Red Hat Enterprise Linux 8

Configurar la autenticación y la autorización en RHEL

Uso de SSSD, authselect y sssctl para configurar la autenticación y la autorización

Last Updated: 2021-03-04

Red Hat Enterprise Linux 8 Configurar la autenticación y la autorización en RHEL

Uso de SSSD, authselect y sssctl para configurar la autenticación y la autorización

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

Esta colección de documentación proporciona instrucciones sobre cómo configurar la autenticación y la autorización en un host Red Hat Enterprise Linux 8.

Table of Contents

HACER QUE EL CÓDIGO ABIERTO SEA MÁS INCLUSIVO 3

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT 4

CAPÍTULO 1. CONFIGURACIÓN DE LA AUTENTICACIÓN DE USUARIOS MEDIANTE AUTHSELECT 5
1.1. PARA QUÉ SIRVE AUTHSELECT 5
1.1.1. Archivos y directorios que authselect modifica 5
1.1.2. Los proveedores de datos en /etc/nsswitch.conf 6
1.2. ELEGIR UN PERFIL AUTHSELECT 7
1.3. MODIFICACIÓN DE UN PERFIL AUTHSELECT YA HECHO 8
1.4. CREACIÓN Y DESPLIEGUE DE SU PROPIO PERFIL AUTHSELECT 9
Ejemplo 10
1.5. CONVERTIR SUS GUIONES DE AUTHCONFIG A AUTHSELECT 11

CAPÍTULO 2. ENTENDER EL SSSD Y SUS BENEFICIOS 13
2.1. CÓMO FUNCIONA EL SSSD 13
2.2. VENTAJAS DEL USO DE LA SSSD 13
2.3. MÚLTIPLES ARCHIVOS DE CONFIGURACIÓN DE SSSD POR CLIENTE 14
Cómo procesa SSSD los archivos de configuración 14
2.4. PROVEEDORES DE IDENTIDAD Y AUTENTICACIÓN PARA SSSD 14
Proveedores de identidad y autenticación como dominios SSSD 14
Proveedores de proxy 15
Combinaciones disponibles de proveedores de identidad y autenticación 15

CAPÍTULO 3. CONFIGURACIÓN DE SSSD PARA USAR LDAP Y REQUERIR AUTENTICACIÓN TLS 17
3.1. UN CLIENTE OPENLDAP QUE UTILIZA SSSD PARA RECUPERAR DATOS DE LDAP DE FORMA ENCRIPTADA 17
3.2. CONFIGURACIÓN DE SSSD PARA USAR LDAP Y REQUERIR AUTENTICACIÓN TLS 17

CAPÍTULO 4. CONFIGURACIÓN DE RHEL PARA UTILIZAR AD COMO PROVEEDOR DE AUTENTICACIÓN ... 20
4.1. UN HOST RHEL INDEPENDIENTE QUE UTILIZA AD COMO PROVEEDOR DE AUTENTICACIÓN 20
4.2. CONFIGURACIÓN DE UN HOST RHEL PARA UTILIZAR AD COMO PROVEEDOR DE AUTENTICACIÓN 20

CAPÍTULO 5. INFORMES SOBRE EL ACCESO DE LOS USUARIOS EN LOS HOSTS QUE UTILIZAN SSSD 24
5.1. EL COMANDO SSSCTL 24
5.2. GENERACIÓN DE INFORMES DE CONTROL DE ACCESO MEDIANTE SSSCTL 24
5.3. VISUALIZACIÓN DE LOS DETALLES DE LA AUTORIZACIÓN DEL USUARIO UTILIZANDO SSSCTL 25

CAPÍTULO 6. CONSULTA DE LA INFORMACIÓN DEL DOMINIO MEDIANTE SSSD 27
6.1. LISTADO DE DOMINIOS CON SSSCTL 27
6.2. VERIFICACIÓN DEL ESTADO DEL DOMINIO MEDIANTE SSSCTL 27

CAPÍTULO 7. ELIMINACIÓN DE ERRORES TIPOGRÁFICOS EN LA CONFIGURACIÓN LOCAL DE SSSD .. 29

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. CONFIGURACIÓN DE LA AUTENTICACIÓN DE USUARIOS MEDIANTE AUTHSELECT

1.1. PARA QUÉ SIRVE AUTHSELECT

Puede utilizar la utilidad **authselect** para configurar la autenticación de usuarios en un host Red Hat Enterprise Linux 8.

Puede configurar la información de identidad y las fuentes y proveedores de autenticación seleccionando uno de los perfiles ya creados:

- El perfil predeterminado **sssd** habilita el demonio de servicios de seguridad del sistema (SSSD) para los sistemas que utilizan la autenticación LDAP.
- El perfil **winbind** habilita la utilidad Winbind para sistemas directamente integrados con Microsoft Active Directory.
- El perfil **nis** garantiza la compatibilidad con los sistemas heredados de Network Information Service (NIS).
- El perfil **minimal** sólo sirve a los usuarios y grupos locales directamente desde los archivos del sistema, lo que permite a los administradores eliminar los servicios de autenticación de red que ya no son necesarios.

Después de seleccionar un perfil **authselect** para un host determinado, el perfil se aplica a todos los usuarios que se conectan al host.

Red Hat recomienda el uso de **authselect** en entornos de gestión de identidades semicentralizados, por ejemplo, si su organización utiliza bases de datos LDAP, Winbind o NIS para autenticar a los usuarios que utilizan los servicios de su dominio.

AVISO

No utilice **authselect** si su host es parte de Red Hat Enterprise Linux Identity Management (IdM). Al unir su host a un dominio IdM con el comando **ipa-client-install** se configura automáticamente la autenticación SSSD en su host.

Del mismo modo, no utilice **authselect** si su host forma parte de Active Directory a través de SSSD. Al llamar al comando **realm join** para unir su host a un dominio de Active Directory, se configura automáticamente la autenticación SSSD en su host.

1.1.1. Archivos y directorios que authselect modifica

La utilidad **authconfig**, utilizada en versiones anteriores de Red Hat Enterprise Linux, creaba y modificaba muchos archivos de configuración diferentes, lo que dificultaba la resolución de problemas. **Authselect** simplifica las pruebas y la resolución de problemas porque sólo modifica los siguientes archivos y directorios:

/etc/nsswitch.conf	La biblioteca C de GNU y otras aplicaciones utilizan este archivo de configuración del conmutador de servicios de nombres (NSS) para determinar las fuentes de las que obtener información de servicios de nombres en un rango de categorías, y en qué orden. Cada categoría de información se identifica con un nombre de base de datos.
/etc/pam.d/* archivos	Linux-PAM (Pluggable Authentication Modules) es un sistema de módulos que se encargan de las tareas de autenticación de las aplicaciones (servicios) del sistema. La naturaleza de la autenticación es configurable dinámicamente: el administrador del sistema puede elegir cómo autenticarán a los usuarios las aplicaciones individuales que prestan servicios. Los archivos de configuración en el directorio **/etc/pam.d/** listan las PAMs que realizarán las tareas de autenticación requeridas por un servicio, y el comportamiento apropiado de la PAM-API en caso de que las PAMs individuales fallen. Entre otras cosas, estos archivos contienen información sobre: • condiciones de bloqueo de la contraseña del usuario • la posibilidad de autentificarse con una tarjeta inteligente • la posibilidad de autentificarse con un lector de huellas dactilares
/etc/dconf/db/distro.d/* archivos	Este directorio contiene perfiles de configuración para la utilidad **dconf**, que puede utilizar para gestionar la configuración de la interfaz gráfica de usuario (GUI) del Escritorio GNOME.

1.1.2. Los proveedores de datos en /etc/nsswitch.conf

El perfil por defecto **sssd** establece el SSSD como fuente de información mediante la creación de entradas **sss** en **/etc/nsswitch.conf**:

```
passwd:     sss files
group:      sss files
netgroup:   sss files
automount:  sss files
services:   sss files
...
```

Esto significa que el sistema busca primero en la SSSD si se solicita información relativa a uno de esos elementos:

- **passwd** para la información del usuario
- **group** para la información del grupo de usuarios
- **netgroup** para la información de NIS **netgroup**

- **automount** para información de automontaje NFS
- **services** para obtener información sobre los servicios

Sólo si la información solicitada no se encuentra en la caché de **sssd** y en el servidor que proporciona la autenticación, o si **sssd** no se está ejecutando, el sistema busca en los archivos locales, es decir **/etc/***.

Por ejemplo, si se solicita información sobre un identificador de usuario, primero se busca en la caché de **sssd**. Si no se encuentra allí, se consulta el archivo **/etc/passwd**. De forma análoga, si se solicita la afiliación a un grupo de usuarios, se busca primero en la caché **sssd** y sólo si no se encuentra allí, se consulta el archivo **/etc/group**.

En la práctica, la base de datos local **files** no suele consultarse. La excepción más importante es el caso del usuario **root**, que nunca es gestionado por **sssd** sino por **files**.

1.2. ELEGIR UN PERFIL AUTHSELECT

Como administrador del sistema, puede seleccionar un perfil para la utilidad **authselect** para un host específico. El perfil se aplicará a todos los usuarios que inicien sesión en el host.

Requisitos previos

- Necesita las credenciales de **root** para ejecutar los comandos de **authselect**

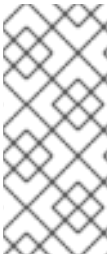
Procedimiento

- Seleccione el perfil **authselect** que sea apropiado para su proveedor de autenticación. Por ejemplo, para iniciar sesión en la red de una empresa que utiliza LDAP, seleccione **sssd**.

```
# authselect select sssd
```

  - (Opcional) Puede modificar la configuración del perfil por defecto añadiendo las siguientes opciones al comando **authselect select sssd** o **authselect select winbind**, por ejemplo:
    - **with-faillock**
    - **with-smartcard**
    - **with-fingerprint**

  Para ver la lista completa de opciones disponibles, consulte Sección 1.5, “Convertir sus guiones de **authconfig** a **authselect**” o la página de manual **authselect-migration(7)**.



NOTA

Asegúrese de que los archivos de configuración relevantes para su perfil están configurados correctamente antes de finalizar el procedimiento **authselect select**. Por ejemplo, si el demonio **sssd** no está configurado correctamente y activo, la ejecución de **authselect select** da como resultado que sólo los usuarios locales puedan autenticarse, utilizando **pam_unix**.

Pasos de verificación

1. Compruebe que las entradas de **sss** para SSSD están presentes en **/etc/nsswitch.conf**:

```
passwd:     sss files
group:      sss files
netgroup:   sss files
automount:  sss files
services:   sss files
...
```

2. Revise el contenido del archivo **/etc/pam.d/system-auth** para ver las entradas de **pam_sss.so**:

```
# Generated by authselect on Tue Sep 11 22:59:06 2018
# Do not modify this file manually.

auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]    pam_succeed_if.so uid >= 1000 quiet
auth        [default=1 ignore=ignore success=ok]    pam_localuser.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        sufficient    pam_sss.so forward_pass
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
...
```

Recursos adicionales

- Para ver una lista de perfiles ya hechos en **authselect**, consulte Sección 1.1, "Para qué sirve authselect".
- Si ajustar un perfil ya hecho añadiendo una de las opciones de la línea de comandos **authselect select** descritas anteriormente no es suficiente para su caso de uso, puede:
  - modificar un perfil ya hecho cambiando el archivo **/etc/authselect/user-nsswitch.conf**. Para más detalles, consulte Sección 1.3, "Modificación de un perfil authselect ya hecho".
  - crear su propio perfil personalizado. Para más detalles, consulte Sección 1.4, "Creación y despliegue de su propio perfil authselect".

1.3. MODIFICACIÓN DE UN PERFIL AUTHSELECT YA HECHO

Como administrador del sistema, puede modificar uno de los perfiles por defecto para adaptarlo a sus necesidades.

Puede modificar cualquiera de los elementos del archivo **/etc/authselect/user-nsswitch.conf** a excepción de:

- **passwd**
- **group**
- **netgroup**
- **automount**

- **services**

Si se ejecuta posteriormente **authselect select profile_name** , se transferirán los cambios permitidos de **/etc/authselect/user-nsswitch.conf** al archivo **/etc/nsswitch.conf**. Los cambios inaceptables son sobrescritos por la configuración del perfil por defecto.

IMPORTANTE

No modifique el archivo **/etc/nsswitch.conf** directamente.

Procedimiento

1. Seleccione un perfil de **authselect**, por ejemplo:

```
# authselect select sssd
```

2. Edite el archivo **/etc/authselect/user-nsswitch.conf** con los cambios que desee.

3. Aplique los cambios del archivo **/etc/authselect/user-nsswitch.conf**:

```
# authselect apply-changes
```

Pasos de verificación

- Revise el archivo **/etc/nsswitch.conf** para verificar que los cambios de **/etc/authselect/user-nsswitch.conf** se han propagado allí.

Recursos adicionales

- Para ver una lista de perfiles ya hechos en **authselect**, consulte Sección 1.1, “Para qué sirve authselect”.

1.4. CREACIÓN Y DESPLIEGUE DE SU PROPIO PERFIL AUTHSELECT

Como administrador del sistema, puede crear e implementar un perfil personalizado haciendo una copia personalizada de uno de los perfiles predeterminados.

Esto es particularmente útil si Sección 1.3, “Modificación de un perfil authselect ya hecho” no es suficiente para sus necesidades. Cuando se despliega un perfil personalizado, el perfil se aplica a todos los usuarios que inician sesión en el host dado.

Procedimiento

1. Cree su perfil personalizado utilizando el comando **authselect create-profile**. Por ejemplo, para crear un perfil personalizado llamado **user-profile** basado en el perfil ya preparado **sssd** pero en el que usted mismo puede configurar los elementos del archivo **/etc/nsswitch.conf**:

```
# authselect create-profile user-profile -b sssd --symlink-meta --symlink-pam
New profile was created at /etc/authselect/custom/user-profile
```

Incluir la opción **--symlink-pam** en el comando significa que las plantillas PAM serán enlaces simbólicos a los archivos del perfil de origen en lugar de su copia; incluir la opción **--symlink-meta** significa que los meta archivos, como README y REQUIREMENTS serán enlaces

simbólicos a los archivos del perfil de origen en lugar de su copia. Esto asegura que todas las futuras actualizaciones de las plantillas PAM y los meta archivos en el perfil original se reflejarán también en su perfil personalizado.

El comando crea una copia del archivo **/etc/nsswitch.conf** en el directorio **/etc/authselect/custom/user-profile/**.

2. Configure el archivo **/etc/authselect/custom/user-profile/nsswitch.conf**.

3. Seleccione el perfil personalizado ejecutando el comando **authselect select**, y añadiendo **custom/*name_of_the_profile*** como parámetro. Por ejemplo, para seleccionar el perfil **user-profile**:

```
# authselect select custom/user-profile
```

La selección del perfil **user-profile** para su máquina significa que si el perfil **sssd** es actualizado posteriormente por Red Hat, se beneficiará de todas las actualizaciones a excepción de las realizadas en el archivo **/etc/nsswitch.conf**.

Ejemplo

El siguiente procedimiento muestra cómo crear un perfil basado en el perfil **sssd** que sólo consulta la búsqueda de la tabla estática local para los nombres de host en el archivo **/etc/hosts**, no en las bases de datos **dns** o **myhostname**.

1. Edite el archivo **/etc/nsswitch.conf** editando la siguiente línea:

```
hosts:      files
```

2. Cree un perfil personalizado basado en **sssd** que excluya los cambios en **/etc/nsswitch.conf**:

```
# authselect create-profile user-profile -b sssd --symlink-meta --symlink-pam
```

3. Seleccione el perfil:

```
# authselect select custom/user-profile
```

4. Opcionalmente, compruebe que la selección del perfil personalizado tiene
   - crear el archivo **/etc/pam.d/system-auth** de acuerdo con el perfil elegido **sssd**
   - dejó la configuración en el **/etc/nsswitch.conf** sin cambios:

```
hosts:      files
```

NOTA

Por el contrario, si se ejecuta **authselect select sssd** , el resultado sería

```
hosts:      files dns myhostname
```

Recursos adicionales

- Para ver una lista de perfiles ya hechos en **authselect**, consulte Sección 1.1, "Para qué sirve authselect".

1.5. CONVERTIR SUS GUIONES DE AUTHCONFIG A AUTHSELECT

Si utilizas **ipa-client-install** o **realm join** para unirte a un dominio, puedes eliminar con seguridad cualquier llamada a **authconfig** en tus scripts. Si no es posible, sustituya cada llamada a **authconfig** por su equivalente **authselect**. Al hacerlo, seleccione el perfil correcto y las opciones adecuadas. Además, edite los archivos de configuración necesarios:

- **/etc/krb5.conf**
- **/etc/sssd/sssd.conf** (para el perfil **sssd**) o **/etc/samba/smb.conf** (para el perfil **winbind**)

Relación de las opciones de authconfig con los perfiles de authselect **authselect** ??? y Los equivalentes de las opciones de authconfig de los perfiles de authselect muestran los equivalentes de las opciones de **authconfig**.

Tabla 1.1. Relación de las opciones de authconfig con los perfiles de authselect

Authconfig options	Authselect profile
--enableldap --enableldapauth	**sssd**
--enablesssd --enablesssdauth	**sssd**
--enablekrb5	**sssd**
--enablewinbind --enablewinbindauth	**winbind**
--enablenis	**nis**

Tabla 1.2. Opciones de perfil Authselect equivalentes a las opciones de authconfig

Authconfig option	Authselect profile feature
--enablesmartcard	**with-smartcard**
--enablefingerprint	**with-fingerprint**
--enableecryptfs	**with-ecryptfs**
--enablemkhomedir	**with-mkhomedir**
--enablefaillock	**with-faillock**
--enablepamaccess	**with-pamaccess**
--enablewinbindkrb5	**with-krb5**

Tabla 1.3, "Ejemplos de comandos authselect equivalentes a los comandos authconfig" muestra ejemplos de transformaciones de llamadas Kickstart a **authconfig** en llamadas Kickstart a **authselect**.

Tabla 1.3. Ejemplos de comandos authselect equivalentes a los comandos authconfig

authconfig command	authselect equivalent
authconfig --enableldap --enableldapauth --enablefaillock --updateall	**authselect select sssd with-faillock**
authconfig --enablesssd --enablesssdauth --enablesmartcard --smartcardmodule=sssd --updateall	**authselect select sssd with-smartcard**
authconfig --enableecryptfs --enablepamaccess --updateall	**authselect select sssd with-ecryptfs with-pamaccess**
authconfig --enablewinbind --enablewinbindauth --winbindjoin=Administrator --updateall	**realm join -U Administrator --client-software=winbind WINBINDDOMAIN**

CAPÍTULO 2. ENTENDER EL SSSD Y SUS BENEFICIOS

2.1. CÓMO FUNCIONA EL SSSD

El demonio de servicios de seguridad del sistema (SSSD) es un servicio del sistema que permite acceder a directorios remotos y mecanismos de autenticación. Puede conectar un sistema local, un SSSD *client*, a un sistema back-end externo, un *provider*, por ejemplo:

- Un directorio LDAP
- Un dominio de gestión de identidades (IdM)
- Un dominio de Active Directory (AD)
- Un reino Kerberos

El SSSD funciona en dos etapas:

1. Conecta al cliente con un proveedor remoto para recuperar la información de identidad y autenticación.
2. Utiliza la información de autenticación obtenida para crear una caché local de usuarios y credenciales en el cliente.

Los usuarios del sistema local pueden entonces autenticarse utilizando las cuentas de usuario almacenadas en el proveedor remoto.

SSSD no crea cuentas de usuario en el sistema local. Sin embargo, SSSD puede configurarse para crear directorios personales para los usuarios de IdM. Una vez creado, el directorio principal de un usuario de IdM y su contenido en el cliente no se eliminan cuando el usuario cierra la sesión.

Figura 2.1. Cómo funciona el SSSD

SSSD también puede proporcionar cachés para varios servicios del sistema, como Name Service Switch (NSS) o Pluggable Authentication Modules (PAM).

2.2. VENTAJAS DEL USO DE LA SSSD

El uso del demonio de servicios de seguridad del sistema (SSSD) ofrece múltiples ventajas en cuanto a la recuperación de la identidad del usuario y la autenticación del mismo.

Autenticación sin conexión

SSSD mantiene opcionalmente una caché de identidades y credenciales de usuario recuperadas de proveedores remotos. En esta configuración, un usuario -siempre que se haya autenticado una vez

contra el proveedor remoto al inicio de la sesión- puede autenticarse con éxito en los recursos incluso si el proveedor remoto o el cliente están desconectados.

Una sola cuenta de usuario: mejora de la coherencia del proceso de autenticación

Con SSSD, no es necesario mantener tanto una cuenta central como una cuenta de usuario local para la autenticación sin conexión. Las condiciones son:

- En una sesión concreta, el usuario debe haberse conectado al menos una vez: el cliente debe estar conectado al proveedor remoto cuando el usuario se conecte por primera vez.
- El almacenamiento en caché debe estar activado en SSSD.
  Sin SSSD, los usuarios remotos suelen tener varias cuentas de usuario. Por ejemplo, para conectarse a una red privada virtual (VPN), los usuarios remotos tienen una cuenta para el sistema local y otra cuenta para el sistema VPN. En este escenario, primero hay que autenticarse en la red privada para obtener el usuario del servidor remoto y almacenar en caché las credenciales del usuario a nivel local.

  Con SSSD, gracias al almacenamiento en caché y a la autenticación sin conexión, los usuarios remotos pueden conectarse a los recursos de la red simplemente autenticándose en su máquina local. SSSD mantiene entonces sus credenciales de red.

Reducción de la carga de los proveedores de identidad y autenticación

Al solicitar información, los clientes comprueban primero la caché local de SSSD. SSSD se pone en contacto con los proveedores remotos sólo si la información no está disponible en la caché.

2.3. MÚLTIPLES ARCHIVOS DE CONFIGURACIÓN DE SSSD POR CLIENTE

El archivo de configuración por defecto para SSSD es **/etc/sssd/sssd.conf**. Aparte de este archivo, SSSD puede leer su configuración de todos los archivos ***.conf** en el directorio **/etc/sssd/conf.d/**.

Esta combinación le permite utilizar el archivo **/etc/sssd/sssd.conf** por defecto en todos los clientes y añadir ajustes adicionales en otros archivos de configuración para ampliar la funcionalidad de forma individual por cliente.

Cómo procesa SSSD los archivos de configuración

SSSD lee los archivos de configuración en este orden:

1. El archivo principal **/etc/sssd/sssd.conf**
2. Otros archivos de ***.conf** en **/etc/sssd/conf.d/**, en orden alfabético

Si el mismo parámetro aparece en varios archivos de configuración, SSSD utiliza el último parámetro leído.

NOTA

SSSD no lee los archivos ocultos (archivos que empiezan por **.**) en el directorio **conf.d**.

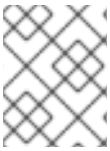
2.4. PROVEEDORES DE IDENTIDAD Y AUTENTICACIÓN PARA SSSD

Proveedores de identidad y autenticación como dominios SSSD

Los proveedores de identidad y autenticación se configuran como *domains* en el archivo de configuración de SSSD, **/etc/sssd/sssd.conf**. Los proveedores aparecen en la sección **[domain/*name of the domain*]** o **[domain/default]** del archivo.

Un solo dominio puede ser configurado como uno de los siguientes proveedores:

- Un *identity provider*, que proporciona información del usuario, como el UID y el GID.
  - Especifique un dominio como el *identity provider* utilizando la opción **id_provider** en la sección **[domain/*name of the domain*]** sección del archivo **/etc/sssd/sssd.conf**.
- Un *authentication provider*, que gestiona las solicitudes de autenticación.
  - Especifique un dominio como el *authentication provider* utilizando la opción **auth_provider** en la sección **[domain/*name of the domain*]** sección de **/etc/sssd/sssd.conf**.
- Un *access control provider*, que gestiona las solicitudes de autorización.
  - Especifique un dominio como el *access control provider* utilizando la opción **access_provider** en la sección **[domain/*name of the domain*]** sección de **/etc/sssd/sssd.conf**. Por defecto, la opción se establece en **permit**, que siempre permite todo el acceso. Consulte la página de manual **sssd.conf**(5) para más detalles.
- Una combinación de estos proveedores, por ejemplo si todas las operaciones correspondientes se realizan dentro de un mismo servidor.
  - En este caso, las opciones **id_provider**, **auth_provider**, y **access_provider** aparecen en la misma **[domain/*name of the domain*]** o **[domain/default]** sección de **/etc/sssd/sssd.conf**.



NOTA

Puede configurar varios dominios para SSSD. Debe configurar al menos un dominio, de lo contrario SSSD no se iniciará.

Proveedores de proxy

Un proveedor de proxy funciona como un relé intermediario entre SSSD y los recursos que, de otro modo, SSSD no podría utilizar. Cuando se utiliza un proveedor de proxy, SSSD se conecta al servicio de proxy, y el proxy carga las bibliotecas especificadas.

Puede configurar SSSD para que utilice un proveedor de proxy con el fin de habilitarlo:

- Métodos de autenticación alternativos, como el escáner de huellas dactilares
- Sistemas heredados, como NIS
- Una cuenta del sistema local definida en el archivo **/etc/passwd** como proveedor de identidad y un proveedor de autenticación remoto, por ejemplo Kerberos

Combinaciones disponibles de proveedores de identidad y autenticación

Puede configurar SSSD para utilizar las siguientes combinaciones de proveedores de identidad y autenticación.

Tabla 2.1. Combinaciones disponibles de proveedores de identidad y autenticación

Proveedor de identidades	Proveedor de autenticación
Gestión de identidades [a]	Gestión de la identidad
Directorio Activo	Directorio Activo
LDAP	LDAP
LDAP	Kerberos
Proxy	Proxy
Proxy	LDAP
Proxy	Kerberos

[a] Una extensión del tipo de proveedor LDAP.

Recursos adicionales

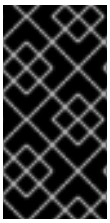
- Puede configurar SSSD utilizando la utilidad **authselect**. Para más detalles sobre el uso de **authselect**, consulte Capítulo 1, *Configuración de la autenticación de usuarios mediante authselect*.
- Si su host está inscrito en Identity Management (IdM) que está en un acuerdo de confianza con un bosque de Active Directory (AD), puede listar y verificar el estado de los dominios utilizando la utilidad **sssctl**. Para más detalles, consulte Capítulo 6, *Consulta de la información del dominio mediante SSSD*.
- Puede utilizar la utilidad **sssctl** para crear informes de control de acceso y visualizar los datos de los usuarios. Para más detalles, consulte Capítulo 5, *Informes sobre el acceso de los usuarios en los hosts que utilizan SSSD*.

CAPÍTULO 3. CONFIGURACIÓN DE SSSD PARA USAR LDAP Y REQUERIR AUTENTICACIÓN TLS

3.1. UN CLIENTE OPENLDAP QUE UTILIZA SSSD PARA RECUPERAR DATOS DE LDAP DE FORMA ENCRIPTADA

El demonio de servicios de seguridad del sistema (SSSD) es un demonio que gestiona la recuperación de datos de identidad y la autenticación en un host RHEL 8. Un administrador del sistema puede configurar el SSSD en el host para utilizar una base de datos de un servidor LDAP independiente como base de datos de cuentas de usuario. Ejemplos de un servidor LDAP incluyen el servidor OpenLDAP y el Red Hat Directory Server. En este capítulo, el escenario también incluye el requisito de que la conexión con el servidor LDAP debe estar encriptada con un certificado TLS.

El método de autenticación de los objetos LDAP puede ser una contraseña Kerberos o una contraseña LDAP. Tenga en cuenta que las cuestiones de autenticación y autorización de los objetos LDAP no se abordan en este capítulo.



IMPORTANTE

La configuración de SSSD con LDAP es un procedimiento complejo que requiere un alto nivel de experiencia en SSSD y LDAP. Considere utilizar una solución integrada y automatizada como Active Directory o Red Hat Identity Management (IdM) en su lugar. Para más detalles sobre IdM, consulte Planificación de la gestión de identidad es.

3.2. CONFIGURACIÓN DE SSSD PARA USAR LDAP Y REQUERIR AUTENTICACIÓN TLS

Complete este procedimiento para configurar su sistema Red Hat Enterprise Linux (RHEL) como un cliente OpenLDAP con la siguiente configuración de cliente:

- El sistema RHEL autentifica a los usuarios almacenados en una base de datos de cuentas de usuario OpenLDAP.
- El sistema RHEL utiliza el servicio System Security Services Daemon (SSSD) para recuperar los datos del usuario.
- El sistema RHEL se comunica con el servidor OpenLDAP a través de una conexión cifrada TLS.

NOTA

También puede utilizar este procedimiento para configurar su sistema RHEL como cliente de un Red Hat Directory Server.

Requisitos previos

- El servidor OpenLDAP está instalado y configurado con la información de los usuarios.
- Tienes permisos de root en el host que estás configurando como cliente LDAP.
- En el host que está configurando como cliente LDAP, se ha creado el archivo **/etc/sssd/sssd.conf** y se ha configurado para especificar **ldap** como el **autofs_provider** y el **id_provider**.

- Tiene una copia con formato PEM de la cadena de certificados de firma de la CA raíz de la autoridad de certificación que emitió el certificado del servidor OpenLDAP, almacenada en un archivo local llamado **core-dirsrv.ca.pem**.

Procedimiento

1. Instale los paquetes necesarios:

```
# dnf -y install openldap-clients sssd sssd-ldap oddjob-mkhomedir
```

2. Cambie el proveedor de autenticación a **sssd**:

```
# authselect select sssd with-mkhomedir
```

3. Copie el archivo **core-dirsrv.ca.pem** que contiene la cadena de certificados de firma de la CA raíz de la autoridad de certificación que emitió el certificado SSL/TLS del servidor OpenLDAP en la carpeta **/etc/openldap/certs**.

```
# cp core-dirsrv.ca.pem /etc/openldap/certs
```

4. Añade la URL y el sufijo de tu servidor LDAP al archivo **/etc/openldap/ldap.conf**:

```
URI ldap://ldap-server.example.com/
BASE dc=example,dc=com
```

5. En el archivo **/etc/openldap/ldap.conf**, añada una línea que señale el parámetro **TLS_CACERT** a **/etc/openldap/certs/core-dirsrv.ca.pem**:

```
# When no CA certificates are specified the Shared System Certificates
# are in use. In order to have these available along with the ones specified
# by TLS_CACERTDIR one has to include them explicitly:
TLS_CACERT /etc/openldap/certs/core-dirsrv.ca.pem
```

6. En el archivo **/etc/sssd/sssd.conf**, añada sus valores de entorno a los parámetros **ldap_uri** y **ldap_search_base**:

```
[domain/default]
id_provider = ldap
autofs_provider = ldap
auth_provider = ldap
chpass_provider = ldap
ldap_uri = ldap://ldap-server.example.com/
ldap_search_base = dc=example,dc=com
ldap_id_use_start_tls = True
cache_credentials = True
ldap_tls_cacertdir = /etc/openldap/certs
ldap_tls_reqcert = allow

[sssd]
services = nss, pam, autofs
domains = default
```

```
[nss]
homedir_substring = /home
…
```

7. En **/etc/sssd/sssd.conf**, especifique el requisito de autenticación TLS modificando los valores **ldap_tls_cacert** y **ldap_tls_reqcert** en la sección **[domain]**:

```
…
cache_credentials = True
ldap_tls_cacert = /etc/openldap/certs/core-dirsrv.ca.pem
ldap_tls_reqcert = hard
…
```

8. Cambie los permisos del archivo **/etc/sssd/sssd.conf**:

```
# chmod 600 /etc/sssd/sssd.conf
```

9. Reinicie y active el servicio SSSD y el demonio **oddjobd**:

```
# systemctl restart sssd oddjobd
# systemctl enable sssd oddjobd
```

10. (Opcional) Si su servidor LDAP utiliza los protocolos obsoletos TLS 1.0 o TLS 1.1, cambie la política criptográfica de todo el sistema en el sistema cliente al nivel LEGACY para permitir que RHEL 8 se comunique utilizando estos protocolos:

```
# update-crypto-policies --set LEGACY
```

Para más detalles, consulte la sección Funcionalidad obsoleta en las Notas de la versión de RHEL 8.0.

Pasos de verificación

- Compruebe que puede recuperar los datos de los usuarios de su servidor LDAP utilizando el comando **id** y especificando un usuario LDAP:

```
# id ldap_user
uid=17388(ldap_user) gid=45367(sysadmins)
groups=45367(sysadmins),25395(engineers),10(wheel),1202200000(admins)
```

El administrador del sistema puede ahora consultar a los usuarios desde LDAP utilizando el comando **id**. El comando devuelve un ID de usuario correcto y la pertenencia a un grupo.

Directiva no resuelta en master.adoc - include::assemblies/assembly_sssd-client-side-view.adoc[leveloffset= 1]

CAPÍTULO 4. CONFIGURACIÓN DE RHEL PARA UTILIZAR AD COMO PROVEEDOR DE AUTENTICACIÓN

4.1. UN HOST RHEL INDEPENDIENTE QUE UTILIZA AD COMO PROVEEDOR DE AUTENTICACIÓN

Como administrador del sistema, puede utilizar Active Directory (AD) como proveedor de autenticación para un host Red Hat Enterprise Linux (RHEL) sin unir el host a AD si, por ejemplo:

- No quiere conceder a los administradores de AD el control sobre la activación y desactivación del host.
- El host, que puede ser un PC corporativo, está destinado a ser utilizado sólo por un usuario de su empresa.

IMPORTANTE

Aplique este procedimiento sólo en los raros casos en que se prefiera este enfoque.

Considere la posibilidad de unir el sistema a AD o a Red Hat Identity Management (IdM). Unir el host RHEL a un dominio hace que la configuración sea más fácil de gestionar. Si le preocupan las licencias de acceso de clientes relacionadas con la unión de clientes a AD directamente, considere aprovechar un servidor IdM que esté en un acuerdo de confianza con AD. Para obtener más información sobre un acuerdo de confianza IdM-AD, consulte Planificación de un acuerdo de confianza entre IdM y AD e Instalación de un acuerdo de confianza entre IdM y AD.

4.2. CONFIGURACIÓN DE UN HOST RHEL PARA UTILIZAR AD COMO PROVEEDOR DE AUTENTICACIÓN

Realice este procedimiento para que el usuario denominado **AD_user** pueda iniciar sesión en el sistema **rhel8_host** utilizando la contraseña establecida en la base de datos de usuarios AD de Active Directory en el dominio **example.com**. En este ejemplo, el dominio **EXAMPLE.COM** Kerberos corresponde al dominio **example.com**.

Requisitos previos

- Tienes acceso de root a **rhel8_host**.
- La cuenta de usuario **AD_user** existe en el dominio **example.com**.
- El ámbito de Kerberos es **EXAMPLE.COM**.
- **rhel8_host** no se ha unido a AD mediante el comando **realm join**.

Procedimiento

1. Cree la cuenta de usuario **AD_user** localmente sin asignarle una contraseña:

```
# useradd AD_user
```

2. Abra el archivo **/etc/nsswitch.conf** para editarlo y asegúrese de que contiene las siguientes líneas:

```
passwd:     sss files systemd
group:      sss files systemd
shadow:     files sss
```

3. Abra el archivo **/etc/krb5.conf** para editarlo y asegúrese de que contiene las siguientes secciones y elementos:

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = /etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_realm = EXAMPLE.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 EXAMPLE.COM = {
     kdc = ad.example.com
     admin_server = ad.example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

4. Cree el archivo **/etc/sssd/sssd.conf** e inserte en él las siguientes secciones y líneas:

```
[sssd]
    services = nss, pam
    domains = EXAMPLE.COM

[domain/EXAMPLE.COM]
    id_provider = files
    auth_provider = krb5
    krb5_realm = EXAMPLE.COM
    krb5_server = ad.example.com
```

5. Cambie los permisos del archivo **/etc/sssd/sssd.conf**:

```
# chmod 600 /etc/sssd/sssd.conf
```

6. Inicie el demonio de servicios del sistema de seguridad (SSSD):

```
# systemctl start sssd
```

7. Activar SSSD:

```
# systemctl enable sssd
```

8. Abra el archivo **/etc/pam.d/system-auth** y modifíquelo para que contenga las siguientes secciones y líneas:

```
# Generated by authselect on Wed May  8 08:55:04 2019
# Do not modify this file manually.

auth        required                                    pam_env.so
auth        required                                    pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]        pam_succeed_if.so uid >= 1000 quiet
auth        [default=1 ignore=ignore success=ok]        pam_localuser.so
auth        sufficient                                  pam_unix.so nullok try_first_pass
auth        requisite                                   pam_succeed_if.so uid >= 1000 quiet_success
auth        sufficient                                  pam_sss.so forward_pass
auth        required                                    pam_deny.so

account     required                                    pam_unix.so
account     sufficient                                  pam_localuser.so
account     sufficient                                  pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                                    pam_permit.so

password    requisite                                   pam_pwquality.so try_first_pass local_users_only
password    sufficient                                  pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password    sufficient                                  pam_sss.so use_authtok
password    required                                    pam_deny.so

session     optional                                    pam_keyinit.so revoke
session     required                                    pam_limits.so
-session    optional                                    pam_systemd.so
session     [success=1 default=ignore]                  pam_succeed_if.so service in crond quiet
use_uid
session     required                                    pam_unix.so
session     optional                                    pam_sss.so
```

9. Copie el contenido del archivo **/etc/pam.d/system-auth** en el archivo **/etc/pam.d/password-auth**. Introduzca **yes** para confirmar la sobreescritura del contenido actual del archivo:

```
# cp /etc/pam.d/system-auth /etc/pam.d/password-auth
cp: overwrite '/etc/pam.d/password-auth'? yes
```

Pasos de verificación

1. Solicite un ticket Kerberos (TGT) para **AD_user**. Introduzca la contraseña de **AD_user** tal y como se solicita:

```
# kinit AD_user
Password for AD_user@EXAMPLE.COM:
```

2. Muestra el TGT obtenido:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: AD_user@EXAMPLE.COM

Valid starting     Expires            Service principal
11/02/20 04:16:38  11/02/20 14:16:38  krbtgt/EXAMPLE.COM@EXAMPLE.COM
 renew until 18/02/20 04:16:34
```

AD_user se ha conectado con éxito a **rhel8_host** utilizando las credenciales del dominio Kerberos **EXAMPLE.COM**.

CAPÍTULO 5. INFORMES SOBRE EL ACCESO DE LOS USUARIOS EN LOS HOSTS QUE UTILIZAN SSSD

El Security System Services Daemon (SSSD) rastrea qué usuarios pueden o no pueden acceder a los clientes. Este capítulo describe la creación de informes de control de acceso y la visualización de los datos de los usuarios mediante la herramienta **sssctl**.

Requisitos previos

- Los paquetes SSSD están instalados en su entorno de red.

5.1. EL COMANDO SSSCTL

sssctl es una herramienta de línea de comandos que utiliza Security System Services Daemon (SSSD) para recopilar información sobre:

- estado del dominio
- autenticación del usuario cliente
- el acceso de los usuarios a los clientes de un determinado dominio
- información sobre el contenido en caché

Con la herramienta **sssctl**, puedes:

- gestionar la caché de SSSD
- gestionar los registros
- comprobar los archivos de configuración

NOTA

La herramienta **sssctl** sustituye a las herramientas **sss_cache** y **sss_debuglevel**.

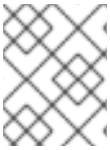
Recursos adicionales

- Para más detalles sobre **sssctl**, entre:

```
# ssctl --help
```

5.2. GENERACIÓN DE INFORMES DE CONTROL DE ACCESO MEDIANTE SSSCTL

Puede enumerar las reglas de control de acceso aplicadas a la máquina en la que está ejecutando el informe, ya que SSSD controla qué usuarios pueden iniciar sesión en el cliente.



NOTA

El informe de acceso no es preciso porque la herramienta no hace un seguimiento de los usuarios bloqueados por el Centro de Distribución de Claves (KDC).

Requisitos previos

- Debe estar conectado con privilegios de administrador
- La página **sssctl** está disponible en los sistemas RHEL 7 y RHEL 8

Procedimiento

- Para generar un informe para el dominio **idm.example.com**, introduzca:

```
[root@client1 ~]# sssctl access-report idm.example.com
1 rule cached

Rule name: example.user
 Member users: example.user
 Member services: sshd
```

5.3. VISUALIZACIÓN DE LOS DETALLES DE LA AUTORIZACIÓN DEL USUARIO UTILIZANDO SSSCTL

El comando **sssctl user-checks** ayuda a depurar problemas en las aplicaciones que utilizan el demonio de servicios de seguridad del sistema (SSSD) para la búsqueda, autenticación y autorización de usuarios.

El comando **sssctl user-checks [USER_NAME]** muestra los datos del usuario disponibles a través del conmutador de servicio de nombres (NSS) y el respondedor InfoPipe para la interfaz D-Bus. Los datos visualizados muestran si el usuario está autorizado a iniciar sesión mediante el servicio **system-auth** Pluggable Authentication Module (PAM).

El comando tiene dos opciones:

- **-a** para una acción PAM
- **-s** para un servicio PAM

Si no define las opciones **-a** y **-s**, la herramienta **sssctl** utiliza las opciones por defecto: **-a acct -s system-auth**.

Requisitos previos

- Debe estar conectado con privilegios de administrador
- La herramienta **sssctl** está disponible en los sistemas RHEL 7 y RHEL 8

Procedimiento

- Para mostrar los datos de un usuario en particular, introduzca:

```
[root@client1 ~]# sssctl user-checks -a acct -s sshd example.user
user: example.user
action: acct
service: sshd
....
```

Recursos adicionales

Recursos adicionales

- Para más detalles sobre **sssctl user-checks**, utilice el siguiente comando:

```
sssctl user-checks --help
```

CAPÍTULO 6. CONSULTA DE LA INFORMACIÓN DEL DOMINIO MEDIANTE SSSD

Security System Services Daemon (SSSD) puede enumerar los dominios en Identity Management (IdM), incluidos los dominios de Active Directory en la confianza entre bosques. También puede verificar el estado de cada uno de los dominios listados:

- Listado de dominios con el comando sssctl
- Verificación del estado del dominio mediante el comando sssctl

6.1. LISTADO DE DOMINIOS CON SSSCTL

El comando **sssctl domain-list** ayuda a depurar problemas con la topología del dominio.

NOTA

Es posible que el estado no esté disponible inmediatamente. Si el dominio no es visible, repita el comando.

Requisitos previos

- Debe estar conectado con privilegios de administrador
- La página **sssctl** está disponible en los sistemas RHEL 7 y RHEL 8

Procedimiento

1. Para mostrar la ayuda del comando sssctl, introduzca:

```
[root@client1 ~]# sssctl --help
....
```

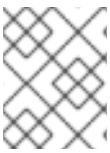
2. Para mostrar una lista de dominios disponibles, introduzca:

```
[root@client1 ~]# sssctl domain-list
implicit_files
idm.example.com
ad.example.com
sub1.ad.example.com
```

La lista incluye dominios en la confianza cruzada entre Active Directory y Gestión de Identidades.

6.2. VERIFICACIÓN DEL ESTADO DEL DOMINIO MEDIANTE SSSCTL

El comando **sssctl domain-status** ayuda a depurar problemas con la topología del dominio.



NOTA

Es posible que el estado no esté disponible inmediatamente. Si el dominio no es visible, repita el comando.

Requisitos previos

- Debe estar conectado con privilegios de administrador
- La página **sssctl** está disponible en los sistemas RHEL 7 y RHEL 8

Procedimiento

1. Para mostrar la ayuda del comando sssctl, introduzca:

```
[root@client1 ~]# sssctl --help
```

2. Para mostrar los datos de los usuarios de un determinado dominio, introduzca:

```
[root@client1 ~]# sssctl domain-status idm.example.com
Online status: Online

Active servers:
IPA: master.idm.example.com

Discovered IPA servers:
- master.idm.example.com
```

El dominio **idm.example.com** está en línea y es visible desde el cliente donde aplicó el comando.

Si el dominio no está disponible, el resultado es:

```
[root@client1 ~]# sssctl domain-status ad.example.com
Unable to get online status
```

CAPÍTULO 7. ELIMINACIÓN DE ERRORES TIPOGRÁFICOS EN LA CONFIGURACIÓN LOCAL DE SSSD

Puede comprobar si el archivo **/etc/sssd/sssd.conf** de su host contiene algún error tipográfico utilizando el comando **sssctl config-check**.

Requisitos previos

- Has iniciado la sesión como root.

Procedimiento

1. Introduzca el comando **sssctl config-check**:

```
# sssctl config-check

Issues identified by validators: 1
[rule/allowed_domain_options]: Attribute 'ldap_search' is not allowed in section
'domain/example1'. Check for typos.

Messages generated during configuration merging: 0

Used configuration snippet files: 0
```

2. Abra el archivo **/etc/sssd/sssd.conf** y corrija el error. Si, por ejemplo, recibió el mensaje de error del paso anterior, sustituya **ldap_search** por **ldap_search_base**:

```
[...]
[domain/example1]
ldap_search_base = dc=example,dc=com
[...]
```

3. Guarda el archivo.

4. Reinicie el SSSD:

```
# systemctl restart sssd
```

Pasos de verificación

- Introduzca el comando **sssctl config-check**:

```
# sssctl config-check

Issues identified by validators: 0

Messages generated during configuration merging: 0

Used configuration snippet files: 0
```

El archivo **/etc/sssd/sssd.conf** ahora no tiene errores tipográficos.