Setting up Samba as an Active Directory Domain Controller

Contents

Introduction

Starting from version 4.0 (released in 2012,) Samba is able to serve as an Active Directory (AD) domain controller (DC). Samba operates at the forest functional level of **Windows Server 2008 R2** which is more than sufficient to manage sophisticated enterprises that use Windows 10/11 with strict compliance requirements (including NIST 800-171.)

If you are installing Samba in a production environment, it is recommended to run two or more DCs for failover reasons, more detail on the provisioning of a failover DC can be found elsewhere on the wiki. This documentation describes how to set up Samba as the first DC to build a new AD forest. Additionally, use this documentation if you are migrating a Samba NT4 domain to Samba AD. To join Samba as an additional DC to an existing AD forest, see Joining a Samba DC to an Existing Active Directory.

Samba as an AD DC only supports:

- The integrated LDAP server as AD back end. For details, see the frequently asked question (FAQ) Does Samba AD DCs Support OpenLDAP or Other LDAP Servers as Back End?
- The Heimdal Kerberos Key Distribution Center (KDC).

Samba provides experimental support for the MIT Kerberos KDC provided by your operating system if you run Samba 4.7 or later and has been built using the `--with-system-mitkrb5` option. In other cases Samba uses the Heimdal KDC included in Samba. For further details about Samba using the MIT KDC, and why it is experimental see Running a Samba AD DC with MIT Kerberos KDC.

- Hosting and Administering of Group Policy Objects to be used for enterprise fleet management

Installation of Samba and associated provisioning of a domain controller does not automatically translate into Group Policy functionality. Please keep this in mind, and expect to update this flag in the `smb.conf` post provisioning

This tutorial assumes that this is a fresh installation of Samba on a fresh operating system installation. It is important to note that there is a distinction between installing of Samba and Provisioning of Samba. In general, the entire process of setting up a Samba domain controller consists of 5 steps which are relatively straight forward. These steps are as follows:

1. Installation of Samba and associated packages
2. Deletion of pre-configured Samba and Kerberos placeholder configuration files
3. Provisioning of Samba using the automatic provisioning tool
4. Editing of the `smb.conf` as needed (enabling of Group Policy and/or other features as needed) see Group Policy for more information
5. Any environmental configuration based on Unix/Linux Distribution

This page covers a lot of ground for Samba installations on both Unix and Linux systems. The installation process varies slightly based on environment, so expect to follow the linked web pages in multiple tabs throughout this read. For the remainder of this tutorial the following example information is used:

- Hostname = `DC1`
- DC local IP Address = `10.99.0.1`
- Authentication Domain = `SAMDOM.EXAMPLE.COM`
- Top level Domain = `EXAMPLE.COM`

Preparing the Installation

Fresh Installation

- Select a DNS domain for your AD forest. It is not recommended to use the top level domain for your organization. This is because the domain used during the installation of Samba will resolve to the domain controller. For Example: If your organization used `EXAMPLE.COM` as their domain and this was used during the Samba installation process, then the public facing website would no longer be acceptable (assuming the publicly accessible website was not running on the DC, which it shouldn't!) It would be wise to define a subdomain for your Domain Controller to reside in. In this tutorial `SAMDOM.EXAMPLE.COM` is used, however in a lab environment it is not necessary to own a publicly accessible domain and `.INTERNAL` could hypothetically be used. The name will also be used as the AD Kerberos realm.

Make sure that you provision the AD using a DNS domain that will not need to be changed. Samba does not support renaming the AD DNS zone and Kerberos realm. Do not use `.local` for the TLD, this is used by Avahi.

For additional information, see Active Directory Naming FAQ.

- Select a host name for your AD DC which consists of less than 15 characters (netbios limitation.) A fantastic hostname is `DC1`

Do not use NT4-only terms as host name, such as `PDC` or `BDC`. These modes do not exist in an AD and cause confusion.

- Set a static IP address on the DC and make the associated reservation on your router. **Important:** The Samba domain controller will become your DNS resolver for all domain-joined workstations. As a result it may be required to assign this IP address outside of your DHCP pool

- Disable tools, such as `resolvconf`, that automatically update your `/etc/resolv.conf` DNS resolver configuration file. AD DCs and domain members must use an DNS server that is able to resolve the AD DNS zones. (More information on this on the Distribution Specific Package Installation page)

- Verify that the `/etc/hosts` file on the DC correctly resolves the fully-qualified domain name (FQDN) and short host name to the LAN IP address of the DC. For example:

```
127.0.0.1     localhost
10.99.0.1     DC1.samdom.example.com     DC1
```

The host name and FQDN must not resolve to the `127.0.0.1` IP address or any other IP address than the one used on the LAN interface of the DC.

- Remove any existing `smb.conf` file. To list the path to the file:

```
# smbd -b | grep "CONFIGFILE"
   CONFIGFILE: /usr/local/samba/etc/samba/smb.conf
```

Only Applicable if Samba was Previously Installed

- If you previously ran a Samba installation on this host:

    - Remove all Samba database files, such as `*.tdb` and `*.ldb` files. To list the folders containing Samba databases:

```
# smbd -b | egrep "LOCKDIR|STATEDIR|CACHEDIR|PRIVATE_DIR"
  LOCKDIR: /usr/local/samba/var/lock/
  STATEDIR: /usr/local/samba/var/locks/
  CACHEDIR: /usr/local/samba/var/cache/
  PRIVATE_DIR: /usr/local/samba/private/
```

Starting with a clean environment helps to prevent confusion and ensures that no files from any previous Samba installation will be mixed with your new domain DC installation.

Installing Samba

- Operating System Requirements

    - Package Dependencies Required to Build Samba
    - File System Support

- Build Samba from Source
- Distribution-specific Package Installation

Install a maintained Samba version. For details, see Samba Release Planning.

Provisioning a Samba Active Directory

The AD provisioning requires root permissions to create files and set permissions.

The Samba AD provisioning process creates the AD databases and adds initial records, such as the domain administrator account and required DNS entries. Samba comes with a built in command lined tool called `samba-tool` which can be used to automatically configure your `smb.conf` when ran in interactive mode.

If you are migrating a Samba NT4 domain to AD, skip this step and run the Samba classic upgrade. For details, see Migrating a Samba NT4 Domain to Samba AD (Classic Upgrade).

The `samba-tool domain provision` command provides several parameters to use with the interactive and non-interactive setup. For details, see:

```
# samba-tool domain provision --help
```

When provisioning a new AD, it is recommended to enable the NIS extensions by passing the `--use-rfc2307` parameter to the `samba-tool domain provision` command. There are no disadvantages to enabling the NIS extensions, but enabling them in an existing domain requires manually extending the AD schema. For further details about Unix attributes in AD, see:

- Setting up RFC2307 in AD
- idmap config = ad

Parameter Reference

Set the following parameters during the provisioning:

Interactive Mode Setting	Non-interactive Mode Parameter	Explanation
`--use-rfc2307`	`--use-rfc2307`	Enables the NIS extensions required for the ADUC Unix Attributes tab.
`Realm`	`--realm`	Kerberos realm. The uppercase version of the AD DNS domain. For example: `SAMDOM.EXAMPLE.COM`.
`Domain`	`--domain`	NetBIOS domain name (Workgroup). This can be anything, but it must be one word, not longer than 15 characters and not containing a dot. It is recommended to use the first part of the AD DNS domain. For example: `samdom`. Do not use the computers short hostname.
`Server Role`	`--server-role`	Installs the domain controller `DC` role.
`DNS backend`	`--dns-backend`	Sets the DNS back end. The first DC in an AD must be installed using a DNS back end. Note that the `BIND9_FLATFILE` is not supported and will be removed in a future Samba version.
`DNS forwarder IP address`	not available	This setting is only available when using the `SAMBA_INTERNAL` DNS back end. For details, see Setting up a DNS Forwarder.
`Administrator password`	`--adminpass`	Sets the domain administrator password. If the password does not match the complexity requirements, the provisioning fails. For details, see Microsoft TechNet: Passwords must meet complexity requirements.

Other parameters frequently used with the `samba-tool domain provision` command:

- `--option="interfaces=lo eth0" --option="bind interfaces only=yes"`: If your server has multiple network interfaces, use these options to bind Samba to the specified interfaces. This enables the `samba-tool` command to register the correct LAN IP address in the directory during the join.

do NOT use `NONE` as the DNS backend, it is not supported and will be removed in a future Samba version.

If using Bind as the DNS backend, do NOT use `BIND9_FLATFILE`, it is not supported and will be removed in a future Samba version.

Once you have provisioned the first DC in an AD domain, do not provision any further DCs in the same domain, Join any further DCs.

Provisioning Samba AD in Interactive Mode

As mentioned above, when run as root, `samba-tool` will automatically configure your `smb.conf` to build a domain controller. Interactive Mode will not automatically enable Group Policy support. However this can be added in afterwards by manually editing `smb.conf`.

When following the instructions below, it may be helpful to have the Group Policy page open in a separate browser tab or window.

The installation of Samba will create a `smb.conf` file that must be discarded prior to running the Provisioning Tool in Interactive mode, or else it will fail. On most Linux distributions this can be

done by running: # mv /etc/samba/smb.conf /etc/samba/smb.conf.initial

With the existing `smb.conf` file removed, provision a Samba AD interactively by running:

```
# samba-tool domain provision --use-rfc2307 --interactive
Realm [SAMDOM.EXAMPLE.COM]: SAMDOM.EXAMPLE.COM
 Domain [SAMDOM]: SAMDOM
 Server Role (dc, member, standalone) [dc]: dc
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: SAMBA_INTERNAL
 DNS forwarder IP address (write 'none' to disable forwarding) [10.99.0.1]: 8.8.8.8
Administrator password: Passw0rd
Retype password: Passw0rd
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
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=samdom,DC=example,DC=com
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=samdom,DC=example,DC=com
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:              DC1
NetBIOS Domain:        SAMDOM
DNS Domain:            samdom.example.com
DOMAIN SID:            S-1-5-21-2614513918-2685075268-614796884
```

The interactive provisioning mode supports passing further parameters to the `samba-tool domain provision` command. This enables you to modify parameters that are not part of the interactive setup.

Provisioning Samba AD in Non-interactive Mode

For example, to provision a Samba AD non-interactively with the following settings:

- Server role: `dc`
- NIS extensions enabled
- Internal DNS back end
- Kerberos realm and AD DNS zone: `samdom.example.com`
- NetBIOS domain name: `SAMDOM`
- Domain administrator password: `Passw0rd`

```
# samba-tool domain provision --server-role=dc --use-rfc2307 --dns-backend=SAMBA_INTERNAL --
realm=SAMDOM.EXAMPLE.COM --domain=SAMDOM --adminpass=Passw0rd
```

Setting up the AD DNS back end

Skip this step if you provisioned the DC using the `SAMBA_INTERNAL` DNS back end.

- Set up the BIND DNS server and the `BIND9_DLZ` module. For details, see Setting up a BIND DNS Server.
- Start the BIND DNS server. For example:

```
# systemctl start named
```

For details how to start services, see you distribution's documentation.

Configuring the DNS Resolver

Domain members in an AD use DNS to locate services, such as LDAP and Kerberos. For that, they need to use a DNS server that is able to resolve the AD DNS zone.

On your DC, set the AD DNS domain in the `search` and the IP of your DC in the `nameserver` parameter of the `/etc/resolv.conf` file. For example:

```
search samdom.example.com
nameserver 10.99.0.1
```

Configuring Kerberos

In an AD, Kerberos is used to authenticate users, machines, and services.

During the provisioning, Samba created a Kerberos configuration file for your DC. Copy this file to your operating system's Kerberos configuration. For instance, if you built Samba yourself:

```
# cp /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

Your `krb5.conf` path probably will be different, always use the path in the provision output. However, wherever Samba creates the `krb5.conf`, you need to copy it to `/etc/krb5.conf`.

Do not create a symbolic link to the the generated `krb5.conf` file. In Samba 4.7 and later, the `/usr/local/samba/private/` directory is no longer accessible by other users than the `root` user. If the file is a symbolic link, other users are not able to read the file and, for example, dynamic DNS updates fail if you use the `BIND_DLZ` DNS back end.

The pre-created Kerberos configuration uses DNS service (SRV) resource records to locate the KDC.

Testing your Samba AD DC

To start the `samba` service manually, enter:

```
# samba
```

Samba does not provide System V init scripts, `systemd`, `upstart`, or other services configuration files.

- If you installed Samba using packages, use the script or service configuration file included in the package to start Samba.
- If you built Samba, see Managing the Samba AD DC Service.

Create a reverse zone

You can optionally add a reverse lookup zone.

```
# samba-tool dns zonecreate <Your-AD-DNS-Server-IP-or-hostname> 0.99.10.in-addr.arpa -U Administrator
Password for [administrator@SAMDOM.EXAMPLE.COM]:
Zone 0.99.10.in-addr.arpa created successfully
```

If you need more than one reverse zone (multiple subnets), just run the above command again but with the data for the other subnet.

The reverse zone is directly live without restarting Samba or BIND.

You must start the Samba AD DC before you can add a reverse zone.

Now that you have created a reversezone, it would be a good time to create the `PTR` (reverse) dns record for the new DC.

For a DC with the FQDN of `dc1.samdom.example.com` and the ipaddress of `10.99.0.1`, to add a record to the `0.99.10.in-addr.arpa`, you would run a command like this:

```
# samba-tool dns add <Your-AD-DNS-Server-IP-or-hostname> 0.99.10.in-addr.arpa 1 PTR dc1.samdom.example.com -
U Administrator
Password for [administrator@SAMDOM.EXAMPLE.COM]:
Record added successfully
```

The reverse records are not added automatically, you must add them manually, or set Windows computers to add them when updating their dns records.

Verifying the File Server (Optional)

To list all shares provided by the DC:

Before Samba 4.11.0:

```
$ smbclient -L localhost -N
Anonymous login successful
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba x.y.z)
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

From Samba 4.11.0:

```
smbclient -L localhost -N
Anonymous login successful

    Sharename       Type      Comment
    ---------       ----      -------
    sysvol          Disk
    netlogon        Disk
    IPC$            IPC       IPC Service (Samba 4.12.6-Debian)
SMB1 disabled -- no workgroup available
```

The `netlogon` and `sysvol` shares were auto-created during the provisioning and must exist on a DC.

To verify authentication, connect to the `netlogon` share using the domain administrator account:

```
$ smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter Administrator's password:
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]
 .                                   D        0  Tue Nov  1 08:40:00 2016
 ..                                  D        0  Tue Nov  1 08:40:00 2016

               49386 blocks of size 524288. 42093 blocks available
```

If one or more tests fail, see Troubleshooting.

Verifying DNS (Optional)

To verify that your AD DNS configuration works correctly, query some DNS records:

- The tcp-based `_ldap` SRV record in the domain:

```
$ host -t SRV _ldap._tcp.samdom.example.com.
_ldap._tcp.samdom.example.com has SRV record 0 100 389 dc1.samdom.example.com.
```

- The udp-based `_kerberos` SRV resource record in the domain:

```
$ host -t SRV _kerberos._udp.samdom.example.com.
_kerberos._udp.samdom.example.com has SRV record 0 100 88 dc1.samdom.example.com.
```

- The A record of the domain controller:

```
$ host -t A dc1.samdom.example.com.
dc1.samdom.example.com has address 10.99.0.1
```

- If you have created a reverse zone, the PTR record of the domain controller:

```
$ host -t PTR 10.99.0.1
1.0.99.10.in-addr.arpa domain name pointer dc1.samdom.example.com.
```

If one or more tests fail, see Troubleshooting.

Verifying Kerberos (Optional)

This is not explicitly required, but it is a good idea to verify that your Domain Controller's authentication mechanisms are operating as intended. To test this, login by requesting a Kerberos ticket for the Domain Administrator account:

```
$ kinit administrator
Password for administrator@SAMDOM.EXAMPLE.COM:
```

If you do not pass the principal in the `user@REALM` format to the `kinit` command, the Kerberos realm is automatically appended.
Always enter the Kerberos realm in uppercase.

- List the cached Kerberos tickets:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SAMDOM.EXAMPLE.COM

Valid starting       Expires              Service principal
01.11.2016 08:45:00  12.11.2016 18:45:00  krbtgt/SAMDOM.EXAMPLE.COM@SAMDOM.EXAMPLE.COM
        renew until 02.11.2016 08:44:59
```

If one or more tests fail, see Troubleshooting.

Configuring Time Synchronization (Optional Depending on Use-Case)

Kerberos requires synchronized time on all domain members. For further details and how to set up the `ntpd` or `chrony` service, see Time Synchronization. However if Samba is being used as a domain controller to administer Group Policy, it is possible to define a Group Policy Object that synchronizes workstations with `time.windows.com` post installation which simplifies this

Using the Domain Controller as a File Server (Optional)

Do not use an AD DC as a fileserver if you have multiple DC's. You should only use a DC as a fileserver, if it is the only Samba instance running in a domain. If you have multiple DC's, you should also set up Unix domain members and use them as fileservers. You should be aware that it is problematic to use a DC as a fileserver and can cause strange errors.

While the Samba AD DC is able to provide file shares like all other installation modes, the Samba team does not recommend using a DC as a file server for the following reasons:

- For anything but the smallest organizations, having more than one DC is a really good backup measure, and makes upgrades safer

- It encourages upgrades of the DC to also be upgrades of the host OS every year or two, because there isn't complex data to transition or other services involved.
- This means upgrades can be done by installing fresh, and replicating in the changes, which is better tested in Samba, gains new features and avoids a number of lingering data corruption risks.
- The DC and file-server have different points at which an organization would wish to upgrade. The needs for new features on the DC and file server come at different times. Currently the AD DC is evolving rapidly to gain features, whereas the fileserver, after over 20 years, is quite rightly more conservative.
- mandatory smb signing is enforced on the DC.

If you do decide to use the Samba DC as a fileserver, please consider running a VM, on the DC, containing a separate Samba Unix domain member and use this instead.

If you must use the Samba DC as a fileserver, you should be aware that the auto-enabled `acl_xattr` virtual file system (VFS) object enables you to only configure shares with Windows access control lists (ACL). Using POSIX ACLs with shares on a Samba DC does not work.

You should be aware that if wish to use a vfs object on a DC share e.g. recycle, you must not just set `vfs objects = recycle` in the share. Doing this will turn off the default vfs objects `dfs_samba4` and `acl_xattr`. You must set `vfs objects = dfs_samba4 acl_xattr recycle`.

To provide network shares with the full capabilities of Samba, set up a Samba domain member with file shares. For details, see:

- Setting up Samba as a Domain Member
- Samba File Serving

If you only have a small domain (small office, home network) and do not want to follow the Samba team's recommendation and use the DC additionally as a file server, configure Winbindd before you start setting up shares. For details, see Configuring Winbindd on a Samba AD DC.


If you do use an AD DC as a fileserver, you must be aware that it can be problematic and can cause strange errors.


If you do use an AD DC as a fileserver, do not add any of the 'idmap config' lines used on a Unix domain member. They will not work and will cause problems.


If you do use an AD DC as a fileserver, You must set the permissions from Windows, do not attempt to use any of the old methods (force user etc) . They will not work correctly and will cause problems.

Troubleshooting

For further details, see Samba AD DC Troubleshooting.

Further Samba-related Documentation

See User Documentation.
