Samba4とSSSDでLinux/Windowsの認証統合環境を構築(ActiveDirectory+NIS)

公開日:2016年11月13日
参照数: 28875

Samba4ではActiveDirecotryが構築できるようになり、またCentOS6からは新しい認証サービスとしてSystem Security Services Daemon (SSSD)が導入されたため、WindowsとLinuxのユーザ管理が非常に簡単にできるようになりました。

今回は、Samba4とCentOS7を利用して、WindowsとLinuxの認証統合環境を構築します。

ざっくり要件をまとめると、

- WindowsとLinuxのユーザID/パスワードをActiveDirecotry で一元管理
- Windows/Linuxどちらにも同じユーザID/パスワードでログインできる
- Linuxのホームディレクトリに Windowsからアクセスできる
- ドメインコントローラにファイルサーバを共存させる
- ユーザはドメインコントローラにsssd経由でログインできる

です。構成環境は下記を想定します。

- ドメイン名　　：TESTDOMAIN.LOCAL
- ドメインコントローラ　：dc01.testdomain.local
- ドメインコントローラIP ：192.168.24.57

ドメインコントローラの冗長化は次回解説します。

ではさっそく構築に移ります。

1. 不要な機能の停止

構築時のエラーを防ぐため、ファイアーウォールの停止とSELinuxを無効化します。

```
# systemctl stop firewalld.service
# systemctl disable firewalld.service
# systemctl list-unit-files | grep firewalld.service
firewalld.service                           disabled

# getenforce
Enforcing
# vi /etc/selinux/config

<略>
#SELINUX=enforcing                # コメントアウト
SELINUX=disabled                  # 追記
<略>

# reboot
# getenforce
Disabled
```

2. hostsファイルの編集

hostsファイルに自ホストの完全修飾ドメイン名（FQDN）と短いホスト名を追記します。

```
# vi /etc/hosts

127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.24.57   dc01.testdomain.local dc01              # 追記
```

3. 必要なパッケージのインストール

ディストリビューションにあわせて必要なパッケージをインストールします。

今回の環境はCentOS7なので下記になりますが、その他ディストリビューションの場合はこちら(https://wiki.samba.org/index.php/Samba_Dependencies_Required_to_Build_Samba)を参照してください。

```
# yum install perl gcc attr libacl-devel libblkid-devel \
gnutls-devel readline-devel python-devel gdb pkgconfig \
krb5-workstation zlib-devel setroubleshoot-server libaio-devel \
setroubleshoot-plugins policycoreutils-python \
libsemanage-python perl-ExtUtils-MakeMaker perl-Parse-Yapp \
perl-Test-Base popt-devel libxml2-devel libattr-devel \
keyutils-libs-devel cups-devel bind-utils libxslt \
docbook-style-xsl openldap-devel autoconf python-crypto pam-devel
```

4. Samba4のダウンロードとインストール

最新のSambaをこちら (https://www.samba.org/)から入手してインストールします。

```
# wget https://download.samba.org/pub/samba/stable/samba-4.5.1.tar.gz
# tar zxvf samba-4.5.1.tar.gz
# cd samba-4.5.1/
# ./configure
# make
# make install
```

5. Active Directoryのセットアップ

WindowsとLinuxの認証統合を構築するため、オプションに 「--use-rfc2307」 を加えます。

```
# /usr/local/samba/bin/samba-tool domain provision --use-rfc2307 --interactive
Realm [TESTDOMAIN.LOCAL]: (変更がなければEnter)
 Domain [TESTDOMAIN]: (変更がなければEnter)
 Server Role (dc, member, standalone) [dc]:  (変更がなければEnter)
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: (変更がなければEnter)
 DNS forwarder IP address (write 'none' to disable forwarding) [192.168.24.1]:  (変更がなければEnter)
Administrator password: (←入力してください)
Retype password: (←入力してください)
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.24.57
Looking up IPv6 addresses
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=testdomain,DC=local
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
```

```
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=testdomain,DC=local
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc01
NetBIOS Domain:        TESTDOMAIN
DNS Domain:            testdomain.local
DOMAIN SID:            S-1-5-21-2957873491-915732319-25383699412
```

下記エラーが発生する場合は

ERROR(ldb): uncaught exception - operations error at ../source4/dsdb/samdb/ldb_modules/password_hash.c:2816

Samba4でエラー /source4/dsdb/samdb/ld b_modules/password_hash.c (/36-samba4-password-hash.html)

を参照ください。

6. Kerberosの設定

Sambaが必要なファイルを用意してくれるのでコピーします。

```
# cat /usr/local/samba/private/krb5.conf
[libdefaults]
        default_realm = TESTDOMAIN.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
# cp /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

ただし上記だけでは設定が足らないので記述を追加します。

```
# vi /etc/krb5.conf

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

[libdefaults]
 default_realm = TESTDOMAIN.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 TESTDOMAIN.LOCAL = {
```

```
 kdc = dc01.testdomain.local
 admin_server = dc01.testdomain.local
}

[domain_realm]
 .testdomain.local = TESTDOMAIN.LOCAL
 testdomain.local = TESTDOMAIN.LOCAL
```

7. Sambaの起動

起動までの準備がすべて完了したのでSambaを起動します。

CentOS7はsystemdが採用されているので、それにあわせた起動スクリプトを用意します。

```
# vi /etc/systemd/system/samba.service

[Unit]
Description= Samba 4 Active Directory
After=syslog.target
After=network.target
[Service]
Type=forking
PIDFile=/usr/local/samba/var/run/samba.pid
ExecStart=/usr/local/samba/sbin/samba
[Install]
WantedBy=multi-user.target
```

Sambaを起動します。

```
# systemctl start samba
# systemctl enable samba
```

8. Sambaの動作確認

無事Sambaが起動したら smbclient を利用してSambaへの接続確認を行います。

```
# /usr/local/samba/bin/smbclient -L localhost -U%
Domain=[TESTDOMAIN] OS=[Windows 6.1] Server=[Samba 4.5.1]
        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.5.1)
Domain=[TESTDOMAIN] OS=[Windows 6.1] Server=[Samba 4.5.1]
        Server               Comment
        ---------            -------
        Workgroup            Master
        ---------            -------
```

次にDNSにSRVレコードが登録されているか確認を行います。

```
# host -t SRV _ldap._tcp.testdomain.local 127.0.0.1
_ldap._tcp.testdomain.local has SRV record 0 100 389 dc01.testdomain.local.

# host -t SRV _kerberos._udp.testdomain.local 127.0.0.1
_kerberos._udp.testdomain.local has SRV record 0 100 88 dc01.testdomain.local.

# host -t A dc01.testdomain.local 127.0.0.1
dc01.testdomain.local has address 192.168.24.57
```

最後にKeroberosの動作確認を行います。

```
# kinit administrator
Password for administrator@TESTDOMAIN.LOCAL (mailto:administrator@TESTDOMAIN.LOCAL):
# klist
```

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TESTDOMAIN.LOCAL (mailto:administrator@TESTDOMAIN.LOCAL)
Valid starting Expires Service principal
2016-11-22T23:38:41 2016-11-23T09:38:41 krbtgt/TESTDOMAIN.LOCAL@TESTDOMAIN.LOCAL
(mailto:TESTDOMAIN.LOCAL@TESTDOMAIN.LOCAL)
renew until 2016-11-29T23:38:36

全てエラー無く結果が表示されれば動作確認完了です。

9. DNSの設定変更

参照先のDNSをsambaで構築したDNSに変更します。

```
# nmcli device
デバイス　タイプ　状態　　接続
enp0s3　　ethernet 接続済み System enp0s3
lo　　loopback 管理無し --
# nmcli connection modify "System enp0s3" ipv4.dns "192.168.24.57"
# systemctl restart NetworkManager
```

/etc/resolv.confファイルの中身を確認して、参照先DNSが自サーバになっていることを確認します。

```
# more /etc/resolv.conf
# Generated by NetworkManager
search testdomain.local
nameserver 192.168.24.57
```

10. Windowsクライアントのドメイン参加

Windowsクライアントを構築したActiveDirectoryに参加させます。

11. Linuxの認証をSSSD経由でActiveDirectoryと連携

必要なパッケージをインストールします。

```
# yum install sssd sssd-ad krb5-workstation oddjob-mkhomedir openldap-clients
```

kerberosのkeytabファイルを作成します。

```
# /usr/local/samba/bin/samba-tool domain exportkeytab /etc/krb5.keytab --principal=dc01$
Export one principal to /etc/krb5.keytab
```

sssdの設定ファイルを編集します。

```
# vi /etc/sssd/sssd.conf
```

```
[sssd]
config_file_version = 2
domains = testdomain.local
services = nss, pam
debug_level = 0

[nss]

[pam]

[domain/testdomain.local]
id_provider = ad
auth_provider = ad
access_provider = ad
chpass_provider = ad
entry_cache_netgroup_timeout = 15
entry_cache_timeout = 15
```

ldap_id_mapping = false
ldap_sasl_authid = dc01$@TESTDOMAIN.LOCAL

# ad_server = server.ad.example.com
# ad_hostname = server.ad.example.com
ad_domain = testdomain.local

設定のポイントはこちらです。

- ldap_id_mapping

  true に設定するとIDを自動生成します。false に設定するとActive DirectoryからIDを取得します。今回は false です。

sssdの設定ファイルのアクセス権を変更します。

```
# chown root:root /etc/sssd/sssd.conf
# chmod 0600 /etc/sssd/sssd.conf
```

NSS/PAMの設定をSSSDに切り替えます。

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

SSSDを起動します。

```
# systemctl restart sssd.service
```

エラーなく起動したら接続テストを行います。

まずはユーザを作成します。

```
# /usr/local/samba/bin/samba-tool user create test01 Passw0rd \
--must-change-at-next-login \
--surname=test01 \
--given-name=test01 \
--description="テストユーザ01" \
--nis-domain=testdomain \
--uid=test01 \
--uid-number=200001 \
--gid-number=100000 \
--login-shell=/bin/bash \
--unix-home=/home/testdomain.local/test01
```

作成したユーザの情報をidコマンドで取得します。

```
# id test01
uid=200001(test01) gid=100000 groups=100000
```

取得できれば接続テストは完了です。

12. 共有フォルダの作成

LinuxユーザのホームディレクトリにWindowsからアクセスできるようにします。

ついで（?）に共有フォルダも作成します。

```
# vi /usr/local/samba/etc/smb.conf
```

下記を追記します。

```
[home$]
        path = /home/testdomain.local
        browseable = no
        read only = no
        guest ok = no

[share]
        path = /opt/share
        read only = no
```

Sambaを再起動します。

systemctl restart samba

13. Domain usersグループのNIS設定

ドメイン参加したWindowsクライアントに testdomain.local ドメインの administrator でログインします。

[Active Directory ユーザーとコンピューター]にて Domain Users グループのプロパティを表示します。

UNIX属性タブを選択し、

- NISドメイン　(例: testdomain)
- GID(グループID)　(例：100000)

を設定します。

[Active Directory ユーザーとコンピューター]がインストールされていない場合は、

リモートサーバー管理ツール(RSAT)のインストール (/21-rsat.html) を参考にインストールしてください。

14. パスワードポリシーの確認と変更

デフォルトのパスワードポリシーを確認します。

```
# /usr/local/samba/bin/samba-tool domain passwordsettings show
Password informations for domain 'DC=testdomain,DC=local'

Password complexity: on                         # パスワードの複雑さ要求
Store plaintext passwords: off                  # パスワードを平文で保管
Password history length: 24                     # 過去のパスワードを保持する件数
Minimum password length: 7                      # 最小パスワード長
Minimum password age (days): 1                  # パスワード変更禁止期間
Maximum password age (days): 42                 # パスワード有効期間
Account lockout duration (mins): 30             # アカウントのロックアウト期間
Account lockout threshold (attempts): 0         # アカウントのロックアウトのしきい値
Reset account lockout after (mins): 30          # 後のアカウントのロックアウトをリセット
```

非常に厳しい内容になっていますので少し見直します。

過去のパスワードを保持する件数を5に変更

/usr/local/samba/bin/samba-tool domain passwordsettings set --history-length=5

パスワードの長さを8文字以上に変更

/usr/local/samba/bin/samba-tool domain passwordsettings set --min-pwd-length=8

パスワード変更禁止期間を0日に変更

/usr/local/samba/bin/samba-tool domain passwordsettings set --min-pwd-age=0

パスワード有効期間を30日に変更

/usr/local/samba/bin/samba-tool domain passwordsettings set --max-pwd-age=30

アカウントのロックアウトのしきい値を50回に変更

/usr/local/samba/bin/samba-tool domain passwordsettings set --account-lockout-threshold=50

以上で全ての設定が完了です。

15. ログインの確認

まずはLinuxにログインします。

初回ログインにパスワード変更を求められる設定の為、パスワード変更後に一旦セッションがクローズします。

```
# ssh test01@localhost
test01@localhost's password:
Password expired. Change your password now.
Creating home directory for test01.
WARNING: Your password has expired.
You must change your password now and login again!
ユーザー test01 のパスワードを変更。
現在のパスワード:
新しいパスワード:
新しいパスワードを再入力してください:
passwd: すべての認証トークンが正しく更新できました。
Connection to localhost closed.
```

新しいパスワードでログインします。

```
# ssh test01@localhost
test01@localhost's password:
$ id;pwd
uid=200001(test01) gid=100000(domain users) groups=100000(domain users)
/home/testdomain.local/test01
```

ログインできれば確認完了です。

検証用にtouchコマンドでホームディレクトリと共有フォルダにファイルを作成します。

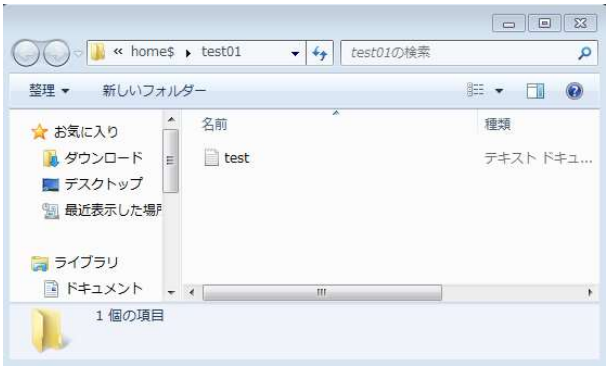
```
$ touch test.txt
$ touch /opt/share/test.txt
```

次にWindowsログオンと共有フォルダアクセスの確認します。

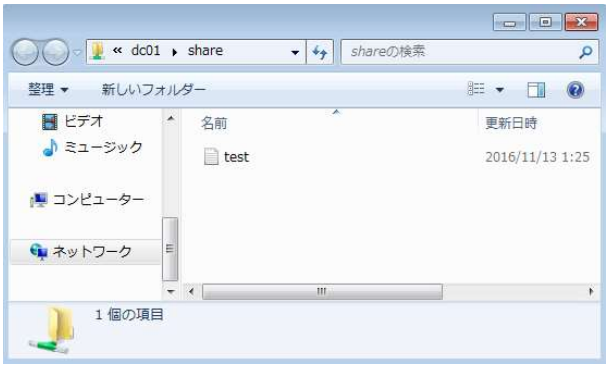
ドメイン参加したPCにLinuxと同じユーザでログインします。

ログオンできたらホームディレクトリにアクセスできるか確認をします。

パスは \\dc01\home$\test01 です。



共有フォルダも同様にアクセスできるか確認します。パスは \\dc01\share です。



問題なくアクセスできれば確認完了です。

お疲れさまでした。

最も読まれた記事

- Xming + Teraterm で画面転送 (/11-xming-teraterm.html)
- xrdpを利用してLinuxにリモートデスクトップ接続 (/8-xrdp-centos72.html)
- Samba4とSSSDでLinux/Windowsの認証統合環境を構築(ActiveDirectory+NIS) (/22-samba4-activedirectory-sssd.html)
- CentOS7で日本語を入力する方法 (/37-japanese-input.html)
- ログインユーザを強制ログアウト (/12-logout.html)

検索

検索...

タグ

- CentOS7 (/component/tags/tag/centos7.html)
- リモートデスクトップ (/component/tags/tag/remotedesktop.html)

古い記事

- Samba4.7（AD with MIT Kerberos）をソースコードから導入 (/40-samba47-ad-with-mit-kerberos.html)
- xrdpのデスクトップ環境を「MATE」にする (/39-xrdp-mate.html)
- CentOS7に軽量デスクトップ環境「MATE」を導入 (/38-centos7-mate.html)
- CentOS7で日本語を入力する方法 (/37-japanese-input.html)
- Samba4でエラー /source4/dsdb/samdb/ldb_modules/password_hash.c (/36-samba4-password-hash.html)
- dracut-initqueue: Warning: Could not boot (/34-dracut-initqueue-could-not-boot.html)

Joomla templates by a4joomla (http://a4joomla.com/)