Red Hat Enterprise Linux 8

Configurando a autenticação e autorização na RHEL

Usando SSSD, authselect, e sssctl para configurar a autenticação e autorização

Last Updated: 2021-03-04

Red Hat Enterprise Linux 8 Configurando a autenticação e autorização na RHEL

Usando SSSD, authselect, e sssctl para configurar a autenticação e autorização

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 configurar a autenticação e autorização em um host Red Hat Enterprise Linux 8.

Índice

TORNANDO O CÓDIGO ABERTO MAIS INCLUSIVO 3

FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT 4

CAPÍTULO 1. CONFIGURANDO A AUTENTICAÇÃO DO USUÁRIO USANDO O AUTHSELECT 5
1.1. O QUE É AUTHSELECT USADO PARA 5
1.1.1. Arquivos e diretórios que a authselect modifica 5
1.1.2. Fornecedores de dados em /etc/nsswitch.conf 6
1.2. ESCOLHENDO UM PERFIL AUTHSELECT 7
1.3. MODIFICANDO UM PERFIL AUTO-SELECIONADO PRONTO 8
1.4. CRIANDO E IMPLANTANDO SEU PRÓPRIO PERFIL AUTHSELECT 9
Exemplo 10
1.5. CONVERTENDO SEUS SCRIPTS DE AUTHCONFIG PARA AUTHSELECT 10

CAPÍTULO 2. ENTENDENDO O SSSD E SEUS BENEFÍCIOS 13
2.1. COMO FUNCIONA O SSSD 13
2.2. BENEFÍCIOS DO USO DO SSSD 13
2.3. MÚLTIPLOS ARQUIVOS DE CONFIGURAÇÃO SSSD POR CLIENTE 14
Como o SSSD processa os arquivos de configuração 14
2.4. FORNECEDORES DE IDENTIDADE E AUTENTICAÇÃO PARA SSSD 14
Provedores de Identidade e Autenticação como domínios SSSD 14
Provedores de Proxy 15
Combinações disponíveis de Provedores de Identidade e Autenticação 15

CAPÍTULO 3. CONFIGURAÇÃO DO SSSD PARA USAR O LDAP E EXIGIR AUTENTICAÇÃO TLS 17
3.1. UM CLIENTE OPENLDAP USANDO SSSD PARA RECUPERAR DADOS DO LDAP DE UMA FORMA CRIPTOGRAFADA 17
3.2. CONFIGURAÇÃO DO SSSD PARA USAR O LDAP E EXIGIR AUTENTICAÇÃO TLS 17

CAPÍTULO 4. CONFIGURANDO A RHEL PARA USAR O AD COMO UM PROVEDOR DE AUTENTICAÇÃO 20
4.1. UM HOST RHEL AUTÔNOMO USANDO O AD COMO UM FORNECEDOR DE AUTENTICAÇÃO 20
4.2. CONFIGURAÇÃO DE UM HOST RHEL PARA USAR O AD COMO UM PROVEDOR DE AUTENTICAÇÃO 20

CAPÍTULO 5. RELATÓRIOS SOBRE O ACESSO DE USUÁRIOS EM HOSTS QUE UTILIZAM SSSD 24
5.1. O COMANDO SSSCTL 24
5.2. GERAÇÃO DE RELATÓRIOS DE CONTROLE DE ACESSO USANDO SSSCTL 24
5.3. EXIBIÇÃO DOS DETALHES DA AUTORIZAÇÃO DO USUÁRIO USANDO SSSCTL 25

CAPÍTULO 6. CONSULTA DE INFORMAÇÕES DE DOMÍNIO USANDO SSSD 27
6.1. LISTAGEM DE DOMÍNIOS USANDO SSSCTL 27
6.2. VERIFICAÇÃO DO STATUS DO DOMÍNIO USANDO SSSCTL 27

CAPÍTULO 7. ELIMINAÇÃO DE ERROS TIPOGRÁFICOS NA CONFIGURAÇÃO LOCAL DO SSSD 29

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. CONFIGURANDO A AUTENTICAÇÃO DO USUÁRIO USANDO O AUTHSELECT

1.1. O QUE É AUTHSELECT USADO PARA

Você pode usar o utilitário **authselect** para configurar a autenticação do usuário em um host Red Hat Enterprise Linux 8.

Você pode configurar informações de identidade e fontes e fornecedores de autenticação selecionando um dos perfis prontos para uso:

- O perfil padrão **sssd** habilita o Daemon System Security Services (SSSD) para sistemas que utilizam autenticação LDAP.
- O perfil **winbind** permite o utilitário Winbind para sistemas integrados diretamente com o Microsoft Active Directory.
- O perfil **nis** garante a compatibilidade com os sistemas herdados do Network Information Service (NIS).
- O perfil **minimal** atende apenas usuários e grupos locais diretamente dos arquivos do sistema, o que permite aos administradores remover serviços de autenticação de rede que não são mais necessários.

Após selecionar um perfil **authselect** para um determinado host, o perfil é aplicado a cada usuário que faz login no host.

A Red Hat recomenda usar **authselect** em ambientes semi-centralizados de gerenciamento de identidade, por exemplo, se sua organização utiliza LDAP, Winbind, ou bancos de dados NIS para autenticar usuários para usar serviços em seu domínio.

ATENÇÃO

Não use **authselect** se seu host fizer parte do Red Hat Enterprise Linux Identity Management (IdM). Unir seu host a um domínio IdM com o comando **ipa-client-install** configura automaticamente a autenticação SSSD em seu host.

Da mesma forma, não utilize **authselect** se seu host fizer parte do Active Directory via SSSD. Chamando o comando **realm join** para unir seu host a um domínio Active Directory, configura automaticamente a autenticação SSSD em seu host.

1.1.1. Arquivos e diretórios que a authselect modifica

O utilitário **authconfig**, usado nas versões anteriores do Red Hat Enterprise Linux, criou e modificou muitos arquivos de configuração diferentes, tornando a solução de problemas mais difícil. **Authselect** simplifica os testes e a solução de problemas porque modifica apenas os seguintes arquivos e diretórios:

/etc/nsswitch.conf	A Biblioteca GNU C e outras aplicações usam este arquivo de configuração do Name Service Switch (NSS) para determinar as fontes das quais se obtêm informações sobre os serviços de nomes em uma gama de categorias, e em que ordem. Cada categoria de informação é identificada por um nome de banco de dados.
/etc/pam.d/* arquivos	Linux-PAM (Pluggable Authentication Modules) é um sistema de módulos que manipulam as tarefas de autenticação de aplicações (serviços) no sistema. A natureza da autenticação é dinamicamente configurável: o administrador do sistema pode escolher como aplicações individuais de prestação de serviços irão autenticar usuários. Os arquivos de configuração no diretório **/etc/pam.d/** listam os PAMs que executarão as tarefas de autenticação exigidas por um serviço, e o comportamento apropriado do PAM-API no caso de falha dos PAMs individuais. Entre outras coisas, estes arquivos contêm informações sobre: • condições de bloqueio da senha do usuário • a capacidade de autenticar com um cartão inteligente • a capacidade de autenticar com um leitor de impressão digital
/etc/dconf/db/distro.d/* arquivos	Este diretório contém perfis de configuração para o utilitário **dconf**, que você pode usar para gerenciar as configurações para a Interface Gráfica do Usuário (GUI) do GNOME.

1.1.2. Fornecedores de dados em /etc/nsswitch.conf

O perfil padrão **sssd** estabelece o SSSD como uma fonte de informação, criando **sss** entradas em **/etc/nsswitch.conf**:

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

Isto significa que o sistema procura primeiro no SSSD se forem solicitadas informações relativas a um desses itens:

- **passwd** para informações do usuário
- **group** para informações sobre grupos de usuários
- **netgroup** para NIS **netgroup** informações
- **automount** para informações sobre a montagem automática NFS

- **services** para informações sobre serviços

Somente se as informações solicitadas não forem encontradas no cache **sssd** e no servidor que fornece a autenticação, ou se **sssd** não estiver em execução, o sistema analisa os arquivos locais, ou seja **/etc/***.

Por exemplo, se for solicitada informação sobre um ID de usuário, o ID de usuário é primeiro pesquisado no cache **sssd**. Se não for encontrado lá, o arquivo **/etc/passwd** é consultado. Analogicamente, se for solicitada a afiliação de um grupo de usuários, ele é procurado primeiro no cache **sssd** e somente se não for encontrado lá, o arquivo **/etc/group** é consultado.

Na prática, o banco de dados local **files** normalmente não é consultado. A exceção mais importante é o caso do usuário **root**, que nunca é tratado por **sssd**, mas por **files**.

1.2. ESCOLHENDO UM PERFIL AUTHSELECT

Como administrador do sistema, você pode selecionar um perfil para o utilitário **authselect** para um host específico. O perfil será aplicado a cada usuário que fizer login no host.

Pré-requisitos

- Você precisa de **root** credenciais para executar **authselect** comandos

Procedimento

- Selecione o perfil **authselect** que é apropriado para seu provedor de autenticação. Por exemplo, para entrar na rede de uma empresa que usa LDAP, escolha **sssd**.

```
# authselect select sssd
```

  - (Opcional) Você pode modificar as configurações de perfil padrão adicionando as seguintes opções ao comando **authselect select sssd** ou **authselect select winbind**, por exemplo:
    - **with-faillock**
    - **with-smartcard**
    - **with-fingerprint**

  Para ver a lista completa das opções disponíveis, consulte Seção 1.5, “Convertendo seus scripts de **authconfig** para **authselect**” ou a página de manual **authselect-migration(7)**.

NOTA

Certifique-se de que os arquivos de configuração que são relevantes para seu perfil estejam configurados corretamente antes de concluir o procedimento **authselect select**. Por exemplo, se o daemon **sssd** não estiver configurado corretamente e ativo, a execução de **authselect select** faz com que somente usuários locais possam se autenticar, usando **pam_unix**.

Passos de verificação

1. Verifique se **sss** entradas para SSSD estão presentes em **/etc/nsswitch.conf**:

```
passwd:     sss files
```

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

2. Reveja o conteúdo do arquivo **/etc/pam.d/system-auth** para ver as entradas em **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 adicionais

- Para uma lista de perfis prontos **authselect**, ver Seção 1.1, “O que é authselect usado para” .
- Se o ajuste de um perfil pronto, adicionando uma das opções de linha de comando **authselect select** descritas acima, não for suficiente para seu caso de uso, você pode:
  - modificar um perfil pronto, alterando o arquivo **/etc/authselect/user-nsswitch.conf**. Para maiores detalhes, ver Seção 1.3, “Modificando um perfil auto-selecionado pronto” .
  - criar seu próprio perfil personalizado. Para maiores detalhes, veja Seção 1.4, “Criando e implantando seu próprio perfil authselect”.

1.3. MODIFICANDO UM PERFIL AUTO-SELECIONADO PRONTO

Como administrador do sistema, você pode modificar um dos perfis padrão para atender às suas necessidades.

Você pode modificar qualquer um dos itens do arquivo **/etc/authselect/user-nsswitch.conf**, com exceção de:

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

A execução de **authselect select profile_name** posteriormente resultará na transferência de alterações permitidas de **/etc/authselect/user-nsswitch.conf** para o arquivo **/etc/nsswitch.conf**. Alterações inaceitáveis são sobrescritas pela configuração padrão do perfil.

IMPORTANTE

Não modifique o arquivo **/etc/nsswitch.conf** diretamente.

Procedimento

1. Selecione um perfil em **authselect**, por exemplo:

```
# authselect select sssd
```

2. Edite o arquivo **/etc/authselect/user-nsswitch.conf** com as mudanças desejadas.

3. Aplique as mudanças do arquivo **/etc/authselect/user-nsswitch.conf**:

```
# authselect apply-changes
```

Etapas de verificação

- Revise o arquivo **/etc/nsswitch.conf** para verificar se as mudanças de **/etc/authselect/user-nsswitch.conf** foram propagadas ali.

Recursos adicionais

- Para uma lista de perfis prontos **authselect**, ver Seção 1.1, “O que é authselect usado para” .

1.4. CRIANDO E IMPLANTANDO SEU PRÓPRIO PERFIL AUTHSELECT

Como administrador do sistema, você pode criar e implantar um perfil personalizado, fazendo uma cópia personalizada de um dos perfis padrão.

Isto é particularmente útil se Seção 1.3, “Modificando um perfil auto-selecionado pronto” não for suficiente para suas necessidades. Quando você implanta um perfil personalizado, o perfil é aplicado a cada usuário que faz login no host em questão.

Procedimento

1. Crie seu perfil personalizado usando o comando **authselect create-profile**. Por exemplo, para criar um perfil personalizado chamado **user-profile** com base no perfil pronto **sssd** mas no qual você mesmo pode configurar os itens no arquivo **/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 a opção **--symlink-pam** no comando significa que os modelos PAM serão links simbólicos para os arquivos de perfil de origem ao invés de sua cópia; incluir a opção **--symlink-meta** significa que os meta arquivos, tais como README e REQUIREMENTS serão links simbólicos para os arquivos de perfil de origem ao invés de sua cópia. Isto assegura que todas as futuras atualizações dos modelos PAM e meta files no perfil original serão refletidas em seu perfil personalizado, também.

O comando cria uma cópia do arquivo **/etc/nsswitch.conf** no diretório **/etc/authselect/custom/user-profile/**.

2. Configure o arquivo **/etc/authselect/custom/user-profile/nsswitch.conf**.

3. Selecione o perfil personalizado executando o comando **authselect select**, e adicionando **custom/*name_of_the_profile*** como um parâmetro. Por exemplo, para selecionar o perfil **user-profile**:

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

A seleção do perfil **user-profile** para sua máquina significa que se o perfil **sssd** for posteriormente atualizado pela Red Hat, você se beneficiará de todas as atualizações, com exceção das atualizações feitas no arquivo **/etc/nsswitch.conf**.

Exemplo

O procedimento a seguir mostra como criar um perfil baseado no perfil **sssd** que só consulta a tabela estática local de busca de nomes de hosts no arquivo **/etc/hosts**, e não nos bancos de dados **dns** ou **myhostname**.

1. Edite o arquivo **/etc/nsswitch.conf** editando a seguinte linha:

```
hosts:      files
```

2. Criar um perfil personalizado baseado em **sssd** que exclui mudanças para **/etc/nsswitch.conf**:

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

3. Selecione o perfil:

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

4. Opcionalmente, verifique se a seleção do perfil personalizado tem

   - criou o arquivo **/etc/pam.d/system-auth** de acordo com o perfil escolhido **sssd**
   - deixou a configuração no site **/etc/nsswitch.conf** inalterada:

```
hosts:      files
```

NOTA

A execução do **authselect select sssd** , em contraste, resultaria em

```
hosts:      files dns myhostname
```

Recursos adicionais

- Para uma lista de perfis prontos **authselect**, ver Seção 1.1, “O que é authselect usado para” .

1.5. CONVERTENDO SEUS SCRIPTS DE AUTHCONFIG PARA AUTHSELECT

Se você usa **ipa-client-install** ou **realm join** para entrar em um domínio, você pode remover com

segurança qualquer chamada **authconfig** em seus scripts. Se isso não for possível, substitua cada chamada **authconfig** por sua chamada **authselect** equivalente. Ao fazer isso, selecione o perfil correto e as opções apropriadas. Além disso, edite os arquivos de configuração necessários:

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

Arelação das opções authconfig com as opções authselect profiles e Authselect profile options equivalentes das opções authconfig mostram o equivalente em **authselect** das opções **authconfig**.

Tabela 1.1. Relação das opções de authconfig para authselecionar perfis

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

Tabela 1.2. Opções de perfil authselect equivalentes a opções 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**

Tabela 1.3, “Exemplos de comandos authselect equivalentes aos comandos authconfig” mostra exemplos de transformações de chamadas Kickstart para **authconfig** em chamadas Kickstart para **authselect**.

Tabela 1.3. Exemplos de comandos authselect equivalentes aos 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. ENTENDENDO O SSSD E SEUS BENEFÍCIOS

2.1. COMO FUNCIONA O SSSD

O System Security Services Daemon (SSSD) é um serviço de sistema que permite o acesso a diretórios remotos e mecanismos de autenticação. Você pode conectar um sistema local, um SSSD *client*, a um sistema back-end externo, um *provider*, por exemplo:

- Um diretório LDAP
- Um domínio de Gerenciamento de Identidade (IdM)
- Um domínio do Active Directory (AD)
- Um reino de Kerberos

O SSSD funciona em duas etapas:

1. Ele conecta o cliente a um fornecedor remoto para recuperar informações de identidade e autenticação.
2. Ele usa as informações de autenticação obtidas para criar um cache local de usuários e credenciais sobre o cliente.

Os usuários no sistema local são então capazes de autenticar usando as contas de usuário armazenadas no provedor remoto.

O SSSD não cria contas de usuário no sistema local. No entanto, o SSSD pode ser configurado para criar diretórios domésticos para usuários do IdM. Uma vez criado, um diretório home do usuário IdM e seu conteúdo no cliente não são excluídos quando o usuário sai do sistema.

Figura 2.1. Como funciona o SSSD

O SSSD também pode fornecer caches para vários serviços de sistema, tais como Name Service Switch (NSS) ou Pluggable Authentication Modules (PAM).

2.2. BENEFÍCIOS DO USO DO SSSD

O uso do System Security Services Daemon (SSSD) oferece múltiplos benefícios em relação à recuperação da identidade do usuário e autenticação do usuário.

Autenticação off-line

O SSSD opcionalmente mantém um cache de identidades de usuários e credenciais recuperadas de provedores remotos. Nesta configuração, um usuário - desde que já tenha se autenticado uma vez

contra o provedor remoto no início da sessão - pode autenticar com sucesso os recursos mesmo que o provedor remoto ou o cliente estejam offline.

Uma única conta de usuário: maior consistência do processo de autenticação

Com SSSD, não é necessário manter tanto uma conta central quanto uma conta de usuário local para autenticação offline. As condições são:

- Em uma determinada sessão, o usuário deve ter feito o login pelo menos uma vez: o cliente deve estar conectado ao provedor remoto quando o usuário faz o login pela primeira vez.

- O cache deve ser ativado no SSSD.
  Sem SSSD, os usuários remotos muitas vezes têm múltiplas contas de usuário. Por exemplo, para se conectar a uma rede privada virtual (VPN), os usuários remotos têm uma conta para o sistema local e outra conta para o sistema VPN. Neste cenário, é necessário primeiro autenticar-se na rede privada para buscar o usuário no servidor remoto e fazer o cache das credenciais do usuário localmente.

  Com SSSD, graças ao cache e à autenticação offline, os usuários remotos podem se conectar aos recursos da rede simplesmente autenticando em sua máquina local. O SSSD então mantém suas credenciais de rede.

Redução da carga sobre os fornecedores de identidade e autenticação

Ao solicitar informações, os clientes verificam primeiro o cache SSSD local. O SSSD entra em contato com os provedores remotos somente se as informações não estiverem disponíveis no cache.

2.3. MÚLTIPLOS ARQUIVOS DE CONFIGURAÇÃO SSSD POR CLIENTE

O arquivo de configuração padrão para SSSD é **/etc/sssd/sssd.conf**. Além deste arquivo, o SSSD pode ler sua configuração em todos os arquivos ***.conf** no diretório **/etc/sssd/conf.d/**.

Esta combinação permite utilizar o arquivo padrão **/etc/sssd/sssd.conf** em todos os clientes e adicionar configurações adicionais em outros arquivos de configuração para ampliar a funcionalidade individualmente por cliente.

Como o SSSD processa os arquivos de configuração

O SSSD lê os arquivos de configuração nesta ordem:

1. O arquivo principal **/etc/sssd/sssd.conf**

2. Outros ***.conf** arquivos em **/etc/sssd/conf.d/**, em ordem alfabética

Se o mesmo parâmetro aparecer em vários arquivos de configuração, o SSSD usa o último parâmetro lido.

NOTA

O SSSD não lê arquivos ocultos (arquivos que começam com **.**) no diretório **conf.d**.

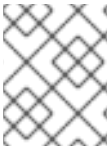
2.4. FORNECEDORES DE IDENTIDADE E AUTENTICAÇÃO PARA SSSD

Provedores de Identidade e Autenticação como domínios SSSD

Os provedores de identidade e autenticação são configurados como *domains* no arquivo de configuração do SSSD, **/etc/sssd/sssd.conf**. Os provedores estão listados no arquivo de **[domain/*name of the domain*]** ou **[domain/default]** seção do arquivo.

Um único domínio pode ser configurado como um dos seguintes provedores:

- Um *identity provider*, que fornece informações para o usuário, como UID e GID.
  - Especifique um domínio como o *identity provider* usando a opção **id_provider** no **[domain/*name of the domain*]** seção do arquivo **/etc/sssd/sssd.conf**.
- Um *authentication provider*, que trata dos pedidos de autenticação.
  - Especifique um domínio como o *authentication provider* usando a opção **auth_provider** no **[domain/*name of the domain*]** seção do site **/etc/sssd/sssd.conf**.
- Um *access control provider*, que trata dos pedidos de autorização.
  - Especifique um domínio como o *access control provider* usando a opção **access_provider** no **[domain/*name of the domain*]** seção do site **/etc/sssd/sssd.conf**. Por padrão, a opção está definida para **permit**, que sempre permite todo o acesso. Veja a página de manual **sssd.conf**(5) para detalhes.
- Uma combinação desses fornecedores, por exemplo, se todas as operações correspondentes forem realizadas dentro de um único servidor.
  - Neste caso, as opções **id_provider**, **auth_provider**, e **access_provider** estão todas listadas no mesmo **[domain/*name of the domain*]** ou **[domain/default]** seção de **/etc/sssd/sssd.conf**.



NOTA

Você pode configurar vários domínios para SSSD. Você deve configurar pelo menos um domínio, caso contrário o SSSD não será iniciado.

Provedores de Proxy

Um provedor proxy trabalha como um relé intermediário entre o SSSD e os recursos que, de outra forma, o SSSD não seria capaz de utilizar. Ao usar um provedor proxy, o SSSD se conecta ao serviço proxy, e o proxy carrega as bibliotecas especificadas.

Você pode configurar o SSSD para usar um provedor proxy a fim de habilitar:

- Métodos alternativos de autenticação, como um leitor de impressões digitais
- Sistemas herdados, como o NIS
- Uma conta de sistema local definida no arquivo **/etc/passwd** como um provedor de identidade e um provedor de autenticação remota, por exemplo, Kerberos

Combinações disponíveis de Provedores de Identidade e Autenticação

Você pode configurar o SSSD para usar as seguintes combinações de provedores de identidade e autenticação.

Tabela 2.1. Combinações disponíveis de Provedores de Identidade e Autenticação

Provedor de Identidade	Provedor de Autenticação
Gestão da Identidade [a]	Gestão da Identidade

Provedor de Identidade	Provedor de Autenticação
Active Directory	Active Directory
LDAP	LDAP
LDAP	Kerberos
Proxy	Proxy
Proxy	LDAP
Proxy	Kerberos

[a] Uma extensão do tipo de fornecedor LDAP.

Recursos adicionais

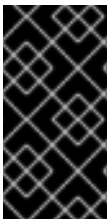
- Você pode configurar o SSSD usando o utilitário **authselect**. Para mais detalhes sobre o uso de **authselect**, veja Capítulo 1, *Configurando a autenticação do usuário usando o authselect* .
- Se seu host estiver registrado em Gerenciamento de Identidade (IdM) que está em um acordo de confiança com uma floresta do Active Directory (AD), você pode listar e verificar o status dos domínios usando o utilitário **sssctl**. Para mais detalhes, veja Capítulo 6, *Consulta de informações de domínio usando SSSD*.
- Você pode usar o utilitário **sssctl** para criar relatórios de controle de acesso e exibir os dados do usuário. Para mais detalhes, veja Capítulo 5, *Relatórios sobre o acesso de usuários em hosts que utilizam SSSD*.

CAPÍTULO 3. CONFIGURAÇÃO DO SSSD PARA USAR O LDAP E EXIGIR AUTENTICAÇÃO TLS

3.1. UM CLIENTE OPENLDAP USANDO SSSD PARA RECUPERAR DADOS DO LDAP DE UMA FORMA CRIPTOGRAFADA

O Daemon System Security Services (SSSD) é um daemon que gerencia a recuperação e autenticação de dados de identidade em um host RHEL 8. Um administrador de sistema pode configurar o SSSD no host para usar um banco de dados de servidor LDAP autônomo como banco de dados de conta de usuário. Exemplos de um servidor LDAP incluem o servidor OpenLDAP e o Red Hat Directory Server. Neste capítulo, o cenário também inclui a exigência de que a conexão com o servidor LDAP deve ser criptografada com um certificado TLS.

O método de autenticação dos objetos LDAP pode ser ou uma senha Kerberos ou uma senha LDAP. Note que as questões de autenticação e autorização dos objetos LDAP não são abordadas neste capítulo.



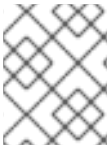
IMPORTANTE

A configuração do SSSD com LDAP é um procedimento complexo que requer um alto nível de especialização em SSSD e LDAP. Considere o uso de uma solução integrada e automatizada, como Active Directory ou Red Hat Identity Management (IdM). Para detalhes sobre IdM, consulte Planejamento de Gerenciamento de Identidade .

3.2. CONFIGURAÇÃO DO SSSD PARA USAR O LDAP E EXIGIR AUTENTICAÇÃO TLS

Complete este procedimento para configurar seu sistema Red Hat Enterprise Linux (RHEL) como um cliente OpenLDAP com a seguinte configuração de cliente:

- O sistema RHEL autentica os usuários armazenados em um banco de dados de contas de usuários OpenLDAP.
- O sistema RHEL usa o serviço System Security Services Daemon (SSSD) para recuperar os dados dos usuários.
- O sistema RHEL se comunica com o servidor OpenLDAP através de uma conexão criptografada em TLS.



NOTA

Alternativamente, você pode usar este procedimento para configurar seu sistema RHEL como cliente de um Red Hat Directory Server.

Pré-requisitos

- O servidor OpenLDAP é instalado e configurado com informações do usuário.
- Você tem permissões de root no host que você está configurando como cliente LDAP.
- No host que você está configurando como cliente LDAP, o arquivo **/etc/sssd/sssd.conf** foi criado e configurado para especificar **ldap** como o **autofs_provider** e o **id_provider**.

- Você tem uma cópia em formato PEM da cadeia de certificados de assinatura da CA raiz da Autoridade Certificadora que emitiu o certificado de servidor OpenLDAP, armazenada em um arquivo local chamado **core-dirsrv.ca.pem**.

Procedimento

1. Instalar os pacotes necessários:

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

2. Mude o fornecedor de autenticação para **sssd**:

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

3. Copie o arquivo **core-dirsrv.ca.pem** contendo a cadeia de certificados de assinatura da CA raiz da Autoridade Certificadora que emitiu o certificado SSL/TLS do servidor OpenLDAP para a pasta **/etc/openldap/certs**.

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

4. Adicione a URL e o sufixo do seu servidor LDAP ao arquivo **/etc/openldap/ldap.conf**:

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

5. No arquivo **/etc/openldap/ldap.conf**, adicione uma linha apontando o parâmetro TLS_CACERT para **/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. No arquivo **/etc/sssd/sssd.conf**, adicione seus valores ambientais aos parâmetros **ldap_uri** e **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. Em **/etc/sssd/sssd.conf**, especifique o requisito de autenticação TLS modificando os valores **ldap_tls_cacert** e **ldap_tls_reqcert** na seção **[domain]**:

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

8. Alterar as permissões no arquivo **/etc/sssd/sssd.conf**:

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

9. Reinicie e habilite o serviço SSSD e o daemon **oddjobd**:

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

10. (Opcional) Se seu servidor LDAP usa os protocolos obsoletos TLS 1.0 ou TLS 1.1, mude a política de criptografia do sistema do cliente para o nível LEGACY para permitir que a RHEL 8 se comunique usando estes protocolos:

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

Para mais detalhes, consulte a seção Funcionalidade Depreciada nas Notas de Lançamento RHEL 8.0.

Etapas de verificação

- Verifique se você pode recuperar dados do usuário de seu servidor LDAP usando o comando **id** e especificando um usuário LDAP:

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

O administrador do sistema pode agora consultar os usuários do LDAP usando o comando **id**. O comando retorna uma identificação correta do usuário e a adesão ao grupo.

Diretriz não resolvida em master.adoc - inclui::assemblies/assembly_sssd-client-side view.adoc[leveloffset= 1]

CAPÍTULO 4. CONFIGURANDO A RHEL PARA USAR O AD COMO UM PROVEDOR DE AUTENTICAÇÃO

4.1. UM HOST RHEL AUTÔNOMO USANDO O AD COMO UM FORNECEDOR DE AUTENTICAÇÃO

Como administrador de sistemas, você pode usar o Active Directory (AD) como fornecedor de autenticação para um host Red Hat Enterprise Linux (RHEL) sem entrar no host para o AD se, por exemplo:

- Você não quer conceder aos administradores AD o controle sobre a habilitação e desativação do host.
- O host, que pode ser um PC corporativo, destina-se apenas a ser usado por um usuário em sua empresa.

IMPORTANTE

Implementar este procedimento somente nos raros casos em que esta abordagem é preferida.

Em vez disso, considere a possibilidade de unir totalmente o sistema ao AD ou ao Red Hat Identity Management (IdM). Unir o host RHEL a um domínio torna a configuração mais fácil de gerenciar. Se você estiver preocupado com as licenças de acesso de clientes relacionadas à entrada de clientes diretamente no AD, considere a possibilidade de aproveitar um servidor IdM que esteja em um acordo de confiança com o AD. Para mais informações sobre uma confiança IdM-AD, consulte Planejando uma confiança entre IdM e AD e Instalando uma confiança entre IdM e AD .

4.2. CONFIGURAÇÃO DE UM HOST RHEL PARA USAR O AD COMO UM PROVEDOR DE AUTENTICAÇÃO

Complete este procedimento para permitir que o usuário **AD_user** faça o login no sistema **rhel8_host** usando a senha definida no banco de dados de usuários do Active Directory AD no domínio **example.com**. Neste exemplo, o domínio **EXAMPLE.COM** Kerberos corresponde ao domínio **example.com**.

Pré-requisitos

- Você tem acesso root a **rhel8_host**.
- A conta de usuário **AD_user** existe no domínio **example.com**.
- O reino de Kerberos é **EXAMPLE.COM**.
- **rhel8_host** não foi unido ao AD usando o comando **realm join**.

Procedimento

1. Criar a conta de usuário **AD_user** localmente sem atribuir uma senha a ela:

```
# useradd AD_user
```

2. Abra o arquivo **/etc/nsswitch.conf** para edição, e certifique-se de que ele contenha as seguintes linhas:

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

3. Abra o arquivo **/etc/krb5.conf** para edição, e certifique-se de que ele contenha as seguintes seções e itens:

```
# 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. Crie o arquivo **/etc/sssd/sssd.conf** e insira as seguintes seções e linhas nele:

```
[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. Alterar as permissões no arquivo **/etc/sssd/sssd.conf**:

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

6. Iniciar o Sistema de Serviços de Segurança Daemon (SSSD):

```
# systemctl start sssd
```

7. Habilitar o SSSD:

```
# systemctl habilita sssd
```

8. Abra o arquivo **/etc/pam.d/system-auth**, e modifique-o de modo que contenha as seguintes seções e linhas:

```
# 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 o conteúdo do arquivo **/etc/pam.d/system-auth** para o arquivo **/etc/pam.d/password-auth**. Digite **yes** para confirmar a sobregravação do conteúdo atual do arquivo:

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

Etapas de verificação

1. Solicite um bilhete de passagem de Kerberos (TGT) para **AD_user**. Digite a senha de **AD_user**, conforme solicitado:

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

2. Mostrar o TGT obtido:

```
# 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 fez login com sucesso em **rhel8_host** usando as credenciais do domínio **EXAMPLE.COM** Kerberos.

CAPÍTULO 5. RELATÓRIOS SOBRE O ACESSO DE USUÁRIOS EM HOSTS QUE UTILIZAM SSSD

O Daemon Security System Services (SSSD) rastreia quais usuários podem ou não acessar os clientes. Este capítulo descreve a criação de relatórios de controle de acesso e a exibição dos dados dos usuários usando a ferramenta **sssctl**.

Pré-requisitos

- Os pacotes SSSD são instalados em seu ambiente de rede.

5.1. O COMANDO SSSCTL

sssctl é uma ferramenta de linha de comando que utiliza o Daemon Security System Services (SSSD) para coletar informações sobre:

- estado de domínio
- autenticação do usuário cliente
- acesso do usuário em clientes de um determinado domínio
- informações sobre o conteúdo do cache

Com a ferramenta **sssctl**, você pode:

- gerenciar o cache SSSD
- gerenciar logs
- verificar arquivos de configuração

NOTA

A ferramenta **sssctl** substitui as ferramentas **sss_cache** e **sss_debuglevel**.

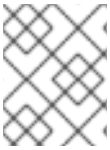
Recursos adicionais

- Para obter detalhes sobre **sssctl**, entre:

```
# ssctl --ajuda
```

5.2. GERAÇÃO DE RELATÓRIOS DE CONTROLE DE ACESSO USANDO SSSCTL

Você pode listar as regras de controle de acesso aplicadas à máquina na qual você está executando o relatório porque o SSSD controla quais usuários podem fazer o login no cliente.



NOTA

O relatório de acesso não é preciso porque a ferramenta não rastreia os usuários bloqueados pelo Key Distribution Center (KDC).

Pré-requisitos

- Você deve estar logado com privilégios de administrador
- O **sssctl** está disponível nos sistemas RHEL 7 e RHEL 8

Procedimento

- Para gerar um relatório para o domínio **idm.example.com**, entre:

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

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

5.3. EXIBIÇÃO DOS DETALHES DA AUTORIZAÇÃO DO USUÁRIO USANDO SSSCTL

O comando **sssctl user-checks** ajuda a depurar problemas em aplicações que utilizam o Daemon System Security Services (SSSD) para busca, autenticação e autorização de usuários.

O comando **sssctl user-checks [USER_NAME]** exibe os dados do usuário disponíveis através do Name Service Switch (NSS) e o InfoPipe respondedor para a interface D-Bus. Os dados exibidos mostram se o usuário está autorizado a fazer login usando o serviço **system-auth** Pluggable Authentication Module (PAM).

O comando tem duas opções:

- **-a** para uma ação do PAM
- **-s** para um serviço PAM

Se você não definir as opções **-a** e **-s**, a ferramenta **sssctl** utiliza as opções padrão: **-a acct -s system-auth**.

Pré-requisitos

- Você deve estar logado com privilégios de administrador
- A ferramenta **sssctl** está disponível nos sistemas RHEL 7 e RHEL 8

Procedimento

- Para exibir dados do usuário para um determinado usuário, digite:

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

Recursos adicionais

- Para obter detalhes em **sssctl user-checks**, use o seguinte comando:

```
sssctl user-checks --ajuda
```

CAPÍTULO 6. CONSULTA DE INFORMAÇÕES DE DOMÍNIO USANDO SSSD

A Security System Services Daemon (SSSD) pode listar domínios em Gerenciamento de Identidade (IdM), incluindo domínios do Active Directory na confiança entre florestas. Você também pode verificar o status de cada um dos domínios listados:

- Listagem de domínios usando o comando sssctl
- Verificando o status do domínio usando o comando sssctl

6.1. LISTAGEM DE DOMÍNIOS USANDO SSSCTL

O comando **sssctl domain-list** ajuda na depuração de problemas com a topologia do domínio.

NOTA

O status pode não estar disponível imediatamente. Se o domínio não for visível, repita o comando.

Pré-requisitos

- Você deve estar logado com privilégios de administrador
- O **sssctl** está disponível nos sistemas RHEL 7 e RHEL 8

Procedimento

1. Para exibir ajuda para o comando sssctl, entre:

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

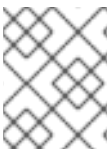
2. Para exibir uma lista de domínios disponíveis, entre:

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

A lista inclui domínios na confiança cruzada entre o Active Directory e a Gestão de Identidade.

6.2. VERIFICAÇÃO DO STATUS DO DOMÍNIO USANDO SSSCTL

O comando **sssctl domain-status** ajuda na depuração de problemas com a topologia do domínio.



NOTA

O status pode não estar disponível imediatamente. Se o domínio não for visível, repita o comando.

Pré-requisitos

- Você deve estar logado com privilégios de administrador
- O **sssctl** está disponível nos sistemas RHEL 7 e RHEL 8

Procedimento

1. Para exibir ajuda para o comando sssctl, entre:

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

2. Para exibir dados do usuário para um determinado domínio, digite:

```
[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
```

O domínio **idm.example.com** está online e visível do cliente onde você aplicou o comando.

Se o domínio não estiver disponível, o resultado é:

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

CAPÍTULO 7. ELIMINAÇÃO DE ERROS TIPOGRÁFICOS NA CONFIGURAÇÃO LOCAL DO SSSD

Você pode testar se o arquivo **/etc/sssd/sssd.conf** em seu host contém algum erro tipográfico usando o comando **sssctl config-check**.

Pré-requisitos

- Você está logado como raiz.

Procedimento

1. Digite o 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 o arquivo **/etc/sssd/sssd.conf** e corrija o erro de digitação. Se você, por exemplo, recebeu a mensagem de erro na etapa anterior, substitua **ldap_search** por **ldap_search_base**:

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

3. Salvar o arquivo.

4. Reinicie o SSSD:

```
# systemctl restart sssd
```

Etapas de verificação

- Digite o comando **sssctl config-check**:

```
# sssctl config-check

Issues identified by validators: 0

Messages generated during configuration merging: 0

Used configuration snippet files: 0
```

O arquivo **/etc/sssd/sssd.conf** agora não tem erros tipográficos.