Serviços de domínio

Capítulo destinado aos softwares provedores de serviços de domínio, como Samba e MS AD Directory Services

Cliente: Configuração do SSSD (controlador de domínio Samba4)

1. Introdução

O System Security Services Daemon é um pacote de software originalmente desenvolvido para o sistema operacional Linux que fornece um conjunto de daemons para gerenciar o acesso a diretórios remotos e mecanismos de autenticação. Funciona como um agregado de daemons que gerenciam mecanismos de autenticação remota, assim como serviços de diretórios que manipula diretamente o PAM e o NSS.

2. Obtendo os dados

Para que a configuração seja realizada com sucesso, **certifique-se de:**

- Ter acesso administrativo ao computador no qual o SSSD será instalado
- Saber a distribuição linux utilizada no computador no qual o SSSD será instalado
- Saber o nome do domínio
- Saber o(s) endereço(s) IP do(s) controlador(es) do domínio
- Possuir um arquivo com o certificado da CA utilizada pelo servidor
- Possuir os dados de usuário e senha utilizados pelo SSSD

3. Executando a configuração

Instale os pacotes necessários para o funcionamento do serviço do SSSD. A lista varia conforme a distribuição.

3.1. Instalação dos pacotes

3.1.a. No Debian/Ubuntu:

```
apt install -y sudo cracklib-runtime ldap-utils libbasicobjects0 libc-ares2 libcollection4 \
 libcrack2 libdhash1 libini-config5 libipa-hbac0 libldap-common libnl-3-200 libnl-route-3-200
```

```
\
 libldb1 libnspr4 libnss-sss libntdb1 libopts25 libpwquality-common libpwquality1 libpam-
pwquality \
 libpath-utils1 libpam-sss libsss-sudo libpython2.7 libref-array1 libsasl2-modules-gssapi-mit
\
 libnss3 libsss-idmap0 libtalloc2 libtdb1 libtevent0 libwbclient0 ntp python-sss python-talloc
\
 samba-libs sssd sssd-ad sssd-ad-common sssd-common sssd-ipa sssd-krb5 sssd-krb5-common sssd-
ldap\
 sssd-proxy krb5-config krb5-user libgssrpc4
```

3.1.b. No Centos:

```
yum install -y sudo sssd ntp openldap sssd-ldap pam_ldap pam_krb5 krb5-workstation
```

3.2. Configuração do sistema

3.2.1. Configuração do DNS

Para que os servidores utilizados por este serviço sejam resolvidos corretamente, defina as configurações de rede para **utilizar o IP do controlador de domínios como o servidor DNS primário do computador cliente** e o **nome do domínio ao qual o computador será ingressado no domínio a ser utilizado para buscas**.

Essa configuração pode ser realizada de formas diferentes. A forma recomendada difere de acordo com o sistemas operacional utilizado.

- No Debian/Ubuntu: Edite o arquivo **/etc/network/interfaces**
- No Centos: Utilize o comando `nmtui`

3.2.2. Certificado da CA utilizado pelo samba

A comunicação entre o cliente e o servidor samba utiliza TLS para proteger os dados. Utilizando esta técnica, o cliente usa um certificado para se autenticar com o servidor.

Crie o arquivo **/etc/ssl/private/sssd-ca.pem** contendo o certificado da CA utilizado pelo samba.

3.2.3. Criação automática da pasta do usuário

Uma vez que o SSSD tenha autenticado os usuários no domínio e tenham acesso ao sistema, a pasta do usuário não será criada automaticamente.

Para habilitar a criação automática da pasta do usuário, siga o procedimento:

3.2.3.a. No Debian/Ubuntu

Execute o seguinte comando no shell do computador

```
nano /etc/pam.d/common-session
```

Insira a linha a seguir após o primeiro bloco de comentários

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

3.2.3.b. No Centos

```
authconfig --update --enablesssd --enablesssdauth --enablemkhomedir
```

3.3. Configuração do sudo

Execute o comando a seguir no shell do computador cliente:

> Neste exemplo, aos membros do grupo chamado "EXEMPLO_SUDO", será permitido o uso do sudo. Substitua pelo grupo correto na hora da execução do comando

```
echo '%EXEMPLO_SUDO ALL=(ALL) ALL' > /etc/sudoers.d/ldap_sudo_group
chmod 0600 /etc/sudoers.d/ldap_sudo_group
```

O item iniciado por um símbolo de percentual (%EXEMPLO_SUDO) indica o nome do grupo que irá receber as permissões do sudo.

3.4. Configuração do kerberos

Cabe ao kerberos garantir a troca de chaves, de forma segura, entre os computadores de uma rede que o utilize. Para tal, é necessário configurar o cliente para se comunicar aos provedores deste serviço.

Execute o comando a seguir no shell do computador cliente:

```
nano /etc/krb5.conf
```

Deixe o arquivo conforme mostrado a seguir.

> Neste exemplo, o nome do domínio utilizado foi "EXEMPLO.LOCAL". Altere o nome para o domínio correto.

Neste exemplo, o FQDN do servidor controlador de domínio utilizado foi "DC01.EXEMPLO.LOCAL". Altere o nome para o FQDN correto.

```
[logging]
default = SYSLOG:NOTICE
default = FILE:/var/log/krb5.log

[libdefaults]
default_realm = DOMINIO.LOCAL

# MIT Kerberos Variables.
krb5_config = /etc/krb.conf
krb5_realms = /etc/krb.realms
default_keytab_name = /etc/krb5.keytab

dns_lookup_kdc = no
dns_lookup_realm = no
ticket_lifetime = 24h
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

[realms]
  DOMINIO.LOCAL= {
    kdc = DC01.DOMINIO.LOCAL
    admin_server = DC01.DOMINIO.LOCAL
    default_domain = DOMINIO.LOCAL
}

[domain_realm]
.ifpe.local = DOMINIO.LOCAL
```

3.5. Configuração do SSSD

O SSSD é o serviço que realiza a autenticação em si, se apoiando na resolução de nomes e nas facilidades oferecidas pelo kerberos.

3.5.1. O arquivo de configuração principal

Execute o comando a seguir no shell do computador cliente:

```
touch /etc/sssd/sssd.conf
chmod 600 /etc/sssd/sssd.conf
nano /etc/sssd/sssd.conf
```

Deixe o arquivo conforme mostrado a seguir.

Neste exemplo, o nome do domínio utilizado foi "EXEMPLO.LOCAL". Altere o nome para o domínio correto.

Neste exemplo, o FQDN do servidor controlador de domínio utilizado foi "DC01.EXEMPLO.LOCAL". Altere o nome para o FQDN correto.

Substitua "CN=USUARIO_SSSD,OU=SUB,DC=DOMINIO,DC=LOCAL" e "XXXXX_SENHA_DO_SSSD_XXXXX" pelo CN e senha corretos

```
[sssd]
debug_level = 7
reconnection_retries = 2

config_file_version = 2
sbus_timeout = 10
services = nss,pam
domains = DOMINIO.LOCAL

[nss]
debug_level = 7
reconnection_retries = 2

filter_users = root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy
override_homedir = /home/%u.%d
fallback_homedir = /home/%u
default_shell = /bin/bash

[pam]
debug_level = 7
reconnection_retries = 2

pam_verbosity = 2
pam_id_timeout = 15

offline_credentials_expiration = 2
offline_failed_login_attempts = 2
offline_failed_login_delay = 2

[domain/DOMINIO.LOCAL]
debug_level = 7
reconnection_retries = 2

enumerate = False
cache_credentials = True
entry_cache_timeout = 600

# access_provider = simple
access_provider = ldap
auth_provider = krb5
chpass_provider = krb5
id_provider = ldap

krb5_server = DC01.DOMINIO.LOCAL
krb5_realm = DOMINIO.LOCAL
krb5_store_password_if_offline = True
krb5_kpasswd = DC01.DOMINIO.LOCAL
krb5_renew_interval = 30m
krb5_renewable_lifetime = 7d

ldap_default_bind_dn = CN=USUARIO_SSSD,OU=SUB,DC=DOMINIO,DC=LOCAL
ldap_default_authtok = XXXXX_SENHA_DO_SSSD_XXXXX
ldap_group_object_class = group
ldap_id_mapping = True
ldap_id_use_start_tls = True
ldap_network_timeout = 5
ldap_referrals = False
ldap_schema = ad
ldap_search_base = DC=DOMINIO,DC=LOCAL
ldap_sudo_search_base = DC=DOMINIO,DC=LOCAL
ldap_tls_reqcert = never
ldap_tls_cacert = /etc/ssl/private/sssd-ca.pem
```

3.5.2. Controlando a execução do serviço

```
systemctl enable sssd # Ativa o início automático do serviço após o boot
systemctl start sssd # Inicia o serviço imediatamente
```