Setup a Samba Active Directory Domain Controller

From SambaWiki

Contents

Introduction

Since version 4.0, Samba can, additionally to a NT4 PDC, act as a Domain Controller that is compatible with Microsoft Active Directory. In the following, we explain how to set up Samba as an Active Directory Domain Controller from scratch. In addition, this documentation is the start for upgrading an existing Samba NT4-style domain to a Samba AD.

Whilst the Domain Controller seems capable of running as a full file server, it is suggested that organisations run a distinct file server to allow upgrades of each without disrupting the other. It is also suggested that medium-sized sites should run more than one DC. It also makes sense to have the DC's distinct from any file servers that may use the Domain Controllers. Additionally using distinct file servers avoids the idiosyncrasies in the winbindd configuration on to the Active Directory Domain Controller. The Samba team do not recommend using the Domain Controller as a file server, the recommendation is to run a separate Domain Member with file shares.

If you are looking for documentation about updating the Samba version of an existing Samba Active Directory Domain Controller, please consult your distribution upgrade procedure or see: Updating Samba.

Samba as an AD DC requires at least version 4.0.0, but it's always recommended to use one of the latest stable versions of Samba. It will contain fixes for bugs from previous releases and may contain improved Microsoft Active Directory compatibility and additional features. See the Samba release plan for more details about the latest maintained versions and their release notes.

Please note that you do not need to install or configure any other Kerberos KDC for Samba to work. Samba includes an AD compatible KDC, currently based on an included copy of the Heimdal (http://www.h5l.se/) project. Likewise Samba ships its own LDAP implementation for AD backends. OpenLDAP or other LDAP servers are not supported at the moment.

If you already have an Active Directory and want to join an additional Samba Domain Controller, see the Join an additional Samba DC to an existing Active Directory documentation.

See the server information used in documentation page for used paths, hostnames, etc.

Preconditions

- Make sure that your future DC uses a static IP address. DHCP can cause trouble if the address changes.
- Read carefully the Active Directory Naming FAQ for information, frequent pitfalls, etc. about choosing a DNS and NetBIOS name for your AD. Currently Samba AD does not support changing this, so this makes it to an important decision!
- Check your /etc/hosts for a correct resolution of the hostname to its IP:

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

  Ensure that your DC hostname resolves to its LAN IP and not to 127.0.0.1!

- Remove any previous existing installation of Samba. If upgrading from a Samba NT4 domain to Samba AD, only keep your previous smb.conf and the databases.

Installation

Before you start, check the Operating System requirements for dependencies.

You have the following options to install Samba:

- Build Samba yourself
- Install distribution specific packages

  Make sure that you use a recent Samba and note, that not all distributions currently ship Samba packages, with Active Directory Domain Controller capabilities. One of the reasons is, that some distributions are based on MIT Kerberos, while Samba (currently) only supports Heimdal Kerberos. E. g. Red Hat operating systems (RHEL, CentOS, Fedora, etc.) are affected. In this case, choose one of the other install options.

- Install SerNet Samba+ (http://www.samba.plus) /Enterprise (http://www.samba.plus/older-packages/) packages

Paths

You should consider putting the directories "/usr/local/samba/bin/" and "/usr/local/samba/sbin/" at the beginning of your $PATH variable:

```
export PATH=/usr/local/samba/bin/:/usr/local/samba/sbin/:$PATH
```

To permanently add this to your system or user configuration, see your distributions documentation.

Provisioning the Samba Active Directory

Migration of a Samba NT4 domain: *If you plan to migrate an existing Samba NT4 domain to Samba AD, you do not manually provision the domain. The migration is done by the classicupgrade process. Skip this section and follow Migrating a Samba NT4 domain to a Samba AD domain (classic upgrade). Come back afterwards and continue with Testing your Samba Domain Controller.*

When Samba sets up the first Domain Controller in a Domain, the provisioning creates an initial Active Directory database. This must be done with root privileges, to enable writing to the installation directory and setting the correct permissions on files and folders.

First make yourself familiar with the possible parameters and options of the provisioning:

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

If your Domain Controller has multiple network interfaces, the following two "samba-tool" options are required, to prevent the tool auto-choosing one of the IPv4/IPv6 addresses of the interfaces. Furthermore it is necessary to bind Samba to the desired interface.

```
# samba-tool domain provision ..... --option="interfaces=lo eth0" --option="bind interfaces only=yes"
```

Interactively provision a new domain (parameter explanation below):

```
# 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
```

Parameter explanations:

--use-rfc2307: Enables NIS extensions. They allow a central management of Unix attributes (UIDs, shells, GIDs, etc.) inside Active Directory. It is recommended to always enable this feature during the provisioning. There are no disadvantages in not using it, but you may later find yourself in a situation where the central management of Unix account/group information becomes a requirement. Enabling it afterwards requires additional work such as manually extending the AD schema. For further information about RFC2307, see General information on RFC2307 and Setting up RFC2307 in AD.

--interactive: Use interactive provisioning. The defaults are the values in the squared brackets, they will be used if no other input is made.

Realm: Kerberos Realm and AD DNS domain written in upper case. You should always use a subdomain of your domain name (e. g. samdom.example.com). Never use your domain name (example.com) for your Active Directory DNS domain. This prevent you accessing accessing servers using that name, like web server, because the domain is resolved to the IP(s) of your Domain Controller(s) instead! See the Active Directory Naming FAQ for further information and help.

Domain: NT4 NetBIOS domain name in upper case used by AD for compatibility reasons. Maximum name length: 15 characters. Usually - and that's what we recommend - this is the first part of the AD DNS name. In any case if using something different, make sure that it matches the naming conventions in Active Directory (section "NetBIOS domain names") (https://support.microsoft.com/en-us/kb/909264) . Please note, that even if some punctuation marks like periods are allowed, they can cause trouble in some situations and should be avoided! See the Active Directory Naming FAQ for further information and help.

Server Role: 'dc' for Domain Controller.

DNS backend: Supported DNS backends are the Samba internal DNS server and BIND9_DLZ. We used the default - the internal DNS - in our example above. It is the best choice if you do not have complex DNS requirements. See Which DNS backend should I choose? for a comparison and suggestions. If you have chosen BIND9_DLZ as backend, you must setup and configure BIND, before first starting your Domain Controller. See Configure BIND as backend for Samba AD for further setup information. If you later find out that your DNS backend choice doesn't fit your needs, you can change it afterwards. Do not use BIND9_FLATFILE as the DNS backend. It isn't documented and is not supported! Seeing as AD heavily relies on DNS, the first DC in an AD must act as a DNS server, so you can't choose NONE here.

DNS forwarder IP address: You are only prompted for this information, if you choose the Samba internal DNS as the backend. It defines the IP address of one DNS server, to which DNS queries should be forwarded, when your DNS server isn't authoritative for a zone. Commonly it is your providers DNS server IP address.

Administrator password: The Domain Administrators password. It must meet the complexity requirements (see https://technet.microsoft.com/en-us/library/cc786468%28v=ws.10%29.aspx):

- At least 8 characters
- Containing at least three of the following five character groups
  - Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
  - Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
  - Base 10 digits (0 through 9)
  - Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
  - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

If the password doesn't fulfil the complexity requirements, the provisioning will fail and you will have to start over (remove the newly generated "smb.conf" in this case).

Testing your Samba Domain Controller

Note: If you are running any "smbd", "nmbd" or "winbindd" processes from previous installations, they need to be stopped before starting "samba" from your new DC installation!

To start the Samba Active Directory Domain Controller in "standard" mode, which is suitable for production use, run

```
# samba
```

Samba doesn't yet have init scripts included. You can find examples on the Samba Init-Script page.

Run "smbclient", to check if Samba provides the AD DC default shares "netlogon" and "sysvol", that were created in your "smb.conf" during provisioning/upgrading:

```
$ smbclient -L localhost -U%
Domain=[SAMDOM] OS=[Unix] Server=[Samba 4.x.y]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.x.y)
Domain=[SAMDOM] OS=[Unix] Server=[Samba 4.x.y]

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

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

To test that authentication is working, you should try to connect to the „netlogon“ share, using the Domain Administrator account that was created during provisioning/upgrading:

```
$ smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter Administrator's password: Passw0rd
Domain=[SAMDOM] OS=[Unix] Server=[Samba 4.x.y]
 .                                   D        0  Sat Jul  5 08:40:00 2015
 ..                                  D        0  Sat Jul  5 08:40:00 2015

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

If any of the connection tests fail, check out the Samba AD DC Troubleshooting page.

Configure DNS

A working DNS is essential for the correct operation of an Active Directory! E. g. without the right DNS entries, Kerberos won't work, which in turn means that many of the basic features won't work. It is worth spending some extra time ensuring your DNS setup is correct, because debugging problems caused by incorrect DNS configuration, can take a lot of time later.

Configure /etc/resolv.conf

Your Domain Controller requires a name server that is able to resolve queries to Active Directory zones. Because this is your first Domain Controller in your AD forest, use the DCs IP and domain name in your /etc/resolv.conf:

```
domain samdom.example.com
nameserver 10.99.0.1
```

Testing DNS

To test that DNS is working properly, run the following commands and compare the output to what is shown:

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

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

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

If you receive any errors, check your system logs to locate the problem.

Configure Kerberos

Configure /etc/krb5.conf

Kerberos is an important part of Active Directory. Typically the configuration is done in /etc/krb5.conf. During provisioning, a working sample configuration will be created. You can replace your krb5.conf file with the sample by copying or creating a symlink:

```
# ln -sf /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

Testing Kerberos

Use "kinit" to obtain a Kerberos ticket:

```
# kinit administrator@SAMDOM.EXAMPLE.COM
Password for administrator@SAMDOM.EXAMPLE.COM: Passw0rd
```

Note: *You must always specify your realm in uppercase letters!*

Depending on your distribution, "kinit" may just return you to a prompt when successful. To verify that Kerberos is working and that you had received a ticket, run:

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

Valid starting       Expires              Service principal
08.09.2015 14:27:45  09.09.2015 00:27:45  krbtgt/SAMDOM.EXAMPLE.COM@SAMDOM.EXAMPLE.COM
        renew until 09.09.2015 14:27:42
```

Configure NTP

Active Directory requires an accurate time synchronization between all participant machines for Kerberos to work properly. It's highly recommended to use NTP or another form of time synchronization on your Domain Controller! The Time synchronisation documentation will provide all necessary information, to configure NTP on an AD Domain Controller.

Troubleshooting

If you encounter any problems when using this documentation, see the Samba AD DC Troubleshooting page.

Further documentation

The Samba Wiki provides a lot of useful documentation on administering your DC, (Backup and restore an Samba AD DC, Setup shares with Windows ACLs, etc.) and daily work (Joining a Windows client to a Domain, Installing RSAT on Windows for AD Management, etc.).

See the Samba user documentation for a great overview.

Report your success/failure!

We would encourage you to report your successes and failures to the Samba mailing list on https://lists.samba.org/mailman/listinfo/samba.

Suggestions on improving the documentation has the same importance as reporting Bugs (https://bugzilla.samba.org/) and complications.