Red Hat Enterprise Linux 8

Integrando os sistemas RHEL diretamente com o Active Directory do Windows

Entendendo e configurando os sistemas RHEL para se conectar diretamente com o Active Directory

Last Updated: 2021-03-07

Red Hat Enterprise Linux 8 Integrando os sistemas RHEL diretamente com o Active Directory do Windows

Entendendo e configurando os sistemas RHEL para se conectar diretamente com o Active Directory

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.

Nota Legal

Resumo

Esta coleção de documentação fornece instruções sobre como integrar os sistemas RHEL diretamente com o Active Directory do Windows usando SSSD.

Índice

TORNANDO O CÓDIGO ABERTO MAIS INCLUSIVO

A Red Hat tem o compromisso de substituir a linguagem problemática em nosso código, documentação e propriedades da web. Estamos começando com estes quatro termos: master, slave, blacklist e whitelist. Por causa da enormidade deste esforço, estas mudanças serão implementadas gradualmente ao longo de vários lançamentos futuros. Para mais detalhes, veja a mensagem de nosso CTO Chris Wright.

FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT

Agradecemos sua contribuição em nossa documentação. Por favor, diga-nos como podemos melhorá-la. Para fazer isso:

- Para comentários simples sobre passagens específicas:
  1. Certifique-se de que você está visualizando a documentação no formato *Multi-page HTML*. Além disso, certifique-se de ver o botão **Feedback** no canto superior direito do documento.
  2. Use o cursor do mouse para destacar a parte do texto que você deseja comentar.
  3. Clique no pop-up **Add Feedback** que aparece abaixo do texto destacado.
  4. Siga as instruções apresentadas.
- Para enviar comentários mais complexos, crie um bilhete Bugzilla:
  1. Ir para o site da Bugzilla.
  2. Como Componente, use **Documentation**.
  3. Preencha o campo **Description** com sua sugestão de melhoria. Inclua um link para a(s) parte(s) relevante(s) da documentação.
  4. Clique em **Submit Bug**.

CAPÍTULO 1. CONECTANDO OS SISTEMAS RHEL DIRETAMENTE AO AD USANDO SSSD

Esta seção descreve o uso do System Security Services Daemon (SSSD) para conectar um sistema RHEL ao Active Directory (AD). Você precisa de dois componentes para conectar um sistema RHEL ao Active Directory (AD). Um componente, SSSD, interage com a identidade central e fonte de autenticação, e o outro componente, **realmd**, detecta domínios disponíveis e configura os serviços subjacentes do sistema RHEL, neste caso o SSSD, para se conectar ao domínio.

- Visão geral da integração direta usando SSSD
- Plataformas Windows suportadas para integração direta
- Garantia de suporte para tipos comuns de criptografia em AD e RHEL
- Conectando-se diretamente ao AD
- Como o provedor AD lida com as atualizações dinâmicas do DNS
- Modificando configurações DNS dinâmicas para o provedor AD
- Como o provedor AD lida com domínios confiáveis
- comandos do reino

1.1. VISÃO GERAL DA INTEGRAÇÃO DIRETA USANDO SSSD

Você usa SSSD para acessar um diretório de usuários para autenticação e autorização através de uma estrutura comum com cache de usuários para permitir logins offline. O SSSD é altamente configurável; ele fornece Módulos de Autenticação Plugáveis (PAM) e integração com Serviço de Troca de Nomes (NSS) e um banco de dados para armazenar usuários locais, bem como dados estendidos de usuários recuperados de um servidor central. O SSSD é o componente recomendado para conectar um sistema RHEL com um dos seguintes tipos de servidor de identidade:

- Active Directory
- Gestão da Identidade (IdM) na RHEL
- Qualquer servidor genérico LDAP ou Kerberos

NOTA

A integração direta com o SSSD funciona apenas dentro de uma única floresta AD por padrão.

A maneira mais conveniente de configurar o SSSD para integrar diretamente um sistema Linux com AD é usar o serviço **realmd**. Ele permite aos chamadores configurar a autenticação da rede e a adesão ao domínio de uma forma padrão. O serviço **realmd** descobre automaticamente informações sobre domínios e reinos acessíveis e não requer configuração avançada para aderir a um domínio ou reino.

Você pode usar SSSD para integração direta e indireta com AD e ele permite mudar de uma abordagem de integração para outra. A integração direta é uma maneira simples de introduzir os sistemas RHEL a um ambiente AD. Entretanto, à medida que a participação dos sistemas RHEL cresce, suas implementações geralmente precisam de uma melhor gestão centralizada das políticas relacionadas à identidade, tais como controle de acesso baseado em host, sudo, ou mapeamentos de usuários SELinux.

Inicialmente, você pode manter a configuração destes aspectos dos sistemas RHEL em arquivos de configuração local. Entretanto, com um número crescente de sistemas, a distribuição e o gerenciamento dos arquivos de configuração é mais fácil com um sistema de provisionamento como o Red Hat Satellite. Quando a integração direta não for mais escalonada, você deve considerar a integração indireta. Para mais informações sobre como passar da integração direta (os clientes RHEL estão no domínio AD) para a integração indireta (IdM com confiança para AD), consulte Mudando clientes RHEL do domínio AD para o servidor IdM.

Para mais informações sobre qual tipo de integração se adequa ao seu caso de uso, consulte Decidindo entre integração indireta e direta.

Recursos adicionais

- A página do homem **realm(8)**.
- A página do homem **sssd-ad(5)**.
- A página do homem **sssd(8)**.

1.2. PLATAFORMAS WINDOWS SUPORTADAS PARA INTEGRAÇÃO DIRETA

Você pode integrar diretamente seu sistema RHEL com as florestas do Active Directory que utilizam os seguintes níveis funcionais de floresta e domínio:

- Faixa de nível funcional da floresta: Windows Server 2008 - Windows Server 2016
- Gama de níveis funcionais de domínio: Windows Server 2008 - Windows Server 2016

A integração direta foi testada nos seguintes sistemas operacionais suportados:

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

NOTA

O Windows Server 2019 não introduz um novo nível funcional. O nível funcional mais alto que o Windows Server 2019 usa é o Windows Server 2016.

1.3. GARANTIA DE SUPORTE PARA TIPOS COMUNS DE CRIPTOGRAFIA EM AD E RHEL

Por padrão, o SSSD suporta os tipos de criptografia RC4, AES-128, e AES-256 Kerberos.

A criptografia RC4 foi depreciada e desativada por padrão no RHEL 8, pois é considerada menos segura que os novos tipos de criptografia AES-128 e AES-256. Em contraste, as credenciais de usuário do Active Directory (AD) e os trusts entre domínios AD suportam a criptografia RC4 e podem não suportar os tipos de criptografia AES.

Sem nenhum tipo de criptografia comum, a comunicação entre hosts RHEL e domínios AD pode não funcionar, ou algumas contas AD podem não ser capazes de autenticar. Para remediar esta situação, modifique uma das seguintes configurações:

- **Enable AES encryption support in Active Directory (recommended option)** Para garantir a confiança entre os domínios AD em uma floresta AD suporta fortes tipos de criptografia AES, veja o seguinte artigo da Microsoft: AD DS: Segurança: Kerberos Erro de tipo "Unsupported etype" ao acessar um recurso em um domínio confiável

- **Enable RC4 support in RHEL**: Em cada host RHEL onde ocorre a autenticação contra os Controladores de Domínios AD:

  1. Use o comando **update-crypto-policies** para ativar a subpolítica criptográfica **AD-SUPPORT**, além da política criptográfica **DEFAULT**.

     ```
     [root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT
     Setting system policy to DEFAULT:AD-SUPPORT
     Note: System-wide crypto policies are applied on application start-up.
     It is recommended to restart the system for the change of policies
     to fully take place.
     ```

  2. Reinicie o anfitrião.

IMPORTANTE

A sub-política criptográfica **AD-SUPPORT** só está disponível no RHEL 8.3 e mais recente.

- Para permitir o suporte ao RC4 no RHEL 8.2, crie e habilite uma política de módulos criptográficos personalizados com **cipher = RC4-128** . Para obter mais detalhes, consulte Personalização de políticas criptográficas em todo o sistema com modificadores de políticas.

- Para permitir o suporte ao RC4 no RHEL 8.0 e RHEL 8.1, adicione **rc4** à opção **permitted_enctypes** no arquivo **/etc/crypto-policies/back-ends/krb5.config**:

  ```
  [libdefaults]
  permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac +rc4
  ```

Recursos adicionais

- Para mais informações sobre como trabalhar com políticas criptográficas RHEL, consulte Utilizando políticas criptográficas de todo o sistema no guia Security Hardening.

1.4. CONECTANDO-SE DIRETAMENTE AO AD

Esta seção descreve como integrar diretamente com AD usando o mapeamento de ID ou atributos POSIX.

- Descobrir e unir um domínio AD usando SSSD

- Opções para integração com AD: usando o mapeamento de ID ou atributos POSIX

- Conexão ao AD usando atributos POSIX definidos no Active Directory
- Conectando-se a múltiplos domínios em diferentes florestas AD com SSSD

1.4.1. Descobrir e unir um domínio AD usando SSSD

Este procedimento descreve como descobrir um domínio AD e conectar um sistema RHEL a esse domínio usando SSSD.

Pré-requisitos

- Certifique-se de que as seguintes portas no host RHEL estejam abertas e acessíveis para os controladores de domínio AD.

  Tabela 1.1. Portos necessários para a integração direta de sistemas Linux no AD usando SSSD

Serviço	Porto	Protocolo	Notas
DNS	53	UDP e TCP	
LDAP	389	UDP e TCP	
Kerberos	88	UDP e TCP	
Kerberos	464	UDP e TCP	Usado pela kadmin para definir e alterar uma senha
Catálogo global LDAP	3268	TCP	Se a opção **id_provider = ad** estiver sendo utilizada
NTP	123	UDP	Opcional

- Certifique-se de que você está usando o servidor controlador de domínio AD para DNS.
- Verificar se o tempo do sistema em ambos os sistemas está sincronizado. Isto assegura que Kerberos seja capaz de trabalhar corretamente.

Procedimento

1. Instale os seguintes pacotes:

```
# yum instalar realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. Para exibir informações para um domínio específico, execute **realm discover** e adicione o nome do domínio que você deseja descobrir:

```
# realm discover ad.example.com
ad.example.com
  type: kerberos
```

```
realm-name: AD.EXAMPLE.COM
domain-name: ad.example.com
configured: no
server-software: active-directory
client-software: sssd
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common
```

O sistema **realmd** usa pesquisas DNS SRV para encontrar automaticamente os controladores de domínio neste domínio.

NOTA

O sistema **realmd** pode descobrir tanto o Active Directory quanto os domínios de Gerenciamento de Identidade. Se ambos os domínios existirem em seu ambiente, você pode limitar os resultados da descoberta a um tipo específico de servidor usando a opção **--server-software=active-directory**.

3. Configure o sistema RHEL local com o comando **realm join**. A suíte **realmd** edita automaticamente todos os arquivos de configuração necessários. Por exemplo, para um domínio chamado **ad.example.com**:

```
# realm join ad.example.com
```

Etapas de verificação

- Exibir os detalhes de um usuário AD, como por exemplo o usuário administrador:

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:1450400500:1450400513:Administrator:/home/administrator
@ad.example.com:/bin/bash
```

Recursos adicionais

- Veja a página de manual **realm(8)**.
- Veja a página de manual **nmcli(1)**.

1.4.2. Opções para integração com AD: usando o mapeamento de ID ou atributos POSIX

Os sistemas Linux e Windows utilizam identificadores diferentes para usuários e grupos:

- Linux usa *user IDs* (UID) e *group IDs* (GID). Veja Managing Users and Groups em *Configuring Basic System Settings*. As UIDs e GIDs do Linux estão em conformidade com a norma POSIX.
- O Windows usa *security IDs* (SID).

IMPORTANTE

Não usar o mesmo nome de usuário em Windows e Linux.

Para autenticar em um sistema RHEL como usuário AD, é necessário ter um UID e um GID designados. O SSSD fornece a opção de integração com o AD usando o mapeamento de ID ou atributos POSIX. O padrão é usar o mapeamento de ID.

1.4.2.1. Gerar automaticamente novos UIDs e GIDs para usuários AD

O SSSD pode usar o SID de um usuário AD para gerar algorítmicamente IDs POSIX em um processo chamado *ID mapping*. O mapeamento de ID cria um mapa entre os SIDs no AD e IDs no Linux.

- Quando o SSSD detecta um novo domínio AD, ele atribui uma gama de IDs disponíveis para o novo domínio.
- Quando um usuário AD faz o login em uma máquina cliente SSSD pela primeira vez, o SSSD cria uma entrada para o usuário no cache SSSD, incluindo um UID baseado no SID do usuário e na faixa de ID para aquele domínio.
- Como os IDs para um usuário AD são gerados de forma consistente a partir do mesmo SID, o usuário tem o mesmo UID e GID ao fazer o login em qualquer sistema Red Hat Enterprise Linux.

Veja Descobrindo e unindo um domínio AD usando SSSD .

NOTA

Quando todos os sistemas clientes usam SSSD para mapear SIDs para IDs Linux, o mapeamento é consistente. Se alguns clientes utilizam softwares diferentes, escolha um dos seguintes:

- Garantir que o mesmo algoritmo de mapeamento seja usado em todos os clientes.
- Utilizar atributos POSIX explícitos definidos no AD.

1.4.2.2. Usar atributos POSIX definidos no AD

AD pode criar e armazenar atributos POSIX, tais como **uidNumber**, **gidNumber**, **unixHomeDirectory**, ou **loginShell**.

Ao utilizar o mapeamento de ID descrito acima, o SSSD cria novos UIDs e GIDs, que se sobrepõem aos valores definidos no AD. Para manter os valores definidos no AD, você deve desativar o mapeamento de ID no SSSD.

Veja Conectando ao AD usando atributos POSIX definidos no Active Directory .

1.4.3. Conexão ao AD usando atributos POSIX definidos no Active Directory

Para melhor desempenho, publique os atributos POSIX no catálogo global AD. Se os atributos POSIX não estiverem presentes no catálogo global, o SSSD se conecta aos controladores de domínio individuais diretamente na porta LDAP.

Pré-requisitos

- Certifique-se de que as seguintes portas no host RHEL estejam abertas e acessíveis para os controladores de domínio AD.

Tabela 1.2. Portos necessários para a integração direta de sistemas Linux no AD usando SSSD

Serviço	Porto	Protocolo	Notas
DNS	53	UDP e TCP	
LDAP	389	UDP e TCP	
Kerberos	88	UDP e TCP	
Kerberos	464	UDP e TCP	Usado pela kadmin para definir e alterar uma senha
Catálogo global LDAP	3268	TCP	Se a opção **id_provider = ad** estiver sendo utilizada
NTP	123	UDP	Opcional

- Certifique-se de que você está usando o servidor controlador de domínio AD para DNS.
- Verificar se o tempo do sistema em ambos os sistemas está sincronizado. Isto assegura que Kerberos seja capaz de trabalhar corretamente.

Procedimento

1. Instale os seguintes pacotes:

```
# yum instalar realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. Configure o sistema RHEL local com o mapeamento de identificação desabilitado usando o comando **realm join** com a opção **--automatic-id-mapping=no**. A suíte **realmd** edita automaticamente todos os arquivos de configuração necessários. Por exemplo, para um domínio chamado **ad.example.com**:

```
# Reino Unido --automatic-id-mapping=no ad.example.com
```

3. Se você já entrou em um domínio, você pode desativar manualmente o mapeamento de identificação no SSSD:

   a. Abra o arquivo **/etc/sssd/sssd.conf**.

   b. Na seção de domínio AD, adicione a configuração **ldap_id_mapping = false**.

   c. Remover as caches SSSD:

```
rm -f /var/lib/sss/db/*
```

d. Reinicie o SSSD:

```
systemctl restart sssd
```

O SSSD agora usa atributos POSIX do AD, em vez de criá-los localmente.

NOTA

Você deve ter os atributos POSIX relevantes (**uidNumber**, **gidNumber**, **unixHomeDirectory**, e **loginShell**) configurados para os usuários no AD.

Etapas de verificação

- Exibir os detalhes de um usuário AD, como por exemplo o usuário administrador:

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:10000:10000:Administrator:/home/Administrator:/bin/bash
```

Recursos adicionais

- Para mais detalhes sobre o mapeamento de ID e o parâmetro **ldap_id_mapping**, consulte a página de manual **sssd-ldap(8)**.

1.4.4. Conectando-se a múltiplos domínios em diferentes florestas AD com SSSD

Este procedimento descreve a união e autenticação de múltiplos domínios do Active Directory (AD) em diferentes florestas onde não há confiança entre eles.

Este exemplo descreve a união de dois domínios, **addomain1.com** e **addomain2.com**. Use **realmd** para entrar no primeiro domínio e configurar automaticamente SSSD, Kerberos e outros utilitários para esse domínio. Use **adcli** para entrar em domínios adicionais e edite manualmente os arquivos de configuração para incluir esses domínios.

Pré-requisitos

- Certifique-se de que as seguintes portas no host RHEL estejam abertas e acessíveis para os controladores de domínio AD.

Tabela 1.3. Portos necessários para a integração direta de sistemas Linux no AD usando SSSD

Serviço	Porto	Protocolo	Notas
DNS	53	UDP e TCP	
LDAP	389	UDP e TCP	
Kerberos	88	UDP e TCP	
Kerberos	464	UDP e TCP	Usado pela kadmin para definir e alterar uma senha

Serviço	Porto	Protocolo	Notas
Catálogo global LDAP	3268	TCP	Se a opção **id_provider = ad** estiver sendo utilizada
NTP	123	UDP	Opcional

- Certifique-se de que você está usando o servidor controlador de domínio AD para DNS.
- Verificar se o tempo do sistema em ambos os sistemas está sincronizado. Isto assegura que Kerberos seja capaz de trabalhar corretamente.
- Garantir que você tenha credenciais para uma conta de administrador AD em cada domínio AD que tenha direitos de ingressar em máquinas para esse domínio

Procedimento

1. Instalar os pacotes necessários.

```
# yum install sssd realmd adcli samba-common-tools oddjob oddjob-mkhomedir
```

2. Use **realmd** para entrar no primeiro domínio AD, **addomain1.com**.

```
# reino junte-se a ADDOMAIN1.COM
```

3. Renomeie o keytab do sistema para um nome único.

```
# mv /etc/krb5.keytab /etc/addomain1.com.krb5.keytab
```

4. Use **adcli** para entrar no segundo domínio AD, e quaisquer domínios adicionais. Use a opção **-K** para especificar um caminho único para o keytab Kerberos onde as credenciais do host serão escritas.

```
# adcli join -D dc2.addomain2.com -K /etc/addomain2.com.krb5.keytab
```

5. Modificar **/etc/krb5.conf**.
   - Adicione a opção **includedir** para incluir arquivos de configuração SSSD.
   - Habilitar consultas DNS para Controladores de Domínios AD com a opção **dns_lookup_kdc**.

```
includedir /var/lib/sss/pubconf/krb5.include.d/

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

[libdefaults]
```

```
default_realm = ADDOMAIN1.COM
dns_lookup_realm = false
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true

...
```

6. Modifique **/etc/sssd/sssd.conf** para incluir informações sobre todos os domínios AD em uso.

```
[sssd]
services = nss, pam
config_file_version = 2
domains = addomain1.com, addomain2.com

[domain/addomain1.com]
id_provider = ad
access_provider = ad
krb5_keytab = /etc/addomain1.com.krb5.keytab
ldap_krb5_keytab = /etc/addomain1.com.krb5.keytab
ad_server = dc1.addomain1.com
ad_maximum_machine_account_password_age = 0
use_fully_qualified_names = true
default_shell=/bin/bash
override_homedir=/home/%d/%u

[domain/addomain2.com]
id_provider = ad
access_provider = ad
krb5_keytab = /etc/addomain2.com.krb5.keytab
ldap_krb5_keytab = /etc/addomain2.com.krb5.keytab
ad_server = dc2.addomain2.com
ad_maximum_machine_account_password_age = 0
use_fully_qualified_names = true
default_shell=/bin/bash
override_homedir=/home/%d/%u

[nss]

[pam]
```

- Para cada seção de domínio, especifique o caminho para o keytab Kerberos que corresponde a cada domínio com as opções **krb5_keytab** e **ldap_krb5_keytab**.
- Defina **ad_maximum_machine_account_password_age = 0** para desativar a renovação das chaves Kerberos do host.
- Defina **use_fully_qualified_names = true** para diferenciar os usuários de diferentes domínios.
- Definir **override_homedir = /home/%d/%u** para que os usuários (**%u**) de diferentes domínios (**%d**) each receive unique home directories. For example, the home directory for user **linuxuser@addomain1.com** is **/home/addomain1.com/linuxuser**.

7. O SSH recupera as chaves do host da tabela de chaves do sistema e fornece uma única

funcionalidade de sinalização através de GSSAPI/Kerberos. Se você gostaria de usar o single sign-on, copie todas as chaves de host atuais do Kerberos para a guia de chaves do sistema **/etc/kbr5.keytab**.

```
# ktutil
ktutil:  rkt /etc/addomain1.com.krb5.keytab
ktutil:  rkt /etc/addomain2.com.krb5.keytab
ktutil:  wkt /etc/krb5.keytab
```

8. Reinicie e habilite o serviço SSSD.

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

Etapas de verificação

1. Mostrar os detalhes do usuário para os usuários de cada domínio AD:

```
# id administrator@addomain1.com
uid=1240800500(administrator@addomain1.com) gid=1240800513(domain
users@addomain1.com) groups=1240800513(domain
users@addomain1.com),1240800512(domain
admins@addomain1.com),1240800518(schema
admins@addomain1.com),1240800520(group policy creator
owners@addomain1.com),1240800572(denied rodc password replication
group@addomain1.com),1240800519(enterprise admins@addomain1.com)

# id administrator@addomain2.com
uid=1013800500(administrator@addomain2.com)
gid=1013800500(administrator@addomain2.com)
groups=1013800500(administrator@addomain2.com),1013800513(domain
users@addomain2.com)
```

2. Faça o login como usuário de cada domínio e verifique se o diretório home correto foi criado para o usuário.

```
# ssh administrator@addomain1.com@localhost
administrator@addomain1.com@localhost's password:
Creating directory '/home/addomain1.com/administrator'.

$ pwd
/home/addomain1.com/administrator
```

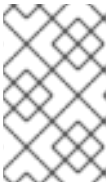
```
# ssh administrator@addomain2.com@localhost
administrator@addomain2.com@localhost's password:
Creating directory '/home/addomain2.com/administrator'.

$ pwd
/home/addomain2.com/administrator
```

1.5. COMO O PROVEDOR AD LIDA COM AS ATUALIZAÇÕES DINÂMICAS DO DNS

O Active Directory (AD) mantém ativamente seus registros DNS através de cronograma (*aging*) e remoção (*scavenging*) de registros inativos.

Por padrão, o serviço SSSD atualiza o registro DNS de um cliente RHEL nos seguintes intervalos:

- Toda vez que o fornecedor de identidade entra on-line.
- Toda vez que o sistema RHEL é reinicializado.
- No intervalo especificado pela opção **dyndns_refresh_interval** no arquivo de configuração **/etc/sssd/sssd.conf**. O valor padrão é **86400** segundos (24 horas).



NOTA

Se você definir a opção **dyndns_refresh_interval** para o mesmo intervalo que a locação DHCP, você pode atualizar o registro DNS após a renovação da locação IP.

SSSD envia atualizações dinâmicas do DNS para o servidor AD usando Kerberos/GSSAPI para DNS (GSS-TSIG). Isto significa que você só precisa habilitar conexões seguras ao AD.

Recursos adicionais

- A página do homem **sssd-ad(5)**.

1.6. MODIFICANDO CONFIGURAÇÕES DNS DINÂMICAS PARA O PROVEDOR AD

O procedimento a seguir ajusta as configurações dentro do serviço SSSD para afetar como ele atualiza automaticamente o registro DNS para um host RHEL unido a um ambiente Active Directory.

Pré-requisitos

- Você juntou um host RHEL a um ambiente Active Directory com o serviço SSSD.
- Você precisa de **root** permissões para editar o arquivo de configuração **/etc/sssd/sssd.conf**.

Procedimento

1. Abra o arquivo de configuração **/etc/sssd/sssd.conf** em um editor de texto.
2. Adicione as seguintes opções à seção **[domain]** para seu domínio AD para definir o intervalo de atualização do registro DNS para 12 horas, desabilitar a atualização dos registros PTR e definir o registro DNS Time To Live (TTL) para 1 hora.

```
[domain/ad.example.com]
id_provider = ad
...
dyndns_refresh_interval = 43200
dyndns_update_ptr = false
dyndns_ttl = 3600
```

3. Salve e feche o arquivo de configuração **/etc/sssd/sssd.conf**.

4. Reinicie o serviço SSSD para carregar as mudanças de configuração.

```
[root@client ~]# systemctl restart sssd
```

NOTA

Você pode desativar atualizações dinâmicas do DNS configurando a opção **dyndns_update** no arquivo **sssd.conf** para **false**:

```
[domain/ad.example.com]
id_provider = ad
...

dyndns_update = false
```

Recursos adicionais

- **sssd-ad(5)** página do homem

1.7. COMO O PROVEDOR AD LIDA COM DOMÍNIOS CONFIÁVEIS

Esta seção descreve como o SSSD lida com domínios confiáveis se você definir a opção **id_provider = ad** no arquivo de configuração **/etc/sssd/sssd.conf**.

- O SSSD só suporta domínios em uma única floresta AD. Se o SSSD requer acesso a múltiplos domínios de múltiplas florestas, considere o uso do IPA com trusts (de preferência) ou o serviço **winbindd** em vez do SSSD.

- Por padrão, o SSSD descobre todos os domínios na floresta e, se chegar um pedido de um objeto em um domínio confiável, o SSSD tenta resolvê-lo.
  Se os domínios confiáveis não forem alcançáveis ou geograficamente distantes, o que os torna lentos, você pode definir o parâmetro **ad_enabled_domains** em **/etc/sssd/sssd.conf** para limitar de quais domínios confiáveis o SSSD resolve os objetos.

- Por padrão, você deve usar nomes de usuário totalmente qualificados para resolver usuários de domínios confiáveis.

Recursos adicionais

- A página do homem **sssd.conf(5)**.

1.8. COMANDOS DO REINO

O sistema **realmd** tem duas grandes áreas de trabalho:

- Sistema de gerenciamento de matrículas em um domínio.

- Controlar quais usuários de domínio estão autorizados a acessar os recursos do sistema local.

Em **realmd** use a ferramenta de linha de comando **realm** para executar comandos. A maioria dos comandos **realm** exige que o usuário especifique a ação que o utilitário deve executar, e a entidade, como um domínio ou conta de usuário, para a qual deve executar a ação.

Tabela 1.4. comandos do reino

Comando	Descrição
Realm Commands	
descubra	Executar uma varredura de descoberta de domínios na rede.
junte-se a	Acrescentar o sistema ao domínio especificado.
sair	Remover o sistema do domínio especificado.
lista	Liste todos os domínios configurados para o sistema ou todos os domínios descobertos e configurados.
Login Commands	
autorização	Permitir o acesso para usuários específicos ou para todos os usuários dentro de um domínio configurado para acessar o sistema local.
negue	Restringir o acesso para usuários específicos ou para todos os usuários dentro de um domínio configurado para acessar o sistema local.

Para mais informações sobre os comandos **realm**, consulte a página de manual **realm(8)**.

CAPÍTULO 2. CONECTANDO OS SISTEMAS RHEL DIRETAMENTE AO AD USANDO SAMBA WINBIND

Esta seção descreve o uso do Samba Winbind para conectar um sistema RHEL ao Active Directory (AD). Você precisa de dois componentes para conectar um sistema RHEL ao AD. Um componente, Samba Winbind, interage com a identidade e fonte de autenticação do AD, e o outro componente, **realmd**, detecta domínios disponíveis e configura os serviços subjacentes do sistema RHEL, neste caso Samba Winbind, para conectar-se ao domínio AD.

- Visão geral da integração direta usando Samba Winbind
- Plataformas Windows suportadas para integração direta
- Garantia de suporte para tipos comuns de criptografia em AD e RHEL
- Juntando um sistema RHEL a um domínio AD
- comandos do reino

2.1. VISÃO GERAL DA INTEGRAÇÃO DIRETA USANDO SAMBA WINBIND

Samba Winbind emula um cliente Windows em um sistema Linux e se comunica com servidores AD.

Você pode usar o serviço **realmd** para configurar o Samba Winbind por:

- Configurando a autenticação da rede e a adesão ao domínio de uma forma padrão.
- Descobrir automaticamente informações sobre domínios e reinos acessíveis.
- Não requer configuração avançada para ingressar em um domínio ou reino.

Note que:

- A integração direta com Winbind em uma configuração AD multifloresta requer fundos bidirecionais.
- As florestas remotas devem confiar na floresta local para garantir que o plug-in **idmap_ad** manipule corretamente os usuários florestais remotos.

O serviço **winbindd** do Samba fornece uma interface para o Name Service Switch (NSS) e permite que os usuários do domínio se autentiquem no AD ao efetuar login no sistema local.

O uso do **winbindd** oferece o benefício de poder melhorar a configuração para compartilhar diretórios e impressoras sem instalar software adicional. Para maiores detalhes, veja a seção sobre o Uso do Samba como servidor no Guia de Implementação de Diferentes Tipos de Servidores .

Recursos adicionais

- Veja a página de manual **realmd**.
- Veja a página de manual **windbindd**.

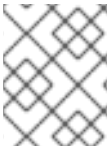
2.2. PLATAFORMAS WINDOWS SUPORTADAS PARA INTEGRAÇÃO DIRETA

Você pode integrar diretamente seu sistema RHEL com as florestas do Active Directory que utilizam os seguintes níveis funcionais de floresta e domínio:

- Faixa de nível funcional da floresta: Windows Server 2008 - Windows Server 2016
- Gama de níveis funcionais de domínio: Windows Server 2008 - Windows Server 2016

A integração direta foi testada nos seguintes sistemas operacionais suportados:

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



NOTA

O Windows Server 2019 não introduz um novo nível funcional. O nível funcional mais alto que o Windows Server 2019 usa é o Windows Server 2016.

2.3. GARANTIA DE SUPORTE PARA TIPOS COMUNS DE CRIPTOGRAFIA EM AD E RHEL

Por padrão, Samba Winbind suporta os tipos de criptografia RC4, AES-128, e AES-256 Kerberos.

A criptografia RC4 foi depreciada e desativada por padrão no RHEL 8, pois é considerada menos segura que os novos tipos de criptografia AES-128 e AES-256. Em contraste, as credenciais de usuário do Active Directory (AD) e os trusts entre domínios AD suportam a criptografia RC4 e podem não suportar os tipos de criptografia AES.

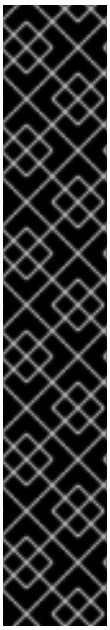
Sem nenhum tipo de criptografia comum, a comunicação entre hosts RHEL e domínios AD pode não funcionar, ou algumas contas AD podem não ser capazes de autenticar. Para remediar esta situação, modifique uma das seguintes configurações:

- **Enable AES encryption support in Active Directory (recommended option)** Para garantir a confiança entre os domínios AD em uma floresta AD suporta fortes tipos de criptografia AES, veja o seguinte artigo da Microsoft: AD DS: Segurança: Kerberos Erro de tipo "Unsupported etype" ao acessar um recurso em um domínio confiável
- **Enable RC4 support in RHEL**: Em cada host RHEL onde ocorre a autenticação contra os Controladores de Domínios AD:

  1. Use o comando **update-crypto-policies** para ativar a subpolítica criptográfica **AD-SUPPORT**, além da política criptográfica **DEFAULT**.

     ```
     [root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT
     Setting system policy to DEFAULT:AD-SUPPORT
     Note: System-wide crypto policies are applied on application start-up.
     It is recommended to restart the system for the change of policies
     to fully take place.
     ```

  2. Reinicie o anfitrião.



IMPORTANTE

A sub-política criptográfica **AD-SUPPORT** só está disponível no RHEL 8.3 e mais recente.

- Para permitir o suporte ao RC4 no RHEL 8.2, crie e habilite uma política de módulos criptográficos personalizados com **cipher = RC4-128** . Para obter mais detalhes, consulte Personalização de políticas criptográficas em todo o sistema com modificadores de políticas.
- Para permitir o suporte ao RC4 no RHEL 8.0 e RHEL 8.1, adicione **rc4** à opção **permitted_enctypes** no arquivo **/etc/crypto-policies/back-ends/krb5.config**:

```
[libdefaults]
permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac +rc4
```

Recursos adicionais

- Para mais informações sobre como trabalhar com políticas criptográficas RHEL, consulte Utilizando políticas criptográficas de todo o sistema no guia Security Hardening.

2.4. JUNTANDO UM SISTEMA RHEL A UM DOMÍNIO AD

Esta seção descreve como unir um sistema Red Hat Enterprise Linux a um domínio AD, usando **realmd** para configurar o Samba Winbind.

Procedimento

1. Se seu AD requer o tipo de criptografia RC4 obsoleto para autenticação Kerberos, habilite o suporte para estas cifras na RHEL:

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

2. Instale os seguintes pacotes:

```
# yum install realmd oddjob-mkhomedir oddjob samba-winbind-clients \ samba-winbind samba-common-tools samba-winbind-krb5-locator
```

3. Para compartilhar diretórios ou impressoras no membro do domínio, instale o pacote **samba**:

```
# yum install samba
```

4. Faça o backup do arquivo de configuração existente **/etc/samba/smb.conf** Samba:

```
# mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

5. Junte-se ao domínio. Por exemplo, para ingressar em um domínio chamado **ad.example.com**:

```
# realm join --membership-software=samba --client-software=winbind ad.example.com
```

Usando o comando anterior, o utilitário **realm** automaticamente:

- Cria um arquivo **/etc/samba/smb.conf** para uma associação no domínio **ad.example.com**
- Adiciona o módulo **winbind** para pesquisas de usuários e grupos ao arquivo **/etc/nsswitch.conf**
- Atualiza os arquivos de configuração do Módulo de Autenticação Pluggável (PAM) no diretório **/etc/pam.d/**
- Inicia o serviço **winbind** e permite que o serviço seja iniciado quando o sistema inicia

6. Opcionalmente, defina um mapeamento alternativo de identificação no back end ou configurações personalizadas de mapeamento de identificação no arquivo **/etc/samba/smb.conf**. Para detalhes, consulte a seção Entendendo e configurando o Samba ID mapping na documentação **Deploying different types of servers**.

7. Edite o arquivo **/etc/krb5.conf** e adicione a seguinte seção:

```
[plugins]
  localauth = {
    module = winbind:/usr/lib64/samba/krb5/winbind_krb5_localauth.so
    enable_only = winbind
  }
```

8. Verifique se o serviço **winbind** está funcionando:

```
# systemctl status winbind
...
  Active: active (running) since Tue 2018-11-06 19:10:40 CET; 15s ago
```

IMPORTANTE

Para que o Samba possa consultar informações de usuários e grupos de domínio, o serviço **winbind** deve estar em execução antes de você iniciar **smb**.

9. Se você instalou o pacote **samba** para compartilhar diretórios e impressoras, ative e inicie o serviço **smb**:

```
# systemctl enable --now smb
```

Etapas de verificação

1. Exibir os detalhes de um usuário AD, tais como a conta do administrador AD no domínio AD:

```
# getent passwd "AD\administrator"
AD\administrator:*:10000:10000::/home/administrator@AD:/bin/bash
```

2. Consultar os membros do grupo de usuários do domínio no domínio AD:

```
# getent group "AD\Domain Users"
  AD\domain users:x:10000:user1,user2
```

3. Opcionalmente, verifique se você pode utilizar usuários e grupos de domínio quando definir permissões em arquivos e diretórios. Por exemplo, para definir o proprietário do arquivo **/srv/samba/example.txt** para **AD\administrator** e o grupo para **AD\Domain Users**:

```
# chown "AD\administrator":"AD\Domain Users" /srv/samba/example.txt
```

4. Verificar se a autenticação Kerberos funciona como esperado:

   a. No membro do domínio AD, obtenha um ticket para o principal **administrator@AD.EXAMPLE.COM**:

```
# kinit administrator@AD.EXAMPLE.COM
```

   b. Exibir o bilhete Kerberos em cache:

```
# klist
Ticket cache: KCM:0
Default principal: administrator@AD.EXAMPLE.COM

Valid starting       Expires              Service principal
01.11.2018 10:00:00  01.11.2018 20:00:00
krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
        renew until 08.11.2018 05:00:00
```

5. Mostrar os domínios disponíveis:

```
# wbinfo --all-domains
BUILTIN
SAMBA-SERVER
AD
```

Recursos adicionais

- Se você não quiser usar as cifras RC4 depreciadas, você pode habilitar o tipo de criptografia AES em AD. Veja Habilitar o tipo de criptografia AES no Active Directory usando um GPO na documentação **Deploying different types of servers**.
- Para mais detalhes sobre a utilidade **realm**, consulte a página de manual **realm(8)**.

2.5. COMANDOS DO REINO

O sistema **realmd** tem duas grandes áreas de trabalho:

- Sistema de gerenciamento de matrículas em um domínio.
- Controlar quais usuários de domínio estão autorizados a acessar os recursos do sistema local.

Em **realmd** use a ferramenta de linha de comando **realm** para executar comandos. A maioria dos comandos **realm** exige que o usuário especifique a ação que o utilitário deve executar, e a entidade, como um domínio ou conta de usuário, para a qual deve executar a ação.

Tabela 2.1. comandos do reino

Comando	Descrição
Realm Commands	
descubra	Executar uma varredura de descoberta de domínios na rede.
junte-se a	Acrescentar o sistema ao domínio especificado.
sair	Remover o sistema do domínio especificado.
lista	Liste todos os domínios configurados para o sistema ou todos os domínios descobertos e configurados.
Login Commands	
autorização	Permitir o acesso para usuários específicos ou para todos os usuários dentro de um domínio configurado para acessar o sistema local.
negue	Restringir o acesso para usuários específicos ou para todos os usuários dentro de um domínio configurado para acessar o sistema local.

Para mais informações sobre os comandos **realm**, consulte a página de manual **realm(8)**.

CAPÍTULO 3. GERENCIANDO CONEXÕES DIRETAS COM AD

Esta seção descreve como modificar e gerenciar sua conexão com o Active Directory.

Pré-requisitos

- Você conectou seu sistema RHEL ao domínio do Active Directory.

3.1. MODIFICANDO O INTERVALO PADRÃO DE RENOVAÇÃO DO KERBEROS HOST KEYTAB

O SSSD renova automaticamente o arquivo keytab do host Kerberos em um ambiente AD se o pacote **adcli** estiver instalado. O daemon verifica diariamente se a senha da conta da máquina é mais antiga do que o valor configurado e a renova se necessário.

O intervalo de renovação padrão é de 30 dias. Para alterar o padrão, siga as etapas deste procedimento.

Procedimento

1. Adicione o seguinte parâmetro ao fornecedor de AD em seu arquivo **/etc/sssd/sssd.conf**:

```
ad_maximum_machine_account_password_age = value_in_days
```

2. Reinicie o SSSD:

```
# systemctl restart sssd
```

3. Para desativar a renovação automática do Kerberos host keytab, defina **ad_maximum_machine_account_password_age = 0**.

Recursos adicionais

- A página do homem **adcli(8)**.
- A página do homem **sssd.conf(5)**.

3.2. REMOÇÃO DE UM SISTEMA RHEL DE UM DOMÍNIO AD

Este procedimento descreve como remover um sistema RHEL de um domínio do Active Directory (AD).

Procedimento

1. Remover um sistema de um domínio de identidade usando o comando **realm leave**. O comando remove a configuração do domínio do SSSD e do sistema local.

```
# licença do reino ad.example.com
```

NOTA

Quando um cliente deixa um domínio, a conta não é excluída do AD; a configuração do cliente local é apenas removida. Se você quiser excluir a conta do AD, execute o comando com a opção **--remove**. Você é solicitado a fornecer sua senha de usuário e deve ter os direitos de remover uma conta do Active Directory.

2. Use a opção **-U** com o comando **realm leave** para especificar um usuário diferente para remover um sistema de um domínio de identidade.
   Por padrão, o comando **realm leave** é executado como o administrador padrão. Para AD, a conta do administrador é chamada **Administrator**. Se um usuário diferente foi usado para ingressar no domínio, pode ser necessário realizar a remoção como esse usuário.

```
# licença do reino [ad.example.com] -U [AD.EXAMPLE.COM\user]'
```

O comando primeiro tenta se conectar sem credenciais, mas pede uma senha, se necessário.

Etapas de verificação

- Verificar se o domínio não está mais configurado:

```
# realm discover [ad.example.com]
ad.example.com
   type: kerberos
   realm-name: EXAMPLE.COM
   domain-name: example.com
   configured: no
   server-software: active-directory
   client-software: sssd
   required-package: oddjob
   required-package: oddjob-mkhomedir
   required-package: sssd
   required-package: adcli
   required-package: samba-common-tools
```

Recursos adicionais

- Veja a página de manual **realm(8)**`.

3.3. GERENCIANDO PERMISSÕES DE LOGIN PARA USUÁRIOS DE DOMÍNIO

Por padrão, o controle de acesso do lado do domínio é aplicado, o que significa que as políticas de login para usuários do Active Directory (AD) são definidas no próprio domínio AD. Este comportamento padrão pode ser substituído para que seja utilizado o controle de acesso do lado do cliente. Com o controle de acesso do lado do cliente, a permissão de login é definida apenas pelas políticas locais.

Se um domínio aplica o controle de acesso do lado do cliente, você pode usar o **realmd** para configurar regras básicas de permissão ou negação de acesso para usuários daquele domínio.

NOTA

As regras de acesso permitem ou negam o acesso a todos os serviços do sistema. Regras de acesso mais específicas devem ser definidas em um recurso específico do sistema ou no domínio.

3.3.1. Permitindo o acesso a usuários dentro de um domínio

Esta seção descreve como permitir o acesso a usuários dentro de um domínio.

IMPORTANTE

É mais seguro permitir o acesso apenas a usuários ou grupos específicos do que negar o acesso a alguns, ao mesmo tempo em que permite o acesso a todos os outros. Portanto, não é recomendável permitir o acesso a todos por padrão, negando-o apenas a usuários específicos com permissão do reino -x. Ao invés disso, a Red Hat recomenda manter uma política default de não acesso para todos os usuários e conceder acesso somente a usuários selecionados usando a permissão do reino.

Pré-requisitos

- Seu sistema RHEL é um membro do domínio do Active Directory.

Procedimento

1. Conceder acesso a todos os usuários:

```
# licença do reino -- tudo
```

2. Conceder acesso a usuários específicos:

```
$ realm permit aduser01@example.com
$ realm permit 'AD.EXAMPLE.COM\aduser01'
```

Atualmente, você só pode permitir o acesso a usuários em domínios primários e não a usuários em domínios confiáveis. Isto se deve ao fato de que o login do usuário deve conter o nome do domínio e o SSSD não pode atualmente fornecer informações sobre os domínios infantis disponíveis em **realmd**.

Etapas de verificação

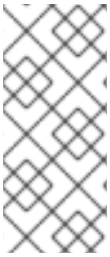
1. Use SSH para entrar no servidor como o usuário aduser01@example.com:

```
$ ssh aduser01@example.com@server_name
[aduser01@example.com@server_name ~]$
```

2. Use o comando ssh uma segunda vez para acessar o mesmo servidor, desta vez como o usuário aduser02@example.com:

```
$ ssh aduser02@example.com@server_name
Authentication failed.
```

Observe como o **aduser02@example.com** é negado o acesso ao sistema. Você concedeu a permissão para entrar no sistema somente ao usuário do aduser01@example.com. Todos os outros usuários desse domínio do Active Directory são rejeitados por causa da política de login especificada.



NOTA

Se você definir **use_fully_qualified_names** como verdadeiro no arquivo **sssd.conf**, todas as solicitações devem usar o nome de domínio totalmente qualificado. Entretanto, se você definir **use_fully_qualified_names** como falso, é possível usar o nome totalmente qualificado nas solicitações, mas somente a versão simplificada é exibida na saída.

Recursos adicionais

- Veja a página de manual **realm(8)**`.

3.3.2. Negação de acesso a usuários dentro de um domínio

Esta seção descreve como negar o acesso a todos os usuários dentro de um domínio.

IMPORTANTE

É mais seguro permitir o acesso apenas a usuários ou grupos específicos do que negar o acesso a alguns, ao mesmo tempo em que permite o acesso a todos os outros. Portanto, não é recomendável permitir o acesso a todos por padrão, negando-o apenas a usuários específicos com permissão do reino -x. Ao invés disso, a Red Hat recomenda manter uma política default de não acesso para todos os usuários e conceder acesso somente a usuários selecionados usando a permissão do reino.

Pré-requisitos

- Seu sistema RHEL é um membro do domínio do Active Directory.

Procedimento

1. Negar acesso a todos os usuários dentro do domínio:

```
# negar o reino... tudo
```

   Este comando impede que as contas **realm** entrem na máquina local. Use **realm permit** para restringir o login a contas específicas.

2. Verifique se o endereço **login-policy** do usuário do domínio está configurado para **deny-any-login**:

```
[root@replica1 ~]# realm list
example.net
  type: kerberos
  realm-name: EXAMPLE.NET
  domain-name: example.net
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
```

```
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common-tools
login-formats: %U@example.net
login-policy: deny-any-login
```

3. Negar acesso a usuários específicos, utilizando a opção -x:

```
Licença do reino -x 'AD.EXEMPLO.COM02aduser
```

Etapas de verificação

- Use SSH para entrar no servidor como o usuário **aduser01@example.net**.

```
$ ssh aduser01@example.net@server_name
Authentication failed.
```

NOTA

Se você definir **use_fully_qualified_names** como verdadeiro no arquivo **sssd.conf**, todas as solicitações devem usar o nome de domínio totalmente qualificado. Entretanto, se você definir **use_fully_qualified_names** como falso, é possível usar o nome totalmente qualificado nas solicitações, mas somente a versão simplificada é exibida na saída.

Recursos adicionais

- Veja a página de manual **realm(8)`**.

3.4. APLICANDO A POLÍTICA DE GRUPO CONTROLE DE ACESSO A OBJETOS NA RHEL

Um *Group Policy Object* (GPO) é uma coleção de configurações de controle de acesso armazenadas no Microsoft Active Directory (AD) que pode ser aplicado a computadores e usuários em um ambiente AD. Ao especificar GPOs no AD, os administradores podem definir políticas de login honradas tanto por clientes Windows quanto por hosts do Red Hat Enterprise Linux (RHEL) unidos ao AD.

As seções seguintes descrevem como você pode gerenciar GPOs em seu ambiente:

- Seção 3.4.1, “Como a SSSD interpreta as regras de controle de acesso do GPO”
- Seção 3.4.2, “Lista de configurações GPO que o SSSD suporta”
- Seção 3.4.3, “Lista de opções de SSSD para controlar a aplicação da GPO”
- Seção 3.4.4, “Mudando o modo de controle de acesso do GPO”
- Seção 3.4.5, “Criação e configuração de um GPO para um host RHEL na GUI AD”

3.4.1. Como a SSSD interpreta as regras de controle de acesso do GPO

Por padrão, o SSSD recupera objetos de política de grupo (GPOs) dos controladores de domínio do Active Directory (AD) e os avalia para determinar se um usuário tem permissão para fazer login em um host RHEL em particular juntado ao AD.

O SSSD mapeia o AD *Windows Logon Rights* para nomes de serviços do Módulo de Autenticação Plugável (PAM) para reforçar essas permissões em um ambiente GNU/Linux.

Como Administrador AD, você pode limitar o escopo das regras do GPO a usuários, grupos ou anfitriões específicos, listando-os em uma lista *security filter*.

3.4.1.1. Limitações à filtragem por hospedeiros

Versões mais antigas do SSSD não avaliam os hospedeiros nos filtros de segurança AD GPO.

- **RHEL 8.3.0 and newer:** SSSD suporta usuários, grupos e hosts em filtros de segurança.
- **RHEL versions older than 8.3.0:** O SSSD ignora as entradas do host e só suporta usuários e grupos em filtros de segurança.
  Para garantir que o SSSD aplique controle de acesso baseado em GPO a um host específico, crie uma nova Unidade Organizacional (OU) no domínio AD, mova o sistema para a nova OU e, em seguida, conecte a GPO a esta OU.

3.4.1.2. Limitações da filtragem por grupos

O SSSD atualmente não suporta os grupos incorporados no Active Directory, como **Administrators** com o Security Identifier (SID) **S-1-5-32-544**. A Red Hat recomenda contra o uso de grupos incorporados de AD nos GPOs AD direcionados aos hosts RHEL.

Recursos adicionais

- Para uma lista de opções GPO do Windows e suas opções SSSD correspondentes, consulte Lista de configurações GPO que o SSSD suporta .

3.4.2. Lista de configurações GPO que o SSSD suporta

A tabela a seguir mostra as opções SSSD que correspondem às opções do Active Directory GPO, conforme especificado no *Group Policy Management Editor* no Windows.

Tabela 3.1. Opções de controle de acesso GPO recuperadas pelo SSSD

Opção GPO	Opção correspondente **sssd.conf**
Permitir log on local Negar log on local	**ad_gpo_map_interactive**
Permitir logon através de Remote Desktop Services Negar logon através de Remote Desktop Services	**ad_gpo_map_remote_interactive**
Acessar este computador da rede Negar o acesso a este computador da rede	**ad_gpo_map_network**
Permitir logon como um trabalho em lote Negar logon como um trabalho em lote	**ad_gpo_map_batch**

Opção GPO	Opção correspondente **sssd.conf**
Permitir logon como um serviço Negar logon como um serviço	**ad_gpo_map_service**

- Para mais informações sobre estas configurações **sssd.conf**, como os serviços do Módulo de Autenticação Pluggable Authentication Module (PAM) que mapeiam as opções do GPO, consulte a entrada de página do manual **sssd-ad(5)**.

3.4.3. Lista de opções de SSSD para controlar a aplicação da GPO

3.4.3.1. A opção ad_gpo_access_control

Você pode definir a opção **ad_gpo_access_control** no arquivo **/etc/sssd/sssd.conf** para escolher entre três modos diferentes nos quais o controle de acesso baseado em GPO opera.

Tabela 3.2. Tabela de valores ad_gpo_access_control

Valor do ad_gpo_access_control	Comportamento
enforcing	As regras de controle de acesso baseadas em GPO são avaliadas e aplicadas. **This is the default setting in RHEL 8.**
permissive	As regras de controle de acesso baseadas em GPO são avaliadas, mas **not** é aplicado; uma mensagem **syslog** é registrada toda vez que o acesso seria negado. Esta é a configuração padrão no RHEL 7. Este modo é ideal para testar ajustes de políticas enquanto permite que os usuários continuem a fazer login.
disabled	As regras de controle de acesso baseadas em GPO não são avaliadas nem aplicadas.

3.4.3.2. A opção ad_gpo_implicit_deny

A opção **ad_gpo_implicit_deny** está configurada para **False** por padrão. Neste estado padrão, os usuários têm permissão de acesso se os GPOs aplicáveis não forem encontrados. Se você definir esta opção para **True**, você deve permitir explicitamente o acesso dos usuários com uma regra de GPO.

Você pode usar este recurso para endurecer a segurança, mas tenha cuidado para não negar o acesso involuntariamente. A Red Hat recomenda testar este recurso enquanto **ad_gpo_access_control** está configurado para **permissive**.

As duas tabelas a seguir ilustram quando um usuário tem permissão ou recusa de acesso com base na permissão e recusa de direitos de login definidos no lado do servidor AD e no valor de **ad_gpo_implicit_deny**.

Tabela 3.3. Comportamento de login com ad_gpo_implicit_deny set to False (default)

regras de permissão	regras de negação	resultado
em falta	em falta	todos os usuários são permitidos
em falta	presente	somente usuários que não estão nas regras de negação são permitidos
presente	em falta	somente usuários em regras de permissão são permitidos
presente	presente	somente usuários em regras de permissão e não em regras de negação são permitidos

Tabela 3.4. Comportamento de login com`ad_gpo_implicit_deny` set to`True`

regras de permissão	regras de negação	resultado
em falta	em falta	nenhum usuário é permitido
em falta	presente	nenhum usuário é permitido
presente	em falta	somente usuários em regras de permissão são permitidos
presente	presente	somente usuários em regras de permissão e não em regras de negação são permitidos

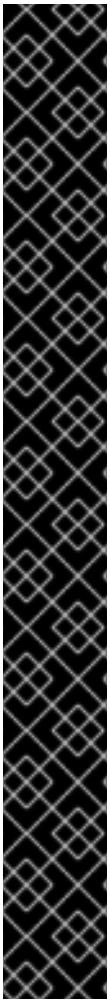
Recursos adicionais

- Para o procedimento para mudar o modo de aplicação da GPO no SSSD, consulte Mudando o modo de controle de acesso da GPO.
- Para obter mais detalhes sobre cada um dos diferentes modos de operação do GPO, consulte a entrada **ad_gpo_access_control** na página **sssd-ad(5)** do Manual.

3.4.4. Mudando o modo de controle de acesso do GPO

Este procedimento muda a forma como as regras de controle de acesso baseadas em GPO são avaliadas e aplicadas em um host RHEL unido a um ambiente Active Directory (AD).

Neste exemplo, você mudará o modo de operação do GPO de **enforcing** (o padrão) para **permissive** para fins de teste.



IMPORTANTE

Se você vir os seguintes erros, os usuários do Active Directory não poderão fazer login devido aos controles de acesso baseados em GPO:

- Em **/var/log/secure**:

```
Oct 31 03:00:13 client1 sshd[124914]: pam_sss(sshd:account): Access
denied for user aduser1: 6 (Permission denied)
Oct 31 03:00:13 client1 sshd[124914]: Failed password for aduser1 from
127.0.0.1 port 60509 ssh2
Oct 31 03:00:13 client1 sshd[124914]: fatal: Access denied for user aduser1
by PAM account configuration [preauth]
```

- Em **/var/log/sssd/sssd__example.com_.log**:

```
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]]
[ad_gpo_perform_hbac_processing] (0x0040): GPO access check failed:
[1432158236](Host Access Denied)
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_cse_done]
(0x0040): HBAC processing failed: [1432158236](Host Access Denied}
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_access_done]
(0x0040): GPO-based access control failed.
```

Se este for um comportamento indesejado, você pode definir temporariamente **ad_gpo_access_control** para **permissive**, como descrito neste procedimento, enquanto você resolve problemas com as configurações GPO adequadas no AD.

Pré-requisitos

- Você juntou um host RHEL a um ambiente AD usando SSSD.
- A edição do arquivo de configuração **/etc/sssd/sssd.conf** requer **root** permissões.

Procedimento

1. Parar o serviço SSSD.

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

2. Abra o arquivo **/etc/sssd/sssd.conf** em um editor de texto.
3. Defina **ad_gpo_access_control** para **permissive** na seção **domain** para o domínio AD.

```
[domain/example.com]
ad_gpo_access_control=permissive
...
```

4. Salvar o arquivo **/etc/sssd/sssd.conf**.
5. Reinicie o serviço SSSD para carregar as mudanças de configuração.

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

Recursos adicionais

- Para a lista de diferentes modos de controle de acesso GPO, consulte Lista de opções SSSD para controlar a aplicação do GPO.

3.4.5. Criação e configuração de um GPO para um host RHEL na GUI AD

O seguinte procedimento cria um Objeto de Política de Grupo (GPO) no Active Directory (AD) interface gráfica do usuário (GUI) para controlar o acesso de logon a um host RHEL.

Pré-requisitos

- Você juntou um host RHEL a um ambiente AD usando SSSD.
- Você tem privilégios de Administrador de AD para fazer mudanças no AD usando o GUI.

Procedimento

1. Dentro de **Active Directory Users and Computers**, crie uma Unidade Organizacional (OU) para se associar com o novo GPO:
   a. Clique com o botão direito do mouse sobre o domínio.
   b. Escolha **New**.
   c. Escolha **Organizational Unit**.
2. Clique no nome do objeto de computador que representa o host RHEL (criado quando ele entrou no Active Directory) e arraste-o para a nova OU. Ao ter o host RHEL em sua própria OU, o GPO visa este host.
3. Dentro do **Group Policy Management Editor**, crie um novo GPO para a OU que você criou:
   a. Expandir **Forest**.
   b. Expandir **Domains**.
   c. Expandir seu domínio.
   d. Clique com o botão direito do mouse sobre a nova OU.
   e. Escolha **Create a GPO in this domain**.
4. Especifique um nome para o novo GPO, tal como **Allow SSH access** ou **Allow Console/GUI access** e clique em **OK**.
5. Edite o novo GPO:
   a. Selecione a OU dentro do editor **Group Policy Management**.
   b. Clique com o botão direito do mouse e escolha **Edit**.
   c. Selecione **User Rights Assignment**.
   d. Selecione **Computer Configuration**
   e. Selecione **Policies**.

f. Selecione **Windows Settings**.

g. Selecione **Security Settings**.

h. Selecione **Local Policies**.

i. Selecione **User Rights Assignment**.

6. Atribuir permissões de login:

   a. Clique duas vezes em **Allow log on locally** para conceder acesso ao console local/GUI.

   b. Clique duas vezes em **Allow log on through Remote Desktop Services** para conceder acesso ao SSH.

7. Adicione o(s) usuário(s) que você gostaria de acessar qualquer uma destas políticas às próprias políticas:

   a. Clique em **Add User or Group**.

   b. Digite o nome de usuário dentro do campo em branco.

   c. Clique em **OK**.

Recursos adicionais

- Para mais detalhes sobre Objetos de Política de Grupo, consulte Objetos de Política de Grupo na documentação da Microsoft.

3.4.6. Recursos adicionais

- Para mais informações sobre como unir um host RHEL a um ambiente Active Directory, consulte Conectando os sistemas RHEL diretamente ao AD usando SSSD