Red Hat Enterprise Linux 8

Planificación de la gestión de la identidad

Documentación para la planificación de la gestión de identidades y el establecimiento del control de acceso

Last Updated: 2021-03-07

Red Hat Enterprise Linux 8 Planificación de la gestión de la identidad

Documentación para la planificación de la gestión de identidades y el establecimiento del control de acceso

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

Legal Notice

Resumen

Este documento describe la planificación de los servicios de Gestión de Identidades en Red Hat Enterprise Linux 8. La versión actual del documento sólo contiene historias de usuarios seleccionadas de la vista previa.

Table of Contents

HACER QUE EL CÓDIGO ABIERTO SEA MÁS INCLUSIVO 4

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT 5

CAPÍTULO 1. VISIÓN GENERAL DE LA PLANIFICACIÓN DE IDM Y CONTROL DE ACCESO EN RHEL 6
1.1. INTRODUCCIÓN A LA IDM 6
1.2. INTRODUCCIÓN A LOS SERVIDORES Y CLIENTES DE IDM 8
1.3. IDM Y CONTROL DE ACCESO EN RHEL: CENTRAL VS. LOCAL 10
1.4. TERMINOLOGÍA DE LA IDM 10
1.5. RECURSOS ADICIONALES 17

CAPÍTULO 2. PLANIFICACIÓN DE LA TOPOLOGÍA DE RÉPLICA 18
2.1. MÚLTIPLES SERVIDORES DE RÉPLICA COMO SOLUCIÓN DE ALTO RENDIMIENTO Y RECUPERACIÓN DE DESASTRES 18
2.2. INTRODUCCIÓN A LOS SERVIDORES Y CLIENTES DE IDM 18
2.3. ACUERDOS DE RÉPLICA 19
2.4. DETERMINAR EL NÚMERO ADECUADO DE RÉPLICAS 20
2.5. CONEXIÓN DE LAS RÉPLICAS EN UNA TOPOLOGÍA 20
2.6. EJEMPLOS DE TOPOLOGÍA DE RÉPLICA 21
2.7. EL MODO DE RÉPLICA OCULTA 23

CAPÍTULO 3. PLANIFICACIÓN DE LOS SERVICIOS DNS Y DE LOS NOMBRES DE HOST 24
3.1. SERVICIOS DNS DISPONIBLES EN UN SERVIDOR IDM 24
3.2. DIRECTRICES PARA PLANIFICAR EL NOMBRE DE DOMINIO DNS Y EL NOMBRE DE DOMINIO KERBEROS 24
Notas adicionales sobre la planificación del nombre de dominio DNS y del nombre de dominio Kerberos 25

CAPÍTULO 4. PLANIFICACIÓN DE LOS SERVICIOS DE AC 27
4.1. SERVICIOS DE CA DISPONIBLES EN UN SERVIDOR IDM 27
4.2. CA TEMA DN 28
4.3. DIRECTRICES PARA LA DISTRIBUCIÓN DE LOS SERVICIOS DE AC 28

CAPÍTULO 5. PLANIFICACIÓN DE LA INTEGRACIÓN CON AD 30
5.1. INTEGRACIÓN DIRECTA 30
Recomendaciones 30
5.2. INTEGRACIÓN INDIRECTA 31
5.3. DECIDIR ENTRE LA INTEGRACIÓN INDIRECTA Y LA DIRECTA 32
Número de sistemas que deben conectarse a Active Directory 32
Frecuencia de despliegue de nuevos sistemas y su tipo 32
Active Directory es el proveedor de autenticación requerido 32

CAPÍTULO 6. PLANIFICACIÓN DE UNA CONFIANZA CRUZADA ENTRE IDM Y AD 33
6.1. CONFIANZA CRUZADA ENTRE IDM Y AD 33
Una confianza externa a un dominio AD 33
6.2. CONTROLADORES DE CONFIANZA Y AGENTES DE CONFIANZA 33
6.3. FIDEICOMISOS UNIDIRECCIONALES Y BIDIRECCIONALES 34
6.4. GRUPOS EXTERNOS NO POSIX Y ASIGNACIÓN DE SID 35
6.5. CONFIGURAR EL DNS 35
6.6. NOMBRES NETBIOS 36
6.7. VERSIONES SOPORTADAS DE WINDOWS SERVER 36
6.8. CONFIGURACIÓN DE LA DETECCIÓN Y AFINIDAD DEL SERVIDOR AD 36
Opciones para configurar LDAP y Kerberos en el cliente IdM para la comunicación con los servidores IdM locales 37
Opciones para configurar Kerberos en el cliente IdM para la comunicación con los servidores locales de AD 37

Opciones para configurar los clientes integrados en los servidores IdM para la comunicación con los servidores AD locales a través de Kerberos y LDAP 38
6.9. OPERACIONES REALIZADAS DURANTE LA INTEGRACIÓN INDIRECTA DE IDM A AD 38

CAPÍTULO 7. COPIA DE SEGURIDAD Y RESTAURACIÓN DE IDM 59
7.1. TIPOS DE COPIAS DE SEGURIDAD DE IDM 59
7.2. CONVENCIONES DE NOMENCLATURA PARA LOS ARCHIVOS DE COPIA DE SEGURIDAD DE IDM 59
7.3. CONSIDERACIONES AL CREAR UNA COPIA DE SEGURIDAD 60
7.4. CREACIÓN DE UNA COPIA DE SEGURIDAD DE IDM 61
7.5. CREACIÓN DE COPIAS DE SEGURIDAD CIFRADAS DE IDM 62
7.5.1. Creación de una clave GPG2 para cifrar las copias de seguridad de IdM 62
7.5.2. Creación de una copia de seguridad de IdM cifrada con GPG2 63
7.6. CUÁNDO RESTAURAR DESDE UNA COPIA DE SEGURIDAD DE IDM 64
7.7. CONSIDERACIONES AL RESTAURAR DESDE UNA COPIA DE SEGURIDAD DE IDM 65
7.8. RESTAURACIÓN DE UN SERVIDOR IDM A PARTIR DE UNA COPIA DE SEGURIDAD 65
7.9. RESTAURACIÓN A PARTIR DE UNA COPIA DE SEGURIDAD ENCRIPTADA 69

HACER QUE EL CÓDIGO ABIERTO SEA MÁS INCLUSIVO

Red Hat se compromete a sustituir el lenguaje problemático en nuestro código, documentación y propiedades web. Estamos empezando con estos cuatro términos: maestro, esclavo, lista negra y lista blanca. Debido a la enormidad de este esfuerzo, estos cambios se implementarán gradualmente a lo largo de varias versiones próximas. Para más detalles, consulte el mensaje de nuestro CTO Chris Wright .

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT

Agradecemos su opinión sobre nuestra documentación. Por favor, díganos cómo podemos mejorarla. Para ello:

- Para comentarios sencillos sobre pasajes concretos:
  1. Asegúrese de que está viendo la documentación en el formato *Multi-page HTML*. Además, asegúrese de ver el botón **Feedback** en la esquina superior derecha del documento.
  2. Utilice el cursor del ratón para resaltar la parte del texto que desea comentar.
  3. Haga clic en la ventana emergente **Add Feedback** que aparece debajo del texto resaltado.
  4. Siga las instrucciones mostradas.
- Para enviar comentarios más complejos, cree un ticket de Bugzilla:
  1. Vaya al sitio web de Bugzilla.
  2. Como componente, utilice **Documentation**.
  3. Rellene el campo **Description** con su sugerencia de mejora. Incluya un enlace a la(s) parte(s) pertinente(s) de la documentación.
  4. Haga clic en **Submit Bug**.

CAPÍTULO 1. VISIÓN GENERAL DE LA PLANIFICACIÓN DE IDM Y CONTROL DE ACCESO EN RHEL

Las secciones siguientes proporcionan una visión general de las opciones para la gestión de identidades (IdM) y el control de acceso en Red Hat Enterprise Linux. Después de leer estas secciones, podrá abordar la etapa de planificación de su entorno.

1.1. INTRODUCCIÓN A LA IDM

Este módulo explica el propósito de la Gestión de identidades (IdM) en Red Hat Enterprise Linux. También proporciona información básica sobre el dominio IdM, incluyendo las máquinas cliente y servidoras que forman parte del dominio.

El objetivo de IdM en Red Hat Enterprise Linux

IdM en Red Hat Enterprise Linux proporciona una forma centralizada y unificada de gestionar almacenes de identidad, autenticación, políticas y políticas de autorización en un dominio basado en Linux. IdM reduce significativamente la sobrecarga administrativa de la gestión de diferentes servicios de forma individual y el uso de diferentes herramientas en diferentes máquinas.

IdM es una de las pocas soluciones de software de identidad, política y autorización centralizadas que admiten:

- Características avanzadas de los entornos del sistema operativo Linux
- Unificación de grandes grupos de máquinas Linux
- Integración nativa con Active Directory

IdM crea un dominio basado y controlado por Linux:

- IdM se basa en herramientas y protocolos nativos de Linux ya existentes. Tiene sus propios procesos y configuración, pero sus tecnologías subyacentes están bien establecidas en los sistemas Linux y son de confianza para los administradores de Linux.
- Los servidores y clientes de IdM son máquinas Red Hat Enterprise Linux. Los clientes de IdM también pueden ser otras distribuciones de Linux y UNIX si soportan los protocolos estándar. Los clientes Windows no pueden ser miembros del dominio IdM, pero los usuarios que inician sesión en sistemas Windows gestionados por Active Directory (AD) pueden conectarse a clientes Linux o acceder a servicios gestionados por IdM. Esto se consigue estableciendo una confianza cruzada entre los dominios AD e IdM.

Gestión de identidades y políticas en múltiples servidores Linux

Without IdM: Cada servidor se administra por separado. Todas las contraseñas se guardan en las máquinas locales. El administrador de TI gestiona los usuarios en cada máquina, establece las políticas de autenticación y autorización por separado y mantiene las contraseñas locales. Sin embargo, lo más frecuente es que los usuarios confíen en otra solución centralizada, por ejemplo la integración directa con AD. Los sistemas pueden integrarse directamente con AD utilizando varias soluciones diferentes:

- Herramientas heredadas de Linux (no se recomienda su uso)
- Solución basada en Samba winbind (recomendada para casos de uso específicos)
- Solución basada en un software de terceros (suele requerir una licencia de otro proveedor)

- Solución basada en SSSD (nativo de Linux y recomendado para la mayoría de los casos de uso)

With IdM: El administrador de TI puede:

- Mantener las identidades en un lugar central: el servidor IdM
- Aplicar políticas de manera uniforme a múltiples máquinas al mismo tiempo
- Establezca diferentes niveles de acceso para los usuarios utilizando el control de acceso basado en el host, la delegación y otras reglas
- Gestionar de forma centralizada las reglas de escalada de privilegios
- Definir cómo se montan los directorios personales

SSO para empresas

En el caso de IdM Enterprise, el inicio de sesión único (SSO) se implementa aprovechando el protocolo Kerberos. Este protocolo es popular en el nivel de infraestructura y permite el SSO con servicios como SSH, LDAP, NFS, CUPS, o DNS. Los servicios web que utilizan diferentes pilas web (Apache, EAP, Django y otros) también pueden ser habilitados para utilizar Kerberos para el SSO. Sin embargo, la práctica demuestra que el uso de OpenID Connect o SAML basado en SSO es más conveniente para las aplicaciones web. Para unir las dos capas, se recomienda implementar una solución de proveedor de identidad (IdP) que sea capaz de convertir la autenticación Kerberos en un ticket de OpenID Connect o una aserción SAML. La tecnología SSO de Red Hat basada en el proyecto de código abierto Keycloak es un ejemplo de este tipo de IdP

Without IdM: Los usuarios se conectan al sistema y se les pide una contraseña cada vez que acceden a un servicio o aplicación. Estas contraseñas pueden ser diferentes, y los usuarios tienen que recordar qué credencial utilizar para cada aplicación.

With Idm: Después de que los usuarios se conecten al sistema, pueden acceder a múltiples servicios y aplicaciones sin que se les pidan repetidamente sus credenciales. Esto ayuda a:

- Mejorar la usabilidad
- Reducir el riesgo de que las contraseñas se escriban o se almacenen de forma insegura
- Aumentar la productividad de los usuarios

Gestión de un entorno mixto Linux y Windows

Without IdM: Los sistemas Windows se gestionan en un bosque AD, pero los equipos de desarrollo, producción y otros tienen muchos sistemas Linux. Los sistemas Linux están excluidos del entorno AD.

With IdM: El administrador de TI puede:

- Gestionar los sistemas Linux utilizando herramientas nativas de Linux
- Integrar los sistemas Linux en los entornos gestionados centralmente por Active Directory, conservando así un almacén de usuarios centralizado.
- Implante fácilmente nuevos sistemas Linux a escala o según sus necesidades.
- Reaccionar rápidamente a las necesidades de la empresa y tomar decisiones relacionadas con la gestión de la infraestructura de Linux sin depender de otros equipos evitando retrasos.

Contraste de IdM con un directorio LDAP estándar

Un directorio LDAP estándar, como Red Hat Directory Server, es un directorio de propósito general: puede ser personalizado para adaptarse a una amplia gama de casos de uso.

- Esquema: un esquema flexible que puede personalizarse para una amplia gama de entradas, como usuarios, máquinas, entidades de red, equipos físicos o edificios.
- Normalmente se utiliza como: un directorio back-end para almacenar datos para otras aplicaciones, como las aplicaciones empresariales que proporcionan servicios en Internet.

La IdM tiene un propósito específico: gestionar las identidades internas, dentro de la empresa, así como las políticas de autenticación y autorización que se relacionan con estas identidades.

- Esquema: un esquema específico que define un conjunto particular de entradas relevantes para su propósito, como las entradas para las identidades de usuarios o máquinas.
- Normalmente se utiliza como: el servidor de identidad y autenticación para gestionar las identidades dentro de los límites de una empresa o un proyecto.

La tecnología del servidor de directorio subyacente es la misma tanto para Red Hat Directory Server como para IdM. Sin embargo, IdM está optimizado para gestionar identidades dentro de la empresa. Esto limita su extensibilidad general, pero también aporta ciertas ventajas: una configuración más sencilla, una mejor automatización de la gestión de recursos y una mayor eficiencia en la gestión de las identidades empresariales.

Recursos adicionales

- Gestión de identidades o Red Hat Directory Server - ¿Cuál debería usar? en el blog de Red Hat Enterprise Linux.
- Artículo de la base de conocimientos sobre los protocolos estándar.
- Notas de la versión beta de Red Hat Enterprise Linux 8

1.2. INTRODUCCIÓN A LOS SERVIDORES Y CLIENTES DE IDM

El dominio de la gestión de identidades (IdM) incluye los siguientes tipos de sistemas:

Servidores IdM

Los servidores IdM son sistemas Red Hat Enterprise Linux que responden a las solicitudes de identidad, autenticación y autorización dentro de un dominio IdM. En la mayoría de las implementaciones, también se instala una autoridad de certificación (CA) integrada con el servidor IdM.
Los servidores IdM son los repositorios centrales de información sobre identidades y políticas. Los servidores IdM también pueden alojar cualquiera de los servicios opcionales utilizados por los miembros del dominio:

- Autoridad de certificación (CA)
- Autoridad de Recuperación de Llaves (KRA)
- DNS
- Controlador de confianza de Active Directory (AD)
- Agente de confianza de Active Directory (AD)

El primer servidor instalado para crear el dominio es el *IdM master* o *master server*. No hay que confundir el maestro IdM con el servidor *master CA*: pueden funcionar en dos máquinas diferentes.

Clientes de IdM

Los clientes de IdM son sistemas Red Hat Enterprise Linux inscritos en los servidores y configurados para utilizar los servicios de IdM en estos servidores.
Los clientes interactúan con los servidores de IdM para acceder a los servicios que proporcionan. Por ejemplo, los clientes utilizan el protocolo Kerberos para realizar la autenticación y adquirir tickets para el inicio de sesión único (SSO) de la empresa, utilizan LDAP para obtener información sobre la identidad y las políticas, utilizan DNS para detectar dónde se encuentran los servidores y los servicios y cómo conectarse a ellos.

Los servidores de IdM también son clientes de IdM integrados. Como clientes inscritos en sí mismos, los servidores proporcionan la misma funcionalidad que otros clientes.

Para proporcionar servicios a un gran número de clientes, así como para la redundancia y la disponibilidad, IdM permite el despliegue en múltiples servidores de IdM en un solo dominio. Es posible desplegar hasta 60 servidores. Este es el número máximo de servidores IdM, también llamados réplicas, que se admite actualmente en el dominio IdM. Los servidores IdM proporcionan diferentes servicios al cliente. No es necesario que todos los servidores proporcionen todos los servicios posibles. Algunos componentes del servidor como Kerberos y LDAP están siempre disponibles en cada servidor. Otros servicios como CA, DNS, Trust Controller o Vault son opcionales. Esto significa que, en general, los distintos servidores desempeñan diferentes funciones en el despliegue.

Si su topología de IdM contiene una CA integrada, un servidor también tiene la función de maestro de generación de listas de revocación de certificados (CRL) y de maestro de renovación de CA . Este servidor es el *master CA*.

AVISO

El servidor *master CA* es fundamental para su implementación de IdM porque es el único sistema del dominio responsable del seguimiento de los certificados y las claves del subsistema de CA y de la generación de la CRL. Para obtener más información sobre cómo recuperarse de un desastre que afecte a la implementación de IdM, consulte Cómo realizar la recuperación de desastres con la gestión de identidades.

Para la redundancia y el equilibrio de carga, los administradores crean servidores adicionales mediante la creación de un *replica* de cualquier servidor existente, ya sea el servidor maestro u otra réplica. Al crear una réplica, IdM clona la configuración del servidor existente. Una réplica comparte con el servidor inicial su configuración principal, incluida la información interna sobre usuarios, sistemas, certificados y políticas configuradas.

NOTA

Una réplica y el servidor desde el que se creó son funcionalmente idénticos, excepto por el papel de maestro de generación de CRL. Por lo tanto, los términos *server* y *replica* se utilizan indistintamente aquí dependiendo del contexto.

1.3. IDM Y CONTROL DE ACCESO EN RHEL: CENTRAL VS. LOCAL

En Red Hat Enterprise Linux, puede gestionar las identidades y las políticas de control de acceso utilizando herramientas centralizadas para todo un dominio de sistemas, o utilizando herramientas locales para un solo sistema.

Gestión de identidades y políticas en múltiples servidores Red Hat Enterprise Linux: Con y sin IdM

Con Identity Management IdM, el administrador de TI puede:

- Mantener las identidades y los mecanismos de agrupación en un lugar central: el servidor de IdM
- Gestione de forma centralizada diferentes tipos de credenciales como contraseñas, certificados PKI, tokens OTP o claves SSH
- Aplicar políticas de manera uniforme a múltiples máquinas al mismo tiempo
- Gestionar los atributos POSIX y otros atributos para los usuarios externos de Active Directory
- Establezca diferentes niveles de acceso para los usuarios utilizando el control de acceso basado en el host, la delegación y otras reglas
- Gestionar de forma centralizada las reglas de escalada de privilegios (sudo) y el control de acceso obligatorio (asignación de usuarios de SELinux)
- Mantener la infraestructura PKI central y el almacén de secretos
- Definir cómo se montan los directorios personales

Sin IdM:

- Cada servidor se administra por separado.
- Todas las contraseñas se guardan en las máquinas locales.
- El administrador de TI gestiona los usuarios en cada máquina, establece las políticas de autenticación y autorización por separado y mantiene las contraseñas locales.

1.4. TERMINOLOGÍA DE LA IDM

Bosque de Active Directory

Un bosque de Active Directory (AD) es un conjunto de uno o más árboles de dominio que comparten un catálogo global, un esquema de directorio, una estructura lógica y una configuración de directorio comunes. El bosque representa el límite de seguridad dentro del cual los usuarios, equipos, grupos y otros objetos son accesibles. Para más información, consulte el documento de Microsoft sobre Bosques.

Catálogo global de Active Directory

El catálogo global es una característica de Active Directory (AD) que permite a un controlador de dominio proporcionar información sobre cualquier objeto del bosque, independientemente de si el objeto es miembro del dominio del controlador de dominio. Los controladores de dominio con la función de catálogo global activada se denominan servidores de catálogo global. El catálogo global proporciona un catálogo con capacidad de búsqueda de todos los objetos de cada dominio en un Servicio de Dominio de Active Directory (AD DS) multidominio.

Identificador de seguridad de Active Directory

Un identificador de seguridad (SID) es un número de identificación único asignado a un objeto en Active Directory, como un usuario, grupo o host. Es el equivalente funcional de los UIDs y GIDs en Linux.

Juego de Ansible

Los plays de Ansible son los bloques de construcción de los playbooks de Ansible . El objetivo de un play es asignar un grupo de hosts a algunos roles bien definidos, representados por tareas Ansible.

Libro de jugadas de Ansible

Un playbook de Ansible es un archivo que contiene uno o más plays de Ansible. Para más información, consulte la documentación oficial de Ansible sobre los playbooks .

Tarea Ansible

Las tareas Ansible son unidades de acción en Ansible. Una obra de Ansible puede contener varias tareas. El objetivo de cada tarea es ejecutar un módulo, con argumentos muy específicos. Una tarea Ansible es un conjunto de instrucciones para lograr un estado definido, en sus términos generales, por un rol o módulo Ansible específico, y afinado por las variables de ese rol o módulo. Para más información, consulte la documentación oficial de las tareas de Ansible.

Certificado

Un certificado es un documento electrónico que sirve para identificar a una persona, un servidor, una empresa u otra entidad y para asociar esa identidad a una clave pública. Al igual que una licencia de conducir o un pasaporte, un certificado proporciona una prueba generalmente reconocida de la identidad de una persona. La criptografía de clave pública utiliza los certificados para resolver el problema de la suplantación de identidad.

Autoridades de certificación (CA) en IdM

Una entidad que emite certificados digitales. En Red Hat Identity Management, la CA principal es **ipa**, la CA de IdM. El certificado de la CA **ipa** es uno de los siguientes tipos:

- Autofirmado. En este caso, la CA **ipa** es la CA raíz.
- Firmado externamente. En este caso, la CA de **ipa** está subordinada a la CA externa.

En IdM, también se pueden crear múltiples **sub-CAs**. Las sub-CAs son CAs de IdM cuyos certificados son de uno de los siguientes tipos:

- Firmado por el **ipa** CA.
- Firmado por cualquiera de las CA intermedias entre ella y **ipa** CA. El certificado de una sub-CA no puede ser autofirmado.

Confianza transfronteriza

Una confianza establece una relación de acceso entre dos dominios de Kerberos, permitiendo a los usuarios y servicios de un dominio acceder a los recursos de otro dominio.
Con una confianza cruzada entre el dominio raíz de un bosque de Active Directory (AD) y un dominio de IdM, los usuarios de los dominios del bosque de AD pueden interactuar con los equipos y servicios Linux del dominio de IdM. Desde la perspectiva de AD, la gestión de identidades representa un bosque AD independiente con un único dominio AD. Para obtener más información, consulte Cómo funciona la confianza.

Registros PTR del DNS

Los registros de puntero DNS (PTR) resuelven una dirección IP de un host a un nombre de dominio o de host. Los registros PTR son lo contrario de los registros DNS A y AAAA, que resuelven nombres de host a direcciones IP. Los registros PTR del DNS permiten realizar búsquedas inversas en el DNS. Los registros PTR se almacenan en el servidor DNS.

Registros DNS SRV

Un registro de servicio DNS (SRV) define el nombre de host, el número de puerto, el protocolo de transporte, la prioridad y el peso de un servicio disponible en un dominio. Puede utilizar los registros SRV para localizar servidores y réplicas de IdM.

Controlador de dominio (DC)

Un controlador de dominio (DC) es un host que responde a las solicitudes de autenticación de seguridad dentro de un dominio y controla el acceso a los recursos de ese dominio. Los servidores IdM funcionan como DCs para el dominio IdM. Un DC autentifica a los usuarios, almacena la información de las cuentas de los usuarios y aplica la política de seguridad de un dominio. Cuando un usuario se conecta a un dominio, el DC autentica y valida sus credenciales y permite o deniega el acceso.

Nombre de dominio completo

Un nombre de dominio completo (FQDN) es un nombre de dominio que especifica la ubicación exacta de un host dentro de la jerarquía del Sistema de Nombres de Dominio (DNS). Un dispositivo con el nombre de host **myhost** en el dominio principal **example.com** tiene el FQDN **myhost.example.com**. El FQDN distingue de forma exclusiva el dispositivo de cualquier otro host llamado **myhost** en otros dominios.
Si está instalando un cliente IdM en el host **machine1** utilizando la detección automática de DNS y sus registros DNS están correctamente configurados, el FQDN de **machine1** es todo lo que necesita. Para obtener más información, consulte Requisitos de nombre de host y DNS para IdM .

Réplica oculta

Una réplica oculta es una réplica de IdM que tiene todos los servicios en ejecución y disponibles, pero sus roles de servidor están deshabilitados, y los clientes no pueden descubrir la réplica porque no tiene registros SRV en DNS.
Las réplicas ocultas están diseñadas principalmente para servicios como copias de seguridad, importación y exportación masiva, o acciones que requieren el cierre de los servicios de IdM. Dado que ningún cliente utiliza una réplica oculta, los administradores pueden apagar temporalmente los servicios de este host sin afectar a ningún cliente. Para obtener más información, consulte El modo de réplica oculta.

Rangos de identificación

Un rango de ID es un rango de números de ID asignados a la topología de IdM o a una réplica específica. Puedes utilizar rangos de ID para especificar el rango válido de UIDs y GIDs para nuevos usuarios, hosts y grupos. Los rangos de ID se utilizan para evitar conflictos de números de ID. Hay dos tipos distintos de rangos de ID en IdM:

- *IdM ID range*
  Utilice este rango de ID para definir los UID y GID de los usuarios y grupos en toda la topología de IdM. Al instalar el primer maestro de IdM se crea el rango de ID de IdM. No se puede modificar el rango de ID de IdM después de crearlo. Sin embargo, se puede crear un rango de IdM ID adicional, por ejemplo, cuando el original está a punto de agotarse.

- *Distributed Numeric Assignment (DNA) ID range*
  Utilice este rango de ID para definir los UID y GID que utiliza una réplica al crear nuevos usuarios. Al agregar una nueva entrada de usuario o host a una réplica de IdM por primera vez, se asigna un rango de ID de ADN a dicha réplica. Un administrador puede modificar el rango de ID de ADN, pero la nueva definición debe ajustarse a un rango de ID de IdM existente.

  Tenga en cuenta que el rango de IdM y el rango de ADN coinciden, pero no están interconectados. Si cambia un rango, asegúrese de cambiar el otro para que coincida.

Para más información, consulte los rangos de ID.

Vistas de identificación

Las vistas de ID le permiten especificar nuevos valores para los atributos de usuario o grupo POSIX, y definir en qué host o hosts cliente se aplicarán los nuevos valores. Por ejemplo, puede utilizar las vistas de ID para:

- Definir diferentes valores de atributos para diferentes entornos.
- Reemplazar un valor de atributo generado previamente por un valor diferente.

En una configuración de confianza IdM-AD, el **Default Trust View** es una vista de ID aplicada a los usuarios y grupos de AD. Mediante **Default Trust View**, puede definir atributos POSIX personalizados para los usuarios y grupos de AD, anulando así los valores definidos en AD.

Para obtener más información, consulte Uso de una vista de ID para anular un valor de atributo de usuario en un cliente IdM.

Servidor IdM CA

Un servidor IdM en el que está instalado y en funcionamiento el servicio de autoridad de certificación (CA) IdM.
Nombres alternativos **CA server**

Implantación de IdM

Término que se refiere a la totalidad de su instalación de IdM. Puedes describir tu implementación de IdM respondiendo a las siguientes preguntas:

- ¿Su implantación de IdM es de prueba o de producción?
  - ¿Cuántos servidores IdM tiene?
- ¿Su implementación de IdM contiene una CA integrada?
  - Si lo hace, ¿la CA integrada está autofirmada o firmada externamente?
  - Si es así, ¿en qué servidores está disponible el rol de CA? ¿En qué servidores está disponible el rol KRA?
- ¿Su implementación de IdM contiene un DNS integrado?
  - Si es así, ¿en qué servidores está disponible la función DNS?
- ¿Está su implementación de IdM en un acuerdo de confianza con un bosque de AD?
  - Si es así, ¿en qué servidores está disponible el rol de controlador de confianza AD o de agente de confianza AD?

Maestro y réplicas de IdM

El primer servidor instalado mediante el comando **ipa-server-install**, utilizado para crear el dominio IdM, se conoce como **master server** o **IdM master**.
Los administradores pueden utilizar el comando **ipa-replica-install** para instalar **replicas** además del maestro. Por defecto, la instalación de una réplica crea un acuerdo de replicación con el servidor IdM desde el que se creó, lo que permite recibir y enviar actualizaciones al resto de IdM.

No hay ninguna diferencia funcional entre un maestro y una réplica. Ambos son servidores IdM totalmente funcionales.

Nombres alternativos: **master**, **master server**, **IdM master server**

Servidor CA maestro de IdM

Si su topología de IdM contiene una autoridad de certificación (CA) integrada, un servidor tiene la función de maestro de generación de listas de revocación de certificados (CRL) y de maestro de renovación de CA. Este servidor es el **master CA server**. En una implementación sin CA integrada, no hay un servidor de CA maestro.
Nombres alternativos **master CA**

IMPORTANTE

IdM master y **master CA server** son dos términos diferentes. Por ejemplo, en el siguiente escenario de despliegue, el primer servidor es el maestro de IdM y la réplica es el servidor maestro de CA:

1. Instala el primer servidor IdM en su entorno sin CA integrada.
2. Instalas una réplica.
3. Se instala una CA en la réplica.

En este escenario, el primer servidor es el maestro de IdM y la réplica es el servidor maestro de CA.

Topología IdM

Término que se refiere a la estructura de su solución IdM , especialmente a los acuerdos de replicación entre y dentro de los centros de datos y clusters individuales.

Indicadores de autenticación Kerberos

Los indicadores de autenticación se adjuntan a los tickets de Kerberos y representan el método de autenticación inicial utilizado para adquirir un ticket:

- **otp** para la autenticación de dos factores (contraseña de un solo uso)
- **radius** para la autentificación del Servicio de Autentificación Remota de Usuarios (RADIUS) (comúnmente para la autentificación 802.1x)
- **pkinit** para la criptografía de clave pública para la autenticación inicial en Kerberos (PKINIT), la tarjeta inteligente o la autenticación de certificados
- **hardened** para contraseñas reforzadas contra intentos de fuerza bruta

Para más información, consulte los indicadores de autenticación de Kerberos .

Keytab de Kerberos

Mientras que una contraseña es el método de autenticación por defecto para un usuario, los keytabs son el método de autenticación por defecto para hosts y servicios. Un keytab de Kerberos es un archivo que contiene una lista de directores de Kerberos y sus claves de encriptación asociadas, para que un servicio pueda recuperar su propia clave de Kerberos y verificar la identidad de un usuario. Por ejemplo, cada cliente IdM tiene un archivo **/etc/krb5.keytab** que almacena información sobre la entidad de seguridad **host**, que representa la máquina cliente en el ámbito de Kerberos.

Principal de Kerberos

Las entidades principales de Kerberos son únicas e identifican a cada usuario, servicio y host en un reino de Kerberos:

Entidad	Convención de nombres	Ejemplo
Usuarios	**identifier@REALM**	**admin@EXAMPLE.COM**
Servicios	**service/fully-qualified-hostname@REALM**	**http/master.example.com@EXAMPLE.COM**
Anfitriones	**host/fully-qualified-hostname@REALM**	**host/client.example.com@EXAMPLE.COM**

Protocolo Kerberos

Kerberos es un protocolo de autenticación de red que proporciona una autenticación fuerte para las aplicaciones de cliente y servidor mediante el uso de criptografía de clave secreta. IdM y Active Directory utilizan Kerberos para autenticar usuarios, hosts y servicios.

Reino de Kerberos

Un reino Kerberos abarca todos los directores administrados por un Centro de Distribución de Claves Kerberos (KDC). En una implementación de IdM, el ámbito de Kerberos incluye todos los usuarios, hosts y servicios de IdM.

Políticas de tickets de Kerberos

El Centro de Distribución de Claves de Kerberos (KDC) aplica el control de acceso a los tickets mediante políticas de conexión, y gestiona la duración de los tickets de Kerberos mediante políticas de ciclo de vida de los tickets. Por ejemplo, la duración global predeterminada de los tickets es de un día, y la edad máxima de renovación global predeterminada es de una semana. Para obtener más información, consulte Tipos de políticas de tickets IdM Kerberos .

Centro de distribución de llaves (KDC)

El Centro de Distribución de Claves de Kerberos (KDC) es un servicio que actúa como autoridad central de confianza que gestiona la información de las credenciales de Kerberos. El KDC emite tickets Kerberos y garantiza la autenticidad de los datos que se originan en las entidades de la red IdM.
Para más información, consulte La función del KDC de IdM .

Sub-CA ligero

En IdM, una sub-CA ligera es una autoridad de certificación (CA) cuyo certificado está firmado por una CA raíz de IdM o por una de las CA subordinadas a ella. Una sub-CA ligera emite certificados sólo para un propósito específico, por ejemplo para asegurar una conexión VPN o HTTP.
Para más información, consulte Restringir una aplicación para que confíe sólo en un subconjunto de certificados.

Política de contraseñas

Una política de contraseñas es un conjunto de condiciones que deben cumplir las contraseñas de un determinado grupo de usuarios de IdM. Las condiciones pueden incluir los siguientes parámetros:

- La longitud de la contraseña
- El número de clases de caracteres utilizados

- La duración máxima de una contraseña.

Para más información, consulte Qué es una política de contraseñas .

Atributos POSIX

Los atributos POSIX son atributos de usuario para mantener la compatibilidad entre sistemas operativos.
En un entorno de Gestión de Identidades de Red Hat, los atributos POSIX para los usuarios incluyen:

- **cn**, el nombre del usuario
- **uid**, el nombre de la cuenta (login)
- **uidNumber**, un número de usuario (UID)
- **gidNumber**, el número de grupo primario (GID)
- **homeDirectory**, el directorio principal del usuario

En un entorno de Gestión de Identidades de Red Hat, los atributos POSIX para los grupos incluyen:

- **cn**, el nombre del grupo
- **gidNumber**, el número de grupo (GID)

Estos atributos identifican a los usuarios y a los grupos como entidades separadas.

Acuerdo de réplica

Un acuerdo de replicación es un acuerdo entre dos servidores de IdM en el mismo despliegue de IdM. El acuerdo de replicación garantiza que los datos y la configuración se replican continuamente entre los dos servidores.
IdM utiliza dos tipos de acuerdos de replicación: los acuerdos *domain replication*, que replican la información de identidad, y los acuerdos *certificate replication*, que replican la información de los certificados.

Para más información, consulte:

- Acuerdos de réplica
- Determinar el número adecuado de réplicas
- Conexión de las réplicas en una topología
- Ejemplos de topología de réplica

Tarjeta inteligente

Una tarjeta inteligente es un dispositivo o tarjeta extraíble que se utiliza para controlar el acceso a un recurso. Pueden ser tarjetas de plástico del tamaño de una tarjeta de crédito con un chip de circuito integrado (IC) incrustado, pequeños dispositivos USB como un Yubikey, u otros dispositivos similares. Las tarjetas inteligentes pueden proporcionar autenticación permitiendo a los usuarios conectar una tarjeta inteligente a un ordenador central, y el software de ese ordenador central interactúa con el material clave almacenado en la tarjeta inteligente para autenticar al usuario.

SSSD

El demonio de servicios de seguridad del sistema (SSSD) es un servicio del sistema que gestiona la

autenticación y autorización de usuarios en un host RHEL. SSSD mantiene opcionalmente una caché de identidades y credenciales de usuario recuperadas de proveedores remotos para la autenticación sin conexión. Para obtener más información, consulte Comprender SSSD y sus ventajas.

Backend SSSD

Un backend de SSSD, también llamado proveedor de datos, es un proceso hijo de SSSD que gestiona y crea la caché de SSSD. Este proceso se comunica con un servidor LDAP, realiza diferentes consultas de búsqueda y almacena los resultados en la caché. También realiza la autenticación en línea contra LDAP o Kerberos y aplica la política de acceso y contraseña al usuario que se está registrando.

Billete de transporte (TGT)

Tras autenticarse en un Centro de Distribución de Claves (KDC) de Kerberos, un usuario recibe un ticket de concesión (TGT), que es un conjunto temporal de credenciales que puede utilizarse para solicitar tickets de acceso a otros servicios, como sitios web y correo electrónico.
El uso de un TGT para solicitar más acceso proporciona al usuario una experiencia de inicio de sesión único, ya que el usuario sólo necesita autenticarse una vez para acceder a varios servicios. Los TGT son renovables, y las políticas de tickets de Kerberos determinan los límites de renovación de tickets y el control de acceso.

Para obtener más información, consulte Administración de las políticas de tickets de Kerberos .

Glosas adicionales

Si no encuentra un término de gestión de identidades en este glosario, consulte los glosarios del servidor de directorio y del sistema de certificados:

- Glosario del Servidor de Directorio 11
- Glosario del Sistema de Certificación 9

1.5. RECURSOS ADICIONALES

- Para obtener información general sobre Red Hat IdM, consulte la página del producto Red Hat Identity Management en el Portal del Cliente de Red Hat.

CAPÍTULO 2. PLANIFICACIÓN DE LA TOPOLOGÍA DE RÉPLICA

Las siguientes secciones ofrecen consejos para determinar la topología de réplica adecuada para su caso de uso.

2.1. MÚLTIPLES SERVIDORES DE RÉPLICA COMO SOLUCIÓN DE ALTO RENDIMIENTO Y RECUPERACIÓN DE DESASTRES

La funcionalidad continua y la alta disponibilidad de los servicios de gestión de identidades (IdM) es vital para los usuarios que acceden a los recursos. Una de las soluciones integradas para lograr una funcionalidad continua y una alta disponibilidad de la infraestructura de IdM mediante el equilibrio de carga es la replicación del directorio central mediante la creación de servidores de réplica del servidor maestro.

IdM permite colocar servidores adicionales en centros de datos dispersos geográficamente para reflejar la estructura organizativa de su empresa. De esta manera, se acorta el camino entre los clientes de IdM y el servidor accesible más cercano. Además, tener varios servidores permite repartir la carga y escalar para más clientes.

Mantener varios servidores de IdM redundantes y dejar que se repliquen entre sí es también un mecanismo de copia de seguridad común para mitigar o prevenir la pérdida de servidores. Por ejemplo, si un servidor falla, los otros servidores siguen proporcionando servicios al dominio. También puede recuperar el servidor perdido creando una nueva réplica basada en uno de los servidores restantes.

2.2. INTRODUCCIÓN A LOS SERVIDORES Y CLIENTES DE IDM

El dominio de la gestión de identidades (IdM) incluye los siguientes tipos de sistemas:

Servidores IdM

Los servidores IdM son sistemas Red Hat Enterprise Linux que responden a las solicitudes de identidad, autenticación y autorización dentro de un dominio IdM. En la mayoría de las implementaciones, también se instala una autoridad de certificación (CA) integrada con el servidor IdM.
Los servidores IdM son los repositorios centrales de información sobre identidades y políticas. Los servidores IdM también pueden alojar cualquiera de los servicios opcionales utilizados por los miembros del dominio:

- Autoridad de certificación (CA)
- Autoridad de Recuperación de Llaves (KRA)
- DNS
- Controlador de confianza de Active Directory (AD)
- Agente de confianza de Active Directory (AD)

El primer servidor instalado para crear el dominio es el *IdM master* o *master server*. No hay que confundir el maestro IdM con el servidor *master CA*: pueden funcionar en dos máquinas diferentes.

Clientes de IdM

Los clientes de IdM son sistemas Red Hat Enterprise Linux inscritos en los servidores y configurados para utilizar los servicios de IdM en estos servidores.
Los clientes interactúan con los servidores de IdM para acceder a los servicios que proporcionan. Por ejemplo, los clientes utilizan el protocolo Kerberos para realizar la autenticación y adquirir tickets para el inicio de sesión único (SSO) de la empresa, utilizan LDAP para obtener información sobre la identidad y las políticas, utilizan DNS para detectar dónde se encuentran los servidores y los servicios y cómo conectarse a ellos.

Los servidores de IdM también son clientes de IdM integrados. Como clientes inscritos en sí mismos, los servidores proporcionan la misma funcionalidad que otros clientes.

Para proporcionar servicios a un gran número de clientes, así como para la redundancia y la disponibilidad, IdM permite el despliegue en múltiples servidores de IdM en un solo dominio. Es posible desplegar hasta 60 servidores. Este es el número máximo de servidores IdM, también llamados réplicas, que se admite actualmente en el dominio IdM. Los servidores IdM proporcionan diferentes servicios al cliente. No es necesario que todos los servidores proporcionen todos los servicios posibles. Algunos componentes del servidor como Kerberos y LDAP están siempre disponibles en cada servidor. Otros servicios como CA, DNS, Trust Controller o Vault son opcionales. Esto significa que, en general, los distintos servidores desempeñan diferentes funciones en el despliegue.

Si su topología de IdM contiene una CA integrada, un servidor también tiene la función de maestro de generación de listas de revocación de certificados (CRL) y de maestro de renovación de CA . Este servidor es el *master CA*.

AVISO

El servidor *master CA* es fundamental para su implementación de IdM porque es el único sistema del dominio responsable del seguimiento de los certificados y las claves del subsistema de CA y de la generación de la CRL. Para obtener más información sobre cómo recuperarse de un desastre que afecte a la implementación de IdM, consulte Cómo realizar la recuperación de desastres con la gestión de identidades.

Para la redundancia y el equilibrio de carga, los administradores crean servidores adicionales mediante la creación de un *replica* de cualquier servidor existente, ya sea el servidor maestro u otra réplica. Al crear una réplica, IdM clona la configuración del servidor existente. Una réplica comparte con el servidor inicial su configuración principal, incluida la información interna sobre usuarios, sistemas, certificados y políticas configuradas.

NOTA

Una réplica y el servidor desde el que se creó son funcionalmente idénticos, excepto por el papel de maestro de generación de CRL. Por lo tanto, los términos *server* y *replica* se utilizan indistintamente aquí dependiendo del contexto.

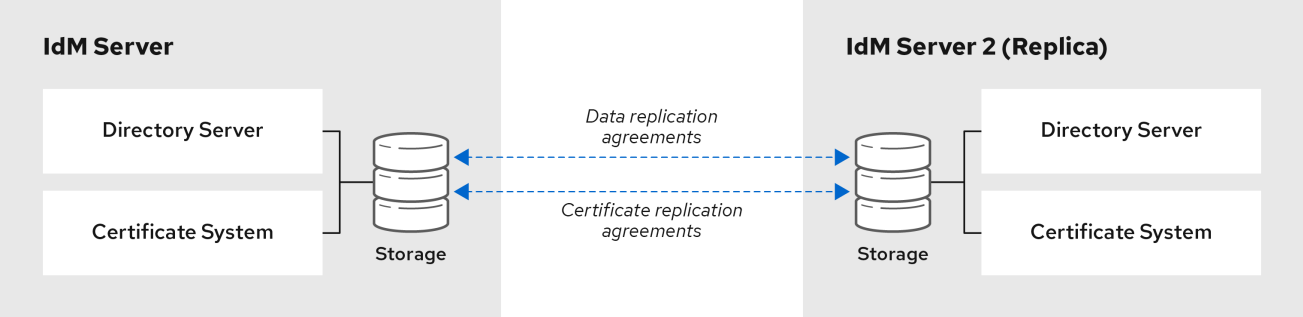
2.3. ACUERDOS DE RÉPLICA

Cuando un administrador crea una réplica basada en un servidor existente, Identity Management (IdM) crea un *replication agreement* entre el servidor inicial y la réplica. El acuerdo de réplica garantiza que los datos y la configuración se replican continuamente entre los dos servidores.

Los acuerdos de replicación son siempre bilaterales: los datos se replican de un servidor a otro, así como del otro servidor al primero.

IdM utiliza *multi-master replication*. En la replicación multimáster, todas las réplicas unidas en un acuerdo de replicación reciben actualizaciones y, por lo tanto, se consideran maestros de datos.

Figura 2.1. Acuerdos sobre servidores y réplicas



IdM utiliza dos tipos de acuerdos de replicación:

Acuerdos de replicación de dominios

Estos acuerdos replican la información sobre la identidad.

Acuerdos de réplica de certificados

Estos acuerdos replican la información del certificado.

Ambos canales de replicación son independientes. Dos servidores pueden tener uno o ambos tipos de acuerdos de replicación configurados entre ellos. Por ejemplo, cuando el servidor A y el servidor B sólo tienen configurado el acuerdo de replicación de dominio, sólo se replica la información de identidad entre ellos, no la información del certificado.

2.4. DETERMINAR EL NÚMERO ADECUADO DE RÉPLICAS

Establecer al menos dos réplicas en cada centro de datos (no es un requisito estricto)

Un centro de datos puede ser, por ejemplo, una oficina principal o una ubicación geográfica.

Establezca un número suficiente de servidores para atender a sus clientes

Un servidor de gestión de identidades (IdM) puede dar servicio a entre 2000 y 3000 clientes. Esto supone que los clientes consultan los servidores varias veces al día, pero no, por ejemplo, cada minuto. Si espera que las consultas sean más frecuentes, planifique más servidores.

Configurar un número suficiente de réplicas de Autoridades de Certificación (CA)

Sólo las réplicas con el rol de CA instalado pueden replicar los datos de los certificados. Si utiliza la CA de IdM, asegúrese de que su entorno tiene al menos dos réplicas de CA con acuerdos de replicación de certificados entre ellas.

Configurar un máximo de 60 réplicas en un único dominio IdM

Red Hat admite entornos con hasta 60 réplicas.

2.5. CONEXIÓN DE LAS RÉPLICAS EN UNA TOPOLOGÍA

Conectar cada réplica con al menos otras dos réplicas

La configuración de acuerdos de replicación adicionales garantiza que la información se replique no sólo entre la réplica inicial y el servidor maestro, sino también entre otras réplicas.

Conectar una réplica a un máximo de otras cuatro réplicas (no es un requisito estricto)

Un gran número de acuerdos de replicación por servidor no añade beneficios significativos. Una réplica receptora sólo puede ser actualizada por otra réplica a la vez y, mientras tanto, los otros acuerdos de replicación están inactivos. Más de cuatro acuerdos de replicación por réplica suele significar un desperdicio de recursos.

NOTA

Esta recomendación se aplica tanto a los acuerdos de replicación de certificados como a los de replicación de dominios.

Hay dos excepciones al límite de cuatro acuerdos de replicación por réplica:

- Usted quiere rutas de conmutación por error si ciertas réplicas no están en línea o no responden.
- En los despliegues más grandes, usted quiere enlaces directos adicionales entre nodos específicos.

La configuración de un número elevado de acuerdos de replicación puede tener un impacto negativo en el rendimiento general: cuando varios acuerdos de replicación en la topología están enviando actualizaciones, ciertas réplicas pueden experimentar una alta contención en el archivo de la base de datos de registro de cambios entre las actualizaciones entrantes y las salientes.

Si decide utilizar más acuerdos de replicación por réplica, asegúrese de no experimentar problemas de replicación y latencia. Sin embargo, tenga en cuenta que las grandes distancias y el elevado número de nodos intermedios también pueden causar problemas de latencia.

Conectar las réplicas de un centro de datos entre sí

Esto asegura la replicación del dominio dentro del centro de datos.

Conectar cada centro de datos con al menos otros dos centros de datos

Esto asegura la replicación del dominio entre los centros de datos.

Conectar los centros de datos utilizando al menos un par de acuerdos de replicación

Si los centros de datos A y B tienen un acuerdo de replicación de A1 a B1, tener un acuerdo de replicación de A2 a B2 garantiza que si uno de los servidores se cae, la replicación puede continuar entre los dos centros de datos.

2.6. EJEMPLOS DE TOPOLOGÍA DE RÉPLICA

Las figuras siguientes muestran ejemplos de topologías de gestión de identidades (IdM) basadas en las directrices para crear una topología fiable.

Figura 2.2, “Ejemplo de topología de réplica 1” muestra cuatro centros de datos, cada uno con cuatro servidores. Los servidores están conectados con acuerdos de replicación.

Figura 2.2. Ejemplo de topología de réplica 1

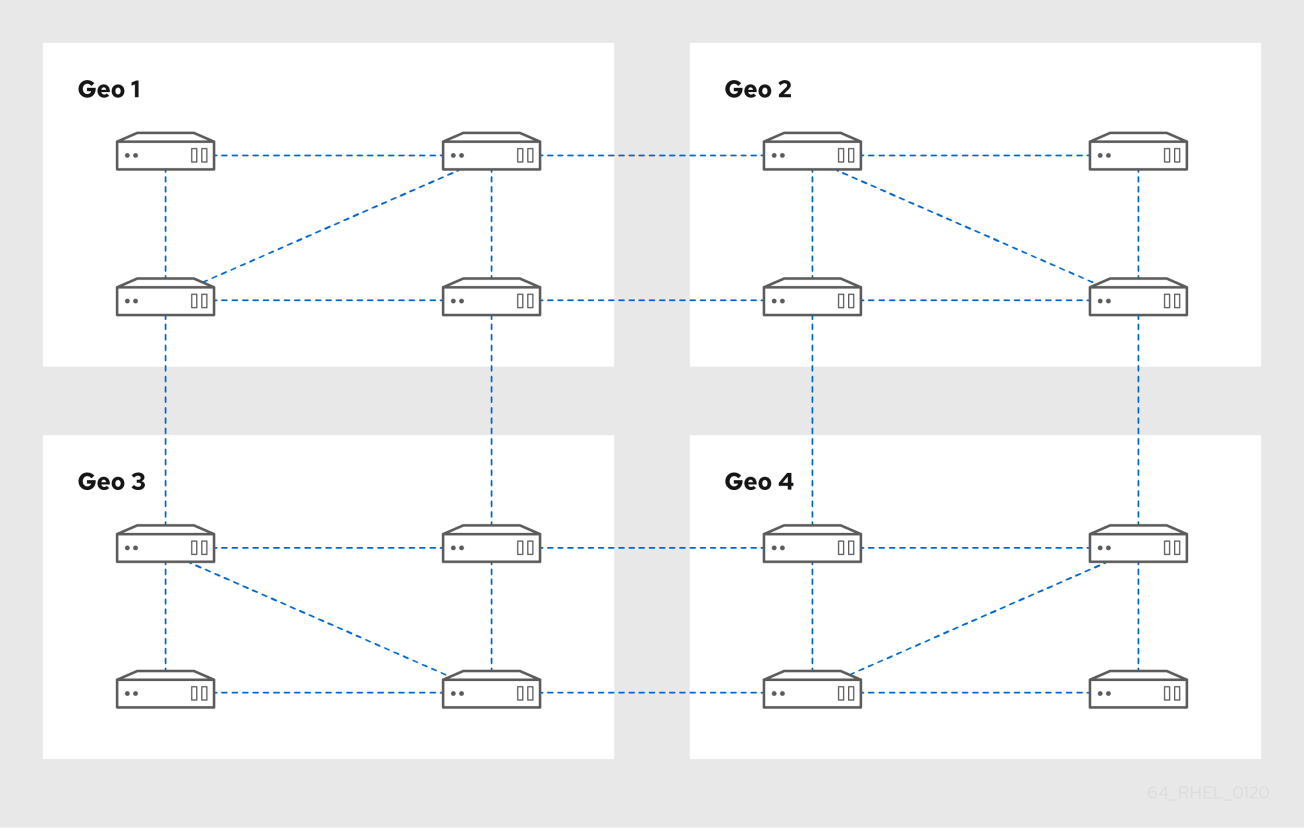
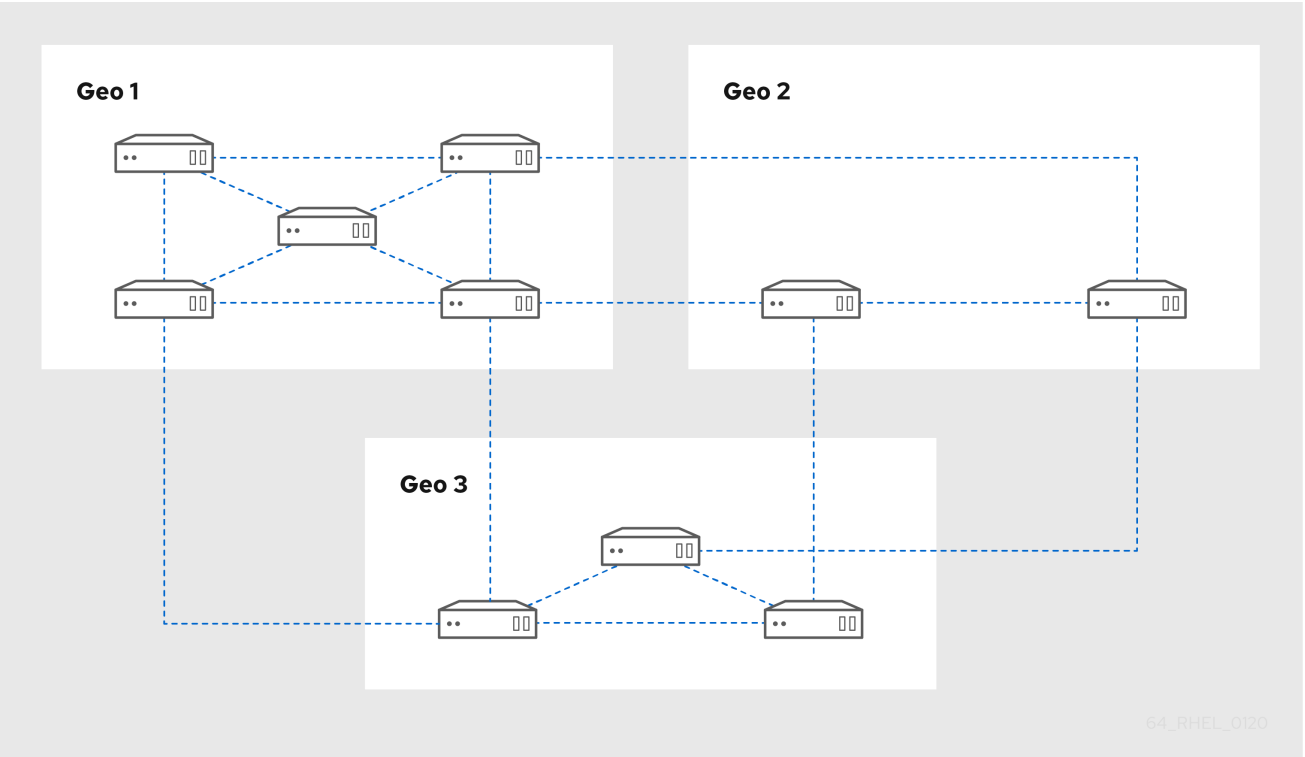


Figura 2.3, "Ejemplo de topología de réplica 2" muestra tres centros de datos, cada uno con un número diferente de servidores. Los servidores están conectados con acuerdos de replicación.

Figura 2.3. Ejemplo de topología de réplica 2



2.7. EL MODO DE RÉPLICA OCULTA

Por defecto, cuando se configura una nueva réplica, el instalador crea automáticamente registros de recursos de servicio (SRV) en DNS. Estos registros permiten a los clientes descubrir automáticamente la réplica y sus servicios. Una réplica oculta es un servidor IdM que tiene todos los servicios en funcionamiento y disponibles. Sin embargo, no tiene registros SRV en DNS y los roles del servidor LDAP no están habilitados. Por lo tanto, los clientes no pueden utilizar el descubrimiento de servicios para detectar estas réplicas ocultas.

NOTA

La función de réplica oculta está disponible en Red Hat Enterprise Linux 8.1 y posteriores como Technology Preview y, por lo tanto, no es compatible.

Las réplicas ocultas están diseñadas principalmente para servicios dedicados que, de otro modo, pueden interrumpir a los clientes. Por ejemplo, una copia de seguridad completa de IdM requiere apagar todos los servicios de IdM en el maestro o la réplica. Dado que ningún cliente utiliza una réplica oculta, los administradores pueden apagar temporalmente los servicios en este host sin afectar a ningún cliente.

NOTA

- La restauración de una copia de seguridad de una réplica oculta en un nuevo host siempre da como resultado una réplica no oculta (normal).
- Todos los roles de servidor utilizados en un clúster, especialmente el rol de Autoridad de Certificación si se utiliza la CA integrada, deben estar instalados en la réplica oculta para que la copia de seguridad pueda restaurar esos servicios.
- Para obtener más información sobre cómo crear y trabajar con las copias de seguridad de IdM, consulte Copia de seguridad y restauración de IdM .

Otros casos de uso son las operaciones de alta carga en la API de IdM o el servidor LDAP, como una importación masiva o consultas extensas. Para instalar una réplica como oculta, pase el parámetro **--hidden-replica** al comando **ipa-replica-install**.

Para obtener más detalles sobre la instalación de una réplica, consulte Instalación de una réplica de gestión de identidades.

Alternativamente, puede cambiar el estado de una réplica existente. Para obtener más detalles, consulte Degradación y promoción de réplicas ocultas .

CAPÍTULO 3. PLANIFICACIÓN DE LOS SERVICIOS DNS Y DE LOS NOMBRES DE HOST

La Gestión de Identidades (IdM) proporciona diferentes tipos de configuraciones de DNS en el servidor IdM. Las siguientes secciones las describen y proporcionan consejos sobre cómo determinar cuál es la mejor para su caso de uso.

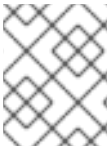
3.1. SERVICIOS DNS DISPONIBLES EN UN SERVIDOR IDM

Puede instalar un servidor de gestión de identidades (IdM) con o sin DNS integrado.

Tabla 3.1. Comparación de IdM con DNS integrado y sin DNS integrado

	Con DNS integrado	Sin DNS integrado
Resumen:	IdM ejecuta su propio servicio DNS para el dominio IdM.	IdM utiliza los servicios DNS proporcionados por un servidor DNS externo.
Limitaciones:	El servidor DNS integrado proporcionado por IdM sólo soporta las características relacionadas con la implementación y el mantenimiento de IdM. No soporta algunas de las características avanzadas de DNS. No está diseñado para ser utilizado como un servidor DNS de propósito general.	El DNS no está integrado con las herramientas nativas de IdM. Por ejemplo, IdM no actualiza los registros DNS automáticamente después de un cambio en la topología.
Funciona mejor para:	Uso básico dentro del despliegue de IdM. Cuando el servidor de IdM gestiona el DNS, éste se integra estrechamente con las herramientas nativas de IdM, lo que permite automatizar algunas de las tareas de gestión de registros DNS.	Entornos en los que se necesitan funciones de DNS avanzadas más allá del alcance del DNS de IdM. Entornos con una infraestructura DNS bien establecida en los que se desea seguir utilizando un servidor DNS externo.

Aunque se utilice un servidor de gestión de identidades como servidor DNS primario, se pueden seguir utilizando otros servidores DNS externos como servidores secundarios. Por ejemplo, si su entorno ya utiliza otro servidor DNS, como un servidor DNS integrado en Active Directory (AD), puede delegar sólo el dominio primario de IdM en el DNS integrado en IdM. No es necesario migrar las zonas DNS al DNS de IdM.



NOTA

Si necesita emitir certificados para clientes IdM con una dirección IP en la extensión del nombre alternativo del sujeto (SAN), debe utilizar el servicio DNS integrado de IdM.

3.2. DIRECTRICES PARA PLANIFICAR EL NOMBRE DE DOMINIO DNS Y EL NOMBRE DE DOMINIO KERBEROS

Al instalar el primer servidor de gestión de identidades (IdM), la instalación solicita un nombre DNS primario del dominio IdM y un nombre de dominio Kerberos. Las directrices de esta sección pueden ayudarle a establecer los nombres correctamente.

AVISO

No podrá cambiar el nombre del dominio primario de IdM ni el nombre del reino de Kerberos una vez que el servidor esté instalado. No espere poder pasar de un entorno de pruebas a un entorno de producción cambiando los nombres, por ejemplo de ***lab.example.com*** a ***production.example.com***.

Un dominio DNS separado para los registros de servicio

Asegúrese de que el *primary DNS domain* utilizado para el IdM no se comparte con ningún otro sistema. Esto ayuda a evitar conflictos a nivel de DNS.

Delegación adecuada de nombres de dominio DNS

Asegúrese de que tiene una delegación válida en el árbol DNS público para el dominio DNS. No utilice un nombre de dominio que no le haya sido delegado, ni siquiera en una red privada.

Dominio DNS multietiqueta

No utilice nombres de dominio de una sola etiqueta, por ejemplo **.company**. El dominio IdM debe estar compuesto por uno o varios subdominios y un dominio de nivel superior, por ejemplo **example.com** o **company.example.com**.

Un nombre de dominio único de Kerberos

Asegúrese de que el nombre del dominio no entra en conflicto con ningún otro nombre de dominio de Kerberos existente, como un nombre utilizado por Active Directory (AD).

El nombre del dominio Kerberos como una versión en mayúsculas del nombre DNS primario

Considere la posibilidad de establecer el nombre del dominio como una versión en mayúsculas (***EXAMPLE.COM***) del nombre de dominio DNS primario (***example.com***).

AVISO

Si no configura el nombre del dominio de Kerberos para que sea la versión en mayúsculas del nombre DNS primario, no podrá utilizar los fideicomisos de AD.

Notas adicionales sobre la planificación del nombre de dominio DNS y del nombre de dominio Kerberos

- Una implementación de IdM siempre representa un reino de Kerberos.
- Puedes unirte a clientes IdM desde varios dominios DNS distintos (***example.com***, ***example.net***, ***example.org***) a un único dominio Kerberos (***EXAMPLE.COM***).

- Los clientes de IdM no necesitan estar en el dominio DNS primario. Por ejemplo, si el dominio IdM es ***idm.example.com*** los clientes pueden estar en el dominio ***clients.example.com*** pero debe configurarse un mapeo claro entre el dominio DNS y el reino Kerberos.

NOTA

El método estándar para crear el mapeo es el uso de los registros DNS **_kerberos** TXT. El DNS integrado en IdM añade estos registros automáticamente.

CAPÍTULO 4. PLANIFICACIÓN DE LOS SERVICIOS DE AC

La Gestión de Identidades (IdM) en Red Hat Enterprise Linux proporciona diferentes tipos de configuraciones de autoridades de certificación (CA). Las siguientes secciones describen diferentes escenarios y proporcionan consejos para ayudarle a determinar qué configuración es la mejor para su caso de uso.

4.1. SERVICIOS DE CA DISPONIBLES EN UN SERVIDOR IDM

Puede instalar un servidor de gestión de identidades (IdM) con una autoridad de certificación (CA) de IdM integrada o sin una CA.

Tabla 4.1. Comparación de IdM con CA integrada y sin CA

	CA integrada	Sin una CA
Resumen:	IdM utiliza su propio servicio de infraestructura de clave pública (PKI) con un *CA signing certificate* para crear y firmar los certificados en el dominio IdM. ● Si la CA raíz es la CA integrada, IdM utiliza un certificado de CA autofirmado. ● Si la CA raíz es una CA externa, la CA de IdM integrada está subordinada a la CA externa. El certificado de CA utilizado por IdM está firmado por la CA externa, pero todos los certificados para el dominio de IdM son emitidos por la instancia del sistema de certificación integrado. ● La CA integrada también puede emitir certificados para usuarios, hosts o servicios. La CA externa puede ser una CA corporativa o una CA de terceros.	IdM no establece su propia CA, sino que utiliza certificados de host firmados por una CA externa. La instalación de un servidor sin una CA requiere que se soliciten los siguientes certificados a una autoridad de terceros: ● Un certificado de servidor LDAP ● Un certificado de servidor Apache ● Un certificado PKINIT ● Cadena completa de certificados de la CA que emitió los certificados de los servidores LDAP y Apache

	CA integrada	Sin una CA
Limitaciones:	Si la CA integrada está subordinada a una CA externa, los certificados emitidos dentro del dominio IdM están potencialmente sujetos a las restricciones establecidas por la CA externa para varios atributos del certificado, como por ejemplo • El periodo de validez. • Restricciones sobre los nombres de sujetos que pueden aparecer en los certificados emitidos por la CA de IDM o sus subordinadas.. • Restricciones en cuanto a si la CA de IDM puede emitir ella misma certificados de CA subordinados, o cuán "profunda" puede ser la cadena de certificados subordinados.	La gestión de los certificados fuera de IdM provoca un montón de actividades adicionales, como : • La creación, carga y renovación de certificados es un proceso manual. • El servicio **certmonger** no realiza un seguimiento de los certificados IPA (servidor LDAP, servidor Apache y certificados PKINIT) y no notifica cuando los certificados están a punto de caducar. Los administradores deben configurar manualmente las notificaciones para los certificados emitidos externamente, o establecer solicitudes de seguimiento para esos certificados si quieren que **certmonger** los rastree.
Funciona mejor para:	Entornos que le permiten crear y utilizar su propia infraestructura de certificados.	Casos muy raros en los que las restricciones de la infraestructura no permiten instalar servicios de certificados integrados en el servidor.

NOTA

Es posible cambiar de la CA autofirmada a una CA firmada externamente, o al revés, así como cambiar qué CA externa emite el certificado de la CA de IdM, incluso después de la instalación. También es posible configurar una CA integrada incluso después de una instalación sin CA.

4.2. CA TEMA DN

El nombre distinguido (DN) del sujeto de la Autoridad de Certificación (CA) es el nombre de la CA. Debe ser único a nivel mundial en la infraestructura de la CA de Gestión de Identidades (IdM) y no puede cambiarse después de la instalación. En caso de que necesite que la CA de IdM esté firmada externamente, es posible que tenga que consultar al administrador de la CA externa sobre la forma que debe adoptar el DN de asunto de su CA de IdM.

4.3. DIRECTRICES PARA LA DISTRIBUCIÓN DE LOS SERVICIOS DE AC

Los siguientes pasos proporcionan directrices para la distribución de sus servicios de autoridad de certificación (CA).

- Instalar los servicios de CA en más de un servidor en la topología

Las réplicas configuradas sin una CA reenvían todas las solicitudes de operaciones de certificados a los servidores de CA de su topología.

AVISO

Si pierde todos los servidores con una CA, perderá toda la configuración de la CA sin posibilidad de recuperación. En tal caso, deberá configurar una nueva CA y emitir e instalar nuevos certificados.

- Mantenga un número suficiente de servidores de CA para manejar las solicitudes de CA en su despliegue

Para la recomendación, véase la siguiente tabla:

Tabla 4.2. Directrices para establecer un número adecuado de servidores CA

Descripción del despliegue	Número sugerido de servidores CA
Un despliegue con un gran número de certificados emitidos	Tres o cuatro servidores CA
Un despliegue con problemas de ancho de banda o disponibilidad entre varias regiones	Un servidor CA por región, con un mínimo de tres servidores en total para la implantación
Todos los demás despliegues	Dos servidores CA

CAPÍTULO 5. PLANIFICACIÓN DE LA INTEGRACIÓN CON AD

Las siguientes secciones presentan las opciones para integrar Red Hat Enterprise Linux con Active Directory (AD).

- Para una visión general de la integración directa, véase Sección 5.1, “Integración directa” .
- Para una visión general de la integración indirecta, véase Sección 5.2, “Integración indirecta” .
- Para saber cómo decidir entre ellos, consulte Sección 5.3, “Decidir entre la integración indirecta y la directa”.

5.1. INTEGRACIÓN DIRECTA

En la integración directa, los sistemas Linux se conectan directamente a Active Directory (AD). Son posibles los siguientes tipos de integración:

Integración con el demonio de servicios de seguridad del sistema (SSSD)

SSSD puede conectar un sistema Linux con varios almacenes de identidad y autenticación: AD, Identity Management (IdM), o un servidor LDAP o Kerberos genérico.
Requisitos notables para la integración con el SSSD:

- Al integrarse con AD, SSSD sólo funciona por defecto dentro de un único bosque de AD. Para la configuración de varios bosques, configure la enumeración manual de dominios.
- Los bosques remotos de AD deben confiar en el bosque local para garantizar que el complemento **idmap_ad** gestione correctamente los usuarios del bosque remoto.

SSSD admite tanto la integración directa como la indirecta. Además, permite pasar de un enfoque de integración a otro sin costes de migración significativos.

Integración con Samba Winbind

El componente Winbind del paquete Samba emula un cliente Windows en un sistema Linux y se comunica con los servidores AD.
Requisitos notables para la integración con Samba Winbind:

- La integración directa con Winbind en una configuración AD multiforestal requiere confianzas bidireccionales.
- Debe existir una ruta bidireccional desde el dominio local de un sistema Linux hasta el dominio de un usuario en un bosque de AD remoto para permitir que la información completa sobre el usuario del dominio de AD remoto esté disponible para el complemento **idmap_ad**.

Recomendaciones

- SSSD satisface la mayoría de los casos de uso para la integración de AD y proporciona una solución sólida como pasarela genérica entre un sistema cliente y diferentes tipos de proveedores de identidad y autenticación: AD, IdM, Kerberos y LDAP.
- Se recomienda el uso de Winbind en aquellos servidores miembros del dominio AD en los que se planea desplegar Samba FS.

5.2. INTEGRACIÓN INDIRECTA

En la integración indirecta, los sistemas Linux se conectan primero a un servidor central que, a su vez, está conectado a Active Directory (AD). La integración indirecta permite al administrador gestionar los sistemas y las políticas de Linux de forma centralizada, mientras que los usuarios de AD pueden acceder de forma transparente a los sistemas y servicios de Linux.

Integración basada en la confianza entre bosques con AD

El servidor de gestión de identidades (IdM) actúa como servidor central para controlar los sistemas Linux. Se establece una confianza Kerberos cruzada con AD, lo que permite a los usuarios de AD iniciar sesión para acceder a los sistemas y recursos Linux. IdM se presenta ante AD como un bosque independiente y aprovecha las confianzas a nivel de bosque que admite AD.
Cuando se utiliza un fideicomiso:

- Los usuarios de AD pueden acceder a los recursos de IdM.
- Los servidores y clientes de IdM pueden resolver las identidades de los usuarios y grupos de AD.
- Los usuarios y grupos de AD acceden a IdM bajo las condiciones definidas por IdM, como el control de acceso basado en el host.
- Los usuarios y grupos de AD siguen siendo gestionados en el lado de AD.

Integración basada en la sincronización

Este enfoque se basa en la herramienta WinSync. Un acuerdo de replicación WinSync sincroniza las cuentas de usuario de AD a IdM.

AVISO

WinSync ya no se desarrolla activamente en Red Hat Enterprise Linux 8. La solución preferida para la integración indirecta es la confianza entre bosques.

Las limitaciones de la integración basada en la sincronización incluyen:

- Los grupos no se sincronizan de IdM a AD.
- Los usuarios están duplicados en AD e IdM.
- WinSync sólo admite un único dominio AD.
- Sólo se puede utilizar un controlador de dominio en AD para sincronizar los datos con una instancia de IdM.
- Las contraseñas de los usuarios deben estar sincronizadas, lo que requiere que el componente PassSync esté instalado en todos los controladores de dominio del dominio AD.
- Después de configurar la sincronización, todos los usuarios de AD deben cambiar manualmente las contraseñas antes de que PassSync pueda sincronizarlas.

5.3. DECIDIR ENTRE LA INTEGRACIÓN INDIRECTA Y LA DIRECTA

Las directrices de esta sección pueden ayudar a decidir qué tipo de integración se ajusta a su caso de uso.

Número de sistemas que deben conectarse a Active Directory

Conectar menos de 30-50 sistemas (no es un límite estricto)

Si conecta menos de 30-50 sistemas, considere la integración directa. La integración indirecta podría introducir una sobrecarga innecesaria.

Conectar más de 30-50 sistemas (no es un límite estricto)

Si conecta más de 30-50 sistemas, considere la integración indirecta con la gestión de identidades. Con este enfoque, puede beneficiarse de la gestión centralizada para los sistemas Linux.

Gestionar un pequeño número de sistemas Linux, pero esperar que el número crezca rápidamente

En este caso, considere la integración indirecta para evitar tener que migrar el entorno posteriormente.

Frecuencia de despliegue de nuevos sistemas y su tipo

Despliegue de sistemas bare metal de forma irregular

Si despliega nuevos sistemas con poca frecuencia y suelen ser sistemas bare metal, considere la integración directa. En estos casos, la integración directa suele ser la más sencilla y fácil.

Despliegue frecuente de sistemas virtuales

Si despliega nuevos sistemas con frecuencia y suelen ser sistemas virtuales aprovisionados bajo demanda, considere la integración indirecta. Con la integración indirecta, puede utilizar un servidor central para gestionar los nuevos sistemas de forma dinámica e integrarlos con herramientas de orquestación, como Red Hat Satellite.

Active Directory es el proveedor de autenticación requerido

¿Sus políticas internas establecen que todos los usuarios deben autenticarse en Active Directory?

Puede elegir la integración directa o indirecta. Si utiliza la integración indirecta con una confianza entre Gestión de identidades y Active Directory, los usuarios que acceden a los sistemas Linux se autentican en Active Directory. Las políticas que existen en Active Directory se ejecutan y aplican durante la autenticación.

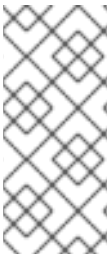
CAPÍTULO 6. PLANIFICACIÓN DE UNA CONFIANZA CRUZADA ENTRE IDM Y AD

Active Directory (AD) y Identity Management (IdM) son dos entornos alternativos que gestionan diversos servicios básicos, como Kerberos, LDAP, DNS y servicios de certificados. Una relación *cross-forest trust* integra de forma transparente estos dos entornos diversos permitiendo que todos los servicios básicos interactúen sin problemas. Las siguientes secciones ofrecen consejos sobre cómo planificar y diseñar una implementación de confianza entre bosques.

6.1. CONFIANZA CRUZADA ENTRE IDM Y AD

En un entorno puro de Active Directory (AD), una confianza entre bosques conecta dos dominios raíz de bosques de AD separados. Cuando se crea una confianza entre bosques entre AD e IdM, el dominio de IdM se presenta ante AD como un bosque separado con un único dominio. A continuación, se establece una relación de confianza entre el dominio raíz del bosque de AD y el dominio de IdM. Como resultado, los usuarios del bosque AD pueden acceder a los recursos del dominio IdM.

IdM puede establecer una confianza con un bosque de AD o con varios bosques no relacionados.



NOTA

Se pueden conectar dos reinos Kerberos separados en un *cross-realm trust*. Sin embargo, un reino Kerberos sólo se refiere a la autenticación, no a otros servicios y protocolos implicados en las operaciones de identidad y autorización. Por lo tanto, establecer una confianza Kerberos entre reinos no es suficiente para permitir a los usuarios de un reino acceder a los recursos de otro reino.

Una confianza externa a un dominio AD
Una confianza externa es una relación de confianza entre IdM y un dominio de Active Directory. Mientras que una confianza de bosque siempre requiere establecer una confianza entre IdM y el dominio raíz de un bosque de Active Directory, se puede establecer una confianza externa desde IdM a cualquier dominio dentro de un bosque.

6.2. CONTROLADORES DE CONFIANZA Y AGENTES DE CONFIANZA

La gestión de identidades (IdM) proporciona los siguientes tipos de servidores IdM que admiten la confianza en Active Directory (AD):

Agentes de confianza

Servidores de IdM que pueden realizar búsquedas de identidades contra los controladores de dominio de AD.

Controladores de confianza

Agentes de confianza que también ejecutan la suite Samba. Los controladores de dominio de AD se ponen en contacto con los agentes de confianza al establecer y verificar la confianza en AD.
El primer controlador de confianza se crea cuando se configura la confianza.

Los controladores de confianza ejecutan más servicios orientados a la red que los agentes de confianza y, por tanto, presentan una mayor superficie de ataque para los posibles intrusos.

Además de los agentes y controladores de confianza, el dominio de IdM también puede incluir servidores de IdM estándar. Sin embargo, estos servidores no se comunican con AD. Por lo tanto, los clientes que

se comunican con los servidores estándar no pueden resolver los usuarios y grupos de AD ni autenticar y autorizar a los usuarios de AD.

Tabla 6.1. Comparación de las capacidades soportadas por los controladores de confianza y los agentes de confianza

Capacidad	Agente fiduciario	Controlador de confianza
Resolver los usuarios y grupos de AD	Sí	Sí
Inscribir a los clientes de IdM que ejecutan servicios accesibles para los usuarios de los bosques de AD de confianza	Sí	Sí
Gestionar el fideicomiso (por ejemplo, añadir contratos de fideicomiso)	No	Sí

A la hora de planificar el despliegue de controladores y agentes de confianza, tenga en cuenta estas directrices:

- Configure al menos dos controladores de confianza por implementación de IdM.
- Configure al menos dos controladores de confianza en cada centro de datos.

Si alguna vez desea crear controladores de confianza adicionales o si falla un controlador de confianza existente, cree un nuevo controlador de confianza promoviendo un agente de confianza o un servidor estándar. Para ello, utilice la utilidad **ipa-adtrust-install** en el servidor de IdM.

IMPORTANTE

No se puede degradar un controlador de confianza existente a un agente de confianza.

6.3. FIDEICOMISOS UNIDIRECCIONALES Y BIDIRECCIONALES

En un sentido confía, Identity Management (IdM) confía en Active Directory (AD) pero AD no confía en IdM. Los usuarios de AD pueden acceder a los recursos del dominio de IdM, pero los usuarios de IdM no pueden acceder a los recursos del dominio de AD. El servidor de IdM se conecta a AD utilizando una cuenta especial, y lee la información de identidad que luego se entrega a los clientes de IdM a través de LDAP.

En los fideicomisos bidireccionales, los usuarios de IdM pueden autenticarse en AD, y los usuarios de AD pueden autenticarse en IdM. Los usuarios de AD pueden autenticarse y acceder a los recursos del dominio IdM como en el caso de la confianza unidireccional. Los usuarios de IdM pueden autenticarse pero no pueden acceder a la mayoría de los recursos de AD. Sólo pueden acceder a los servicios Kerberizados en los bosques de AD que no requieren ninguna comprobación de control de acceso.

Para poder conceder acceso a los recursos de AD, IdM necesita implementar el servicio de Catálogo Global. Este servicio aún no existe en la versión actual del servidor IdM. Por ello, una confianza bidireccional entre IdM y AD es casi funcionalmente equivalente a una confianza unidireccional entre IdM y AD.

6.4. GRUPOS EXTERNOS NO POSIX Y ASIGNACIÓN DE SID

La Gestión de Identidades (IdM) utiliza LDAP para gestionar los grupos. Las entradas de Active Directory (AD) no se sincronizan ni se copian en IdM, lo que significa que los usuarios y grupos de AD no tienen objetos LDAP en el servidor LDAP, por lo que no pueden utilizarse directamente para expresar la pertenencia a un grupo en el LDAP de IdM. Por esta razón, los administradores en IdM necesitan crear grupos externos no POSIX, referenciados como objetos LDAP normales de IdM para significar la pertenencia a un grupo para los usuarios y grupos de AD en IdM.

Los identificadores de seguridad (SID) de los grupos externos no POSIX son procesados por SSSD, que mapea los SID de los grupos en Active Directory a los grupos POSIX en IdM. En Active Directory, los SID están asociados a los nombres de usuario. Cuando se utiliza un nombre de usuario de AD para acceder a los recursos de IdM, SSSD utiliza el SID del usuario para construir una información completa de pertenencia a grupos para el usuario en el dominio de IdM.

6.5. CONFIGURAR EL DNS

Estas directrices pueden ayudarle a conseguir la configuración de DNS adecuada para establecer una confianza cruzada entre Identity Management (IdM) y Active Directory (AD).

Dominios DNS primarios únicos

Asegúrese de que tanto AD como IdM tienen configurados sus propios dominios DNS primarios. Por ejemplo:

- ***ad.example.com*** para AD y ***idm.example.com*** para IdM
- ***example.com*** para AD y ***idm.example.com*** para IdM

La solución de gestión más conveniente es un entorno en el que cada dominio DNS es gestionado por servidores DNS integrados, pero también se puede utilizar cualquier otro servidor DNS que cumpla con los estándares.

No hay solapamiento entre los dominios IdM y ADS DNS

Los sistemas unidos a IdM pueden estar distribuidos en varios dominios DNS. Asegúrese de que los dominios DNS que contienen clientes de IdM no se solapan con los dominios DNS que contienen sistemas unidos a AD.

Registros SRV adecuados

Asegúrese de que el dominio DNS primario de IdM tiene los registros SRV adecuados para admitir los fideicomisos de AD.
Para otros dominios DNS que formen parte del mismo reino IdM, no es necesario configurar los registros SRV cuando se establezca la confianza en AD. La razón es que los controladores de dominio de AD no utilizan los registros SRV para descubrir los centros de distribución de claves (KDC) de Kerberos, sino que basan el descubrimiento de los KDC en la información de enrutamiento del sufijo del nombre para la confianza.

Registros DNS resolubles desde todos los dominios DNS de la confianza

Asegúrese de que todos los equipos puedan resolver los registros DNS de todos los dominios DNS implicados en la relación de confianza:

- Al configurar el DNS de IdM, siga las instrucciones descritas en Instalación de un servidor de IdM con una CA externa.
- Si utiliza IdM sin DNS integrado, siga las instrucciones descritas en Instalación de un servidor IdM sin DNS integrado.

Nombres de dominio Kerberos como versiones en mayúsculas de los nombres de dominio DNS primarios

Asegúrese de que los nombres de dominio de Kerberos sean los mismos que los nombres de dominio DNS primario, con todas las letras en mayúscula. Por ejemplo, si los nombres de dominio son ***ad.example.com*** para AD y ***idm.example.com*** para IdM, los nombres de dominio de Kerberos deben ser ***AD.EXAMPLE.COM*** y ***IDM.EXAMPLE.COM***.

6.6. NOMBRES NETBIOS

El nombre NetBIOS suele ser el componente izquierdo del nombre de dominio. Por ejemplo:

- En el nombre de dominio ***linux.example.com***el nombre NetBIOS es **linux**.
- En el nombre de dominio ***example.com***el nombre NetBIOS es **example**.

Diferentes nombres NetBIOS para los dominios de Identity Management (IdM) y Active Directory (AD)

Asegúrese de que los dominios IdM y AD tienen nombres NetBIOS diferentes.
El nombre NetBIOS es fundamental para identificar el dominio AD. Si el dominio de IdM está dentro de un subdominio del DNS de AD, el nombre NetBIOS también es fundamental para identificar el dominio y los servicios de IdM.

Límite de caracteres para los nombres NetBIOS

La longitud máxima de un nombre NetBIOS es de 15 caracteres.

6.7. VERSIONES SOPORTADAS DE WINDOWS SERVER

Puede establecer una relación de confianza con los bosques de Active Directory (AD) que utilizan los siguientes niveles funcionales de bosque y dominio:

- Rango de nivel funcional del bosque: Windows Server 2008 - Windows Server 2016
- Rango de nivel funcional del dominio: Windows Server 2008 - Windows Server 2016

La gestión de identidades (IdM) es compatible con los siguientes sistemas operativos:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

6.8. CONFIGURACIÓN DE LA DETECCIÓN Y AFINIDAD DEL SERVIDOR AD

La configuración de descubrimiento y afinidad de servidores afecta a los servidores de Active Directory (AD) con los que se comunica un cliente de gestión de identidades (IdM). Esta sección proporciona una visión general de cómo funcionan el descubrimiento y la afinidad en un entorno con una confianza

cruzada entre IdM y AD.

Configurar los clientes para que prefieran servidores en la misma ubicación geográfica ayuda a evitar retrasos y otros problemas que se producen cuando los clientes contactan con servidores de otro centro de datos remoto. Para asegurarse de que los clientes se comunican con los servidores locales, debe asegurarse de que:

- Los clientes se comunican con los servidores locales de IdM a través de LDAP y de Kerberos
- Los clientes se comunican con los servidores locales de AD a través de Kerberos
- Los clientes integrados en los servidores IdM se comunican con los servidores AD locales a través de LDAP y de Kerberos

Opciones para configurar LDAP y Kerberos en el cliente IdM para la comunicación con los servidores IdM locales

Cuando se utiliza IdM con DNS integrado

Por defecto, los clientes utilizan la búsqueda automática de servicios basada en los registros DNS. En esta configuración, también puede utilizar la función *DNS locations* para configurar la búsqueda de servicios basada en DNS.
Para anular la búsqueda automática, puede desactivar el descubrimiento de DNS de una de las siguientes maneras:

- Durante la instalación del cliente IdM, proporcionando los parámetros de conmutación por error desde la línea de comandos
- Después de la instalación del cliente, modificando la configuración de System Security Services Daemon (SSSD)

Cuando se utiliza IdM sin DNS integrado

Debe configurar explícitamente los clientes de una de las siguientes maneras:

- Durante la instalación del cliente IdM, proporcionando los parámetros de conmutación por error desde la línea de comandos
- Después de la instalación del cliente modificando la configuración del SSSD

Opciones para configurar Kerberos en el cliente IdM para la comunicación con los servidores locales de AD

Los clientes de IdM no pueden descubrir automáticamente con qué servidores AD deben comunicarse. Para especificar los servidores AD manualmente, modifique el archivo **krb5.conf**:

- Añade la información del dominio de AD
- Enumerar explícitamente los servidores AD con los que hay que comunicarse

Por ejemplo:

```
[realms]
AD.EXAMPLE.COM = {
kdc = server1.ad.example.com
kdc = server2.ad.example.com
}
```

Opciones para configurar los clientes integrados en los servidores IdM para la comunicación con los servidores AD locales a través de Kerberos y LDAP

El cliente incrustado en un servidor IdM funciona también como cliente del servidor AD. Puede descubrir y utilizar automáticamente el sitio AD apropiado.

Cuando el cliente incrustado realiza la detección, podría descubrir primero un servidor AD en una ubicación remota. Si el intento de contactar con el servidor remoto tarda demasiado, el cliente podría detener la operación sin establecer la conexión. Utilice la opción **dns_resolver_timeout** en el archivo **sssd.conf** en el cliente para aumentar la cantidad de tiempo durante el cual el cliente espera una respuesta del resolver DNS. Consulte la página man *sssd.conf(5)* para más detalles.

Una vez que el cliente integrado ha sido configurado para comunicarse con los servidores AD locales, el SSSD recuerda el sitio AD al que pertenece el cliente integrado. Gracias a esto, SSSD normalmente envía un ping LDAP directamente a un controlador de dominio local para refrescar la información de su sitio. Si el sitio ya no existe o el cliente ha sido asignado mientras tanto a un sitio diferente, SSSD comienza a consultar los registros SRV en el bosque y pasa por todo un proceso de autodescubrimiento.

Utilizando *trusted domain sections* en **sssd.conf**, también puede anular explícitamente parte de la información que se descubre automáticamente por defecto.

6.9. OPERACIONES REALIZADAS DURANTE LA INTEGRACIÓN INDIRECTA DE IDM A AD

Tabla 6.2, “Operaciones realizadas desde un controlador de confianza IdM hacia los controladores de dominio AD” muestra qué operaciones y solicitudes se realizan durante la creación de una confianza de Identity Management (IdM) a Active Directory (AD) desde el controlador de confianza de IdM hacia los controladores de dominio de AD.

Tabla 6.2. Operaciones realizadas desde un controlador de confianza IdM hacia los controladores de dominio AD

Operación	Protocolo utilizado	Propósito
Resolución de DN	DNS	Para descubrir l

Operación	Protocolo utilizado	Propósito
Solvedor resde DNS de AD configurados en un controlad		Un es IP de los controlad ores de dominio AD

Operación	Protocolo utilizado	Propósito
Organización del dM		

Operación	Protocolo utilizado	Propósito
Solicitud de sal puerto UDP/UDP 63889 en un DC AD	LDAP sin conexión (CLDAP)	Para realizar el descubrimiento de ADDC

Operación	Protocolo utilizado	Propósito
Solicitudes al puerto TCP/TCP 6389 y 32768 en un DCd	LDAP	Para consultar la información de usuarios y grupos d

Operación	Protocolo utilizado	Propósito
Solicitud desde los puertos TCP/TCP 63889 y 32768 en un DC de AD	DCE RPC y SMB	Establecer la confianza entre bosques en AD

Operación	Protocolo utilizado	Propósito
Peticiones al puerto TCP/TCP 6135, 139, 445 en un D	DCE RPC y SMB	Establecer y apoyar la confianza entre bosques en AD

Operación	Protocolo utilizado	Propósito
Solicitudes a los puertos abiertos dinámicamente en un DC de	DCE RPC y SMB	Para responder a las solicitudes de DCE RPC End-point mappe

Operación	Protocolo utilizado	Propósito
Indicaciones del controlador de dominio de Active Dir		5 TCP/TCP 6)

Operación	Protocolo utilizado	Propósito
Obligatorio para implementar el rango de 49152-65535 (TCP/TCP6)		
So	Kerberos	Pa

Operación	Protocolo utilizado	Propósito
Los puertos 88 (TCP/TCP6 y UDP/UDP6), 464 (TCP/TCP6 y UD		Ticket de Kerberos; cambiar una contraseña de Kerber

Operación	Protocolo utilizado	Propósito
49 (TCP/TCP6) en un DC de AD		Tráfico Kerberos de formación remota

Tabla 6.3, “Operaciones realizadas desde un controlador de dominio AD hacia los controladores de confianza IdM” muestra qué operaciones y solicitudes se realizan durante la creación de una confianza IdM a AD desde el controlador de dominio AD hacia los controladores de confianza IdM.

Tabla 6.3. Operaciones realizadas desde un controlador de dominio AD hacia los controladores de confianza IdM

Operación	Protocolo utilizado	Propósito
	DNS	

Operación	Protocolo utilizado	Propósito
DNS contra los resolvedores DNS del dMconfigurados en		Para descubrir los controladores de confian

Operación	Protocolo utilizado	Propósito
Solicitud de dominio AD		
Solicitud de sal puerto UDP/UDP 63899 en	CLDAP	Para realizar el descubrimiento del

Operación	Protocolo utilizado	Propósito
unicación del servidor de confianza IdM		comunicación del servidor de confianza IdM
Solicitudes al puerto TCP/TC	DCE RPC y SMB	Para verificar la confianza ent

Operación	Protocolo utilizado	Propósito
Puerto 135, 389, 445 en un controlador de confianza IdM		AD
Solicitud de sapue	DCE RPC y SMB	Para responder a

Operación	Protocolo utilizado	Propósito
rtos abiertos dinámicamente en un controlador de confianza de IdM		las solicitudes de DCERPC End-point mapper (puerto 135 TCP/TCP6)

Operación	Protocolo utilizado	Propósito
Sincronización de las modificaciones del controlador de confianza del IdM, prueba		

Operación	Protocolo utilizado	Propósito
El rango de 49152-65535 (TCP/TCP6)		
Solicitudes salos	Kerberos	Para obtener un

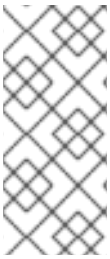
Operación	Protocolo utilizado	Propósito
TCP/TCP6 y UDP/UDP6), 464 (TCP/TCP6 y UDP/UDP6) y 749 (		ros; cambiar una contraseña de Kerberos; administr

Operación	Protocolo utilizado	Propósito
Controlador de configuración de IdM		Para configurar remotamente

CAPÍTULO 7. COPIA DE SEGURIDAD Y RESTAURACIÓN DE IDM

La Gestión de Identidades de Red Hat Enterprise Linux proporciona una solución para realizar manualmente una copia de seguridad y restaurar el sistema IdM. Esto puede ser necesario después de un evento de pérdida de datos.

Durante la copia de seguridad, el sistema crea un directorio que contiene información sobre su configuración de IdM y lo almacena. Durante la restauración, puede utilizar este directorio de copia de seguridad para recuperar su configuración original de IdM.



NOTA

Las funciones de copia de seguridad y restauración de IdM están diseñadas para ayudar a prevenir la pérdida de datos. Para mitigar el impacto de la pérdida de un servidor y garantizar la continuidad del funcionamiento proporcionando servidores alternativos a los clientes, asegúrese de tener una topología de réplica de acuerdo con Mitigar la pérdida de servidores con replicación.

7.1. TIPOS DE COPIAS DE SEGURIDAD DE IDM

Con la utilidad **ipa-backup**, puedes crear dos tipos de copias de seguridad:

Copia de seguridad de todo el servidor

- **Contains** todos los archivos de configuración del servidor relacionados con IdM, y los datos LDAP en archivos de formato de intercambio de datos LDAP (LDIF)
- Los servicios de IdM deben ser **offline**.
- **Suitable for** reconstruir un despliegue de IdM desde cero.

Copia de seguridad sólo de datos

- **Contains** datos LDAP en archivos LDIF y el registro de cambios de la replicación
- Los servicios de IdM pueden ser **online or offline**.
- **Suitable for** restaurar los datos de IdM a un estado en el pasado

7.2. CONVENCIONES DE NOMENCLATURA PARA LOS ARCHIVOS DE COPIA DE SEGURIDAD DE IDM

Por defecto, IdM almacena las copias de seguridad como archivos **.tar** en subdirectorios del directorio **/var/lib/ipa/backup/**.

Los archivos y subdirectorios siguen estas convenciones de nomenclatura:

Copia de seguridad de todo el servidor

Un archivo llamado **ipa-full.tar** en un directorio llamado **ipa-full-*<YEAR-MM-DD-HH-MM-SS>***con la hora especificada en la hora GMT.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-full-2021-01-29-12-11-46
```

```
total 3056
-rw-r--r--. 1 root root     158 Jan 29 12:11 header
-rw-r--r--. 1 root root 3121511 Jan 29 12:11 ipa-full.tar
```

Copia de seguridad sólo de datos

Un archivo llamado **ipa-data.tar** en un directorio llamado **ipa-data-*<YEAR-MM-DD-HH-MM-SS>***con la hora especificada en la hora GMT.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-data-2021-01-29-12-14-23
total 1072
-rw-r--r--. 1 root root     158 Jan 29 12:14 header
-rw-r--r--. 1 root root 1090388 Jan 29 12:14 ipa-data.tar
```

NOTA

La desinstalación de un servidor IdM no elimina automáticamente los archivos de copia de seguridad.

7.3. CONSIDERACIONES AL CREAR UNA COPIA DE SEGURIDAD

Esta sección describe comportamientos y limitaciones importantes del comando **ipa-backup**.

- Por defecto, la utilidad **ipa-backup** se ejecuta en modo offline, lo que detiene todos los servicios de IdM. La utilidad reinicia automáticamente los servicios de IdM una vez finalizada la copia de seguridad.

- Una copia de seguridad completa del servidor debe **always** ejecutarse con los servicios de IdM desconectados, pero una copia de seguridad de sólo datos puede realizarse con los servicios conectados.

- Por defecto, la utilidad **ipa-backup** crea copias de seguridad en el sistema de archivos que contiene el directorio **/var/lib/ipa/backup/**. Red Hat recomienda crear copias de seguridad regularmente en un sistema de archivos separado del sistema de archivos de producción utilizado por IdM, y archivar las copias de seguridad en un medio fijo, como una cinta o almacenamiento óptico.

- Considere la posibilidad de realizar copias de seguridad en las réplicas ocultas. Los servicios de IdM pueden cerrarse en las réplicas ocultas sin afectar a los clientes de IdM.

- A partir de RHEL 8.3.0, la utilidad **ipa-backup** comprueba si todos los servicios utilizados en el clúster de IdM, como la Autoridad de Certificación (CA), el Sistema de Nombres de Dominio (DNS) y el Agente de Recuperación de Claves (KRA), están instalados en el servidor donde se está ejecutando la copia de seguridad. Si el servidor no tiene todos estos servicios instalados, la utilidad **ipa-backup** sale con una advertencia, porque las copias de seguridad realizadas en ese host no serían suficientes para una restauración completa del clúster.
  Por ejemplo, si su implementación de IdM utiliza una Autoridad de Certificación (CA) integrada, una copia de seguridad ejecutada en una réplica no CA no capturará los datos de la CA. Red Hat recomienda verificar que la réplica en la que se realiza un **ipa-backup** tenga instalados todos los servicios IdM utilizados en el cluster.

  Se puede omitir la comprobación del rol del servidor IdM con el comando **ipa-backup --disable-role-check**, pero la copia de seguridad resultante no contendrá todos los datos necesarios para restaurar IdM por completo.

7.4. CREACIÓN DE UNA COPIA DE SEGURIDAD DE IDM

Esta sección describe cómo crear una copia de seguridad de todo el servidor y de sólo datos en los modos offline y online utilizando el comando **ipa-backup**.

Requisitos previos

- Debe tener privilegios en **root** para ejecutar la utilidad **ipa-backup**.

Procedimiento

- Para crear una copia de seguridad de todo el servidor en modo offline, utilice la utilidad **ipa-backup** sin opciones adicionales.

```
[root@server ~]# ipa-backup
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
The ipa-backup command was successful
```

- Para crear una copia de seguridad sólo de datos sin conexión, especifique la opción **--data**.

```
[root@server ~]# ipa-backup --data
```

- Para crear una copia de seguridad completa del servidor que incluya los archivos de registro de IdM, utilice la opción **--logs**.

```
[root@server ~]# ipa-backup --logs
```

- Para crear una copia de seguridad sólo de datos mientras los servicios de IdM se están ejecutando, especifique las opciones **--data** y **--online**.

```
[root@server ~]# ipa-backup --data --online
```

NOTA

Si la copia de seguridad falla por falta de espacio en el directorio **/tmp**, utilice la variable de entorno **TMPDIR** para cambiar el destino de los archivos temporales creados por el proceso de copia de seguridad:

```
[root@server ~]# TMPDIR=/new/location ipa-backup
```

Para más detalles, consulte El comando ipa-backup no finaliza .

Pasos de verificación

- El directorio de copia de seguridad contiene un archivo con la copia de seguridad.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
header  ipa-full.tar
```

7.5. CREACIÓN DE COPIAS DE SEGURIDAD CIFRADAS DE IDM

Puedes crear copias de seguridad encriptadas utilizando el cifrado GNU Privacy Guard (GPG). Para crear copias de seguridad encriptadas de IdM, primero tendrás que crear una clave GPG2.

7.5.1. Creación de una clave GPG2 para cifrar las copias de seguridad de IdM

El siguiente procedimiento describe cómo generar una clave GPG2 para la utilidad **ipa-backup**.

Procedimiento

1. Instale y configure la utilidad **pinentry**.

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. Cree un archivo **key-input** utilizado para generar un par de claves GPG con los detalles que prefiera. Por ejemplo:

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: IPA Backup
Name-Comment: IPA Backup
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. Por defecto, GPG2 almacena su llavero en el archivo **~/.gnupg**. Para utilizar una ubicación de llavero personalizada, establezca la variable de entorno **GNUPGHOME** en un directorio al que sólo pueda acceder el usuario root.

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. Comienza a generar una nueva clave GPG2 basada en el contenido de **key-input**.

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

   a. Introduzca una frase de contraseña para proteger la clave GPG2.

```
┌──────────────────────────────────────────────────────┐
┐
│ Please enter the passphrase to                       │
```

```
| protect your new key                          |
|                                               |
| Passphrase: SecretPassphrase42                |
|                                               |
|  <OK>                    <Cancel>             |
└──────────────────────────────────────────────┘
```

b. Confirme la frase de contraseña correcta introduciéndola de nuevo.

```
┌──────────────────────────────────────────────┐
| Please re-enter this passphrase               |
|                                               |
| Passphrase: SecretPassphrase42                |
|                                               |
|  <OK>                    <Cancel>             |
└──────────────────────────────────────────────┘
```

c. La nueva clave GPG2 ya está creada.

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

Pasos de verificación

- Enumerar las claves GPG en el servidor.

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] IPA Backup (IPA Backup) <root@example.com>
```

Recursos adicionales

- Para más información sobre el cifrado GPG y sus usos, consulte el sitio web de GNU Privacy Guard.

7.5.2. Creación de una copia de seguridad de IdM cifrada con GPG2

El siguiente procedimiento crea una copia de seguridad de IdM y la cifra utilizando una clave GPG2.

Requisitos previos

- Has creado una clave GPG2. Ver Crear una clave GPG2 para cifrar las copias de seguridad de IdM.

Procedimiento

- Crea una copia de seguridad cifrada con GPG especificando la opción **--gpg**.

```
[root@server ~]# ipa-backup --gpg
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Encrypting /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00/ipa-full.tar
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
The ipa-backup command was successful
```

Pasos de verificación

- Asegúrese de que el directorio de la copia de seguridad contiene un archivo cifrado con una extensión de archivo **.gpg**.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
header  ipa-full.tar.gpg
```

Recursos adicionales

- Para obtener información general sobre la creación de una copia de seguridad, consulte Crear una copia de seguridad.

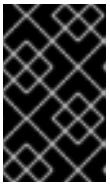
7.6. CUÁNDO RESTAURAR DESDE UNA COPIA DE SEGURIDAD DE IDM

Puede responder a varios escenarios de desastre restaurando desde una copia de seguridad de IdM:

- **Undesirable changes were made to the LDAP content** Las entradas fueron modificadas o eliminadas, la replicación llevó a cabo esos cambios a lo largo del despliegue, y usted desea revertir esos cambios. La restauración de una copia de seguridad de sólo datos devuelve las entradas LDAP al estado anterior sin afectar a la propia configuración de IdM.

- **Total Infrastructure Loss, or loss of all CA instances** Si un desastre daña todas las réplicas de la Autoridad de Certificación, el despliegue ha perdido la capacidad de reconstruirse desplegando servidores adicionales. En esta situación, restaure una copia de seguridad de una réplica de CA y construya nuevas réplicas a partir de ella.

- **An upgrade on an isolated server failed** El sistema operativo sigue funcionando, pero los datos de IdM están dañados, por lo que se desea restaurar el sistema IdM a un estado bueno conocido. Red Hat recomienda trabajar con el soporte técnico para diagnosticar y solucionar el problema. Si estos esfuerzos fallan, restaure desde una copia de seguridad completa del servidor.



IMPORTANTE

La solución preferida para los fallos de hardware o de actualización es reconstruir el servidor perdido a partir de una réplica. Para obtener más información, consulte Recuperación de la pérdida de un servidor con replicación .

7.7. CONSIDERACIONES AL RESTAURAR DESDE UNA COPIA DE SEGURIDAD DE IDM

Si tienes una copia de seguridad creada con la utilidad **ipa-backup**, puedes restaurar tu servidor IdM o el contenido LDAP al estado en que se encontraban cuando se realizó la copia de seguridad.

Las siguientes son las consideraciones clave al restaurar desde una copia de seguridad de IdM:

- Sólo se puede restaurar una copia de seguridad en un servidor que coincida con la configuración del servidor donde se creó originalmente la copia de seguridad. El servidor **must** tiene:
  - El mismo nombre de host
  - La misma dirección IP
  - La misma versión del software IdM
- Si se restaura un servidor IdM en un entorno multimaster, el servidor restaurado se convierte en la única fuente de información para IdM. Todos los demás servidores maestros **must** se reiniciarán desde el servidor restaurado.
- Dado que cualquier dato creado después de la última copia de seguridad se perderá, no utilice la solución de copia de seguridad y restauración para el mantenimiento normal del sistema.
- Si se pierde un servidor, Red Hat recomienda reconstruir el servidor reinstalándolo como una réplica, en lugar de restaurarlo desde una copia de seguridad. La creación de una nueva réplica conserva los datos del entorno de trabajo actual. Para más información, consulte Preparación para la pérdida de un servidor con replicación.
- Las funciones de copia de seguridad y restauración sólo se pueden gestionar desde la línea de comandos y no están disponibles en la interfaz web de IdM.
- No se puede restaurar a partir de archivos de copia de seguridad ubicados en los directorios **/tmp** o **/var/tmp**. El Servidor de directorios IdM utiliza un directorio **PrivateTmp** y no puede acceder a los directorios **/tmp** o **/var/tmp** comúnmente disponibles para el sistema operativo.

SUGERENCIA

La restauración desde una copia de seguridad requiere las mismas versiones de software (RPM) en el host de destino que estaban instaladas cuando se realizó la copia de seguridad. Debido a esto, Red Hat recomienda restaurar desde una instantánea de la máquina virtual en lugar de una copia de seguridad. Para más información, consulte Recuperación de la pérdida de datos con instantáneas de máquinas virtuales.

7.8. RESTAURACIÓN DE UN SERVIDOR IDM A PARTIR DE UNA COPIA DE SEGURIDAD

El siguiente procedimiento describe la restauración de un servidor IdM, o de sus datos LDAP, a partir de una copia de seguridad de IdM.

Figura 7.1. Topología de replicación utilizada en este ejemplo

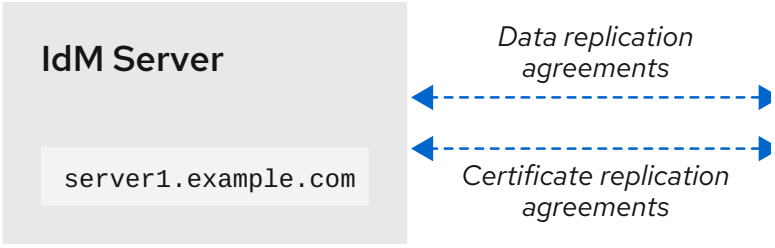


Tabla 7.1. Convenciones de nomenclatura de servidores utilizadas en este ejemplo

Nombre del servidor	Función
server1.example.com	El servidor que necesita ser restaurado desde la copia de seguridad.
caReplica2.example.com	Una réplica de la Autoridad de Certificación (CA) conectada al host **server1.example.com**.
replica3.example.com	Una réplica conectada al host **caReplica2.example.com**.

Requisitos previos

- Has generado una copia de seguridad del servidor IdM completa o de sólo datos con la utilidad **ipa-backup**. Consulte Creación de una copia de seguridad.
- Sus archivos de copia de seguridad no están en los directorios **/tmp** o **/var/tmp**.
- Antes de realizar una restauración de todo el servidor a partir de una copia de seguridad de todo el servidor, desinstala IdM del servidor y vuelve a instalar IdM utilizando la misma configuración del servidor que antes.

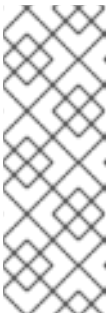
Procedimiento

1. Utiliza la utilidad **ipa-restore** para restaurar una copia de seguridad de todo el servidor o sólo de los datos.
   - Si el directorio de la copia de seguridad está en la ubicación predeterminada **/var/lib/ipa/backup/**, introduzca sólo el nombre del directorio:

     ```
     [root@server1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
     ```

   - Si el directorio de la copia de seguridad no está en la ubicación predeterminada, introduzca su ruta completa:

```
[root@server1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
```



NOTA

La utilidad **ipa-restore** detecta automáticamente el tipo de copia de seguridad que contiene el directorio y realiza el mismo tipo de restauración por defecto. Para realizar una restauración de sólo datos a partir de una copia de seguridad completa del servidor, añada la opción **--data** a **ipa-restore**:

```
[root@server1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
```

2. Introduzca la contraseña del Administrador de directorios.

```
Contraseña del administrador del directorio (maestro existente):
```

3. Introduzca **yes** para confirmar la sobrescritura de los datos actuales con la copia de seguridad.

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
server1.example.com
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data. Continue to restore? [no]: yes
```

4. La utilidad **ipa-restore** desactiva la replicación en todos los servidores que están disponibles:

```
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Disabling replication agreement on server1.example.com to caReplica2.example.com
Disabling CA replication agreement on server1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

A continuación, la utilidad detiene los servicios de IdM, restaura la copia de seguridad y reinicia los servicios:

```
Stopping IPA services
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in EXAMPLE-COM
Restoring from ipaca in EXAMPLE-COM
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

5. Reinicie todas las réplicas conectadas al servidor restaurado:

   a. Enumerar todos los segmentos de topología de replicación para el sufijo **domain**, tomando nota de los segmentos de topología que implican al servidor restaurado.

```
[root@server1 ~]# ipa topologysegment-find domain
------------------
2 segments matched
------------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both

  Segment name: caReplica2.example.com-to-replica3.example.com
  Left node: caReplica2.example.com
  Right node: replica3.example.com
  Connectivity: both
----------------------------
Number of entries returned 2
----------------------------
```

   b. Reinicie el sufijo **domain** para todos los segmentos de topología con el servidor restaurado. En este ejemplo, realice una reinicialización de **caReplica2** con datos de **server1**.

```
[root@caReplica2 ~]# ipa-replica-manage re-initialize --from=server1.example.com
Update in progress, 2 seconds elapsed
Update succeeded
```

   c. Pasando a los datos de la Autoridad de Certificación, liste todos los segmentos de topología de replicación para el sufijo **ca**.

```
[root@server1 ~]# ipa topologysegment-find ca
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

   d. Reinicie todas las réplicas de CA conectadas al servidor restaurado. En este ejemplo, realice una reinicialización de **csreplica** de **caReplica2** con datos de **server1**.

```
[root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
from=server1.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

6. Continúe moviéndose hacia afuera a través de la topología de replicación, reiniciando las sucesivas réplicas, hasta que todos los servidores hayan sido actualizados con los datos del servidor restaurado **server1.example.com**.
   En este ejemplo, sólo tenemos que reiniciar el sufijo **domain** en **replica3** con los datos de **caReplica2**:

```
[root@replica3 ~]# ipa-replica-manage re-initialize --from=caReplica2.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

7. Borre la caché de SSSD en cada servidor para evitar problemas de autenticación debido a datos no válidos:

   a. Detenga el servicio SSSD:

```
[root@server ~]# systemctl stop sssd
```

   b. Eliminar todo el contenido en caché de SSSD:

```
[root@server ~]# sss_cache -E
```

   c. Inicie el servicio SSSD:

```
[root@server ~]# systemctl start sssd
```

   d. Reinicie el servidor.

Recursos adicionales

- La página de manual **ipa-restore**(1) también cubre en detalle cómo manejar escenarios complejos de replicación durante la restauración.

7.9. RESTAURACIÓN A PARTIR DE UNA COPIA DE SEGURIDAD ENCRIPTADA

La utilidad **ipa-restore** detecta automáticamente si una copia de seguridad de IdM está encriptada, y la restaura utilizando el llavero raíz GPG2 y **gpg-agent** por defecto.

Requisitos previos

- Una copia de seguridad de IdM cifrada con GPG. Ver Creación de copias de seguridad de IdM encriptadas.
- La contraseña del gestor de directorios LDAP
- El **Passphrase** utilizado al crear la clave GPG

Procedimiento

1. Si ha utilizado una ubicación de llavero personalizada al crear las claves GPG2, asegúrese de que la variable de entorno **$GNUPGHOME** esté establecida en ese directorio. Consulte Creación de una clave GPG2 para cifrar las copias de seguridad de IdM.

```
[root@server ~]# echo $GNUPGHOME
/root/backup
```

2. Proporcione a la utilidad **ipa-restore** la ubicación del directorio de la copia de seguridad.

```
[root@server ~]# ipa-restore ipa-full-2020-01-13-18-30-54
```

   a. Introduzca la contraseña del Administrador de directorios.

```
Contraseña del administrador del directorio (maestro existente):
```

   b. Introduzca la dirección **Passphrase** que utilizó al crear la clave GPG.

```
┌──────────────────────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:        │
│ "IPA Backup (IPA Backup) <root@example.com>"                         │
│ 2048-bit RSA key, ID BF28FFA302EF4557,                               │
│ created 2020-01-13.                                                  │
│                                                                      │
│                                                                      │
│ Passphrase: SecretPassPhrase42                                       │
│                                                                      │
│       <OK>                                <Cancel>                   │
└──────────────────────────────────────────────────────────────────────┘
```

3. Reinicie todas las réplicas conectadas al servidor restaurado. Consulte Restauración de un servidor IdM a partir de una copia de seguridad.