Instalar y configurar VMware Identity Manager

VMware Identity Manager 2.8

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

https://docs.vmware.com/es/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Acerca de la instalación y configuración de VMware Identity Manager

La guía *Instalación y configuración de VMware Identity Manager* proporciona información sobre el proceso de instalación y configuración del dispositivo de VMware Identity Manager. Al finalizar la instalación, se puede utilizar la consola de administración para autorizar a los usuarios a acceder desde varios dispositivos a las aplicaciones de la organización, incluyendo aplicaciones de Windows, aplicaciones de SaaS (software como servicio) y escritorios de Horizon o de View. La guía también explica cómo configurar la implementación para conseguir una elevada disponibilidad.

Público objetivo

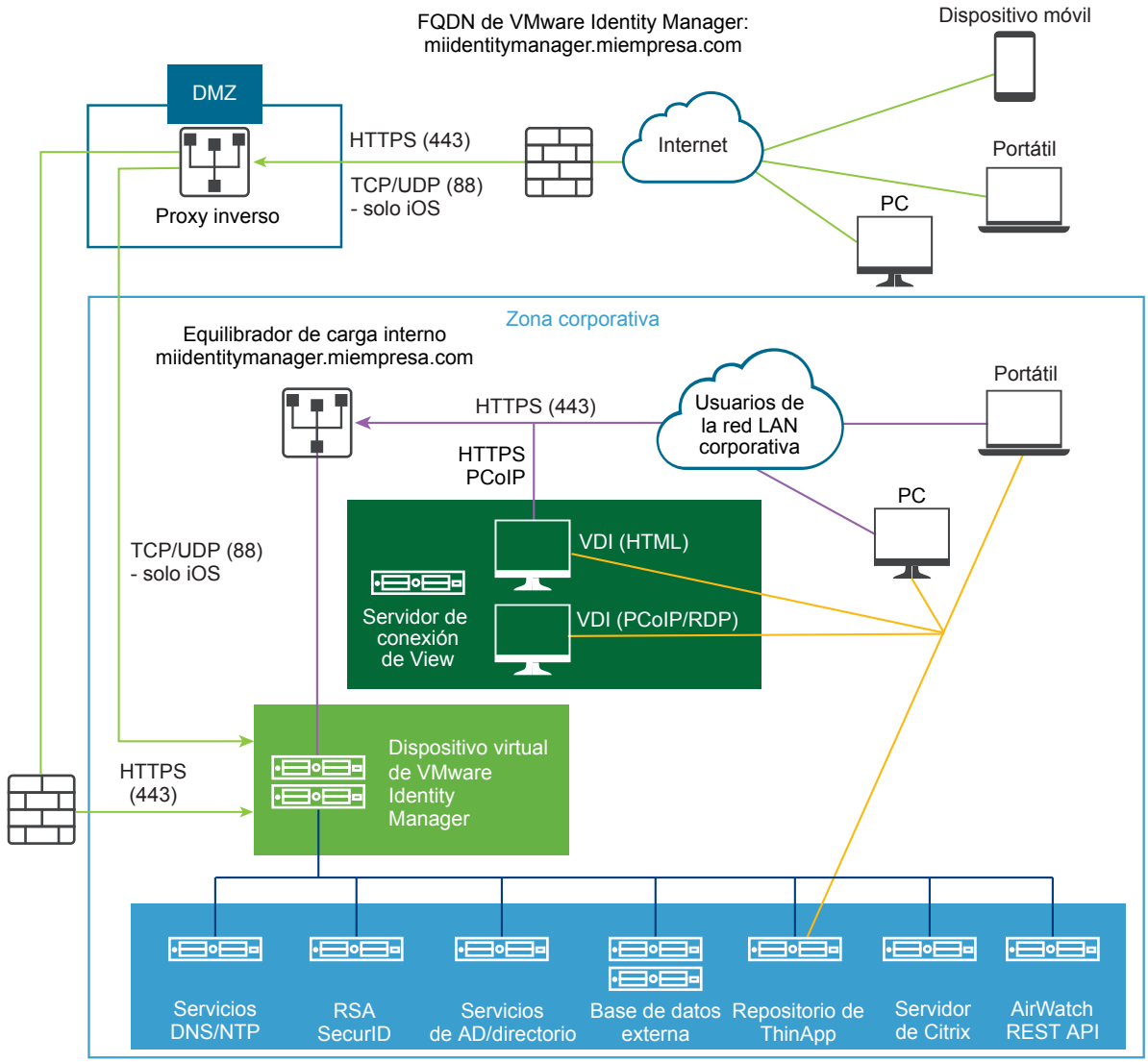
Esta información está dirigida a los administradores de VMware Identity Manager. La información está escrita para administradores expertos de sistemas Windows y Linux que están familiarizados con tecnologías de VMware, especialmente con vCenter™, ESX™, vSphere® y View™, con conceptos de redes, con servidores, bases de datos y procedimientos de copia de seguridad y restauración de Active Directory, y con servidores NTP y Simple Mail Transfer Protocol (SMTP). SUSE Linux 11 es el sistema operativo subyacente del dispositivo virtual. Es útil conocer también otras tecnologías como VMware ThinApp® y RSA SecurID si está prevista su implementación.

Preparar la instalación de VMware Identity Manager

1

Las tareas de implementación y configuración de VMware Identity Manager requieren completar los requisitos previos, implementar el archivo OVA de VMware Identity Manager y completar la configuración desde el asistente de configuración de VMware Identity Manager.

Figura 1-1. Diagrama de la arquitectura de VMware Identity Manager para implementaciones típicas



NOTA: Si prevé habilitar la autenticación con certificado o smart card, utilice la configuración de pass-through de SSL en el equilibrador de carga en lugar de la configuración de terminación de SSL. Esta configuración asegura que la negociación handshake se realice entre el conector, un componente de VMware Identity Manager, y el cliente.

NOTA: Las REST API de Airwatch pueden estar en la nube o en las instalaciones, según la ubicación de la implementación.

Este capítulo cubre los siguientes temas:

- "Requisitos de configuración de la red y el sistema," página 11
- "Preparar la implementación de VMware Identity Manager," página 15
- "Programa para la mejora de la experiencia del usuario," página 18

Requisitos de configuración de la red y el sistema

Al tomar decisiones respecto a requisitos de hardware, recursos y red, considere la implementación completa, incluyendo la integración de recursos.

Versiones compatibles de vSphere y ESX

Son compatibles las siguientes versiones de servidor ESX y vSphere:

- 5.0 U2 y posteriores
- 5.1 y posteriores
- 5.5 y posteriores
- 6.0 y posteriores

NOTA: Se debe activar la sincronización de hora en el nivel de host de ESX mediante un servidor NTP. De lo contrario, se produce una variación horaria entre los dispositivos virtuales.

Si se implementan varios dispositivos virtuales en distintos host, se debe considerar desactivar la opción de sincronización con el host y configurar el servidor NTP directamente en cada dispositivo virtual, para asegurar que no haya diferencia horaria entre los dispositivos virtuales.

Requisitos de hardware

Asegúrese de que cumple con los requisitos de cantidad de dispositivos virtuales de VMware Identity Manager y recursos asignados a cada dispositivo.

Número de usuarios	Hasta 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.000
Número de servidores de VMware Identity Manager	1 servidor	3 servidores con equilibrio de carga	3 servidores con equilibrio de carga	3 servidores con equilibrio de carga	3 servidores con equilibrio de carga
CPU (por servidor)	2 CPU	2 CPU	4 CPU	8 CPU	8 CPU
RAM (por servidor)	6 GB	6 GB	8 GB	16 GB	32 GB
Espacio de disco (por servidor)	60 GB	100 GB	100 GB	100 GB	100 GB

Si instala dispositivos virtuales de conectores adicionales externos, asegúrese de cumplir con los siguientes requisitos.

Número de usuarios	Hasta 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.1000
Número de servidores de conector	1 servidor	2 servidores con equilibrio de carga	2 servidores con equilibrio de carga	2 servidores con equilibrio de carga	2 servidores con equilibrio de carga
CPU (por servidor)	2 CPU	4 CPU	4 CPU	4 CPU	4 CPU

Número de usuarios	Hasta 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.1000
RAM (por servidor)	6 GB	6 GB	8 GB	16 GB	16 GB
Espacio de disco (por servidor)	60 GB	60 GB	60 GB	60 GB	60 GB

Requisitos de base de datos

Configure VMware Identity Manager con una base de datos externa para almacenar y organizar datos del servidor. Existe una base de datos de PostgreSQL interna integrada en el dispositivo virtual, pero no se recomienda usarla para implementaciones de producción.

Para obtener información sobre las versiones de base de datos y las configuraciones de service pack compatibles, consulte las matrices de interoperabilidad de productos VMware en https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Los siguientes requisitos se aplican a una base de datos de SQL Server externa.

Número de usuarios	Hasta 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.000
CPU	2 CPU	2 CPU	4 CPU	8 CPU	8 CPU
RAM	4 GB	4 GB	8 GB	16 GB	32 GB
Espacio en disco	50 GB	50 GB	50 GB	100 GB	100 GB

Requisitos de configuración de red

Componente	Requisito mínimo
Dirección IP y registro de DNS	Registro de DNS y dirección IP
Puerto del firewall	Compruebe que el puerto entrante 443 del firewall esté abierto para usuario fuera de la red hacia la instancia de VMware Identity Manager o al equilibrador de carga.
Proxy inverso	Implemente un proxy inverso como el administrador de directivas de acceso F5 en DMZ para permitir que los usuarios accedan de forma remota y segura al portal de VMware Identity Manager.

Requisitos de puertos

Los puertos utilizados en la configuración del servidor se describen a continuación. La implementación solo puede incluir un subconjunto de ellos. Estos son dos casos posibles:

- Para sincronizar usuarios y grupos desde Active Directory, VMware Identity Manager se debe conectar a Active Directory.
- Para sincronizar con ThinApp, VMware Identity Manager se debe unir al dominio de Active Directory y conectar a la unidad compartida de repositorio de ThinApp.

Puerto	Portal	Origen	destino	Descripción
443	HTTPS	Equilibrador de carga	Dispositivo virtual de VMware Identity Manager	
443	HTTPS	Dispositivo virtual de VMware Identity Manager	Dispositivo virtual de VMware Identity Manager	

Puerto	Portal	Origen	destino	Descripción
443	HTTPS	Navegadores	Dispositivo virtual de VMware Identity Manager	
443	HTTPS	Dispositivo virtual de VMware Identity Manager	vapp-updates.vmware.com	Acceso al servidor de actualización
8443	HTTPS	Navegadores	Dispositivo virtual de VMware Identity Manager	Puerto de administrador
25	SMTP	Dispositivo virtual de VMware Identity Manager	SMTP	Puerto para redireccionamiento de correo saliente
389 636 3268 3269	LDAP LDAPS MSFT-GC MSFT-GC-SSL	Dispositivo virtual de VMware Identity Manager	Active Directory	Se muestran los valores predeterminados. Estos puertos se pueden configurar.
445	TCP	Dispositivo virtual de VMware Identity Manager	Repositorio de ThinApp de VMware	Acceso al repositorio de ThinApp
5500	UDP	Dispositivo virtual de VMware Identity Manager	Sistema RSA SecurID	Se muestra el valor predeterminado. Este puerto se puede configurar.
53	TCP/UDP	Dispositivo virtual de VMware Identity Manager	Servidor DNS	Todos los dispositivos virtuales deben tener acceso al servidor DNS en el puerto 53 y permitir el tráfico SSH entrante en el puerto 22.
88, 464, 135	TCP/UDP	Dispositivo virtual de VMware Identity Manager	Controlador de dominio	
9300–9400	TCP	Dispositivo virtual de VMware Identity Manager	Dispositivo virtual de VMware Identity Manager	Necesidades de auditoría
54328	UDP			
1433, 5432, 1521	TCP	Dispositivo virtual de VMware Identity Manager	Base de datos	El puerto predeterminado de Microsoft SQL es el 1433 El puerto predeterminado de Oracle es el 1521
443		Dispositivo virtual de VMware Identity Manager	Servidor de View	Acceso al servidor de View
80, 443	TCP	Dispositivo virtual de VMware Identity Manager	Servidor del agente de integración de Citrix	Conexión con el agente de integración de Citrix. La opción del puerto depende de si se instala un certificado en el servidor del agente de integración.

Puerto	Portal	Origen	destino	Descripción
443	HTTPS	Dispositivo virtual de VMware Identity Manager	REST API de AirWatch	Para comprobar el cumplimiento normativo del dispositivo y el método de autenticación de contraseña de AirWatch Cloud Connector, si se utiliza.
88	TCP/UDP	Dispositivo móvil iOS	Dispositivo virtual de VMware Identity Manager	Puerto utilizado para el tráfico de Kerberos desde el dispositivo iOS hasta el KDC integrado.
5262	TCP	Dispositivo móvil Android	Servicio de proxy HTTPS de AirWatch	El cliente de AirWatch Tunnel enruta el tráfico al proxy HTTPS para los dispositivos Android.

Active Directory

VMware Identity Manager es compatible con Active Directory en Windows 2008, 2008 R2, 2012 y 2012 R2, con las opciones de Nivel funcional del dominio y Nivel funcional de bosque de Windows 2003 y versiones posteriores.

Navegadores web admitidos para obtener acceso a la consola de administración

La consola de administración de VMware Identity Manager es una aplicación basada en web que le permite administrar su arrendatario. Los navegadores siguientes le permiten obtener acceso a la consola de administración.

- Internet Explorer 11 para sistemas Windows
- Google Chrome 42.0 o posterior para sistemas Windows y Mac
- Mozilla Firefox 40 o posterior para sistemas Windows y Mac
- Safari 6.2.8 y posterior para sistemas Mac

NOTA: En Internet Explorer 11, es necesario tener habilitado JavaScript y el uso de cookies para superar la autenticación de VMware Identity Manager.

Navegadores compatibles para acceder al portal Workspace ONE

Los siguientes navegadores permiten a los usuarios finales obtener acceso al portal de Workspace ONE.

- Mozilla Firefox (más reciente)
- Google Chrome (más reciente)
- Safari (más reciente)
- Internet Explorer 11
- Navegador Microsoft Edge

- Navegador nativo y Google Chrome en dispositivos con Android
- Safari en dispositivos con iOS

NOTA: En Internet Explorer 11, es necesario tener habilitado JavaScript y el uso de cookies para superar la autenticación de VMware Identity Manager.

Preparar la implementación de VMware Identity Manager

Antes de implementar VMware Identity Manager, debe preparar el entorno. Esta preparación incluye la descarga del archivo OVA de VMware Identity Manager, la creación de los registros de DNS y la obtención de las direcciones IP.

Prerequisitos

Antes de comenzar a instalar VMware Identity Manager, complete las tareas previas requeridas.

- Para implementar el dispositivo virtual de VMware Identity Manager se necesitan uno o varios servidores ESX.

  NOTA: Para obtener información sobre las versiones del servidor ESX y vSphere compatibles, consulte las matrices de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- Se necesita VMware vSphere Client o vSphere Web Client y acceder el dispositivo virtual de forma remota para configurar la red.
- Descargue el archivo OVA de VMware Identity Manager desde el sitio web de VMware.

Crear registros de DNS y direcciones IP

Deben estar disponibles una entrada DNS y una dirección IP estática para el dispositivo virtual de VMware Identity Manager. Dado que cada empresa administra sus direcciones IP y registros de DNS de forma distinta, debe solicitar el registro de DNS y las direcciones de IP que se van a utilizar antes de empezar la instalación.

La configuración de la búsqueda inversa es opcional. Cuando implemente la búsqueda inversa, debe definir un registro PTR en el servidor DNS para que el dispositivo virtual utilice la configuración de red correcta.

Puede utilizar la siguiente lista de ejemplos de registros de DNS cuando se ponga en contacto con el administrador de la red. Sustituya la información de los ejemplos con la información de su entorno. En este ejemplo se muestran los registros de DNS directas y las direcciones IP.

Tabla 1-1. Ejemplos de registros de DNS directas y direcciones IP

Nombre de dominio	Tipo de recurso	Dirección IP
miidentitymanager.empresa.com	A	10.28.128.3

En este ejemplo se muestran los registros de DNS inversas y las direcciones IP.

Tabla 1-2. Ejemplos de registros de DNS inversas y direcciones IP

Dirección IP	Tipo de recurso	Nombre del host
10.28.128.3	PTR	miidentitymanager.empresa.com

Después de completar la configuración de DNS, compruebe que la búsqueda de DNS inversas está correctamente configurada. Por ejemplo, el comando `host IPaddress` del dispositivo virtual debe resolverse en la búsqueda del nombre de DNS.

Utilizar un servidor DNS basado en Linux o Unix

Si utiliza un servidor DNS basado en Linux o Unix y desea conectar el de VMware Identity Manager al dominio de Active Directory, compruebe que se crean los registros SRV adecuados para cada controlador del dominio de Active Directory.

NOTA: Si tiene un equilibrador de carga con una dirección IP virtual (VIP) frente a los servidores DNS, tenga en cuenta que VMware Identity Manager no admite el uso de VIP. Puede especificar varios servidores DNS separados por comas.

Opciones de base de datos con VMware Identity Manager

Configure VMware Identity Manager con una base de datos externa para almacenar y organizar datos del servidor. Una base de datos PostgreSQL interna está incrustada en el dispositivo, aunque no se recomienda usarla para implementaciones de producción.

Para utilizar una base de datos externa, el administrador de la base de datos debe preparar una base de datos externa vacía y un esquema antes de conectar a la base de datos externa en el asistente de configuración. Los usuarios con licencia pueden utilizar un servidor de base de datos de Oracle o de Microsoft SQL para configurar un entorno de base de datos externa de alta disponibilidad. Consulte "Establecer conexión con la base de datos," página 34.

Conectar al directorio empresarial

VMware Identity Manager utiliza la infraestructura del directorio empresarial para la administración y la autenticación del usuario. Puede integrar VMware Identity Manager con un entorno de Active Directory formado por un único dominio de Active Directory, varios dominios en un único bosque de Active Directory o varios dominios en varios bosques de Active Directory. También puede integrar VMware Identity Manager con un directorio LDAP. Para sincronizar usuarios y grupos, el dispositivo virtual de VMware Identity Manager debe conectarse al directorio.

Se debe poder acceder al directorio desde la misma red de LAN que la del dispositivo virtual de VMware Identity Manager.

Consulte Capítulo 4, "Integración con el directorio empresarial," página 45 para obtener más información.

Listas de comprobación de implementación

La lista de comprobación de implementación le permite recopilar la información necesaria para instalar el dispositivo virtual de VMware Identity Manager.

Información sobre el nombre de dominio plenamente cualificado

Tabla 1-3. Lista de comprobación de información sobre el nombre de dominio plenamente cualificado (FQDN, Fully Qualified Domain Name)

Información para recopilar	Muestra la información
FQDN del VMware Identity Manager de	

Información de red del dispositivo virtual del de VMware Identity Manager

Tabla 1-4. Lista de comprobación de información de red

Información para recopilar	Muestra la información
Dirección IP	Debe utilizar una dirección IP estática y debe tener un PTR y un registro A definidos en el DNS.
Nombre de DNS de este dispositivo virtual	

Tabla 1-4. Lista de comprobación de información de red (Continua)

Información para recopilar	Muestra la información
Dirección de puerta de enlace predeterminada	
Prefijo o máscara de red	

Información del directorio

VMware Identity Manager es compatible con los entornos de Active Directory o de los directorios LDAP.

Tabla 1-5. Lista de comprobación de información sobre el controlador de dominio de Active Directory

Información para recopilar	Muestra la información
Nombre del servidor de Active Directory	
Nombre del dominio de Active Directory	
DN base	
Para Active Directory mediante LDAP, el nombre de usuario y la contraseña de DN de enlace	
Para Active Directory con autenticación integrada de Windows (IWA, Integrated Windows Authentication), el nombre de usuario y la contraseña de la cuenta con privilegios para unir equipos al dominio.	

Tabla 1-6. Lista de comprobación de información del servidor del directorio LDAP

Información para recopilar	Muestra la información
Dirección IP o nombre del servidor del directorio LDAP	
Número de puerto del servidor del directorio LDAP	
DN base	
Nombre de usuario DN de enlace y contraseña	
Filtro de búsqueda de LDAP para objetos de grupo, objetos de usuarios de enlace y objetos de usuarios	
Nombres de atributos LDAP de la pertenencia a grupos, UUID del objeto y nombre distintivo	

certificados SSL

Puede agregar un certificado SSL después de implementar el dispositivo virtual VMware Identity Manager.

Tabla 1-7. Lista de comprobación de información sobre el certificado SSL

Información para recopilar	Muestra la información
Certificado SSL	
Clave privada	

Clave de licencia

Tabla 1-8. Lista de comprobación de información sobre la clave de licencia de VMware Identity Manager

Información para recopilar	Muestra la información
Clave de licencia	

NOTA: La información sobre la clave de licencia se introduce en la página **Configuración de dispositivos > Licencia** de la consola de administración después de completar la instalación.

Base de datos externa

Tabla 1-9. Lista de comprobación de información sobre la base de datos externa

Información para recopilar	Muestra la información
Nombre del host de la base de datos	
Puerto	
Nombre de usuario	
Contraseña	

Programa para la mejora de la experiencia del usuario

Al instalar el dispositivo virtual VMware Identity Manager, puede elegir participar en el programa para la mejora de la experiencia del usuario de VMware.

Si participa en el programa, VMware recopilará información anónima sobre su implementación para mejorar la respuesta de VMware a los requisitos del usuario. No se recopila ningún dato que identifique a su organización.

Antes de recopilar la información, VMware convierte en anónimos todos los campos que contengan información específica de su organización.

NOTA: Si su red está configurada para acceder a Internet a través de un proxy HTTP, para poder enviar esta información deberá ajustar la configuración del proxy en el dispositivo virtual VMware Identity Manager. Consulte "Configurar los valores del servidor proxy para VMware Identity Manager," página 30.

Implementación de VMware Identity Manager 2

Para implementar VMware Identity Manager, debe implementar la plantilla OVF mediante vSphere Client o vSphere Web Client, encender el dispositivo virtual de VMware Identity Manager y configurar las opciones.

Después de implementar el dispositivo virtual de VMware Identity Manager, use el asistente de configuración para configurar el entorno de VMware Identity Manager.

Use la información de la lista de comprobación de implementación para completar la instalación. Consulte "Listas de comprobación de implementación," página 16.

Este capítulo cubre los siguientes temas:

Instalación del archivo OVA de VMware Identity Manager

El archivo OVA de VMware Identity Manager se implementa mediante vSphere Client o vSphere Web Client. Puede descargar e implementar el archivo OVA desde una ubicación local a la que pueda obtener acceso vSphere Client, o bien implementarlo desde una URL web.

NOTA: Si usa vSphere Web Client, use los navegadores Firefox o Chrome para implementar el archivo OVA. No use Internet Explorer.

Prerequisitos

Revise Capítulo 1, "Preparar la instalación de VMware Identity Manager," página 9.

Procedimiento

1 Descargue el archivo OVA de VMware Identity Manager desde My VMware.

2 Inicie sesión en vSphere Client o vSphere Web Client.

3 Seleccione **Archivo > Implementar plantilla OVF**.

4 En el asistente de implementación de la plantilla OVF, especifique la información siguiente.

Página	Descripción
Origen	Desplácese hasta la ubicación del paquete de OVA o introduzca una URL específica.
Detalles de la plantilla OVF	Revise los detalles del producto, incluidos los requisitos de tamaño y versión.
Acuerdo de licencia de usuario final	Lea el Contrato de licencia para el usuario final y haga clic en **Aceptar**.
Nombre y ubicación	Introduzca un nombre para el dispositivo virtual de VMware Identity Manager. El nombre debe ser único en la carpeta de inventario y puede tener hasta 80 caracteres. Los nombres distinguen entre mayúsculas y minúsculas. Seleccione una ubicación para el dispositivo virtual.
Host / Clúster	Seleccione el host o clúster en el que se ejecutará el dispositivo virtual.
Grupo de recursos	Seleccione el grupo de recursos.
Almacenamiento	Seleccione la ubicación de almacenamiento de los archivos del dispositivo virtual. Puede seleccionar un perfil de almacenamiento de máquina virtual.
Formato de disco	Seleccione el formato de disco de los archivos. Para entornos de producción, seleccione uno de los formatos de aprovisionamiento pesado. Para evaluación y pruebas, use el formato de aprovisionamiento ligero. En el formato de aprovisionamiento pesado, todo el espacio requerido para el disco virtual se asigna durante la implementación. En el formato de aprovisionamiento ligero, el disco solo usa la cantidad de espacio de almacenamiento que necesita para sus operaciones iniciales.
Asignación de redes	Asigne las redes usadas en VMware Identity Manager a redes de su inventario.
Propiedades	a En el campo **Configuración de zona horaria**, seleccione la zona horaria correcta. b La casilla **Programa para la mejora de la experiencia del cliente** se encuentra seleccionada de manera predeterminada. VMware recopila datos anónimos sobre su implementación con el fin de mejorar la respuesta de VMware a los requisitos del usuario. Anule la selección de la casilla si no desea que se recopilen datos. c En el cuadro de texto **Nombre de host (FQDN)**, introduzca el nombre del host que se usará. Si se deja en blanco, se utilizará la DNS inversa para buscar el nombre de host. d Configure las propiedades de la red. ■ Para configurar una dirección IP estática para VMware Identity Manager, introduzca la información necesaria en los campos **Puerta de enlace predeterminada**, **DNS**, **Dirección IP** y **Máscara de red**. **NOTA:** Si tiene un equilibrador de carga con una dirección IP virtual (VIP) frente a los servidores DNS, tenga en cuenta que VMware Identity Manager no admite el uso de VIP. Puede especificar varios servidores DNS separados por comas. **IMPORTANTE:** Si se deja en blanco cualquiera de estos cuatro campos de dirección, incluido **Nombre de host**, se usará DHCP. ■ Para configurar DHCP, deje en blanco los campos de dirección. **NOTA:** Los campos **Nombre del dominio** y **Ruta de búsqueda de dominio** no se usan. Puede dejarlos en blanco. (Opcional) Después de instalar VMware Identity Manager, pude configurar grupos de IP. Consulte "(Opcional) Agregar grupos de direcciones IP," página 21.
Listo para finalizar	Revise las selecciones y haga clic en **Finalizar**.

En función de la velocidad de la red, la implementación puede tardar varios minutos. El cuadro de diálogo que se abre le mostrará el progreso de la operación.

5 Cuando se complete la implementación, en el cuadro de diálogo de progreso, haga clic en **Cerrar**.

6 Seleccione el dispositivo virtual de VMware Identity Manager que implementó, haga clic con el botón derecho y seleccione **Energía > Encender**.

Se inicializará el dispositivo virtual de VMware Identity Manager. Para ver los detalles, vaya a la pestaña **consola**. Cuando se completa la inicialización del dispositivo virtual, la pantalla de la consola muestra las URL, la dirección IP y la versión de VMware Identity Manager para iniciar sesión en la interfaz web de VMware Identity Manager y completar la configuración.

Qué hacer a continuación

- (Opcional) Agregue grupos de IP.
- Configure las opciones de VMware Identity Manager, lo que incluye la conexión a Active Directory o al directorio LDAP y la selección de los usuarios y grupos que se sincronizarán con VMware Identity Manager.

(Opcional) Agregar grupos de direcciones IP

La configuración de la red con grupos de direcciones IP es opcional en VMware Identity Manager. Es posible agregar grupo de direcciones IP manualmente al dispositivo virtual de VMware Identity Manager después de que se haya instalado.

Los grupos de direcciones IP actúan como servidores DHCP para asignar direcciones IP del grupo al dispositivo virtual de VMware Identity Manager. Para utilizar grupos de direcciones IP, se deben editar las propiedades de red del dispositivo virtual para cambiarlas a dinámicas y configurar la máscara de red, la puerta de enlace y la configuración de DNS.

Prerequisitos

El dispositivo virtual debe estar apagado.

Procedimiento

1 En vSphere Client o vSphere Web Client, haga clic con el botón derecho en el dispositivo virtual de VMware Identity Manager y seleccione **Editar configuración**.

2 Seleccione la pestaña **Opciones**.

3 En las **opciones de vApp**, haga clic en **Avanzado**.

4 En la sección Propiedades de la derecha, haga clic en el botón **Propiedades**.

5 En el cuadro de diálogo de configuración avanzada de propiedades, configure las claves siguientes:

- vami.DNS.WorkspacePortal
- vami.netmask0.WorkspacePortal
- vami.gateway.WorkspacePortal

a Seleccione una de las claves y haga clic en **Editar**.

b En el cuadro de diálogo de edición de la configuración de la propiedad, junto al campo **Tipo**, haga clic en **Editar**.

c En el cuadro de diálogo de edición de tipo de propiedad, seleccione **propiedad dinámica** y, en el menú desplegable, seleccione el valor adecuado de **máscara de red**, **dirección de puerta de enlace** y **servidor DNS** respectivamente.

d Haga clic en **Aceptar** y en **Aceptar** de nuevo.

e Repita estos pasos para configurar cada clave.

6 Encienda el dispositivo virtual.

Las propiedades están configuradas para usar grupos de direcciones IP.

Qué hacer a continuación

Configure los parámetros de VMware Identity Manager.

Configurar las opciones de VMware Identity Manager

Después de implementar el OVA de VMware Identity Manager, debe utilizar el asistente de configuración para establecer contraseñas y seleccionar una base de datos. En ese momento puede configurar la conexión a Active Directory o al directorio LDAP.

Prerequisitos

- El dispositivo virtual de VMware Identity Managerdebe estar encendido.
- Si utiliza una base de datos externa, esta debe estar configurada y la información de la base de la conexión de la base de datos externa debe estar disponible. Para obtener más información, consulte "Establecer conexión con la base de datos," página 34.
- Consulte Capítulo 4, "Integración con el directorio empresarial," página 45, "Integrar con Active Directory," página 47 y "Integrar un directorio LDAP en el servicio," página 62 para obtener información sobre requisitos y limitaciones.
- Debe tener la información de su directorio LDAP o de Active Directory.
- Cuando configura Active Directory con varios bosques y el grupo local de dominios contiene miembros de dominios de diferentes bosques, debe agregar el usuario de DN de enlace utilizado en la página Directorio de VMware Identity Manager al grupo de administradores del dominio en el que reside el grupo local de dominios. De lo contrario, estos miembros estarán ausentes del grupo local del dominio.
- Debe disponer de una lista de los atributos de usuario que desea utilizar como filtros y una lista de los grupos que desea agregar a VMware Identity Manager.

Procedimiento

1 Acceda a la URL de VMware Identity Manager que se muestra en la pantalla azul en la pestaña **Consola**. Por ejemplo, `https://nombredehost.ejemplo.com`.

2 Si se le solicita, acepte el certificado.

3 En la página Comenzar, haga clic en **Continuar**.

4 En la página Establecer contraseñas establezca las contraseñas de las siguientes cuentas de administrador, que se utilizan para administrar el dispositivo, y haga clic en **Continuar**.

Cuenta	
Administrador del dispositivo	Establezca la contraseña del usuario **admin**. Este nombre de usuario no se puede cambiar. La cuenta del usuario **admin** se utiliza para administrar la configuración del dispositivo. **IMPORTANTE:** La contraseña del usuario **admin** debe tener 6 caracteres como mínimo.
Raíz del dispositivo	Establezca la contraseña de usuario **raíz**. El usuario **raíz** tiene todos los derechos sobre el dispositivo.
Usuario remoto	Establezca la contraseña **sshuser**. Esta contraseña se utiliza para iniciar sesión de forma remota en el dispositivo con una conexión SSH.

5 En la página Seleccionar base de datos, seleccione la base de datos que va a utilizar.

Consulte "Establecer conexión con la base de datos," página 34 para obtener más información.

- Si utiliza una base de datos externa, seleccione **Base de datos externa** e introduzca el nombre de usuario, la contraseña y la información de la conexión de la base de datos externa. Para comprobar que VMware Identity Manager puede conectarse a la base de datos, haga clic en **Probar conexión**.

  Después de comprobar la conexión, haga clic en **Continuar**.

- Si utiliza la base de datos interna, haga clic en **Continuar**.

  NOTA: No se recomienda usar la base de datos interna para implementaciones de producción.

La conexión a la base de datos se configurará y la base de datos se inicializará. Cuando el proceso finalice, aparecerá la página **La configuración se completó**.

6 Haga clic en el vínculo **Inicie la sesión en la consola de administración** de la página **La configuración se completó** para iniciar sesión en la consola de administración y configurar la conexión de Active Directory o del directorio LDAP.

7 Inicie sesión en la consola de administración como usuario **admin** con la contraseña que estableció.

Iniciará sesión como administrador local. Se mostrará la página Directorios. Antes de agregar un directorio, asegúrese de revisar Capítulo 4, "Integración con el directorio empresarial," página 45, "Integrar con Active Directory," página 47 y "Integrar un directorio LDAP en el servicio," página 62 para obtener más información sobre requisitos y limitaciones.

8 Haga clic en la pestaña **Administración de acceso e identidad**.

9 Haga clic en **Configurar > Atributos de usuario** para seleccionar los atributos del usuario que se van a sincronizar con el directorio.

Aparecerán los atributos predeterminados y podrá seleccionar los que sean necesarios. Si un atributo está marcado como obligatorio, solo se sincronizan al servicio los usuarios con dicho atributo. También puede agregar otros atributos.

IMPORTANTE: Después de crear un directorio, no podrá convertir un atributo en un atributo obligatorio. Debe elegir esa opción ahora.

Compruebe también que todas las configuraciones de la página Atributos de usuario se apliquen a todos los directorios del servicio. Cuando marque un atributo como obligatorio, tenga en cuenta el efecto que pueda causar en otros directorios. Si un atributo está marcado como obligatorio, no se sincronizan con el servicio de los usuarios sin dicho atributo.

IMPORTANTE: Si va a sincronizar recursos de XenApp con VMware Identity Manager, debe convertir **distinguishedName** en un atributo obligatorio.

10 Haga clic en **Guardar**.

11 Haga clic en la pestaña **Administración de acceso e identidad**.

12 En la página Directorios, haga clic en **Agregar directorio** y seleccione **Agregar Active Directory en LDAP/IWA** o **Agregar directorio LDAP**, según el tipo de directorio que está integrando.

También puede crear un directorio local en el servicio. Para obtener más información sobre cómo usar los directorios locales, consulte Capítulo 5, "Usar directorios locales," página 69.

13 En el caso de Active Directory, siga estos pasos.

a Introduzca un nombre para el directorio que está creando en VMware Identity Manager y seleccione el tipo de directorio, ya sea **Active Directory mediante LDAP** o **Active Directory (Autenticación de Windows integrada)**.

b Proporcione la información de la conexión.

Opción	Descripción
Active Directory mediante LDAP	1 En el campo **Conector de sincronización**, seleccione el conector que desee utilizar para sincronizar usuarios y grupos de Active Directory con el directorio de VMware Identity Manager. De forma predeterminada, un componente del conector estará siempre disponible con el servicio de VMware Identity Manager. Este conector aparecerá en la lista desplegable. Si instala varios dispositivos de VMware Identity Manager para lograr una alta disponibilidad, el componente del conector de cada uno aparecerá en la lista. 2 En el campo **Autenticación**, seleccione **Sí** si desea utilizar Active Directory para autenticar a los usuarios. Si desea utilizar un proveedor de identidades externo para autenticar a los usuarios, haga clic en **No**. Después de configurar la conexión de Active Directory para sincronizar usuarios y grupos, acceda a la página **Administración de acceso e identidad > Administrar > Proveedores de identidades** para agregar el proveedor de identidades externo para realizar la autenticación. 3 En el campo **Atributo de búsqueda de directorios**, seleccione el atributo de la cuenta que contiene el nombre de usuario. 4 Si Active Directory utiliza la búsqueda de ubicaciones de servicio de DNS, seleccione las opciones siguientes. ■ En la sección **Ubicación del servidor**, active la casilla **Este directorio admite la ubicación de servicio de DNS**. Se creará un archivo `domain_krb.properties` rellenado automáticamente con una lista de controladores de dominios cuando se cree el directorio. Consulte "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49 . ■ Si Active Directory requiere el cifrado STARTTLS, active la casilla **Este directorio requiere que todas las conexiones usen SSL** en la sección **Certificados**, copie el certificado de CA raíz de Active Directory y péguelo en el campo **Certificado SSL**. Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE". **NOTA:** Si Active Directory requiere STARTTLS y usted no proporciona el certificado, no podrá crear el directorio. 5 Si Active Directory no utiliza la búsqueda de ubicaciones de servicio de DNS, seleccione las opciones siguientes. ■ En la sección **Ubicación del servidor**, compruebe que la casilla **Este directorio admite la ubicación de servicio de DNS** no esté seleccionada y introduzca el número de puerto y el nombre de host del servidor de Active Directory. Para configurar el directorio como un catálogo global, consulte la sección Entorno de varios dominios y un único bosque de Active Directory de "Entornos de Active Directory," página 47. ■ Si Active Directory requiere acceso mediante SSL, active la casilla **Este directorio requiere que todas las conexiones usen SSL** en la sección **Certificados**, copie el certificado de CA raíz de Active Directory y péguelo en el campo **Certificado SSL**.

Opción	Descripción
	Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE". **NOTA:** Si Active Directory requiere SSL y usted no proporciona el certificado, no podrá crear el directorio. 6 En la sección **Permitir el cambio de contraseña**, seleccione **Habilitar el cambio de contraseña** si desea permitir a los usuarios que puedan restablecer sus contraseñas en la página de inicio de sesión de VMware Identity Manager en caso de que la contraseña caduque o si el administrador de Active Directory restablece la contraseña del usuario. 7 En el campo **DN base**, introduzca el DN desde el que deben empezar las búsquedas en cuentas. Por ejemplo, OU=myUnit,DC=myCorp,DC=com. 8 En el campo **DN de enlace**, introduzca la cuenta que puede buscar usuarios. Por ejemplo, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **NOTA:** Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque. 9 Después de introducir la contraseña de enlace, haga clic en **Probar conexión** para verificar que el directorio se puede conectar a Active Directory.
Active Directory (Autenticación de Windows integrada)	1 En el campo **Conector de sincronización**, seleccione el conector que desee utilizar para sincronizar usuarios y grupos de Active Directory con el directorio de VMware Identity Manager. De forma predeterminada, un componente del conector estará siempre disponible con el servicio de VMware Identity Manager. Este conector aparecerá en la lista desplegable. Si instala varios dispositivos de VMware Identity Manager para lograr una alta disponibilidad, el componente del conector de cada uno aparecerá en la lista. 2 En el campo **Autenticación**, haga clic en **Sí** si desea utilizar Active Directory para autenticar a los usuarios. Si desea utilizar un proveedor de identidades externo para autenticar a los usuarios, haga clic en **No**. Después de configurar la conexión de Active Directory para sincronizar usuarios y grupos, acceda a la página **Administración de acceso e identidad > Administrar > Proveedores de identidades** para agregar el proveedor de identidades externo para realizar la autenticación. 3 En el campo **Atributo de búsqueda de directorios**, seleccione el atributo de la cuenta que contiene el nombre de usuario. 4 Si Active Directory requiere el cifrado STARTTLS, active la casilla **Este directorio requiere que todas las conexiones usen STARTTLS** en la sección **Certificados**, copie el certificado de CA raíz de Active Directory y péguelo en el campo **Certificado SSL**. Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE". Si el directorio tiene varios dominios, agregue los certificados CA raíz para todos los dominios de uno en uno. **NOTA:** Si Active Directory requiere STARTTLS y usted no proporciona el certificado, no podrá crear el directorio. 5 Introduzca el nombre del dominio de Active Directory al que desea unirse. Introduzca un nombre de usuario y una contraseña que tenga los derechos para unirse al dominio. Consulte "Permisos necesarios para unir un dominio," página 54 para obtener más información.

Opción	Descripción
	6 En la sección **Permitir el cambio de contraseña**, seleccione **Habilitar el cambio de contraseña** si desea permitir a los usuarios que puedan restablecer sus contraseñas en la página de inicio de sesión de VMware Identity Manager en caso de que la contraseña caduque o si el administrador de Active Directory restablece la contraseña del usuario. 7 En el campo **UPN del usuario de enlace**, introduzca el nombre principal de usuario que puede autenticarse con el dominio. Por ejemplo nombredeusuario@ejemplo.com. **NOTA:** Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque. 8 Introduzca la contraseña de usuario de DN de enlace.

c Haga clic en **Guardar y Siguiente**.

Aparecerá la página con la lista de dominios.

14 En el caso de las directivas de LDAP, siga estos pasos.

a Proporcione la información de la conexión.

Opción	Descripción
Nombre de directorio	Un nombre para el directorio que está creando en VMware Identity Manager.
Sincronización de directorio y autenticación	1 En el campo **Conector de sincronización**, seleccione el conector que desee utilizar para sincronizar usuarios y grupos del directorio LDAP con el directorio de VMware Identity Manager. De forma predeterminada, un componente del conector estará siempre disponible con el servicio de VMware Identity Manager. Este conector aparecerá en la lista desplegable. Si instala varios dispositivos de VMware Identity Manager para lograr una alta disponibilidad, el componente del conector de cada uno aparecerá en la lista. No es necesario un conector diferente para un directorio LDAP. Un conector puede ser compatible con varios directorios, independientemente de si cuentan con directorios LDAP o Active Directory. 2 En el campo **Autenticación**, seleccione **Sí** si desea utilizar el directorio LDAP para autenticar a los usuarios. Si desea utilizar un proveedor de identidades externo para autenticar a los usuarios, seleccione **No**. Después de agregar la conexión del directorio para sincronizar usuarios y grupos, acceda a la página **Administración de acceso e identidad > Administrar > Proveedores de identidades** para agregar el proveedor de identidades externo para realizar la autenticación. 3 En el campo **Atributo de búsqueda de directorios**, especifique el atributo del directorio LDAP que se utiliza para el nombre de usuario. Si el atributo no aparece en la lista, seleccione **Personalizado** y escriba el nombre del atributo. Por ejemplo, **`cn`**.
Ubicación del servidor	Introduzca el número de puerto y el host del servidor del directorio LDAP. En el caso del host del servidor, puede especificar el nombre del dominio plenamente cualificado o la dirección IP. Por ejemplo, **`myLDAPserver.example.com`** o **`100.00.00.0`**. Si cuenta con un clúster de servidores bajo un equilibrador de carga, introduzca la información de este último en su lugar.
Configuración LDAP	Especifica los atributos y los filtros de búsqueda de LDAP que VMware Identity Manager puede utilizar para solicitar su directorio LDAP. Los valores predeterminados se proporcionan según el esquema principal de LDAP. **Solicitudes LDAP** ■ **Obtener grupos**: es el filtro de búsqueda para obtener los objetos de grupo. Por ejemplo: **`(objectClass=group)`** ■ **Obtener usuario de enlace**: es el filtro de búsqueda para obtener el objeto de usuario de enlace, es decir, al usuario que puede enlazarse al directorio. Por ejemplo: **`(objectClass=person)`** ■ **Obtener usuario**: es el filtro de búsqueda para obtener los usuarios para sincronizar. Por ejemplo:**`(&(objectClass=user)(objectCategory=person))`** **Atributos** ■ **Afiliación**: es el atributo que se utiliza en su directorio LDAP para definir los miembros de un grupo. Por ejemplo: **`member`**

Opción	Descripción
	■ **UUID del objeto**: es el atributo que se utiliza en su directorio LDAP para definir el UUID. Por ejemplo: **`entryUUID`** ■ **Nombre distintivo**: es el atributo que se utiliza en su directorio LDAP para definir el nombre distintivo de un usuario o un grupo. Por ejemplo: **`entryDN`**
Certificados	Si el directorio LDAP requiere acceso mediante SSL, seleccione la opción **Este directorio requiere que todas las conexiones usen SSL** y copie y pegue el certificado CA SSL raíz del servidor del directorio LDAP. Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE".
Detalles del usuario de enlace	**DN base**: introduzca el DN desde el que deben empezar las búsquedas. Por ejemplo, cn=users,dc=example,dc=com **DN de enlace**: introduzca el nombre del usuario que enlaza al directorio LDAP. **NOTA:** Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque. **Contraseña DN de enlace**: introduzca la contraseña del usuario DN de enlace.

b Para probar la conexión al servidor del directorio LDAP, haga clic en **Probar conexión**.

Si no se realizó la conexión correctamente, compruebe la información que introdujo y haga los cambios necesarios.

c Haga clic en **Guardar y Siguiente**.

Aparece la página con la lista del dominio.

15 En un directorio LDAP, el dominio aparece en la lista y no se puede modificar.

En Active Directory mediante LDAP, los dominios aparecen en la lista y no se pueden modificar.

Para Active Directory (Autenticación de Windows integrada), seleccione los dominios que deberán asociarse con esta conexión de Active Directory.

NOTA: Si agrega un dominio de confianza una vez creado el directorio, el servicio no detectará automáticamente el nuevo dominio de confianza. Para permitir que el servicio detecte el dominio, el conector deberá abandonar el dominio y, a continuación, volver a unirse a él. Una vez que el conector vuelva a unirse al dominio, el dominio de confianza aparecerá en la lista.

Haga clic en **Siguiente**.

16 Compruebe que los nombres de los atributos de VMware Identity Manager estén asignados a los atributos de Active Directory o LDAP correctos y realice los cambios que sean necesarios.

IMPORTANTE: Si integra un directorio LDAP, debe especificar una asignación para el atributo de **dominio**.

17 Haga clic en **Siguiente**.

18 Seleccione los grupos que desee sincronizar desde Active Directory o desde el directorio LDAP al directorio de VMware Identity Manager.

Opción	Descripción
Especificar los DN de grupo	Para seleccionar los grupos, especifique un DN o varios y seleccione los grupos que aparecen a continuación. a Haga clic en **+** y especifique el DN de grupo. Por ejemplo, CN=users,DC=example,DC=company,DC=com. **IMPORTANTE:** Especifique los DN de grupo que aparecen a continuación del DN base que introdujo. Si un DN de grupo aparece fuera del DN base, los usuarios de dicho DN se sincronizarán, pero no podrán iniciar sesión. b Haga clic en **Buscar grupos**. La columna **Grupos para sincronizar** muestra el número de grupos que se encuentran en el DN. c Para seleccionar todos los grupos en el DN, haga clic en **Seleccionar todo**, o bien haga clic en **Seleccionar** y seleccione los grupos específicos que desea sincronizar. **NOTA:** Si cuenta con varios grupos con el mismo nombre en su directorio LDAP, debe especificar nombres únicos para ellos en VMware Identity Manager. Puede cambiar el nombre al seleccionar el grupo. **NOTA:** Cuando sincroniza un grupo, los usuarios que no tengan Usuarios del dominio como su grupo principal en Active Directory no se sincronizan.
Sincronizar miembros de grupo anidados	La opción **Sincronizar miembros de grupo anidados** se habilita de forma predeterminada. Cuando se habilita esta opción, todos los usuarios que pertenezcan al grupo que seleccione y los que pertenezcan a grupos anidados dentro de este grupo se sincronizan. Tenga en cuenta que los grupos anidados no se sincronizan. Solo se sincronizarán los usuarios que pertenezcan a los grupos anidados. En el directorio de VMware Identity Manager, estos usuarios serán miembros del grupo de nivel principal que seleccionó para sincronizarse. Si deshabilita la opción **Sincronizar miembros de grupo anidados**, todos los usuarios que pertenezcan directamente a ese grupo se sincronizarán en el grupo que especificó. Los usuarios que pertenezcan a grupos anidados bajo este grupo no se sincronizarán. Deshabilitar esta opción resulta útil para las grandes configuraciones de Active Directory en las que atravesar un árbol de grupo requiera demasiado tiempo o demasiados recursos. Si deshabilita esta opción, asegúrese de que selecciona todos los grupos cuyos usuarios desee sincronizar.

19 Haga clic en **Siguiente**.

20 Especifique los usuarios adicionales que desea sincronizar, si es necesario.

a Haga clic en **+** e introduzca los DN del usuario. Por ejemplo, CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

IMPORTANTE: Especifique los DN de usuario que aparecen a continuación del DN base que introdujo. Si un DN de usuario aparece fuera del DN base, los usuarios de dicho DN se sincronizarán, pero no podrán iniciar sesión.

b (Opcional) Para excluir usuarios, cree un filtro que excluya algunos tipos de usuarios.

Debe seleccionar el atributo de usuario por el que desea filtrar, la regla de consulta y el valor.

21 Haga clic en **Siguiente**.

22 Revise la página para ver cuántos usuarios y grupos se sincronizarán con el directorio así como la programación de la sincronización.

   Para realizar cambios en los usuarios y los grupos o en la frecuencia de sincronización, haga clic en los vínculos **Editar**.

23 Haga clic en **Sincronizar directorio** para iniciar la sincronización del directorio.

NOTA: Si se produce un error en la red y el nombre del host no puede resolverse de forma única con una DNS inversa, el proceso de configuración se detendrá. Deberá resolver los problemas relacionados con la red y reiniciar el dispositivo virtual. A continuación, podrá continuar el proceso de implementación. La nueva configuración de la red no estará disponible hasta que reinicie el dispositivo virtual.

Qué hacer a continuación

Para obtener más información sobre cómo configurar un equilibrador de carga o sobre la configuración de alta disponibilidad, consulte Capítulo 6, "Configuración avanzada del dispositivo VMware Identity Manager," página 77.

Puede personalizar el catálogo de recursos de las aplicaciones de su organización y conceder a los usuarios acceso a estos recursos. También puede configurar otros recursos, como aplicaciones basadas en Citrix, View y ThinApp. Consulte *Configurar recursos en VMware Identity Manager*.

Configurar los valores del servidor proxy para VMware Identity Manager

El dispositivo virtual de VMware Identity Manager accede al catálogo de aplicaciones en la nube y a otros servicios web en Internet. Si su configuración de red proporciona acceso a Internet a través de un proxy HTTP, deberá ajustar la configuración del proxy en el dispositivo VMware Identity Manager.

Habilite su proxy para gestionar solo el tráfico de Internet. Para asegurar que el proxy esté configurado correctamente, establezca el parámetro de tráfico interno en la opción `no-proxy` dentro del dominio.

NOTA: Los servidores proxy que requieren autenticación no son compatibles.

Procedimiento

1 Desde vSphere Client, inicie la sesión como usuario root en el dispositivo virtual de VMware Identity Manager.

2 Introduzca `YaST` en la línea de comandos para ejecutar la utilidad `YaST`.

3 En el panel izquierdo, seleccione **Servicios de red** y, a continuación, **Proxy**.

4 Introduzca las URL del servidor proxy en los campos de **URL del proxy HTTP** y **URL del proxy HTTPS**.

5 Seleccione **Finalizar** y salga de la utilidad `YaST`.

6 Reinicie el servidor Tomcat en el dispositivo virtual de VMware Identity Manager para utilizar la nueva configuración del proxy.

```
service horizon-workspace restart
```

El catálogo de aplicaciones en la nube y otros servicios web ya están disponibles en VMware Identity Manager.

Introducir la clave de licencia

Después de implementar el dispositivo de VMware Identity Manager, introduzca la clave de licencia.

Procedimiento

1 Inicie la sesión en la consola de administración de VMware Identity Manager.

2 Seleccione la pestaña **Configuración de dispositivos** y haga clic en **Licencia**.

3 En la página Ajustes de licencia, introduzca la clave de licencia y haga clic en **Guardar**.

Administración de opciones de configuración del sistema del dispositivo

3

Una vez completada la configuración inicial del dispositivo, puede ir a las páginas de administración del mismo para instalar certificados, administrar contraseñas y supervisar información del sistema del dispositivo virtual.

Puede actualizar también la base de datos, el FQDN y el registro del sistema, así como descargar archivos de registro.

Nombre de la página	Descripción de la configuración
Conexión de la base de datos	La conexión a la base de datos, interna o externa, se encuentra habilitada. Puede cambiar el tipo de base de datos. Al seleccionar una base de datos externa, tiene que introducir una URL, un nombre de usuario y una contraseña. Para configurar una base de datos externa, consulte "Establecer conexión con la base de datos," página 34.
Instalar el certificado	Esta página permite instalar un certificado personalizado o autofirmado para VMware Identity Manager y, si VMware Identity Manager está configurado con un equilibrador de carga, puede instalar el certificado raíz del equilibrador de carga. La ubicación del certificado de CA raíz de VMware Identity Manager se muestra también en esta página, en la pestaña **Terminar SSL en un equilibrador de carga**. Consulte "Utilizar certificados SSL," página 38.
FQDN de Identity Manager	El FQDN de VMware Identity Manager se muestra en esta página. Puede cambiarlo si lo desea. El FQDN de VMware Identity Manager es la URL que emplean los usuarios para obtener acceso al servicio.
Configurar registro del sistema	En esta página, puede habilitar un servidor syslog externo. Los registros de VMware Identity Manager se envían a este servidor externo. Consulte "Habilitación del servidor syslog," página 42.
Cambiar contraseña	Esta página permite cambiar la contraseña del usuario admin de VMware Identity Manager.
Seguridad del sistema	Esta página permite cambiar la contraseña raíz del dispositivo VMware Identity Manager y la contraseña de usuario SSH usado para iniciar sesión de manera remota.
Ubicaciones de los archivos de registro	En esta página se muestra una lista de los archivos de registro y la ubicación de su directorio. Puede agrupar los archivos de registro en un archivo comprimido en formato zip para descargarlo. Consulte "Información del archivo de registro," página 42.

También puede modificar la URL del conector. Consulte "Modificar la URL del conector," página 41.

Este capítulo cubre los siguientes temas:

Cambiar ajustes de configuración del dispositivo

Después de configurar VMware Identity Manager, se puede acceder a las páginas de configuración de dispositivos para actualizar la configuración actual y supervisar la información del sistema del dispositivo virtual.

Procedimiento

1 Inicie sesión en la consola de administración.

2 Seleccione la pestaña **Configuración de dispositivos** y haga clic en **Administrar configuración**.

3 Inicie la sesión con la contraseña del administrador del servicio.

4 En el panel izquierdo, seleccione la página que desee ver o editar.

Qué hacer a continuación

Verifique que los cambios o actualizaciones realizados sean efectivos.

Establecer conexión con la base de datos

Una base de datos PostgreSQL interna está incrustada en el dispositivo VMware Identity Manager, aunque no se recomienda usarla para implementaciones de producción. Para utilizar una base de datos externa con VMware Identity Manager, el administrador de la base de datos debe preparar una base de datos y un esquema vacíos antes de establecer conexión con la base de datos de VMware Identity Manager.

Puede establecer conexión con la base de datos externa cuando ejecute el asistente de configuración de VMware Identity Manager. También puede acceder a Configuración de dispositivos > Configuración del dispositivo virtual > Configuración de la conexión de la base de datos para configurar la conexión con la base de datos externa.

Los usuarios con licencia pueden utilizar una base de datos externa de Oracle o Microsoft SQL Server para configurar un entorno de base de datos de alta disponibilidad.

Configurar una base de datos de Microsoft SQL

Para utilizar una base de datos de Microsoft SQL para VMware Identity Manager, debe crear una nueva base de datos en el servidor de Microsoft SQL.

Debe crear una base de datos llamada **saas** en el servidor de Microsoft SQL y crear un usuario de inicio de sesión llamado **horizon**.

NOTA: La intercalación predeterminada distingue mayúsculas de minúsculas.

Prerequisitos

- Versión compatible del servidor de Microsoft SQL instalada como un servidor de base de datos externa.
- Implementación de equilibrado de carga configurada.
- Derechos de administrador para crear los componentes de la base de datos y acceder a ellos utilizando Microsoft SQL Server Management Studio u otro cliente de CLI del servidor de Microsoft SQL.

Procedimiento

1 Inicie la sesión en Microsoft SQL Server Management Studio como administrador del sistema o con una cuenta con privilegios de administrador del sistema.

Se abrirá la ventana del editor.

2 En la barra de herramientas, haga clic en **Nueva consulta**.

3 Copie y pegue los comandos siguientes en la ventana del editor.

Comandos de Microsoft SQL

```
CREATE DATABASE saas
COLLATE Latin1_General_CS_AS;
ALTER DATABASE saas SET READ_COMMITTED_SNAPSHOT ON;
GO
BEGIN
CREATE LOGIN horizon WITH PASSWORD = N'H0rizon!';
END
GO
USE saas;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name = N'horizon')
DROP USER [horizon]
GO
CREATE USER horizon FOR LOGIN horizon
WITH DEFAULT_SCHEMA = saas;
GO
CREATE SCHEMA saas AUTHORIZATION horizon
GRANT ALL ON DATABASE::saas TO horizon;
GO
```

4 En la barra de herramientas, haga clic en **!Ejecutar**.

El servidor de base de datos de Microsoft SQL ya está preparado para conectarse a la base de datos de VMware Identity Manager

Qué hacer a continuación

Configure la base de datos externa en el servidor de VMware Identity Manager. Vaya a la consola de administración de VMware Identity Manager y acceda a la página Configuración de dispositivos > Configuración del dispositivo virtual > Configuración de la conexión de la base de datos. Introduzca la URL de JDBC como **`jdbc:sqlserver://<hostname-or-DB_VM_IP_ADDR>;DatabaseName=saas`**. Introduzca el nombre de usuario y la contraseña creados para la base de datos. Consulte "Configure VMware Identity Manager para usar una base de datos externa," página 37

Configurar una base de datos de Oracle

Durante la instalación de la base de datos de Oracle, se deberán especificar determinadas configuraciones de Oracle para conseguir un rendimiento óptimo con VMware Identity Manager.

Prerequisitos

La base de datos de Oracle que se cree se va a llamar `saas`. VMware Identity Manager requiere identificadores con comillas de Oracle para el nombre de usuario y el esquema. Por tanto, se deben utilizar dobles comillas al crear el nombre de usuario y el esquema en la base de datos `saas` de Oracle.

Procedimiento

1 Al crear la base de datos de Oracle, especifique los parámetros siguientes.

   a Seleccione la opción de configuración de la base de datos **Uso General/Procesamiento de Transacciones**.

   b Haga clic en la opción para utilizar **Unicode > UTF8**.

   c Utilice el conjunto de caracteres nacional.

2 Al finalizar la instalación, conéctese a la base de datos de Oracle.

3 Inicie la sesión en la base de datos de Oracle como usuario sys.

4 Aumente las conexiones de procesos. Cada máquina virtual de servicio adicional requiere un mínimo de 300 conexiones de procesos para funcionar con VMware Identity Manager. Por ejemplo, si su entorno dispone de dos máquinas virtuales de servicio, ejecute el comando `alter` como usuario sys o system.

   a Aumente las conexiones de procesos mediante el comando `alter`.

   ```
   alter system set processes=600 scope=spfile
   ```

   b Reinicie la base de datos.

5 Cree un activador de base de datos que puedan utilizar todos los usuarios.

SQL de ejemplo para crear un activador de base de datos

```
CREATE OR REPLACE
TRIGGER CASE_INSENSITIVE_ONLOGON
AFTER LOGON ON DATABASE
DECLARE
username VARCHAR2(30);
BEGIN
username:=SYS_CONTEXT('USERENV','SESSION_USER');
IF username = 'saas' THEN
execute immediate 'alter session set NLS_SORT=BINARY_CI';
execute immediate 'alter session set NLS_COMP=LINGUISTIC';
END IF;
EXCEPTION
WHEN OTHERS THEN
NULL;
END;
```

6 Ejecute los comandos de Oracle para crear un nuevo esquema de usuario.

SQL de ejemplo para crear un nuevo usuario

```
CREATE USER "saas"
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT
ACCOUNT UNLOCK;
GRANT RESOURCE TO "saas" ;
GRANT CONNECT TO "saas" ;
ALTER USER "saas" DEFAULT ROLE ALL;
GRANT UNLIMITED TABLESPACE TO "saas";
```

Administrar la base de datos interna

De forma predeterminada, la base de datos interna PostgreSQL está configurada y preparada para su uso. Tenga en cuenta que no se recomienda usar la base de datos interna para implementaciones de producción.

Cuando se instala y se conecta VMware Identity Manager, se genera una contraseña aleatoria para el usuario de la base de datos interna durante el proceso de inicialización. Esta contraseña es única para cada implementación y se puede encontrar en el archivo `/usr/local/horizon/conf/db.pwd`.

Si desea configurar su base de datos interna para lograr una alta disponibilidad, consulte el artículo 2094258 de la Base de conocimiento.

Configure VMware Identity Manager para usar una base de datos externa

Tras configurar la base de datos en el asistente de configuración de VMware Identity Manager, puede configurar VMware Identity Manager para utilizar otra base de datos.

Debe indicar a VMware Identity Manager una base de datos inicializada y con datos. Por ejemplo, puede utilizar una base de datos configurada como resultado de una ejecución correcta del asistente de configuración de VMware Identity Manager, una base de datos desde una copia de seguridad o una base de datos existente de una instantánea recuperada.

Prerequisitos

- Instale y configure la edición de Microsoft SQL u Oracle compatible como el servidor de base de datos externa. Para obtener información sobre versiones específicas compatibles con VMware Identity Manager, consulte las matrices de interoperabilidad de los productos de VMware en la página http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Procedimiento

1. En la consola de administración, haga clic en **Configuración de dispositivos** y seleccione **Configuración del dispositivo virtual**.
2. Haga clic en **Administrar configuración**.
3. Inicie sesión con la contraseña del administrador de VMware Identity Manager.
4. En la página Configuración de la conexión de la base de datos, seleccione **Base de datos externa** como tipo de base de datos.
5. Introduzca la información sobre la conexión de la base de datos.
   a. Escriba la URL de JDBC del servidor de la base de datos.

      Microsoft SQL `jdbc:sqlserver://nombre del host_o_dirección_IP;Nombre de la base de datos=horizon`

      Oracle `jdbc:oracle:thin:@//nombre del host_o_dirección_IP:puerto/sid`

   b. Escriba el nombre del usuario con privilegios de lectura y escritura en la base de datos.

      Microsoft SQL `horizon`

      Oracle `"saas"`

   c. Escriba la contraseña del usuario que creó cuando configuró la base de datos.
6. Haga clic en **Probar conexión** para verificar y guardar la información.

Utilizar certificados SSL

Al instalar el dispositivo VMware Identity Manager, se genera automáticamente un certificado de servidor SSL predeterminado. Este certificado autofirmado se puede utilizar para una comprobación general de la implementación. VMware recomienda encarecidamente generar e instalar certificados SSL comerciales en el entorno de producción.

Una autoridad de certificación (CA) es una entidad de confianza que garantiza la identidad del certificado y de su creador. Si un certificado está firmado por una CA de confianza, los usuarios dejan de recibir mensajes en los que se les pide que verifiquen el certificado.

Si se implementa VMware Identity Manager con el certificado SSL autofirmado, el certificado de CA raíz debe estar disponible como CA de confianza para todos los clientes que accedan a VMware Identity Manager. Los clientes pueden incluir equipos de usuarios finales, equilibradores de carga, servidores proxy, etc. La CA raíz se puede descargar de *https://myconnector.domain.com/horizon_workspace_rootca.pem*.

Los certificados de CA firmados se pueden instalar desde la página **Configuración de dispositivos > Administrar configuración > Instalar el certificado**. En esta página también se puede agregar el certificado de CA raíz del equilibrador de carga.

Aplicar una autoridad de certificación pública

Al instalar el servicio VMware Identity Manager, se genera un certificado de servidor SSL predeterminado. El certificado predeterminado se puede usar para hacer pruebas. Usted debe generar e instalar certificados SSL comerciales para su entorno.

NOTA: Si el VMware Identity Manager dirige a un equilibrador de carga, el certificado SSL se aplica al equilibrador de carga.

Prerequisitos

Genere una solicitud de firma del certificado (CSR) y obtenga un certificado válido y firmado de una autoridad de certificación. Si su organización proporciona certificados SSL firmados por una CA, podrá utilizar estos certificados. El certificado debe estar en formato PEM.

Procedimiento

1 En la consola de administración, haga clic en **Configuración de dispositivos**.

La pestaña Configuración del dispositivo virtual está seleccionada de manera predeterminada.

2 Haga clic en **Administrar configuración**.

3 En el cuadro de diálogo que se abrirá, introduzca la contraseña del usuario administrador del servidor de VMware Identity Manager.

4 Seleccione **Instalar el certificado**.

5 En la pestaña Terminar SSL en el dispositivo de Identity Manager, seleccione **Certificado personalizado**.

6 En el cuadro de texto **Cadena de certificados SSL**, pegue los certificados de host, intermedio y raíz, en ese orden.

El certificado SSL solo funciona si se incluye toda la cadena de certificados en el orden correcto. Para cada certificado, copie todo lo que hay entre las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE----, incluyendo estas líneas.

Asegúrese de que el certificado incluya el nombre de host de FQDN.

7 Pegue la clave privada en el cuadro de texto Clave privada. Copie todo entre ----BEGIN RSA PRIVATE KEY y ---END RSA PRIVATE KEY.

8 Haga clic en **Guardar**.

Ejemplo: Ejemplos de certificados

Ejemplo de cadena de certificados
-----BEGIN CERTIFICATE-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... ... W53+O05j5xsxzDJfWr1lqBlFF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Ejemplo de cadena de certificados
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... ... O05j5xsxzDJfWr1lqBlFF/OkIYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... ... 5j5xsxzDJfWr1lqW53+O0BlFF/OkIYCPcyK1
-----END CERTIFICATE-----

Ejemplo de clave privada
-----BEGIN RSA PRIVATE KEY-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+ ... ... 1lqBlFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----END RSA PRIVATE KEY-----

Adición de certificados SSL

Al aplicar el certificado, asegúrese de incluir la cadena de certificados completa. El certificado que se va a instalar debe estar en formato PEM.

El certificado SSL solo funciona si se incluye toda la cadena de certificados. Para cada certificado, copie todo lo que hay entre las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE----, incluyendo estas líneas.

IMPORTANTE: Debe agregar la cadena de certificados en el orden siguiente: certificado SSL, certificados de CA intermedios y certificado de CA raíz.

Ejemplo de cadena de certificados
-----BEGIN CERTIFICATE-----
Certificado SSL - Certificado SSL del dispositivo
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Certificado de CA emisora/Intermedio
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Certificado de CA raíz
-----END CERTIFICATE-----

Modificar la URL del servicio VMware Identity Manager

Es posible cambiar la URL del servicio VMware Identity Manager, que es la que utilizan los usuarios para acceder al servicio. Por ejemplo, se puede cambiar la URL por la de un equilibrador de carga.

Procedimiento

1 Inicie sesión en la consola de administración de VMware Identity Manager.

2 Haga clic en la pestaña **Configuración de dispositivos** y, a continuación, seleccione **Configuración del dispositivo virtual**.

3 Haga clic en **Administrar configuración** e inicie la sesión con la contraseña de usuario **`administrador`**.

4 Haga clic en **FQDN de Identity Manager** e introduzca la nueva URL en el campo **FQDN de Identity Manager**.

   Utilice el formato **`https://FQDN:port`**. La especificación del puerto es opcional. El puerto predeterminado es 443.

   Por ejemplo, **`https://miservicio.ejemplo.com`**.

5 Haga clic en **Guardar**.

Qué hacer a continuación

Habilite la nueva interfaz de usuario del portal.

1 Vaya a https://*VMwareIdentityManagerURL*/admin para acceder a la consola de administración.

2 En la consola de administración, haga clic en la flecha de la pestaña **Catálogo** y seleccione **Configuración**.

3 Seleccione **Nueva interfaz del portal de usuario final** en el panel de la izquierda y haga clic en **Habilitar nueva interfaz del portal**.

Modificar la URL del conector

Puede actualizar la URL del conector actualizando el nombre de host del proveedor de identidades en la consola de administración. Si utiliza el conector como proveedor de identidades, la URL es la de la página de inicio y los usuarios finales podrán verla.

Procedimiento

1 Inicie la sesión en la consola de administración de VMware Identity Manager.

2 Haga clic en la pestaña **Administración de acceso e identidad** y, a continuación, en la pestaña **Proveedores de identidades**.

3 En la página Proveedores de identidades, seleccione el proveedor de identidades que desee actualizar.

4 En el campo **Nombre de host de IdP**, introduzca el nuevo nombre de host.

   Utilice el formato **`nombre de host:puerto`**. La especificación del puerto es opcional. El puerto predeterminado es 443.

   Por ejemplo, **`vidm.ejemplo.com`**.

5 Haga clic en **Guardar**.

Habilitación del servidor syslog

Los eventos en el nivel de aplicaciones del servicio se pueden exportar a un servidor syslog externo. Los eventos del sistema operativo no se exportan.

Dado que la mayoría de empresas no disponen de espacio en disco ilimitado, el dispositivo virtual no guarda el historial de registro completo. Si desea guardar una cantidad de historial mayor o crear una ubicación centralizada para su historial de registro, puede configurar un servidor syslog externo.

Si no especifica un servidor syslog durante la configuración inicial, puede configurarlo más tarde en la página **Configuración de dispositivos > Configuración del dispositivo virtual > Administrar configuración > Configuración del Syslog**.

Prerequisitos

Configure un servidor syslog externo. Puede usar cualquiera de los servidores syslog estándar disponibles. Varios servidores syslog incluyen capacidades de búsqueda avanzada.

Procedimiento

1 Inicie sesión en la consola de administración.

2 Haga clic en la pestaña **Configuración de dispositivos**, seleccione **Configuración del dispositivo virtual** en el panel izquierdo y haga clic en **Administrar configuración**.

3 Seleccione **Configurar Syslog** en el panel izquierdo.

4 Haga clic en **Habilitar**.

5 Introduzca la dirección IP o el FQDN del servidor syslog donde desee almacenar los registros.

6 Haga clic en **Guardar**.

Se enviará una copia de sus registros al servidor del registro del sistema.

Información del archivo de registro

Los archivos de registro del VMware Identity Manager de pueden resultarle de ayuda para depurar errores y resolver problemas. Los archivos de registro que se enumeran a continuación son un punto de partida común. En el directorio `/opt/vmware/horizon/workspace/logs` encontrará registros adicionales.

Tabla 3-1. Archivos de registro

Componente	Ubicación del archivo de registro	Descripción
Registros del servicio de Identity Manager	`/opt/vmware/horizon/workspace/logs/horizon.log`	Información sobre la actividad en la aplicación VMware Identity Manager, como autorizaciones, usuarios y grupos.
Registros del configurador	`/opt/vmware/horizon/workspace/logs/configurator.log`	Solicitudes que recibe el configurador del cliente REST y de la interfaz web.
Registros del conector	`/opt/vmware/horizon/workspace/logs/connector.log`	Un registro de cada solicitud recibida desde la interfaz web. Cada entrada del registro incluye también la URL, la marca de hora y las excepciones de la solicitud. No se registra ninguna acción de sincronización.

Tabla 3-1. Archivos de registro (Continua)

Componente	Ubicación del archivo de registro	Descripción
Registros de actualización	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	Un registro de los mensajes de salida relacionados con las solicitudes de actualización durante una actualización de VMware Identity Manager. Los archivos del directorio `/opt/vmware/var/log/vami` son útiles para resolver problemas. Encontrará estos archivos en todas las máquinas virtuales después de una actualización.
Registros de Apache Tomcat	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat registra los mensajes que no se registran en otros archivos de registro.

Recopilar información de registro

Durante las pruebas o la resolución de problemas, los registros pueden proporcionar información sobre la actividad y el rendimiento del dispositivo virtual, así como información sobre los problemas que puedan ocurrir.

Puede recopilar los registros de cada uno de los dispositivos presentes en su entorno.

Procedimiento

1 Inicie la sesión en la consola de administración.

2 Seleccione la pestaña **Configuración de dispositivos** y haga clic en **Administrar configuración**.

3 Haga clic en **Ubicaciones de los archivos de registro** y en **Preparar paquete de registro**.

La información se recopila en un archivo tar.gz que se puede descargar.

4 Descargue el paquete preparado.

Qué hacer a continuación

Para recopilar todos los registros, haga esta operación con cada dispositivo.

Administración de contraseñas de dispositivo

Cuando configuró el dispositivo virtual, creó contraseñas para los usuarios admin, root y sshuser. Puede cambiar estas contraseñas en las páginas Configuración de dispositivos.

Asegúrese de crear contraseñas seguras. Las contraseñas seguras deben tener como mínimo ocho caracteres, estar formadas por mayúsculas y minúsculas e incluir al menos un número o un carácter especial.

Procedimiento

1 En la consola de administración, haga clic en la pestaña **Configuración de dispositivos**.

2 Haga clic en **Configuración del dispositivo virtual > Administrar configuración**.

3 Para cambiar la contraseña de administrador, seleccione **Cambiar contraseña**. Para cambiar las contraseñas de los usuarios root o sshuser, seleccione **Seguridad del sistema**.

IMPORTANTE: La contraseña del usuario admin debe tener 6 caracteres como mínimo.

4 Introduzca la nueva contraseña.

5 Haga clic en **Guardar**.

Configurar las opciones de SMTP

Configure el servidor SMTP para recibir notificaciones por correo electrónico desde el servicio de VMware Identity Manager.

Los correos electrónicos de notificación se envían a los nuevos usuarios que se crean como usuarios locales y cuando se restablece una contraseña en el servicio de VMware Identity Manager.

Procedimiento

1 Inicie sesión en la consola de administración.

2 Seleccione la pestaña **Configuración de dispositivos** y haga clic en **SMTP**.

3 Introduzca el nombre de host del servidor SMTP.

Por ejemplo: `smtp.example.com`

4 Introduzca el número de puerto del servidor SMTP.

Por ejemplo: `25`

5 (Opcional) Introduzca un nombre de usuario y una contraseña si el servidor SMTP requiere autenticación.

6 Haga clic en **Guardar**.

Integración con el directorio empresarial

4

Puede integrar VMware Identity Manager con el directorio empresarial para sincronizar usuarios y grupos del directorio empresarial al servicio de VMware Identity Manager.

Los siguientes tipos de directorios son compatibles.

- Active Directory mediante LDAP
- Active Directory, Autenticación de Windows integrada
- directorio LDAP

Realice las siguientes tareas para efectuar la integración con su directorio empresarial.

- Especifique los atributos que desea que tengan los usuarios en el servicio de VMware Identity Manager.
- Cree un directorio en el servicio de VMware Identity Manager del mismo tipo que el directorio empresarial y especifique los detalles de conexión.
- Asigne los atributos de VMware Identity Manager a los atributos utilizados en Active Directory o el directorio LDAP.
- Especifique los usuarios y los grupos que se sincronizan.
- Sincronice los usuarios y los grupos.

Después de integrar el directorio empresarial y realizar la sincronización inicial, puede actualizar la configuración, configurar una programación para que se sincronice de forma periódica o comenzar una sincronización en cualquier momento.

Este capítulo cubre los siguientes temas:

Conceptos importantes relacionados con la integración de directorios

Varios conceptos son esenciales para comprender cómo el servicio de VMware Identity Manager se integra con el entorno de Active Directory o del directorio LDAP.

Conector

El conector, un componente del servicio, realiza las siguientes funciones.

- Sincroniza en el servicio la información de los usuarios y los grupos desde Active Directory o el directorio LDAP.
- Cuando se usa como proveedor de identidades, autentica a los usuarios en el servicio.

  El conector es el proveedor de identidades predeterminado. También puede usar proveedores de identidades de terceros que admitan el protocolo SAML 2.0. Use un proveedor de identidades de terceros para un tipo de autenticación que el conector no admita o si el proveedor de identidades de terceros es preferible en función de la política de seguridad de su empresa.

  NOTA: Si usa proveedores de identidades de terceros, puede configurar el conector para que sincronice los datos de usuarios y grupos o puede configurar el aprovisionamiento de usuarios Just-in-Time. Consulte la sección Aprovisionamiento de usuarios Just-in-Time del tema sobre la *administración de VMware Identity Manager* para obtener más información.

Directorio

El servicio de VMware Identity Manager tiene su propio concepto de directorio, correspondiente a Active Directory o al directorio LDAP que se encuentra en su entorno. Este directorio utiliza atributos para definir los usuarios y los grupos. Se crean uno o varios directorios en el servicio y después se sincronizan con Active Directory o el directorio LDAP. Puede crear los siguientes tipos de directorio en el servicio.

- Active Directory
  - Active Directory a través de LDAP. Cree este tipo de directorio si va a conectarse a un solo entorno de dominio de Active Directory. Para el tipo de directorio Active Directory a través de LDAP, el conector se enlaza a Active Directory mediante la autenticación de enlace simple.
  - Active Directory, Autenticación de Windows integrada. Cree este tipo de directorio si va a conectarse a un entorno de Active Directory con varios dominios o bosques. El conector se enlaza a Active Directory mediante Autenticación de Windows integrada.

  El tipo y el número de directorios que cree varían según el entorno de Active Directory, es decir, con un solo dominio o con varios, y según el tipo de confianza usada entre los dominios. En la mayoría de los entornos, se crea un solo directorio.
- Directorio LDAP

El servicio no tiene acceso directo a Active Directory o al directorio LDAP. Solo el conector tiene acceso directo. Por tanto, se asocia cada directorio creado en el servicio con una instancia del conector.

Trabajo

Cuando se asocia un directorio a una instancia del conector, el conector crea una partición para el directorio asociado que se denomina trabajo. Una instancia del conector tiene varios trabajos asociados a ella. Cada trabajo actúa como proveedor de identidades. Se definen y configuran los métodos de autenticación para cada trabajo.

El conector sincroniza los datos de usuarios y grupos entre Active Directory o el directorio LDAP y el servicio a través de uno o varios trabajos.

IMPORTANTE: No puede tener dos trabajos del tipo Active Directory con Autenticación de Windows integrada en la misma instancia del conector.

Consideraciones de seguridad

Para los directorios empresariales integrados en el servicio de VMware Identity Manager, las opciones de seguridad, como las reglas de complejidad de la contraseña y las directivas de bloqueo de cuenta, se deben establecer directamente en el directorio empresarial. VMware Identity Manager no reemplaza estas opciones.

Integrar con Active Directory

Es posible integrar VMware Identity Manager con la implementación de Active Directory para sincronizar usuarios y grupos desde Active Directory a VMware Identity Manager.

Consulte también "Conceptos importantes relacionados con la integración de directorios," página 46.

Entornos de Active Directory

Es posible integrar el servicio con un entorno de Active Directory formado por un único dominio de Active Directory, varios dominios en un único bosque de Active Directory o varios dominios en varios bosques de Active Directory.

Entorno de dominio único de Active Directory

La implementación única de Active Directory permite sincronizar usuarios y grupos desde un único dominio de Active Directory.

Para este tipo de entorno, cuando añada un directorio al servicio, seleccione la opción Active Directory en LDAP.

Para obtener más información, consulte:

- "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49
- "Administrar atributos de usuario que se sincronizan desde Active Directory," página 53
- "Permisos necesarios para unir un dominio," página 54
- "Configurar la conexión de Active Directory con el servicio," página 55

Entorno de varios dominios y un único bosque de Active Directory

La implementación en varios dominios y un único bosque de Active Directory permite sincronizar usuarios y grupos desde varios dominios de Active Directory dentro de un único bosque.

Puede configurar el servicio para este tipo de entorno de Active Directory como un tipo de directorio único de Active Directory con Autenticación de Windows integrada o, si lo desea, como un tipo de directorio Active Directory en LDAP configurado con la opción de catálogo global.

- La opción que se recomienda es crear un tipo de directorio único de Active Directory con Autenticación de Windows integrada.

  Cuando añada un directorio a este entorno, seleccione la opción Active Directory (Autenticación de Windows integrada).

  Para obtener más información, consulte:

  - "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49

- "Administrar atributos de usuario que se sincronizan desde Active Directory," página 53
- "Permisos necesarios para unir un dominio," página 54
- "Configurar la conexión de Active Directory con el servicio," página 55

- Si la autenticación integrada en Windows (IWA, Integrated Windows Authentication) no funciona en su entorno Active Directory, cree un directorio del tipo Active Directory mediante LDAP y seleccione la opción de catálogo global.

  Entre las limitaciones que existen al seleccionar la opción de catálogo global se incluyen las siguientes:

  - Los atributos del objeto de Active Directory que se replican en el catálogo global se identifican en el esquema de Active Directory como un conjunto de atributos parcial (PAS, Partial Attribute Set). Solo estarán disponibles estos atributos para la asignación de atributos por parte del servicio. Si es necesario, edite el esquema para agregar o eliminar atributos que están almacenados en el catálogo global.
  - El catálogo global almacena la pertenencia a grupos (el atributo de miembro) únicamente de grupos universales. Solo los grupos universales se sincronizan con el servicio. Si es necesario, cambie el ámbito de un grupo de un dominio local o global a universal.
  - La cuenta de DN de enlace que defina al configurar un directorio en el servicio debe disponer de permisos de lectura sobre el atributo Token-Groups-Global-And-Universal (TGGAU).

  Active Directory usa los puertos 389 y 636 para consultas LDAP estándar. Para las consultas del catálogo global, se usan los puertos 3268 y 3269.

  Cuando agregue un directorio al entorno de catálogo global, especifique lo siguiente durante la configuración.

  - Seleccione la opción Active Directory mediante LDAP.
  - Anule la selección de la casilla correspondiente a la opción **Este directorio admite la ubicación de servicio de DNS**.
  - Seleccione la opción **Este directorio tiene un catálogo global**. Al seleccionar esta opción, el número de puerto del servidor cambia automáticamente a 3268. Además, y debido a que no se necesita el DN base para configurar la opción de catálogo global, no se mostrará el cuadro de texto DN base.
  - Agregue el nombre de host del servidor de Active Directory.
  - Si su Active Directory necesita acceder mediante SSL, seleccione la opción **Este directorio requiere que todas las conexiones usen SSL** y pegue el certificado en el cuadro de texto proporcionado. Al seleccionar esta opción, el número de puerto del servidor cambia automáticamente a 3269.

Entorno de varios bosques de Active Directory con relaciones de confianza

La implementación de varios bosques de Active Directory con relaciones de confianza permite sincronizar usuarios y grupos de varios dominios de Active Directory de diversos bosques entre los que exista una relación de confianza bidireccional.

Cuando añada un directorio a este entorno, seleccione la opción Active Directory (Autenticación de Windows integrada).

Para obtener más información, consulte:

- "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49
- "Administrar atributos de usuario que se sincronizan desde Active Directory," página 53
- "Permisos necesarios para unir un dominio," página 54
- "Configurar la conexión de Active Directory con el servicio," página 55

Entorno de varios bosques de Active Directory sin relaciones de confianza

La implementación de varios bosques de Active Directory sin relaciones de confianza permite sincronizar usuarios y grupos de varios dominios de Active Directory de diversos bosques sin la existencia de una relación de confianza entre los dominios. Para este tipo de entorno se crean varios directorios en el servicio, uno para cada bosque.

El tipo de directorios que se creen en el servicio dependerá del bosque. En el caso de bosques con varios dominios, seleccione la opción Active Directory (Autenticación de Windows integrada). En el caso de un bosque con un único dominio, seleccione la opción Active Directory en LDAP.

Para obtener más información, consulte:

- "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49
- "Administrar atributos de usuario que se sincronizan desde Active Directory," página 53
- "Permisos necesarios para unir un dominio," página 54
- "Configurar la conexión de Active Directory con el servicio," página 55

Acerca de la selección de controladores de dominio (archivo domain_krb.properties)

El archivo `domain_krb.properties` determina qué controladores de dominio se utilizarán para los directorios que tengan habilitada la búsqueda de ubicación del servicio DNS (registros SRV). Contiene una lista de controladores de dominio para cada dominio. El conector crea inicialmente el archivo, y posteriormente deberá mantenerlo usted. El archivo anula la búsqueda de ubicación del servicio DNS (SRV).

Los siguientes tipos de directorio tienen habilitada la búsqueda de ubicación del servicio DNS:

- Active Directory mediante LDAP con la opción **Este directorio admite la ubicación de servicio de DNS** seleccionada
- Active Directory (autenticación integrada de Windows), que tiene siempre habilitada la búsqueda de ubicación del servicio DNS

Al crear por primara vez un directorio que tenga habilitada la búsqueda de ubicación del servicio DNS, se creará automáticamente un archivo `domain_krb.properties` en el directorio `/usr/local/horizon/conf` de la máquina virtual, que se rellenará automáticamente con los controladores de dominio para cada dominio. Para rellenar el archivo, el conector intenta encontrar controladores de dominio que se encuentren en el mismo sitio que el conector y selecciona dos a los que se pueda acceder y que respondan más rápido.

Al crear directorios adicionales que tengan habilitada la ubicación del servicio DNS, o al agregar nuevos dominios a un directorio de autenticación integrada de Windows, los nuevos dominios se agregarán al archivo, junto con una lista de controladores de dominio para ellos.

Para anular en cualquier momento la selección predeterminada, edite el archivo `domain_krb.properties`. Después de crear un directorio, se recomienda revisar el archivo `domain_krb.properties` y verificar que los controladores de dominio indicados son los óptimos para esa configuración. En implementaciones globales de Active Directory con varios controladores de dominio en distintas ubicaciones geográficas, si se utiliza un controlador de dominio que esté muy próximo al conector se asegura una comunicación más rápida con Active Directory.

También se deben actualizar manualmente otros cambios en el archivo. Se aplican las siguientes reglas.

- El archivo `domain_krb.properties` se crea en la máquina virtual que contiene el conector. En una implementación típica, sin conectores adicionales, el archivo se crea en la máquina virtual del servicio VMware Identity Manager. Si se utiliza un conector adicional para el directorio, el archivo se crea en la máquina virtual del conector. Una máquina virtual solo puede tener un archivo `domain_krb.properties`.

- El archivo se crea y se rellena automáticamente con los controladores de dominio para cada dominio al crear por primera vez un directorio que tenga habilitada la búsqueda de ubicación del servicio DNS.
- Los controladores de dominio de cada dominio se indican en orden de prioridad. Para conectar a Active Directory, el conector intenta utilizar el primer controlador de dominio de la lista. Si no está accesible, lo intenta con el segundo de la lista, y así sucesivamente.
- El archivo solo se actualiza al crear un nuevo directorio que tenga habilitada la búsqueda de ubicación del servicio DNS, o bien al agregar un dominio a un directorio de autenticación integrada de Windows. El nuevo dominio y la lista de sus controladores de dominio se agregarán al archivo.

  Tenga en cuenta que si ya existe una entrada para un dominio en el archivo, no se actualizará. Por ejemplo, si se crea un directorio y se elimina a continuación, la entrada de dominio original permanece en el archivo y no se actualiza.
- El archivo no se actualiza automáticamente en ningún otro caso. Por ejemplo, si se elimina un directorio, la entrada de dominio no se elimina en el archivo.
- Si no se puede acceder a un controlador de dominio de la lista del archivo, edite el archivo y elimínelo.
- Si se agrega o elimina una entrada de dominio manualmente, los cambios no se sobrescribirán.

Para obtener información sobre cómo editar el archivo `domain_krb.properties`, consulte "Editar el archivo domain_krb.properties," página 51.

IMPORTANTE: El archivo `/etc/krb5.conf` debe ser coherente con el archivo `domain_krb.properties`. Cuando actualice el archivo `domain_krb.properties`, actualice también el archivo `krb5.conf`. Consulte "Editar el archivo domain_krb.properties," página 51 y el artículo 2091744 de la base de conocimientos para obtener más información.

Cómo se seleccionan controladores de dominio para rellenar automáticamente el archivo domain_krb.properties

Para seleccionar los controladores de dominio con los que rellenar automáticamente el archivo `domain_krb.properties`, se determina en primer lugar la subred en la que reside el conector (según la máscara de red y la dirección IP) y, a continuación, se utiliza la configuración de Active Directory para identificar el sitio de esa subred, se obtiene la lista de controladores de dominio para ese sitio, se filtra la lista para el dominio correspondiente y se eligen los dos controladores de dominio que respondan más rápido.

Para detectar los controladores de dominio que estén más próximos, VMware Identity Manager aplica los requisitos siguientes:

- La subred del conector debe estar presente en la configuración de Active Directory, o bien se debe especificar una subred en el archivo `runtime-config.properties`. Consulte "Anular la selección de subred predeterminada," página 51.

  La subred se utiliza para determinar el sitio.
- La configuración de Active Directory debe poder conocer el sitio.

Si no se puede determinar la subred, o si la configuración de Active Directory no permite conocer el sitio, se utilizará la búsqueda de ubicación del servicio DNS para encontrar controladores de dominio y el archivo se rellenará con algunos controladores de dominio accesibles. Tenga en cuenta que estos controladores de dominio pueden no estar en la misma ubicación geográfica que el conector, lo que puede ocasionar retardos o que se agote el tiempo de espera al comunicarse con Active Directory. En este caso, edite manualmente el archivo `domain_krb.properties` y especifique los controladores de dominio correctos que se deben utilizar para cada dominio. Consulte "Editar el archivo domain_krb.properties," página 51.

Archivo domain_krb.properties de ejemplo

```
example.com=host1.example.com:389,host2.example.com:389
```

Anular la selección de subred predeterminada

Para rellenar automáticamente el archivo `domain_krb.properties`, el conector intenta encontrar controladores de dominio situados en la misma ubicación, para que la latencia entre el conector y Active Directory sea mínima.

Para encontrar la ubicación, el conector determina la subred en la que reside, a partir de la dirección IP y la máscara de red, y utiliza entonces la configuración de Active Directory para identificar la ubicación de esa subred. Si la subred de la máquina virtual no está en Active Directory, o si se desea anular la selección automática de subred, se puede especificar una subred en el archivo `runtime-config.properties`.

Procedimiento

1 Inicie sesión en el dispositivo virtual VMware Identity Manager como usuario root.

NOTA: Si se utiliza un conector adicional para el directorio, inicie la sesión en la máquina virtual del conector.

2 Edite el archivo `/usr/local/horizon/conf/runtime-config.properties` para agregar el atributo siguiente.

`siteaware.subnet.override=`*`subnet`*

donde *subnet* es una subred de la ubicación cuyos controladores de dominio se desea utilizar. Por ejemplo:

`siteaware.subnet.override=10.100.0.0/20`

3 Guarde y cierre el archivo.

4 Reinicie el servicio.

```
service horizon-workspace restart
```

Editar el archivo domain_krb.properties

El archivo `/usr/local/horizon/conf/domain_krb.properties` determina qué controladores de dominio se utilizarán para los directorios que tengan habilitada la búsqueda de ubicación del servicio DNS. El archivo se puede editar en cualquier momento para modificar la lista de controladores de dominio de un dominio o para agregar o eliminar entradas de dominios. Los cambios no se sobrescribirán.

El archivo se creará y el conector lo rellenará automáticamente. En casos como los siguientes, se debe actualizar manualmente:

- Si los controladores de dominio seleccionados de forma predeterminada no son los ideales para la configuración, edite el archivo y especifique los controladores de dominio que se deben utilizar.
- Si se elimina un directorio, se debe eliminar la entrada del dominio correspondiente del archivo.
- Si alguno de los controladores de dominio no es accesible, se debe eliminar del archivo.

Consulte también "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49.

Procedimiento

1 Inicie sesión en la máquina virtual VMware Identity Manager como usuario root.

NOTA: Si se utiliza un conector adicional para el directorio, inicie la sesión en la máquina virtual del conector.

2 Cambie los directorios a `/usr/local/horizon/conf`.

3 Edite el archivo `domain_krb.properties` para agregar o editar la lista de valores de dominio a host.

Utilice el siguiente formato:

`domain=host:port,host2:port,host3:port`

Por ejemplo:

```
example.com=examplehost1.example.com:389,examplehost2.example.com:389
```

Indique los controladores de dominio en orden de prioridad. Para conectar a Active Directory, el conector intenta utilizar el primer controlador de dominio de la lista. Si no está accesible, lo intenta con el segundo de la lista, y así sucesivamente.

IMPORTANTE: Los nombres de dominio debes estar en minúsculas.

4 Cambie el propietario del archivo `domain_krb.properties` a `horizon` y el grupo a `www` mediante el comando siguiente.

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

5 Reinicie el servicio.

```
service horizon-workspace restart
```

Qué hacer a continuación

Después de editar el archivo `domain_krb.properties`, edite el archivo `/etc/krb5.conf`. El archivo `krb5.conf` debe ser coherente con el archivo `domain_krb.properties`.

1 Edite el archivo `/etc/krb5.conf` y actualice la sección `realms` para especificar los mismos valores de dominio a host que se utilizan en el archivo `/usr/local/horizon/conf/domain_krb.properties`. No es necesario especificar el número de puerto. Por ejemplo, si el archivo `domain_krb.properties` tiene la entrada de dominio `example.com=examplehost.example.com:389`, debería actualizar el archivo `krb5.conf` a los siguientes valores.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

NOTA: Es posible tener varias entradas kdc, aunque no es un requisito, ya que en muchos casos solo hay un único valor kdc. Si decide definir valores kdc adicionales, cada línea tendrá una entrada kdc que definirá un controlador de dominio.

2 Reinicie el servicio del área de trabajo.

```
service horizon-workspace restart
```

Consulte el artículo 2091744 de la Base de conocimientos.

Resolver problemas del archivo domain_krb.properties

Utilice la información siguiente para resolver problemas del archivo `domain_krb.properties`.

Error al resolver el dominio

Si el archivo `domain_krb.properties` ya incluye una entrada de un dominio y se intenta crear un nuevo directorio de otro tipo para el mismo dominio, se producirá un error al resolver el dominio. Se debe editar el archivo `domain_krb.properties` y eliminar manualmente la entrada del dominio antes de crear el nuevo directorio.

No se puede acceder a los controladores de dominio

Después de agregar una entrada de dominio al archivo `domain_krb.properties`, no se actualiza automáticamente. Si no se puede acceder a alguno de los controladores de dominio de la lista del archivo, edite el archivo manualmente y elimínelo.

Administrar atributos de usuario que se sincronizan desde Active Directory

Durante la configuración del directorio del servicio de VMware Identity Manager, selecciona los filtros y atributos del usuario de Active Directory para especificar los usuarios que se sincronizan en el directorio de VMware Identity Manager. Puede cambiar los atributos de usuario que se sincronizan en la consola de administración, pestaña Administración de acceso e identidades, Configurar > Atributos de usuario.

Los cambios que se realizan y guardan en la página Atributos de usuario se añaden a la página Atributos asignados en el directorio de VMware Identity Manager. Los cambios en los atributos se actualizan en el directorio durante la siguiente sincronización con Active Directory.

En la página Atributos de usuario, se muestran los atributos de directorio predeterminados que se pueden asignar a atributos de Active Directory. Seleccione los atributos que sean obligatorios; también puede agregar otros atributos de Active Directory que desee para sincronizarlos con el directorio. Al agregar atributos, tenga en cuenta que el nombre de atributo que introduzca distingue entre mayúsculas y minúsculas. Por ejemplo, dirección, Dirección y DIRECCIÓN son atributos diferentes.

Tabla 4-1. Atributos de Active Directory predeterminados para sincronizar con el directorio

Nombre de atributo de directorio de VMware Identity Manager	Asignación predeterminada al atributo de Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Añade el nombre de dominio completo del objeto.
disabled (usuario externo deshabilitado)	userAccountControl. Marcado con UF_Account_Disable Cuando se deshabilita una cuenta, los usuarios no pueden iniciar sesión en sus aplicaciones ni en sus recursos. Los recursos para los que los usuarios tienen autorización no se quitan de la cuenta para que, cuando se quite la marca de la cuenta, puedan iniciar sesión y acceder a los recursos autorizados.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName.

Seleccionar atributos para sincronizar con el directorio

Al configurar el directorio de VMware Identity Manager para sincronizar con Active Directory, se especifican los atributos de usuario que se sincronizan con el directorio. Antes de configurar el directorio, puede especificar en la página Atributos de usuario qué atributos predeterminados son obligatorios y añadir otros adicionales que desee asignar a atributos de Active Directory.

Cuando configura la página Atributos de usuario antes de que se cree el directorio, puede cambiar los atributos predeterminados de obligatorios a no obligatorios, marcar atributos como obligatorios y añadir atributos personalizados.

Una vez creado el directorio, puede convertir un atributo obligatorio en no obligatorio, y puede eliminar atributos personalizados. No se puede convertir un atributo en atributo obligatorio.

Cuando añada otros atributos para que se sincronicen con el directorio, una vez creado el directorio, vaya a la página Atributos asignados del directorio para asignar estos atributos a atributos de Active Directory.

IMPORTANTE: Si va a sincronizar recursos de XenApp con VMware Identity Manager, debe convertir **distinguishedName** en atributo obligatorio. Debe especificar esto antes de crear el directorio de VMware Identity Manager.

Procedimiento

1 En la pestaña Administración de acceso e identidades de la consola de administración, seleccione **Configuración > Atributos de usuario**.

2 En la sección Atributos predeterminados, repase la lista de atributos obligatorios y realice los cambios necesarios para reflejar cuáles deben serlo.

3 En la sección Atributos, añada el nombre de atributo de directorio de VMware Identity Manager a la lista.

4 Haga clic en **Guardar**.

Se actualiza el estado de atributo predeterminado y los atributos que añadió se incorporan a la lista Atributos asignados del directorio.

5 Tras la creación del directorio, vaya a la página **Administrar > Directorios** y seleccione el directorio.

6 Haga clic en **Configuración de sincronización > Atributos asignados**.

7 En el menú desplegable de los atributos que haya añadido, seleccione el atributo de Active Directory al que realizar la asignación.

8 Haga clic en **Guardar**.

El directorio se actualizará la próxima vez que se sincronice con Active Directory.

Permisos necesarios para unir un dominio

En algunos casos, puede que necesite unir el conector de VMware Identity Manager a un dominio. Para directorios Active Directory mediante LDAP, puede unirse a un dominio después de crear el directorio. Para directorios del tipo Active Directory (autenticación IWA), el conector se une automáticamente al dominio al crear el directorio. En ambos casos se le pedirán las correspondientes credenciales.

Para unirse a un dominio, necesita credenciales de Active Directory con el privilegio para "unir el equipo al dominio de AD". Esto se configura en Active Directory con los derechos siguientes:

- Crear objetos de equipo
- Eliminar objetos de equipo

Al unir un dominio se crea un objeto de equipo en la ubicación predeterminada en Active Directory, a menos que especifique una unidad organizativa personalizada.

Siga los siguientes pasos si no cuenta con los derechos necesarios para unirse a un dominio y desea realizar este proceso.

1 Pida a su administrador de Active Directory que cree el objeto de equipo en Active Directory, en una ubicación determinada por la directiva de la empresa. Proporcione el nombre de host del conector. Asegúrese de que proporciona el nombre de dominio plenamente cualificado, como `servidor.ejemplo.com`.

Tip Puede consultar el nombre de host en la columna **Nombre de host** de la página Conectores de la consola de administración. Haga clic en **Administración de acceso e identidad > Configurar > Conectores** para abrir la página Conectores.

2 Después de crear el objeto de equipo, únase al dominio mediante cualquier cuenta de usuario del dominio en la consola de administración de VMware Identity Manager.

El comando **Unirse al dominio** está disponible en la página **Conectores**; para obtener acceso a ella, haga clic en **Administración de acceso e identidad > Configurar > Conectores**.

Opción	Descripción
Dominio	Seleccione o introduzca el dominio de Active Directory que desee unir. Compruebe que introduce el nombre de dominio completo. Por ejemplo: **servidor.ejemplo.com**.
Usuario de dominio	El nombre de un usuario de Active Directory que tenga derecho para unir sistemas al dominio de Active Directory.
Contraseña de dominio	La contraseña del usuario.
Unidad organizativa (OU)	(Opcional) La unidad organizativa (OU) del objeto del equipo. Esta opción crea un objeto de equipo en la unidad organizativa especificada en lugar de la predeterminada del equipo. Por ejemplo, **ou=testou,dc=test,dc=example,dc=com**.

Configurar la conexión de Active Directory con el servicio

En la consola de administración, especifique la información necesaria para conectar con Active Directory y seleccionar usuarios y grupos para sincronizar con el directorio de VMware Identity Manager.

Las opciones de conexión de Active Directory son mediante LDAP o mediante la autenticación integrada de Windows de Active Directory. La conexión de Active Directory mediante LDAP es compatible con la búsqueda de ubicación del servicio DNS. Con la autenticación integrada de Windows de Active Directory es necesario configurar el dominio al que se unirá.

Prerequisitos

- Seleccione los atributos necesarios y agregue atributos adicionales, en caso de que sea necesario, en la página Atributos de usuario. Consulte "Seleccionar atributos para sincronizar con el directorio," página 54.

  IMPORTANTE: Si va a sincronizar recursos de XenApp con VMware Identity Manager, debe convertir **distinguishedName** en atributo obligatorio. Debe realizar esta selección antes de crear un directorio, ya que los atributos no se pueden cambiar para que sean obligatorios después de crear el directorio.

- Lista de grupos y usuarios de Active Directory para sincronizar desde Active Directory.

- Para Active Directory mediante LDAP, la información necesaria incluye DN base, DN de enlace y contraseña de DN de enlace.

  NOTA: Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque.

- Para la Autenticación de Windows integrada de Active Directory, la información necesaria incluye la dirección UPN del usuario de enlace del dominio y la contraseña.

  NOTA: Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque.

- Si Active Directory necesita que el acceso sea mediante SSL o STARTTLS, se requerirá el certificado de CA raíz del controlador de dominio de Active Directory.
- Para la Autenticación de Windows integrada de Active Directory, cuando se tiene configurado Active Directory con varios bosques y el grupo local de dominios contiene miembros de dominios de diferentes bosques, asegúrese de que el usuario de enlace se añada al grupo de Administradores del dominio en el que reside el grupo local de dominios. De lo contrario, estos miembros no estarán en el grupo local de dominios.

Procedimiento

1 En la consola de administración, haga clic en la pestaña **Administración de acceso e identidad**.

2 En la página Directorios, haga clic en **Agregar directorio**.

3 Introduzca un nombre para este directorio de VMware Identity Manager.

4 Seleccione el tipo de Active Directory de su entorno y configure la información de conexión.

Opción	Descripción
Active Directory mediante LDAP	a En el campo **Conector de sincronización**, seleccione el conector que se utilizará para sincronizar con Active Directory. b En el campo **Autenticación**, si se utiliza este Active Directory para autenticar usuarios, haga clic en **Sí**. Si se utiliza otro proveedor para autenticar usuarios, haga clic en **No**. Después de configurar la conexión de Active Directory para sincronizar usuarios y grupos, acceda a la página Administración de acceso e identidad > Administrar > Proveedores de identidades para agregar el proveedor de identidades externo para la autenticación. c En el campo **Atributo de búsqueda de directorios**, seleccione el atributo de la cuenta que contiene el nombre de usuario. d Si Active Directory utiliza la búsqueda de ubicaciones de servicio de DNS, seleccione las opciones siguientes. ■ En la sección **Ubicación del servidor**, active la casilla **Este directorio admite la ubicación de servicio de DNS**. Se creará un archivo `domain_krb.properties` rellenado automáticamente con una lista de controladores de dominios cuando se cree el directorio. Consulte "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49 . ■ Si Active Directory requiere el cifrado STARTTLS, active la casilla **Este directorio requiere que todas las conexiones usen SSL** en la sección **Certificados**, copie el certificado de CA raíz de Active Directory y péguelo en el campo **Certificado SSL**. Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE". **NOTA:** Si Active Directory requiere STARTTLS y usted no proporciona el certificado, no podrá crear el directorio. e Si Active Directory no utiliza la búsqueda de ubicaciones de servicio de DNS, seleccione las opciones siguientes. ■ En la sección **Ubicación del servidor**, compruebe que la casilla **Este directorio admite la ubicación de servicio de DNS** no esté seleccionada y introduzca el número de puerto y el nombre de host del servidor de Active Directory. Para configurar el directorio como un catálogo global, consulte la sección Entorno de varios dominios y un único bosque de Active Directory de "Entornos de Active Directory," página 47. ■ Si Active Directory requiere acceso mediante SSL, active la casilla **Este directorio requiere que todas las conexiones usen SSL** en la sección **Certificados**, copie el certificado de CA raíz de Active Directory y péguelo en el campo **Certificado SSL**.

Opción	Descripción
	Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE". **NOTA:** Si Active Directory requiere SSL y usted no proporciona el certificado, no podrá crear el directorio. f En el campo **DN base**, introduzca el DN desde el que deben empezar las búsquedas en cuentas. Por ejemplo, OU=myUnit,DC=myCorp,DC=com. g En el campo **DN de enlace**, introduzca la cuenta que puede buscar usuarios. Por ejemplo, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **NOTA:** Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque. h Después de introducir la contraseña de enlace, haga clic en **Probar conexión** para verificar que el directorio se puede conectar a Active Directory.
Active Directory (Autenticación de Windows integrada)	a En el campo **Conector de sincronización**, seleccione el conector que se utilizará para sincronizar con Active Directory. b En el campo **Autenticación**, si se utiliza este Active Directory para autenticar usuarios, haga clic en **Sí**. Si se utiliza otro proveedor para autenticar usuarios, haga clic en **No**. Después de configurar la conexión de Active Directory para sincronizar usuarios y grupos, acceda a la página Administración de acceso e identidad > Administrar > Proveedores de identidades para agregar el proveedor de identidades externo para la autenticación. c En el campo **Atributo de búsqueda de directorios**, seleccione el atributo de la cuenta que contiene el nombre de usuario. d Si Active Directory requiere el cifrado STARTTLS, active la casilla **Este directorio requiere que todas las conexiones usen STARTTLS** en la sección **Certificados**, copie el certificado de CA raíz de Active Directory y péguelo en el campo **Certificado SSL**. Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE". Si el directorio tiene varios dominios, agregue los certificados CA raíz para todos los dominios de uno en uno. **NOTA:** Si Active Directory requiere STARTTLS y usted no proporciona el certificado, no podrá crear el directorio. e Introduzca el nombre del dominio de Active Directory al que desea unirse. Introduzca un nombre de usuario y una contraseña que tenga los derechos para unirse al dominio. Consulte "Permisos necesarios para unir un dominio," página 54 para obtener más información. f En el campo Dirección UPN de usuario de enlace, escriba el nombre principal del usuario que podrá autenticarse en el dominio. Por ejemplo nombredeusuario@ejemplo.com. **NOTA:** Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque. g Escriba la contraseña del usuario de enlace.

5 Haga clic en **Guardar y Siguiente**.

Aparecerá la página con la lista de dominios.

6 En Active Directory mediante LDAP, los dominios aparecen con una marca de verificación.

Para Active Directory (Autenticación de Windows integrada), seleccione los dominios que deberán asociarse con esta conexión de Active Directory.

NOTA: Si añade un dominio de confianza una vez creado el directorio, el servicio no detectará automáticamente el nuevo dominio de confianza. Para permitir que el servicio detecte el dominio, el conector deberá abandonar el dominio y, a continuación, volver a unirse a él. Una vez que el conector vuelva a unirse al dominio, el dominio de confianza aparecerá en la lista.

Haga clic en **Siguiente**.

7 Verifique que los nombres de los atributos del directorio VMware Identity Manager están asignados a los atributos de Active Directory correctos, realice los cambios necesarios y haga clic en **Siguiente**.

8 Seleccione los grupos que desee sincronizar desde Active Directory al directorio de VMware Identity Manager.

Opción	Descripción
Especificar los DN de grupo	Para seleccionar los grupos, especifique un DN o varios y seleccione los grupos que aparecen a continuación. a Haga clic en **+** y especifique el DN de grupo. Por ejemplo, CN=users,DC=example,DC=company,DC=com. **IMPORTANTE:** Especifique los DN de grupo que aparecen a continuación del DN base que introdujo. Si un DN de grupo aparece fuera del DN base, los usuarios de dicho DN se sincronizarán, pero no podrán iniciar sesión. b Haga clic en **Buscar grupos**. La columna **Grupos para sincronizar** muestra el número de grupos que se encuentran en el DN. c Para seleccionar todos los grupos en el DN, haga clic en **Seleccionar todo**, o bien haga clic en **Seleccionar** y seleccione los grupos específicos que desea sincronizar. **NOTA:** Cuando sincroniza un grupo, los usuarios que no tengan Usuarios del dominio como su grupo principal en Active Directory no se sincronizan.
Sincronizar miembros de grupo anidados	La opción **Sincronizar miembros de grupo anidados** se habilita de forma predeterminada. Cuando se habilita esta opción, todos los usuarios que pertenezcan al grupo que seleccione y los que pertenezcan a grupos anidados dentro de este grupo se sincronizan. Tenga en cuenta que los grupos anidados no se sincronizan. Solo se sincronizarán los usuarios que pertenezcan a los grupos anidados. En el directorio de VMware Identity Manager, estos usuarios serán miembros del grupo de nivel principal que seleccionó para sincronizarse. Si deshabilita la opción **Sincronizar miembros de grupo anidados**, todos los usuarios que pertenezcan directamente a ese grupo se sincronizarán en el grupo que especificó. Los usuarios que pertenezcan a grupos anidados bajo este grupo no se sincronizarán. Deshabilitar esta opción resulta útil para las grandes configuraciones de Active Directory en las que atravesar un árbol de grupo requiera demasiado tiempo o demasiados recursos. Si deshabilita esta opción, asegúrese de que selecciona todos los grupos cuyos usuarios desee sincronizar.

9 Haga clic en **Siguiente**.

10 Especifique los usuarios adicionales que desea sincronizar, si es necesario.

a Haga clic en **+** e introduzca los DN del usuario. Por ejemplo, CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

IMPORTANTE: Especifique los DN de usuario que aparecen a continuación del DN base que introdujo. Si un DN de usuario aparece fuera del DN base, los usuarios de dicho DN se sincronizarán, pero no podrán iniciar sesión.

b (Opcional) Para excluir usuarios, cree un filtro que excluya algunos tipos de usuarios.

Debe seleccionar el atributo de usuario por el que desea filtrar, la regla de consulta y el valor.

11 Haga clic en **Siguiente**.

12 Revise la página para ver cuántos usuarios y grupos se sincronizan en el directorio y la programación de sincronización.

Para realizar cambios en los usuarios y los grupos o en la frecuencia de sincronización, haga clic en los vínculos **Editar**.

13 Haga clic en **Sincronizar directorio** para iniciar la sincronización.

Se establece la conexión con Active Directory y los usuarios y los grupos se sincronizan desde Active Directory al directorio VMware Identity Manager. El usuario de DN de enlace tiene una función de administrador en VMware Identity Manager de forma predeterminada.

Qué hacer a continuación

- Si se creó un directorio compatible con la ubicación del servicio DNS, se creará un archivo `domain_krb.properties` que se rellenará con una lista de controladores de dominio. Consulte el archivo para verificar o editar la lista de controladores de dominio. Consulte "Acerca de la selección de controladores de dominio (archivo domain_krb.properties)," página 49.
- Configure los métodos de autenticación. Una vez sincronizados los usuarios y grupos con el directorio, si también se utiliza el conector para la autenticación, podrá configurar otros métodos de autenticación en este último. Si el proveedor de identidades de autenticación es un tercero, configúrelo en el conector.
- Revise la política de acceso predeterminada. La política de acceso predeterminada se configura para permitir que todos los dispositivos de todos los rangos de redes accedan al explorador web, con un tiempo de espera de sesión definido en ocho horas, o bien acceder a una aplicación del cliente con un tiempo de espera de sesión de 2.160 horas (90 días). Puede cambiar la política de acceso predeterminada. Asimismo, cuando añada aplicaciones web al catálogo, podrá crear otras nuevas.
- Aplique la personalización de marca a la consola de administración, a las páginas del portal de usuario y a la pantalla de inicio de sesión.

Permitir a los usuarios cambiar las contraseñas de Active Directory

Puede proporcionar a los usuarios la capacidad de cambiar las contraseñas de Active Directory desde la aplicación o el portal de Workspace ONE cuando lo deseen. Los usuarios también pueden restablecer sus contraseñas de Active Directory desde la página de inicio de sesión de VMware Identity Manager si la contraseña caducó o si el administrador de Active Directory restableció la contraseña, lo cual obliga al usuario a cambiarla en el siguiente inicio de sesión.

Puede habilitar esta opción por directorios, al seleccionar **Permitir el cambio de contraseña** en la página de Configuración del directorio.

Los usuarios puede cambiar sus contraseñas cuando inician sesión en el portal de Workspace ONE al hacer clic en el nombre situado en la esquina superior derecha, seleccionar **Cuenta** en el menú desplegable y hacer clic en el vínculo **Cambiar contraseña**. En la aplicación Workspace ONE, los usuarios pueden cambiar las contraseñas al hacer clic en el icono de menú de barra triple y seleccionar **Contraseña**.

Las contraseñas caducadas o restablecidas por el administrador en Active Directory se pueden cambiar desde la página de inicio de sesión. Cuando un usuario intenta iniciar sesión con una contraseña caducada, se le solicita que restablezca la contraseña. El usuario debe introducir la contraseña anterior así como la nueva.

La directiva de contraseñas de Active Directory determina los requisitos para la nueva contraseña. El número de intentos permitidos también depende de la directiva de contraseñas de Active Directory.

Se aplican las siguientes limitaciones.

- Si usa dispositivos virtuales adicionales independientes del conector, tenga en cuenta que la opción **Permitir el cambio de contraseña** solo está disponible con la versión 2016.11.1 y posteriores del conector.
- Cuando se agrega un directorio a VMware Identity Manager como catálogo global, la opción **Permitir el cambio de contraseña** no está disponible. Los directorios se pueden agregar como Active Directory mediante LDAP o la autenticación integrada de Windows, a través de los puertos 389 o 636.
- La contraseña de un usuario DN de enlace no puede restablecerse desde VMware Identity Manager, aunque caduque o el administrador de Active Directory la restablezca.

  NOTA: Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque.

- Las contraseñas de los usuarios cuyos nombres de inicio de sesión contengan caracteres multibyte (caracteres que no son ASCII) no se pueden restablecer desde VMware Identity Manager.

Prerequisitos

- El puerto 464 debe estar abierto desde VMware Identity Manager hasta los controladores de dominio.

Procedimiento

1. En la consola de administración, haga clic en la pestaña **Administración de acceso e identidad**.
2. En la página **Directorios**, haga clic en el directorio.
3. En la sección **Permitir el cambio de contraseña**, seleccione la casilla de verificación **Habilitar el cambio de contraseña**.
4. Habilitar la contraseña DN de enlace en la sección **Detalles del usuario de enlace** y haga clic en **Guardar**.

Integrar los directorios LDAP

Es posible integrar el directorio LDAP de su empresa en VMware Identity Manager para sincronizar usuarios y grupos del directorio LDAP en el servicio VMware Identity Manager.

Consulte también "Conceptos importantes relacionados con la integración de directorios," página 46.

Limitaciones de la integración del directorio LDAP

Las siguientes limitaciones se aplican a la función de integración en el directorio LDAP.

- Solo puede integrar un entorno del directorio LDAP con un dominio único.

  Para integrar varios dominios desde un directorio LDAP, necesita crear directorios de VMware Identity Manager adicionales, uno para cada dominio.

- Los siguientes métodos de autenticación no son compatibles para los directorios de VMware Identity Manager de tipo LDAP.
  - autenticación de Kerberos

  - Autenticación adaptativa de RSA
  - ADFS como proveedor de identidades externo
  - SecurID
  - Autenticación de Radius con el servidor de código de acceso SMS y Vasco
- No puede unirse a un dominio LDAP.
- La integración a los recursos publicados por Citrix o de View no es compatible para los directorios de VMware Identity Manager de tipo LDAP.
- Los nombres de usuario no deben tener espacios. Si un nombre de usuario tiene un espacio, el usuario se sincroniza pero las autorizaciones no están disponibles para dicho usuario.
- Si tiene previsto agregar los directorios LDAP y Active Directory, asegúrese de que no marca ningún atributo obligatorio en la página Atributo de usuario, excepto userName, que puede ser obligatorio que se marque. Las configuraciones de la página Atributos de usuario se aplican a todos los directorios del servicio. Si un atributo está marcado como obligatorio, los usuarios sin dicho atributo no se sincronizan con el servicio de VMware Identity Manager.
- Si cuenta con varios grupos con el mismo nombre en su directorio LDAP, debe especificar nombres únicos para ellos en el servicio de VMware Identity Manager. Puede especificar los nombres cuando selecciona los grupos que desea sincronizar.
- La opción para permitir a los usuarios restablecer las contraseñas caducadas no está disponible.
- No es compatible el archivo `domain_krb.properties`.

Integrar un directorio LDAP en el servicio

Es posible integrar el directorio LDAP de su empresa en VMware Identity Manager para sincronizar usuarios y grupos del directorio LDAP en el servicio VMware Identity Manager.

Para integrar el directorio LDAP, cree el directorio VMware Identity Manager correspondiente y sincronice los usuarios y los grupos del directorio LDAP al directorio VMware Identity Manager. Puede programar una sincronización periódica para las actualizaciones siguientes.

Seleccione también los atributos LDAP que quiera sincronizar para los usuarios y asígnelos a los atributos de VMware Identity Manager.

La configuración del directorio LDAP puede basarse en las programaciones predeterminadas o puede crear programaciones personalizadas. También debe definir los atributos personalizados. Para que VMware Identity Manager pueda solicitar el directorio LDAP para obtener los objetos de grupo o usuario, debe proporcionar los nombres de los filtros de búsqueda de LDAP que se apliquen a su directorio LDAP.

En concreto, debe proporcionar la siguiente información.

- Los filtros de búsqueda para obtener los grupos, los usuarios y el usuario de enlace
- Los nombres de atributos LDAP de la pertenencia a grupos, UUID y el nombre distintivo

Se aplican algunas limitaciones a la función de integración en el directorio LDAP. Consulte "Limitaciones de la integración del directorio LDAP," página 61.

Prerequisitos

- Si usa dispositivos virtuales del conector externos y adicionales, tenga en cuenta que capacidad de integrar directorios LDAP solo está disponible con la versión del conector 2016.6.1 y posteriores.

- Compruebe los atributos en la página **Administración de acceso e identidad > Configurar > Atributos de usuario** y agregue los atributos adicionales que quiera sincronizar. Asigne estos atributos de VMware Identity Manager a los atributos del directorio LDAP después de crear el directorio. Estos atributos se sincronizan para los usuarios del directorio.

  NOTA: Si realiza cambios en los atributos de usuario, tenga en cuenta los efectos que puedan tener en otros directorios del servicio. Si tiene previsto agregar los directorios LDAP y Active Directory, compruebe que ningún atributo obligatorio está marcado excepto **userName**, que sí debe estarlo. Las configuraciones de la página Atributos de usuario se aplican a todos los directorios del servicio. Si un atributo está marcado como obligatorio, los usuarios sin dicho atributo no se sincronizan con el servicio de VMware Identity Manager.

- Cuenta de usuario DN de enlace. Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque.
- En el directorio LDAP, el UUID de los usuarios y los grupos debe aparecer como texto sin formato.
- En el directorio LDAP, debe existir un atributo de dominio para todos los usuarios y los grupos.

  Asígnelo al atributo del **dominio** de VMware Identity Manager cuando cree el directorio VMware Identity Manager.

- Los nombres de usuario no deben tener espacios. Si un nombre de usuario tiene un espacio, el usuario se sincroniza pero las autorizaciones no están disponibles para dicho usuario.
- Si utiliza la autenticación con certificado, los usuarios deben tener los valores para los atributos de la dirección de correo electrónico y userPrincipalName.

Procedimiento

1 En la consola de administración, haga clic en la pestaña **Administración de acceso e identidad**.

2 En la página Directorios, haga clic en **Agregar directorio** y seleccione **Agregar directorio LDAP**.

3 Introduzca la información solicitada en la página Agregar directorio LDAP.

Opción	Descripción
Nombre de directorio	Un nombre para el directorio VMware Identity Manager.
Sincronización de directorio y autenticación	a En el campo **Conector de sincronización**, seleccione el conector que desee utilizar para sincronizar usuarios y grupos del directorio LDAP con el directorio de VMware Identity Manager. De forma predeterminada, un componente del conector estará siempre disponible con el servicio de VMware Identity Manager. Este conector aparecerá en la lista desplegable. Si instala varios dispositivos de VMware Identity Manager para lograr una alta disponibilidad, el componente del conector de cada uno aparecerá en la lista. No es necesario un conector diferente para un directorio LDAP. Un conector puede ser compatible con varios directorios, independientemente de si cuentan con directorios LDAP o Active Directory. Para los escenarios en los que necesite conectores adicionales, consulte la sección "Instalación de dispositivos de conector adicionales" en la *Guía de instalación de VMware Identity Manager*. b En el campo **Autenticación**, seleccione **Sí** si desea utilizar el directorio LDAP para autenticar a los usuarios. Si desea utilizar un proveedor de identidades externo para autenticar a los usuarios, seleccione **No**. Después de agregar la conexión del directorio para sincronizar usuarios y grupos, acceda a la página **Administración de acceso e identidad > Administrar > Proveedores de identidades** para agregar el proveedor de identidades externo para realizar la autenticación. c En el campo **Atributo de búsqueda de directorios**, especifique el atributo del directorio LDAP que se utiliza para el nombre de usuario. Si el atributo no aparece en la lista, seleccione **Personalizado** y escriba el nombre del atributo. Por ejemplo, **`cn`**.
Ubicación del servidor	Introduzca el número de puerto y el host del servidor del directorio LDAP. En el caso del host del servidor, puede especificar el nombre del dominio plenamente cualificado o la dirección IP. Por ejemplo, **`myLDAPserver.example.com`** o **`100.00.00.0`**. Si cuenta con un clúster de servidores bajo un equilibrador de carga, introduzca la información de este último en su lugar.

Opción	Descripción
Configuración LDAP	Especifica los atributos y los filtros de búsqueda de LDAP que VMware Identity Manager puede utilizar para solicitar su directorio LDAP. Los valores predeterminados se proporcionan según el esquema principal de LDAP. **Solicitudes LDAP** ■ **Obtener grupos**: es el filtro de búsqueda para obtener los objetos de grupo. Por ejemplo: **`(objectClass=group)`** ■ **Obtener usuario de enlace**: es el filtro de búsqueda para obtener el objeto de usuario de enlace, es decir, al usuario que puede enlazarse al directorio. Por ejemplo: **`(objectClass=person)`** ■ **Obtener usuario**: es el filtro de búsqueda para obtener los usuarios para sincronizar. Por ejemplo:**`(&(objectClass=user)(objectCategory=person))`** **Atributos** ■ **Afiliación**: es el atributo que se utiliza en su directorio LDAP para definir los miembros de un grupo. Por ejemplo: **`member`** ■ **UUID del objeto**: es el atributo que se utiliza en su directorio LDAP para definir el UUID. Por ejemplo: **`entryUUID`** ■ **Nombre distintivo**: es el atributo que se utiliza en su directorio LDAP para definir el nombre distintivo de un usuario o un grupo. Por ejemplo: **`entryDN`**
Certificados	Si el directorio LDAP requiere acceso mediante SSL, seleccione la opción **Este directorio requiere que todas las conexiones usen SSL** y copie y pegue el certificado CA SSL raíz del servidor del directorio LDAP. Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE".
Detalles del usuario de enlace	**DN base**: introduzca el DN desde el que deben empezar las búsquedas. Por ejemplo, cn=users,dc=example,dc=com **DN de enlace**: introduzca el nombre del usuario que enlaza al directorio LDAP. **NOTA:** Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque. **Contraseña DN de enlace**: introduzca la contraseña del usuario DN de enlace.

4 Para probar la conexión al servidor del directorio LDAP, haga clic en **Probar conexión**.

Si no se realizó la conexión correctamente, compruebe la información que introdujo y haga los cambios necesarios.

5 Haga clic en **Guardar y Siguiente**.

6 En la página de los dominios, compruebe que el dominio correcto aparece en la lista, y a continuación, haga clic en **Siguiente**.

7 En la página Asignar atributos, compruebe que los atributos de VMware Identity Manager se asignaron a los atributos LDAP correctos.

IMPORTANTE: Debe especificar una asignación para los atributos de **dominio**.

Puede agregar atributos a la lista desde la página Atributos de usuario.

8 Haga clic en **Siguiente**.

9 En la página de los grupos, haga clic en **+** para seleccionar los grupos que desee sincronizar desde el directorio LDAP al directorio de VMware Identity Manager.

Si cuenta con varios grupos con el mismo nombre en su directorio LDAP, debe especificar nombres únicos para ellos en la página de grupos.

La opción **Sincronizar miembros de grupo anidados** se habilita de forma predeterminada. Cuando se habilita esta opción, todos los usuarios que pertenezcan al grupo que seleccione y los que pertenezcan a grupos anidados dentro de este grupo se sincronizan. Tenga en cuenta que los grupos anidados no se sincronizan. Solo se sincronizarán los usuarios que pertenezcan a los grupos anidados. En el directorio de VMware Identity Manager, estos usuarios aparecerán como los miembros del grupo de nivel superior que seleccionó para sincronizarse. De hecho, la jerarquía bajo un grupo seleccionado es plana y los usuarios de todos los niveles aparecen en VMware Identity Manager como miembros del grupo seleccionado.

Si deshabilita esta opción, todos los usuarios que pertenezcan directamente a ese grupo se sincronizarán cuando especifique un grupo para que se sincronice. Los usuarios que pertenezcan a grupos anidados bajo este grupo no se sincronizarán. Deshabilitar esta opción resulta útil para las grandes configuraciones del directorio en las que atravesar un árbol de grupo requiera demasiado tiempo o demasiados recursos. Si deshabilita esta opción, asegúrese de que selecciona todos los grupos cuyos usuarios desee sincronizar.

10 Haga clic en **Siguiente**.

11 Haga clic en **+** para agregar más usuarios. Por ejemplo, introduzca `CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`.

Para excluir usuarios, cree un filtro que excluya algunos tipos de usuarios. Debe seleccionar el atributo de usuario por el que desea filtrar, la regla de consulta y el valor.

Haga clic en **Siguiente**.

12 Revise la página para ver cuántos usuarios y grupos se sincronizarán con el directorio así como la programación de la sincronización predeterminada.

Para realizar cambios en los usuarios y los grupos o en la frecuencia de sincronización, haga clic en los vínculos **Editar**.

13 Haga clic en **Sincronizar directorio** para iniciar la sincronización del directorio.

Se establece la conexión al directorio LDAP y los usuarios y los grupos se sincronizan desde el directorio LDAP al directorio VMware Identity Manager. El usuario de DN de enlace tiene una función de administrador en VMware Identity Manager de forma predeterminada.

Agregar un directorio después de configurar la conmutación por error y la redundancia

Si se agrega un nuevo directorio al servicio VMware Identity Manager después de haber implementado un clúster para alta disponibilidad, y se desea que el nuevo directorio forme parte de la configuración de alta disponibilidad, se debe agregar el directorio a todos los dispositivos del clúster.

Para ello, se agrega el componente del conector de cada una de las instancias del servicio al nuevo directorio.

Procedimiento

1 Inicie la sesión en la consola de administración de VMware Identity Manager.

2 Haga clic en la pestaña **Administración de acceso e identidad** y, a continuación, seleccione la pestaña **Proveedores de identidades**.

3 En la página Proveedores de identidades, busque el proveedor de identidades del nuevo directorio y haga clic en su nombre.

4 En el campo **nombre de host de IdP**, introduzca el FQDN del equilibrador de carga, si aún no está establecido el FQDN del equilibrador de carga correcto.

5 En el campo **Conector(es)**, seleccione el conector que se va a agregar.

6 Introduzca la contraseña y haga clic en **Guardar**.

7 En la página Proveedores de identidades, haga clic de nuevo en el nombre del proveedor de identidades y verifique que el campo **Nombre de host de IdP** muestre el nombre de host correcto. El campo **Nombre de host de IdP** debería mostrar el FQDN del equilibrador de carga. Si el nombre no es correcto, introduzca el FQDN del equilibrador de carga y haga clic en **Guardar**.

8 Repita los pasos anteriores para agregar todos los conectores indicados en el campo **Conector(es)**.

NOTA: Después de agregar cada conector, compruebe el nombre de host de IdP y, si es necesario, modifíquelo como se describe en el paso 7.

El directorio ya está asociado a todos los conectores de la implementación.

Usar directorios locales 5

Un directorio local es uno de los tipos de directorios que puede crear en el servicio de VMware Identity Manager. Este directorio le permite aprovisionar a los usuarios locales en el servicio y proporcionales acceso a aplicaciones específicas, sin tener que agregarlos al directorio empresarial. Un directorio local no está conectado a un directorio de empresa y los usuarios y los grupos no se sincronizan desde ningún directorio de empresa. En su lugar, puede crear usuarios locales directamente en el directorio local.

Un directorio local predeterminado, denominado directorio del sistema, está disponible en el servicio. También puede crear varios directorios locales nuevos.

Directorio del sistema

El directorio del sistema es un directorio local que se crea automáticamente en el servicio cuando se configura por primera vez. Este directorio cuenta con el dominio de sistema. No puede cambiar el nombre ni el dominio del directorio del sistema, ni agregar nuevos dominios. Tampoco puede eliminar el directorio del sistema ni el dominio del sistema.

El usuario administrador local que se crea cuando configura por primera vez el dispositivo de VMware Identity Manager se genera en el dominio del sistema del directorio del sistema.

Puede agregar otros usuarios al directorio del sistema. El directorio del sistema se suele utilizar para establecer que algunos usuarios administradores locales gestionen el servicio. Se recomienda crear un nuevo directorio local para aprovisionar usuarios finales y administradores adicionales y otorgarles autorización para las aplicaciones.

Directorios locales

Puede crear varios directorios locales. Cada directorio local puede tener uno o varios dominios. Cuando cree un usuario local, especifique el directorio y el dominio de este usuario.

También puede seleccionar atributos para todos los usuarios de un directorio local. Los atributos de los usuarios como userName, lastName y firstName se especifican en el nivel global del servicio de VMware Identity Manager. Está disponible una lista predeterminada de atributos en la que puede agregar atributos personalizados. Los atributos de usuario globales se aplican a todos los directorios del servicio, incluidos los locales. En el nivel del directorio local, puede seleccionar qué atributos son necesarios para el directorio. Esto le permite tener un conjunto personalizado de atributos para directorios locales diferentes. Tenga en cuenta que userName, firstName, lastName y email son siempre obligatorios para los directorios locales.

NOTA: La capacidad de personalizar los atributos de usuario en el nivel del directorio solo está disponible para los directorios locales, no para los directorios LDAP ni Active Directory.

Crear directorios locales es útil en escenarios como el siguiente.

- Puede crear un directorio local para un tipo específico de usuarios que no sea parte del directorio empresarial. Por ejemplo, puede crear un directorio local para partners, que no suelen ser parte del directorio empresarial, y proporcionarles acceso únicamente a las aplicaciones específicas que necesitan.
- Puede crear varios directorios locales si desea asignar diferentes atributos de usuario o métodos de autenticación para diferentes grupos de usuarios. Por ejemplo, puede crear un directorio local para distribuidores que tengan atributos de usuario como la región o el tamaño del mercado, y otro directorio local para proveedores que tengan atributos de usuario como tipo de proveedor y categoría de producto.

Proveedor de identidades del directorio del sistema y de los directorios locales

De forma predeterminada, el directorio del sistema se asocia con un proveedor de identidades denominado Proveedor de identidades del sistema. El método Contraseña (directorio en la nube) está habilitado de forma predeterminada en este proveedor de identidades y se aplica a la directiva default_access_policy_set para el rango de red TODOS LOS INTERVALOS y el tipo de dispositivo del navegador web. Puede configurar métodos de autenticación adicionales y establecer directivas de autenticación.

Cuando cree un directorio local nuevo, no estará asociado con ningún proveedor de identidades. Una vez que haya creado el directorio, cree un nuevo proveedor de identidades del tipo Incrustado y asócielo al directorio. Habilite el método de autenticación Contraseña (directorio en la nube) en el proveedor de identidades. Se pueden asociar varios directorios locales al mismo proveedor de identidades.

El conector de VMware Identity Manager no es necesario para el directorio del sistema ni para los directorios locales que cree.

Para obtener más información, consulte "Configurar la autenticación de usuario en VMware Identity Manager" en *Administración de VMware Identity Manager*.

Administración de contraseñas para los usuarios del directorio local

De forma predeterminada, todos los usuarios de los directorios locales tienen la capacidad de cambiar la contraseña en la aplicación o el portal de Workspace ONE. Puede establecer una contraseña para los usuarios locales. También puede restablecer las contraseñas de los usuarios locales según sea necesario.

Los usuarios pueden cambiar sus contraseñas cuando inician sesión en el portal de Workspace ONE al hacer clic en el nombre situado en la esquina superior derecha, seleccionar **Cuenta** en el menú desplegable y hacer clic en el vínculo **Cambiar contraseña**. En la aplicación Workspace ONE, los usuarios pueden cambiar las contraseñas al hacer clic en el icono de menú de barra triple y seleccionar **Contraseña**.

Para obtener más información sobre cómo establecer directivas de contraseñas y restablecer contraseñas de usuarios locales, consulte "Administrar usuarios y grupos" en *Administración de VMware Identity Manager*.

Este capítulo cubre los siguientes temas:

- "Crear un directorio local," página 70
- "Cambiar la configuración del directorio local," página 75
- "Eliminar un directorio local," página 76

Crear un directorio local

Para crear un directorio local, especifique los atributos del usuario para dicho directorio, créelo e identifíquelo con un proveedor de identidades.

1 Establecer atributos de usuario a nivel global página 71

Antes de crear un directorio local, revise los atributos de usuario en la página Atributos de usuario y, si es necesario, agregue atributos personalizados.

2 Crear un directorio local página 72

Después de revisar y establecer los atributos de usuario globales, cree el directorio local.

3 Asociar el directorio local a un proveedor de identidades página 74

Asocie el directorio local a un proveedor de identidades para que se pueden autenticar los usuarios del directorio. Cree un nuevo proveedor de identidades del tipo Incrustado y habilite en él el método de autenticación Contraseña (directorio local).

Establecer atributos de usuario a nivel global

Antes de crear un directorio local, revise los atributos de usuario en la página Atributos de usuario y, si es necesario, agregue atributos personalizados.

Los atributos de usuario, como firstName, lastName, email y domain, son parte del perfil del usuario. En el servicio de VMware Identity Manager, los atributos de usuario se definen a nivel global y se aplican a todos los directorios del servicio, incluidos los directorios locales. En el nivel del directorio local, puede sobrescribir si desea que un atributo sea obligatorio u opcional para los usuarios en ese directorio, pero no puede agregar atributos personalizados. Si un atributo es obligatorio, le debe asignar un valor cuando cree un usuario.

No se pueden utilizar las siguientes palabras cuando cree atributos personalizados.

Tabla 5-1. Palabras que no se pueden usar como nombres de atributos personalizados

active	addresses	costCenter
department	displayName	division
emails	employeeNumber	autorizaciones
externalId	grupos	id
ims	locale	manager
meta	name	nickName
organization	contraseña	phoneNumber
photos	preferredLanguage	profileUrl
funciones	timezone	title
userName	userType	x509Certificate

NOTA: La capacidad de sobrescribir los atributos de usuario en el nivel del directorio solo se aplica a los directorios locales, no a los directorios LDAP ni Active Directory.

Procedimiento

1 En la consola de administración, haga clic en la pestaña **Administración de acceso e identidad**.

2 Haga clic en **Configuración** y, a continuación, en la pestaña **Atributos de usuario**.

3 Revise la lista de atributos de usuario y, si es necesario, agregue atributos adicionales.

NOTA: Aunque esta página le permite seleccionar los atributos obligatorios, se recomienda que haga la selección para los directorios locales a nivel de estos directorios. Si un atributo se marca como obligatorio en esta página, se aplica a todos los directorios en el servicio, incluidos los de Active Directory o LDAP.

4 Haga clic en **Guardar**.

Qué hacer a continuación

Cree el directorio local.

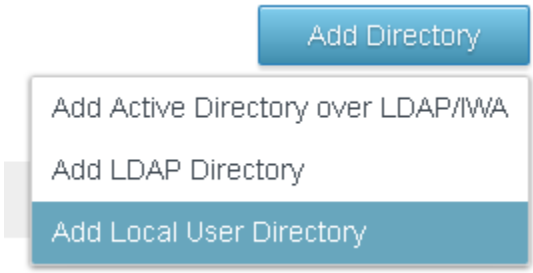
Crear un directorio local

Después de revisar y establecer los atributos de usuario globales, cree el directorio local.

Procedimiento

1 En la consola de administración, haga clic en la pestaña **Administración de acceso e identidad** y, a continuación, en la pestaña **Directorios**.

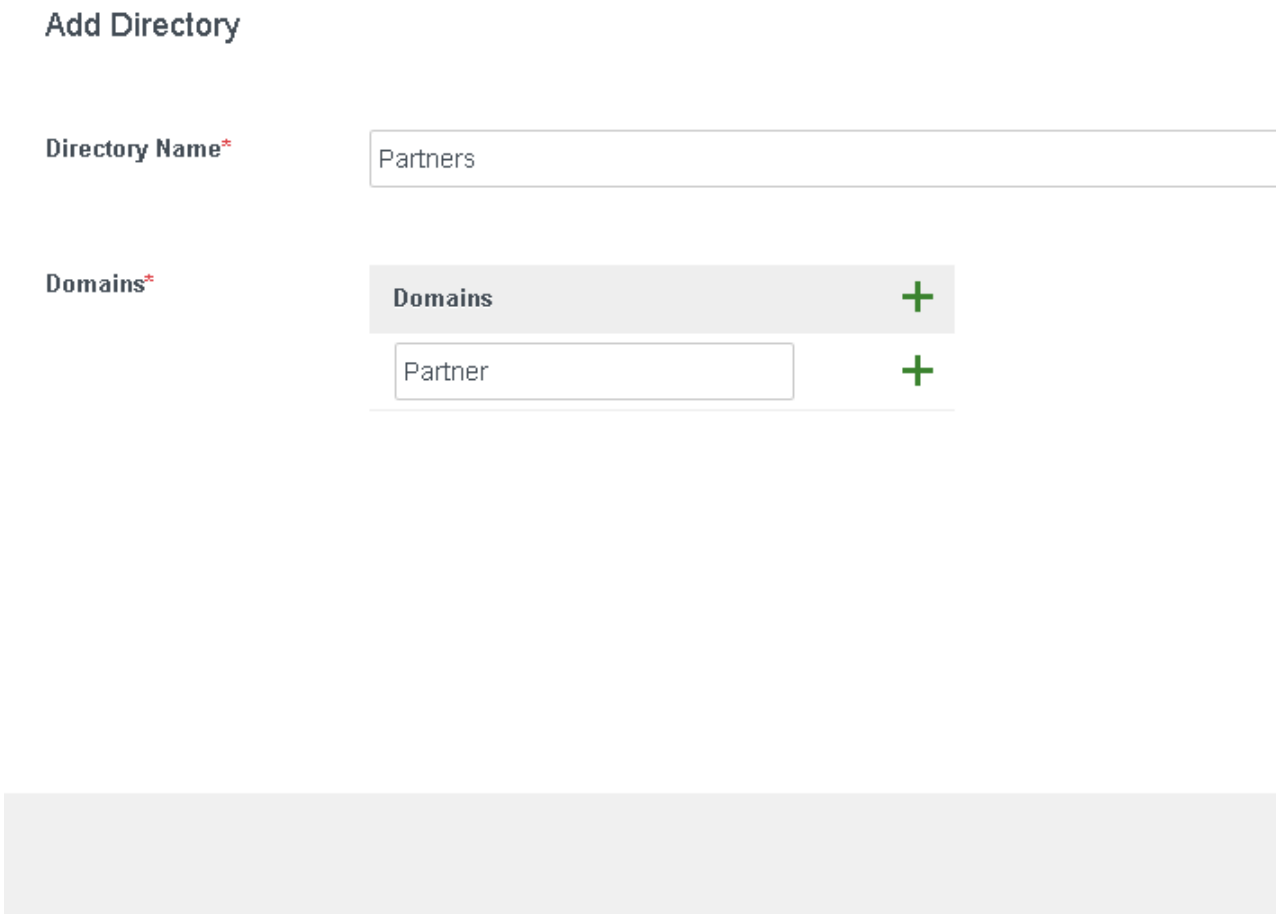
2 Haga clic en **Agregar directorio** y seleccione **Agregar directorio de usuario local** en el menú desplegable.



3 En la página Agregar directorio, introduzca un nombre de directorio y especifique al menos un nombre de dominio.

El nombre de los dominios debe ser único en todos los directorios del servicio.

Por ejemplo:



4 Haga clic en **Guardar**.

5 En la página Directorios, haga clic en el nuevo directorio.

6 Haga clic en la pestaña **Atributos de usuario**.

Aparecen todos los atributos de la página Administración de acceso e identidad > Configuración > Atributos de usuario del directorio local. Los atributos que están seleccionados como obligatorio en esta página también aparecen como obligatorios en la página del directorio local.

7 Personalice los atributos para el directorio local.

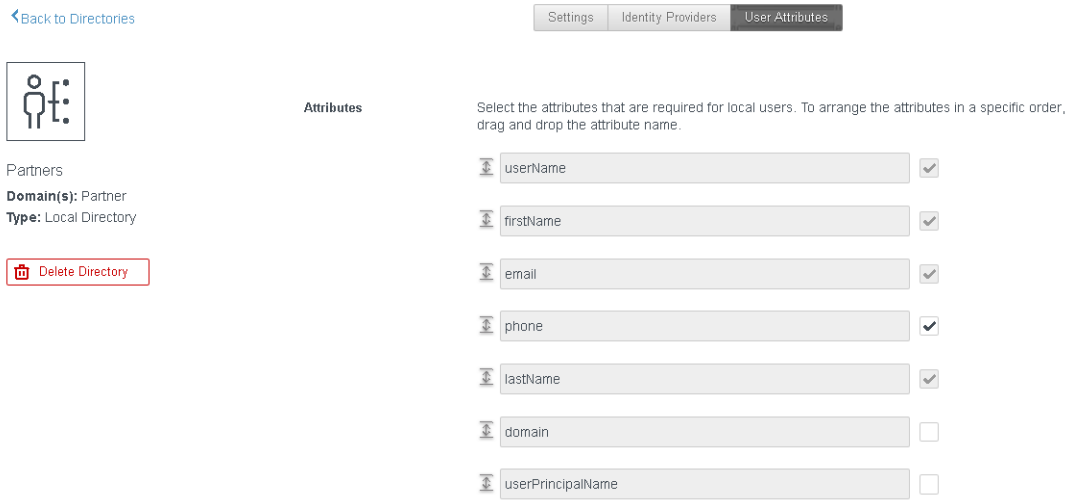
Puede especificar los atributos obligatorios y los opcionales. También puede cambiar el orden en el que aparecen los atributos.

IMPORTANTE: Los atributos userName, firstName, lastName y email son siempre obligatorios para los directorios locales.

- Para que un atributo sea obligatorio, seleccione la casilla de verificación que aparece junto al nombre del atributo.
- Para que un atributo sea opcional, desmarque la casilla de verificación que aparece junto al nombre del atributo.
- Para cambiar el orden de los atributos, haga clic y arrastre el atributo a la nueva posición.

Si un atributo es obligatorio, debe especificar un valor para dicho atributo cuando cree un usuario.

Por ejemplo:



8 Haga clic en **Guardar**.

Qué hacer a continuación

Asocie el directorio local al proveedor de identidades que desee usar para autenticar usuarios en el directorio.

Asociar el directorio local a un proveedor de identidades

Asocie el directorio local a un proveedor de identidades para que se pueden autenticar los usuarios del directorio. Cree un nuevo proveedor de identidades del tipo Incrustado y habilite en él el método de autenticación Contraseña (directorio local).

NOTA: No utilice el proveedor de identidades integrado. No se recomienda habilitar el método de autenticación Contraseña (directorio local) en el proveedor de identidades integrado.

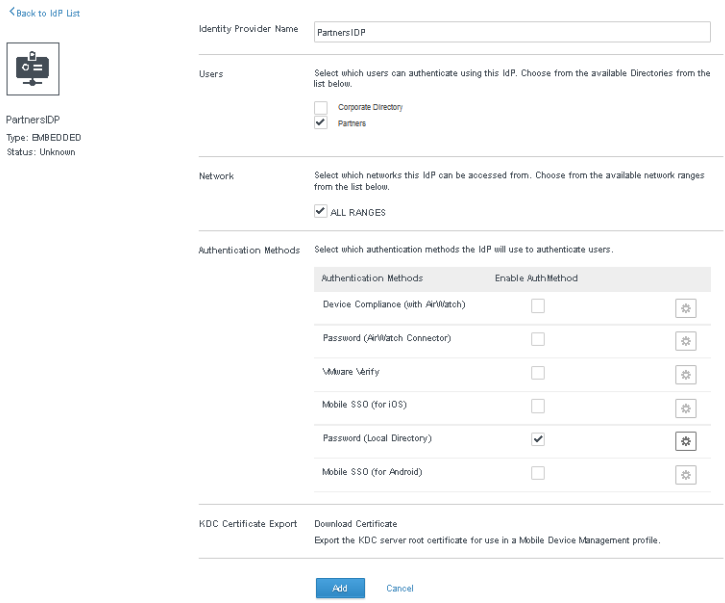
Procedimiento

1 En la pestaña **Administración de acceso e identidad**, haga clic en la pestaña **Proveedores de identidades**.

2 Haga clic en **Agregar proveedor de identidades** y seleccione **Crear IDP integrado**.

3 Escriba la siguiente información.

Opción	Descripción
Nombre del proveedor de identidades	Escriba un nombre para el proveedor de identidades.
Usuarios	Seleccione el directorio local que ha creado.
Red	Seleccione las redes desde las que se puede acceder a este proveedor de identidades.
Métodos de autenticación	Seleccione Contraseña (directorio local).
Exportación de certificado KDC	No es necesario que descargue el certificado, a menos que vaya a configurar el SSO móvil para dispositivos iOS gestionados por AirWatch.



4 Haga clic en **Agregar**.

El proveedor de identidades se crea y se asocia al directorio local. Podrá configurar otros métodos de autenticación en el proveedor de identidades más adelante. Para obtener más información sobre la autenticación, consulte "Configurar la autenticación de usuario en VMware Identity Manager" en *Administración de VMware Identity Manager*.

Puede usar el mismo proveedor de identidades para varios directorios locales.

Qué hacer a continuación

Crear grupos y usuarios locales. Puede crear grupos y usuarios locales en la pestaña **Usuarios y grupos** de la consola de administración. Consulte "Administrar usuarios y grupos" en *Administración de VMware Identity Manager* para obtener más información.

Cambiar la configuración del directorio local

Después de crear un directorio local, puede modificar su configuración en cualquier momento.

Puede cambiar las siguientes opciones:

- Cambiar el nombre del directorio.
- Agregar, eliminar o cambiar el nombre de los dominios.
  - Los nombres de los dominios deben ser únicos en todos los directorios del servicio.
  - Cuando cambia un nombre de dominio, los usuarios que estaban asociados al dominio antiguo se asocian al nuevo.
  - El directorio debe tener un dominio al menos.
  - No puede agregar un dominio al directorio del sistema ni eliminar el dominio del sistema.
- Agregar nuevos atributos de usuarios o establecer un atributo existente como obligatorio u opcional.
  - Si el directorio local no cuenta con ningún usuario aún, puede agregar nuevos atributos como obligatorios u opcionales y cambiar estas categorías en los existentes.
  - Si ya creó usuarios en el directorio local, solo puede agregar nuevos atributos como opcionales y cambiar los existentes de obligatorios a opcionales. No puede cambiar un atributo opcional a obligatorio después de crear los usuarios.

- Los atributos userName, firstName, lastName y email son siempre obligatorios para los directorios locales.
- Como los atributos de los usuarios se definen en el nivel global del servicio de VMware Identity Manager, los nuevos atributos que agregue aparecerán en todos los directorios del servicio.

- Cambiar el orden en el que aparecen los atributos.

Procedimiento

1 Haga clic en la pestaña **Administración de acceso e identidad**.

2 En la página Directorios, haga clic en el directorio que desea editar.

3 Edite la configuración del directorio local.

Opción	Acción
Cambiar el nombre del directorio	a En la pestaña **Configuración**, edite el nombre del directorio. b Haga clic en **Guardar**.
Agregar, eliminar o cambiar el nombre de un dominio	a En la pestaña **Configuración**, edite la lista **Dominios**. b Para agregar un dominio, haga clic en el icono verde del símbolo más. c Para eliminar un dominio, haga clic en el icono rojo. d Para cambiar el nombre de un dominio, edítelo en el cuadro de texto.
Agregar atributos de usuario en el directorio	a Haga clic en la pestaña **Administración de acceso e identidad** y, a continuación, en **Configuración**. b Haga clic en la pestaña **Atributos de usuario**. c Agregue los atributos en la lista **Agregar otros atributos que desee utilizar** y haga clic en **Guardar**.
Establecer un atributo como obligatorio u opcional para el directorio	a En la pestaña **Administración de acceso e identidad**, haga clic en **Directorios**. b Haga clic en el nombre del directorio local y, a continuación, en la pestaña **Atributos de usuario**. c Marque la casilla que aparece junto a un atributo para que sea obligatorio o desmárquela para que sea opcional. d Haga clic en **Guardar**.
Cambiar el orden de los atributos	a En la pestaña **Administración de acceso e identidad**, haga clic en **Directorios**. b Haga clic en el nombre del directorio local y, a continuación, en la pestaña **Atributos de usuario**. c Haga clic y arrastre el atributo a su nueva posición. d Haga clic en **Guardar**.

Eliminar un directorio local

Puede eliminar un directorio local que creó en el servicio de VMware Identity Manager. No puede eliminar el directorio del sistema, que se creó de forma predeterminada cuando configuró por primera vez el servicio.

ADVERTENCIA: Cuando elimina un directorio, todos los usuarios de dicho directorio también se eliminan del servicio.

Procedimiento

1 Haga clic en la pestaña **Administración de acceso e identidad** y, a continuación, en la pestaña **Directorios**.

2 Haga clic en el directorio que desea eliminar.

3 En la página de directorios, haga clic en **Eliminar directorio**.

Configuración avanzada del dispositivo VMware Identity Manager 6

Cuando haya completado la instalación de dispositivos virtuales de VMware Identity Manager, puede que tenga que completar otras tareas de configuración, como habilitar el acceso externo a VMware Identity Manager y configurar la redundancia.

El diagrama de la arquitectura de VMware Identity Manager demuestra cómo se puede implementar el entorno de VMware Identity Manager. Consulte una implementación típica en Capítulo 1, "Preparar la instalación de VMware Identity Manager," página 9.

Este capítulo cubre los siguientes temas:

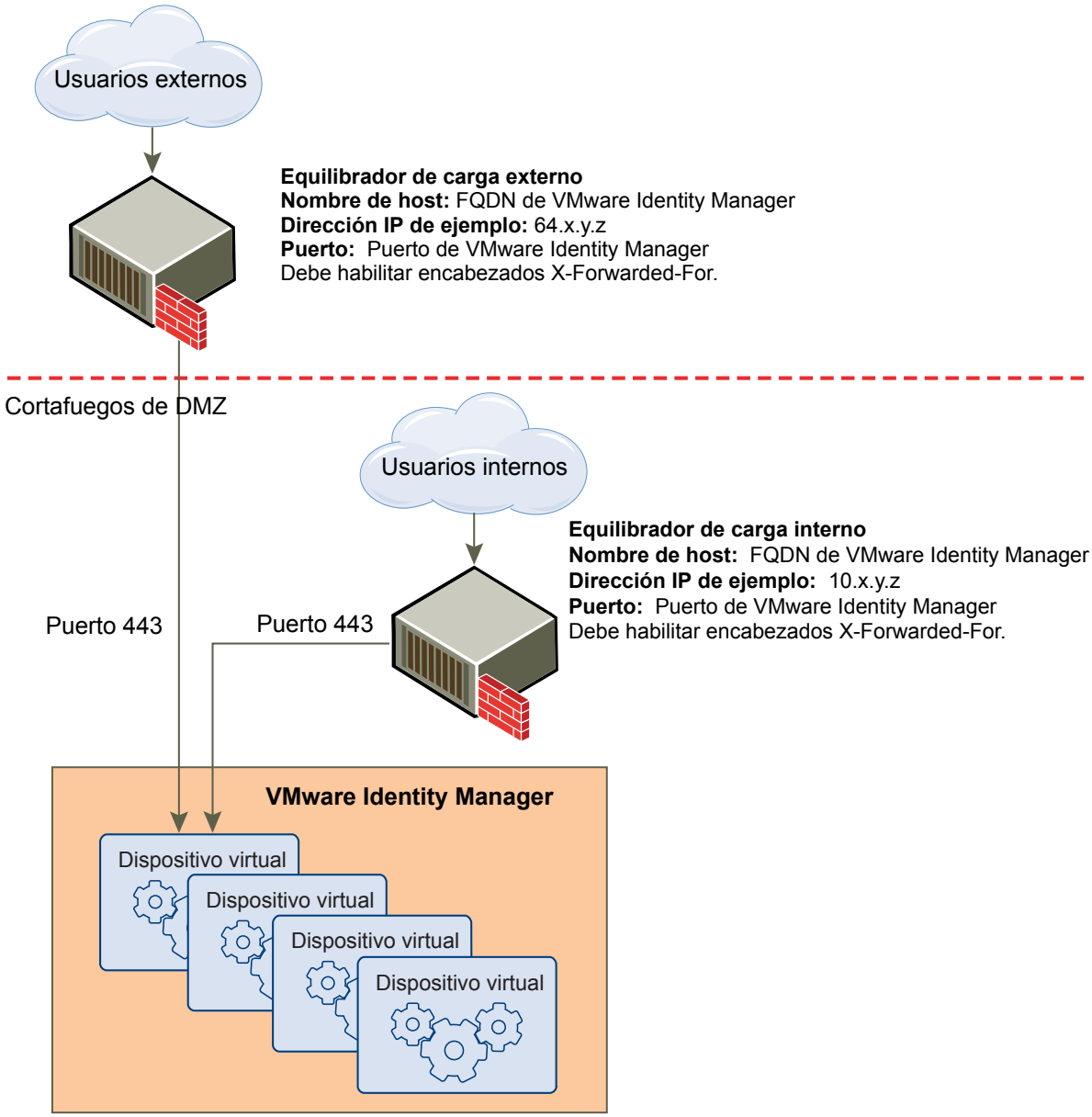
- "Usar un equilibrador de carga o un proxy inverso para habilitar el acceso externo a VMware Identity Manager," página 77
- "Configurar la conmutación por error y la redundancia en un centro de datos único," página 81
- "Implementar VMware Identity Manager en un centro de datos secundario para la conmutación de error y la redundancia," página 87

Usar un equilibrador de carga o un proxy inverso para habilitar el acceso externo a VMware Identity Manager

Durante la implementación, el dispositivo virtual VMware Identity Manager se configura en el interior de la red interna. Si desea proporcionar acceso al servicio a aquellos usuarios que se conectan desde redes exteriores, debe instalar un equilibrador de carga o un proxy inverso, como Apache, nginx o F5 en la red perimetral o DMZ.

Si no usa un equilibrador de carga o un proxy inverso, no podrá ampliar en otra ocasión el número de dispositivos de VMware Identity Manager. Puede que necesite agregar más dispositivos para proporcionar redundancia y equilibrio de carga. El diagrama siguiente muestra la arquitectura de implementación básica que puede usar para habilitar el acceso externo.

Figura 6-1. Proxy de equilibrador de carga externo con máquina virtual



Especifique el FQDN del de VMware Identity Manager durante la implementación

Durante la implementación de la máquina virtual VMware Identity Manager , proporciona el número de puerto y el FQDN de VMware Identity Manager . Estos valores deben dirigir al nombre de host al que desea que los usuarios finales obtengan acceso.

La máquina virtual VMware Identity Manager siempre se ejecuta a través del puerto 443. Puede usar un número de puerto diferente para el equilibrador de carga. Si usa un número de puerto diferente, debe especificarlo durante la implementación.

Opciones del equilibrador de carga para configurar

La configuración del equilibrador de carga incluye habilitar encabezados X-Forwarded-For, establecer correctamente el tiempo de espera del equilibrador de carga y habilitar sesiones sticky. Además, se debe configurar una confianza SSL entre el equilibrador de carga y el dispositivo virtual VMware Identity Manager.

- Encabezados X-Forwarded-For

  Debe habilitar encabezados X-Forwarded-For para su equilibrador de carga. Esto determina el método de autenticación. Consulte la documentación proporcionada por el proveedor de su equilibrador de carga para obtener más información.

- Tiempo de espera del equilibrador de carga

  Para que VMware Identity Manager funcione correctamente, es posible que necesite aumentar el valor predeterminado correspondiente al tiempo de espera para las solicitudes del equilibrador de carga. Este valor se expresa en minutos. Si el valor del tiempo de espera es demasiado bajo, puede que se muestre el mensaje de error 502, que indica que el servicio no se encuentra disponible en ese momento.

- Habilitar sesiones sticky

  Debe habilitar la configuración de las sesiones sticky en el equilibrador de carga si la implementación tiene varios dispositivos de VMware Identity Manager. El equilibrador de carga enlazará entonces la sesión de un usuario a una instancia específica.

Aplicar el certificado raíz de VMware Identity Manager al equilibrador de carga

Cuando el dispositivo virtual VMware Identity Manager se configure con un equilibrador de carga, deberá establecer la confianza SSL entre este y VMware Identity Manager. El certificado raíz de VMware Identity Manager se debe copiar en el equilibrador de carga.

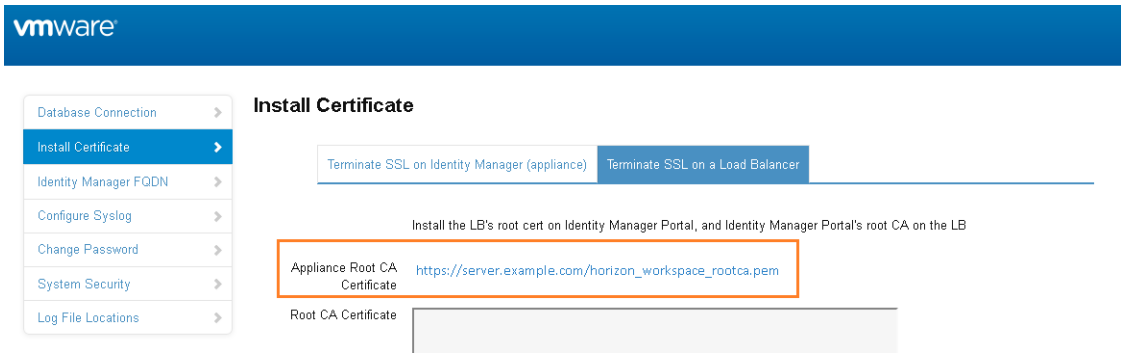
El certificado de VMware Identity Manager se puede descargar de la consola de administración, desde la página **Configuración de dispositivos > Configuración del dispositivo virtual > Administrar configuración**.

Si el FQDN de VMware Identity Manager dirige a un equilibrador de carga, el certificado SSL solo se puede aplicar al equilibrador de carga.

Como el equilibrador de carga se comunica con el dispositivo virtual del VMware Identity Manager , debe copiar el certificado raíz de la CA de VMware Identity Manager al equilibrador de carga como certificado raíz de confianza.

Procedimiento

1. En la consola de administración, seleccione la pestaña **Configuración de dispositivos** y, a continuación, **Configuración del dispositivo virtual**.
2. Haga clic en **Administrar configuración**.
3. Seleccione **Instalar el certificado**.
4. Seleccione la pestaña **Terminar SSL en un equilibrador de carga** y, en el campo **Certificado de CA raíz del dispositivo**, haga clic en el vínculo `https://`*`nombre de host`*`/horizon_workspace_rootca.pem`.



5 Copie todo lo que hay entre las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE----, incluyendo estas líneas, y pegue el certificado raíz en la ubicación correcta de cada uno de sus equilibradores de carga. Consulte la documentación proporcionada por el proveedor de equilibradores de carga.

Qué hacer a continuación

Copie y pegue el certificado raíz del equilibrador de carga en el dispositivo VMware Identity Managerconector.

Aplicar el certificado raíz del equilibrador de carga a VMware Identity Manager

Cuando el dispositivo virtual VMware Identity Manager se configure con un equilibrador de carga, deberá establecer la confianza entre este y VMware Identity Manager. Además de copiar el certificado raíz de VMware Identity Manager al equilibrador de carga, deberá copiar el certificado del equilibrador de carga a VMware Identity Manager.

Procedimiento

1 Obtenga el certificado raíz del equilibrador de carga.

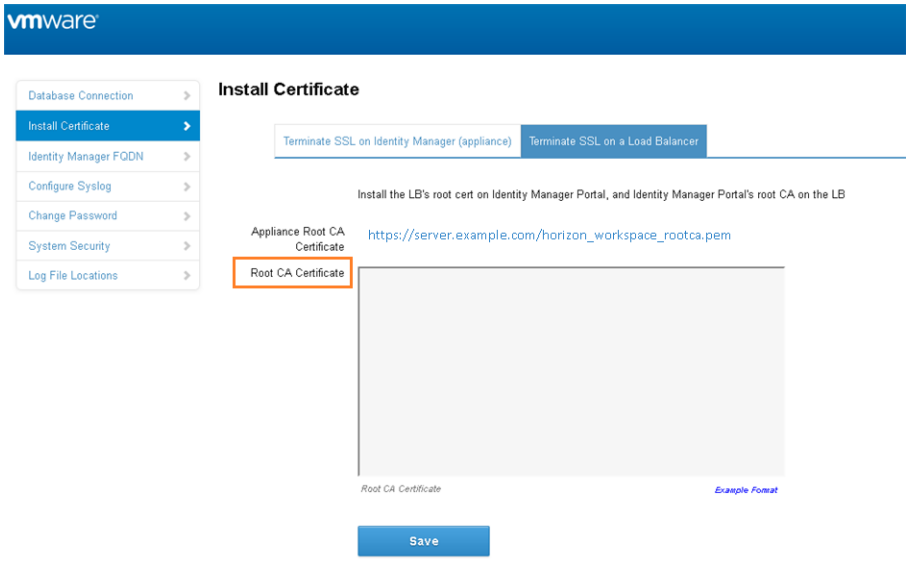
2 En la consola de administración de VMware Identity Manager, seleccione la pestaña **Configuración de dispositivos** y, a continuación, **Configuración del dispositivo virtual**.

3 Haga clic en **Administrar configuración**.

4 Inicie la sesión con la contraseña de administrador

5 En la página **Instalar el certificado**, seleccione la pestaña **Terminar SSL en un equilibrador de carga**.

6 Pegue el texto del certificado del equilibrador de carga en el campo **Certificado de CA raíz**.



7 Haga clic en **Guardar**.

Configurar los valores del servidor proxy para VMware Identity Manager

El dispositivo virtual de VMware Identity Manager accede al catálogo de aplicaciones en la nube y a otros servicios web en Internet. Si su configuración de red proporciona acceso a Internet a través de un proxy HTTP, deberá ajustar la configuración del proxy en el dispositivo VMware Identity Manager.

Habilite su proxy para gestionar solo el tráfico de Internet. Para asegurar que el proxy esté configurado correctamente, establezca el parámetro de tráfico interno en la opción `no-proxy` dentro del dominio.

NOTA: Los servidores proxy que requieren autenticación no son compatibles.

Procedimiento

1 Desde vSphere Client, inicie la sesión como usuario root en el dispositivo virtual de VMware Identity Manager.

2 Introduzca `YaST` en la línea de comandos para ejecutar la utilidad `YaST`.

3 En el panel izquierdo, seleccione **Servicios de red** y, a continuación, **Proxy**.

4 Introduzca las URL del servidor proxy en los campos de **URL del proxy HTTP** y **URL del proxy HTTPS**.

5 Seleccione **Finalizar** y salga de la utilidad `YaST`.

6 Reinicie el servidor Tomcat en el dispositivo virtual de VMware Identity Manager para utilizar la nueva configuración del proxy.

```
service horizon-workspace restart
```

El catálogo de aplicaciones en la nube y otros servicios web ya están disponibles en VMware Identity Manager.

Configurar la conmutación por error y la redundancia en un centro de datos único

Para obtener la conmutación por error y la redundancia, puede agregar varios dispositivos virtuales de VMware Identity Manager en un clúster. VMware Identity Manager seguirá disponible aunque uno de los dispositivos virtuales se apague por algún motivo.

Debe instalar y configurar primero un dispositivo virtual de VMware Identity Manager y, a continuación, clonarlo. Al clonar el dispositivo virtual, se crea un duplicado del mismo con la misma configuración que el original. Puede personalizar el dispositivo virtual clonado para que el nombre, la configuración de red y otras propiedades pasen a ser obligatorios.

Antes de clonar el dispositivo virtual de VMware Identity Manager, debe configurarlo detrás de un equilibrador de carga y cambiar su nombre de dominio completo (FQDN) para que coincida con el FQDN del equilibrador de carga. Además, debe completar la configuración del directorio en el servicio de VMware Identity Manager antes de clonar el dispositivo.

Tras realizar el proceso de clonación, debe asignar una nueva dirección IP al dispositivo virtual clonado antes de encenderlo. La dirección IP del dispositivo virtual clonado debe seguir las mismas directrices que la del dispositivo virtual original. La dirección IP debe resolverse en un nombre de host válido con una DNS directa e inversa.

Los nodos del clúster de VMware Identity Manager son copias idénticas y casi sin estado unas de otras. La sincronización con Active Directory y con los recursos configurados, como View o ThinApp, está deshabilitada en los dispositivos virtuales clonados.

1 Número recomendado de nodos en el clúster de VMware Identity Manager página 82

   Se recomienda configurar un clúster de VMware Identity Manager con tres nodos.

2 Cambiar el FQDN de VMware Identity Manager al FQDN del equilibrador de carga página 83

   Antes de clonar el dispositivo virtual VMware Identity Manager, debe cambiar su nombre de dominio plenamente cualificado (FQDN) para que coincida con el FQDN del equilibrador de carga.

3 Clonar el dispositivo virtual. página 83

4 Asignar una nueva dirección IP a un dispositivo virtual clonado página 84

   Se debe asignar una nueva dirección IP a cada dispositivo virtual clonado antes de encenderlo. La dirección IP se debe poder resolver en el servidor DNS. Si la dirección no está en el DNS inverso, se debe asignar también el nombre de host.

5 Habilitar la sincronización de directorio en otra instancia de en caso de fallo página 86

Número recomendado de nodos en el clúster de VMware Identity Manager

Se recomienda configurar un clúster de VMware Identity Manager con tres nodos.

El dispositivo VMware Identity Manager incluye Elasticsearch, un motor de búsqueda y análisis. Elasticsearch tiene una limitación conocida con los clústeres de dos nodos. Consulte la documentación de Elasticsearch para obtener una descripción sobre la limitación de "cerebro dividido". Tenga en cuenta que no tiene que configurar Elasticsearch.

Un clúster de VMware Identity Manager con dos nodos produce una función de error con algunas limitaciones relacionadas con Elasticsearch. Si se desconecta uno de los nodos, se aplican las siguientes limitaciones hasta que el nodo vuelve a conectarse:

- El panel de control no muestra ningún dato.
- La mayoría de los informes no está disponible.
- La información del registro de sincronización no aparece en los directorios.
- El campo de búsqueda situado en la esquina superior derecha de la consola de administración no devuelve ningún resultado.
- La función de autocompletar no está disponible en los campos de texto.

No hay ninguna pérdida de datos durante el tiempo en el que el nodo está desconectado. La información del registro de sincronización y del evento de auditoría se almacena y se mostrará cuando se restablezca el nodo.

Cambiar el FQDN de VMware Identity Manager al FQDN del equilibrador de carga

Antes de clonar el dispositivo virtual VMware Identity Manager, debe cambiar su nombre de dominio plenamente cualificado (FQDN) para que coincida con el FQDN del equilibrador de carga.

Prerequisitos

- El dispositivo VMware Identity Manager se agrega a un equilibrador de carga.
- Se aplicó el certificado raíz de CA a VMware Identity Manager.

Procedimiento

1 Inicie la sesión en la consola de administración de VMware Identity Manager.

2 Seleccione la pestaña **Configuración de dispositivos**.

3 En la página Configuración del dispositivo virtual, haga clic en **Administrar configuración**.

4 Introduzca su contraseña de administrador para iniciar la sesión.

5 Haga clic en **Configuración de Identity Manager**.

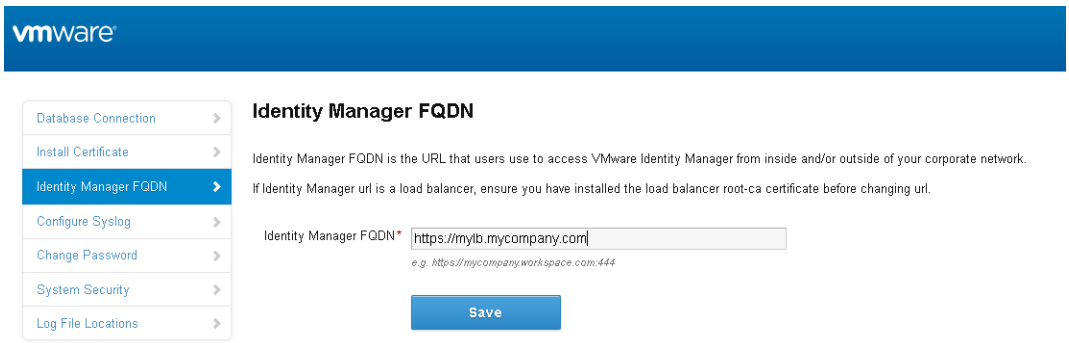
6 En el campo **FQDN de Identity Manager**, cambie la parte del nombre de host de la URL del nombre de host de VMware Identity Manager por el nombre de host del equilibrador de carga.

Por ejemplo, si su nombre de host de VMware Identity Manager es `miservicio` y el nombre de host de su equilibrador de carga es `milb`, cambiaría la URL

`https://myservice.mycompany.com`

por la siguiente:

`https://mylb.mycompany.com`



7 Haga clic en **Guardar**.

- El FQDN se cambiará por el FQDN del equilibrador de carga.
- La URL del proveedor de identidades se cambiará por la URL del equilibrador de carga.

Qué hacer a continuación

Clone el dispositivo virtual.

Clonar el dispositivo virtual.

Clone el dispositivo virtual de VMware Identity Manager para crear varios dispositivos virtuales del mismo tipo para distribuir el tráfico y eliminar el tiempo de inactividad potencial.

Al utilizar varios dispositivos virtuales de VMware Identity Manager se mejora la disponibilidad, se cargan solicitudes de balances al servicio y se disminuyen los tiempos de respuesta al usuario final.

Prerequisitos

- El dispositivo virtual de VMware Identity Manager debe configurarse tras un equilibrador de carga. Compruebe que el puerto del equilibrador de carga es el 443. No use el puerto 8443 ya que es el puerto administrativo y es de uso exclusivo para cada dispositivo virtual.
- Se configura una base de datos externa como se describe en "Establecer conexión con la base de datos," página 34.
- Compruebe que completa la configuración del directorio en VMware Identity Manager.
- Inicie sesión en la consola de dispositivos virtuales como usuario raíz y elimine el archivo `/etc/udev/rules.d/70-persistent-net.rules`, si existe. Si no elimina este archivo antes de la clonación, la red no se configura correctamente en el dispositivo virtual clonado.

Procedimiento

1. Inicie sesión en vSphere Client o en vSphere Web Client y diríjase al dispositivo virtual de VMware Identity Manager.
2. Haga clic con el botón derecho en el dispositivo virtual y seleccione **Clonar**.
3. Introduzca el nombre del dispositivo virtual clonado y haga clic en **Siguiente**.

   El nombre debe ser único dentro de la carpeta de la máquina virtual.
4. Seleccione el host o el clúster en el que desea ejecutar el dispositivo virtual clonado y haga clic en **Siguiente**.
5. Seleccione el grupo de recursos en el que va a ejecutar el dispositivo virtual y haga clic en **Siguiente**.
6. Para el formato de disco virtual, seleccione **Mismo formato que el origen**.
7. Seleccione la ubicación del almacén de datos donde quiera almacenar los archivos del dispositivo virtual y haga clic en **Siguiente**.
8. Seleccione la opción de **no personalizar** como la opción del sistema operativo invitado.
9. Revise las opciones y haga clic en **Finalizar**.

Se implementará el dispositivo virtual clonado. No puede utilizar ni editar el dispositivo virtual hasta que la clonación finalice.

Qué hacer a continuación

Asigne una dirección IP al dispositivo virtual clonado antes de conectarlo y agréguelo al equilibrador de carga.

Asignar una nueva dirección IP a un dispositivo virtual clonado

Se debe asignar una nueva dirección IP a cada dispositivo virtual clonado antes de encenderlo. La dirección IP se debe poder resolver en el servidor DNS. Si la dirección no está en el DNS inverso, se debe asignar también el nombre de host.

Procedimiento

1. En vSphere Client o vSphere Web Client, seleccione el dispositivo virtual clonado.
2. En la pestaña **Resumen**, en **Comandos**, haga clic en **Editar configuración**.
3. Seleccione **Opciones** y, en la lista de **opciones de vApp**, seleccione **Propiedades**.
4. Cambie la dirección IP en el campo **Dirección IP**.

5 Si la dirección IP no se encuentra en el servidor DNS inverso, agregue el nombre de host en el cuadro de texto **HostName**.

6 Haga clic en **Aceptar.**

7 Encienda el dispositivo clonado y espere a que aparezca la pantalla azul de inicio de sesión en la pestaña **Consola**.

IMPORTANTE: Antes de encender el dispositivo clonado, asegúrese de que el dispositivo original esté completamente encendido.

Qué hacer a continuación

- Espere unos minutos a que se creen los clústeres de Elasticsearch y RabbitMQ antes de agregar el dispositivo virtual clonado al equilibrador de carga.

  Elasticsearch, un motor de búsqueda y análisis, y RabbitMQ, un agente de mensajería, están integrados en el dispositivo virtual.

  a Inicie la sesión en el dispositivo virtual clonado.

  b Compruebe el clúster de Elasticsearch:

  ```
  curl –XGET 'http://localhost:9200/_cluster/health?pretty=true'
  ```

  Compruebe que el resultado corresponda al número de nodos.

  c Compruebe el clúster de RabbitMQ:

  ```
  rabbitmqctl cluster_status
  ```

  Compruebe que el resultado corresponda al número de nodos.

- Agregue el dispositivo virtual clonado al equilibrador de carga y configure el equilibrador de carga para distribuir el tráfico. Para obtener información, consulte la documentación del proveedor del equilibrador de carga.

- Si se había unido a un dominio en la instancia del servicio original, deberá unirse al dominio en las instancias del servicio clonado.

  a Inicie sesión en la consola de administración de VMware Identity Manager.

  b Seleccione la pestaña **Administración de acceso e identidad** y, a continuación, haga clic en **Configuración**.

  El componente de conector de cada una de las instancias del servicio clonadas se indica en la página Conectores.

  c En cada conector de la lista, haga clic en **Unirse al dominio** y especifique la información del dominio.

  Para obtener más información sobre Active Directory, consulte "Integrar con Active Directory," página 47.

- En directorios con tipo de autenticación integrada de Windows (IWA), se debe hacer lo siguiente:

  a En las instancias del servicio clonadas, únase al dominio al que estaba unido el directorio de IWA en la instancia del servicio original.

  1 Inicie sesión en la consola de administración de VMware Identity Manager.

  2 Seleccione la pestaña **Administración de acceso e identidad** y, a continuación, haga clic en **Configuración**.

  El componente de conector de cada una de las instancias del servicio clonadas se indica en la página Conectores.

3 En cada conector de la lista, haga clic en **Unirse al dominio** y especifique la información del dominio.

b Guarde la configuración del directorio de IWA.

1 Seleccione la pestaña **Administración de acceso e identidad**.

2 En la página Directorios, haga clic en el enlace del directorio de IWA.

3 Haga clic en **Guardar** para guardar la configuración del directorio.

- Si actualizó el archivo `/etc/krb5.conf` de forma manual en la instancia del servicio principal para, por ejemplo, resolver el error de la sincronización de View o la lentitud de este proceso, debe actualizar el archivo en la instancia clonada después de que esta se conecte al dominio. En todas las instancias del servicio clonado, realice las siguientes tareas:

  a Edite el archivo `/etc/krb5.conf` y actualice la sección `realms` para especificar los mismos valores de dominio a host que se utilizan en el archivo `/usr/local/horizon/conf/domain_krb.properties`. No es necesario especificar el número de puerto. Por ejemplo, si el archivo `domain_krb.properties` tiene la entrada de dominio `example.com=examplehost.example.com:389`, debería actualizar el archivo `krb5.conf` a los siguientes valores.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

  NOTA: Es posible tener varias entradas kdc, aunque no es un requisito, ya que en muchos casos solo hay un único valor kdc. Si decide definir valores kdc adicionales, cada línea tendrá una entrada kdc que definirá un controlador de dominio.

  b Reinicie el servicio del área de trabajo.

```
service horizon-workspace restart
```

  NOTA: Consulte también el artículo 2091744 de la Base de conocimientos.

- Habilite los métodos de autenticación configurados para conector en cada una de las instancias clonadas. Para obtener más información, consulte la *Guía de administración de VMware Identity Manager*.

El dispositivo virtual del servicio VMware Identity Manager ya es de alta disponibilidad. El tráfico se distribuye a los dispositivos virtuales del clúster según la configuración del equilibrador de carga. La autenticación en el servicio es de alta disponibilidad. No obstante, para la función de sincronización de directorio del servicio, en caso de fallo de una instancia del servicio, se deberá habilitar manualmente la sincronización de directorio en una instancia del servicio clonada. De la sincronización del directorio se encarga el componente de conector del servicio y solo se puede habilitar en un conector cada vez. Consulte "Habilitar la sincronización de directorio en otra instancia de en caso de fallo," página 86.

Habilitar la sincronización de directorio en otra instancia de en caso de fallo

En caso de un fallo de la instancia del servicio, la autenticación la gestiona automáticamente una instancia clonada, como se configuró en el equilibrador de carga. No obstante, para la sincronización del directorio es necesario modificar la configuración del directorio en el servicio VMware Identity Manager para utilizar una instancia clonada. De la sincronización del directorio se encarga el componente de conector del servicio y solo se puede habilitar en un conector cada vez.

Procedimiento

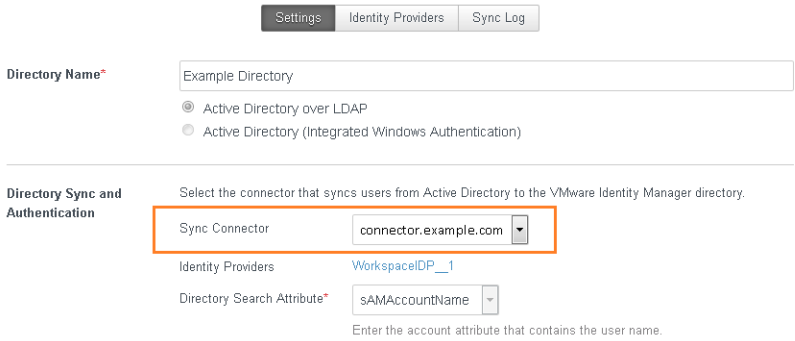
1 Inicie sesión en la consola de administración de VMware Identity Manager.

2 Haga clic en la pestaña **Administración de acceso e identidad** y, a continuación, en **Directorios**.

3 Haga clic en el directorio asociado al a instancia del servicio original.

Puede consultar esta información en la página **Configuración > Conectores**. La página indica el componente de conector de cada uno de los dispositivos virtuales del servicio del clúster.

4 En la sección **Sincronización y autenticación de directorios** de la página del directorio, en el campo **Conector de sincronización**, seleccione uno de los otros conectores.



5 En el campo **Contraseña del DN de enlace**, introduzca la contraseña de la cuenta de enlace de Active Directory.

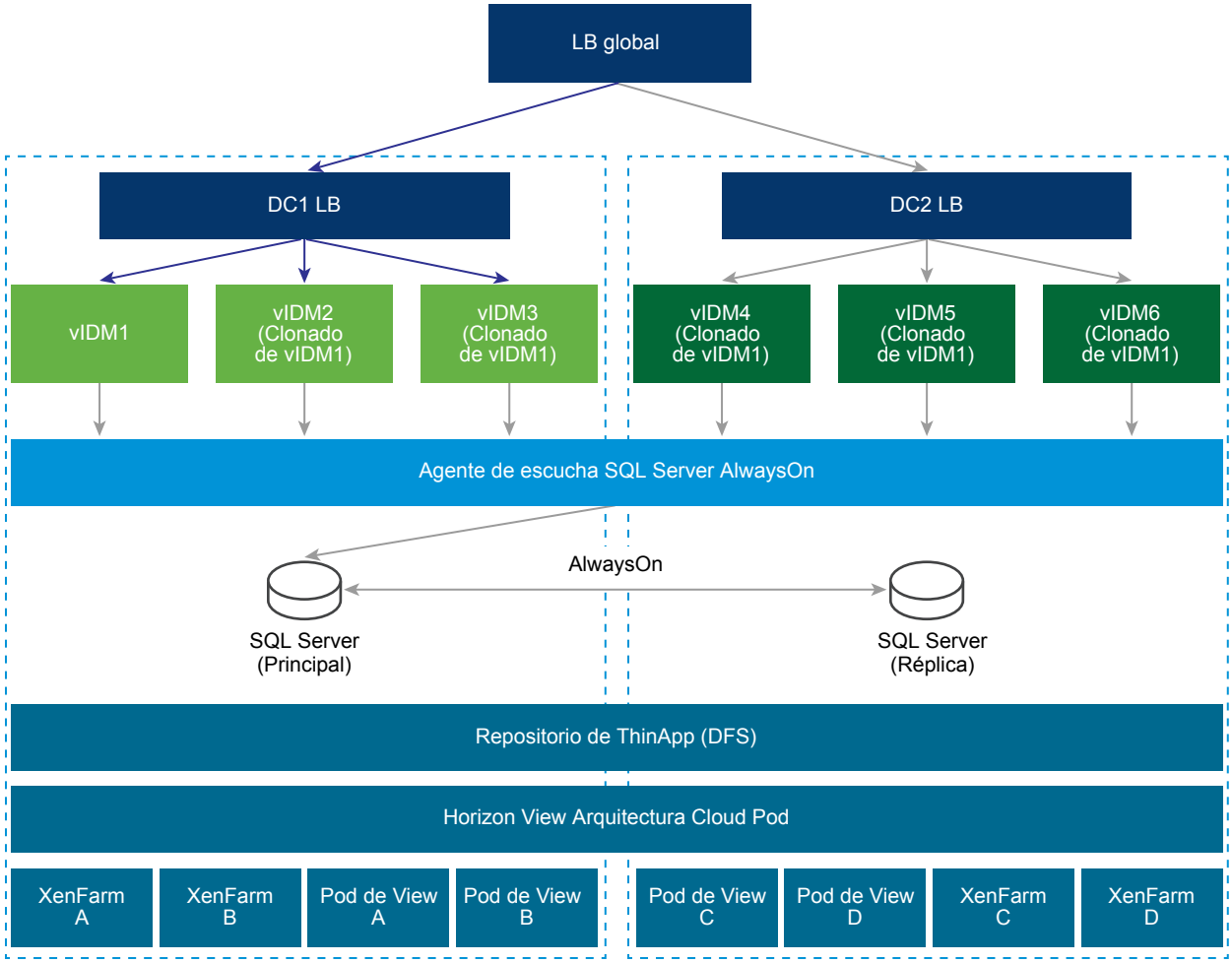
6 Haga clic en **Guardar**.

Implementar VMware Identity Manager en un centro de datos secundario para la conmutación de error y la redundancia

Para proporcionar funcionalidades de conmutación por error si el centro de datos de VMware Identity Manager primario no se encuentra disponible, es necesario que VMware Identity Manager se implemente en un centro de datos secundario.

Al usar un centro de datos secundario, los usuarios finales pueden iniciar sesión y usar las aplicaciones sin tiempo de inactividad. Un centro de datos secundario también le proporciona a los administradores la capacidad de actualizar VMware Identity Manager a la siguiente versión sin ningún tiempo de inactividad. Consulte “Actualizar VMware Identity Manager sin tiempo de inactividad,” página 99.

A continuación se muestra una implementación típica con un centro de datos secundario.



Siga estas instrucciones para realizar una implementación de centro de datos múltiple.

- Implementación del clúster: es necesario implementar como un clúster un grupo de tres o más dispositivos virtuales de VMware Identity Manager en un centro de datos y otro grupo de tres o más dispositivos virtuales como otro clúster en el segundo centro de datos. Consulte "Configurar un centro de datos secundario," página 89 para obtener más información.
- Base de datos: VMware Identity Manager usa la base de datos para almacenar información. Para realizar una implementación de un centro de datos múltiple, es crucial la replicación de las bases de datos entre los dos centros de datos. Consulte la documentación de la base de datos para obtener más información sobre cómo configurar una base de datos en centros de datos múltiples. Por ejemplo, con SQL Server, se recomienda la implementación de AlwaysOn. Consulte Grupos de disponibilidad AlwaysOn (SQL Server) en el sitio web de Microsoft para obtener más información. Las funciones de VMware Identity Manager esperan una latencia muy baja entre la base de datos y el dispositivo de VMware Identity Manager. Por lo tanto, se espera que los dispositivos en un centro de datos se conecten a la base de datos del mismo centro de datos.
- No activo-Activo: VMware Identity Manager no es compatible con una implementación Activo-Activo donde se puede proporcionar usuarios desde ambos centros de datos al mismo tiempo. El centro de datos secundario es un método de espera activa y se puede usar para proporcionar a los usuarios finales una continuidad del trabajo. Los dispositivos de VMware Identity Manager en el centro de datos secundario están en modo de solo lectura. Por lo tanto, después de producirse una conmutación por error en ese centro de datos, no funcionarán la mayoría de las operaciones de administrador, como agregar usuarios o aplicaciones o autorizar usuarios.

- Conmutación por recuperación en el primario: en la mayoría de los escenarios de error, puede realizar una conmutación por recuperación en el centro de datos primario una vez que vuelva a la normalidad. Para obtener más información, consulte "Realizar una conmutación por recuperación en el centro de datos primario," página 98.
- Ascender el secundario a primario: en caso de un error extendido del centro de datos, el centro de datos secundario puede pasar a ser primario. Para obtener más información, consulte "Ascender un centro de datos secundario a primario," página 98.
- Nombre de dominio completo: el nombre de dominio completo para acceder a VMware Identity Manager debe ser el mismo en todos los centros de datos.
- Auditorías: VMware Identity Manager usa Elasticsearch incrustado en el dispositivo de VMware Identity Manager para realizar informes de la auditoría y para los registros de sincronización de los directorios. Se deben crear clústeres de Elasticsearch independientes en cada centro de datos. Consulte "Configurar un centro de datos secundario," página 89 para obtener más información.
- Active Directory: VMware Identity Manager puede conectarse a Active Directory con la API LDAP o con la Autenticación de Windows integrada. En ambos métodos, VMware Identity Manager puede utilizar los informes SRV de Active Directory para llegar al controlador de dominio apropiado de cada centro de datos.
- Aplicaciones de Windows: VMware Identity Manager admite acceder a las aplicaciones de Windows con ThinApp, así como a los escritorios y las aplicaciones de Windows con las tecnologías Horizon View o Citrix. Suele ser importante enviar estos recursos desde un centro de datos cercano al usuario, también denominado Geo-Affinity. Tenga en cuenta los siguientes aspectos sobre los recursos de Windows:
  - ThinApp: VMware Identity Manager admite Windows Distributed File Systems como un repositorio de ThinApp. Use la documentación de Windows Distributed File Systems para configurar las directivas específicas de la ubicación.
  - Horizon View (con Arquitectura Cloud Pod): VMware Identity Manager admite la Horizon Arquitectura Cloud Pod. La Horizon Arquitectura Cloud Pod proporciona Geo-Affinity con autorizaciones globales. Consulte "Integrar las implementaciones de la Arquitectura Cloud Pod" en *Configurar recursos en VMware Identity Manager* para obtener más información. No son necesarios cambios adicionales para la implementación de un centro de datos múltiple de VMware Identity Manager.
  - Horizon View (sin la Arquitectura Cloud Pod): si la Horizon Arquitectura Cloud Pod no está habilitada en su entorno, no puede habilitar Geo-Affinity. Después de un evento de conmutación por error, puede cambiar de forma manual VMware Identity Manager para iniciar los recursos de Horizon View desde los pods de View configurados en el centro de datos secundario. Consulte "Configurar el orden de conmutación por error de los recursos basados en Citrix y en Horizon View," página 95 para obtener más información.
  - Recursos de Citrix: como con Horizon View (sin la Arquitectura Cloud Pod), no puede habilitar los recursos de Citrix para Geo-Affinity. Después de un evento de conmutación por error, puede cambiar de forma manual VMware Identity Manager para iniciar los recursos de Citrix desde XenFarms configurados en el centro de datos secundario. Consulte "Configurar el orden de conmutación por error de los recursos basados en Citrix y en Horizon View," página 95 para obtener más información.

Configurar un centro de datos secundario

El centro de datos secundario se administra normalmente con un servidor vCenter distinto. Al configurar el centro de datos secundario puede configurar e implementar lo siguiente según sus necesidades.

- Los dispositivos de VMware Identity Manager en el centro de datos secundario, creados a partir de un archivo OVA importado del centro de datos primario

- Equilibrador de carga del centro de datos secundario
- Autorizaciones y recursos basados en Citrix y Horizon View duplicado
- Configuración de base de datos
- Entrada de DNS o del equilibrador de carga en los centros de datos primario y secundario para conmutación por error

Modificar el centro de datos primario para la replicación

Antes de configurar el centro de datos secundario, configure el primario para las replicaciones de Elasticsearch, RabbitMQ y Ehcache en los clústeres.

Elasticsearch, RabbitMQ y Ehcache se incrustan en el dispositivo virtual de VMware Identity Manager. Elasticsearch es un motor de búsqueda y de análisis usado para los registros de sincronización de directorios, informes y auditorías. RabbitMQ es un agente de mensajería. Ehcache proporciona funciones de almacenamiento en caché.

Configure estos cambios en todos los nodos del clúster del centro de datos primario.

Prerequisitos

Puede configurar un clúster de VMware Identity Manager en el centro de datos primario.

Procedimiento

1 Configure Elasticsearch para la replicación.

  Realice estos cambios en cada nodo del clúster del centro de datos primario.

  a Deshabilite la tarea de cron de Elasticsearch.

    1 Edite el archivo `/etc/cron.d/hznelasticsearchsync`:

      ```
      vi /etc/cron.d/hznelasticsearchsync
      ```

    2 Realice los comentarios fuera de esta línea:

      ```
      #*/1 * * * * root /usr/local/horizon/scripts/elasticsearchnodes.hzn
      ```

  b Agregue las direcciones IP de todos los nodos del clúster del centro de datos primario.

    1 Edite el archivo `/etc/sysconfig/elasticsearch`.

      ```
      vi /etc/sysconfig/elasticsearch
      ```

    2 Agregue las direcciones IP de todos los nodos del clúster:

      ```
      ES_UNICAST_HOSTS=DirecciónIP1,DirecciónIP2,DirecciónIP3
      ```

  c Agregue el FQDN del equilibrador de carga del clúster del centro de datos secundario en el archivo `/usr/local/horizon/conf/runtime-config.properties`.

    1 Edite el archivo `/usr/local/horizon/conf/runtime-config.properties`.

      ```
      vi /usr/local/horizon/conf/runtime-config.properties
      ```

    2 Agregue esta línea al archivo:

      ```
      analytics.replication.peers=LB_FQDN_of_second_cluster
      ```

2 Configure RabbitMQ para la replicación.

Realice estos cambios en cada nodo del clúster del centro de datos primario.

a Deshabilite la tarea de cron de RabbitMQ.

1 `vi /etc/cron.d/hznrabbitmqsync`

2 Realice los comentarios fuera de esta línea:

```
#*/1 * * * * root /usr/local/horizon/scripts/rabbitmqnodes.hzn
```

b Realice los siguientes cambios en el archivo `/usr/local/horizon/scripts/rabbitmqnodes.hzn`.

1 `vi /usr/local/horizon/scripts/rabbitmqnodes.hzn`

2 Realice los comentarios fuera de estas líneas.

```
#make sure SAAS is up, otherwise we won't have an accurate node list
#if test $(curl –X GET –k https://localhost/SAAS/API/1.0/REST/system/health/allOk –
sL –w "% {http_code}\\n" –o /dev/null) –ne 200 ; then
#    echo SAAS not running, aborting
#    exit 0
#fi
```

También comente fuera de la siguiente línea.

```
#nodes=$(uniqList true $(enumeratenodenames))
```

3 Agregue los nombres de host de todos los nodos del clúster del centro de datos primario. Use únicamente los nombres del host, no los nombres de dominio completo. Separe los nombres con un espacio.

```
nodes="nodo1 nodo2 nodo3"
```

c Agregue la asignación del nombre de host y la dirección IP del resto de nodos en el clúster en el archivo `/etc/hosts`. No agregue una entrada para el nodo que está editando. Este paso solo es necesario si no hay ninguna entrada DNS que pueda resolver el nombre de dominio completo o nombres de dominio parciales.

```
DirecciónIP nodo2FQDN nodo2

DirecciónIP nodo3FQDN nodo3
```

d Ejecute el script para compilar el clúster RabbitMQ.

```
/usr/local/horizon/scripts/rabbitmqnodes.hzn
```

3 Configure Ehcache para la replicación.

Realice estos cambios en cada nodo del clúster del centro de datos primario.

a `vi /usr/local/horizon/conf/runtime–config.properties`

b Agregue el FQDN del resto de nodos del clúster. No agregue el FQDN del nodo que está editando. Separe los FQDN con dos puntos.

```
ehcache.replication.rmi.servers=nodo2FQDN:nodo3FQDN
```

Por ejemplo:

```
ehcache.replication.rmi.servers=server2.example.com:server3.example.com
```

4 Reinicie el servicio de VMware Identity Manager en todos los nodos.

```
service horizon–workspace restart
```

5 Compruebe que el clúster está configurado correctamente.

Ejecute estos comandos en todos los nodos del primer clúster.

a Compruebe el estado de Elasticsearch.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

El comando debe devolver un resultado similar al siguiente.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Si aparecen problemas, consulte "Solucionar problemas de Elasticsearch y RabbitMQ," página 110.

b Compruebe el estado de RabbitMQ.

```
rabbitmqctl cluster_status
```

El comando debe devolver un resultado similar al siguiente.

```
Cluster status of node 'rabbitmq@node3' ...
[{nodes,[{disc,['rabbitmq@node2','rabbitmq@node3']}]},
 {running_nodes,['rabbitmq@node3']},
 {cluster_name,<<"rabbitmq@node2.example.com">>},
 {partitions,[]},
 {alarms,[{'rabbitmq@node3',[]}]}]
```

Si aparecen problemas, consulte "Solucionar problemas de Elasticsearch y RabbitMQ," página 110.

c Compruebe que el archivo `/opt/vmware/horizon/workspace/logs/ horizon.log` contiene esta línea.

```
Added ehcache replication peer: //node3.example.com:40002
```

Los nombres de los hosts deben ser los de los otros nodos del clúster.

Qué hacer a continuación

Cree un clúster en el centro de datos secundario. Cree los nodos exportando el archivo OVA del primer dispositivo virtual de VMware Identity Manager desde el clúster del centro de datos primario y usándolo para implementar los nuevos dispositivos virtuales en el centro de datos secundarios.

Crear dispositivos virtuales de VMware Identity Manager en centros de datos secundarios

Para configurar un clúster de VMware Identity Manager en un centro de datos secundario, debe exportar el archivo OVA del dispositivo de VMware Identity Manager original en el centro de datos primario y usarlo para implementar dispositivos en el secundario.

Prerequisitos

- El archivo OVA de VMware Identity Manager que se exportó del dispositivo VMware Identity Manager original en el centro de datos principal
- Direcciones IP y registros DNS del centro de datos secundario

Procedimiento

1 En el centro de datos primario, exporte el archivo OVA del dispositivo de VMware Identity Manager original.

Consulte la documentación de vSphere para obtener más información.

2 En el centro de datos secundario, implemente el archivo OVA de VMware Identity Manager que se exportó para crear los nuevos nodos.

Consulte la documentación de vSphere para obtener más información. Consulte también "Instalación del archivo OVA de VMware Identity Manager," página 19.

3 Después de encender los dispositivos de VMware Identity Manager, actualice la configuración de cada uno de ellos.

Los dispositivos de VMware Identity Manager del centro de datos secundario son copias idénticas del dispositivo de VMware Identity Manager original del centro de datos principal. La sincronización con Active Directory y los recursos configurados en el centro de datos principal está deshabilitada.

Qué hacer a continuación

Vaya a las páginas de consola de administración y configure lo siguiente:

- Habilite la opción Unirse al dominio como se configuró en el dispositivo virtual de VMware Identity Manager original del centro de datos principal.
- En la página Adaptadores de autenticación, agregue los métodos de autenticación que están configurados en el centro de datos principal.
- En la página Método de autenticación de directorio, habilite la autenticación de Windows, si está configurada en el centro de datos principal.

Diríjase a la página Instalar el certificado de configuración de dispositivos para agregar certificados firmados por la entidad de certificación, duplicando los certificados de los dispositivos de VMware Identity Manager del centro de datos principal. Consulte "Utilizar certificados SSL," página 38.

Configurar nodos en el centro de datos secundario

Después de crear nodos en el centro de datos secundario con el archivo OVA exportado del primario, configure los nodos.

Realice estos pasos en cada nodo del centro de datos secundario.

Procedimiento

- Actualice las tablas de IP.
  a. Compruebe que existe el archivo `/usr/local/horizon/conf/flags/enable.rabbitmq`.

     ```
     touch /usr/local/horizon/conf/flags/enable.rabbitmq
     ```

  b. En el archivo `/usr/local/horizon/scripts/updateiptables.hzn`, actualice las direcciones IP de todos los nodos en el centro de datos secundario.

     1. `vi /usr/local/horizon/scripts/updateiptables.hzn`
     2. Busque y reemplace la línea `ALL_IPS`. Especifique las direcciones IP separadas con un espacio.

        ```
        ALL_IPS="DirecciónIP_Nodo1 DirecciónIP_Nodo2 DirecciónIP_Nodo3"
        ```

     3. Ejecute este script para abrir los puertos.

        ```
        /usr/local/horizon/scripts/updateiptables.hzn
        ```

  c. Configure los nodos para las replicaciones de Ehcache, Elasticsearch y RabbitMQ, y compruebe que se configuraron correctamente.

     Consulte las instrucciones que aparecen en "Modificar el centro de datos primario para la replicación," página 90 y aplíquelas a los nodos del centro de datos secundario.

     Tenga en cuenta que las tareas de cron ya están deshabilitadas.

Editar el archivo runtime-config.properties en el centro de datos secundario

Si usa una base de datos diferente a una implementación SQL Server AlwaysOn, debe editar los archivos `runtime-config.properties` de los dispositivos de VMware Identity Manager en el centro de datos secundario para que la URL de JDBC se dirija a la base de datos del centro de datos secundario y para configurar el dispositivo para el acceso de solo lectura. Si usa una implementación SQL Server AlwaysOn, este paso no es necesario.

Realice estos cambios en cada dispositivo de VMware Identity Manager en el centro de datos secundario.

Procedimiento

1. Con un cliente ssh, inicie sesión en el dispositivo VMware Identity Manager como usuario root.
2. Abra el archivo `runtime-config.properties` en `/usr/local/horizon/conf/runtime-config.properties`.
3. Cambie la URL de JDBC para que dirija a la base de datos del centro de datos secundario.

   Consulte "Configure VMware Identity Manager para usar una base de datos externa," página 37.
4. Configure el dispositivo VMware Identity Manager para que tenga acceso de solo lectura.

   Agregue la línea `read.only.service=true`.
5. Reinicie el servicio Tomcat en el dispositivo.

   ```
   service horizon-workspace restart
   ```

Configurar el orden de conmutación por error de los recursos basados en Citrix y en Horizon View

Para los recursos basados en Citrix y Horizon View, debe configurar el orden de conmutación por error de los recursos en centros de datos principales y secundarios para que los recursos apropiados estén disponibles desde cualquier centro de datos.

El comando hznAdminTool permite crear una tabla de base de datos con el orden de conmutación por error de los recursos de su organización por instancia de servicio. Al iniciar un recurso se sigue el orden de conmutación por error configurado. Se ejecuta `hznAdminTool failoverConfiguration` en ambos centros de datos para configurar el orden de conmutación por error.

Prerequisitos

Al implementar VMware Identity Manager en varios centros de datos, también se configuran los mismos recursos en cada uno de ellos. Cada grupo de escritorios o aplicaciones de los pods de View o XenFarms de Citrix se considera como un grupo diferente en el catálogo de VMware Identity Manager. Para evitar la duplicación de los recursos en el catálogo, asegúrese de haber habilitado **No sincronizar aplicaciones duplicadas** en los grupos de View o las páginas Aplicaciones publicadas - Citrix en la página consola de administración.

Procedimiento

1 Con un cliente ssh, inicie sesión en el dispositivo VMware Identity Manager como usuario root.

2 Para ver una lista de las instancias de servidor, introduzca `hznAdminTool serviceInstances`.

Se mostrará una lista de las instancias de servicio con el número de ID asignado, como en el ejemplo siguiente.

```
{"id":103,"hostName":"ws4.domain.com","ipaddress":"10.142.28.92"}{"id":
154,"hostName":"ws3.domain.com","ipaddress":"10.142.28.91"}{"id":
1,"hostName":"ws1.domain.com","ipaddress":"10.143.104.176"}{"id":
52,"hostName":"ws2.domain.com","ipaddress":"10.143.104.177"}
```

3 Para cada instancia de servicio de su organización, configure el orden de conmutación por error de los recursos de Citrix y View.

Escriba `hznAdminTool failoverConfiguration –configType <configType> –configuration <configuration> –serviceInstanceId <serviceInstanceId> [–orgId <orgId>]`.

Opción	Descripción
-configType	Introduzca el tipo de recurso que se configura para la conmutación por error. Los valores pueden ser `VIEW` o `XENAPP`.
-configuration	Introduzca el orden de la conmutación por error. Para VIEW configType, escriba en una lista separada por comas los nombres de host del servidor del conector de View principal que se enumeran en la página Grupos de View de la consola de administración. Para XENAPP configType, introduzca los nombres de XenFarm en una lista separada por comas.
-serviceInstanceId	Introduzca el ID de la instancia del servicio para el que se ha definido la configuración. Puede encontrar el ID en la lista mostrada en el paso 2, `"id":`
-orgId	(Opcional). Si se deja en blanco, se define la configuración para la organización predeterminada.

Por ejemplo, `hznAdminTool failoverConfiguration –configType VIEW –configuration pod1vcs1.domain.com,pod2vcs1.hs.trcint.com –orgId 1 –serviceInstanceId 1`.

Al introducir este comando para las instancias de VMware Identity Manager en el centro de datos secundario, invierta el orden de los servidores de conexión de View. En este ejemplo, el comando sería `hznAdminTool failoverConfiguration –configType VIEW –configuration pod2vcs1.hs.trcint.com, pod1vcs1.domain.com –orgId 1 –serviceInstanceId 103`

La tabla de la base de datos de la conmutación por error de los recursos se configura para cada centro de datos.

Qué hacer a continuación

Para ver la configuración de la conmutación por error ya existente de cada uno de los recursos de Citrix y View, ejecute `hznAdminTool failoverConfigurationList –configType <configtype> –<orgId)`.

El valor de <configtype> es VIEW o XENAPP. A continuación, se muestra un ejemplo de la salida de `hznAdminTool failoverConfiguraitonList` con configType VIEW.

```
{"idOrganization":1,"serviceInstanceId":
52,"configType":"VIEW","configuration":"pod1vcs1.domain.com,pod2vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
103,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
154,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
```

Configurar la base de datos para la conmutación por error

En VMware Identity Manager, la replicación de la base de datos se configura para que los datos sean consistentes en los servidores de la base de datos dentro del centro de datos principal y el centro de datos secundario.

Debe configurar la base de datos externa para obtener una alta disponibilidad. Configure una arquitectura de base de datos principal y subordinada, en la que la subordinada sea una réplica exacta de la principal.

Consulte la documentación de la base de datos externa.

Si usa SQL Server AlwaysOn, use el nombre del host o la dirección IP del agente de escucha SQL Server cuando configure la base de datos en cada dispositivo de VMware Identity Manager. Por ejemplo:

`jdbc:sqlserver://<nombredelhost_agentedeescucha>;DatabaseName=saas`

Realizar una conmutación por error en el centro de datos secundario

Cuando se produce un error en el centro de datos primario, puede realizar una conmutación por error en el secundario. Para realizar este proceso, modifique el equilibrador de carga global o el informe DNS para que se dirijan al equilibrador de carga en el centro de datos secundario.

Dependiendo de la configuración de la base de datos, los dispositivos de VMware Identity Manager en el centro de datos secundarios están en modo de solo lectura o en modo de lectura y escritura. Para todas las bases de datos, excepto SQL Server AlwaysOn, los dispositivos VMware Identity Manager se encuentran en modo de solo lectura. Por lo tanto, la mayoría de las operaciones del administrador, como agregar usuarios o aplicaciones o autorizar a los usuarios, no están disponibles.

Si usa una implementación SQL Server AlwaysOn, los dispositivos de VMware Identity Manager en el centro de datos secundario se encuentran en modo de lectura y escritura.

Utilizar un registro de DNS para controlar qué centro de datos está activo

Si se utiliza un registro de Domain Name System (DNS) para dirigir el tráfico de los usuarios en los centros de datos, este registro debe señalar a un equilibrador de carga del centro de datos principal en condiciones de funcionamiento normales.

Si el centro de datos principal no está disponible, el registro de DNS se debe actualizar para que señale al equilibrador de carga del centro de datos secundario.

Cuando el centro de datos principal vuelve a estar disponible, el registro de DNS se debe actualizar para que señale al equilibrador de carga del centro de datos principal.

Configurar el tiempo de vida en el registro de DNS

El valor del parámetro tiempo de vida (TTL) determina el tiempo que debe transcurrir para que se actualice la información relativa a DNS en la caché. Para que la conmutación por error se realice correctamente en aplicaciones y escritorios de View, asegúrese de que el valor del tiempo de vida (TTL) en el registro de DNS sea reducido. Si el valor de TTL es demasiado largo, es posible que los usuarios no puedan acceder a sus aplicaciones y escritorios de View inmediatamente después de la conmutación por error. Para habilitar la actualización rápida de DNS, establezca el valor de TTL de DNS en 30 segundos.

Actividades de VMware Identity Manager no disponibles en modo de solo lectura

El uso de VMware Identity Manager en modo de solo lectura está diseñado para alta disponibilidad y para permitir a los usuarios finales acceder a los recursos de sus portales Mis aplicaciones. Puede que algunas de las actividades de la consola de administración de VMware Identity Manager y otras páginas de servicios de administración no estén disponibles en modo de solo lectura. A continuación se proporciona una lista de actividades habituales que no están disponibles.

Si VMware Identity Manager se ejecuta en modo de solo lectura, no se pueden realizar actividades relacionadas con cambios en Active Directory o en la base de datos y no funciona la sincronización con la base de datos de VMware Identity Manager.

Las funciones administrativas que necesitan escribir en la base de datos no están disponibles durante este tiempo. Se debe esperar a que VMware Identity Manager vuelva al modo de lectura y escritura.

Modo de solo lectura de la consola de administración de VMware Identity Manager

A continuación se indican algunas de las limitaciones de la consola de administración en modo de solo lectura.

- Agregar, eliminar y editar usuarios y grupos en la pestaña **Usuarios y grupos**
- Agregar, eliminar y editar aplicaciones en la pestaña **Catálogo**
- Agregar, eliminar y editar autorizaciones de aplicaciones
- Cambiar la información de marca
- Sincronizar el directorio para agregar, editar y eliminar usuarios y grupos
- Editar información sobre recursos, incluyendo recursos de View, XenApp y de otro tipo
- Editar la página de métodos de autenticación

NOTA: Los componentes del conector de los dispositivos de VMware Identity Manager del centro de datos secundario aparecen en la consola de administración. Asegúrese de no seleccionar un conector del centro de datos secundario como conector de sincronización.

Modo de solo lectura de las páginas Configuración del dispositivo virtual

A continuación se indican algunas de las limitaciones de las páginas Configuración del dispositivo virtual en modo de solo lectura.

- Comprobar la configuración de la conexión de la base de datos
- Cambiar la contraseña de administrador en la página Cambiar contraseña

Modo de solo lectura del portal de aplicaciones del usuario final

Cuando VMware Identity Manager está en modo de solo lectura, los usuarios pueden iniciar la sesión en sus portales de VMware Identity Manager y acceder a sus recursos. En modo de solo lectura no están disponibles las siguientes funciones en el portal del usuario.

- Marcar o desmarcar un recurso como favorito
- Agregar recursos en la página Catálogo o eliminarlos en la página Programa de inicio
- Cambiar la contraseña desde la página del portal de aplicaciones

Modo de solo lectura del cliente de Windows de VMware Identity Manager

Si VMware Identity Manager está en modo de solo lectura, los usuarios no pueden configurar nuevos clientes de Windows. Los clientes de Windows existentes seguirán funcionando.

Realizar una conmutación por recuperación en el centro de datos primario

En la mayoría de los escenarios de error, puede realizar una conmutación por recuperación en el centro de datos primario una vez que vuelva a funcionar.

Procedimiento

1 Modifique el equilibrador de carga global o el informe DNS para que se dirijan al equilibrador de carga en el centro de datos primario.

Consulte "Utilizar un registro de DNS para controlar qué centro de datos está activo," página 97.

2 Limpie la caché en el centro de datos secundario.

Puede usar las REST API para limpiar la caché.

PATH: /SAAS/jersey/manager/api/removeAllCaches

Método: POST

Funciones permitidas: solo OPERATOR

Ascender un centro de datos secundario a primario

En caso de un error extendido del centro de datos, el centro de datos secundario puede pasar a ser primario.

No es necesario ningún cambio en una implementación SQL Server AlwaysOn. Para otras configuraciones de los centros de datos, es necesario editar el archivo `runtime-config.properties` en los dispositivos de VMware Identity Manager del centro de datos secundario para establecer la configuración del modo de lectura y escritura en estos dispositivos.

Realice estos cambios en cada dispositivo de VMware Identity Manager en el centro de datos secundario.

Procedimiento

1 Con un cliente ssh, inicie sesión en el dispositivo VMware Identity Manager como usuario root.

2 Abra el archivo `/usr/local/horizon/conf/runtime-config.properties` para editarlo.

3 Cambie la línea `read.only.service=true` a `read.only.service=false`.

4 Guarde el archivo `runtime-config.properties`.

5 Reinicie el servicio Tomcat en el dispositivo.

```
service horizon-workspace restart
```

Actualizar VMware Identity Manager sin tiempo de inactividad

Con una implementación de centro de datos múltiple, puede realizar una actualización de VMware Identity Manager a la versión siguiente sin tiempo de inactividad. Use el flujo de trabajo sugerido para realizar actualizaciones graduales.

Consulte el diagrama que aparece en "Implementar VMware Identity Manager en un centro de datos secundario para la conmutación de error y la redundancia," página 87 mientras realiza estos pasos.

Procedimiento

1 Cambie el enrutamiento del LB global para que envíe la solicitudes al DC2 LB.

2 Detenga la replicación de la base de datos.

3 Actualice el dispositivo virtual vIDM1, a continuación el vIDM2 y, finalmente, el vIDM3.

4 Pruebe las actualizaciones usando DC1-LB.

5 Cuando esté todo correcto, cambie a LB global para enrutar las solicitudes a DC1 LB.

6 Actualice el dispositivo virtual vIDM4, a continuación el vIDM5 y, finalmente, el vIDM6.

7 Pruebe las actualizaciones usando DC2-LB.

8 Inicie la replicación de la base de datos.

Instalación de dispositivos de conector adicionales

7

El conector es una parte del servicio VMware Identity Manager. Al instalar un dispositivo virtual VMware Identity Manager, se incluye siempre un componente de conector de manera predeterminada.

El conector realiza las funciones siguientes.

- Sincroniza los datos de usuario y grupo entre el directorio empresarial y el directorio correspondiente que creó en el servicio.
- Cuando se usa como un proveedor de identidades, autentica usuarios en el servicio.

  El conector es el proveedor de identidades predeterminado.

Como ya hay un conector disponible como parte del servicio, en las implementaciones típicas no se necesita instalar un conector adicional.

Sin embargo, en algunos casos, puede que necesite un conector adicional. Por ejemplo:

- Si tiene varios directorios del tipo Active Directory (autenticación IWA), necesita un conector diferente para cada uno de ellos.

  Se puede asociar una instancia de conector a varios directorios. En el conector, se crea una partición llamada trabajo para cada directorio. Sin embargo, no puede tener dos trabajos del tipo de autenticación IWA en la misma instancia de conector.
- Si desea administrar el acceso de los usuarios en función de si inician sesión desde una ubicación interna o externa.
- Si desea usar una autenticación basada en certificado pero su equilibrador de carga está configurado para terminar SSL en el equilibrador de carga. La autenticación con certificado requiere el paso de SSL en el equilibrador de carga.

Para instalar un conector adicional, realice las tareas siguientes.

- Descargue el paquete OVA del conector.
- Genere un token de activación en el servicio.
- Implemente el dispositivo virtual del conector.
- Configure las opciones del conector.

Los conectores adicionales que implemente se mostrarán en la interfaz de usuario del servicio.

Este capítulo cubre los siguientes temas:

Generación de un código de activación para el conector

Antes de implementar el dispositivo virtual del conector, genere un código de activación para el nuevo conector desde el servicio de VMware Identity Manager. El código de activación del conector se usa para establecer la comunicación entre el servicio y el conector.

Procedimiento

1 Inicie sesión en la consola de administración de VMware Identity Manager.

2 Haga clic en la pestaña **Administración de acceso e identidad**.

3 Haga clic en **Configurar**.

4 En la página Conectores, haga clic en **Agregar conector**.

5 Introduzca un nombre para la nueva instancia del conector.

6 Haga clic en **Generar código de activación**.

El código de activación se muestra en el campo **Código de activación del conector**.

7 Copie el código de activación del conector y guárdelo.

Usará este código de activación al ejecutar el asistente de configuración de conectores.

Qué hacer a continuación

Instale el dispositivo virtual del conector.

Implementar el archivo OVA de Conector

Para descargar el archivo OVA de conector e implementarlo, debe utilizar VMware vSphere Client o vSphere Web Client.

Prerequisitos

- Identifique los registros de DNS y el nombre de host que utilizará para la implementación de OVA de conector.
- Si utiliza vSphere Web Client, utilice los navegadores Firefox o Chrome. No utilice Internet Explorer para implementar el archivo OVA.
- Descargue el archivo OVA de Connector.

Procedimiento

1 En vSphere Client o vSphere Web Client, seleccione **Archivo > Implementar plantilla de OVF**.

2 En las páginas de Implementar plantilla de OVF, introduzca la información específica de su implementación de conector.

Página	Descripción
Origen	Desplácese hasta la ubicación del paquete de OVA o introduzca una URL específica.
Detalles de la plantilla de OVA	Compruebe que seleccionó la versión correcta.
Licencia	Lea el Contrato de licencia para el usuario final y haga clic en **Aceptar**.
Nombre y ubicación	Introduzca un nombre para el dispositivo virtual. El nombre debe ser único en la carpeta de inventario y puede tener hasta 80 caracteres. Los nombres distinguen entre mayúsculas y minúsculas. Seleccione una ubicación para el dispositivo virtual.

Página	Descripción
Host / Clúster	Seleccione el host o el clúster en el que desea ejecutar la plantilla implementada.
Grupo de recursos	Seleccione el grupo de recursos.
Almacenamiento	Seleccione la ubicación en la que desea almacenar los archivos de la máquina virtual.
Formato de disco	Seleccione el formato de disco de los archivos. Para entornos de producción, seleccione un formato **Thick Provision**. Para evaluación y realización de pruebas, seleccione un formato **Thin Provision**.
Asignación de redes	Asigne las redes de su entorno a las redes de la plantilla de OVF.
Propiedades	a En el campo **Configuración de zona horaria**, seleccione la zona horaria correcta. b La casilla de verificación Programa de mejora de la experiencia del cliente está seleccionada de forma predeterminada. VMware recopila datos anónimos sobre su implementación con el fin de mejorar la respuesta de VMware a los requisitos del usuario. Anule la selección de la casilla si no desea que se recopilen datos. c En el cuadro de texto Nombre de host, introduzca el host que desea utilizar. Si se deja en blanco, se utilizará la DNS inversa para buscar el nombre de host. d Si desea configurar la dirección IP estática para conector, introduzca la dirección de cada una de las opciones siguientes: Puerta de enlace predeterminada, DNS, dirección IP y Máscara de red. **IMPORTANTE:** Si alguno de los cuatro campos de dirección, incluido Nombre de host, se deja en blanco, se utiliza DHCP. Para configurar DHCP, deje en blanco los campos de dirección.
Listo para finalizar	Revise las selecciones y haga clic en **Finalizar**.

En función de la velocidad de la red, la implementación puede tardar varios minutos. Puede ver el progreso en el cuadro de diálogo de progreso.

3 Cuando la implementación finalice, seleccione el dispositivo, haga clic con el botón derecho y seleccione **Power > Power on**.

El dispositivo se inicializará. Para ver los detalles, vaya a la pestaña **consola**. Cuando el dispositivo se inicialice, la pantalla de la consola mostrará la versión de y las URL de inicio de sesión en el asistente de configuración para finalizar la configuración.

Qué hacer a continuación

El asistente de configuración permite agregar el código de activación y las contraseñas administrativas.

Configurar las opciones de Conector

Después de implementar e instalar el OVA del conector, debe ejecutar el asistente de configuración para activar el dispositivo y configurar las contraseñas del administrador.

Prerequisitos

- Debe tener el código de activación del nuevo conector. Consulte "Generación de un código de activación para el conector," página 102.
- Asegúrese de que el dispositivo del conector esté encendido y que dispone de la URL del conector.
- Recopile una lista de contraseñas para utilizarlas en la cuenta raíz, la cuenta sshuser y el administrador del conector.

Procedimiento

1 Para ejecutar el asistente de configuración, introduzca la URL del conector que se mostró en la pestaña Consola tras implementar el OVA.

2 En la página principal, haga clic en **Continuar**.

3 Cree contraseñas seguras para las siguientes cuentas de administrador del dispositivo virtual de conector.

Las contraseñas seguras deben tener al menos ocho caracteres e incluir mayúsculas, minúsculas y al menos un dígito o un carácter especial.

Opción	Descripción
Administrador del dispositivo	Cree la contraseña del administrador del dispositivo. El nombre de usuario es **admin** y no se puede cambiar. Debe utilizar esta cuenta y esta contraseña para iniciar sesión en los servicios del conector y administrar certificados, contraseñas del dispositivo y la configuración del registro del sistema. **IMPORTANTE:** La contraseña del usuario **admin** debe tener 6 caracteres como mínimo.
Cuenta raíz	Se utilizó una contraseña raíz predeterminada de VMware para instalar el dispositivo del conector. Cree una contraseña raíz nueva.
Cuenta sshuser	Cree la contraseña que va a utilizar para acceder de forma remota al dispositivo del conector.

4 Haga clic en **Continuar**.

5 En la página Activar Conector, pegue el código de activación y haga clic en **Continuar**.

El código de activación se verificará y se establecerá la comunicación entre el servicio y la instancia del conector.

La configuración del conector se completó.

Qué hacer a continuación

En el servicio, configure su entorno en función de sus necesidades. Por ejemplo, si agregó otro conector porque desea sincronizar dos directorios con autenticación de Windows integrada, cree el directorio y asócielo al nuevo conector.

Configure los certificados SSL del conector. Consulte "Utilizar certificados SSL," página 38.

Preparación para utilizar la autenticación Kerberos en dispositivos iOS

8

Cuando implementa inicialmente el servicio de VMware Identity Manager, la infraestructura actual de Active Directory se utiliza para la administración y autenticación de usuarios. Integre el servicio con otras soluciones de autenticación como, por ejemplo, Kerberos, Certificate y RSA SecurID desde la consola de administración. Para la autenticación SSO móvil en los dispositivo iOS administrados por AirWatch, puede iniciar manualmente el centro de distribución de claves (KDC, Key Distribution Center) en el dispositivo antes de habilitar el método de autenticación desde la consola de administración.

La autenticación de Kerberos proporciona acceso al portal de aplicaciones sin solicitudes adicionales de credenciales a los usuarios que iniciaron sesión en su dominio correctamente. Para admitir dispositivos iOS que utilicen Kerberos, VMware Identity Manager ofrece el método de autenticación Kerberos integrado SSO móvil para iOS, para acceder al KDC dentro del proveedor de identidades integrado sin el uso de un conector o de un sistema externo.

Después de iniciar el KBC y reiniciar el servicio, cree entradas de DNS públicas para permitir a los clientes de Kerberos encontrar el KBC.

Para utilizar el método de autenticación SSO móvil para iOS, debe configurar el servicio VMware Identity Manager y AirWatch. Consulte la sección sobre cómo implementar la autenticación Kerberos integrada en dispositivos iOS administrados por AirWatch de la guía de administración de VMware Identity Manager.

Este capítulo cubre los siguientes temas:

Decisiones de configuración de KDC previas

Antes de inicializar KDC en VMware Identity Manager, determine el nombre de territorio del servidor KDC, si la implementación incluye subdominios y si se utilizará o no el certificado del servidor KDC predeterminado.

Territorio

El territorio es el nombre de una entidad administrativa que mantiene los datos de autenticación. Es importante seleccionar un nombre descriptivo para el territorio de autenticación de Kerberos. El nombre del territorio debe formar parte de un dominio de DNS que la empresa pueda configurar.

El nombre del territorio y el nombre de dominio plenamente cualificado (FQDN) que se utilice para acceder al servicio VMware Identity Manager son independientes. Su empresa debe controlar los dominios de DNS tanto del nombre de territorio como del FQDN. La convención consiste en que el nombre del territorio sea el mismo que el de dominio, en mayúsculas. A veces, el nombre de territorio y el de dominio son diferentes. Por ejemplo, un nombre de territorio es *EXAMPLE.NET* y el FQDN de VMware Identity Manager es *idm.example.com*. En este caso, se definen las entradas de DNS tanto para el dominio *ejemplo.net* como para *ejemplo.com*.

El cliente de Kerberos utiliza el nombre de territorio para generar nombres de DNS. Por ejemplo, cuando el nombre es example.com, el nombre de Kerberos relacionado para contactar el KDC por TCP es *_kerberos._tcp.EXAMPLE.COM*.

Usar subdominios

El servicio VMware Identity Manager instalado en el propio entorno de las instalaciones puede utilizar el subdominio del FQDN de VMware Identity Manager. Si su sitio VMware Identity Manager accede a varios dominios DNS, configure los dominios como location1.example.com; location2.example.com; location3.example.com. El valor del subdominio es en este caso ejemplo.com, en minúsculas. Para configurar un subdominio en su entorno, consulte al equipo de su servicio de asistencia.

Utilizar certificados del servidor KDC

Al inicializar KDC, se generan un certificado del servidor y un certificado raíz autofirmado. El certificado se utiliza para emitir el certificado del servidor KDC. Este certificado raíz se incluye en el perfil del dispositivo para que este pueda confiar en KDC.

Para generar el certificado KDC manualmente, utilice un certificado raíz o intermedio de la empresa. Para obtener más información sobre esta función, contacte con el equipo de su servicio de asistencia.

El certificado raíz del servidor KDC se descarga de la consola de administración de VMware Identity Manager para utilizarlo en la configuración de AirWatch del perfil de administración del dispositivo iOS.

Inicializar el centro de distribución de claves en el dispositivo

Antes de poder utilizar el método de autenticación SSO móvil para iOS, se debe inicializar el centro de distribución de claves (KDC) en el dispositivo VMware Identity Manager.

Para iniciar KDC, se debe asignar el nombre de host de Identity Manager a los territorios de Kerberos. El nombre de dominio se introduce en mayúsculas. Si se están configurando varios territorios de Kerberos, para ayudar a identificar el territorio, utilice nombres descriptivos que acaben con el nombre de dominio de Identity Manager. Por ejemplo, VENTAS.MI-IDENTITYMANAGER.EJEMPLO.COM. Si se configuran subdominios, sus nombres se deben escribir en minúsculas.

Prerequisitos

VMware Identity Manager está instalado y configurado.

El nombre de territorio está identificado. Consulte "Decisiones de configuración de KDC previas," página 105.

Procedimiento

1 Acceda mediante SSH al dispositivo VMware Identity Manager como usuario root.

2 Inicialice KDC. Escriba `/etc/init.d/vmware-kdc init --realm {REALM.COM} --subdomain {sva-name.subdomain}`.

   Por ejemplo, `/etc/init.d/vmware-kdc init --realm MY-IDM.EXAMPLE.COM --subdomain my-idm.example.com`

   Si utiliza un equilibrador de carga con varios dispositivos Identity Manager, utilice el nombre del equilibrador de carga en ambos casos.

3 Reinicie el servicio VMware Identity Manager. Escriba `service horizon-workspace restart`.

4 Inicie el servicio KDC. Escriba `service vmware-kdc restart`.

Qué hacer a continuación

Cree las entradas de DNS públicas. Se deben aprovisionar los registros de DNS para permitir que los clientes encuentren el KDC. Consulte "Crear entradas de DNS públicas para KDC con Kerberos integrado," página 107.

Crear entradas de DNS públicas para KDC con Kerberos integrado

Tras inicializar KDC en VMware Identity Manager, debe crear registros de DNS públicos para permitir a los clientes de Kerberos buscar el servicio KDC cuando la función de autenticación de Kerberos integrado esté habilitada.

El nombre de territorio de KDC se utiliza como parte del nombre de DNS para las entradas del dispositivo de VMware Identity Manager que se utilizan para descubrir el servicio KDC. Se necesitan un registro SRV de DNS para cada sitio de VMware Identity Manager y dos entradas de direcciones.

NOTA: El valor de la entrada AAAA es una dirección IPv6 que codifica una dirección IPv4. Si el KDC no es direccionable a través de IPv6 y se utiliza una dirección IPv4, es posible que se deba especificar la entrada de AAAA en notación IPv6 estricta igual que `::ffff:175c:e147` en el servidor DNS. Puede utilizar una herramienta de conversión de IPv4 a IPv6 como la que hay disponible en Neustar.UltraTools, para convertir la notación de la dirección IPv4 a IPv6.

Ejemplo: Entradas de registro de DNS para KDC

En este registro de DNS de ejemplo, el territorio es `EXAMPLE.COM`; el nombre de dominio plenamente cualificado de VMware Identity Manager es `idm.example.com` y la dirección IP de VMware Identity Manager `1.2.3.4`.

```
idm.example.com.               1800 IN  AAAA         ::ffff:1.2.3.4

idm.example.com.               1800 IN  A            1.2.3.4

_kerberos._tcp.EXAMPLE.COM           IN  SRV  10  0   88 idm.example.com.

_kerberos._udp.EXAMPLE.COM           IN  SRV  10  0   88 idm.example.com.
```

Solucionar los problemas de la instalación y la configuración 9

Los temas sobre la solución de problemas describen soluciones a problemas potenciales que se puede encontrar al instalar o al configurar VMware Identity Manager.

Este capítulo cubre los siguientes temas:

Los usuarios no pueden iniciar aplicaciones o se aplica un método de autenticación incorrecto en entornos de carga equilibrada

Los usuarios no pueden iniciar aplicaciones desde el portal Workspace ONE o se aplica un método de autenticación incorrecto en un entorno de carga equilibrada.

Problema

En un entorno de carga equilibrada, pueden producirse problemas como los siguientes:

- Los usuarios no pueden iniciar aplicaciones desde el portal de Workspace ONE después de iniciar sesión.
- Se presenta un método incorrecto para la autenticación en la actualización.

Origen

Estos problemas pueden suceder si las directivas de acceso no se determinan correctamente. La dirección IP cliente determina qué directiva de acceso se aplica durante el inicio de sesión y durante el inicio de la aplicación. En un entorno de carga equilibrada, VMware Identity Manager usa el encabezado X-Forwarded-For para determinar la dirección IP cliente. En algunos casos se puede producir un error.

Solución

Establezca la propiedad `service.numberOfLoadBalancers` en el archivo `runtime-config.properties` de cada nodo del clúster de VMware Identity Manager. La propiedad especifica el número de equilibradores de carga frente a las instancias de VMware Identity Manager.

NOTA: La configuración de esta propiedad es opcional.

1 Inicie sesión en el dispositivo de VMware Identity Manager.

2 Edite el archivo `/usr/local/horizon/conf/runtime-config.properties` y añada la siguiente propiedad:

```
service.numberOfLoadBalancers numberOfLBs
```

donde *numberOfLBs* es el número de equilibradores de carga frente a las instancias de VMware Identity Manager.

3 Reinicie el dispositivo del área de trabajo.

```
service horizon-workspace restart
```

Un grupo no muestra ningún miembro después de la sincronización de directorios

La sincronización de directorios se completa correctamente, pero no aparece ningún usuario en los grupos sincronizados.

Problema

Después de sincronizar un directorio, de forma manual o automática según la programación de la sincronización, el proceso se completa correctamente pero no aparece ningún usuario en los grupos sincronizados.

Origen

Este problema sucede cuando tiene dos o más nodos en un clúster y existe una diferencia de hora de más de 5 segundos entre los nodos.

Solución

1 Compruebe que no hay ninguna diferencia de hora entre nodos. Use el mismo servidor NTP entre todos los nodos en el clúster para sincronizar la hora.

2 Reinicie el servicio en todos los nodos.

```
service horizon-workspace restart
```

3 (Opcional) En la consola de administración, elimine el grupo, vuelva a agregarlo en las opciones de sincronización y vuelva a sincronizar el directorio.

Solucionar problemas de Elasticsearch y RabbitMQ

Utilice esta información para solucionar problemas de Elasticsearch y RabbitMQ en un entorno de clúster. Elasticsearch, un motor de búsqueda y análisis usado para registros de sincronización de directorios, informes y auditorías, y RabbitMQ, un agente de mensajería, se encuentran incrustados en el dispositivo virtual VMware Identity Manager.

Solucionar problemas de Elasticsearch

Puede comprobar el estado de Elasticsearch utilizando el siguiente comando en el dispositivo VMware Identity Manager.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

El comando debe devolver un resultado similar al siguiente.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
```

```
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Si Elasticsearch no se inicia correctamente o su estado aparece en color rojo, siga estos pasos para solucionar los problemas.

1 Asegúrese de que el puerto 9300 está abierto.

   a Actualice la información de los nodos agregando las direcciones IP de todos los nodos del clúster en el archivo `/usr/local/horizon/scripts/updateiptables.hzn`:

   ```
   ALL_IPS="node1IPadd node2IPadd node3IPadd"
   ```

   b Ejecute el siguiente script en todos los nodos del clúster.

   ```
   /usr/local/horizon/scripts/updateiptables.hzn
   ```

2 Reinicie Elasticsearch en todos los nodos del clúster.

   ```
   service elasticsearch restart
   ```

3 Revise los registros para obtener más detalles.

   ```
   cd /opt/vmware/elasticsearch/logs
   ```

   ```
   tail –f horizon.log
   ```

Solucionar problemas de RabbitMQ

Puede comprobar el estado de RabbitMQ utilizando el siguiente comando en el dispositivo VMware Identity Manager.

```
rabbitmqctl cluster_status
```

El comando debe devolver un resultado similar al siguiente.

```
Cluster status of node 'rabbitmq@node3' ...
[{nodes,[{disc,['rabbitmq@node2','rabbitmq@node3']}]},
 {running_nodes,['rabbitmq@node3']},
 {cluster_name,<<"rabbitmq@node2.example.com">>},
 {partitions,[]},
 {alarms,[{'rabbitmq@node3',[]}]}]
```

Si RabbitMQ no se inicia o la URL de estado https://hostname/SAAS/API/1.0/REST/system/health/ muestra `"MessagingConnectionOk":"false"`, siga estos pasos para solucionar los problemas.

1 Asegúrese de que los puertos 4369, 5700 y 25672 están abiertos. Para abrir puertos:

   a Cree el archivo con este comando:

   ```
   touch /usr/local/horizon/conf/flags/enable.rabbitmq
   ```

   b Ejecute el siguiente script:

   ```
   /usr/local/horizon/scripts/updateiptables.hzn
   ```

2 Reinicie RabbitMQ.

   a Cierre todos los procesos de `rabbitmq` abiertos.

   b `rabbitmqctl stop`

c `rabbitmq-server -detached`

3 Es posible que necesite reiniciar el servicio de VMware Identity Manager si RabbitMQ no se inicia correctamente.

```
service horizon-workspace restart
```

Índice