LDAPS (LDAPS del lado del cliente) de la página Directory details (Detalles del directorio).

2. Revise el estado actual del registro de certificado que se muestra en la columna Registration status (Estado del registro). Cuando el valor de estado de registro cambia a Registered (Registrado), el certificado se ha registrado correctamente.

Método 2: para comprobar el estado del registro del certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando. Si el valor de estado devuelve `Registered`, el certificado se ha registrado correctamente.

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

Paso 3: habilitar LDAPS del cliente

Utilice cualquiera de los métodos siguientes para deshabilitar LDAPS en AWS Directory Service.

> **Note**
>
> Debe haber registrado correctamente al menos un certificado para poder habilitar LDAPS en el lado del cliente.

Método 1: para habilitar LDAPS en el lado cliente en AWS Directory Service (AWS Management Console)

1. Vaya a la sección Client-side LDAPS (LDAPS del lado del cliente) de la página Directory details (Detalles del directorio).
2. Elija Enable (Habilitar). Si esta opción no está disponible, compruebe que se ha registrado correctamente un certificado válido y vuelva a intentarlo.
3. En el cuadro de diálogo Enable client-side LDAPS (Habilitar LDAPS del lado del cliente), elija Enable (Habilitar).

Método 2: para habilitar LDAPS en el lado cliente en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando.

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

Paso 4: comprobar el estado de LDAPS

Utilice cualquiera de los métodos siguientes para comprobar el estado de LDAPS en AWS Directory Service.

Método 1: para comprobar el estado de LDAPS en AWS Directory Service (AWS Management Console)

1. Vaya a la sección Client-side LDAPS (LDAPS del lado del cliente) de la página Directory details (Detalles del directorio).
2. Si el valor de estado se muestra como Enabled (Habilitado), LDAPS se ha configurado correctamente.

Método 2: para comprobar el estado LDAPS en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando. Si el valor de estado devuelve `Enabled`, LDAPS se ha configurado correctamente.

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

Administración de LDAPS del cliente

Utilice estos comandos para administrar la configuración de LDAPS.

Puede utilizar dos métodos distintos para administrar la configuración de LDAPS del lado del cliente. Puede utilizar el método de la AWS Management Console o AWS CLI.

Ver detalles del certificado

Utilice cualquiera de los métodos siguientes para ver cuándo está establecida la caducidad de un certificado.

Método 1: para ver los detalles del certificado en AWS Directory Service (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).

4. En la sección Client-side LDAPS (LDAPS del lado del cliente), en CA certificates (Certificados de entidad de certificación), se mostrará la información del certificado.

Método 2: para ver los detalles del certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando. Para obtener el ID de certificado, utilice el identificador devuelto por `register-certificate` o `list-certificates`.

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

Anular el registro de un certificado

Utilice cualquiera de los métodos siguientes para anular el registro de un certificado.

> **Note**
>
> Si sólo se registra un certificado, primero debe deshabilitar LDAPS antes de anular el registro del certificado.

Método 1: para anular el registro de un certificado en AWS Directory Service (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).
4. En la sección Client-side LDAPS (LDAPS del lado del cliente), elija Actions (Acciones) y, a continuación, elija Deregister certificate (Anular registro del certificado).
5. En el cuadro de diálogo Deregister a CA certificate (Anular el registro del certificado de entidad de certificación), elija Deregister (Anular registro).

Método 2: para anular el registro de un certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando. Para obtener el ID de certificado, utilice el identificador devuelto por `register-certificate` o `list-certificates`.

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

Deshabilitar LDAPS del cliente

Utilice cualquiera de los métodos siguientes para deshabilitar LDAPS del lado del cliente.

Método 1: para deshabilitar LDAPS del lado del cliente en AWS Directory Service (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).
4. En la sección Client-side LDAPS (LDAPS del lado del cliente), elija Disable (Deshabilitar).
5. En el cuadro de diálogo Disable client-side LDAPS (Deshabilitar LDAPS del lado del cliente), elija Disable (Deshabilitar).

Método 2: para deshabilitar LDAPS del lado cliente en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando.

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

Habilitación de la autenticación mTLS en Conector AD para usarla con tarjetas inteligentes

Puede utilizar la autenticación mutua de Transport Layer Security (mTLS) basada en certificados con tarjetas inteligentes para autenticar a los usuarios en Amazon a WorkSpaces través de Active Directory (AD) y AD Connector autogestionados. Cuando está habilitada, los usuarios seleccionan su tarjeta inteligente en la pantalla de inicio de WorkSpaces sesión e introducen un PIN para autenticarse, en lugar de utilizar un nombre de usuario y una contraseña. A partir de ahí, el escritorio virtual de Windows o Linux utiliza la tarjeta inteligente para autenticarse en AD desde el sistema operativo nativo del escritorio.

> **Note**
>
> La autenticación con tarjeta inteligente en AD Connector solo está disponible en los siguientes Regiones de AWS casos y solo con WorkSpaces. Por el momento, no se admiten otras AWS aplicaciones.
>
> - Este de EE. UU. (Norte de Virginia)
> - Oeste de EE. UU. (Oregón)
> - Asia-Pacífico (Sídney)
> - Asia Pacífico (Tokio)
> - Europa (Irlanda)
> - AWS GovCloud (US-Oeste)

Temas

Requisitos previos

Para habilitar la autenticación mutua de Transport Layer Security (mTLS) basada en certificados mediante tarjetas inteligentes para el WorkSpaces cliente de Amazon, necesita una infraestructura de tarjetas inteligentes operativa integrada en su sistema autogestionado. Active Directory Para obtener más información sobre cómo configurar la autenticación con tarjeta inteligente con Amazon WorkSpaces Active Directory, consulta la Guía de WorkSpaces administración de Amazon.

Antes de activar la autenticación con tarjeta inteligente WorkSpaces, revise las siguientes consideraciones:

- Requisitos del certificado de CA
- Requisitos del certificado de usuario
- Proceso de comprobación de la revocación de certificados
- Otras consideraciones

Requisitos del certificado de CA

Conector AD requiere un certificado de entidad de certificación (CA), que representa al emisor de los certificados de usuario, para la autenticación con tarjeta inteligente. Conector AD hace coincidir los certificados de CA con los certificados presentados por los usuarios con sus tarjetas inteligentes. Tenga en cuenta los siguientes requisitos de los certificados de CA:

- Antes de registrar un certificado de CA, deben quedar más de 90 días para que caduque.
- Los certificados de CA deben estar en formato Privacy-Enhanced Mail (PEM). Si exporta certificados de CA desde Active Directory, elija X.509 (.CER) codificado en base64 como formato de archivo de exportación.
- Para que la autenticación con tarjeta inteligente se haga correctamente, se deben cargar todos los certificados de CA raíz e intermediaria que van desde la CA emisora hasta los certificados de usuario.
- Se puede almacenar un máximo de 100 certificados de entidad de certificación por directorio del Conector AD.
- Conector AD no admite el algoritmo de firma RSASSA-PSS para los certificados de CA.
- Compruebe que el Servicio de propagación de certificados esté configurado como Automático y en ejecución.

Requisitos del certificado de usuario

Los siguientes son algunos de los requisitos del certificado de usuario:

- El certificado de tarjeta inteligente del usuario tiene un nombre alternativo del sujeto (SAN) del usuario userPrincipalName (UPN).
- El certificado de tarjeta inteligente del usuario tiene un uso de claves mejorado al iniciar sesión con la tarjeta inteligente (1.3.6.1.4.1.311.20.2.2). Autenticación del cliente (1.3.6.1.5.5.7.3.2).
- La información del Protocolo de estado de certificados en línea (OCSP) para el certificado de tarjeta inteligente del usuario debe ser Método de acceso = Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) en el Authority Information Access.

Para obtener más información sobre los requisitos de autenticación de AD Connector y tarjetas inteligentes, consulta los requisitos de la Guía de WorkSpaces administración de Amazon. Para obtener ayuda para solucionar WorkSpaces problemas de Amazon, como iniciar sesión WorkSpaces,

restablecer la contraseña o conectarse a WorkSpaces, consulta Solución de problemas con los WorkSpaces clientes en la Guía WorkSpaces del usuario de Amazon.

Proceso de comprobación de la revocación de certificados

Para llevar a cabo la autenticación con tarjeta inteligente, Conector AD debe comprobar el estado de revocación de los certificados de usuario mediante el protocolo Online Certificate Status Protocol (OCSP). Para llevar a cabo la comprobación la revocación de certificados, la URL de un agente de respuesta OCSP ser accesible desde Internet. Si usa un nombre de DNS, la URL de un agente de respuesta OCSP debe usar un dominio de nivel superior que se encuentre en la Base de datos de la zona raíz de la Internet Assigned Numbers Authority (IANA).

La comprobación de revocación de certificados del Conector AD utiliza el siguiente proceso:

- Conector AD debe comprobar la extensión Authority Information Access (AIA) del certificado de usuario para una URL del agente de respuesta OCSP y, a continuación, Conector AD utiliza la URL para comprobar la revocación.
- Si Conector AD no puede resolver la URL que se encuentra en la extensión AIA del certificado de usuario o encuentra una URL del agente de respuesta OCSP en el certificado de usuario, Conector AD utiliza la URL de OCSP opcional proporcionada durante el registro del certificado de CA raíz.

  Si la URL de la extensión AIA del certificado de usuario se resuelve, pero no tiene respuesta, se produce un error en la autenticación del usuario.
- Si la URL del agente de respuesta OCSP proporcionada durante el registro del certificado de CA raíz no se resuelve, no responde o, en cambio, no se proporcionó ninguna URL del agente de respuesta OCSP, se producirá un error en la autenticación del usuario.
- El servidor OCSP debe cumplir con la RFC 6960. Además, el servidor OCSP debe admitir las solicitudes que utilicen el método GET para las solicitudes que tengan un total de 255 bytes o menos.

> **Note**
>
> Conector AD requiere una URL HTTP para la URL del agente de respuesta OCSP.

Otras consideraciones

Antes de habilitar la autenticación con tarjeta inteligente en Conector AD, tenga en cuenta lo siguiente:

- Conector AD utiliza la autenticación Mutual Transport Layer Security (mutual TLS) basada en certificados para autenticar a los usuarios en Active Directory mediante certificados de tarjetas inteligentes basados en hardware o software. Por el momento, solo se admiten las tarjetas de acceso común (CAC) y las tarjetas de verificación de identidad personal (PIV). Es posible que funcionen otros tipos de tarjetas inteligentes basadas en hardware o software, pero no se han probado para su uso con el Protocolo de WorkSpaces transmisión.
- La autenticación con tarjeta inteligente sustituye a la autenticación por nombre de usuario y contraseña por WorkSpaces.

  Si tiene otras AWS aplicaciones configuradas en el directorio de AD Connector con la autenticación con tarjeta inteligente habilitada, esas aplicaciones seguirán presentando la pantalla de introducción de nombre de usuario y contraseña.
- Al habilitar la autenticación con tarjeta inteligente, se limita la duración de la sesión del usuario a la duración máxima de los tickets de servicio de Kerberos. Puede configurar esta opción mediante una política de grupo (de forma predeterminada, está configurada en 10 horas). Para obtener más información sobre esta configuración, consulte la documentación de Microsoft.
- El tipo de cifrado Kerberos compatible con la cuenta de servicio del Conector AD debe coincidir con todos los tipos de cifrado Kerberos compatibles con el controlador de dominio.

Habilitación de la autenticación con tarjeta inteligente

Para habilitar la autenticación con tarjeta inteligente WorkSpaces en el AD Connector, primero debe importar los certificados de la entidad de certificación (CA) al AD Connector. Puede importar sus certificados de CA a AD Connector mediante la AWS Directory Service consola, la API o la CLI. Siga estos pasos para importar los certificados de CA y, posteriormente, habilitar la autenticación con tarjeta inteligente.

Temas

- Paso 3: habilitación de la autenticación con tarjeta inteligente para las aplicaciones y los servicios de AWS compatibles

Paso 1: habilitación de la delegación restringida de Kerberos para la cuenta de servicio del Conector AD

Para usar la autenticación con tarjeta inteligente con Conector AD, debe habilitar la delegación limitada de Kerberos (KCD) para la cuenta del servicio del Conector AD en el servicio LDAP del directorio AD autoadministrado.

La delegación limitada de Kerberos es una característica de Windows Server. Esta característica les permite a los administradores del servicio especificar y aplicar límites de confianza en una aplicación limitando el alcance hasta el que pueden actuar los servicios de esta última en representación de un usuario. Para obtener más información, consulte Delegación limitada de Kerberos.

> **Note**
>
> La delegación restringida de Kerberos (KCD) requiere que la parte del nombre de usuario de la cuenta de servicio AD Connector coincida con el SaM AccountName del mismo usuario. El SaM AccountName está restringido a 20 caracteres. SaM AccountName es un atributo de Microsoft Active Directory que se utiliza como nombre de inicio de sesión en versiones anteriores de clientes y servidores de Windows.

1. Use el comando `SetSpn` para establecer un nombre principal de servicio (SPN) para la cuenta de servicio del Conector AD en el AD autoadministrado. Esto habilita la cuenta de servicio para la configuración de delegación.

   El SPN puede ser cualquier combinación de servicios o nombres, pero no un duplicado de un SPN existente. `-s` comprueba si hay duplicados.

   ```
   setspn -s my/spn service_account
   ```

2. En Usuarios y equipos de AD, abra el menú contextual (haga clic con el botón derecho), elija la cuenta de servicio del Conector AD y elija Propiedades.
3. Seleccione la pestaña Delegación.
4. Elija las opciones Confiar en este usuario para delegar únicamente en el servicio especificado y Utilizar cualquier protocolo de autenticación.

5. Seleccione Agregar y, a continuación, Usuarios o equipos para localizar el controlador de dominio.
6. Haga clic en Aceptar para mostrar una lista de los servicios disponibles que se utilizan para la delegación.
7. Elija el tipo de servicio ldap y seleccione Aceptar.
8. Elija Aceptar para guardar la nueva configuración.
9. Repita este proceso para otros controladores de dominio de Active Directory. Como alternativa, puede automatizar el proceso utilizando PowerShell.

Paso 2: registro del certificado de CA en Conector AD

Utilice uno de los métodos siguientes para registrar un certificado de CA para el directorio del Conector AD.

Método 1: para registrar su certificado de CA en Conector AD (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).
4. En la sección Autenticación con tarjeta inteligente, seleccione Acciones y, a continuación, seleccione Registrar certificado.
5. En el cuadro de diálogo Registrar un certificado, seleccione Elegir archivo y, a continuación, seleccione un certificado y elija Abrir. Si lo desea, puede llevar a cabo una comprobación de revocación de este certificado al proporcionar una URL del agente de respuesta OCSP del Protocolo Online Certificate Status Protocol (OCSP). Para obtener más información acerca de OCSP, consulte Proceso de comprobación de la revocación de certificados.
6. Elija Register certificate (Registrar certificado). Cuando vea que el estado del certificado cambia a Registrado, el proceso de registro se habrá completado correctamente.

Método 2: para registrar su certificado de CA en Conector AD (AWS CLI)

- Ejecute el siguiente comando de la . Para los datos del certificado, elija la ubicación del archivo de certificado de CA. Para proporcionar una dirección secundaria del agente de respuesta OCSP, utilice el 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
```

Si se ejecuta correctamente, la respuesta proporciona un ID de certificado. También puede comprobar que el certificado de CA se ha registrado correctamente al ejecutar el siguiente comando de la CLI:

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

Si el valor de estado devuelve `Registered`, el certificado se ha registrado correctamente.

Paso 3: habilitación de la autenticación con tarjeta inteligente para las aplicaciones y los servicios de AWS compatibles

Utilice uno de los métodos siguientes para registrar un certificado de CA para el directorio del Conector AD.

Método 1: habilitación de la autenticación con tarjeta inteligente en Conector AD (AWS Management Console)

1. Vaya a la sección Autenticación con tarjeta inteligente en la página Detalles del directorio y seleccione Habilitar. Si esta opción no está disponible, compruebe que se ha registrado correctamente un certificado válido y vuelva a intentarlo.
2. En el cuadro de diálogo Habilitar la autenticación con tarjeta inteligente, seleccione Habilitar.

Método 2: para habilitar la autenticación con tarjeta inteligente en Conector AD (AWS CLI)

- Ejecute el siguiente comando de la .

```
aws ds enable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Si se hace correctamente, Conector AD devuelve una respuesta `HTTP 200` con un cuerpo HTTP vacío.

Administrar la configuración de autenticación con tarjeta inteligente

Puede utilizar dos métodos distintos para administrar la configuración de la tarjeta inteligente. Puedes usar el AWS Management Console método o el AWS CLI método.

Temas

Ver detalles del certificado

Utilice cualquiera de los métodos siguientes para ver cuándo está establecida la caducidad de un certificado.

Método 1: para ver los detalles del certificado en AWS Directory Service (AWS Management Console)

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el vínculo del ID de su directorio del Conector AD.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).
4. En la sección Autenticación con tarjeta inteligente, en Certificados de CA, elija el ID de certificado para ver los detalles de dicho certificado.

Método 2: ver los detalles del certificado en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando de la . Para obtener el ID de certificado, utilice el identificador devuelto por `register-certificate` o `list-certificates`.

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

Anular el registro de un certificado

Utilice cualquiera de los métodos siguientes para anular el registro de un certificado.

> **Note**
>
> Si sólo se registra un certificado, primero debe deshabilitar la autenticación con tarjeta inteligente antes de anular el registro del certificado.

Método 1: anular el registro de un certificado en AWS Directory Service ()AWS Management Console

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el vínculo del ID de su directorio del Conector AD.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).
4. En la sección Autenticación con tarjeta inteligente, en Certificados de CA, seleccione el certificado que desee anular del registro, elija Acciones y, a continuación, elija Anular el registro del certificado.

   > **Important**
   >
   > Asegúrese de que el certificado que va a anular del registro no esté activo o esté actualmente en uso como parte de una cadena de certificados de CA para la autenticación con tarjeta inteligente.

5. En el cuadro de diálogo Deregister a CA certificate (Anular el registro del certificado de entidad de certificación), elija Deregister (Anular registro).

Método 2: anular el registro de un certificado en () AWS Directory ServiceAWS CLI

- Ejecute el siguiente comando de la . Para obtener el ID de certificado, utilice el identificador devuelto por `register-certificate` o `list-certificates`.

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

Deshabilitación de la autenticación con tarjeta inteligente

Utilice uno de los métodos siguientes para deshabilitar la autenticación con tarjeta inteligente.

Método 1: deshabilitar la autenticación con tarjeta inteligente en AWS Directory Service ()AWS Management Console

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. Elija el vínculo del ID de su directorio del Conector AD.
3. En la página Directory details (Detalles del directorio), elija la pestaña Networking & security (Redes y seguridad).
4. En la sección Autenticación con tarjeta inteligente, seleccione Deshabilitar.
5. En el cuadro de diálogo Deshabilitar la autenticación con tarjeta inteligente, seleccione Deshabilitar.

Método 2: deshabilitar la autenticación con tarjeta inteligente en AWS Directory Service (AWS CLI)

- Ejecute el siguiente comando de la .

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Configurar el AWS Private CA conector para AD

Puede integrar su Active Directory (AD) autogestionado con AWS Private Certificate Authority (CA) con AD Connector para emitir y administrar certificados para los usuarios, grupos y máquinas unidos al dominio de AD. AWS Private CA Connector para AD te permite utilizar un sustituto directo y AWS Private CA totalmente gestionado para tus CA empresariales autogestionadas sin necesidad de implementar, aplicar parches o actualizar agentes locales o servidores proxy.

Puede configurar la AWS Private CA integración con su directorio a través de la consola Directory Service, la consola AWS Private CA Connector for AD o llamando a la `CreateTemplate`API. Para configurar la integración de una CA privada a través de la consola de AWS Private CA Connector for Active Directory, consulte AWS Private CA Connector for Active Directory. Consulte a continuación los pasos para configurar esta integración desde la AWS Directory Service consola.

Requisitos previos

Cuando usa Conector AD, debe delegar permisos adicionales a la cuenta de servicio. Configure la lista de control de acceso (ACL) en su cuenta de servicio para poder hacer lo siguiente.

- Agregue y elimine un nombre principal del servicio (SPN) para sí mismo.

- Cree y actualice las entidades de certificación en los siguientes contenedores:

```
#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
```

- Cree y actualice un objeto de autoridad AuthCertificates de certificación de NT como se muestra en el ejemplo siguiente. Si el objeto de la entidad de AuthCertificates certificación de NT existe, debe delegar los permisos para él. Si el objeto no existe, debe delegar la capacidad de crear objetos secundarios en el contenedor de servicios de clave pública.

```
#objects
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

> **Note**
>
> Si utiliza Microsoft AD AWS administrado, los permisos adicionales se delegarán automáticamente cuando autorice el servicio AWS Private CA Connector for AD con su directorio.

Puede usar el siguiente PowerShell script para delegar los permisos adicionales y crear el objeto de entidad emisora de AuthCertifiates certificados de NT. Sustituya “myconnectoraccount” por el nombre de la cuenta de servicio.

```
$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 AWS Private CA Connector para AD

1. Inicie sesión en AWS Management Console y abra la AWS Directory Service consola enhttps://console.aws.amazon.com/directoryservicev2/.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la pestaña Red y seguridad, en AWS Private CA Conector para AD, selecciona Configurar AWS Private CA conector para AD. Active DirectoryAparece la página Crear un certificado de CA privado para. Siga los pasos de la consola para crear su CA privada para que el Active Directory conector se inscriba en su CA privada. Para obtener más información, consulte Creación de un conector.
4. Después de crear el conector, siga los pasos que se indican a continuación para ver los detalles, incluido el estado del conector y el estado de la entidad de certificación (CA) privada asociada.

Para ver AWS Private CA Connector for AD

1. Inicie sesión en AWS Management Console y abra la AWS Directory Service consola enhttps://console.aws.amazon.com/directoryservicev2/.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En Redes y seguridad, en Conector para AD deAWS Private CA , puede ver sus tanto sus conectores de entidad de certificación (CA) privados como las entidades de certificación (CA) asociadas. De forma predeterminada, verá los siguientes campos:

a. AWS Private CA ID de conector: el identificador único de un AWS Private CA conector. Al hacer clic en él, se accede a la página de detalles de ese AWS Private CA conector.

b. AWS Private CA asunto: información sobre el nombre distintivo de la CA. Al hacer clic en él, se accede a la página de detalles de AWS Private CA.

c. Estado: basado en una verificación de estado del AWS Private CA conector y del AWS Private CA. Si se aprueban ambas comprobaciones, aparecerá Activo. Si una de las comprobaciones falla, aparece 1/2 comprobaciones con errores. Si ambas comprobaciones fallan, aparece Error. Para obtener más información sobre un estado fallido, coloque el puntero del ratón sobre el hipervínculo para saber qué comprobación tuvo errores. Siga las instrucciones de la consola para solucionarlo.

d. Fecha de creación: el día en que se creó el AWS Private CA conector.

Para obtener más información, consulte View connector details.

Supervisión del directorio de Conector AD

Puede supervisar su directorio de Conector AD con los siguientes métodos:

Temas

- Descripción del estado del directorio
- Configurar las notificaciones de estado del directorio con Amazon SNS

Descripción del estado del directorio

Estos son los diferentes estados de un directorio.

Activo

El directorio funciona con normalidad. AWS Directory Service no ha detectado problemas en su directorio.

Creando

El directorio se está creando en estos momentos. Los directorios suelen tardar entre 20 y 45 minutos en crearse, pero esto depende de la carga del sistema.

Eliminado

El directorio se ha eliminado. Se han liberado todos los recursos para el directorio. Una vez que un directorio entra en este estado, no se puede recuperar.

Eliminando

El directorio se está eliminando. El directorio permanecerá en este estado hasta que se haya eliminado por completo. Una vez que un directorio entra en este estado, la operación de eliminación no se puede cancelar y el directorio no se puede recuperar.

Con error

No se pudo crear el directorio. Elimine este directorio. Si este problema sigue sin resolverse, contacte con el Centro de AWS Support.

Deteriorado

El directorio se está ejecutando en estado degradado. Se han detectado uno o varios problemas y no todas las operaciones de directorios pueden funcionar con plena capacidad operativa. Hay muchas razones posibles para que el directorio se encuentre en este estado. Entre ellas se incluyen las actividades normales de mantenimiento operativo, como la aplicación de parches o la rotación de instancias de EC2, la sobrecarga provocada por una aplicación en uno de los controladores de dominio o los cambios que haga en la red que interrumpan de forma inadvertida las comunicaciones del directorio. Para obtener más información, consulte Solución de problemas de Microsoft AD AWS administrado, Solución de problemas de Conector AD y Solución de problemas de Simple AD. En el caso de problemas normales relacionados con el mantenimiento, los AWS resuelve en 40 minutos. Si después de revisar el tema de solución de problemas, su directorio sigue dañado durante más de 40 minutos, le recomendamos que contacte con el Centro de AWS Support.

> **Important**
>
> No restaure una instantánea mientras el directorio esté deteriorado. Es poco frecuente que la restauración de las instantáneas sea necesaria para resolver los problemas. Para obtener más información, consulte Creación de una instantánea o restauración del directorio.

Inoperable

El directorio no es funcional. Todos los puntos de enlace del directorio han informado de la existencia de problemas.

Solicitada

Actualmente hay pendiente una solicitud para crear su directorio.

Configurar las notificaciones de estado del directorio con Amazon SNS

Mediante Amazon Simple Notification Service (Amazon SNS), puede recibir mensajes de correo electrónico o de texto (SMS) cuando cambie el estado del directorio. Puede recibir notificaciones si el directorio pasa de un estado Activo a un estado Deteriorado o Inoperativo. También recibirá una notificación cuando el directorio vuelva a estar en estado activo.

Cómo funcionan

Amazon SNS utiliza “temas” para recopilar y distribuir mensajes. Cada tema cuenta con uno o varios suscriptores que reciben los mensajes que se han publicado en dicho tema. Si sigue los pasos que se indican a continuación, puede añadir AWS Directory Service un editor a un tema de Amazon SNS. Cuando AWS Directory Service detecta un cambio en el estado de su directorio, publica un mensaje sobre ese tema, que luego se envía a los suscriptores del tema.

Puede asociar varios directorios como publicadores a un único tema. También puede agregar mensajes de estado del directorio a los temas que ha creado anteriormente en Amazon SNS. Tiene un control detallado sobre quién puede publicar un tema y suscribirse a él. Para obtener información completa sobre Amazon SNS, consulte ¿Qué es Amazon SNS?.

Habilitación de la mensajería SNS para su directorio

1. Inicia sesión en la AWS Directory Service consola AWS Management Console y ábrela.
2. En la página Directories (Directorios), elija el ID del directorio.
3. Seleccione la pestaña Mantenimiento.
4. En la sección Supervisión de directorios, elija Acciones y, a continuación, seleccione Crear notificación.
5. En la página Crear notificación, seleccione Elegir un tipo de notificación y, a continuación, Crear una nueva notificación. También, si ya dispone de un tema de SNS, puede seleccionar Asociar un tema de SNS existente para enviar mensajes de estado desde este directorio a ese tema.

> **Note**
>
> Si elige Crear una nueva notificación, pero, a continuación, utiliza el mismo nombre para un tema de SNS que ya existe, Amazon SNS no creará un nuevo tema, sino que tan solo agregará la información de la nueva suscripción al existente.
> Si selecciona Asociar tema de SNS existentes, solo podrá elegir un tema de SNS que se encuentre en la misma región que el directorio.

6. Elija una opción en Tipo de destinatario e ingrese la información del contacto en Destinatario. Si escribe un número de teléfono para SMS, utilice solo números. No incluya guiones, espacios o paréntesis.
7. (Opcional) Proporcione un nombre para su tema y un nombre de visualización de SNS. El nombre de visualización es una abreviatura de hasta 10 caracteres que se incluye en todos los mensajes SMS de este tema. Cuando se utiliza la opción de SMS, es necesario el nombre de visualización.

> **Note**
>
> Si ha iniciado sesión con un usuario o rol de IAM que solo tiene la política DirectoryServiceFullAccessadministrada, el nombre del tema debe empezar por «DirectoryMonitoring». Si desea personalizar aún más su nombre de tema necesitará privilegios adicionales de SNS.

8. Seleccione Crear.

Si desea designar suscriptores de SNS adicionales, como una dirección de correo electrónico adicional, colas de Amazon SQS, AWS Lambdao puede hacerlo desde la consola de Amazon SNS.

Habilitación de mensajes de estado del directorio de un tema

1. Inicie sesión en la consola AWS Management Console y ábrala.AWS Directory Service
2. En la página Directories (Directorios), elija el ID del directorio.
3. Seleccione la pestaña Mantenimiento.
4. En la sección Supervisión de directorios, seleccione un nombre de tema de SNS de la lista, elija Acciones y, a continuación, seleccione Eliminar.
5. Elija Eliminar.

Así eliminará su directorio como publicador en el tema de SNS seleccionado. Si quieres eliminar todo el tema, puedes hacerlo desde la consola de Amazon SNS.

> **Note**
>
> Antes de eliminar un tema de Amazon SNS mediante la consola de SNS, debe asegurarse de que un directorio no está enviando mensajes de estado a dicho tema.
> Si elimina un tema de Amazon SNS mediante la consola de SNS, este cambio no se reflejará inmediatamente en la consola de Directory Services. Solo se le informaría la próxima vez que un directorio publique una notificación en el tema eliminado, en cuyo caso vería un estado actualizado en la pestaña Monitoring del directorio que indica que no se ha encontrado el tema.
> Por lo tanto, para evitar perder mensajes importantes sobre el estado del directorio, antes de eliminar cualquier tema del que reciba mensajes AWS Directory Service, asocie su directorio a un tema diferente de Amazon SNS.

Unir una instancia de Amazon EC2 a su Active Directory

AD Connector es una puerta de enlace de directorios con la que puedes redirigir las solicitudes de directorio a tu entorno local Microsoft Active Directory sin almacenar en caché ninguna información en la nube. A continuación, encontrará más información sobre cómo unir una instancia de Amazon EC2 a un dominio de Active Directory:

- Puede unir sin problemas una instancia de Amazon EC2 a su Active Directory dominio cuando se lance la instancia. Para obtener más información, consulte Una sin problemas una Windows instancia de Amazon EC2 a su AWS Microsoft AD gestionado con AD Connector.
- Si necesita unir manualmente una instancia EC2 a su Active Directory dominio, debe lanzar la instancia en el grupo o subred de seguridad adecuado Región de AWS y, a continuación, unir la instancia al dominio. Active Directory
- Para poder conectarse de forma remota a estas instancias, debe disponer de conectividad IP a las instancias desde la red en la que se está conectando. En la mayoría de los casos, esto requiere conectar una puerta de enlace de Internet a su Amazon VPC y que la instancia tenga una dirección IP pública. Para obtener más información sobre las puertas de enlace de Internet, consulte Conectar subredes a Internet por medio de una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.

> **Note**
>
> Una vez que unes una instancia a tu servidor autogestionado Active Directory (local), la instancia se comunica directamente con tu AD Connector Active Directory y lo omite.

Temas

Una sin problemas una Windows instancia de Amazon EC2 a su AWS Microsoft AD gestionado con AD Connector

Este procedimiento une sin problemas una Windows instancia de Amazon EC2 a su AWS Microsoft AD administrado. Active Directory

Para unirse sin problemas a una instancia EC2 Windows

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, elija el Región de AWS mismo directorio que el existente.
3. En el panel de control de EC2, en la sección Lanzar instancia, elija Lanzar instancia.
4. En la página Lanzar una instancia, en la sección Nombre y etiquetas, ingrese el nombre que desee utilizar para la instancia de EC2 de Windows.
5. (Opcional) Elija Agregar etiquetas adicionales para agregar uno o varios pares clave-valor de etiqueta para organizar o controlar el acceso a esta instancia de EC2 o hacer su seguimiento.
6. En la sección Imagen de aplicación y sistema operativo (Imagen de máquina de Amazon), elija Windows en el panel Inicio rápido. Puede cambiar la imagen de máquina de Amazon (AMI) de Windows desde la lista desplegable Imagen de máquina de Amazon (AMI).
7. En la sección Tipo de instancia, elija el tipo de instancia que desee usar en la lista desplegable Tipo de instancia.
8. En la sección Par de claves (inicio de sesión), puede elegir entre crear un nuevo par de claves o elegir un par de claves existente.

a. Para crear un nuevo par de claves, elija Crear nuevo par de claves.
b. Ingrese un nombre para el par de claves y seleccione una opción en Tipo de par de claves y Formato de archivo de clave privada.
c. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija .pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija .ppk.
d. Elija Crear par de claves.
e. Su navegador descargará el archivo de clave privada automáticamente. Guarde el archivo de clave privada en un lugar seguro.

> **Important**
>
> Esta es la única oportunidad para guardar el archivo de clave privada.

9. En la página Lanzar una instancia, en la sección Configuración de red, elija Editar. Elija la VPC en la que se creó el directorio en la lista desplegable VPC: obligatoria.
10. Elija una de las subredes públicas de su VPC en la lista desplegable Subred. La subred que elija debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.

    Para obtener más información sobre cómo conectar una puerta de enlace de Internet, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.
11. En Autoasignar IP pública, elija Habilitar.

    Para obtener más información sobre el direccionamiento IP público y privado, consulte el direccionamiento IP de las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.
12. En la configuración Firewall (grupos de seguridad), puede usar la configuración predeterminada o hacer cambios para adaptarla a sus necesidades.
13. En la configuración Configurar almacenamiento, puede utilizar los ajustes predeterminados o hacer los cambios necesarios para adaptarlos a sus necesidades.
14. Seleccione la sección Detalles avanzados y elija su dominio en la lista desplegable Directorio de unión de dominios.

> **Note**
>
> Tras elegir el directorio de unión de dominios, es posible que vea:

> An error was detected in your existing SSM document. You can delete the existing SSM document here and we'll create a new one with correct properties on instance launch.

Este error se produce si el asistente de lanzamiento de EC2 identifica un documento SSM existente con propiedades inesperadas. Puede elegir una de las opciones siguientes:

- Si ya ha editado el documento SSM y las propiedades son las esperadas, seleccione cerrar y proceda a lanzar la instancia de EC2 sin cambios.
- Seleccione el enlace para eliminar el documento SSM existente aquí para eliminar el documento SSM. Esto permitirá crear un documento SSM con las propiedades correctas. El documento SSM se creará automáticamente al lanzar la instancia EC2.

15. En Perfil de instancia de IAM, puede seleccionar un perfil de instancia de IAM existente o crear uno nuevo. Seleccione un perfil de instancia de IAM que tenga DirectoryServiceAccess adjuntas las políticas AWS administradas AmazonSSM ManagedInstanceCore y AmazonSSM en la lista desplegable de perfiles de instancias de IAM. Para crear uno nuevo, elija el enlace Crear un nuevo perfil de IAM y, a continuación, haga lo siguiente:

    1. Elija Crear rol.
    2. En Seleccionar tipo de entidad de confianza, elija Servicio de AWS .
    3. En Caso de uso, elija EC2.
    4. En Añadir permisos, en la lista de políticas, seleccione las políticas de AmazonSSM ManagedInstanceCore y AmazonSSM. DirectoryServiceAccess Para filtrar la lista, escriba **`SSM`** en el cuadro de búsqueda. Elija Siguiente.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess proporciona los permisos para unir instancias a una instancia gestionada por. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore proporciona los permisos mínimos necesarios para usar el servicio. AWS Systems Manager Para obtener más información sobre la creación de un rol con estos permisos y para obtener información sobre otros permisos y políticas

que puede asignar a su rol de IAM, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

5. En la página Asignar un nombre, revisar, crear, ingrese un Nombre de rol. Necesitará este nombre de rol para asociarlo a la instancia de EC2.
6. (Opcional) Puede proporcionar una descripción del perfil de instancia de IAM en el campo Descripción.
7. Elija Crear rol.
8. Vuelva a la página Lanzar una instancia y elija el icono de actualización situado junto al perfil de instancia de IAM. El nuevo perfil de instancia de IAM debería estar visible en la lista desplegable Perfil de instancia de IAM. Elija el nuevo perfil y deje el resto de la configuración con sus valores predeterminados.

16. Seleccione Iniciar instancia.

Una sin problemas una instancia Linux de Amazon EC2 a su AWS Microsoft AD gestionado con AD Connector

Este procedimiento une sin problemas una instancia Linux de Amazon EC2 a su directorio gestionado de AWS Microsoft AD.

Son compatibles las siguientes distribuciones y versiones de instancias de Linux:

- 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 y Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Las distribuciones anteriores a Ubuntu 14 y Red Hat Enterprise Linux 7 no admiten la característica de unión fluida de dominios.

Requisitos previos

Antes de poder configurar una unión de dominio perfecta a una instancia EC2 de Linux, debe completar los procedimientos de esta sección.

Selección de la cuenta de servicio de unión de dominios fluida

Puede unir sin problemas ordenadores Linux a su Active Directory dominio local a través de AD Connector. Para ello, debe crear una cuenta de usuario con permisos de creación de cuentas de equipos para unir los equipos al dominio. Si lo prefiere, puede utilizar su cuenta de servicio de Conector AD. O bien, puede usar cualquier otra cuenta que tenga privilegios suficientes para unir equipos al dominio. Si bien es posible que los miembros de los administradores del dominio u otros grupos tengan privilegios suficientes para unir los equipos al dominio, no lo recomendamos. Como práctica recomendada, le recomendamos que utilice una cuenta de servicio que tenga los privilegios mínimos necesarios para unir los equipos al dominio.

Para delegar una cuenta con los privilegios mínimos necesarios para unir los ordenadores al dominio, puedes ejecutar los siguientes PowerShell comandos. Debe ejecutar estos comandos desde un Windows equipo unido a un dominio que tenga el Instalación de las herramientas de administración de Active Directory para Microsoft AD AWS administrado instalado. Además, debe utilizar una cuenta que tenga permiso para modificar los permisos de la unidad organizativa o el contenedor del equipo. El PowerShell comando establece los permisos que permiten a la cuenta de servicio crear objetos de ordenador en el contenedor de ordenadores predeterminado del dominio. Si prefiere utilizar una interfaz de usuario gráfica (GUI), puede utilizar el proceso manual que se describe en Privilegios delegados a su cuenta de servicio.

```
$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"
```

Si prefiere utilizar una interfaz de usuario gráfica (GUI), puede utilizar el proceso manual descrito en Privilegios delegados a su cuenta de servicio.

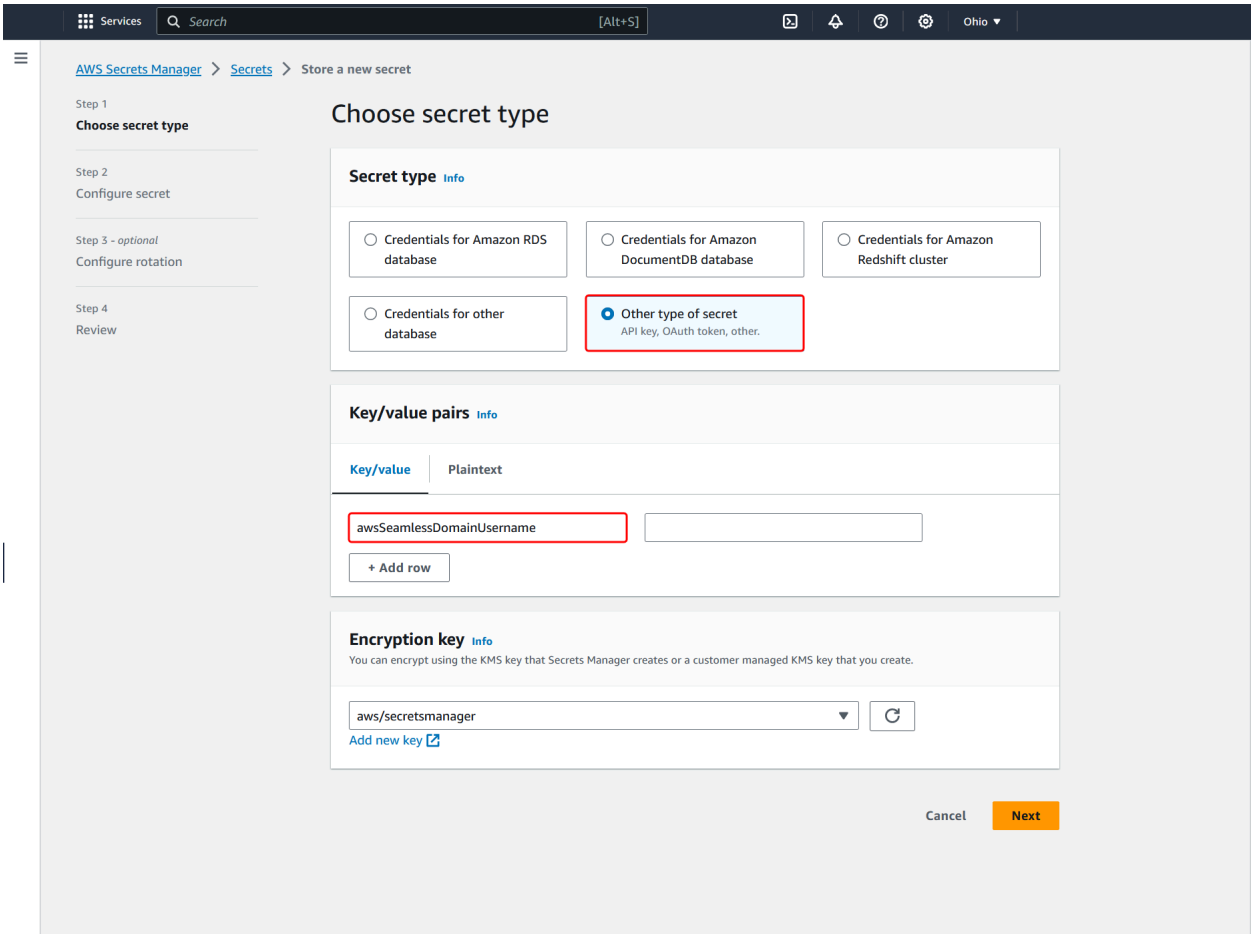
Creación de secretos para almacenar la cuenta de servicio de dominio

Puede utilizarlos AWS Secrets Manager para almacenar la cuenta de servicio del dominio.

Creación de secretos y almacenamiento de la información de la cuenta de servicio de dominio

1. Inicie sesión AWS Management Console y abra la AWS Secrets Manager consola en https://console.aws.amazon.com/secretsmanager/.
2. Elija Almacenar un secreto nuevo.
3. En la página Store a new secret (Almacenar un nuevo secreto), haga lo siguiente:
   a. En Tipo de secreto, seleccione Otro tipo de secretos.
   b. En Pares clave/valor, haga lo siguiente:
      i. En el cuadro de filtro, escriba **`awsSeamlessDomainUsername`**. En la misma fila, en el cuadro siguiente, introduce el nombre de usuario de tu cuenta de servicio. Por ejemplo, si utilizó el PowerShell comando anteriormente, el nombre de la cuenta de servicio sería**`awsSeamlessDomain`**.

> **Note**
>
> Debe ingresar **`awsSeamlessDomainUsername`** exactamente como está. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.



ii. Seleccione Agregar regla.

iii. En la nueva fila, en el primer cuadro, ingrese **`awsSeamlessDomainPassword`**. En la misma fila, en el cuadro siguiente, ingrese la contraseña de su cuenta de servicio.

> **Note**
>
> Debe ingresar **`awsSeamlessDomainPassword`** exactamente como está. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.

iv. En Clave de cifrado, deje el valor predeterminado`aws/secretsmanager`. AWS Secrets Manager siempre cifra el secreto al elegir esta opción. También puede elegir una clave que haya creado.

> **Note**
>
> Hay tarifas asociadas AWS Secrets Manager, según el secreto que utilices. Para obtener la lista de precios completa, consulte Precios de AWS Secrets Manager.
>
> Puedes usar la clave AWS gestionada `aws/secretsmanager` que crea Secrets Manager para cifrar tus secretos de forma gratuita. Si crea sus propias claves de KMS para cifrar sus secretos, se le AWS cobrará la tarifa actual AWS KMS . Para obtener más información, consulte AWS Key Management Service Precios.

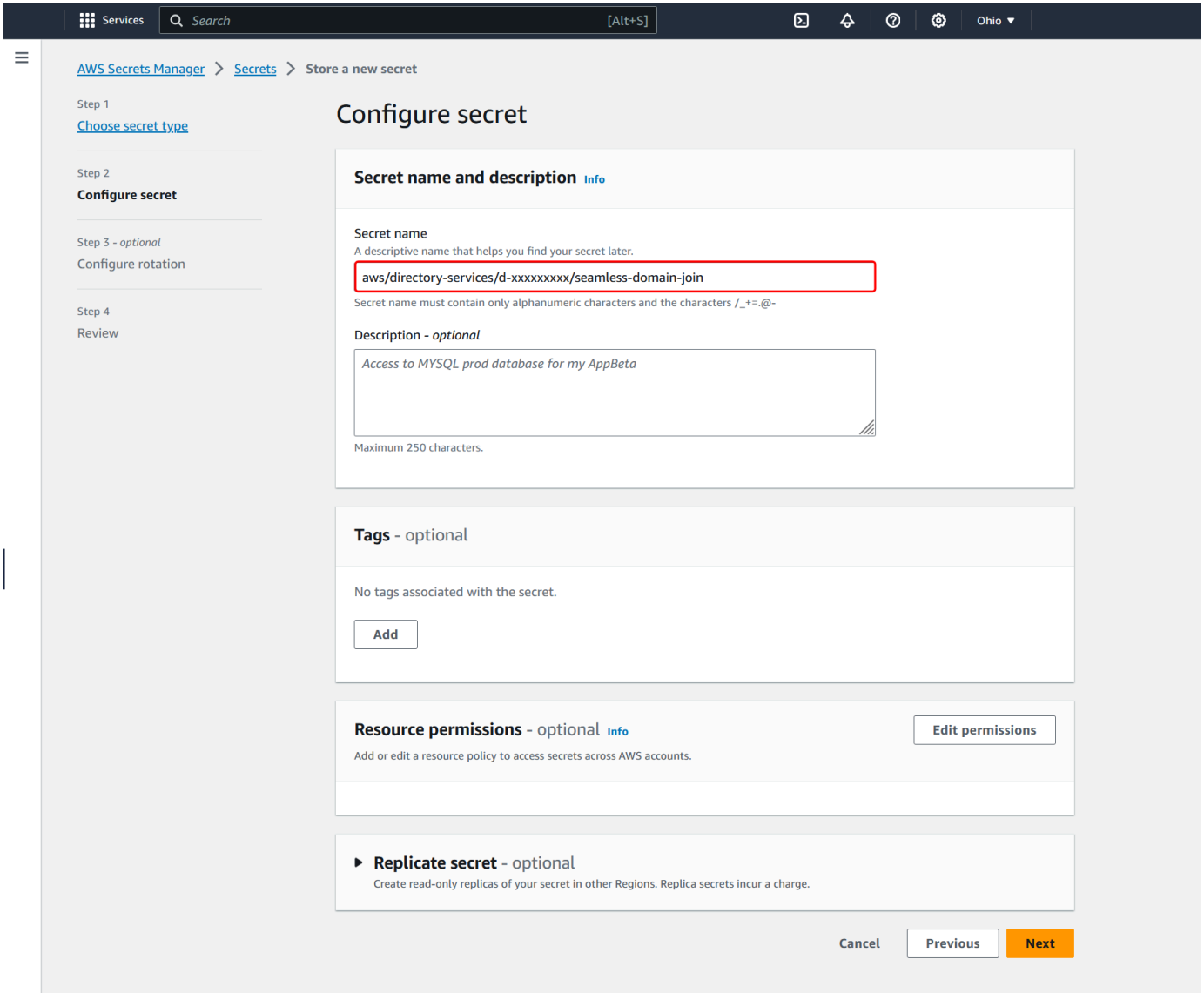
v. Elija Siguiente.

4. En Nombre secreto, introduzca un nombre secreto que incluya su ID de directorio con el siguiente formato y sustituya *d-xxxxxxxxx* por su ID de directorio:

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

Se usará para recuperar los secretos de la aplicación.

> **Note**
>
> Debe escribir **`aws/directory-services/d-xxxxxxxxx/seamless-domain-join`** exactamente como está, pero sustituya *d-xxxxxxxxxx* por su ID de directorio. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.



5. Deje todo lo demás con los valores predeterminados y, a continuación, elija Siguiente.
6. En Configurar rotación automática, elija Deshabilitar rotación automática y, a continuación, Siguiente.

   Puedes activar la rotación de este secreto después de guardarlo.
7. Revise la configuración y, a continuación, elija Almacenar para guardar los cambios. La consola de Secrets Manager vuelve a la lista de secretos de su cuenta con el nuevo secreto ahora incluido en la lista.
8. Elija el nombre del secreto recién creado de la lista y tome nota del valor del ARN del secreto. Lo necesitará en la sección siguiente.

Activa la rotación del secreto de la cuenta del servicio de dominio

Te recomendamos que cambies los secretos con regularidad para mejorar tu postura de seguridad.

Para activar la rotación del secreto de la cuenta del servicio de dominio

- Sigue las instrucciones de la Guía del AWS Secrets Manager usuario sobre cómo configurar la rotación automática de datos AWS Secrets Manager secretos.

  Para el paso 5, utilice la plantilla de rotación de credenciales de Microsoft Active Directory en la Guía del AWS Secrets Manager usuario.

  Para obtener ayuda, consulte Solucionar problemas de AWS Secrets Manager rotación en la Guía del AWS Secrets Manager usuario.

Creación del rol y la política de IAM obligatorios

Siga los siguientes pasos previos para crear una política personalizada que permita el acceso de solo lectura a su secreto de unión a dominios integrada de Secrets Manager (que creó anteriormente) y para crear un nuevo rol de IAM de DomainJoin LinuxEC2.

Creación de la política de lectura de IAM de Secrets Manager

Utilizará la consola de IAM para crear una política que concede acceso de solo lectura a su secreto de Secrets Manager.

Creación de la política de lectura de IAM de Secrets Manager

1. Inicie sesión AWS Management Console como usuario con permiso para crear políticas de IAM. A continuación, abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, Administración de acceso, selecciona Políticas.
3. Elija Crear política.
4. Seleccione la pestaña JSON y copie el texto del siguiente documento de política JSON. A continuación, péguelo en el cuadro de texto JSON.

   > **Note**
   >
   > Asegúrate de reemplazar el ARN de región y recurso por el ARN y la región reales del secreto que creaste 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. Cuando haya terminado, elija Next. El validador de políticas notifica los errores de sintaxis. Para obtener más información, consulte Validación de políticas de IAM.
6. En la página Revisar política, ingrese un nombre para la política, como **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Revise el Resumen de la política para ver los permisos concedidos por su política. Seleccione Crear política para guardar los cambios. La nueva política aparece en la lista de las políticas administradas y está lista para asociar a una identidad.

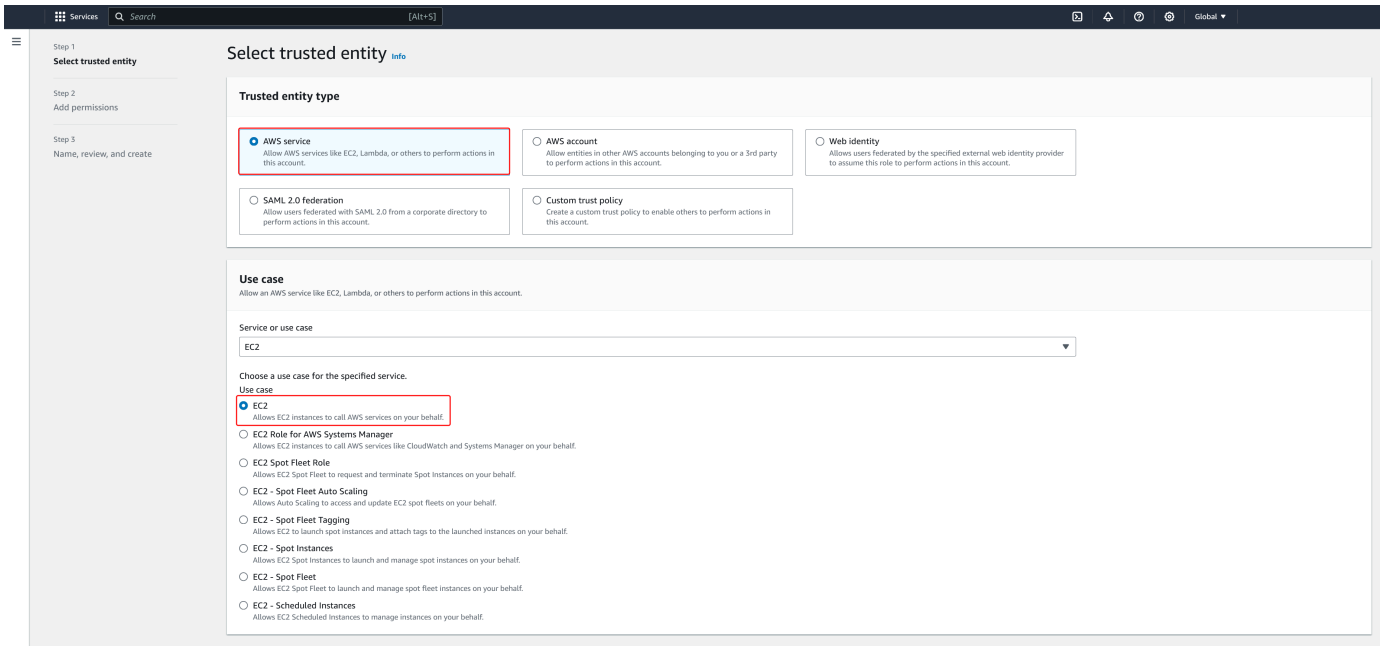
> **Note**
>
> Le recomendamos que cree una política por secreto. De este modo, se garantiza que las instancias solo tengan acceso al secreto adecuado y se minimiza el impacto en caso de que una instancia se vea comprometida.

Cree el rol LinuxEC2 DomainJoin

Utilice la consola de IAM para crear el rol que utilizará para unirse al dominio de su instancia de EC2 de Linux.

Para crear el rol LinuxEC2 DomainJoin

1. Inicie sesión AWS Management Console como usuario con permiso para crear políticas de IAM. A continuación, abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, en Administración del acceso, elija Roles.
3. En el panel de contenido, elija Crear rol.
4. En Seleccionar tipo de entidad de confianza, seleccione Servicio de AWS .
5. En Caso de uso, elija EC2 y, a continuación, elija Siguiente.



6. En Políticas de filtro, haga lo siguiente:
   a. Escriba **`AmazonSSMManagedInstanceCore`**. A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   b. Escriba **`AmazonSSMDirectoryServiceAccess`**. A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   c. Ingrese **`SM-Secret-Linux-DJ-`***`d-xxxxxxxxxx`***`-Read`** (o el nombre de la política creada en el procedimiento anterior). A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   d. Tras añadir las tres políticas enumeradas anteriormente, seleccione Crear función.

> **Note**
>
> AmazonSSM DirectoryServiceAccess proporciona los permisos para unir instancias a una instancia Active Directory gestionada por. AWS Directory Service AmazonSSM ManagedInstanceCore proporciona los permisos mínimos necesarios para usar el servicio. AWS Systems Manager Para obtener más información sobre la creación de un rol con estos permisos y para obtener información sobre otros permisos y políticas que puede asignar a su rol de IAM, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

7. Introduzca un nombre para su nueva función, por ejemplo, **`LinuxEC2DomainJoin`** u otro nombre que prefiera en el campo Nombre de la función.
8. (Opcional) En Role description (Descripción del rol), escriba una descripción.
9. (Opcional) Selecciona Añadir nueva etiqueta en el paso 3: Añadir etiquetas para añadir etiquetas. Los pares clave-valor de etiquetas se utilizan para organizar, rastrear o controlar el acceso de este rol.
10. Elija Crear rol.

Una sin problemas su instancia de Amazon EC2 Linux a su AWS Microsoft AD gestionado Active Directory

Ahora que ha configurado todas las tareas previas, puede utilizar el siguiente procedimiento para unir sin problemas su instancia EC2 de Linux.

Para unirse sin problemas a su instancia de Linux

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En el selector de regiones de la barra de navegación, elija el Región de AWS mismo directorio que el existente.
3. En el panel de control de EC2, en la sección Lanzar instancia, elija Lanzar instancia.
4. En la página Lanzar una instancia, en la sección Nombre y etiquetas, introduce el nombre que deseas usar para tu instancia EC2 de Linux.
5. (Opcional) Elija Agregar etiquetas adicionales para agregar uno o varios pares clave-valor de etiqueta para organizar o controlar el acceso a esta instancia de EC2 o hacer su seguimiento.

6. En la sección Imagen de aplicación e sistema operativo (Amazon Machine Image), elija la AMI de Linux que desee lanzar.

> **Note**
>
> La AMI utilizada debe tener AWS Systems Manager (SSM Agent) la versión 2.3.1644.0 o superior. Para comprobar la versión de SSM Agent instalada en la AMI mediante el lanzamiento de una instancia desde esa AMI, consulte Obtener la versión de SSM Agent instalada actualmente. Si necesita actualizar SSM Agent, consulte Instalación y configuración de SSM Agent en instancias de EC2 para Linux.
> SSM usa el `aws:domainJoin` complemento al unir una instancia de Linux a un dominio. Active Directory *El complemento cambia el nombre de host de las instancias de Linux al formato EC2AMAZ-XXXXXXX.* Para obtener más información al respecto*`aws:domainJoin`*, consulte la referencia del complemento del documento de AWS Systems Manager comandos en la Guía del usuario.AWS Systems Manager

7. En la sección Tipo de instancia, elija el tipo de instancia que desee usar en la lista desplegable Tipo de instancia.
8. En la sección Par de claves (inicio de sesión), puede elegir entre crear un nuevo par de claves o elegir un par de claves existente. Para crear un nuevo par de claves, elija Crear nuevo par de claves. Ingrese un nombre para el par de claves y seleccione una opción en Tipo de par de claves y Formato de archivo de clave privada. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija .pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija .ppk. Elija Crear par de claves. Su navegador descargará el archivo de clave privada automáticamente. Guarde el archivo de clave privada en un lugar seguro.

> **Important**
>
> Esta es la única oportunidad para guardar el archivo de clave privada.

9. En la página Lanzar una instancia, en la sección Configuración de red, elija Editar. Elija la VPC en la que se creó el directorio en la lista desplegable VPC: obligatoria.
10. Elija una de las subredes públicas de su VPC en la lista desplegable Subred. La subred que elija debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.

Para obtener más información sobre cómo conectar una puerta de enlace de Internet, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.

11. En Autoasignar IP pública, elija Habilitar.

    Para obtener más información sobre el direccionamiento IP público y privado, consulte el direccionamiento IP de las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

12. En la configuración Firewall (grupos de seguridad), puede usar la configuración predeterminada o hacer cambios para adaptarla a sus necesidades.
13. En la configuración Configurar almacenamiento, puede utilizar los ajustes predeterminados o hacer los cambios necesarios para adaptarlos a sus necesidades.
14. Seleccione la sección Detalles avanzados y elija su dominio en la lista desplegable Directorio de unión de dominios.

> **Note**
>
> Tras elegir el directorio de unión de dominios, es posible que vea:
>
> ⚠ An error was detected in your existing SSM document. You can delete the existing SSM document here and we'll create a new one with correct properties on instance launch. ✕
>
> Este error se produce si el asistente de lanzamiento de EC2 identifica un documento SSM existente con propiedades inesperadas. Puede elegir una de las opciones siguientes:
>
> - Si ya ha editado el documento SSM y las propiedades son las esperadas, seleccione cerrar y proceda a lanzar la instancia de EC2 sin cambios.
> - Seleccione el enlace para eliminar el documento SSM existente aquí para eliminar el documento SSM. Esto permitirá crear un documento SSM con las propiedades correctas. El documento SSM se creará automáticamente al lanzar la instancia EC2.

15. Para el perfil de instancia de IAM, elija el rol de IAM que creó anteriormente en la sección de requisitos previos. Paso 2: Crear el rol LinuxEC2. DomainJoin
16. Seleccione Iniciar instancia.

> **Note**
>
> Si va a llevar a cabo una unión de dominio fluida con SUSE Linux, es necesario reiniciarla para que las autenticaciones funcionen. Para reiniciar SUSE desde el terminal Linux, escriba sudo reboot.

Mantenimiento de su directorio del Conector AD

En esta sección, se describe cómo llevar a cabo las tareas administrativas comunes para su entorno de Conector AD.

Temas

Eliminación de Conector AD

Cuando se elimina un directorio de Conector AD, su directorio en las instalaciones permanece intacto. Todas las instancias que están unidas al directorio también permanecen intactas y permanecen unidas al directorio local. Puede seguir utilizando las credenciales del directorio para iniciar sesión en estas instancias.

Eliminación de Conector AD

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios. Asegúrese de estar en el Región de AWS lugar donde está desplegado su AD Connector. Para obtener más información, consulte Elegir una región.
2. Asegúrese de que no haya ninguna AWS aplicación habilitada para el AD Connector que desea eliminar. AWS Las aplicaciones habilitadas le impedirán eliminar su AD Connector.

   a. En la página Directories (Directorios), elija el ID del directorio.

   b. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones). En la sección de AWS aplicaciones y servicios, verá qué AWS aplicaciones están habilitadas para su AD Connector.

      - Inhabilita AWS Management Console el acceso. Para obtener más información, consulte Deshabilitación del acceso a la AWS Management Console.

- Para deshabilitar Amazon WorkSpaces, debes anular el registro del servicio en el directorio de la consola. WorkSpaces Para obtener más información, consulta Cómo anular el registro de un directorio en la Guía de WorkSpaces administración de Amazon.
- Para deshabilitar Amazon WorkDocs, debes eliminar el WorkDocs sitio de Amazon en la WorkDocs consola de Amazon. Para obtener más información, consulta Eliminar un sitio en la Guía de WorkDocs administración de Amazon.
- Para deshabilitar Amazon WorkMail, debes eliminar la WorkMail organización de Amazon en la WorkMail consola de Amazon. Para obtener más información, consulta Eliminar una organización en la Guía del WorkMail administrador de Amazon.
- Para deshabilitar Amazon FSx para Windows File Server, debe eliminar el sistema de archivos de Amazon FSx del dominio. Para obtener más información, consulte Cómo trabajar con Active Directory fSx for Windows File Server en la Guía del usuario de Amazon FSx for Windows File Server.
- Para deshabilitar Amazon Relational Database Service, debe eliminar la instancia de Amazon RDS del dominio. Para obtener más información, consulte Administración de una instancia de base de datos en un dominio en la Guía del usuario de Amazon RDS.
- Para deshabilitar el AWS Client VPN servicio, debe eliminar el servicio de directorio del punto final Client VPN. Para obtener más información, consulte Active DirectoryAutenticación en la Guía AWS Client VPN del administrador.
- Para deshabilitar Amazon Connect, debe eliminar la instancia de Amazon Connect. Para obtener más información, consulte Eliminación de una instancia de Amazon Connect en la Guía de administración de Amazon Connect.
- Para deshabilitar Amazon QuickSight, debes darte de baja de Amazon QuickSight. Para obtener más información, consulta Cómo cerrar tu Amazon QuickSight cuenta en la Guía del QuickSight usuario de Amazon.

> **Note**
>
> Si lo está utilizando AWS IAM Identity Center y ya lo ha conectado anteriormente al directorio AWS administrado de Microsoft AD que planea eliminar, primero debe cambiar la fuente de identidad antes de poder eliminarlo. Para obtener más información, consulte Cambio del origen de identidad en la Guía del usuario de IAM Identity Center.

3. En el panel de navegación, elija Directories (Directorios).

4. Seleccione únicamente el Conector AD que se va a eliminar y haga clic en Eliminar. La eliminación de Conector AD puede tardar varios minutos. Cuando Conector AD se haya eliminado, también se eliminará de la lista de directorios.

Ver información del directorio

Puede ver información detallada sobre un directorio.

Visualización de información detallada del directorio

1. En el panel de navegación de la AWS Directory Service consola, en Active Directory, selecciona Directorios.
2. Haga clic en el enlace del identificador de directorio correspondiente al directorio. La información acerca del directorio se muestra en la sección Detalles del directorio.

Para obtener más información acerca del campo Status, consulte Descripción del estado del directorio.

Habilite el acceso a AWS aplicaciones y servicios

Los usuarios pueden autorizar a AD Connector a que dé acceso a sus AWS aplicaciones y servicios WorkSpaces, como AmazonActive Directory. Las siguientes AWS aplicaciones y servicios se pueden activar o desactivar para que funcionen con AD Connector.

AWS aplicación/servicio	Más información…
Amazon Chime	Para obtener más información, consulte la Guía de administración de Amazon Chime.
Amazon Connect	Para obtener más información, consulte la Guía de administración de Amazon Connect.
Amazon WorkDocs	Para obtener más información, consulta la Guía de WorkDocs administración de Amazon.
Amazon WorkMail	Para obtener más información, consulta la Guía del WorkMail administrador de Amazon.

AWS aplicación/servicio	Más información…
Amazon WorkSpaces	Puede crear un AD Simple, un AD AWS administrado de Microsoft o un AD Connector directamente desde WorkSpaces. Solo tiene que lanzar Advanced Setup al crear su espacio de Workspace. Para obtener más información, consulta la Guía de WorkSpaces administración de Amazon.
AWS Client VPN	Para más información, consulte la Guía del usuario deAWS Client VPN.
AWS IAM Identity Center	Para más información, consulte la Guía del usuario deAWS IAM Identity Center.
AWS Management Console	Para obtener más información, consulte Habilitación del acceso a la AWS Management Console con credenciales de AD.
AWS Transfer Family	Para más información, consulte la Guía del usuario deAWS Transfer Family.

Una vez habilitado, el acceso a los directorios se gestiona en la consola de la aplicación o del servicio al que desea otorgar acceso a su directorio. Para encontrar los enlaces de AWS aplicaciones y servicios descritos anteriormente en la AWS Directory Service consola, lleve a cabo los siguientes pasos.

Para mostrar las aplicaciones y los servicios para un directorio

1. En el panel de navegación de la consola deAWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. Consulte la lista en la sección de Aplicaciones y servicios deAWS .

Para obtener más información sobre cómo autorizar o desautorizar el uso de AWS aplicaciones y servicios AWS Directory Service, consulteAutorización para AWS aplicaciones y servicios que utilizan AWS Directory Service.

Actualización de la dirección de DNS del Conector AD

Siga estos pasos para actualizar las direcciones de DNS a las que apunta su Conector AD.

> **Note**
>
> Si tiene una actualización en curso, espere hasta que se haya completado antes de iniciar otra.
> Si utiliza WorkSpaces con su Conector AD, asegúrese de que las direcciones DNS de WorkSpace también estén actualizadas. Para obtener más información, consulte Actualización de servidores DNS para WorkSpaces.

Para actualizar la configuración de DNS de Conector AD

1. En el panel de navegación de la consola de AWS Directory Service, en Active Directory, elija Directorios.
2. Elija el enlace del ID de directorio correspondiente a su directorio.
3. En la página Detalles del directorio, elija la pestaña Redes y seguridad.
4. En la sección Configuración de DNS existente, elija Actualizar.
5. En el cuadro de diálogo Update existing DNS addresses (Actualizar direcciones de DNS existentes), escriba las direcciones IP de DNS actualizadas y, a continuación, elija Update (Actualizar).

Para obtener más información sobre la solución de problemas del Conector AD, consulte Solución de problemas del Conector AD.

Prácticas recomendadas para Conector AD

A continuación se indican algunas sugerencias y directrices que debe tener en cuenta para evitar problemas y sacar el máximo provecho del Conector AD.

Configuración: requisitos previos

Plantéese estas directrices antes de crear el directorio.

Compruebe que tena el tipo de directorio correcto

AWS Directory Service proporciona varias formas de usarlo Microsoft Active Directory con otros AWS servicios. Puede elegir el servicio de directorio con las características que necesita con un costo que se adapte a su presupuesto:

- AWS Directory Service for Microsoft Active Directory es un servicio gestionado y Microsoft Active Directory alojado en la AWS nube con numerosas funciones. AWS Microsoft AD administrado es la mejor opción si tiene más de 5000 usuarios y necesita establecer una relación de confianza entre un directorio AWS hospedado y sus directorios locales.
- AD Connector simplemente conecta su entorno local existente Active Directory a AWS. Conector AD es la mejor opción si desea utilizar su directorio en las instalaciones con los servicios de AWS .
- Simple AD es un directorio de bajo coste y escala con Active Directory compatibilidad básica. Admite 5000 usuarios o menos, aplicaciones compatibles con Samba 4 y compatibilidad LDAP para aplicaciones compatibles con LDAP.

Para obtener una comparación más detallada de AWS Directory Service las opciones, consulte¿Cuál debe elegir?.

Asegúrese de que sus VPC y sus instancias se hayan configurado correctamente

Para gestionar y utilizar sus directorios, así como conectarse a ellos, debe configurar correctamente las VPC a las que están asociados los directorios. Consulte AWS Requisitos previos de Microsoft AD gestionado, Requisitos previos de Conector AD o Requisitos previos para Simple AD para obtener información sobre la seguridad de VPC y los requisitos de red.

Si está añadiendo una instancia a su dominio, asegúrese de que dispone de conectividad y acceso remoto a la instancia, tal y como se describe en Unir una instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory.

Sea consciente de sus límites

Obtenga información sobre los distintos límites de su tipo de directorio específico. El almacenamiento disponible y el tamaño total de los objetos son las únicas limitaciones en cuanto al número de objetos que puede almacenar en el directorio. Consulte cualquiera de las opciones AWS Cuotas

administradas de Microsoft AD, Cuotas de Conector AD o Cuotas de Simple AD para obtener más información sobre el directorio que ha elegido.

Comprenda la configuración y el uso de los grupos de AWS seguridad de su directorio

AWS crea un grupo de seguridad y lo adjunta a las interfaces de red elásticas del directorio, a las que se puede acceder desde las VPC emparejadas o redimensionadas. AWS configura el grupo de seguridad para bloquear el tráfico innecesario al directorio y permite el tráfico necesario.

Modificación del grupo de seguridad del directorio

Si desea modificar la seguridad de los grupos de seguridad de sus directorios, puede hacerlo. Realice esos cambios únicamente si comprende completamente cómo funcionan los filtros de los grupos de seguridad. Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias de Linux en la Guía del usuario de Amazon EC2. Los cambios incorrectos pueden provocar la pérdida de comunicaciones con los equipos e instancias previstos. AWS recomienda que no intente abrir puertos adicionales al directorio, ya que esto reduce la seguridad del directorio. Lea detenidamente el Modelo de responsabilidad compartida de AWS.

> **Warning**
>
> Técnicamente, puede asociar el grupo de seguridad del directorio a otras instancias EC2 que cree. Sin embargo, no AWS recomienda esta práctica. AWS puede tener motivos para modificar el grupo de seguridad sin previo aviso para satisfacer las necesidades funcionales o de seguridad del directorio gestionado. Estos cambios afectan a cualquier instancia a la que asocie el grupo de seguridad del directorio y puede interrumpir el funcionamiento de las instancias asociadas. Además, al asociar el grupo de seguridad del directorio a las instancias EC2 se puede crear un posible riesgo de seguridad para las instancias EC2.

Configurar sitios y subredes en las instalaciones correctamente al usar Conector AD

Si la red en las instalaciones tiene definidos sitios de Active Directory, debe asegurarse de que las subredes de la VPC en la que reside el directorio del Conector AD estén definidas en un sitio de Active Directory y que no existen conflictos entre las subredes de la VPC y las subredes de sus otros sitios.

Para detectar los controladores de dominio, directorio del Conector AD utiliza el sitio de Active Directory cuyos rangos de direcciones IP de subred que sean próximos a los de la VPC que contienen el directorio del Conector AD. Si hay un sitio cuyas subredes tienen los mismos rangos

de direcciones IP que los de su VPC, el directorio del Conector AD detectará los controladores de dominio en ese sitio, que puede no estar físicamente cerca de su región.

Comprenda las restricciones de nombre de usuario para AWS las aplicaciones

AWS Directory Service proporciona compatibilidad con la mayoría de los formatos de caracteres que se pueden utilizar en la construcción de nombres de usuario. Sin embargo, hay restricciones de caracteres que se aplican a los nombres de usuario que se utilizarán para iniciar sesión en AWS aplicaciones, como WorkSpaces Amazon WorkMail, WorkDocs Amazon o Amazon. QuickSight Estas restricciones requieren que no se utilicen los siguientes caracteres:

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

> **Note**
>
> El símbolo @ se permite siempre que preceda a un sufijo UPN.

Programación de las aplicaciones

Antes de programar sus aplicaciones, tenga en cuenta lo siguiente:

Pruebas de carga antes de la puesta en producción

Asegúrese de hacer pruebas de laboratorio con aplicaciones y solicitudes que sean representativos de su carga de trabajo de producción para confirmar que el directorio puede adaptarse a la carga de su aplicación. Si necesita capacidad adicional, distribuya las cargas en varios directorios de AD Connector.

Uso del directorio

Estas son algunas sugerencias que tener en cuenta al utilizar su directorio.

Rotar con regularidad sus credenciales de administrador

Cambie la contraseña de administrador de la cuenta del servicio del Conector AD con regularidad y asegúrese de que la contraseña sea coherente con las políticas de contraseñas de Active Directory

existentes. Para obtener instrucciones sobre cómo cambiar la contraseña de la cuenta del servicio, consulte Actualización de las credenciales de su cuenta de servicio de Conector AD en AWS Directory Service.

Utilizar directorios del Conector AD únicos para cada dominio

Los Conectores AD y sus dominios AD en las instalaciones deben tener una relación de confianza unívoca. Es decir, para cada dominio en las instalaciones, incluidos los dominios secundarios en un bosque de AD que desee autenticar, debe crear un Conector AD único. Cada Conector AD que cree deberá utilizar una cuenta de servicio diferente, incluso si está conectado al mismo directorio.

Compruebe si hay compatibilidad

Al utilizar AD Connector, debe asegurarse de que su directorio local sea y siga siendo compatible con AWS Directory Service s. Para obtener más información acerca de sus responsabilidades, consulte nuestro modelo de responsabilidad compartida.

Cuotas de Conector AD

A continuación se indican los límites predeterminados para Conector AD. A menos que se indique lo contrario, cada cuota es por cada región.

Cuotas de Conector AD

Recurso	Cuota predeterminada
Directorios del Conector AD	10
Número máximo de certificados de entidad de certificación (CA) registrados por directorio	5

Política de compatibilidad de las aplicaciones para AD Connector

Como alternativa a AWS Directory Service para Microsoft Active Directory (AWS Microsoft AD gestionado), Conector AD es un proxy de Active Directory exclusivo para aplicaciones y servicios creados para AWS. Se debe configurar el proxy para que utilice un dominio determinado de Active Directory. Cuando la aplicación debe buscar un usuario o un grupo en Active Directory, Conector AD envía la solicitud al directorio. Del mismo modo, cuando un usuario inicia sesión en la aplicación,

Conector AD envía la solicitud de autenticación al directorio. No hay ninguna aplicación de terceros que funcione con Conector AD.

A continuación se muestra una lista de aplicaciones y servicios de AWS compatibles:

- Amazon Chime: para obtener instrucciones detalladas, consulte Conexión con Active Directory.
- Amazon Connect: para obtener más información, consulte Cómo funciona Amazon Connect.
- Amazon EC2 para Windows o Linux: puede utilizar la función integrada de unión de dominios de Active Directory de Amazon EC2 para Windows o Linux para unir su instancia a su Active Directory autogestionado (local). Una vez unida, la instancia se comunica directamente con su Active Directory sin pasar por Conector AD. Para obtener más información, consulte Unir una instancia de Amazon EC2 a su Active Directory.
- AWS Management Console: también puede utilizar Conector AD para autenticar usuarios de AWS Management Console con sus credenciales de Active Directory sin necesidad de configurar una infraestructura de SAML. Para obtener más información, consulte Habilitación del acceso a la AWS Management Console con credenciales de AD.
- Amazon QuickSight : para obtener más información, consulte Administración de cuentas de usuario en Amazon QuickSight Enterprise Edition.
- AWS IAM Identity Center: para obtener instrucciones detalladas, consulte Conectar IAM Identity Center a una instancia de Active Directory en las instalaciones.
- AWS Transfer Family: para obtener instrucciones detalladas, consulte Trabajar con AWS Directory Service para Microsoft Active Directory.
- AWS Client VPN: para obtener instrucciones detalladas, consulte Autenticación y autorización de clientes.
- Amazon WorkDocs : para obtener instrucciones detalladas, consulte Conexión a su directorio local con AD Connector.
- Amazon WorkMail : para obtener instrucciones detalladas, consulte Integrar Amazon WorkMail con un directorio existente (configuración estándar).
- WorkSpaces - Para obtener instrucciones detalladas, consulte Iniciar un conector WorkSpace con AD Connector.

> **Note**
>
> Amazon RDS solo es compatible con AWS Managed Microsoft AD y no es compatible con Conector AD. Para obtener más información, consulte la sección Microsoft AD AWS administrado en la página de AWS Directory Servicepreguntas frecuentes.

Solución de problemas de Conector AD

Lo siguiente puede ayudarte a solucionar algunos problemas comunes que pueden surgir al crear o usar tu AD Connector.

Temas

Problemas de creación

Los siguientes son problemas de creación comunes para AD Connector:

He recibido un error “AZ Constrained” a la hora de crear un directorio

Es posible que algunas AWS cuentas creadas antes de 2012 tengan acceso a zonas de disponibilidad en las regiones EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Norte de California) o Asia Pacífico (Tokio) que no admiten AWS Directory Service directorios. Si recibe un error como este al crear unaActive Directory, elija una subred en una zona de disponibilidad diferente e intente crear el directorio de nuevo.

Aparece el error «Se han detectado problemas de conectividad» cuando intento crear AD Connector

Si recibes el error «Se ha detectado un problema de conectividad» al intentar crear un conector AD, el error podría deberse a la disponibilidad de los puertos o a la complejidad de la contraseña del conector AD. Puedes probar la conexión del conector AD para comprobar si están disponibles los siguientes puertos:

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

Para probar la conexión, consulteProbar el conector de AD. La prueba de conexión debe realizarse en la instancia unida a las dos subredes a las que están asociadas las direcciones IP del conector AD.

Si la prueba de conexión se realiza correctamente y la instancia se une al dominio, comprueba la contraseña del conector AD. AD Connector debe cumplir con los requisitos de complejidad de las AWS contraseñas. Para obtener más información, consulte Cuenta de servicio enRequisitos previos de Conector AD.

Si su AD Connector no cumple estos requisitos, vuelva a crearlo con una contraseña que cumpla con estos requisitos.

Problemas de conectividad

Los siguientes son problemas de conectividad comunes para AD Connector

- Aparece el error “Problemas de conectividad detectados” cuando intento conectarme a mi directorio en las instalaciones
- Aparece el error “DNS no disponible” cuando intento conectarme a mi directorio on-premise
- Aparece el error “Registro SRV” cuando intento conectarme a mi directorio en las instalaciones

Aparece el error “Problemas de conectividad detectados” cuando intento conectarme a mi directorio en las instalaciones

Cuando se conecta al directorio on-premise, aparece un error similar al siguiente:

```
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.
```

Es necesario que Conector AD pueda comunicarse con los controladores de dominio en las instalaciones a través de TCP y UDP en los siguientes puertos. Asegúrese de que los grupos de seguridad y los firewall on-premise permiten la comunicación TCP y UDP a través de dichos puertos. Para obtener más información, consulte Requisitos previos de Conector AD.

- 88 (Kerberos)
- 389 (LDAP)

Es posible que necesite puertos TCP/UDP adicionales según sus necesidades. Consulte la siguiente lista para ver algunos de estos puertos. Para obtener más información sobre los puertos que utilizanActive Directory, consulte Cómo configurar un firewall para Active Directory dominios y confianzas en Microsoft la documentación.

- 135 (RPC Endpoint Mapper)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

Aparece el error “DNS no disponible” cuando intento conectarme a mi directorio on-premise

Cuando se conecta al directorio on-premise, aparece un error similar al siguiente:

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

Es necesario que Conector AD pueda comunicarse con los servidores DNS en las instalaciones a través de TCP y UDP en el puerto 53. Asegúrese de que los grupos de seguridad y los firewalls on-premise permiten la comunicación TCP y UDP a través de dicho puerto. Para obtener más información, consulte Requisitos previos de Conector AD.

Aparece el error “Registro SRV” cuando intento conectarme a mi directorio en las instalaciones

Al conectarse al directorio on-premise, puede aparecer un error similar a los siguientes:

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos
 does not exist for IP: <DNS IP address>
```

Cuando Conector AD se conecta al directorio, necesita obtener los registros SRV `_ldap._tcp.<DnsDomainName>` y `_kerberos._tcp.<DnsDomainName>`. Este error aparecerá si el servicio no puede obtener estos registros de los servidores DNS que especificó al conectarse a su directorio. Para obtener más información acerca de estos registros SRV, consulte SRV record requirements.

Problemas de autenticación

Estos son algunos de los problemas de autenticación más comunes con AD Connector:

- Aparece el mensaje de error «No se pudo validar el certificado» cuando intento iniciar sesión Amazon WorkSpaces con una tarjeta inteligente
- He recibido un error “Credenciales no válidas” cuando la cuenta de servicio que utiliza Conector AD intenta autenticarse
- Aparece el mensaje de error «No se puede autenticar» cuando utilizo AWS aplicaciones para buscar usuarios o grupos
- Recibo un error sobre las credenciales de mi directorio cuando intento actualizar la cuenta de servicio AD Connector
- Algunos de mis usuarios no pueden autenticarse con mi directorio

Aparece el mensaje de error «No se pudo validar el certificado» cuando intento iniciar sesión Amazon WorkSpaces con una tarjeta inteligente

Al intentar iniciar sesión en su cuenta WorkSpaces con una tarjeta inteligente, recibe un mensaje de error similar al siguiente:

```
ERROR: Certificate Validation failed. Please try again by restarting your browser or
 application and make sure you select the correct certificate.
```

El error se produce si el certificado de la tarjeta inteligente no está almacenado correctamente en el cliente que usa los certificados. Para obtener más información sobre los requisitos de AD Connector y tarjetas inteligentes, consulteRequisitos previos.

Utilice los siguientes procedimientos para solucionar problemas relacionados con la capacidad de la tarjeta inteligente para almacenar certificados en el almacén de certificados del usuario:

1. En el dispositivo que tiene problemas para acceder a los certificados, acceda al Microsoft Management Console (MMC).

   > **Important**
   >
   > Antes de continuar, cree una copia del certificado de la tarjeta inteligente.

2. Navegue hasta el almacén de certificados de la MMC. Elimine el certificado de tarjeta inteligente del usuario del almacén de certificados. Para obtener más información sobre cómo ver el almacén de certificados en la MMC, consulte Cómo ver los certificados con el complemento MMC en la documentación. Microsoft
3. Extraiga la tarjeta inteligente.
4. Vuelva a insertar la tarjeta inteligente para que pueda volver a rellenar el certificado de la tarjeta inteligente en el almacén de certificados del usuario.

   > **Warning**
   >
   > Si la tarjeta inteligente no rellena el certificado en el almacén de usuarios, no se puede utilizar para la autenticación con tarjeta inteligente. WorkSpaces

La cuenta de servicio del conector AD debe tener lo siguiente:

- `my/spn`agregado al nombre principal del servicio
- Delegado para el servicio LDAP

Una vez rellenado el certificado en la tarjeta inteligente, se debe comprobar el controlador de dominio local para determinar si se ha bloqueado la asignación del nombre principal de usuario (UPN) al nombre alternativo del sujeto. Para obtener más información sobre este cambio, consulte Cómo

deshabilitar el nombre alternativo del sujeto para la asignación de UPN en la documentación. Microsoft

Utilice el siguiente procedimiento para comprobar la clave de registro del controlador de dominio:

1. En el Editor del Registro, navegue hasta la siguiente clave secundaria

   HKEY_LOCAL_MACHINE\ SYSTEM\\ Services\ Kdc\ CurrentControlSet UseSubjectAltName

2. UseSubjectAltNameSeleccione. Asegúrese de que el valor esté establecido en 0.

> **Note**
>
> Si la clave de registro está configurada en los controladores de dominio locales, el AD Connector no podrá localizar a los usuarios Active Directory y generará el mensaje de error anterior.

Los certificados de la entidad de certificación (CA) se deben cargar en el certificado de la tarjeta inteligente AD Connector. El certificado debe contener información sobre el OCSP. A continuación se enumeran los requisitos adicionales para la CA:

- El certificado debe estar en la autoridad raíz de confianza del controlador de dominio, el servidor de la autoridad de certificación y el WorkSpaces.
- Los certificados de CA raíz y fuera de línea no contendrán la información de la OSCP. Estos certificados contienen información sobre su revocación.
- Si utiliza un certificado de CA de terceros para la autenticación con tarjeta inteligente, la CA y los certificados intermedios deben publicarse en el almacén de Active Directory NTauth. Deben estar instalados en la entidad raíz de confianza para todos los controladores de dominio, los servidores de la entidad de certificación y. WorkSpaces
  - Puede usar el siguiente comando para publicar certificados en el almacén de Active Directory NTauth:

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

Para obtener más información sobre la publicación de certificados en la tienda de NTauth, consulte Importación del certificado de CA emisor a la tienda de NTauth empresarial en la Guía de instalación de Access Amazon WorkSpaces with Common Access Cards.

Para comprobar si OCSP verifica el certificado de usuario o los certificados en cadena de CA, sigue este procedimiento:

1. Exporte el certificado de la tarjeta inteligente a una ubicación de la máquina local, como la unidad C:.
2. Abra una línea de comandos y vaya a la ubicación en la que está almacenado el certificado de tarjeta inteligente exportado.
3. Escriba el siguiente comando:

```
certutil -URL Certficate_name.cer
```

4. Tras el comando, debería aparecer una ventana emergente. Seleccione la opción OCSP en la esquina derecha y seleccione Recuperar. El estado debería volver a ser verificado.

Para obtener más información sobre el comando certutil, consulte certutil en la documentación Microsoft

He recibido un error “Credenciales no válidas” cuando la cuenta de servicio que utiliza Conector AD intenta autenticarse

Esto puede ocurrir si el disco duro del controlador de dominio se queda sin espacio. Asegúrese de que los discos duros del controlador de dominio no estén llenos.

Aparece el mensaje de error «No se puede autenticar» cuando utilizo AWS aplicaciones para buscar usuarios o grupos

Es posible que se produzcan errores al buscar usuarios mientras utiliza AWS aplicaciones, como WorkSpaces Amazon QuickSight, incluso cuando el estado del AD Connector estaba activo. Las credenciales caducadas pueden impedir que Conector AD complete consultas en Active Directory. Actualiza la contraseña de la cuenta de servicio siguiendo los pasos ordenados que se indican enLa unión de dominios perfecta para las instancias de Amazon EC2 dejó de funcionar.

Recibo un error sobre las credenciales de mi directorio cuando intento actualizar la cuenta de servicio AD Connector

Al intentar actualizar la cuenta de servicio de AD Connector, recibe un mensaje de error similar a uno o varios de los siguientes:

```
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
```

Es posible que haya un problema con la sincronización horaria y Kerberos. AD Connector envía las solicitudes de autenticación de Kerberos aActive Directory. Estas solicitudes son urgentes y, si se retrasan, fallarán. Para resolver este problema, consulte la recomendación: configurar el PDC raíz con una fuente horaria autorizada y evitar un sesgo horario generalizado en la documentación. Microsoft Para obtener más información sobre el servicio horario y la sincronización, consulte lo siguiente:

- Cómo funciona el servicio Windows horario
- Tolerancia máxima para la sincronización del reloj del ordenador
- WindowsHerramientas y ajustes del servicio horario

Algunos de mis usuarios no pueden autenticarse con mi directorio

Las cuentas de usuario deben tener habilitada la autenticación previa de Kerberos. Es la configuración predeterminada para cuentas de usuario nuevas y no debe modificarse. Para obtener más información sobre esta configuración, consulte Autenticación previa activada Microsoft TechNet.

Problemas de mantenimiento

Los siguientes son problemas de mantenimiento comunes del AD Connector:

- Mi directorio se bloquea en el estado “Solicitado”
- La unión de dominios perfecta para las instancias de Amazon EC2 dejó de funcionar

Mi directorio se bloquea en el estado “Solicitado”

Si tiene un directorio que haya estado en estado “Solicitado” durante más de cinco minutos, pruebe a eliminar el directorio y vuelva a crearlo. Si este problema sigue sin resolverse, póngase en contacto con AWS Support.

La unión de dominios perfecta para las instancias de Amazon EC2 dejó de funcionar

La unión a dominios sencilla para instancias de EC2 estaba funcionando y, a continuación, se detuvo mientras Conector AD estaba activo, es posible que las credenciales de la cuenta de servicio de Conector AD hayan caducado. Las credenciales caducadas pueden impedir que AD Connector cree objetos de ordenador en suActive Directory.

Para resolver este problema, actualice las contraseñas de la cuenta de servicio en el orden que se indica a continuación, de modo que las contraseñas coincidan:

1. Actualice la contraseña de la cuenta de servicio de suActive Directory.
2. Actualiza la contraseña de la cuenta de servicio en tu AD Connector en AWS Directory Service. Para obtener más información, consulte Actualización de las credenciales de su cuenta de servicio de Conector AD en AWS Directory Service.

> **Important**
>
> Si se actualiza la contraseña solo en, el cambio de contraseña AWS Directory Service no se transfiere a la versión local existente, Active Directory por lo que es importante hacerlo en el orden indicado en el procedimiento anterior.

No puedo eliminar mi Conector AD

Si Conector AD pasa a un estado inoperativo, ya no tendrá acceso a los controladores de dominio. Bloqueamos la eliminación de un Conector AD cuando todavía hay aplicaciones vinculadas a él porque es posible que una de esas aplicaciones siga utilizando el directorio. Para obtener una lista de las aplicaciones que debe deshabilitar para eliminar su AD Connector, consulteEliminación de Conector AD. Si sigues sin poder eliminar tu AD Connector, puedes solicitar ayuda a través de este enlace AWS Support.

AD sencillo

Simple AD es un directorio administrado independiente que utiliza tecnología de un servidor compatible con Active Directory de Samba 4. Está disponible en dos tamaños.

- Pequeño: admite hasta 500 usuarios (aproximadamente 2000 objetos incluidos usuarios, grupos y equipos).
- Grande: admite hasta 5000 usuarios (aproximadamente 20 000 objetos incluidos usuarios, grupos y equipos).

Simple AD ofrece un subconjunto de las funciones que ofrece AWS Managed Microsoft AD, incluida la capacidad de gestionar cuentas de usuario y membresías a grupos, crear y aplicar políticas de grupo, conectarse de forma segura a instancias de Amazon EC2 y proporcionar un inicio de sesión único (SSO) basado en Kerberos. Sin embargo, tenga en cuenta que Simple AD no admite funciones como la autenticación multifactor (MFA), las relaciones de confianza con otros dominios, el Centro de administración de Active Directory, el soporte PowerShell , la papelera de reciclaje de Active Directory, las cuentas de servicio gestionadas por grupos y las extensiones de esquema para aplicaciones POSIX y Microsoft.

Simple AD ofrece muchas ventajas:

- Simple AD facilita la administración de las instancias de Amazon EC2 que ejecutan Linux y Windows y la implementación de aplicaciones de Windows en la AWS nube.
- Muchas de las aplicaciones y herramientas que utiliza hoy que requieren soporte de Microsoft Active Directory se pueden usar con Simple AD.
- Las cuentas de usuario de Simple AD permiten el acceso a AWS aplicaciones como WorkSpaces Amazon WorkDocs o Amazon WorkMail.
- Puede administrar AWS los recursos mediante el acceso basado en roles de IAM al. AWS Management Console
- Las instantáneas automatizadas diarias permiten la recuperación. point-in-time

Simple AD no es compatible con ninguno de los elementos siguientes:

- Amazon AppStream 2.0
- Amazon Chime

- Amazon RDS para SQL Server
- Amazon RDS para Oracle
- AWS IAM Identity Center
- Relaciones de confianza con otros dominios
- Centro de administración de Active Directory
- PowerShell
- Papelera de reciclaje de Active Directory
- Cuentas de servicio administradas por grupos
- Ampliaciones de esquema para aplicaciones Microsoft y POSIX

Siga leyendo los temas de esta sección para obtener información sobre cómo crear su propio Simple AD.

Temas

Introducción a Simple AD

Simple AD crea un directorio totalmente gestionado y basado en Samba en la AWS nube. Cuando crea un directorio con Simple AD, AWS Directory Service crea dos controladores de dominio y servidores DNS en su nombre. Los controladores de dominio se crean en diferentes subredes de una Amazon VPC. Esta redundancia ayuda a garantizar que el directorio permanezca accesible incluso si se produce un error.

Temas

- Qué se crea con tu Simple AD Active Directory
- Configurar DNS para Simple AD

Requisitos previos para Simple AD

Para crear un Simple ADActive Directory, necesitas una Amazon VPC con lo siguiente:

- La VPC debe disponer de tenencia de hardware predeterminada.
- La VPC no debe configurarse con los siguientes puntos de enlace de la VPC:
  - Puntos de enlace de VPC de Route53 que incluyen anulaciones condicionales de DNS para *.amazonaws.com que se resuelven en direcciones IP no públicas AWS
  - CloudWatch Punto final de VPC
  - Punto de conexión de VPC de Systems Manager
  - Punto de conexión de VPC de Security Token Service
- Al menos dos subredes en dos zonas de disponibilidad diferentes. Las subredes deben estar en el mismo rango de enrutamiento entre dominios sin clase (CIDR). Si desea ampliar o cambiar el tamaño de la VPC del directorio, asegúrese de seleccionar las dos subredes de controlador de dominio al rango de CIDR de la VPC ampliado. Cuando crea un Simple AD, AWS Directory Service crea dos controladores de dominio y servidores DNS en su nombre.
  - Para obtener más información sobre el rango CIDR, consulte el direccionamiento IP de sus VPC y subredes en la Guía del usuario de Amazon VPC.
- Si necesita compatibilidad de LDAPS con Simple AD, le recomendamos que lo configure mediante un equilibrador de carga de red conectado al puerto 389. Este modelo le permite utilizar un certificado seguro para la conexión a través de LDAPS, simplificar el acceso a LDAPS a través de una única dirección IP de NLB y disponer de conmutación por error automática a través del NLB. Simple AD no admite el uso de certificados autofirmados en el puerto 636. Para obtener más información sobre cómo configurar LDAPS con Simple AD, consulte How to configure an LDAPS endpoint for Simple AD en el Blog de seguridad de AWS .
- Deben habilitarse los siguientes tipos de cifrado en el directorio:
  - RC4_HMAC_MD5
  - AES128_HMAC_SHA1
  - AES256_HMAC_SHA1
  - Tipos de cifrado futuros

> **Note**
>
> Si deshabilita estos tipos de cifrado, puede provocar problemas de comunicación con RSAT (Herramientas de administración remota del servidor) y afectar a la disponibilidad o a su directorio.

- Para obtener más información, consulte ¿Qué es Amazon VPC? en la Guía del usuario de Amazon VPC.

AWS Directory Service utiliza una estructura de dos VPC. Las instancias EC2 que componen su directorio se ejecutan fuera de su AWS cuenta y son administradas por. AWS Contienen dos adaptadores de red, `ETH0` y `ETH1`. `ETH0` es el adaptador de administración y se encuentra fuera de su cuenta. `ETH1` se crea dentro de su cuenta.

El rango de IP de administración de la red `ETH0` del directorio se elige mediante programación para garantizar que no entre en conflicto con la VPC en la que está implementado el directorio. Este rango de IP puede estar en cualquiera de los siguientes pares (ya que los directorios se ejecutan en dos subredes):

- 10.0.1.0/24 y 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 y 192.168.2.0/24

Para evitar conflictos, comprobamos el primer octeto del CIDR `ETH1`. Si comienza con un 10, entonces elegimos una VPC 192.168.0.0/16 con subredes 192.168.1.0/24 y 192.168.2.0/24. Si el primer octeto no es un 10, elegimos una VPC 10.0.0.0/16 con subredes 10.0.1.0/24 y 10.0.2.0/24.

El algoritmo de selección no incluye las rutas de la VPC. Por lo tanto, es posible que este escenario provoque un conflicto del enrutamiento IP.

Crea tu Simple AD Active Directory

Para crear un nuevo Simple ADActive Directory, lleve a cabo los siguientes pasos. Antes de comenzar este procedimiento, asegúrese de haber completado los requisitos previos que se indican en Requisitos previos para Simple AD.

Para crear un Simple AD Active Directory

1. En el panel de navegación de la consola de AWS Directory Service, elija Directorios y, a continuación, elija Configurar directorio.
2. En la página Seleccionar tipo de directorio, elija Simple AD y, a continuación, elija Siguiente.
3. En la página Enter directory information (Especifique la información del directorio), facilite la siguiente información:

   Tamaño del directorio

   Elija entre la opción de tamaño Small (Pequeño) o Large (Grande). Para obtener más información acerca de los tamaños, consulte AD sencillo.

   Nombre de organización

   Un nombre de organización único para su directorio que se utilizará para registrar los dispositivos cliente.

   Este campo solo está disponible si está creando su directorio como parte del lanzamiento WorkSpaces.

   Nombre de DNS del directorio

   El nombre completo del directorio, como por ejemplo `corp.example.com`.

   Nombre NetBIOS del directorio

   El nombre abreviado del directorio, como `CORP`.

   Administrator password

   Contraseña del administrador del directorio. Al crear el directorio, se crea también una cuenta de administrador con el nombre de usuario `Administrator` y esta contraseña.

   La contraseña del administrador del directorio distingue entre mayúsculas y minúsculas y debe tener 8 caracteres como mínimo y 64 como máximo. También debe contener al menos un carácter de tres de las siguientes categorías:

   - Letras minúsculas (a-z)
   - Letras mayúsculas (A-Z)
   - Números (0-9)
   - Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmar contraseña

Vuelva a escribir la contraseña de administrador.

Descripción del directorio

Descripción opcional del directorio.

4. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la siguiente información y, a continuación, elija Next (Siguiente).

   VPC

   VPC del directorio.

   Subredes

   Elija las subredes de los controladores de dominio. Las dos subredes deben estar en diferentes zonas de disponibilidad.

5. En la página Review & create (Revisar y crear), revise la información del directorio y haga los cambios que sean necesarios. Cuando la información sea correcta, seleccione Create directory (Crear directorio). La creación del directorio tarda varios minutos. Una vez creado, el valor Status cambia a Active.

Qué se crea con tu Simple AD Active Directory

Cuando crea un Active Directory con Simple AD, AWS Directory Service realiza las siguientes tareas en su nombre:

- Configura un directorio basado en Samba dentro de la VPC.
- Crea una cuenta de administrador del directorio con el nombre de usuario `Administrator` y la contraseña especificada. Esta cuenta le permite administrar el directorio.

> **Important**
>
> Asegúrese de guardar esta contraseña. AWS Directory Service no almacena esta contraseña y no se puede recuperar. Sin embargo, puede restablecer una contraseña desde la AWS Directory Service consola o mediante la ResetUserPasswordAPI.

- Crea un grupo de seguridad para los controladores del directorio.

- Crea una cuenta llamada `AWSAdminD-xxxxxxxx` con privilegios de administrador del dominio. Esta cuenta se utiliza AWS Directory Service para realizar operaciones automatizadas de mantenimiento de directorios, como la toma de instantáneas de directorios y las transferencias de funciones de FSMO. AWS Directory Service almacena de forma segura las credenciales de esta cuenta.
- Crea y asocia automáticamente una interfaz de red elástica (ENI) a cada uno de sus controladores de dominio. Cada uno de estos ENI es esencial para la conectividad entre la VPC AWS Directory Service y los controladores de dominio y nunca debe eliminarse. Puede identificar todas las interfaces de red reservadas para su uso AWS Directory Service mediante la descripción: «interfaz de red AWS creada para el identificador del directorio». Para obtener más información, consulte Elastic Network Interfaces en la Guía del usuario de Amazon EC2. El servidor DNS predeterminado del Microsoft AD AWS administrado Active Directory es el servidor DNS de la VPC en el enrutamiento entre dominios sin clase (CIDR) +2. Para obtener más información, consulte el servidor DNS de Amazon en la Guía del usuario de Amazon VPC.

> **Note**
>
> De forma predeterminada, los controladores de dominio se implementan en dos zonas de disponibilidad de una región y se conectan a su nube privada virtual (VPC) de Amazon. Las copias de seguridad se hacen automáticamente una vez al día y los volúmenes de Amazon Elastic Block Store (EBS) se cifran para garantizar la seguridad de los datos en reposo. Los controladores de dominio que tienen errores se sustituyen automáticamente en la misma zona de disponibilidad con la misma dirección IP y se puede llevar a cabo una recuperación de desastres completa con la última copia de seguridad.

Configurar DNS para Simple AD

Simple AD reenvía las solicitudes de DNS a la dirección IP de los servidores DNS proporcionados por Amazon para Amazon VPC. Estos servidores DNS resolverán nombres configurados en sus zonas alojadas privadas de Amazon Route 53. Al apuntar sus equipos en las instalaciones a su Simple AD, ya puede resolver las solicitudes de DNS en la zona alojada privada. Para obtener más información sobre Route 53, consulte Qué es Route 53.

Tenga en cuenta que, para permitir que su Simple AD responda a las consultas de DNS externas, debe configurar la lista de control de acceso (ACL) a la red de la VPC que contenga su Simple AD para que permita el tráfico desde fuera de la VPC.

- Si no utiliza las zonas alojadas privadas de Route 53, sus solicitudes de DNS se reenviarán a los servidores DNS públicos.
- Si utiliza servidores DNS personalizados que están fuera de la VPC y desea utilizar DNS privado, deberá cambiar la configuración para utilizar los servidores DNS personalizados en instancias EC2 dentro de la VPC. Para obtener más información, consulte Uso de zonas alojadas privadas.
- Si desea que su Simple AD resuelva nombres mediante servidores DNS dentro de su VPC y servidores DNS privados fuera de su VPC, puede hacerlo a través de un conjunto de opciones de DHCP. Para ver un ejemplo detallado, consulte este artículo.

> **Note**
>
> Las actualizaciones dinámicas de DNS no se admiten en dominios de Simple AD. En lugar de ello, puede realizar los cambios directamente en su directorio utilizando el Administrador de DNS en una instancia que esté unida al dominio.

Cómo administrar Simple AD

En esta sección, se presentan todos los procedimientos de uso y mantenimiento de un entorno de Simple AD.

Temas

Administración de usuarios y grupos en Simple AD

Los usuarios representan a las personas físicas o entidades que tienen acceso al directorio. Los grupos resultan muy útiles para conceder o denegar privilegios a un conjunto de usuarios en lugar de asignar esos privilegios a cada usuario por separado. Si un usuario se va a otra organización,

basta con cambiarlo a un grupo diferente y automáticamente recibirá los privilegios necesarios para la nueva organización.

Para crear usuarios y grupos en un directorio de AWS Directory Service, debe usar cualquier instancia (ya sea en las instalaciones o EC2) que se haya unido a su directorio de AWS Directory Service y haber iniciado sesión como usuario con privilegios para crear usuarios y grupos. También es necesario instalar las herramientas de Active Directory en su instancia de EC2 para que pueda agregar sus usuarios y grupos con el complemento Usuarios y equipo de Active Directory. Para obtener más información acerca de cómo configurar una instancia EC2 e instalar las herramientas necesarias, consulte Unir una instancia de Amazon EC2 a su Active Directory de Simple AD.

> **Note**
>
> Las cuentas de usuario deben tener habilitada la autenticación previa de Kerberos. Es la configuración predeterminada para cuentas de usuario nuevas y no debe modificarse. Para obtener más información acerca de esta configuración, consulta Autenticación previa en Microsoft TechNet.

En los temas siguientes se incluyen instrucciones sobre cómo crear y administrar usuarios y grupos.

Temas

Instale las herramientas de administración de Active Directory para Simple AD

Para administrar Active Directory desde una instancia de Amazon EC2 Windows Server, debe instalar los servicios de dominio de Active Directory y las herramientas de servicios de directorio ligero de Active Directory en la instancia. Utilice el siguiente procedimiento para instalar estas herramientas en una instancia EC2 de Windows Server.

Requisitos previos

Antes de comenzar este procedimiento, complete lo siguiente:

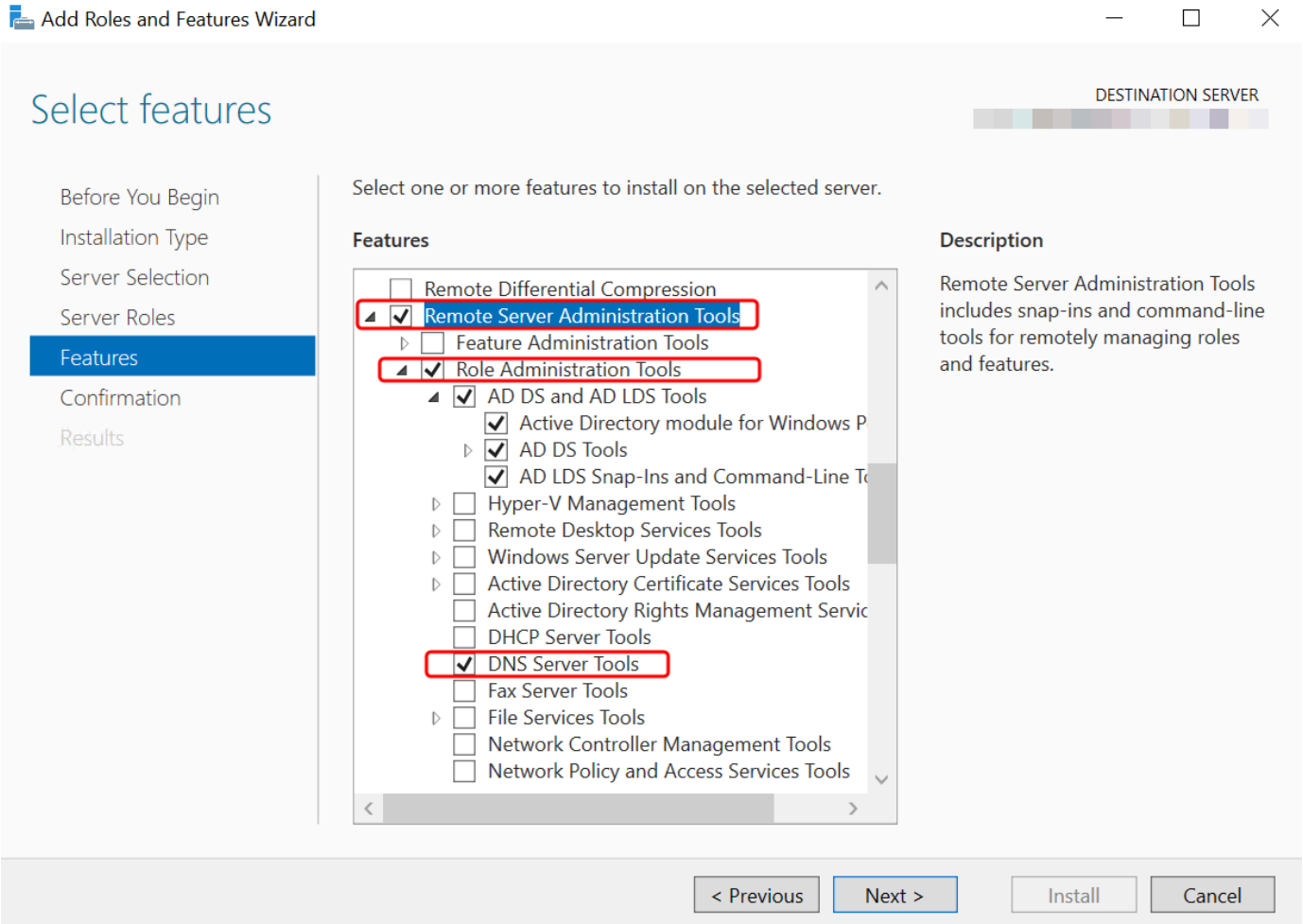
1. Cree un Active Directory de AD simple. Para obtener más información, consulte Crea tu Simple AD Active Directory.
2. Inicie una instancia EC2 de Windows Server y únala a su Active Directory Simple AD. La instancia EC2 necesita las siguientes políticas para crear usuarios y grupos: **`AWSSSMManagedInstanceCore`** y. **`AmazonSSMDirectoryServiceAccess`** Para obtener más información, consulte Una sin problemas una instancia Amazon EC2 para Windows a su Active Directory Simple AD.
3. Necesitará las credenciales de su administrador de dominio de Active Directory. Estas credenciales se crearon cuando se creó el Simple AD. Si ha seguido el procedimiento indicado enCrea tu Simple AD Active Directory, su nombre de usuario de administrador incluye su nombre de NetBIOS,. **`corp\administrator`**

Instale las herramientas de administración de Active Directory en la instancia EC2 de Windows Server

Para instalar las herramientas de administración de Active Directory en la instancia EC2 de Windows Server

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la consola de Amazon EC2, elija Instancias, seleccione la instancia de Windows Server y, a continuación, elija Conectarse.
3. En la página Conectarse a la instancia, elija Cliente RDP.
4. En la pestaña Cliente RDP, elija Descargar archivo de Escritorio remoto y, a continuación, seleccione Obtener contraseña para recuperar la contraseña.
5. En la sección Obtener contraseña de Windows, seleccione Cargar archivo de clave privada. Elija el archivo de clave privada .pem asociado a la instancia de Windows Server. Tras cargar el archivo de clave privada, seleccione Descifrar contraseña.
6. En el cuadro de diálogo de seguridad de Windows, copie las credenciales de administrador local del equipo Windows Server para iniciar sesión. El nombre de usuario puede tener los siguientes formatos: ***`NetBIOS-Name`***`\administrator` o***`DNS-Name`***`\administrator`. Por ejemplo, **`corp\administrator`** sería el nombre de usuario si hubiera seguido el procedimiento indicado enCrea tu Simple AD Active Directory.

7. Una vez que haya iniciado sesión en la instancia de Windows Server, abra el Administrador del servidor desde el menú Inicio seleccionando el Administrador del servidor.
8. En el panel de Server Manager, elija Agregar roles y características.
9. En Asistente para agregar roles y características, elija Tipo de instalación, seleccione Instalación basada en características o en roles y luego Siguiente.
10. En Selección de servidor, asegúrese de que el servidor local está seleccionado y elija Características en el panel de navegación izquierdo.
11. En el árbol Características, seleccione y abra Herramientas de administración remota del servidor, Herramientas de administración de roles y Herramientas de AD DS y AD LDS. Con las herramientas de AD DS y AD LDS seleccionadas, se selecciona el Active Directorymódulo para Windows PowerShell, las herramientas de AD DS y los complementos y herramientas de línea de comandos de AD LDS. Desplácese hacia abajo y seleccione Herramientas del servidor DNS y, a continuación, elija Siguiente.



12. Revise la información y elija Instalar. Cuando termine de instalarse la característica, las herramientas Active Directory Domain Services y Active Directory Lightweight Directory Services estarán disponibles en el menú de inicio, en la carpeta Herramientas administrativas.

Método alternativo para instalar las herramientas de administración de Active Directory en una instancia EC2 de Windows Server

- Este es otro método para instalar las herramientas de administración de Active Directory:
  - Si lo desea, puede optar por instalar las herramientas de administración de Active Directory medianteWindows PowerShell. Por ejemplo, puede instalar las herramientas de administración remota de Active Directory desde una PowerShell ventana de comandos utilizando`Install-WindowsFeature RSAT-ADDS`. Para obtener más información, consulte Instalar-WindowsFeature en el sitio web de Microsoft.

Crear un usuario de Simple AD

Utilice el siguiente procedimiento para crear un usuario con una instancia de Amazon EC2 unida a su directorio Simple AD. Antes de poder crear usuarios, debe completar los procedimientos de Instalación de las herramientas de administración de Active Directory.

> **Note**
>
> Cuando se utiliza Simple AD, si se crea una cuenta de usuario en una instancia de Linux con la opción “Obligar al usuario a cambiar la contraseña en el primer inicio de sesión”, el usuario no podrá cambiar inicialmente la contraseña con kpasswd. Para cambiar la contraseña la primera vez, un administrador del dominio debe actualizar la contraseña de usuario utilizando las herramientas de administración de Active Directory.

Puede utilizar cualquiera de los métodos siguientes para crear un usuario:

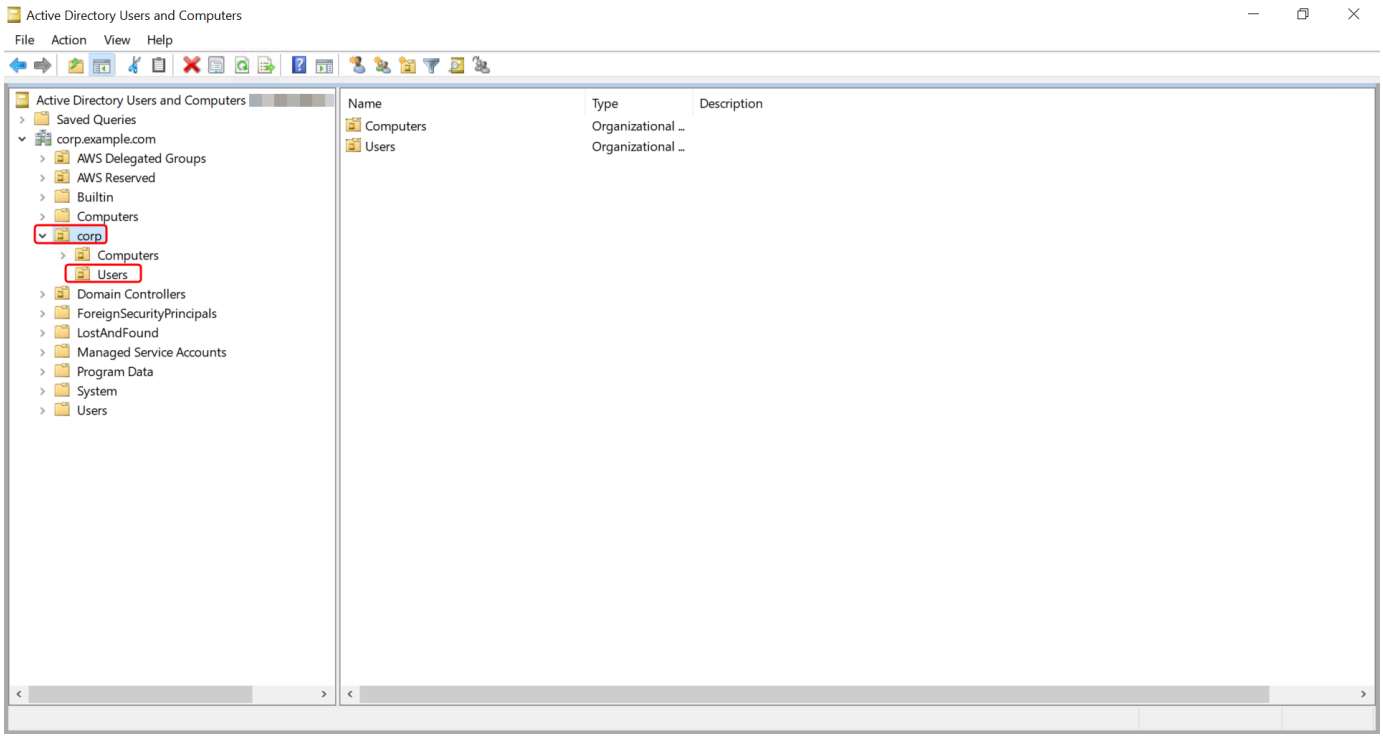
- Active DirectoryHerramientas de administración
- Windows PowerShell

Cree un usuario con las herramientas Active Directory de administración

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.
2. Abra la herramienta Usuarios y equipos de Active Directory desde el menú Inicio de Windows. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas de Windows.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. En el árbol de directorios, seleccione una unidad organizativa con el nombre de NetBIOS de su directorio (OU) en la que desee almacenar el usuario (por ejemplo,**`corp\Users`**). Para obtener más información sobre la estructura de unidades organizativas que utilizan los directorios AWS, consulteQué se crea con su Active Directory AWS administrado de Microsoft AD.



4. En el menú Acción, haga clic en Nuevo y, a continuación, haga clic en Usuario para abrir el asistente de nuevo usuario.

5. En la primera página del asistente, introduzca los valores de los siguientes campos y, a continuación, elija Siguiente.
   - First name (Nombre)
   - Last name (Apellidos)
   - Nombre de inicio de sesión de usuario
6. En la segunda página del asistente, especifique una contraseña temporal en Contraseña y Confirmar contraseña. Asegúrese de que está seleccionada la opción El usuario debe cambiar la contraseña en el próximo inicio de sesión. No debe estar seleccionada ninguna otra opción. Elija Siguiente.
7. En la tercera página del asistente, compruebe que la información de este es correcta y elija Finalizar. El nuevo usuario aparecerá en la carpeta Users.

Cree un usuario en Windows PowerShell

1. Conéctese a la instancia unida a su Active Directory dominio como Active Directory administrador.
2. Abra Windows PowerShell.
3. Escribe el siguiente comando sustituyendo el nombre **`jane.doe`** de usuario por el nombre de usuario que quieres crear. Se le pedirá Windows PowerShell que proporcione una contraseña para el nuevo usuario. Para obtener más información sobre los requisitos de complejidad de las Active Directory contraseñas, consulte Microsoftla documentación. Para obtener más información sobre el comando New-ADUser, consulte la documentación. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Eliminar un usuario de Simple AD

Utilice el siguiente procedimiento para eliminar un usuario con una instancia de Amazon EC2 para Windows que esté unida al directorio Simple AD.

Puede utilizar cualquiera de los métodos siguientes para eliminar un usuario:

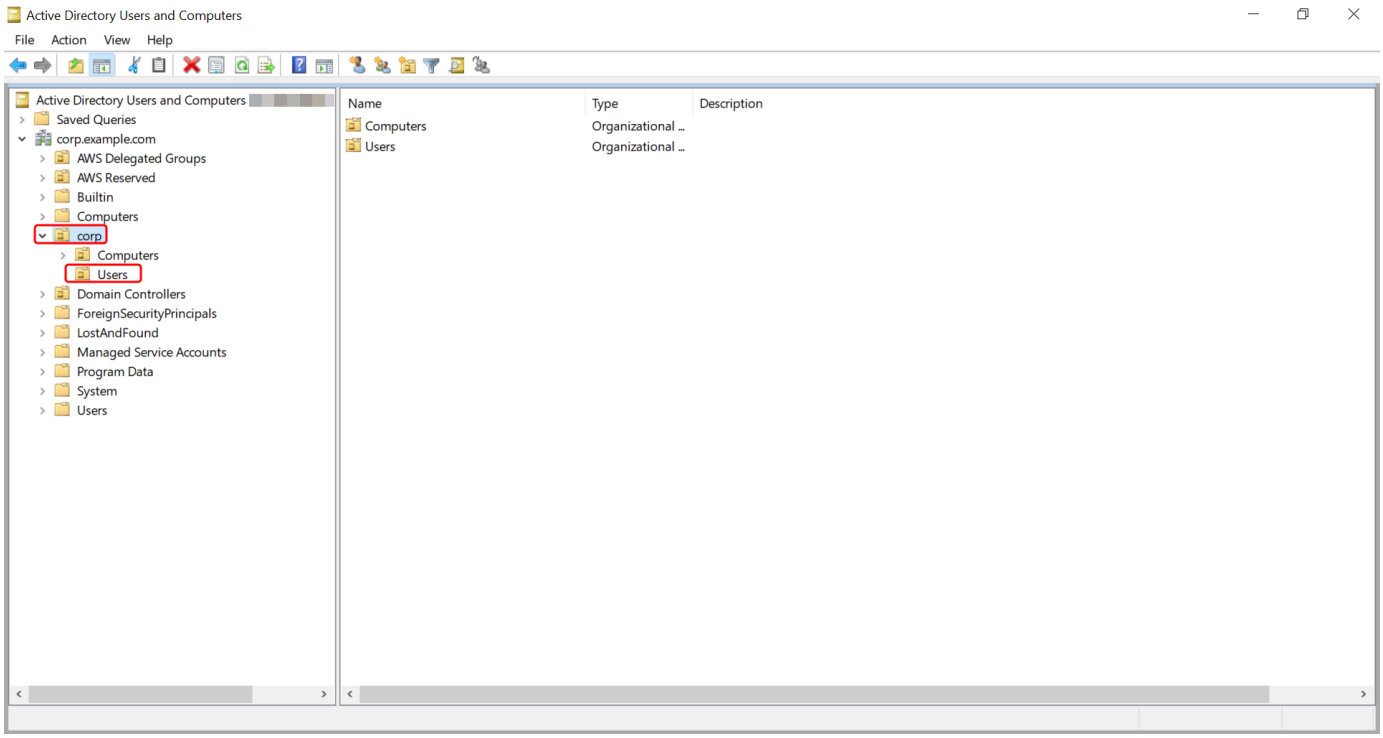
- Active DirectoryHerramientas de administración
- Windows PowerShell

Eliminar un usuario con las herramientas Active Directory de administración

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.
2. Abra la herramienta Usuarios y equipos de Active Directory desde el menú Inicio de Windows. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas de Windows.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. En el árbol de directorios, seleccione la unidad organizativa que contiene el usuario que desea eliminar (por ejemplo,**`corp\Users`**).



4. Seleccione el usuario que desee eliminar. En el menú Acciones, elija Eliminar.
5. Aparecerá un cuadro de diálogo en el que se le solicitará que confirme que desea eliminar el usuario. Seleccione Sí para eliminar el usuario. Esto elimina permanentemente el usuario seleccionado.

Elimine un usuario en Windows PowerShell

1. Conéctese a la instancia unida a su Active Directory dominio como Active Directory administrador.
2. Abra Windows PowerShell.
3. Escribe el siguiente comando para reemplazar el nombre **`jane.doe`** de usuario por el nombre del usuario que deseas eliminar. Para obtener más información sobre el comando Remove-ADUser, consulte la documentación. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Restablecer una contraseña de usuario de Simple AD

Los usuarios deben cumplir con las políticas de contraseñas tal como se definen en laActive Directory. A veces, esto puede afectar a los usuarios, incluido el Active Directory administrador, y estos olvidan su contraseña. Cuando esto sucede, puede restablecer rápidamente la contraseña del usuario AWS Directory Service si el usuario reside en Simple AD.

Debe iniciar sesión como usuario con los permisos necesarios para restablecer las contraseñas. Para obtener más información sobre los permisos, consulte Descripción general de la administración de los permisos de acceso a sus AWS Directory Service recursos.

Puedes restablecer la contraseña de cualquier usuario tuyo, Active Directory con las siguientes excepciones:

- Puede restablecer la contraseña de cualquier usuario de la unidad organizativa (OU) que se base en el nombre de NetBIOS que utilizó al crear su. Active Directory Por ejemplo, si ha seguido el procedimiento descrito enCrea tu Simple AD Active Directory, su nombre de NetBIOS sería CORP y las contraseñas de los usuarios que podría restablecer serían miembros de Corp/Users OU.
- No puede restablecer la contraseña de ningún usuario ajeno a la OU que se base en el nombre de NetBIOS que utilizó al crear su. Active Directory Para obtener más información sobre la estructura de unidades organizativas de Simple AD, consulteQué se crea con tu Simple AD Active Directory.
- No puede restablecer la contraseña de ningún usuario que sea miembro de dos dominios. Tampoco puede restablecer la contraseña de ningún usuario que sea miembro del grupo de administradores de dominio o de administradores de empresa, excepto el usuario administrador.

- No puede restablecer la contraseña de ningún usuario que sea miembro del grupo de administradores de dominio o de administradores de empresa, excepto el usuario administrador.

Puede utilizar cualquiera de los siguientes métodos para restablecer la contraseña de un usuario:

- AWS Management Console
- AWS CLI
- Windows PowerShell

Restablezca una contraseña de usuario en AWS Management Console

1. En el panel de navegación de la AWS Directory Service consola, en Active Directory, elija Directorios y, a continuación, seleccione el elemento de la lista Active Directory en el que desee restablecer la contraseña de usuario.
2. En la página Detalles del directorio, seleccione Acciones, y elija Restablecer contraseña.
3. En el cuadro de diálogo Restablecer la contraseña de usuario, en Nombre de usuario escriba el nombre de usuario cuya contraseña debe cambiar.
4. Escriba una contraseña en Nueva contraseña y Confirmar contraseña y, a continuación, seleccione Restablecer contraseña.

Restablezca la contraseña de un usuario en AWS CLI

1. Para instalar el AWS CLI, consulte Instalar o actualizar la última versión del AWS CLI.
2. Abre el AWS CLI.
3. Escriba el siguiente comando y sustituya el ID del directorio, el nombre de usuario **`jane.doe`** y la contraseña **`P@ssw0rd`** por el ID del Active Directory directorio y las credenciales deseadas. Consulte reset-user-passwordla Referencia de AWS CLI comandos para obtener más información.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Restablezca una contraseña de usuario en Windows PowerShell

1. Conéctese a la instancia unida a su Active Directory dominio como Active Directory administrador.
2. Abra Windows PowerShell.
3. Escribe el siguiente comando para sustituir el nombre de usuario**jane.doe**, el ID del directorio y la contraseña **P@ssw0rd** por el ID del Active Directory directorio y las credenciales que desees. Consulte el UserPassword cmdlet Reset-DS para obtener más información.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Crear un grupo de Simple AD

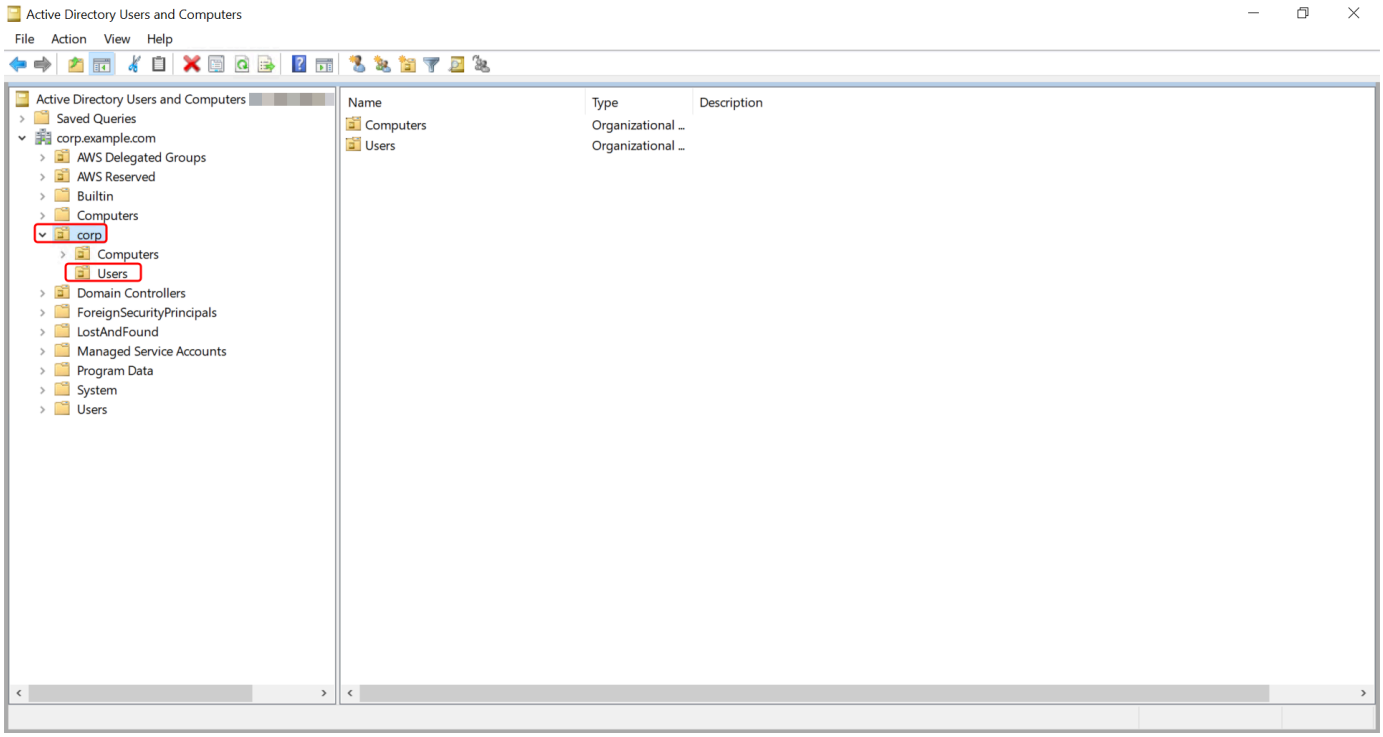
Utilice el siguiente procedimiento para crear un grupo de seguridad con una instancia de Amazon EC2 unida al directorio Simple AD. Antes de poder crear grupos de seguridad, debe completar los procedimientos de Instalación de las herramientas de administración de Active Directory.

Creación de un grupo

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.
2. Abra la herramienta Usuarios y equipos de Active Directory. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. En el árbol del directorio, seleccione una unidad organizativa (OU) bajo el nombre de NetBIOS de su directorio en la que desee almacenar el grupo (por ejemplo, Corp\Users). Para obtener más información sobre la estructura de unidades organizativas que utilizan los directorios de AWS, consulteQué se crea con su Active Directory AWS administrado de Microsoft AD.



4. En el menú Action, haga clic en New y, a continuación, haga clic en Group para abrir el asistente de nuevo grupo.
5. Escriba un nombre para el grupo en Nombre del grupo, seleccione un Ámbito del grupo que se adapte a sus necesidades y seleccione Seguridad para el Tipo de grupo. Para obtener más información sobre el ámbito de los grupos y los grupos de seguridad de Active Directory, consulte los Grupos de seguridad de Active Directory en la documentación de Microsoft Windows Server.
6. Haga clic en OK (Aceptar). El nuevo grupo de seguridad aparecerá en la carpeta Usuarios.

Añadir un usuario de Simple AD a un grupo

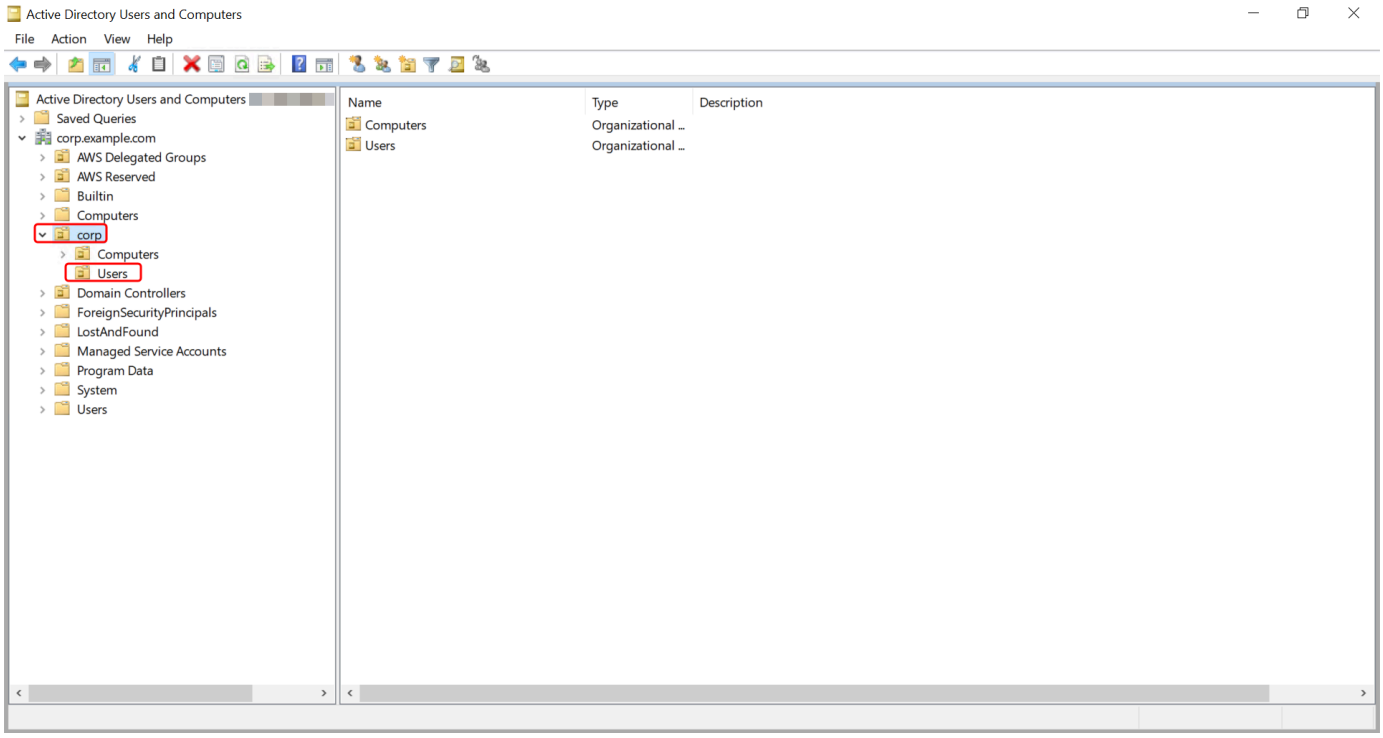
Utilice el siguiente procedimiento para agregar un usuario a un grupo de seguridad con una instancia de EC2 unida al directorio de Simple AD.

Adición de un usuario a un grupo

1. Conéctese a la instancia donde se han instalado las herramientas de administración de Active Directory.
2. Abra la herramienta Usuarios y equipos de Active Directory. Hay un acceso directo a esta herramienta en la carpeta Herramientas administrativas.

> **Tip**
>
> Puede ejecutar lo siguiente desde la línea de comandos de la instancia para abrir directamente el cuadro de herramientas de Usuarios y equipos de Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. En el árbol del directorio, seleccione la unidad organizativa (OU) situada bajo el nombre de NetBIOS en la que ha almacenado el grupo y seleccione el grupo al que desea agregar un usuario como miembro.



4. En el menú Acción, haga clic en Propiedades para abrir el cuadro de diálogo de propiedades del grupo.
5. Seleccione la pestaña Miembros y haga clic en Agregar.
6. En Introduzca los nombres de los objetos que desea seleccionar, escriba el nombre de usuario que desee añadir y haga clic en Aceptar. El nombre aparecerá en la lista de Miembros. Haga clic en OK de nuevo para actualizar la pertenencia a grupos.
7. Para comprobar que el usuario es ahora miembro del grupo, selecciónelo en la carpeta Usuarios y haga clic en Propiedades en el menú Acción para abrir el cuadro de diálogo de propiedades.

Seleccione la pestaña Miembro de. Debería ver el nombre del grupo en la lista de grupos a los que pertenece el usuario.

Supervisión del directorio de Simple AD

Puede supervisar el directorio de Simple AD con los siguientes métodos:

Temas

Descripción del estado del directorio

Estos son los diferentes estados de un directorio.

Activo

El directorio funciona con normalidad. AWS Directory Service no ha detectado problemas en su directorio.

Creando

El directorio se está creando en estos momentos. Los directorios suelen tardar entre 20 y 45 minutos en crearse, pero esto depende de la carga del sistema.

Eliminado

El directorio se ha eliminado. Se han liberado todos los recursos para el directorio. Una vez que un directorio entra en este estado, no se puede recuperar.

Eliminando

El directorio se está eliminando. El directorio permanecerá en este estado hasta que se haya eliminado por completo. Una vez que un directorio entra en este estado, la operación de eliminación no se puede cancelar y el directorio no se puede recuperar.

Con error

No se pudo crear el directorio. Elimine este directorio. Si este problema sigue sin resolverse, contacte con el Centro de AWS Support.

Deteriorado

El directorio se está ejecutando en estado degradado. Se han detectado uno o varios problemas y no todas las operaciones de directorios pueden funcionar con plena capacidad operativa. Hay muchas razones posibles para que el directorio se encuentre en este estado. Entre ellas se incluyen las actividades normales de mantenimiento operativo, como la aplicación de parches o la rotación de instancias de EC2, la sobrecarga provocada por una aplicación en uno de los controladores de dominio o los cambios que haga en la red que interrumpan de forma inadvertida las comunicaciones del directorio. Para obtener más información, consulte Solución de problemas de Microsoft AD AWS administrado, Solución de problemas de Conector AD y Solución de problemas de Simple AD. En el caso de problemas normales relacionados con el mantenimiento, los AWS resuelve en 40 minutos. Si después de revisar el tema de solución de problemas, su directorio sigue dañado durante más de 40 minutos, le recomendamos que contacte con el Centro de AWS Support.

> **Important**
>
> No restaure una instantánea mientras el directorio esté deteriorado. Es poco frecuente que la restauración de las instantáneas sea necesaria para resolver los problemas. Para obtener más información, consulte Creación de una instantánea o restauración del directorio.

Inoperable

El directorio no es funcional. Todos los puntos de enlace del directorio han informado de la existencia de problemas.

Solicitada

Actualmente hay pendiente una solicitud para crear su directorio.

RestoreFailed

Error al restaurar el directorio a partir de una instantánea. Vuelva a intentar restaurarlo. Si el problema continúa, use otra instantánea o contacte con el Centro de AWS Support.

Restauración

El directorio se está restaurando actualmente a partir de una instantánea automática o manual. La restauración a partir de una instantánea suele tardar unos minutos, en función del tamaño del directorio de datos en la instantánea.

Para obtener más información, consulte Motivos de los estados del directorio de Simple AD.

Configurar las notificaciones de estado del directorio con Amazon SNS

Mediante Amazon Simple Notification Service (Amazon SNS), puede recibir mensajes de correo electrónico o de texto (SMS) cuando cambie el estado del directorio. Puede recibir notificaciones si el directorio pasa de un estado Activo a un estado Deteriorado o Inoperativo. También recibirá una notificación cuando el directorio vuelva a estar en estado activo.

Cómo funcionan

Amazon SNS utiliza “temas” para recopilar y distribuir mensajes. Cada tema cuenta con uno o varios suscriptores que reciben los mensajes que se han publicado en dicho tema. Si sigue los pasos que se indican a continuación, puede añadir AWS Directory Service un editor a un tema de Amazon SNS. Cuando AWS Directory Service detecta un cambio en el estado de su directorio, publica un mensaje sobre ese tema, que luego se envía a los suscriptores del tema.

Puede asociar varios directorios como publicadores a un único tema. También puede agregar mensajes de estado del directorio a los temas que ha creado anteriormente en Amazon SNS. Tiene un control detallado sobre quién puede publicar un tema y suscribirse a él. Para obtener información completa sobre Amazon SNS, consulte ¿Qué es Amazon SNS?.

Habilitación de la mensajería SNS para su directorio

1. Inicia sesión en la AWS Directory Service consola AWS Management Console y ábrela.
2. En la página Directories (Directorios), elija el ID del directorio.
3. Seleccione la pestaña Mantenimiento.
4. En la sección Supervisión de directorios, elija Acciones y, a continuación, seleccione Crear notificación.
5. En la página Crear notificación, seleccione Elegir un tipo de notificación y, a continuación, Crear una nueva notificación. También, si ya dispone de un tema de SNS, puede seleccionar Asociar un tema de SNS existente para enviar mensajes de estado desde este directorio a ese tema.

> **Note**
>
> Si elige Crear una nueva notificación, pero, a continuación, utiliza el mismo nombre para un tema de SNS que ya existe, Amazon SNS no creará un nuevo tema, sino que tan solo agregará la información de la nueva suscripción al existente.

Si selecciona Asociar tema de SNS existentes, solo podrá elegir un tema de SNS que se encuentre en la misma región que el directorio.

6. Elija una opción en Tipo de destinatario e ingrese la información del contacto en Destinatario. Si escribe un número de teléfono para SMS, utilice solo números. No incluya guiones, espacios o paréntesis.
7. (Opcional) Proporcione un nombre para su tema y un nombre de visualización de SNS. El nombre de visualización es una abreviatura de hasta 10 caracteres que se incluye en todos los mensajes SMS de este tema. Cuando se utiliza la opción de SMS, es necesario el nombre de visualización.

> **Note**
>
> Si ha iniciado sesión con un usuario o rol de IAM que solo tiene la política DirectoryServiceFullAccessadministrada, el nombre del tema debe empezar por «DirectoryMonitoring». Si desea personalizar aún más su nombre de tema necesitará privilegios adicionales de SNS.

8. Seleccione Crear.

Si desea designar suscriptores de SNS adicionales, como una dirección de correo electrónico adicional, colas de Amazon SQS, AWS Lambdao puede hacerlo desde la consola de Amazon SNS.

Habilitación de mensajes de estado del directorio de un tema

1. Inicie sesión en la consola AWS Management Console y ábrala.AWS Directory Service
2. En la página Directories (Directorios), elija el ID del directorio.
3. Seleccione la pestaña Mantenimiento.
4. En la sección Supervisión de directorios, seleccione un nombre de tema de SNS de la lista, elija Acciones y, a continuación, seleccione Eliminar.
5. Elija Eliminar.

Así eliminará su directorio como publicador en el tema de SNS seleccionado. Si quieres eliminar todo el tema, puedes hacerlo desde la consola de Amazon SNS.

> **Note**
>
> Antes de eliminar un tema de Amazon SNS mediante la consola de SNS, debe asegurarse de que un directorio no está enviando mensajes de estado a dicho tema.
> Si elimina un tema de Amazon SNS mediante la consola de SNS, este cambio no se reflejará inmediatamente en la consola de Directory Services. Solo se le informaría la próxima vez que un directorio publique una notificación en el tema eliminado, en cuyo caso vería un estado actualizado en la pestaña Monitoring del directorio que indica que no se ha encontrado el tema.
> Por lo tanto, para evitar perder mensajes importantes sobre el estado del directorio, antes de eliminar cualquier tema del que reciba mensajes AWS Directory Service, asocie su directorio a un tema diferente de Amazon SNS.

Unir una instancia de Amazon EC2 a su Active Directory de Simple AD

Puede unir sin problemas una instancia de Amazon EC2 a su Active Directory dominio cuando se lance la instancia. Para obtener más información, consulte Unir sin problemas una instancia de Amazon EC2 para Windows a su AWS Microsoft AD gestionado Active Directory. También puede lanzar una instancia EC2 y unirla a un Active Directory dominio directamente desde la AWS Directory Service consola con AWS Systems Manager Automation.

Si necesita unir manualmente una instancia EC2 a su Active Directory dominio, debe lanzar la instancia en la región y el grupo de seguridad o la subred adecuados y, a continuación, unir la instancia al dominio.

Para poder conectarse de forma remota a estas instancias, debe disponer de conectividad IP a las instancias desde la red en la que se está conectando. En la mayoría de los casos, esto requiere conectar una puerta de enlace de Internet a su VPC y que la instancia tenga una dirección IP pública.

Temas

- Crear un conjunto de opciones de DHCP

Una sin problemas una instancia Amazon EC2 para Windows a su Active Directory Simple AD

Este procedimiento une sin problemas una instancia de Amazon EC2 para Windows a su Active Directory Simple AD.

Para unir sin problemas una instancia EC2 de Windows

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, elija el Región de AWS mismo directorio que el existente.
3. En el panel de control de EC2, en la sección Lanzar instancia, elija Lanzar instancia.
4. En la página Lanzar una instancia, en la sección Nombre y etiquetas, ingrese el nombre que desee utilizar para la instancia de EC2 de Windows.
5. (Opcional) Elija Agregar etiquetas adicionales para agregar uno o varios pares clave-valor de etiqueta para organizar o controlar el acceso a esta instancia de EC2 o hacer su seguimiento.
6. En la sección Imagen de aplicación y sistema operativo (Imagen de máquina de Amazon), elija Windows en el panel Inicio rápido. Puede cambiar la imagen de máquina de Amazon (AMI) de Windows desde la lista desplegable Imagen de máquina de Amazon (AMI).
7. En la sección Tipo de instancia, elija el tipo de instancia que desee usar en la lista desplegable Tipo de instancia.
8. En la sección Par de claves (inicio de sesión), puede elegir entre crear un nuevo par de claves o elegir un par de claves existente.
   a. Para crear un nuevo par de claves, elija Crear nuevo par de claves.
   b. Ingrese un nombre para el par de claves y seleccione una opción en Tipo de par de claves y Formato de archivo de clave privada.
   c. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija .pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija .ppk.
   d. Elija Crear par de claves.
   e. Su navegador descargará el archivo de clave privada automáticamente. Guarde el archivo de clave privada en un lugar seguro.

> **Important**
>
> Esta es la única oportunidad para guardar el archivo de clave privada.

9. En la página Lanzar una instancia, en la sección Configuración de red, elija Editar. Elija la VPC en la que se creó el directorio en la lista desplegable VPC: obligatoria.
10. Elija una de las subredes públicas de su VPC en la lista desplegable Subred. La subred que elija debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.

    Para obtener más información sobre cómo conectar una puerta de enlace de Internet, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.
11. En Autoasignar IP pública, elija Habilitar.

    Para obtener más información sobre el direccionamiento IP público y privado, consulte el direccionamiento IP de las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.
12. En la configuración Firewall (grupos de seguridad), puede usar la configuración predeterminada o hacer cambios para adaptarla a sus necesidades.
13. En la configuración Configurar almacenamiento, puede utilizar los ajustes predeterminados o hacer los cambios necesarios para adaptarlos a sus necesidades.
14. Seleccione la sección Detalles avanzados y elija su dominio en la lista desplegable Directorio de unión de dominios.

> **Note**
>
> Tras elegir el directorio de unión de dominios, es posible que vea:
>
> > An error was detected in your existing SSM document. You can delete the existing SSM document here and we'll create a new one with correct properties on instance launch.
>
> Este error se produce si el asistente de lanzamiento de EC2 identifica un documento SSM existente con propiedades inesperadas. Puede elegir una de las opciones siguientes:

- Si ya ha editado el documento SSM y las propiedades son las esperadas, seleccione cerrar y proceda a lanzar la instancia de EC2 sin cambios.
- Seleccione el enlace para eliminar el documento SSM existente aquí para eliminar el documento SSM. Esto permitirá crear un documento SSM con las propiedades correctas. El documento SSM se creará automáticamente al lanzar la instancia EC2.

15. En Perfil de instancia de IAM, puede seleccionar un perfil de instancia de IAM existente o crear uno nuevo. Seleccione un perfil de instancia de IAM que tenga DirectoryServiceAccess adjuntas las políticas AWS administradas AmazonSSM ManagedInstanceCore y AmazonSSM en la lista desplegable de perfiles de instancias de IAM. Para crear uno nuevo, elija el enlace Crear un nuevo perfil de IAM y, a continuación, haga lo siguiente:

    1. Elija Crear rol.
    2. En Seleccionar tipo de entidad de confianza, elija Servicio de AWS .
    3. En Caso de uso, elija EC2.
    4. En Añadir permisos, en la lista de políticas, seleccione las políticas de AmazonSSM ManagedInstanceCore y AmazonSSM. DirectoryServiceAccess Para filtrar la lista, escriba **`SSM`** en el cuadro de búsqueda. Elija Siguiente.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess proporciona los permisos para unir instancias a una instancia gestionada por. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore proporciona los permisos mínimos necesarios para usar el servicio. AWS Systems Manager Para obtener más información sobre la creación de un rol con estos permisos y para obtener información sobre otros permisos y políticas que puede asignar a su rol de IAM, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

    5. En la página Asignar un nombre, revisar, crear, ingrese un Nombre de rol. Necesitará este nombre de rol para asociarlo a la instancia de EC2.
    6. (Opcional) Puede proporcionar una descripción del perfil de instancia de IAM en el campo Descripción.
    7. Elija Crear rol.

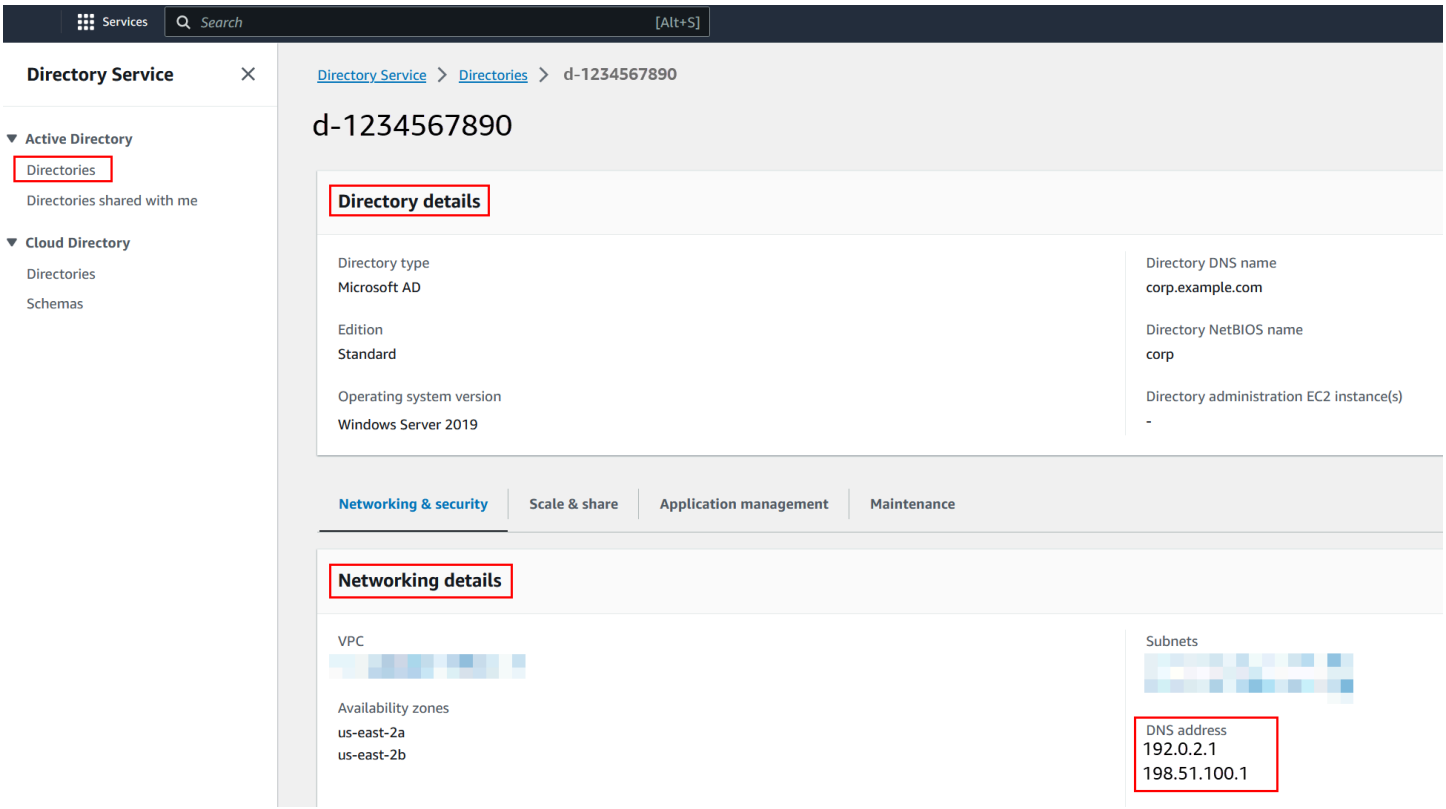
8. Vuelva a la página Lanzar una instancia y elija el icono de actualización situado junto al perfil de instancia de IAM. El nuevo perfil de instancia de IAM debería estar visible en la lista desplegable Perfil de instancia de IAM. Elija el nuevo perfil y deje el resto de la configuración con sus valores predeterminados.

16. Seleccione Iniciar instancia.

Unir manualmente una instancia de Amazon EC2 para Windows a su Active Directory de Simple AD

Para unir manualmente una instancia Amazon EC2 Windows existente a un Active Directory Simple AD, la instancia debe lanzarse con los parámetros que se especifican en. Una sin problemas una instancia Amazon EC2 para Windows a su Active Directory Simple AD

Necesitará las direcciones IP de los servidores DNS de Simple AD. Puede encontrar esta información en las secciones Servicios de directorio > Directorios > el enlace del ID de directorio de su directorio > Detalles del directorio y Redes y seguridad.



Para unir una instancia de Windows a un Active Directory de Simple AD

1. Conéctese a la instancia mediante un cliente de Protocolo de escritorio remoto.

2. Abra el cuadro de diálogo de propiedades TCP/IPv4 en la instancia.

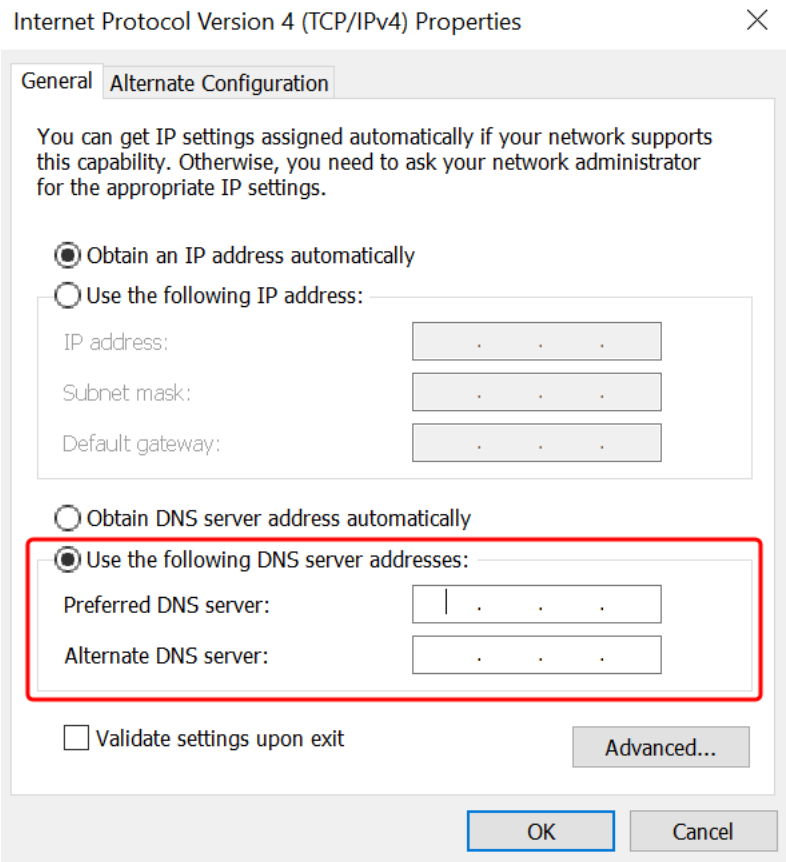
   a. Abra Conexiones de red.

   > **Tip**
   >
   > Puede abrir Conexiones de red directamente ejecutando lo siguiente en un símbolo del sistema en la instancia.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Abra el menú contextual (haga clic con el botón) de cualquier conexión de red habilitada y elija Propiedades.

   c. En el cuadro de diálogo de propiedades de conexión, abra (doble clic) Protocolo de Internet versión 4.

3. Seleccione Usar las siguientes direcciones de servidor DNS, cambie las direcciones del servidor DNS preferido y del servidor DNS alternativo por las direcciones IP de los servidores DNS proporcionados por Simple AD y, a continuación, pulse Aceptar.



4. Abra el cuadro de diálogo Propiedades del sistema de la instancia, seleccione la pestaña Nombre de equipo y elija Cambiar.

> **Tip**
>
> Puede abrir el cuadro de diálogo Propiedades del sistema directamente en un símbolo del sistema en la instancia.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. En el campo Miembro de, seleccione Dominio, introduzca el nombre completo de su Active Directory de Simple AD y pulse Aceptar.
6. Cuando se le pida el nombre y la contraseña del administrador del dominio, introduzca el nombre de usuario y la contraseña de una cuenta que tenga privilegios de unión a un dominio. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para Simple AD.

> **Note**
>
> Puede introducir el nombre completo del dominio o el nombre de NetBIOS, seguido de una barra invertida (\) y, a continuación, el nombre de usuario. El nombre de usuario sería Administrador. Por ejemplo, **`corp.example.com\administrator`** o **`corp\administrator`**.

7. Cuando reciba el mensaje de bienvenida al dominio, reinicie la instancia para que se apliquen los cambios.

Ahora que la instancia se ha unido al dominio Simple AD Active Directory, puede iniciar sesión en esa instancia de forma remota e instalar utilidades para administrar el directorio, como agregar usuarios y grupos. Las herramientas de administración de Active Directory se pueden usar para crear usuarios y grupos. Para obtener más información, consulte Instale las herramientas de administración de Active Directory para Simple AD.

Unir sin problemas una instancia de Amazon EC2 Linux a su Active Directory de Simple AD

Este procedimiento une sin problemas una instancia Linux de Amazon EC2 a su Active Directory Simple AD.

Son compatibles las siguientes distribuciones y versiones de instancias de Linux:

- 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 y Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Las distribuciones anteriores a Ubuntu 14 y Red Hat Enterprise Linux 7 no admiten la característica de unión fluida de dominios.

Requisitos previos

Para poder configurar una unión de dominio perfecta a una instancia de Linux, debe completar los procedimientos de esta sección.

Selección de la cuenta de servicio de unión de dominios fluida

Puede unir de forma fluida equipos Linux a su dominio de Simple AD. Para ello, debe crear una cuenta de usuario con permisos de creación de cuentas de equipos para unir los equipos al dominio. Si bien es posible que los miembros de los administradores del dominio u otros grupos tengan privilegios suficientes para unir los equipos al dominio, no lo recomendamos. Como práctica recomendada, le recomendamos que utilice una cuenta de servicio que tenga los privilegios mínimos necesarios para unir los equipos al dominio.

Para obtener información sobre cómo procesar y delegar los permisos de su cuenta de servicio para la creación de cuentas de equipo, consulte Privilegios delegados a su cuenta de servicio.

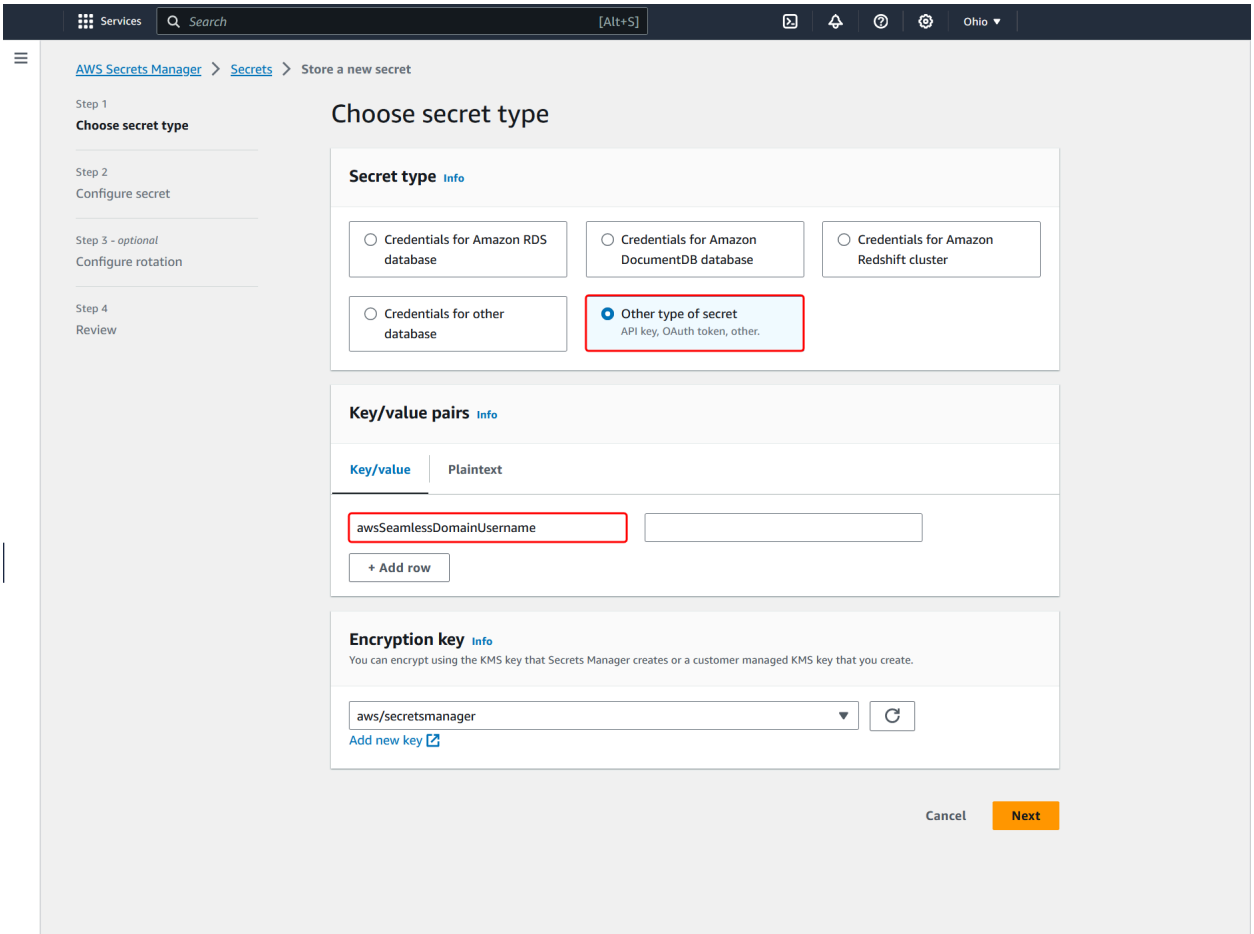
Creación de secretos para almacenar la cuenta de servicio de dominio

Puede utilizarla AWS Secrets Manager para almacenar la cuenta de servicio de dominio.

Creación de secretos y almacenamiento de la información de la cuenta de servicio de dominio

1. Inicie sesión AWS Management Console y abra la AWS Secrets Manager consola en https://console.aws.amazon.com/secretsmanager/.
2. Elija Almacenar un secreto nuevo.
3. En la página Store a new secret (Almacenar un nuevo secreto), haga lo siguiente:
   a. En Tipo de secreto, seleccione Otro tipo de secretos.
   b. En Pares clave/valor, haga lo siguiente:
      i. En el cuadro de filtro, escriba **`awsSeamlessDomainUsername`**. En la misma fila, en el cuadro siguiente, introduce el nombre de usuario de tu cuenta de servicio. Por ejemplo, si utilizó el PowerShell comando anteriormente, el nombre de la cuenta de servicio sería**`awsSeamlessDomain`**.

> **Note**
>
> Debe ingresar **`awsSeamlessDomainUsername`** exactamente como está. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.



ii. Seleccione Agregar regla.

iii. En la nueva fila, en el primer cuadro, ingrese **`awsSeamlessDomainPassword`**. En la misma fila, en el cuadro siguiente, ingrese la contraseña de su cuenta de servicio.

> **Note**
>
> Debe ingresar **`awsSeamlessDomainPassword`** exactamente como está. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.

iv. En Clave de cifrado, deje el valor predeterminado`aws/secretsmanager`. AWS Secrets Manager siempre cifra el secreto al elegir esta opción. También puede elegir una clave que haya creado.

> **Note**
>
> Hay tarifas asociadas AWS Secrets Manager, según el secreto que utilices. Para obtener la lista de precios completa, consulte Precios de AWS Secrets Manager.
>
> Puedes usar la clave AWS gestionada `aws/secretsmanager` que crea Secrets Manager para cifrar tus secretos de forma gratuita. Si crea sus propias claves de KMS para cifrar sus secretos, se le AWS cobrará la tarifa actual AWS KMS . Para obtener más información, consulte AWS Key Management Service Precios.

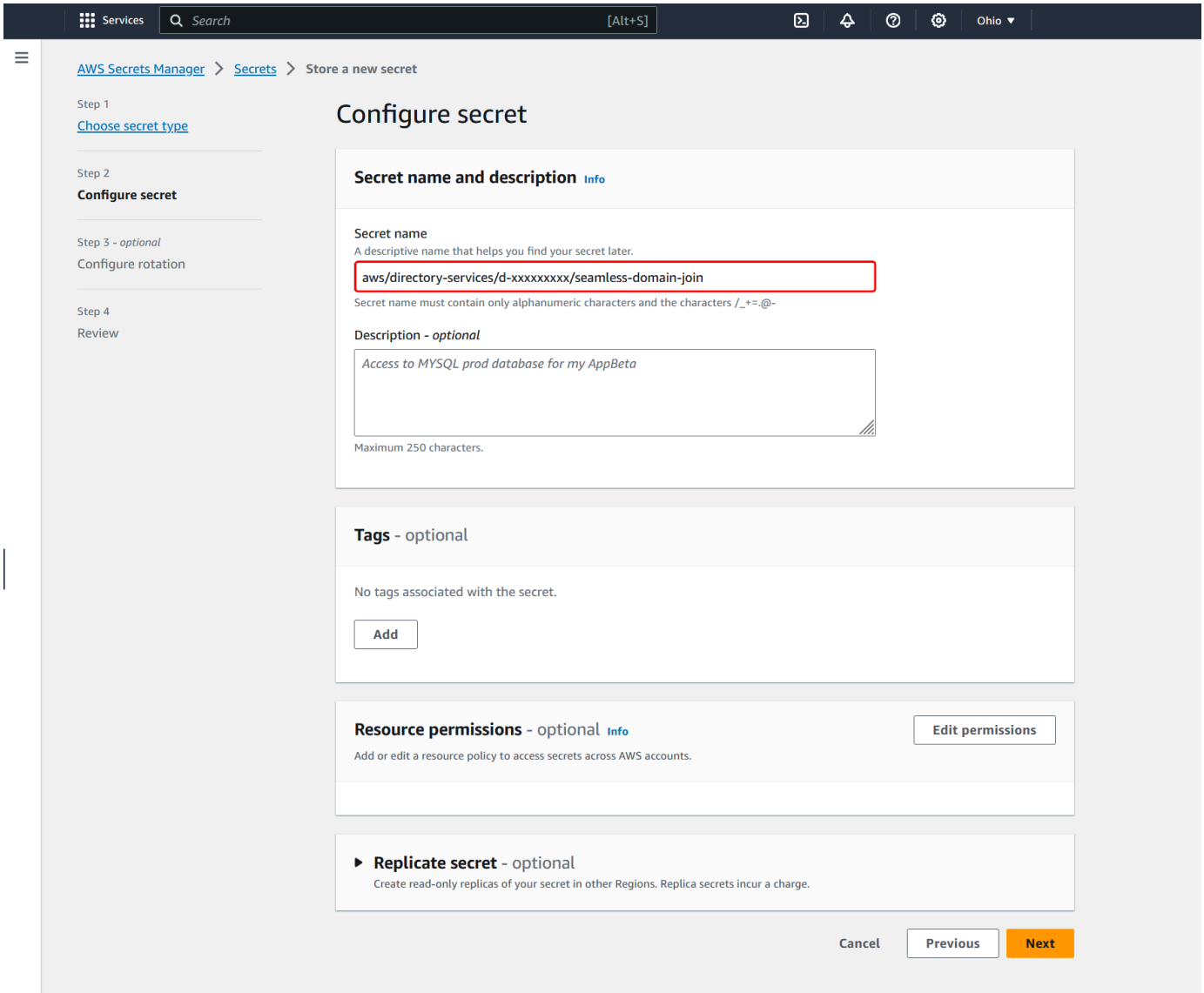
v. Elija Siguiente.

4. En Nombre secreto, introduzca un nombre secreto que incluya su ID de directorio con el siguiente formato y sustituya *`d-xxxxxxxxx`* por su ID de directorio:

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

Se usará para recuperar los secretos de la aplicación.

> **Note**
>
> Debe escribir **`aws/directory-services/`*`d-xxxxxxxxx`*`/seamless-domain-join`** exactamente como está, pero sustituya *`d-xxxxxxxxxx`* por su ID de directorio. Asegúrese de que no haya espacios al principio ni al final. De lo contrario, la unión de dominio fallará.



5. Deje todo lo demás con los valores predeterminados y, a continuación, elija Siguiente.
6. En Configurar rotación automática, elija Deshabilitar rotación automática y, a continuación, Siguiente.

   Puedes activar la rotación de este secreto después de guardarlo.
7. Revise la configuración y, a continuación, elija Almacenar para guardar los cambios. La consola de Secrets Manager vuelve a la lista de secretos de su cuenta con el nuevo secreto ahora incluido en la lista.
8. Elija el nombre del secreto recién creado de la lista y tome nota del valor del ARN del secreto. Lo necesitará en la sección siguiente.

Activa la rotación del secreto de la cuenta del servicio de dominio

Te recomendamos que cambies los secretos con regularidad para mejorar tu postura de seguridad.

Para activar la rotación del secreto de la cuenta del servicio de dominio

- Sigue las instrucciones de la Guía del AWS Secrets Manager usuario sobre cómo configurar la rotación automática de datos AWS Secrets Manager secretos.

  Para el paso 5, utilice la plantilla de rotación de credenciales de Microsoft Active Directory en la Guía del AWS Secrets Manager usuario.

  Para obtener ayuda, consulte Solucionar problemas de AWS Secrets Manager rotación en la Guía del AWS Secrets Manager usuario.

Creación del rol y la política de IAM obligatorios

Siga los siguientes pasos previos para crear una política personalizada que permita el acceso de solo lectura a su secreto de unión a dominios integrada de Secrets Manager (que creó anteriormente) y para crear un nuevo rol de IAM de DomainJoin LinuxEC2.

Creación de la política de lectura de IAM de Secrets Manager

Utilizará la consola de IAM para crear una política que concede acceso de solo lectura a su secreto de Secrets Manager.

Creación de la política de lectura de IAM de Secrets Manager

1. Inicie sesión AWS Management Console como usuario con permiso para crear políticas de IAM. A continuación, abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, Administración de acceso, selecciona Políticas.
3. Elija Crear política.
4. Seleccione la pestaña JSON y copie el texto del siguiente documento de política JSON. A continuación, péguelo en el cuadro de texto JSON.

> **Note**
>
> Asegúrate de reemplazar el ARN de región y recurso por el ARN y la región reales del secreto que creaste 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. Cuando haya terminado, elija Next. El validador de políticas notifica los errores de sintaxis. Para obtener más información, consulte Validación de políticas de IAM.
6. En la página Revisar política, ingrese un nombre para la política, como **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Revise el Resumen de la política para ver los permisos concedidos por su política. Seleccione Crear política para guardar los cambios. La nueva política aparece en la lista de las políticas administradas y está lista para asociar a una identidad.

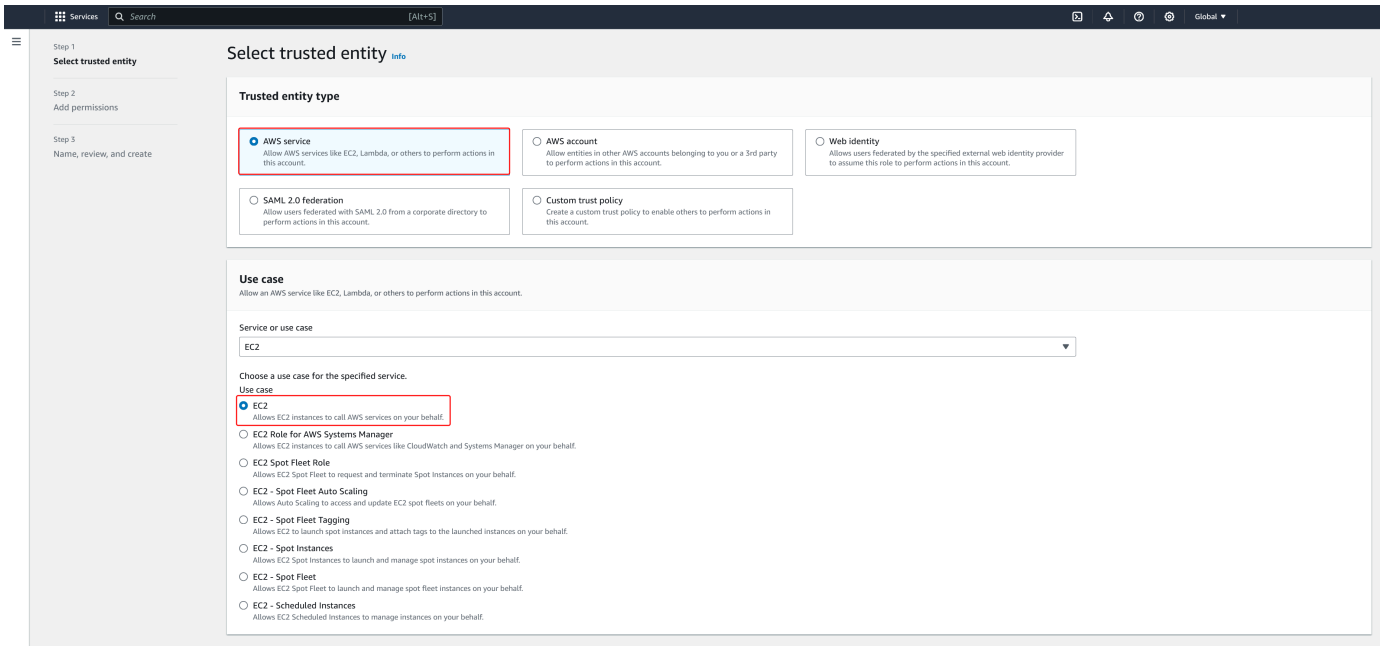
> **Note**
>
> Le recomendamos que cree una política por secreto. De este modo, se garantiza que las instancias solo tengan acceso al secreto adecuado y se minimiza el impacto en caso de que una instancia se vea comprometida.

Cree el rol LinuxEC2 DomainJoin

Utilice la consola de IAM para crear el rol que utilizará para unirse al dominio de su instancia de EC2 de Linux.

Para crear el rol LinuxEC2 DomainJoin

1. Inicie sesión AWS Management Console como usuario con permiso para crear políticas de IAM. A continuación, abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, en Administración del acceso, elija Roles.
3. En el panel de contenido, elija Crear rol.
4. En Seleccionar tipo de entidad de confianza, seleccione Servicio de AWS .
5. En Caso de uso, elija EC2 y, a continuación, elija Siguiente.



6. En Políticas de filtro, haga lo siguiente:
   a. Escriba **`AmazonSSMManagedInstanceCore`**. A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   b. Escriba **`AmazonSSMDirectoryServiceAccess`**. A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   c. Ingrese **`SM-Secret-Linux-DJ-`***`d-xxxxxxxxxx`***`-Read`** (o el nombre de la política creada en el procedimiento anterior). A continuación, seleccione la casilla de verificación de ese elemento de la lista.
   d. Tras añadir las tres políticas enumeradas anteriormente, seleccione Crear función.

> **Note**
>
> AmazonSSM DirectoryServiceAccess proporciona los permisos para unir instancias a una instancia Active Directory gestionada por. AWS Directory Service AmazonSSM ManagedInstanceCore proporciona los permisos mínimos necesarios para usar el servicio. AWS Systems Manager Para obtener más información sobre la creación de un rol con estos permisos y para obtener información sobre otros permisos y políticas que puede asignar a su rol de IAM, consulte Creación de un perfil de instancia de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .

7. Introduzca un nombre para su nueva función, por ejemplo, **`LinuxEC2DomainJoin`** u otro nombre que prefiera en el campo Nombre de la función.
8. (Opcional) En Role description (Descripción del rol), escriba una descripción.
9. (Opcional) Selecciona Añadir nueva etiqueta en el paso 3: Añadir etiquetas para añadir etiquetas. Los pares clave-valor de etiquetas se utilizan para organizar, rastrear o controlar el acceso de este rol.
10. Elija Crear rol.

Une sin problemas una instancia de Linux a tu Active Directory de Simple AD

Ahora que ha configurado todas las tareas previas, puede utilizar el siguiente procedimiento para unirse sin problemas a su instancia EC2 de Linux.

Para unirse sin problemas a su instancia de Linux

1. Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.
2. En el selector de regiones de la barra de navegación, elija el Región de AWS mismo directorio que el existente.
3. En el panel de control de EC2, en la sección Lanzar instancia, elija Lanzar instancia.
4. En la página Lanzar una instancia, en la sección Nombre y etiquetas, introduce el nombre que deseas usar para tu instancia EC2 de Linux.
5. (Opcional) Elija Agregar etiquetas adicionales para agregar uno o varios pares clave-valor de etiqueta para organizar o controlar el acceso a esta instancia de EC2 o hacer su seguimiento.

6. En la sección Imagen de aplicación e sistema operativo (Amazon Machine Image), elija la AMI de Linux que desee lanzar.

> **Note**
>
> La AMI utilizada debe tener AWS Systems Manager (SSM Agent) la versión 2.3.1644.0 o superior. Para comprobar la versión de SSM Agent instalada en la AMI mediante el lanzamiento de una instancia desde esa AMI, consulte Obtener la versión de SSM Agent instalada actualmente. Si necesita actualizar SSM Agent, consulte Instalación y configuración de SSM Agent en instancias de EC2 para Linux.
> SSM usa el `aws:domainJoin` complemento al unir una instancia de Linux a un dominio. Active Directory *El complemento cambia el nombre de host de las instancias de Linux al formato EC2AMAZ-XXXXXXX.* Para obtener más información al respecto*`aws:domainJoin`*, consulte la referencia del complemento del documento de AWS Systems Manager comandos en la Guía del usuario.AWS Systems Manager

7. En la sección Tipo de instancia, elija el tipo de instancia que desee usar en la lista desplegable Tipo de instancia.
8. En la sección Par de claves (inicio de sesión), puede elegir entre crear un nuevo par de claves o elegir un par de claves existente. Para crear un nuevo par de claves, elija Crear nuevo par de claves. Ingrese un nombre para el par de claves y seleccione una opción en Tipo de par de claves y Formato de archivo de clave privada. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija .pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija .ppk. Elija Crear par de claves. Su navegador descargará el archivo de clave privada automáticamente. Guarde el archivo de clave privada en un lugar seguro.

> **Important**
>
> Esta es la única oportunidad para guardar el archivo de clave privada.

9. En la página Lanzar una instancia, en la sección Configuración de red, elija Editar. Elija la VPC en la que se creó el directorio en la lista desplegable VPC: obligatoria.
10. Elija una de las subredes públicas de su VPC en la lista desplegable Subred. La subred que elija debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.

Para obtener más información sobre cómo conectar una puerta de enlace de Internet, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.

11. En Autoasignar IP pública, elija Habilitar.

    Para obtener más información sobre el direccionamiento IP público y privado, consulte el direccionamiento IP de las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

12. En la configuración Firewall (grupos de seguridad), puede usar la configuración predeterminada o hacer cambios para adaptarla a sus necesidades.
13. En la configuración Configurar almacenamiento, puede utilizar los ajustes predeterminados o hacer los cambios necesarios para adaptarlos a sus necesidades.
14. Seleccione la sección Detalles avanzados y elija su dominio en la lista desplegable Directorio de unión de dominios.

> **Note**
>
> Tras elegir el directorio de unión de dominios, es posible que vea:
>
> ⚠ An error was detected in your existing SSM document. You can delete the existing SSM document here and we'll create a new one with correct properties on instance launch. ✕
>
> Este error se produce si el asistente de lanzamiento de EC2 identifica un documento SSM existente con propiedades inesperadas. Puede elegir una de las opciones siguientes:
>
> - Si ya ha editado el documento SSM y las propiedades son las esperadas, seleccione cerrar y proceda a lanzar la instancia de EC2 sin cambios.
> - Seleccione el enlace para eliminar el documento SSM existente aquí para eliminar el documento SSM. Esto permitirá crear un documento SSM con las propiedades correctas. El documento SSM se creará automáticamente al lanzar la instancia EC2.

15. Para el perfil de instancia de IAM, elija el rol de IAM que creó anteriormente en la sección de requisitos previos. Paso 2: Crear el rol LinuxEC2. DomainJoin
16. Seleccione Iniciar instancia.

> **Note**
>
> Si va a llevar a cabo una unión de dominio fluida con SUSE Linux, es necesario reiniciarla para que las autenticaciones funcionen. Para reiniciar SUSE desde el terminal Linux, escriba sudo reboot.

Unir manualmente una instancia de Amazon EC2 Linux a su Active Directory de Simple AD

Además de las instancias Windows de Amazon EC2, también puede unir determinadas instancias de Amazon EC2 Linux a su Active Directory de Simple AD. Son compatibles las siguientes distribuciones y versiones de instancias de Linux:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI de Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS y Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Puede que funcionen otras versiones y distribuciones de Linux, pero no se han probado.

Requisitos previos

Antes de poder unir una instancia de Amazon Linux, CentOS, Red Hat o Ubuntu a su directorio, la instancia debe lanzarse primero como se especifica en Unir sin problemas una instancia de Amazon EC2 Linux a su Active Directory de Simple AD.

> **Important**
>
> Algunos de los siguientes procedimientos, si no se siguen correctamente, pueden hacer que la instancia resulte inaccesible o inservible. Por lo tanto, recomendamos encarecidamente

que realice una copia de seguridad o una instantánea de la instancia antes de realizar estos procedimientos.

Para unir una instancia de Linux al directorio

Siga los pasos para su instancia de Linux específica mediante una de las siguientes pestañas:

Amazon Linux

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para que utilice las direcciones IP del servidor DNS AWS Directory Service de los servidores DNS proporcionados. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de 64 bits de Amazon Linux esté actualizada.

   ```
   sudo yum -y update
   ```

4. Instale los paquetes necesarios de Amazon Linux en la instancia de Linux.

   > **Note**
   > Algunos de estos paquetes pueden estar ya instalados.
   > Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

   Amazon Linux

   ```
   sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
    krb5-workstation
   ```

> **Note**
>
> Si necesita ayuda para determinar la versión de Amazon Linux que está utilizando, consulte Identificación de imágenes de Amazon Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.

5. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Una cuenta en el dominio *example.com* con privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

6. Configure el servicio SSH para permitir autenticación de contraseñas.

   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Establezca la opción `PasswordAuthentication` en `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Reinicie el servicio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Otra opción:

```
sudo service sshd restart
```

7. Una vez que la instancia se haya reiniciado, conéctese a ella con cualquier cliente SSH y añada el grupo de administradores de dominios a la lista sudoers siguiendo estos pasos:

   a. Abra el archivo `sudoers` con el siguiente comando:

   ```
   sudo visudo
   ```

   b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

CentOS

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para que utilice las direcciones IP del servidor DNS AWS Directory Service de los servidores DNS proporcionados. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de CentOS 7 esté actualizada.

   ```
   sudo yum -y update
   ```

4. Instale los paquetes necesarios de CentOS 7 en la instancia de Linux.

   > **Note**
   >
   > Algunos de estos paquetes pueden estar ya instalados.

Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Una cuenta en el dominio *example.com* con privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

6. Configure el servicio SSH para permitir autenticación de contraseñas.
   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Establezca la opción `PasswordAuthentication` en `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Reinicie el servicio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Otra opción:

```
sudo service sshd restart
```

7. Una vez que la instancia se haya reiniciado, conéctese a ella con cualquier cliente SSH y añada el grupo de administradores de dominios a la lista sudoers siguiendo estos pasos:

   a. Abra el archivo `sudoers` con el siguiente comando:

   ```
   sudo visudo
   ```

   b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

Red hat

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para que utilice las direcciones IP del servidor DNS AWS Directory Service de los servidores DNS proporcionados. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de 64 bits de Red Hat esté actualizada.

   ```
   sudo yum -y update
   ```

4. Instale los paquetes necesarios de Red Hat en la instancia de Linux.

   > **Note**
   >
   > Algunos de estos paquetes pueden estar ya instalados.

Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

El SaM AccountName de una cuenta del dominio *example.com* que tiene privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

6. Configure el servicio SSH para permitir autenticación de contraseñas.
   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Establezca la opción `PasswordAuthentication` en `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Reinicie el servicio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Otra opción:

```
sudo service sshd restart
```

7. Una vez que la instancia se haya reiniciado, conéctese a ella con cualquier cliente SSH y añada el grupo de administradores de dominios a la lista sudoers siguiendo estos pasos:

   a. Abra el archivo `sudoers` con el siguiente comando:

   ```
   sudo visudo
   ```

   b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

Ubuntu

1. Conéctese a la instancia con cualquier cliente SSH.
2. Configure la instancia de Linux para que utilice las direcciones IP del servidor DNS AWS Directory Service de los servidores DNS proporcionados. Puede hacerlo configurándolo en el conjunto de opciones de DHCP asociado a la VPC o ajustándolo manualmente en la instancia. Si desea ajustarlo de forma manual, consulte Cómo asignar un servidor DNS estático a una instancia de Amazon EC2 privada en el Centro de conocimientos de AWS para obtener información sobre la configuración del servidor DNS persistente para una distribución y una versión de Linux específicas.
3. Asegúrese de que la instancia de 64 bits de Ubuntu esté actualizada.

   ```
   sudo apt-get update
   sudo apt-get -y upgrade
   ```

4. Instale los paquetes necesarios de Ubuntu en la instancia de Linux.

   > **Note**
   >
   > Algunos de estos paquetes pueden estar ya instalados.

Al instalar los paquetes, es posible que aparezcan varias pantallas de configuración emergentes. Por lo general, puede dejar vacíos los campos de estas pantallas.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Deshabilite la resolución inversa de DNS y establezca el dominio predeterminado en el FQDN de su dominio. Las instancias de Ubuntu deben poder resolverse de forma inversa en el DNS para que el dominio funcione. De lo contrario, tiene que deshabilitar el DNS inverso en /etc/krb5.conf de la manera siguiente:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Una la instancia al directorio con el siguiente comando.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

El SaM AccountName de una cuenta del dominio *example.com* que tiene privilegios de unión a dominios. Introduzca la contraseña de la cuenta cuando se le solicite. Para obtener más información sobre cómo delegar estos privilegios, consulte Delegación de privilegios de unión a directorios para AWS Managed Microsoft AD.

example.com

El nombre de DNS completo del directorio.

```
...
 * Successfully enrolled machine in realm
```

7. Configure el servicio SSH para permitir autenticación de contraseñas.

   a. Abra el archivo `/etc/ssh/sshd_config` en un editor de texto.

```
sudo vi /etc/ssh/sshd_config
```

b. Establezca la opción `PasswordAuthentication` en `yes`.

```
PasswordAuthentication yes
```

c. Reinicie el servicio SSH.

```
sudo systemctl restart sshd.service
```

Otra opción:

```
sudo service sshd restart
```

8. Una vez que la instancia se haya reiniciado, conéctese a ella con cualquier cliente SSH y añada el grupo de administradores de dominios a la lista sudoers siguiendo estos pasos:

a. Abra el archivo `sudoers` con el siguiente comando:

```
sudo visudo
```

b. Agregue lo siguiente a la parte inferior del archivo `sudoers` y guárdelo.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(En el ejemplo anterior, se utiliza“\<espacio>” para crear el carácter de espacio en Linux).

> **Note**
>
> Cuando se utiliza Simple AD, si se crea una cuenta de usuario en una instancia de Linux con la opción “Obligar al usuario a cambiar la contraseña en el primer inicio de sesión”, el usuario no podrá cambiar inicialmente la contraseña con kpasswd. Para cambiar la contraseña la primera vez, un administrador del dominio debe actualizar la contraseña de usuario utilizando las herramientas de administración de Active Directory.

Administración de cuentas desde una instancia de Linux

Para administrar cuentas de Simple AD desde una instancia de Linux, debe actualizar los archivos de configuración específicos de la instancia de Linux como se indica a continuación:

1. Establezca krb5_use_kdcinfo en False en el archivo /etc/sssd/sssd.conf. Por ejemplo:

```
[domain/example.com]
    krb5_use_kdcinfo = False
```

2. Para que se aplique la configuración, debe reiniciar el servicio sssd:

```
$ sudo systemctl restart sssd.service
```

   También puede usar:

```
$ sudo service sssd start
```

3. Si va a administrar usuarios desde una instancia de CentOS Linux, también debe editar el archivo /etc/smb.conf para incluir:

```
[global]
  workgroup = EXAMPLE.COM
  realm = EXAMPLE.COM
  netbios name = EXAMPLE
  security = ads
```

Restricción de acceso de inicio de sesión de cuenta

Como todas las cuentas están definidas en Active Directory, todos los usuarios del directorio pueden iniciar sesión en la instancia de forma predeterminada. Puede permitir que solo unos usuarios específicos inicien sesión en la instancia con ad_access_filter en sssd.conf. Por ejemplo:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica que solo debe permitirse el acceso a la instancia a los usuarios si son miembros de un grupo específico.

cn

El nombre común del grupo que debería tener acceso. En este ejemplo, el nombre del grupo es *admins*.

ou

Esta es la unidad organizativa en la que se encuentra el grupo anterior. En este ejemplo, el valor de OU es *Testou*.

dc

Este es el componente de dominio de su dominio. En este ejemplo, *example*.

dc

Este es un componente de dominio adicional. En este ejemplo, *com*.

Debe agregar manualmente ad_access_filter a su /etc/sssd/sssd.conf.

Abra el archivo /etc/sssd/sssd.conf en un editor de texto.

```
sudo vi /etc/sssd/sssd.conf
```

Después de hacerlo, su sssd.conf podrá tener este aspecto:

```
[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 se aplique la configuración, debe reiniciar el servicio sssd:

```
sudo systemctl restart sssd.service
```

También puede usar:

```
sudo service sssd restart
```

Mapeo de ID

El mapeo de ID se puede realizar mediante dos métodos para mantener una experiencia unificada entre las identidades del identificador de usuario (UID) y el identificador de grupo (GID) de UNIX/Linux y las identidades del identificador de Active Directory seguridad (SID).

1. Centralizado
2. Distribuido

> **Note**
>
> El mapeo centralizado de la identidad de los usuarios Active Directory requiere una interfaz de sistema operativo portátil o POSIX.

Mapeo centralizado de identidades de usuarios

Active Directoryu otro servicio de Protocolo ligero de acceso a directorios (LDAP) proporciona UID y GID a los usuarios de Linux. EnActive Directory, estos identificadores se almacenan en los atributos de los usuarios:

- UID: el nombre de usuario de Linux (cadena)
- Número de UID: el número de ID de usuario de Linux (entero)
- Número GID: el número de ID del grupo de Linux (entero)

Para configurar una instancia de Linux para usar el UID y el GIDActive Directory, configúrelo `ldap_id_mapping = False` en el archivo sssd.conf. Antes de establecer este valor, compruebe

que ha agregado un UID, un número UID y un número GID a los usuarios y grupos que contiene. Active Directory

Mapeo distribuido de identidades de usuarios

Si Active Directory no tiene la extensión POSIX o si decide no gestionar de forma centralizada el mapeo de identidades, Linux puede calcular los valores de UID y GID. Linux utiliza el identificador de seguridad (SID) único del usuario para mantener la coherencia.

Para configurar el mapeo de ID de usuario distribuido, configúrelo `ldap_id_mapping = True` en el archivo sssd.conf.

Conéctese a la instancia de Linux

Cuando un usuario se conecta a la instancia mediante un cliente SSH, se le solicita que indique su nombre de usuario. El usuario puede introducir el nombre de usuario en formato `username@example.com` o `EXAMPLE\username`. La respuesta tendrá un aspecto similar al siguiente, en función de la distribución de Linux que utilice:

Amazon Linux, Red Hat Enterprise Linux y 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%
```

Delegación de privilegios de unión a directorios para Simple AD

Para unir un equipo al directorio, necesita una cuenta con privilegios para unir equipos al directorio.

Con Simple AD, los miembros del grupo Administradores de dominios tienen privilegios suficientes para unir equipos al directorio.

No obstante, la práctica recomendada es que use una cuenta que tenga solo los privilegios mínimos necesarios. En el procedimiento siguiente se explica cómo crear un nuevo grupo denominado `Joiners` y cómo delegar en este grupo los privilegios necesarios para unir equipos al directorio.

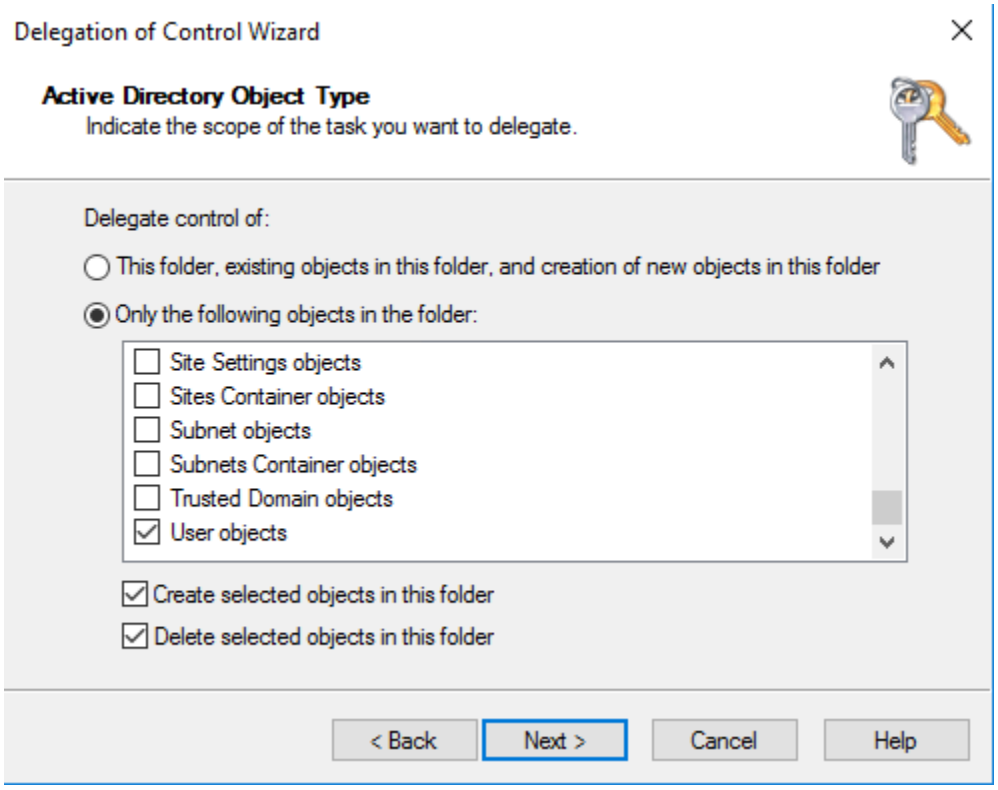
Debe llevar a cabo este procedimiento en un equipo que esté unido al directorio y que tenga instalado el complemento de MMC Usuarios y equipos de Active Directory. Además, es necesario la sesión se inicie como administrador del dominio.

Para delegar privilegios de unión para Simple AD

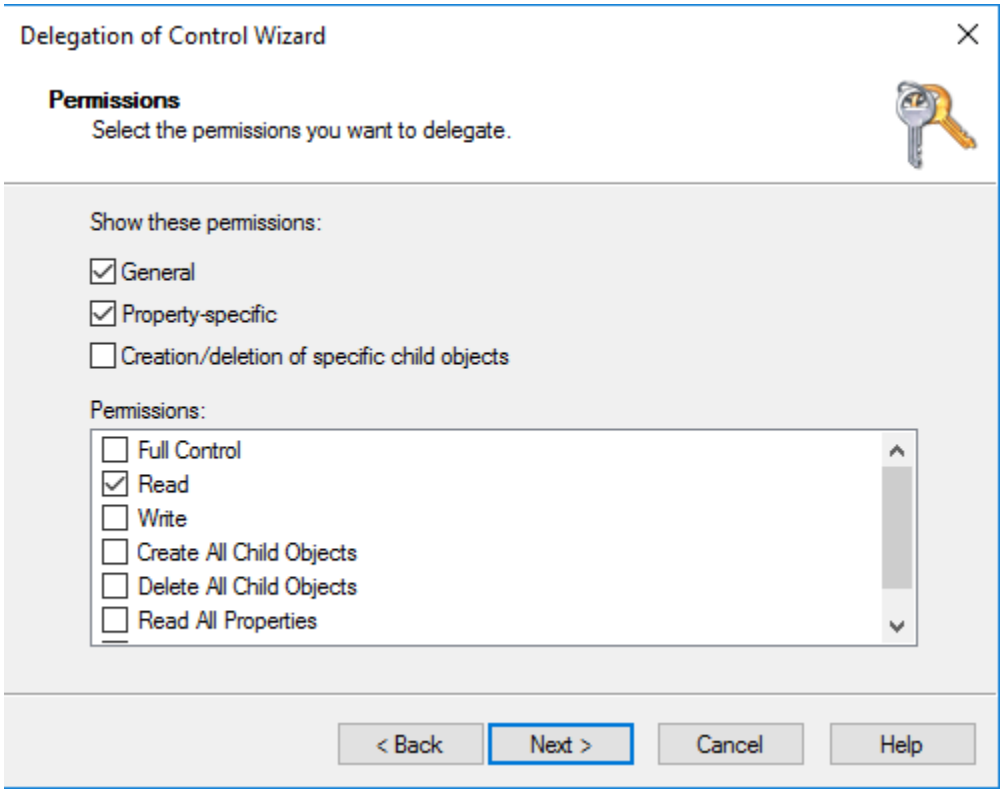
1. Abra Usuarios y equipos de Active Directory y seleccione la raíz del dominio en el árbol de navegación.
2. En el árbol de navegación de la izquierda, abra el menú contextual (haga clic con el botón derecho) Users (Usuarios), seleccione New (Nuevo) y, a continuación, elija Group (Grupo).
3. En el cuadro Nuevo objeto - Grupo, escriba lo siguiente y haga clic en Aceptar.
   - En Group Name (Nombre de grupo), escriba **`Joiners`**.
   - En Ámbito de grupo, escriba Global.

- En Tipo de grupo, seleccione Seguridad.

4. En el árbol de navegación, seleccione la raíz del dominio. En el menú Acción, elija Delegar control.
5. En la página Asistente para delegación de control, elija Siguiente y después seleccione Agregar.
6. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, escriba `Joiners` y haga clic en Aceptar. Si se encuentran varios objetos, seleccione el grupo `Joiners` que creó anteriormente. Elija Siguiente.
7. En la página Tareas que se delegarán, seleccione Crear una tarea personalizada para delegar y luego elija Siguiente.
8. Seleccione Sólo los siguientes objetos en la carpeta y, a continuación, seleccione Objetos de equipo.
9. Seleccione Crear los objetos seleccionados en esta carpeta y Eliminar los objetos seleccionados en esta carpeta. A continuación, elija Next.



10. Seleccione Lectura y Escritura y luego elija Siguiente.



11. Compruebe la información en la página Finalización del Asistente para delegación de control y seleccione Finalizar.
12. Cree un usuario con una contraseña segura y añádalo al grupo `Joiners`. El usuario dispondrá entonces de los privilegios suficientes para conectarse AWS Directory Service al directorio.

Crear un conjunto de opciones de DHCP

AWS recomienda crear un conjunto de opciones de DHCP para el AWS Directory Service directorio y asignar el conjunto de opciones de DHCP a la VPC en la que se encuentra el directorio. De este modo, las instancias de la VPC apuntarán al dominio y a los servidores DNS especificados para resolver los nombres de dominio.

Para obtener más información sobre los conjuntos de opciones de DHCP, consulte Conjuntos de opciones de DHCP en la Guía del usuario de Amazon VPC.

Creación de un conjunto de opciones de DHCP para un directorio

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija DHCP Options Sets y, a continuación, elija Create DHCP options set.

3. En la página Crear conjunto de opciones de DHCP, facilite los siguientes valores para el directorio:

   Nombre

   Etiqueta opcional para el conjunto de opciones.

   Nombre del dominio

   El nombre completo del directorio, por ejemplo `corp.example.com`.

   Domain name servers

   Las direcciones IP de los servidores DNS del directorio AWS proporcionado.

   > **Note**
   > Para encontrarlas, en el panel de navegación de la consola de AWS Directory Service seleccione Directorios y elija el identificador de directorio correspondiente.

   NTP servers

   Deje este campo en blanco.

   NetBIOS name servers

   Deje este campo en blanco.

   NetBIOS node type

   Deje este campo en blanco.

4. Luego, Create DHCP options set (Crear conjunto de opciones de DHCP). El nuevo conjunto de opciones de DHCP aparecerá en la lista de opciones de DHCP.
5. Anote el ID del nuevo conjunto de opciones de DHCP (dopt-*xxxxxxxx*). Lo necesitará para asociar dicho conjunto a su VPC.

Para cambiar el conjunto de opciones de DHCP asociado a una VPC

Los conjuntos de opciones de DHCP no se pueden modificar una vez creados. Si quiere que su VPC utilice un conjunto de opciones de DHCP distinto, tendrá que crear uno nuevo y asociarlo a la VPC. También puede configurar la VPC para que no utilice opciones de DHCP.

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione la VPC y, a continuación, elija Acciones, Editar la configuración de la VPC.
4. En Conjunto de opciones de DHCP, seleccione un conjunto de opciones o elija Sin conjunto de opciones de DHCP y, a continuación, elija Guardar.

Para cambiar el conjunto de opciones de DHCP asociado a una VPC mediante la línea de comandos, consulte lo siguiente:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Mantenimiento de su directorio de Simple AD

En esta sección, se describe cómo llevar a cabo las tareas administrativas comunes para su entorno de Simple AD.

Temas

Eliminación de Simple AD

Cuando se elimina un Simple AD, se eliminan todos los datos del directorio y las instantáneas y no se pueden recuperar. Una vez que se elimina el directorio, todas las instancias que están unidas a él permanecen intactas. No se puede, sin embargo, utilizar las credenciales del directorio para iniciar sesión en estas instancias. Es necesario iniciar sesión en estas instancias con una cuenta de usuario que sea local para la instancia.

Eliminación de un directorio

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios. Asegúrese de estar en el Región de AWS lugar donde Active Directory está desplegado el suyo. Para obtener más información, consulte Elegir una región.

2. Asegúrese de que no haya ninguna AWS aplicación habilitada en el directorio que desea eliminar. AWS Las aplicaciones habilitadas le impedirán eliminar su Microsoft AD AWS administrado o su AD Simple.

   a. En la página Directories (Directorios), elija el ID del directorio.

   b. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones). En la sección de AWS aplicaciones y servicios, verá qué AWS aplicaciones están habilitadas para su directorio.

      - Deshabilita AWS Management Console el acceso. Para obtener más información, consulte Deshabilitación del acceso a la AWS Management Console.
      - Para deshabilitar Amazon WorkSpaces, debes anular el registro del servicio en el directorio de la consola. WorkSpaces Para obtener más información, consulta Cómo anular el registro de un directorio en la Guía de WorkSpaces administración de Amazon.
      - Para deshabilitar Amazon WorkDocs, debes eliminar el WorkDocs sitio de Amazon en la WorkDocs consola de Amazon. Para obtener más información, consulta Eliminar un sitio en la Guía de WorkDocs administración de Amazon.
      - Para deshabilitar Amazon WorkMail, debes eliminar la WorkMail organización de Amazon en la WorkMail consola de Amazon. Para obtener más información, consulta Eliminar una organización en la Guía del WorkMail administrador de Amazon.
      - Para deshabilitar Amazon FSx para Windows File Server, debe eliminar el sistema de archivos de Amazon FSx del dominio. Para obtener más información, consulte Cómo trabajar con Active Directory fSx for Windows File Server en la Guía del usuario de Amazon FSx for Windows File Server.
      - Para deshabilitar Amazon Relational Database Service, debe eliminar la instancia de Amazon RDS del dominio. Para obtener más información, consulte Administración de una instancia de base de datos en un dominio en la Guía del usuario de Amazon RDS.
      - Para deshabilitar el AWS Client VPN servicio, debe eliminar el servicio de directorio del punto final Client VPN. Para obtener más información, consulte Active DirectoryAutenticación en la Guía AWS Client VPN del administrador.
      - Para deshabilitar Amazon Connect, debe eliminar la instancia de Amazon Connect. Para obtener más información, consulte Eliminación de una instancia de Amazon Connect en la Guía de administración de Amazon Connect.

- Para deshabilitar Amazon QuickSight, debes darte de baja de Amazon QuickSight. Para obtener más información, consulta Cómo cerrar tu Amazon QuickSight cuenta en la Guía del QuickSight usuario de Amazon.

> **Note**
>
> Si lo está utilizando AWS IAM Identity Center y ya lo ha conectado anteriormente al directorio AWS administrado de Microsoft AD que planea eliminar, primero debe cambiar la fuente de identidad antes de poder eliminarlo. Para obtener más información, consulte Cambio del origen de identidad en la Guía del usuario de IAM Identity Center.

3. En el panel de navegación, elija Directories (Directorios).
4. Seleccione únicamente el directorio que se va a eliminar y haga clic en Eliminar. La eliminación del directorio tarda varios minutos. Cuando el directorio se haya eliminado, se eliminará de la lista de directorios.

Creación de una instantánea o restauración del directorio

AWS Directory Service ofrece la posibilidad de tomar instantáneas manuales de los datos para el directorio Simple AD. Estas instantáneas se pueden utilizar para realizar una point-in-time restauración del directorio. No puede tomar instantáneas de directorios de Conector AD.

Temas

Creación de una instantánea del directorio

Se puede usar una instantánea para restaurar el directorio al estado en el que se encontraba cuando se hizo la instantánea. Para crear una instantánea del directorio manualmente, siga estos pasos:

> **Note**
>
> Solo se pueden crear 5 instantáneas manualmente por directorio. Si ya ha alcanzado este límite, para poder crear otra instantánea tendrá que eliminar una instantánea creada manualmente.

Creación de una instantánea manual

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Maintenance (Mantenimiento).
4. En la sección Instantáneas, elija Acciones y, a continuación, seleccione Crear instantánea.
5. En el cuadro de diálogo Crear una instantánea del directorio, proporcione una descripción de la instantánea, si lo desea. Cuando esté todo listo, seleccione Crear.

En función del tamaño del directorio, puede que transcurran varios minutos hasta que se cree la instantánea. Cuando la instantánea esté lista, el valor Status cambia a `Completed`.

Restauración de un directorio a partir de una instantánea

Restaurar un directorio a partir de una instantánea equivale a hacer que el directorio retroceda en el tiempo. Las instantáneas del directorio son exclusivas del directorio desde el que se crearon. Una instantánea solo se puede restaurar en el directorio a partir del cual se creó. Además, la antigüedad máxima admitida de una instantánea manual es de 180 días. Para obtener más información, consulte Tiempo de conservación de una copia de seguridad de estado del sistema de Active Directory en el sitio web de Microsoft.

> **Warning**
>
> Le recomendamos que contacte con el Centro de AWS Support antes de llevar a cabo cualquier restauración de una instantánea; tal vez podamos ayudarle a evitar la necesidad de restaurar instantáneas. Cualquier restauración a partir de una instantánea puede provocar la pérdida de datos, ya que las instantáneas reflejan el estado del directorio en un momento determinado. Es importante que entienda que los servidores DNS y controladores de dominio asociados al directorio funcionarán sin conexión hasta que finalice la restauración.

Para restaurar el directorio a partir de una instantánea, siga estos pasos:

Para restaurar un directorio a partir de una instantánea

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Maintenance (Mantenimiento).
4. En la sección Instantáneas, seleccione una instantánea de la lista, elija Acciones y, a continuación, seleccione Restaurar instantánea.
5. Lea la información del cuadro de diálogo Restaurar instantánea del directorio y elija Restaurar.

En el caso de los directorios de Simple AD, el proceso de restauración puede tardar varios minutos. Cuando la restauración se haya llevado a cabo correctamente, el valor de Estado del directorio cambia a `Active`. Los cambios efectuados en el directorio después de la fecha de instantánea se sobrescriben.

Eliminación de una instantánea

Eliminación de una instantánea

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Maintenance (Mantenimiento).
4. En la sección Instantáneas, elija Acciones y, a continuación, seleccione Eliminar instantánea.
5. Confirme que desea eliminar la instantánea y elija Eliminar.

Ver información del directorio

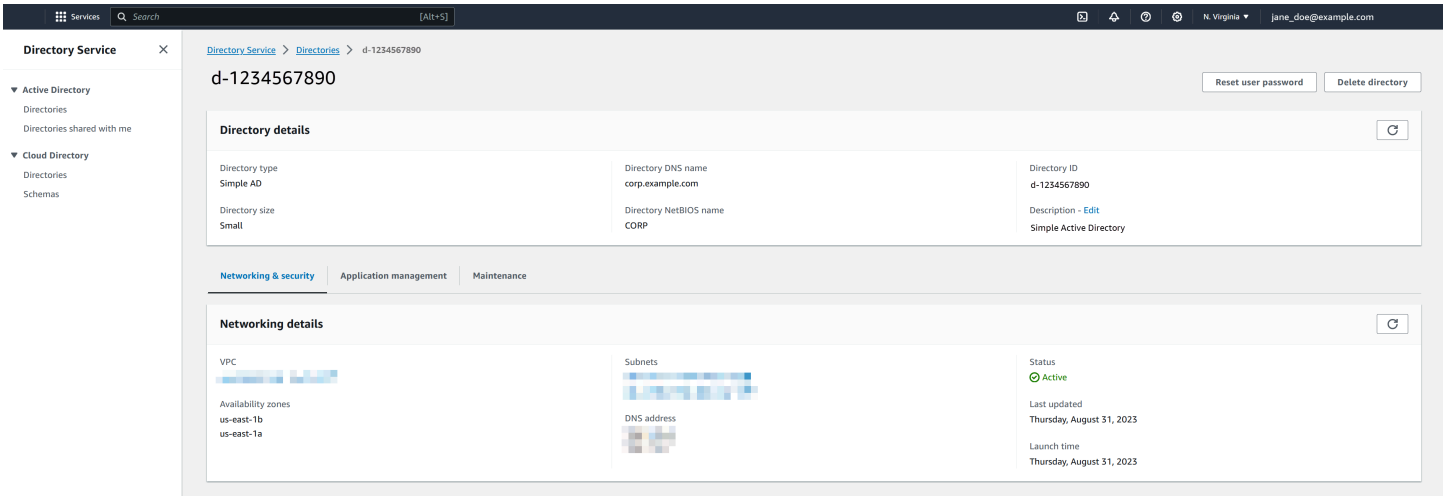
Puede ver información detallada sobre un directorio.

Visualización de información detallada del directorio

1. En el panel de navegación de la AWS Directory Service consola, en Active Directory, selecciona Directorios.

2. Haga clic en el enlace del identificador de directorio correspondiente al directorio. La información acerca del directorio se muestra en la sección Detalles del directorio.

Para obtener más información acerca del campo Status, consulte Descripción del estado del directorio.



Habilite el acceso a AWS aplicaciones y servicios

Los usuarios pueden autorizar a Simple AD para que AWS las aplicaciones y los servicios, como Amazon WorkSpaces, accedan a suActive Directory. Las siguientes AWS aplicaciones y servicios se pueden activar o desactivar para que funcionen con Simple AD.

AWS aplicación/servicio	Más información…
Amazon Chime	Para obtener más información, consulte la Guía de administración de Amazon Chime.
Amazon WorkDocs	Para obtener más información, consulta la Guía de WorkDocs administración de Amazon
Amazon WorkMail	Para obtener más información, consulta la Guía del WorkMail administrador de Amazon.
Amazon WorkSpaces	Puede crear un AD Simple, un AD AWS administrado de Microsoft o un AD Connector directamente desde WorkSpaces. Solo tiene

AWS aplicación/servicio	Más información…
	que lanzar Advanced Setup al crear su espacio de Workspace. Para obtener más información, consulta la Guía de WorkSpaces administración de Amazon.
AWS Management Console	Para obtener más información, consulte Habilitación del acceso a la AWS Management Console con credenciales de AD.

Una vez habilitado, el acceso a los directorios se gestiona en la consola de la aplicación o del servicio al que desea otorgar acceso a su directorio. Para encontrar los enlaces de AWS aplicaciones y servicios descritos anteriormente en la AWS Directory Service consola, lleve a cabo los siguientes pasos.

Para mostrar las aplicaciones y los servicios para un directorio

1. En el panel de navegación de la consola deAWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. Consulte la lista en la sección de Aplicaciones y servicios deAWS .

Para obtener más información sobre cómo autorizar o desautorizar el uso de AWS aplicaciones y servicios AWS Directory Service, consulteAutorización para AWS aplicaciones y servicios que utilizan AWS Directory Service.

Temas

- Creación de una URL de acceso
- Inicio de sesión único

Creación de una URL de acceso

La URL de acceso se usa con las aplicaciones y los servicios de AWS, como Amazon WorkDocs, para llegar a una página de inicio de sesión asociada a su directorio. La dirección URL debe ser única en todo el mundo. Estos son los pasos para crear una URL de acceso para el directorio.

> **Warning**
>
> Cuando se crea una URL de acceso de aplicaciones para este directorio, no se puede modificar. Una vez creada la URL de acceso, nadie más podrá usarla. Si elimina el directorio, se eliminará también la URL de acceso. A partir de ese momento, cualquier otra cuenta podrá usarla.

Para crear una URL de acceso

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. En la sección Application access URL (URL de acceso a aplicaciones), si no se ha asignado una URL de acceso al directorio, se mostrará el botón Create (Crear). Escriba un alias de directorio y elija Create (Crear). Si se devuelve un error La entidad ya existe, eso significa que ya se ha asignado el alias de directorio especificado. Elija otro alias y repita el procedimiento.

   La URL de acceso se muestra en el formato `<alias>`.awsapps.com.

Inicio de sesión único

AWS Directory Service ofrece la posibilidad de permitir a los usuarios acceder a Amazon WorkDocs desde un ordenador unido al directorio sin tener que introducir sus credenciales por separado.

Antes de habilitar el inicio de sesión único, debe tomar determinadas medidas adicionales para permitir que los navegadores web de los usuarios admitan la función de inicio de sesión único. Los usuarios pueden necesitar modificar la configuración de su navegador web para permitir el inicio de sesión único.

> **Note**
>
> La función de inicio de sesión único solo funciona en equipos que se hayan unido al directorio de AWS Directory Service . No puede aplicarse en equipos que no estén vinculados al directorio.

Si el directorio es un directorio de AD Connector y la cuenta de servicio de AD Connector no tiene permiso para agregar o eliminar el atributo de nombre de la entidad principal del servicio, en los pasos 5 y 6 siguientes, tiene dos opciones:

1. Puede continuar y se le pedirá el nombre de usuario y la contraseña de un usuario de directorio que tenga este permiso para agregar o eliminar el atributo del nombre de la entidad principal del servicio en la cuenta de servicio de AD Connector. Estas credenciales solo se usan para permitir el inicio de sesión único; el servicio no las guarda. Los permisos de la cuenta del servicio AD Connector no se cambian.
2. Puede delegar permisos para permitir que la cuenta de servicio de AD Connector añada o elimine el atributo de nombre principal del servicio por sí misma. Puede ejecutar los siguientes PowerShell comandos desde un equipo unido a un dominio mediante una cuenta que tenga permisos para modificar los permisos de la cuenta de servicio de AD Connector. El siguiente comando le dará a la cuenta del servicio de AD Connector la capacidad de agregar y eliminar un atributo de nombre de la entidad principal del servicio solo para ella misma.

```
$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 activar o desactivar el inicio de sesión único con Amazon WorkDocs

1. En el panel de navegación de la consola de AWS Directory Service, seleccione Directorios.
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. En la sección URL de acceso a la aplicación, selecciona Habilitar para habilitar el inicio de sesión único en Amazon. WorkDocs

   Si no ve el botón Habilitar, puede que tenga que crear primero una URL de acceso antes de que se muestre esta opción. Para obtener más información sobre cómo crear una URL de acceso, consulte Creación de una URL de acceso.
5. En el cuadro de diálogo Habilitar el inicio de sesión único para este directorio, elija Habilitar. El inicio de sesión único está habilitado para el directorio.
6. Si más adelante quieres deshabilitar el inicio de sesión único con Amazon WorkDocs, selecciona Inhabilitar y, a continuación, en el cuadro de diálogo Inhabilitar el inicio de sesión único para este directorio, selecciona Inhabilitar de nuevo.

Temas

- Inicio de sesión único en IE y Chrome
- Inicio de sesión único en Firefox

Inicio de sesión único en IE y Chrome

Para permitir que los navegadores Microsoft Internet Explorer (IE) y Google Chrome admitan la función de inicio de sesión único, deberá hacer lo siguiente en el equipo cliente:

- Agregue su URL de acceso (por ejemplo, https://*<alias>*.awsapps.com) a la lista de sitios aprobados para inicio de sesión único.

- Habilita las secuencias de comandos activas (). JavaScript
- Permita el inicio de sesión automático.
- Habilite la autenticación integrada.

Usted o sus usuarios pueden realizar estas tareas manualmente, o bien pueden cambiar estos ajustes mediante la configuración de la política de grupo.

Temas

Actualización manual para inicio de sesión único en Windows

Para habilitar manualmente la función de inicio de sesión único en un equipo Windows, siga estos pasos en el equipo cliente. Es posible que algunos de estos ajustes estén ya establecidos correctamente.

Habilitación manual de la función de inicio de sesión único en Internet Explorer y Chrome en Windows

1. Para abrir el cuadro de diálogo Internet Properties, elija el menú Start, escriba `Internet Options` en el cuadro de búsqueda y elija Internet Options.
2. Añada su URL de acceso a la lista de sitios aprobados para inicio de sesión único siguiendo estos pasos:
   a. En el cuadro de diálogo Internet Properties, seleccione la pestaña Security.
   b. Seleccione Local intranet y elija Sites.
   c. En el cuadro de diálogo Local intranet, elija Advanced.
   d. Añada su URL de acceso a la lista de sitios web y elija Close.
   e. En el cuadro de diálogo Local intranet, elija OK.
3. Para habilitar el scripting activo, siga estos pasos:
   a. En la pestaña Security del cuadro de diálogo Internet Properties, elija Custom level.
   b. En el cuadro de diálogo Security Settings - Local Intranet Zone, desplácese hasta Scripting y seleccione Enable en Active scripting.

   c. En el cuadro de diálogo Security Settings - Local Intranet Zone, elija OK.

4. Para habilitar el inicio de sesión automático, siga estos pasos:

   a. En la pestaña Security del cuadro de diálogo Internet Properties, elija Custom level.
   b. En el cuadro de diálogo Security Settings - Local Intranet Zone, desplácese hasta User Authentication y seleccione Automatic logon only in Intranet zone en Logon.
   c. En el cuadro de diálogo Security Settings - Local Intranet Zone, elija OK.
   d. En el cuadro de diálogo Security Settings - Local Intranet Zone, elija OK.

5. Para habilitar la autenticación integrada, siga estos pasos:

   a. En el cuadro de diálogo Internet Properties, seleccione la pestaña Advanced.
   b. Desplácese hasta Security y seleccione Enable Integrated Windows Authentication.
   c. En el cuadro de diálogo Internet Properties, seleccione OK.

6. Cierre el navegador y vuelva a abrirlo para que se apliquen los cambios.

Actualización manual para inicio de sesión único en OS X

Para habilitar manualmente el inicio de sesión único para Chrome en OS X, siga estos pasos en el equipo cliente. Necesitará derechos de administrador en su equipo para poder completar estos pasos.

Habilitación manual de la función de inicio de sesión único en Chrome en OS X

1. Añada su URL de acceso a la AuthServerAllowlistpolítica ejecutando el siguiente comando:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Abra System Preferences, vaya al panel Profiles y elimine el perfil `Chrome Kerberos Configuration`.
3. Reinicie Chrome y abra chrome://policy en Chrome para confirmar que se haya implementado la nueva configuración.

Configuración de la política de grupo para el inicio de sesión único

El administrador del dominio puede implementar una configuración de política de grupo para aplicar cambios en la configuración de inicio de sesión único en los equipos cliente vinculados al dominio.

> **Note**
>
> Si administras los navegadores web Chrome en los ordenadores de tu dominio con políticas de Chrome, debes añadir tu URL de acceso a la AuthServerAllowlistpolítica. Para obtener más información sobre la configuración de políticas de Chrome, vaya a Policy Settings in Chrome (en inglés).

Habilitación del inicio de sesión único para Internet Explorer y Chrome mediante la configuración de la política de grupo

1. Cree un nuevo objeto de política de grupo siguiendo estos pasos:
   a. Abra la herramienta de administración de directivas de grupo, navegue hasta su dominio y seleccione Group Policy Objects.
   b. En el menú principal, elija Action y seleccione New.
   c. En el cuadro de diálogo Nuevo GPO, escriba un nombre descriptivo para el objeto de políticas de grupo, como `IAM Identity Center Policy`, y deje GPO de inicio de origen establecido en (ninguno). Haga clic en OK (Aceptar).
2. Añada la URL de acceso a la lista de sitios aprobados para inicio de sesión único siguiendo estos pasos:
   a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Objetos de políticas de grupo, abra el menú contextual (clic con el botón derecho) de su política de IAM Identity Center y, a continuación, elija Editar.
   b. En el árbol de políticas, navegue a User Configuration > Preferences > Windows Settings.
   c. En la lista Windows Settings, abra el menú contextual (clic con el botón derecho) de Registry y elija New registry item.
   d. En el cuadro de diálogo New Registry Properties, especifique las siguientes opciones y elija OK:

      Action

      `Update`

      Hive

      `HKEY_CURRENT_USER`

Ruta

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\<alias>
```

El valor de *<alias>* se deriva de la URL de acceso. Si su URL de acceso es `https://examplecorp.awsapps.com`, el alias será `examplecorp`, y la clave de registro será `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Value name

```
https
```

Value type

```
REG_DWORD
```

Value data

```
1
```

3. Para habilitar el scripting activo, siga estos pasos:

   a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Objetos de políticas de grupo, abra el menú contextual (clic con el botón derecho) de su política de IAM Identity Center y, a continuación, elija Editar.

   b. En el árbol de políticas, navegue a Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

   c. En la lista Intranet Zone, abra el menú contextual (clic con el botón derecho) para Allow active scripting y elija Edit.

   d. En el cuadro de diálogo Allow active scripting, especifique las siguientes opciones y elija OK:

      - Seleccione el botón de opción Enabled.
      - En Options ajuste Allow active scripting en Enable.

4. Para habilitar el inicio de sesión automático, siga estos pasos:

a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Group Policy Objects, abra el menú contextual (clic con el botón derecho) de su política de inicio de sesión único y, a continuación, elija Edit.

b. En el árbol de políticas, navegue a Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

c. En la lista Intranet Zone, abra el menú contextual (clic con el botón derecho) para Logon options y elija Edit.

d. En el cuadro de diálogo Logon options, especifique las siguientes opciones y elija OK:

- Seleccione el botón de opción Enabled.
- En Options ajuste Logon options en Automatic logon only in Intranet zone.

5. Para habilitar la autenticación integrada, siga estos pasos:

a. En la herramienta de administración de políticas de grupo, navegue hasta su dominio, seleccione Objetos de políticas de grupo, abra el menú contextual (clic con el botón derecho) de su política de IAM Identity Center y, a continuación, elija Editar.

b. En el árbol de políticas, navegue a User Configuration > Preferences > Windows Settings.

c. En la lista Windows Settings, abra el menú contextual (clic con el botón derecho) de Registry y elija New registry item.

d. En el cuadro de diálogo New Registry Properties, especifique las siguientes opciones y elija OK:

Action

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

Ruta

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

Value name

```
EnableNegotiate
```

Value type

`REG_DWORD`

Value data

`1`

6. Cierre la ventana de Group Policy Management Editor si aún está abierta.
7. Asigne la nueva política a su dominio siguiendo estos pasos:
   a. En el árbol de administración de la directiva de grupo, abra el menú contextual (clic con el botón derecho) de su dominio y elija Link an Existing GPO.
   b. En la lista Objetos de políticas de grupo, seleccione su política de IAM Identity Center y elija Aceptar.

Estos cambios se aplicarán tras la siguiente actualización de la política de grupo en el cliente o la siguiente vez que el usuario inicie sesión.

Inicio de sesión único en Firefox

Para permitir que el navegador Mozilla Firefox admita el inicio de sesión único, agregue su URL de acceso (por ejemplo, https://*<alias>*.awsapps.com) a la lista de sitios aprobados para inicio de sesión único. Esto puede hacerse manualmente o con un script automatizado.

Temas

- Actualización manual para inicio de sesión único
- Actualización automática para inicio de sesión único

Actualización manual para inicio de sesión único

Para añadir manualmente su URL de acceso a la lista de sitios aprobados en Firefox, siga estos pasos en el equipo cliente.

Para añadir manualmente su URL de acceso a la lista de sitios aprobados en Firefox

1. Abra Firefox y abra luego la página `about:config`.
2. Abra la preferencia `network.negotiate-auth.trusted-uris` y agregue su URL de acceso a la lista de sitios. Utilice una coma (,) para separar varias entradas.

Actualización automática para inicio de sesión único

Como administrador del dominio, puede utilizar un script para agregar su URL de acceso a la preferencia de usuario `network.negotiate-auth.trusted-uris` de Firefox en todos los equipos que haya en la red. Para obtener más información, consulte https://support.mozilla.org/es-es/questions/939037.

Habilitación del acceso a la AWS Management Console con credenciales de AD

AWS Directory Service le permite conceder acceso a AWS Management Console a los miembros de su directorio. De forma predeterminada, los miembros de su directorio no tienen acceso a los recursos de AWS. Asigne roles de IAM a los miembros de su directorio para darles acceso a los distintos servicios y recursos de AWS. El rol de IAM define los servicios, los recursos y el nivel de acceso que tienen los miembros de su directorio.

Para que los miembros de su directorio puedan tener acceso a la consola, es preciso que este cuente con una URL de acceso. Para obtener más información sobre cómo ver los detalles del directorio y obtener la URL de acceso, consulte Ver información del directorio. Para obtener más información sobre cómo crear una URL de acceso, consulte Creación de una URL de acceso.

Para obtener más información sobre cómo crear roles de IAM y asignarlos a los miembros del directorio, consulte Otorgar acceso a los recursos de AWS a usuarios y grupos.

Temas

Artículo relacionado del blog de seguridad de AWS

- Cómo acceder a la AWS Management Console con AWS Managed Microsoft AD y las credenciales en las instalaciones

Habilitación del acceso a AWS Management Console

De forma predeterminada, el acceso a la consola no está habilitado para ningún directorio. Para que los grupos y usuarios de su directorio puedan tener acceso a la consola, siga estos pasos:

Para habilitar el acceso a la consola

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. En la sección de la AWS Management Console, elija Habilitar. El acceso a la consola estará habilitado para su directorio.

   Para que los usuarios puedan iniciar sesión en la consola con su URL de acceso, primero debe agregar sus usuarios al rol. Para obtener más información general sobre la asignación de usuarios a roles de IAM, consulte Asignación de usuarios o grupos a una función existente. Una vez asignados los roles de IAM, los usuarios pueden obtener acceso a la consola con su URL de acceso. Por ejemplo, si su URL de acceso al directorio es example-corp.awsapps.com, la URL para obtener acceso a la consola es https://example-corp.awsapps.com/console/.

Deshabilitación del acceso a la AWS Management Console

Para deshabilitar el acceso de los grupos y usuarios de su directorio a la consola, siga estos pasos:

Para deshabilitar el acceso a la consola

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. En la sección de la AWS Management Console, elija Deshabilitar. El acceso a la consola estará deshabilitado para su directorio.
5. Si los roles de IAM se han asignado a usuarios o grupos del directorio, el botón Deshabilitar no estará disponible. En este caso, debe quitar todas las asignaciones del rol de IAM para el directorio antes de continuar, incluidas las asignaciones para los usuarios o grupos del directorio que se han eliminado, que aparecerán como Usuario eliminado o Grupo eliminado.

   Una vez eliminadas todas las asignaciones de rol de IAM, repita los pasos anteriores.

Establecimiento de la duración del inicio de sesión

De forma predeterminada, el tiempo que transcurre desde que los usuarios inician sesión en la consola hasta que se cierra la sesión es de una hora. Al cabo de esa hora, los usuarios deben volver a iniciar sesión, con lo que comienza la siguiente sesión de una hora de duración hasta que se cierre la sesión. Puede utilizar este procedimiento para ampliar el período de tiempo hasta un máximo de 12 horas por sesión.

Para establecer la duración del inicio de sesión

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios).
2. En la página Directories (Directorios), elija el ID del directorio.
3. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
4. En la sección Aplicaciones y servicios de AWS, elija Consola de administración de AWS.
5. En el cuadro de diálogo Administrar el acceso a los recursos de AWS, elija Continuar.
6. En la página Assign users and groups to IAM roles, en Set login session length, edite el valor numerado y luego elija Save.

Tutorial: Crear un Simple AD Active Directory

El siguiente tutorial le guía a través de todos los pasos necesarios para configurar un Active Directory Simple AD. Su objetivo es que pueda empezar a utilizar Simple AD de Active Directory forma rápida y sencilla, pero no está pensado para utilizarse en un entorno de producción a gran escala.

Requisitos previos del tutorial

Este tutorial se basa en los siguientes supuestos:

- Tienes un activo Cuenta de AWS.
- Tu cuenta no ha alcanzado el límite de Amazon VPC para la región en la que quieres usar Simple AD. Para obtener más información sobre la VPC, consulte ¿Qué es Amazon VPC? y las subredes de su VPC en la Guía del usuario de Amazon VPC.
- No tiene una VPC existente en la región con un CIDR de. `10.0.0.0/16`

Para obtener más información, consulte Requisitos previos para Simple AD.

Paso 1: Cree y configure su Amazon VPC para Simple AD Active Directory

Cree y configure una Amazon VPC para usarla con Simple AD. Antes de comenzar este procedimiento, asegúrese de haber completado los Requisitos previos del tutorial.

Cree una VPC para su Simple AD Active Directory

Cree una VPC con dos subredes públicas. AWS Directory Service requiere dos subredes en la VPC y cada subred debe estar en una zona de disponibilidad diferente.

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de VPC, elija Crear VPC.
3. En Configuración de VPC, seleccione VPC y más.
4. Complete los campos como se indica a continuación:
   - Mantenga seleccionada la opción Generado automáticamente en Generación automática de etiquetas de nombre. Cambie un proyecto a `ADS VPC`.
   - El bloque CIDR de IPv4 debería ser `10.0.0.0/16`.
   - Mantenga seleccionada la opción No hay bloque CIDR de IPv6.
   - La opción Tenencia debe permanecer en Valor predeterminado.
   - Seleccione 2 en Número de zonas de disponibilidad (AZ).
   - Seleccione 2 en Número de subredes públicas. El número de subredes privadas se puede cambiar a 0.
   - Elija Personalizar los bloques CIDR de la subred para configurar el rango de direcciones IP de la subred pública. Los bloques CIDR de la subred pública deben ser `10.0.0.0/20` y `10.0.16.0/20`.
5. Seleccione Crear VPC. La creación de la VPC puede tardar varios minutos.

Paso 2: Cree su Active Directory Simple AD

Para crear un nuevo Active Directory Simple AD, lleve a cabo los siguientes pasos. Antes de iniciar este procedimiento, asegúrese de haber completado los requisitos previos identificados en Requisitos previos del tutorial el paso 1: Crear y configurar su Amazon VPC para Simple AD. Active Directory

Para crear un Active Directory de AD simple

1. En el panel de navegación de la consola de AWS Directory Service, elija Directorios y, a continuación, elija Configurar directorio.
2. En la página Seleccionar tipo de directorio, elija Simple AD y, a continuación, elija Siguiente.
3. En la página Enter directory information (Especifique la información del directorio), facilite la siguiente información:

   Tamaño del directorio

   Elija entre la opción de tamaño Small (Pequeño) o Large (Grande). Para obtener más información acerca de los tamaños, consulte AD sencillo.

   Nombre de organización

   Un nombre de organización único para su directorio que se utilizará para registrar los dispositivos cliente.

   Este campo solo está disponible si está creando el directorio como parte del lanzamiento WorkSpaces.

   Nombre de DNS del directorio

   El nombre completo del directorio, como por ejemplo `corp.example.com`.

   Nombre NetBIOS del directorio

   El nombre abreviado del directorio, como `CORP`.

   Administrator password

   Contraseña del administrador del directorio. Al crear el directorio, se crea también una cuenta de administrador con el nombre de usuario `Administrator` y esta contraseña.

   La contraseña del administrador del directorio distingue entre mayúsculas y minúsculas y debe tener 8 caracteres como mínimo y 64 como máximo. También debe contener al menos un carácter de tres de las siguientes categorías:

   - Letras minúsculas (a-z)
   - Letras mayúsculas (A-Z)
   - Números (0-9)
   - Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmar contraseña

Vuelva a escribir la contraseña de administrador.

Descripción del directorio

Descripción opcional del directorio.

4. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la siguiente información y, a continuación, elija Next (Siguiente).

   VPC

   VPC del directorio.

   Subredes

   Elija las subredes de los controladores de dominio. Las dos subredes deben estar en diferentes zonas de disponibilidad.

5. En la página Review & create (Revisar y crear), revise la información del directorio y haga los cambios que sean necesarios. Cuando la información sea correcta, seleccione Create directory (Crear directorio). La creación del directorio tarda varios minutos. Una vez creado, el valor Status cambia a Active.

Prácticas recomendadas para Simple AD

Estas son algunas sugerencias y pautas que debe tener en cuenta para evitar problemas y aprovechar al máximo Simple AD.

Configuración: requisitos previos

Plantéese estas directrices antes de crear el directorio.

Compruebe que tena el tipo de directorio correcto

AWS Directory Service proporciona varias formas de usarlo Microsoft Active Directory con otros AWS servicios. Puede elegir el servicio de directorio con las características que necesita con un costo que se adapte a su presupuesto:

- AWS Directory Service para Microsoft Active Directory es un servicio gestionado y Microsoft Active Directory alojado en la AWS nube con muchas funciones. AWS Microsoft AD administrado es la

mejor opción si tiene más de 5000 usuarios y necesita establecer una relación de confianza entre un directorio AWS hospedado y sus directorios locales.

- AD Connector simplemente conecta su entorno local existente Active Directory a AWS. Conector AD es la mejor opción si desea utilizar su directorio en las instalaciones con los servicios de AWS .
- Simple AD es un directorio de bajo coste y escala con Active Directory compatibilidad básica. Admite 5000 usuarios o menos, aplicaciones compatibles con Samba 4 y compatibilidad LDAP para aplicaciones compatibles con LDAP.

Para obtener una comparación más detallada de AWS Directory Service las opciones, consulte¿Cuál debe elegir?.

Asegúrese de que sus VPC y sus instancias se hayan configurado correctamente

Para gestionar y utilizar sus directorios, así como conectarse a ellos, debe configurar correctamente las VPC a las que están asociados los directorios. Consulte AWS Requisitos previos de Microsoft AD gestionado, Requisitos previos de Conector AD o Requisitos previos para Simple AD para obtener información sobre la seguridad de VPC y los requisitos de red.

Si está añadiendo una instancia a su dominio, asegúrese de que dispone de conectividad y acceso remoto a la instancia, tal y como se describe en Unir una instancia de Amazon EC2 a su AWS Microsoft AD gestionado Active Directory.

Sea consciente de sus límites

Obtenga información sobre los distintos límites de su tipo de directorio específico. El almacenamiento disponible y el tamaño total de los objetos son las únicas limitaciones en cuanto al número de objetos que puede almacenar en el directorio. Consulte cualquiera de las opciones AWS Cuotas administradas de Microsoft AD, Cuotas de Conector AD o Cuotas de Simple AD para obtener más información sobre el directorio que ha elegido.

Comprenda la configuración y el uso de los grupos de AWS seguridad de su directorio

AWS crea un grupo de seguridad y lo adjunta a las interfaces de red elásticas del controlador de dominio de su directorio. AWS configura el grupo de seguridad para bloquear el tráfico innecesario al directorio y permite el tráfico necesario.

Modificación del grupo de seguridad del directorio

Si desea modificar la seguridad de los grupos de seguridad de sus directorios, puede hacerlo. Realice esos cambios únicamente si comprende completamente cómo funcionan los filtros de los grupos de seguridad. Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias de Linux en la Guía del usuario de Amazon EC2. Los cambios incorrectos pueden provocar la pérdida de comunicaciones con los equipos e instancias previstos. AWS recomienda que no intente abrir puertos adicionales al directorio, ya que esto reduce la seguridad del directorio. Lea detenidamente el Modelo de responsabilidad compartida de AWS.

> **Warning**
>
> Técnicamente, puede asociar el grupo de seguridad del directorio a otras instancias EC2 que cree. Sin embargo, no AWS recomienda esta práctica. AWS puede tener motivos para modificar el grupo de seguridad sin previo aviso para satisfacer las necesidades funcionales o de seguridad del directorio gestionado. Estos cambios afectan a cualquier instancia a la que asocie el grupo de seguridad del directorio y puede interrumpir el funcionamiento de las instancias asociadas. Además, al asociar el grupo de seguridad del directorio a las instancias EC2 se puede crear un posible riesgo de seguridad para las instancias EC2.

Utilice Microsoft AD AWS administrado si se requieren confianzas

Simple AD no admite relaciones de confianza. Si necesita establecer una relación de confianza entre su AWS Directory Service directorio y otro directorio, debe usar AWS Directory Service para Microsoft Active Directory.

Configuración: creación del directorio

A continuación se indican algunas sugerencias que debe tener en cuenta en el momento de crear su directorio.

Recuerde su ID de administrador y su contraseña

Cuando se configura el directorio, se proporciona la contraseña de la cuenta de administrador. El ID de esa cuenta es Administrador para Simple AD. Recuerde la contraseña que cree para esta cuenta; de lo contrario, no podrá añadir objetos a su directorio.

Comprenda las restricciones de nombre de usuario para AWS las aplicaciones

AWS Directory Service proporciona compatibilidad con la mayoría de los formatos de caracteres que se pueden utilizar en la construcción de nombres de usuario. Sin embargo, hay restricciones de caracteres que se aplican a los nombres de usuario que se utilizarán para iniciar sesión en AWS aplicaciones, como WorkSpaces Amazon WorkMail, WorkDocs Amazon o Amazon. QuickSight Estas restricciones requieren que no se utilicen los siguientes caracteres:

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

> **Note**
>
> El símbolo @ se permite siempre que preceda a un sufijo UPN.

Programación de las aplicaciones

Antes de programar sus aplicaciones, tenga en cuenta lo siguiente:

Utilice el servicio de localización de DC de Windows

Al desarrollar aplicaciones, utilice el servicio de localización de Windows DC o el servicio DNS dinámico (DDNS) de su AWS Microsoft AD administrado para localizar los controladores de dominio (DC). No incluya la dirección de un DC en el código de las aplicaciones. El servicio de localización de DC ayuda a garantizar la distribución de la carga de directorios y le permite aprovechar el escalado horizontal añadiendo controladores de dominio a su implementación. Si vincula la aplicación a un DC fijo y se somete a una operación de aplicación de parches o de recuperación a dicho DC, la aplicación perderá el acceso al DC en lugar de utilizar uno de los DC restantes. Además, la inclusión de un DC en el código de la aplicación puede provocar que dicho DC se sobrecargue. En casos graves, esto puede hacer que el DC deje de responder. En estos casos, la automatización de AWS directorios también puede marcar el directorio como dañado y desencadenar procesos de recuperación que sustituyan al DC que no responde.

Pruebas de carga antes de la puesta en producción

Asegúrese de hacer pruebas de laboratorio con objetos y solicitudes que sean representativos de su carga de trabajo de producción para confirmar que el directorio puede adaptarse a la carga de su aplicación. Si necesita capacidad adicional, debe utilizarla AWS Directory Service para Microsoft Active Directory, que le permite agregar controladores de dominio para obtener un alto rendimiento. Para obtener más información, consulte Implementación de controladores de dominio adicionales.

Uso de consultas LDAP eficientes

Las consultas amplias de LDAP a un controlador de dominio con miles de objetos pueden consumir un número importante de ciclos de CPU en un único DC, lo que se traduce en una sobrecarga. Esto podría afectar a las aplicaciones que comparten el mismo DC durante la consulta.

Cuotas de Simple AD

Por lo general, no debe agregar más de 500 usuarios a un directorio de Simple AD pequeño y no más de 5000 usuarios a un directorio de Simple AD grande. Para obtener opciones de escalado más flexibles y características de Active Directory adicionales, considere la posibilidad de utilizar AWS Directory Service para Microsoft Active Directory (Standard Edition o Enterprise Edition).

A continuación se indican los límites predeterminados para Simple AD. A menos que se indique lo contrario, cada cuota es por cada región.

Cuotas de Simple AD

Recurso	Cuota predeterminada
Directorios de Simple AD	10
Instantáneas manuales *	5 por Simple AD

*La cuota de instantáneas manuales no se puede cambiar.

> **Note**
>
> No puede asociar una dirección IP pública a su interfaz de red elástica de AWS.

Política de compatibilidad de las aplicaciones para Simple AD

Simple AD es una implementación de Samba que proporciona muchas de las características básicas de Active Directory. Debido a la enorme cantidad de aplicaciones personalizadas y disponibles en el mercado que utilizan Active Directory, AWS no lleva a cabo ni puede llevar a cabo una verificación formal ni amplia de la compatibilidad de las aplicaciones de terceros con Simple AD. Aunque AWS trabaja con los clientes para intentar superar cualquier posible desafío que puedan encontrar durante la instalación de las aplicaciones, no podemos garantizar que ninguna aplicación sea ni continúe siendo compatible con Simple AD.

Las siguientes aplicaciones de terceros son compatibles con Simple AD:

- Microsoft Internet Information Services (IIS) en las siguientes 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 (ediciones Express, Web y Standard)
  - SQL Server 2008 R2 (ediciones Express, Web y Standard)
  - SQL Server 2012 (ediciones Express, Web y Standard)
  - SQL Server 2014 (ediciones Express, Web y Standard)
- Microsoft SharePoint:
  - SharePoint 2010 Foundation
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

Los clientes pueden optar por utilizar AWS Directory Service para Microsoft Active Directory (AWS Microsoft AD gestionado) para conseguir un nivel de compatibilidad más alto basado en el directorio de Active Directory real.

Solución de problemas de Simple AD

La siguiente información puede ayudarle a solucionar algunos problemas comunes que podría encontrar a la hora de crear o utilizar el directorio.

Temas

Recuperación de contraseña

Si un usuario olvida una contraseña o tiene problemas para iniciar sesión en el directorio Simple AD o AWS Managed Microsoft AD, puede restablecer su contraseña mediante el AWS Management Console, Windows PowerShell o el AWS CLI.

Para obtener más información, consulte Restablecer una contraseña de usuario de Simple AD.

Aparece el mensaje “KDC no puede llevar a cabo la operación solicitada” al agregar un usuario a Simple AD

Esto puede ocurrir cuando el cliente de la CLI de Samba no envía correctamente los comandos “net” a todos los controladores de dominio. Si ve este mensaje de error al utilizar el comando “net ads” para añadir un usuario al directorio de Simple AD, utilice el argumento -S y especifique la dirección IP de uno de los controladores de dominio. Si sigue apareciendo el error, pruebe con el otro controlador de dominio. También puede utilizar las herramientas de administración de Active Directory para añadir usuarios al directorio. Para obtener más información, consulte Instale las herramientas de administración de Active Directory para Simple AD.

No puedo actualizar el nombre de DNS o la dirección IP de una instancia unida a mi dominio (actualización dinámica de DNS)

Las actualizaciones dinámicas de DNS no se admiten en dominios de Simple AD. En lugar de ello, puede realizar los cambios directamente en su directorio utilizando el Administrador de DNS en una instancia que esté unida al dominio.

No puedo iniciar sesión en SQL Server con una cuenta de SQL Server

Podría recibir un mensaje de error si intenta utilizar SQL Server Management Studio (SSMS) con una cuenta de SQL Server para iniciar sesión en SQL Server que se ejecuta en una instancia de EC2 de Windows 2012 R2. El problema se produce cuando SSMS se ejecuta como dominio de usuario y puede dar lugar al error “Error de inicio de sesión para el usuario”, incluso aunque se hayan facilitado credenciales válidas. Se trata de un problema conocido y AWS estamos trabajando activamente para resolverlo.

Para solucionar el problema, puede iniciar sesión en SQL Server con la autenticación de Windows en lugar de con la autenticación de SQL. O lanzar SSMS como un usuario local en lugar de un usuario de dominio de Simple AD.

Mi directorio se bloquea en el estado “Solicitado”

Si tiene un directorio que haya estado en estado “Solicitado” durante más de cinco minutos, pruebe a eliminar el directorio y vuelva a crearlo. Si este problema sigue sin resolverse, contacte con el Centro de AWS Support.

He recibido un error “AZ limitada” a la hora de crear un directorio

Es posible que algunas AWS cuentas creadas antes de 2012 tengan acceso a zonas de disponibilidad en las regiones EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Norte de California) o Asia Pacífico (Tokio) que no admiten AWS Directory Service directorios. Si recibe un error como este al crear un directorio, seleccione una subred en una zona de disponibilidad diferente e intente crear el directorio de nuevo.

Algunos de mis usuarios no pueden autenticarse con mi directorio

Las cuentas de usuario deben tener habilitada la autenticación previa de Kerberos. Esta es la configuración predeterminada para nuevas cuentas de usuario y no debe modificarse. Para obtener más información acerca de esta configuración, consulta Autenticación previa en Microsoft TechNet.

Recursos adicionales de

Los siguientes recursos pueden ayudarle a solucionar problemas mientras trabaja con ellos. AWS

- AWS Centro de conocimiento: encuentre preguntas frecuentes y enlaces a otros recursos que le ayudarán a solucionar problemas.
- AWS Support Center: obtenga asistencia técnica.
- AWS Centro de soporte premium: obtenga soporte técnico premium.

Temas

Motivos de los estados del directorio de Simple AD

Si un directorio se ha deteriorado o ha dejado de funcionar, el mensaje de estado del directorio contendrá información adicional. El mensaje de estado se muestra en la consola de AWS Directory Service o lo devuelve en el miembro `DirectoryDescription.StageReason` la API `DescribeDirectories`. Para obtener más información sobre el estado del directorio, consulte Descripción del estado del directorio.

Estos son los mensajes de estado de un directorio de Simple AD:

Temas

La interfaz de red elástica del servicio de directorio no está conectada

Descripción

La interfaz de red elástica (ENI) crítica que se creó en su nombre durante la creación del directorio para establecer la conectividad de red con la VPC no está conectada a la instancia del directorio. Las aplicaciones de AWS respaldadas por este directorio no funcionarán. El directorio no puede conectarse a la red en las instalaciones.

Solución de problemas

Si el ENI está desconectado, pero aún existe, contacte con AWS Support. Si se elimina la ENI, no hay forma de resolver el problema y su directorio queda inutilizable permanentemente. En este caso, debe eliminar su directorio y crear uno nuevo.

Problemas detectados por instancia

Descripción

La instancia detectó un error interno. Por lo general, esto significa que el servicio de supervisión está intentando recuperar activamente las instancias dañadas.

Solución de problemas

En la mayoría de los casos, se trata de un problema transitorio y, finalmente, el directorio vuelve al estado activo. Si el problema persiste, visite AWS Support para obtener asistencia.

El usuario reservado crítico de AWS Directory Service no se encuentra en el directorio

Descripción

Cuando se crea un directorio de Simple AD, AWS Directory Service crea una cuenta de servicio en el directorio con el nombre `AWSAdmin`*`D-xxxxxxxxx`*. Este error se genera cuando no se puede encontrar esta cuenta de servicio. Sin esta cuenta, AWS Directory Service no puede realizar funciones administrativas en el directorio, dejándolo inservible.

Solución de problemas

Para solucionar este problema, restaure el directorio a una instantánea anterior que se haya creado antes de que se eliminara la cuenta de servicio. Se toman instantáneas automáticas de su directorio de Simple AD una vez al día. Si han pasado más de cinco días después de que se

eliminó esta cuenta, es posible que no pueda restaurar el directorio a un estado en el que exista esta cuenta. Si no puede restablecer el directorio a partir de una instantánea en la que exista esta cuenta, su directorio puede quedar permanentemente inservible. En este caso, debe eliminar su directorio y crear uno nuevo.

El usuario reservado crítico de AWS Directory Service debe pertenecer al grupo de administradores de dominio

Descripción

Cuando se crea un directorio de Simple AD, AWS Directory Service crea una cuenta de servicio en el directorio con el nombre `AWSAdmin`*`D-xxxxxxxxx`*. Este error se genera cuando esta cuenta de servicio no es miembro del grupo `Domain Admins`. Es necesaria la pertenencia a este grupo para conceder a AWS Directory Service los privilegios que necesita para realizar operaciones de mantenimiento y recuperación, como transferir roles FSMO, unir al dominio nuevos controladores de directorio y restaurar a partir de instantáneas.

Solución de problemas

Utilice la herramienta Usuarios y equipos de Active Directory para volver a añadir la cuenta de servicio al grupo `Domain Admins`.

El usuario reservado crítico de AWS Directory Service está deshabilitado

Descripción

Cuando se crea un directorio de Simple AD, AWS Directory Service crea una cuenta de servicio en el directorio con el nombre `AWSAdmin`*`D-xxxxxxxxx`*. Este error se genera cuando esta cuenta de servicio está deshabilitada. Esta cuenta debe estar habilitada para que AWS Directory Service pueda realizar operaciones de recuperación y mantenimiento en el directorio.

Solución de problemas

Utilice la herramienta Usuarios y equipos de Active Directory para volver a habilitar la cuenta de servicio.

El controlador de dominio principal no tiene todos los roles FSMO

Descripción

El controlador de directorio de Simple AD no posee todos los roles FSMO. AWS Directory Service no puede garantizar determinado comportamiento y funcionalidad si los roles FSMO no pertenecen al controlador de directorio de Simple AD correcto.

Solución de problemas

Utilice las herramientas de Active Directory para volver a trasladar los roles FSMO al directorio de trabajo original. Para obtener más información acerca de cómo transferir los roles FSMO, consulte https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds. Si esto no resuelve el problema, contacte con AWS Support para obtener más ayuda.

Errores de replicación del controlador de dominio

Descripción

Los controladores de directorio de Simple AD no se pueden replicar entre sí. Esto puede deberse a uno o varios de los siguientes problemas:

- Los grupos de seguridad de los controladores de directorio no tienen abiertos los puertos correctos.
- Las ACL de red son demasiado restrictivas.
- La tabla de ruteo de VPC no enruta correctamente el tráfico de red entre los controladores de directorio.
- Se ha promovido otra instancia a un controlador de dominio del directorio.

Solución de problemas

Para obtener más información acerca de los requisitos de su red de VPC, consulte AWS Requisitos previos de Microsoft AD gestionado de AWS Managed Microsoft AD, Requisitos previos de Conector AD de Conector AD o Requisitos previos para Simple AD de Simple AD. Si existe un controlador de dominio desconocido en su directorio, debe bajarlo de nivel. Si la configuración de su red de VPC es correcta, pero el error persiste, contacte con AWS Support para obtener más ayuda.

Seguridad en AWS Directory Service

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS Directory Service, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Directory Service. Los siguientes temas muestran cómo configurarlo AWS Directory Service para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Directory Service recursos.

Temas de seguridad

En esta sección se pueden encontrar los siguientes temas de seguridad:

- Administración de identidades y accesos para AWS Directory Service
- Inicio de sesión y supervisión AWS Directory Service
- Validación de conformidad para AWS Directory Service
- Resiliencia en AWS Directory Service
- Seguridad de la infraestructura en AWS Directory Service

Temas de seguridad adicionales

En esta guía se pueden encontrar los siguientes temas de seguridad adicionales:

Acceso a cuentas, fideicomisos y AWS recursos

- Permisos para la cuenta de administrador
- Cuentas de servicio administradas por grupos
- Creación de una relación de confianza
- Delegación limitada de Kerberos
- Otorgar acceso a los recursos de AWS a usuarios y grupos
- Autorización para AWS aplicaciones y servicios que utilizan AWS Directory Service

Protección del directorio

- Protección del directorio de AWS Managed Microsoft AD
- Protección del directorio de Conector AD

Registro y monitoreo

- Supervisión de su AWS Managed Microsoft AD
- Supervisión del directorio de Conector AD

Resiliencia

- Aplicación de parches y mantenimiento de AWS Managed Microsoft AD

Administración de identidades y accesos para AWS Directory Service

El acceso a AWS Directory Service requiere credenciales que AWS puede utilizar para autenticar sus solicitudes. Esas credenciales deben tener permisos para acceder a AWS los recursos, como un AWS Directory Service directorio. En las siguientes secciones se proporcionan detalles sobre cómo utilizar AWS Identity and Access Management (IAM) y cómo ayudar AWS Directory Service a proteger los recursos controlando quién puede acceder a ellos:

- Autenticación

- Control de acceso

Autenticación

Aprenda a acceder AWS mediante las identidades de IAM.

Control de acceso

Puede tener credenciales válidas para autenticar sus solicitudes, pero a menos que tenga permisos, no podrá crear recursos ni acceder a AWS Directory Service ellos. Por ejemplo, debe tener permisos para crear un AWS Directory Service directorio o crear una instantánea del directorio.

En las siguientes secciones se describe cómo administrar los permisos para AWS Directory Service. Recomendamos que lea primero la información general.

- Descripción general de la administración de los permisos de acceso a sus AWS Directory Service recursos
- Uso de políticas basadas en la identidad (políticas de IAM) para AWS Directory Service
- AWS Directory Service Permisos de API: referencia a acciones, recursos y condiciones

Descripción general de la administración de los permisos de acceso a sus AWS Directory Service recursos

Cada AWS recurso es propiedad de una AWS cuenta y los permisos para crear o acceder a los recursos se rigen por las políticas de permisos. Un administrador de cuentas puede adjuntar políticas de permisos a las identidades de IAM (es decir, usuarios, grupos y roles), y algunos servicios (por ejemplo AWS Lambda) también permiten adjuntar políticas de permisos a los recursos.

> **Note**
>
> Un administrador de cuentas (o usuario administrador) es un usuario que tiene privilegios de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Temas

- AWS Directory Service recursos y operaciones
- Titularidad de los recursos
- Administración del acceso a los recursos
- Especificación de elementos de política: acciones, efectos, recursos y entidades principales
- Especificación de las condiciones de una política

AWS Directory Service recursos y operaciones

En AWS Directory Service, el recurso principal es un directorio. AWS Directory Service también admite recursos de instantáneas de directorios. Sin embargo, puede crear instantáneas solamente en el contexto de un directorio existente. Por lo tanto, una instantánea se conoce como subrecurso.

Estos recursos tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente tabla.

Tipo de recurso	Formato de ARN
Directorio	`arn:aws:ds:` *`region`*`:`*`account-id`* `:directory/` *`external-directory-id`*
Instantánea	`arn:aws:ds:` *`region`*`:`*`account-id`* `:snapshot/` *`external-snapshot-id`*

AWS Directory Service proporciona un conjunto de operaciones para trabajar con los recursos adecuados. Para ver la lista de operaciones disponibles, consulte las acciones de Directory Service.

Titularidad de los recursos

El propietario de un recurso es la AWS cuenta que creó un recurso. Es decir, el propietario del recurso es la AWS cuenta de la entidad principal (la cuenta raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si utilizas las credenciales de la cuenta raíz de tu AWS cuenta para crear un AWS Directory Service recurso, como un directorio, tu AWS cuenta es la propietaria de ese recurso.

- Si crea un usuario de IAM en su AWS cuenta y concede permisos para crear AWS Directory Service recursos a ese usuario, el usuario también podrá crear AWS Directory Service recursos. Sin embargo, su AWS cuenta, a la que pertenece el usuario, es propietaria de los recursos.
- Si crea un rol de IAM en su AWS cuenta con permisos para crear AWS Directory Service recursos, cualquier persona que pueda asumir el rol podrá crear AWS Directory Service recursos. Tu AWS cuenta, a la que pertenece el rol, es propietaria de los AWS Directory Service recursos.

Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección se analiza el uso de la IAM en el contexto de AWS Directory Service. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte What is IAM? (¿Qué es IAM?) en la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM) y las políticas asociadas a un recurso se denominan políticas basadas en recursos. AWS Directory Service solo admite políticas basadas en la identidad (políticas de IAM).

Temas

- Políticas basadas en identidades (políticas de IAM)
- Políticas basadas en recursos

Políticas basadas en identidades (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Adjunta una política de permisos a un usuario o grupo de tu cuenta: el administrador de una cuenta puede usar una política de permisos asociada a un usuario concreto para conceder permisos a ese usuario para crear un AWS Directory Service recurso, como un directorio nuevo.

- Adjuntar una política de permisos a un rol (conceder permisos para cuentas cruzadas): puede adjuntar una política de permisos basada en identidades a un rol de IAM para conceder permisos para cuentas cruzadas.

  Para obtener más información sobre el uso de IAM para delegar permisos, consulte Access management (Administración de accesos) en la Guía del usuario de IAM.

La siguiente política de permisos concede permisos a un usuario para ejecutar todas las acciones que empiezan por `Describe`. Estas acciones muestran información sobre un AWS Directory Service recurso, como un directorio o una instantánea. Tenga en cuenta que el carácter comodín (*) del `Resource` elemento indica que las acciones están permitidas en todos los AWS Directory Service recursos que son propiedad de la cuenta.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Para obtener más información sobre el uso de políticas basadas en la identidad con AWS Directory Service, consulte. Uso de políticas basadas en la identidad (políticas de IAM) para AWS Directory Service Para obtener más información acerca de los usuarios, los grupos, los roles y los permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede adjuntar una política a un bucket de S3 para administrar los permisos de acceso a ese bucket. AWS Directory Service no admite políticas basadas en recursos.

Especificación de elementos de política: acciones, efectos, recursos y entidades principales

Para cada AWS Directory Service recurso, el servicio define un conjunto de operaciones de API. Para obtener más información, consulte AWS Directory Service recursos y operaciones. Para ver la lista de operaciones de API disponibles, consulte las acciones de Directory Service.

Para conceder permisos para estas operaciones de API, AWS Directory Service define un conjunto de acciones que puede especificar en una política. Tenga en cuenta que la realización de una operación de la API puede requerir permisos para más de una acción.

A continuación, se indican los elementos básicos de la política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. En el AWS Directory Service caso de los recursos, siempre se utiliza el carácter comodín (*) en las políticas de IAM. Para obtener más información, consulte AWS Directory Service recursos y operaciones.
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, el permiso `ds:DescribeDirectories` concede permiso a los usuarios para realizar la operación AWS Directory Service `DescribeDirectories`.
- Efecto: solo debe especificar el efecto cuando el usuario solicita la acción específica. La acción se puede permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. En el caso de las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad para la que desea recibir los permisos (solo se aplica a las políticas basadas en recursos). AWS Directory Service no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Para ver una tabla que muestra todas las acciones de la AWS Directory Service API y los recursos a los que se aplican, consulte. AWS Directory Service Permisos de API: referencia a acciones, recursos y condiciones

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de acceso para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para AWS Directory Service. Sin embargo, hay claves de AWS condición que puede usar según corresponda. Para obtener una lista completa de AWS las claves, consulte las claves de condición globales disponibles en la Guía del usuario de IAM.

Uso de políticas basadas en la identidad (políticas de IAM) para AWS Directory Service

Este tema contiene ejemplos de políticas basadas en identidades, donde los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, a usuarios, grupos y funciones).

> **Important**
>
> Le recomendamos que consulte primero los temas introductorios en los que se explican los conceptos básicos y las opciones disponibles para gestionar el acceso a sus recursos. AWS Directory Service Para obtener más información, consulte Descripción general de la administración de los permisos de acceso a sus AWS Directory Service recursos.

En las secciones de este tema se explica lo siguiente:

- Permisos necesarios para usar la AWS Directory Service consola
- AWS políticas administradas (predefinidas) para AWS Directory Service
- Ejemplos de políticas administradas por el cliente
- Uso de etiquetas con políticas de IAM

A continuación se muestra un ejemplo de una política de permisos.

```
{
```

```
    "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"
                 }
             }
         }
     ]
```

```
}
```

La política incluye lo siguiente:

- La primera declaración otorga permiso para crear un AWS Directory Service directorio. AWS Directory Service no admite permisos para esta acción en particular a nivel de recursos. Por lo tanto, la política especifica un comodín (*) como valor de `Resource` .
- La segunda instrucción concede permisos para determinadas acciones de IAM. El acceso a las acciones de IAM es necesario para AWS Directory Service poder leer y crear funciones de IAM en tu nombre. El carácter comodín (*) que aparece al final del valor `Resource` significa que la declaración concede permiso para la acción de IAM en cualquier rol de IAM. Para limitar este permiso a un rol específico, sustituya el carácter comodín (*) en el ARN del recurso por el nombre de rol específico. Para obtener más información, consulte la sección Acciones de IAM.
- La tercera declaración concede permisos a un conjunto específico de recursos de Amazon EC2 que son necesarios AWS Directory Service para permitir la creación, configuración y destrucción de sus directorios. El carácter comodín (*) al final del valor `Resource` significa que la instrucción concede permiso para las acciones de EC2 en cualquier recurso o subrecurso de EC2. Para limitar este permiso a un rol específico, sustituya el carácter comodín (*) en el ARN del recurso por el recurso o subrecurso específico. Para obtener más información, consulte Acciones de Amazon EC2.

La política no especifica el elemento `Principal`, ya que en una política basada en la identidad no se especifica el elemento principal que obtiene el permiso. Al asociar una política a un usuario, el usuario es la entidad principal implícita. Cuando se asocia una política de permisos a un rol de IAM, la entidad principal identificada en la política de confianza del rol obtiene los permisos.

Para ver una tabla que muestra todas las acciones de la AWS Directory Service API y los recursos a los que se aplican, consulteAWS Directory Service Permisos de API: referencia a acciones, recursos y condiciones.

Permisos necesarios para usar la AWS Directory Service consola

Para que un usuario pueda trabajar con la AWS Directory Service consola, debe tener los permisos enumerados en la política anterior o los permisos otorgados por la función de acceso total de Directory Service o la función de solo lectura de Directory Service, que se describen enAWS políticas administradas (predefinidas) para AWS Directory Service.

Si crea una política de IAM que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para los usuarios con esa política de IAM.

AWS políticas administradas (predefinidas) para AWS Directory Service

AWS aborda muchos casos de uso comunes al proporcionar políticas de IAM independientes que son creadas y administradas por. AWS Las políticas administradas conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Las siguientes políticas AWS gestionadas, que puede adjuntar a los usuarios de su cuenta, son específicas de: AWS Directory Service

- AWSDirectoryServiceReadOnlyAccess— Otorga a un usuario o grupo acceso de solo lectura a todos los AWS Directory Service recursos, las subredes de EC2, las interfaces de red de EC2 y los temas y suscripciones de Amazon Simple Notification Service (Amazon SNS) de la cuenta raíz. AWS Para obtener más información, consulte Uso de políticas administradas de AWS con AWS Directory Service.
- AWSDirectoryServiceFullAccess: otorga a un usuario o grupo lo siguiente:
  - Acceso completo a AWS Directory Service
  - Acceso a los principales servicios de Amazon EC2 necesarios para su uso AWS Directory Service
  - Posibilidad de enumerar los temas de Amazon SNS
  - Posibilidad de crear, gestionar y eliminar temas de Amazon SNS cuyo nombre comience por «» DirectoryMonitoring

  Para obtener más información, consulte Uso de políticas administradas de AWS con AWS Directory Service.

Además, hay otras políticas AWS gestionadas que son adecuadas para su uso con otras funciones de IAM. Estas políticas se asignan a las funciones asociadas a los usuarios de su AWS Directory Service directorio. Estas políticas son necesarias para que esos usuarios tengan acceso a otros AWS recursos, como Amazon EC2. Para obtener más información, consulte Otorgar acceso a los recursos de AWS a usuarios y grupos.

También puede crear políticas de IAM personalizadas que permitan a los usuarios acceder a las acciones y recursos de la API de necesarios. Puede asociar estas políticas personalizadas a los grupos o usuarios de IAM que requieran esos permisos.

Ejemplos de políticas administradas por el cliente

En esta sección, puede encontrar ejemplos de políticas de usuario que otorgan permisos para diversas AWS Directory Service acciones.

> **Note**
>
> Todos los ejemplos utilizan la región Oeste de EE. UU. (Oregón) (`us-west-2`) y contienen identificadores de cuenta ficticios.

Ejemplos

- Ejemplo 1: permitir que un usuario realice cualquier acción de descripción en cualquier AWS Directory Service recurso
- Ejemplo 2: permitir a un usuario crear un directorio

Ejemplo 1: permitir que un usuario realice cualquier acción de descripción en cualquier AWS Directory Service recurso

La siguiente política de permisos concede permisos a un usuario para ejecutar todas las acciones que empiezan por `Describe`. Estas acciones muestran información sobre un AWS Directory Service recurso, como un directorio o una instantánea. Tenga en cuenta que el carácter comodín (*) del `Resource` elemento indica que las acciones están permitidas en todos los AWS Directory Service recursos que son propiedad de la cuenta.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
```

```
}
```

Ejemplo 2: permitir a un usuario crear un directorio

La siguiente política de permisos otorga permisos para permitir a un usuario crear un directorio y todos los demás recursos relacionados, como tales instantáneas y confianzas. Para ello, también se requieren permisos para determinados servicios de Amazon EC2.

```
{
   "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":"*"
         ]
      }
   ]
}
```

Uso de etiquetas con políticas de IAM

Puedes aplicar permisos a nivel de recursos basados en etiquetas en las políticas de IAM que utilices para la mayoría de las acciones de la API. AWS Directory Service Esto le ofrece un mejor control sobre los recursos que un usuario puede crear, modificar o utilizar. Puede utilizar el elemento `Condition` (también llamado bloque `Condition`) junto con las siguientes claves contextuales de condición y valores en una política de IAM para controlar el acceso del usuario (permiso) en función de las etiquetas de un usuario:

- Utilice `aws:ResourceTag/`**`tag-key`**: **`tag-value`** para permitir o denegar acciones de usuario en recursos con etiquetas específicas.
- Utilice `aws:ResourceTag/`**`tag-key`**: **`tag-value`** para exigir (o impedir) el uso de una etiqueta específica al realizar una solicitud de API para crear o modificar un recurso que permita etiquetas.
- Utilice `aws:TagKeys`: [**`tag-key`**, ...] para exigir (o impedir) el uso de un conjunto de claves de etiquetas al realizar una solicitud de API para crear o modificar un recurso que permita etiquetas.

> **Note**
>
> Las claves contextuales de condición y los valores de una política de IAM se aplican únicamente a las acciones de AWS Directory Service en las que un identificador de un recurso que se puede etiquetar es un parámetro obligatorio.

Controlar el acceso mediante etiquetas en la Guía de usuario de IAM incluye información adicional sobre el uso de etiquetas. La sección de referencia de políticas JSON de IAM de esta guía incluye sintaxis, descripciones y ejemplos detallados de los elementos, variables y lógica de evaluación de las políticas JSON de IAM.

El siguiente ejemplo de política de etiquetas permite todas las llamadas `ds` siempre que contenga la etiqueta clave/par “`fooKey`”:”`fooValue`”.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
```

```
            "Effect":"Allow",
            "Action":[
               "ec2:*"
            ],
            "Resource":"*"
         }
      ]
   }
```

En el siguiente ejemplo de política de recursos permite todas las llamadas de `ds` siempre que el recurso contenga el ID de directorio “`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 obtener más información sobre los ARN, consulte Nombres de recursos (ARN) y espacios de nombres de AWS servicios de Amazon.

La siguiente lista de operaciones de AWS Directory Service API admite permisos a nivel de recursos basados en etiquetas:

- 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 Permisos de API: referencia a acciones, recursos y condiciones

Puede usar la tabla AWS Directory Service Permisos de API: referencia a acciones, recursos y condiciones como referencia cuando configure Control de acceso y escriba políticas de permisos que vaya a asociar a una identidad de IAM (políticas basadas en identidad). Cada entrada de la API de la incluye lo siguiente:

- Nombre de la operación de la AWS Directory Service API
- Las acciones correspondientes para las que puede conceder permisos para realizar la acción
- El AWS recurso para el que puedes conceder los permisos

Las acciones se especifican en el campo `Action` de la política y el valor del recurso se especifica en el campo `Resource` de la política. Para especificar una acción, use el prefijo `ds:` seguido del nombre de operación de la API (por ejemplo, `ds:CreateDirectory`). Es posible que algunas AWS aplicaciones requieran el uso de operaciones de AWS Directory Service API no públicas `ds:AuthorizeApplicationds:CheckAlias`, como`ds:CreateIdentityPoolDirectory`,`ds:GetAuthorizedApplicationDetails`,`ds:UpdateAu` y `ds:UnauthorizeApplication` en sus políticas.

Algunas AWS Directory Service API solo se pueden llamar a través de AWS Management Console. No son API públicas, en el sentido de que no se pueden llamar mediante programación y ningún SDK las proporciona. Aceptan credenciales de usuario. Estas operaciones de API incluyen `ds:DisableRoleAccessds:EnableRoleAccess`, `yds:UpdateDirectory`.

Puedes usar claves de condición AWS globales en tus AWS Directory Service políticas para expresar las condiciones. Para obtener una lista completa de AWS las claves, consulte las claves de condición globales disponibles en la Guía del usuario de IAM.

Temas relacionados

- Control de acceso

Autorización para AWS aplicaciones y servicios que utilizan AWS Directory Service

Autorizar una AWS aplicación en un Active Directory

AWS Directory Service concede permisos específicos para que las aplicaciones seleccionadas se integren sin problemas con su Active Directory al autorizar una AWS aplicación. AWS a las aplicaciones solo se les concede el acceso necesario para su caso de uso. A continuación se detalla el conjunto de permisos internos que se conceden a las aplicaciones y a los administradores de aplicaciones tras la autorización:

> **Note**
>
> El `ds:AuthorizationApplication` permiso es necesario para autorizar una nueva AWS aplicación en Active Directory. Los permisos para esta acción solo se deben proporcionar a los administradores que configuran las integraciones con Directory Service.

- Acceso de lectura a los datos de usuarios, grupos, unidades organizativas, ordenadores o entidades de certificación de Active Directory en todas las unidades organizativas (OU) de los directorios AWS gestionados de Microsoft AD, Simple AD y AD Connector, así como en los dominios de confianza de Microsoft AD AWS gestionado, si lo permite una relación de confianza.
- Escriba el acceso a los datos de usuarios, grupos, miembros de grupos, ordenadores o entidades de certificación en su unidad organizativa de AWS Managed Microsoft AD. Acceso por escrito a todas las unidades organizativas de Simple AD.

- Autenticación y administración de sesiones de los usuarios de Active Directory para todos los tipos de directorios.

Algunas aplicaciones AWS gestionadas de Microsoft AD, como Amazon RDS y Amazon FSx, se integran mediante una conexión de red directa a su Active Directory. En este caso, las interacciones de los directorios utilizan protocolos nativos de Active Directory, como LDAP y Kerberos. Los permisos de estas AWS aplicaciones se controlan mediante una cuenta de usuario del directorio creada en la unidad organizativa AWS reservada (OU) durante la autorización de la aplicación, que incluye la administración del DNS y el acceso total a una OU personalizada creada para la aplicación. Para poder utilizar esta cuenta, la aplicación necesita permisos para la acción `ds:GetAuthorizedApplicationDetails` mediante las credenciales de la persona que llama o un rol de IAM.

Para obtener más información sobre los permisos de la AWS Directory Service API, consulteAWS Directory Service Permisos de API: referencia a acciones, recursos y condiciones.

Para obtener más información sobre cómo habilitar AWS aplicaciones y servicios para Microsoft AD AWS administrado, consulteHabilite el acceso a AWS aplicaciones y servicios. Para obtener más información sobre cómo habilitar AWS aplicaciones y servicios para AD Connector, consulteHabilite el acceso a AWS aplicaciones y servicios. Para obtener más información sobre cómo habilitar AWS aplicaciones y servicios para Simple AD, consulteHabilite el acceso a AWS aplicaciones y servicios.

Desautorizar una AWS aplicación en un Active Directory

Para eliminar los permisos de acceso de una AWS aplicación a Active Directory, se requiere el `ds:UnauthorizedApplication` permiso. Siga los pasos que se indican en la aplicación para deshabilitarla.

Inicio de sesión y supervisión AWS Directory Service

Como práctica recomendada, debe supervisar su organización para asegurarse de que los cambios queden registrados. Esto le ayuda a garantizar que se pueda investigar cualquier cambio inesperado y revertir los cambios no deseados. AWS Directory Service actualmente es compatible con los dos AWS servicios siguientes para que pueda supervisar su organización y la actividad que se lleva a cabo en ella.

- Amazon CloudWatch : puedes usar CloudWatch Events con el tipo de directorio AWS administrado de Microsoft AD. Para obtener más información, consulte Habilitación del reenvío de registros.

Además, puedes usar CloudWatch Metrics para monitorear el rendimiento del controlador de dominio. Para obtener más información, consulte Determine cuándo agregar controladores de dominio con CloudWatch métricas.

- AWS CloudTrail - Se puede utilizar CloudTrail con todos los tipos de AWS Directory Service directorios. Para obtener más información, consulta Registrar llamadas a la AWS Directory Service API con CloudTrail.

Validación de conformidad para AWS Directory Service

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar

la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Directory Service

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la infraestructura global.AWS

Además de la infraestructura AWS global, AWS Directory Service ofrece la posibilidad de tomar instantáneas manuales de los datos en cualquier momento para respaldar sus necesidades de respaldo y resiliencia de los datos. Para obtener más información, consulte Creación de una instantánea o restauración del directorio.

Seguridad de la infraestructura en AWS Directory Service

Como servicio gestionado, AWS Directory Service está protegido por los procedimientos de seguridad de la red AWS global que se describen en el documento técnico Amazon Web Services: descripción general de los procesos de seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Directory Service través de la red. Los clientes deben admitir Transport Layer Security (TLS). Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que AWS Directory Service for Microsoft Active Directory otorga a otro servicio al recurso. Si el valor

de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos. Si utiliza claves de contexto de condición global y el valor de `aws:SourceArn` contiene el ID de cuenta, el valor de `aws:SourceAccount` y la cuenta en el valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utiliza en la misma instrucción de política. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

En el siguiente ejemplo, el valor de `aws:SourceArn` debe ser un grupo de CloudWatch registros.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con comodines (`*`) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:servicename:*:123456789012:*`.

El siguiente ejemplo muestra cómo se pueden utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves de contexto de AWS Managed Microsoft AD para evitar el confuso problema de los adjuntos.

```
{
  "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"
      }
    }
  }
}
```

En el siguiente ejemplo, el valor de `aws:SourceArn` debe ser un tema de SNS en la cuenta. Por ejemplo, puedes usar algo como «ap-southeast-1» es tu región, «123456789012" es tu identificador de cliente yDirectoryMonitoring" _d-966739499f» es el nombre del tema de Amazon SNS `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` que has creado.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con comodines (`*`) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

El siguiente ejemplo muestra cómo se pueden utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves de contexto de AWS Managed Microsoft AD para evitar el confuso problema de los adjuntos.

```
{
  "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"
      }
    }
  }
}
```

En el siguiente ejemplo, se muestra una política de confianza de IAM de un rol al que se le ha delegado el acceso a la consola. El valor de `aws:SourceArn` debe ser un recurso del directorio de su cuenta. Para obtener más información, consulte Tipos de recursos definidos por AWS Directory Service. Por ejemplo, puede usar `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890`, en el que `123456789012` es su ID de cliente y `d-1234567890` es su ID de directorio.

```
{
  "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 interfaz para los puntos de enlace de Amazon VPC mediante AWS PrivateLink

Puede establecer una conexión privada entre sus puntos de enlace de Amazon VPC y de AWS Directory Service API mediante la creación de un punto de enlace de VPC de interfaz. Puntos de enlace de tipo interfaz con tecnología de AWS PrivateLink.

AWS PrivateLink le permite acceder de forma privada a las operaciones de la AWS Directory Service API sin necesidad de una pasarela de Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect El tráfico entre su VPC y AWS Directory Service no sale de la AWS red.

Cada punto de conexión de la interfaz está representado por una o más interfaces de redes elásticas en las subredes. Para obtener más información sobre la interfaz de red elástica, consulte la interfaz de red elástica en la Guía del usuario de Amazon EC2.

Para obtener más información sobre los puntos de enlace de VPC, consulte Acceso y Servicio de AWS uso de un punto de enlace de VPC de interfaz en la Guía del usuario de Amazon VPC. Para obtener más información sobre las operaciones de la AWS Directory Service API, consulte la referencia de la API.AWS Directory Service

Consideraciones para los puntos de enlace de VPC

Antes de configurar un punto de enlace de VPC de interfaz para puntos de enlace de AWS Directory Service API, asegúrese de revisar Acceder y Servicio de AWS usar un punto de enlace de VPC de interfaz en la Guía.AWS PrivateLink

Todas las operaciones de AWS Directory Service API relevantes para la administración AWS Directory Service de recursos están disponibles en su VPC mediante. AWS PrivateLink

Las políticas de puntos de conexión de VPC son compatibles con los puntos de conexión de la API de Directory Service. De forma predeterminada, se permite el acceso total a las operaciones de la API de Directory Service a través del punto final. Para obtener más información, consulte Controlar el acceso a los puntos de enlace de la VPC mediante políticas de puntos de enlace en la Guía del usuario de Amazon VPC.

Disponibilidad

AWS Directory Service admite puntos finales de VPC de la siguiente manera: Regiones de AWS

Región de AWS disponibilidad

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Oeste de Canadá (Calgary
- China (Pekín y Ningxia)
- Asia-Pacífico (Hong Kong)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milán)
- Europa (París)
- Europa (España)
- Europa (Estocolmo)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)

- Medio Oriente (EAU)
- América del Sur (São Paulo)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (Estados Unidos-Oeste)

Creación de un punto final de interfaz para la API AWS Directory Service

Puede crear un punto final de interfaz de VPC para la AWS Directory Service API mediante la consola Amazon VPC o el (). AWS Command Line Interface AWS CLI Para obtener más información, consulte Create a VPC endpoint (Creación de un punto de conexión de VPC) en la Guía de AWS PrivateLink .

Cree un punto final de interfaz para la AWS Directory Service API con el siguiente nombre de servicio: `com.amazonaws.region.ds`

A excepción Regiones de AWS de China, si habilitas el DNS privado para el punto final, puedes realizar solicitudes de API al AWS Directory Service punto final de la VPC utilizando su nombre de DNS predeterminado Región de AWS, por ejemplo. `ds.us-east-1.amazonaws.com` En el caso de China (Pekín y Ningxia) Regiones de AWS, puede realizar solicitudes de API con el punto final de la VPC `ds-api.cn-north-1.amazonaws.com.cn` mediante `ds-api.cn-northwest-1.amazonaws.com.cn` y, respectivamente.

Para obtener más información, consulte Acceso y Servicio de AWS uso de un punto final de VPC de interfaz en la Guía del usuario de Amazon VPC.

Creación de una política de punto de enlace de la VPC para la AWS Directory Service API

Puede asociar una política de punto de enlace con el punto de enlace de la VPC que controla el acceso a la AWS Directory Service API. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Controlar el acceso a los puntos de enlace de la VPC mediante políticas de puntos de enlace en la Guía del usuario de Amazon VPC.

Ejemplo: política de puntos finales de VPC para acciones de API AWS Directory Service

El siguiente es un ejemplo de una política de puntos finales para la AWS Directory Service API. Al adjuntar esta política al punto final de la interfaz, se concede acceso a las acciones de la AWS Directory Service API enumeradas a todos los principales de todos los recursos.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:DescribeDirectories",
            "ds:DescribeCertificate",
         ],
         "Resource":"*"
      }
   ]
}
```

Ejemplo: política de punto final de VPC que deniega todos los accesos desde un punto específico Cuenta de AWS

La siguiente política de punto final de VPC deniega a Cuenta de AWS *123456789012* todo acceso a los recursos que utilizan el punto final. La política permite todas las acciones de otras cuentas.

```
{
   "Statement": [
      {
         "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal:" "*"
      },
      {
        "Action": "*",
        "Effect": "Deny",
        "Resource": "*",
        "Principal": {
            "AWS": [
               "123456789012"
            ]
```

```
            }
        ]
}
```

Acuerdo de nivel de servicios de AWS Directory Service

AWS Directory Service es un servicio de alta disponibilidad que se basa en la infraestructura administrada de AWS. Está respaldado por un acuerdo de nivel de servicios que define nuestra política de disponibilidad del servicio.

Para obtener más información, consulte el Acuerdo de nivel de servicio de AWS Directory Service.

Disponibilidad regional para AWS Directory Service

En la siguiente tabla, se proporciona una lista que describe los puntos de conexión específicos de las regiones admitidas por cada tipo de directorio.

Nombres de las regiones	Región	Punto de conexión	Protocolo	AWS Microsoft AD gestionado	Conector	AD sencillo
Este de EE. UU. (Norte de Virginia)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	S	S	Sí
Este de EE. UU. (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	S	S	No
Oeste de EE. UU. (Norte de California)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	S	S	No
Oeste de EE. UU. (Oregón)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	S	S	Sí

Nombres de las regiones	Región	Punto de conexión	Protocolo	AWS Microsoft AD gestionado	Conector	AD sencillo
África (Ciudad del Cabo)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	Sí	Sí	No
Asia-Pacífico (Hong Kong)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	Sí	Sí	No
Asia-Pacífico (Hyderabad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	Sí	Sí	No
Asia-Pacífico (Yakarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	Sí	Sí	No
Asia-Pacífico (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	Sí	Sí	No
Asia Pacífico (Mumbai)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	Sí	Sí	No

Nombres de las regiones	Región	Punto de conexión	Protocolo	AWS Microsoft AD gestionado	Conector	AD sencillo
Asia Pacífico (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	Sí	Sí	No
Asia Pacífico (Seúl)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	Sí	Sí	No
Asia-Pacífico (Singapur)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	Sí	Sí	Sí
Asia Pacífico (Sídney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	Sí	Sí	Sí
Asia-Pacífico (Tokio)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	Sí	Sí	Sí
Canadá (centro)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	Sí	Sí	No
Oeste de Canadá (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	Sí	Sí	No

Nombres de las regiones	Región	Punto de conexión	Protocolo	AWS Microsoft AD gestionado	Conector	AD sencillo
China (Pekín)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	Sí	Sí	No
China (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	Sí	Sí	No
Europa (Fráncfort)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	Sí	Sí	No
Europa (Irlanda)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	Sí	Sí	Sí
Europa (Londres)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	Sí	Sí	No
Europa (Milán)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	Sí	Sí	No
Europa (París)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	Sí	Sí	No
Europa (España)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	Sí	Sí	No

Nombres de las regiones	Región	Punto de conexión	Protocolo	AWS Microsoft AD gestionado	Conector	AD sencillo
Europa (Estocolmo)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	S	S	No
Europa (Zúrich)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	S	S	No
Israel (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	S	S	No
Medio Oriente (Baréin)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	S	S	No
Medio Oriente (EAU)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	S	S	No
América del Sur (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	S	S	No
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	ds. us-gov-west-1.amazonaws.com	HTTPS	S	S	No

Nombres de las regiones	Región	Punto de conexión	Protocolo	AWS Microsoft AD gestionado	Conector	AD sencillo
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	ds. us-gov-east-1.amazonaws.com	HTTPS	S	S	No

Para obtener información sobre el uso AWS Directory Service en las regiones AWS GovCloud (EE. UU. Oeste) y AWS GovCloud (EE. UU. Este), consulte los puntos finales del servicio.

Para obtener información sobre el uso AWS Directory Service en las regiones de Pekín y Ningxia, consulte Puntos de enlace y ARN de Amazon Web Services en China.

Compatibilidad del navegador

AWS aplicaciones y servicios como Amazon WorkSpaces, Amazon Connect WorkMail, Amazon Chime, Amazon y AWS IAM Identity Center todos requieren credenciales de inicio de sesión válidas de un navegador compatible antes de poder acceder a ellos. WorkDocs En la siguiente tabla se describen solo los navegadores y las versiones de navegador que son compatibles con los inicios de sesión.

Navegador	Versión	Compatibilidad
Microsoft Edge	Las 3 últimas versiones	Compatible
Mozilla Firefox	Últimas 3 versiones	Compatible
Google Chrome	Últimas 3 versiones	Compatible
Apple Safari	Últimas 3 versiones	Compatible

Ahora que ha verificado que usa una versión compatible de su navegador, le recomendamos que también consulte la siguiente sección para verificar que su navegador se ha configurado para usar la configuración de seguridad de la capa de transporte (TLS) que requiere AWS.

¿Qué es TLS?

TLS es un protocolo que los navegadores web y otras aplicaciones utilizan para intercambiar datos de forma segura a través de una red. TLS garantiza que la conexión a un punto de enlace remoto es el punto de enlace previsto mediante el cifrado y la verificación de la identidad de punto de enlace. Hasta la fecha, las versiones de TLS son TLS 1.0, 1.1, 1.2 y 1.3.

Qué versiones de TLS admite IAM Identity Center

AWS las aplicaciones y los servicios son compatibles con TLS 1.1, 1.2 y 1.3 para iniciar sesión de forma segura. A partir del 30 de octubre de 2019, ya no se admitirá TLS 1.0, por lo que es importante que todos los navegadores estén configurados para admitir TLS 1.1 o superior. Esto significa que no podrá iniciar sesión en aplicaciones y servicios de AWS si obtiene acceso a ellos mientras TLS 1.0 esté habilitado. Si necesita ayuda para realizar este cambio, contacte con su administrador.

Cómo puedo habilitar las versiones de TLS compatibles en mi navegador

Depende de su navegador. Por lo general, puede encontrar esta configuración en el área de configuración avanzada de la configuración de su navegador. Por ejemplo, en Internet Explorer encontrará las opciones de TLS en Propiedades de Internet, la pestaña Opciones avanzadas y en la seccion Seguridad. Compruebe el sitio web de ayuda del fabricante del navegador para obtener instrucciones específicas.

Historial del documento

En la siguiente tabla se describen los cambios importantes realizados desde la última publicación de la Guía del administrador de AWS Directory Service .

Cambio	Descripción	Fecha
Configuración de autenticación basada en certificados	Se agregó contenido sobre dos nuevas configuraciones de seguridad para AWS Managed Microsoft AD.	11 de abril de 2023
AWS PrivateLink	Se agregó contenido sobre AWS PrivateLink.	31 de marzo de 2023
Puntos de conexión de VPC para Simple AD	Se agregó contenido sobre los puntos de conexión de VPC que no deberían configurarse.	25 de agosto de 2021
Puntos de conexión de VPC para Conector AD	Se agregó contenido sobre los puntos de conexión de VPC que no deberían configurarse.	25 de agosto de 2021
Compatibilidad con tarjetas inteligentes	Se agregó contenido sobre la compatibilidad con tarjetas inteligentes y Amazon WorkSpaces Application Manager en la región AWS GovCloud (EE. UU. Oeste)	1 de diciembre de 2020
Restablecimiento de la contraseña	Se agregó contenido sobre cómo restablecer las contraseñas de los usuarios mediante AWS Management Console, Windows PowerShel l y AWS CLI.	2 de enero de 2019

Uso compartido de directorio	Se agregó contenido sobre cómo usar el uso compartido de directorios con Microsoft AD AWS administrado.	25 de septiembre de 2018
Contenido migrado a la nueva guía para desarrolladores de Amazon Cloud Directory	Se trasladó el contenido de Amazon Cloud Directory de esta guía a la nueva Guía para desarrolladores de Amazon Cloud Directory.	21 de junio de 2018
Renovación completa del índice de la guía del administrador	Se reorganizó el contenido para atender mejor a las necesidades de los clientes. También se agregó contenido nuevo cuando fue necesario.	5 de abril de 2018
AWS grupos delegados	Se agregó una lista de grupos AWS delegados que se pueden asignar a usuarios locales.	8 de marzo de 2018
Políticas de contraseñas detalladas	Se ha agregado contenido sobre nuevas políticas de contraseñas.	5 de julio de 2017
Controladores de dominio adicionales	Se agregó contenido sobre cómo agregar más controladores de dominio a su directorio en Microsoft AD AWS administrado.	30 de junio de 2017
Tutoriales	Se agregaron nuevos tutoriales para probar un entorno de laboratorio AWS administrado de Microsoft AD.	21 de junio de 2017

MFA con AWS Microsoft AD administrado	Se agregó contenido sobre el uso de MFA con AWS Microsoft AD administrado.	13 de febrero de 2017
Amazon Cloud Directory	Se agregó contenido sobre un nuevo tipo de directorio.	26 de enero de 2017
Ampliaciones del esquema	Se agregó contenido sobre las extensiones de esquema con AWS Directory Service para Microsoft Active Directory.	14 de noviembre de 2016
Reorganización importante de la Guía del AWS Directory Service administrador	Se reorganizó el contenido para atender mejor a las necesidades de los clientes.	14 de noviembre de 2016
Notificaciones de SNS	Se agregó contenido sobre las notificaciones de SNS.	25 de febrero de 2016
Autorización y autenticación	Se agregó contenido sobre cómo usar IAM con. AWS Directory Service	25 de febrero de 2016
AWS Microsoft AD gestionado	Se agregó contenido sobre Microsoft AD AWS administrado y guías combinadas en una sola guía.	17 de noviembre de 2015
Posibilidad de unir instancias de Linux a un directorio de Simple AD	Se agregó contenido sobre cómo unir una instancia de Linux a un directorio de Simple AD.	23 de julio de 2015
División de la guía	Se dividió la Guía de administración de AWS Directory Service en guías independientes.	14 de julio de 2015

Compatibilidad con inicio de sesión único	Se agregó contenido sobre la compatibilidad con el inicio de sesión único.	31 de marzo de 2015
Nueva guía	Esta es la primera versión de la Guía del administrador de AWS Directory Service .	21 de octubre de 2014

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.