Join an additional Samba DC to an existing Active Directory

From SambaWiki

Contents

- 1 Introduction
- 2 Preconditions
- 3 Installation
  - 3.1 Paths
- 4 Preparing the host for the domain join
  - 4.1 Local DNS server
  - 4.2 DNS resolving
  - 4.3 Kerberos
- 5 Join the existing domain as a Domain Controller
- 6 Check DNS entries
- 7 Adaptations for the BIND DNS backend
  - 7.1 Workaround: Fix keytab permissions
  - 7.2 Enable the correct BIND9_DLZ module
- 8 GID mappings of built-in groups
- 9 Start Samba
- 10 Directory replication
- 11 Start BIND
- 12 Testing the local DNS
- 13 Best practice: DNS configuration on DCs
- 14 SYSVOL replication
- 15 Testing directory replication
  - 15.1 ldapcmp
- 16 Troubleshooting

Introduction

The minimum number of Domain Controllers in an Active Directory forest is one. However, in an enterprise environment, it is always recommended to add further DCs, to provide failure safety, high availability and load balancing. For fail-over reasons, at least two DCs are recommended. Depending on your network, there can be many different reasons in deciding just how many DCs are required. A common scenario is, an AD forest is spread across multiple locations, connected via VPN or the like, here it is reasonable to have at least one DC at each site. This keeps AD services available everywhere, even if the branch office is temporary not connected to the central office. Unless you're running a RODC, each Domain Controller has a write-enabled database, this allows changes inside the AD to be done on every DC. Password changes, user creation, domain joins, etc. will still possible, even if other DCs are temporary not available due to e. g. network outages and users on each site can continue to authenticate and work with local servers without problems.

An NT4 domain has only one Primary Domain Controller (PDC) and possibly additional Backup Domain Controllers (BDC). In an AD forest there's no such difference any more, there is no such thing as a "master server" , They are all simply called "Domain Controller" (DC) and are equal. Please use only this term, when talking about an Active Directory, to avoid confusion, especially when asking for help.

The process of joining a new Samba DC to an existing AD differs in some points to provisioning a new domain. The following steps for joining a Samba DC to an existing domain are the same - regardless if the existing AD is based on Windows or Samba DCs. However, if you're joining the first Samba DC into a Windows based AD, you should read the Setup a Samba Active Directory Domain Controller documentation before you continue. It contains some basic information about the environment, command explanation, etc. not repeated here.

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

Preconditions

- Make sure that your future DC uses a static IP address. Using one set by DHCP can cause trouble, if the address changes.
- Check your /etc/hosts for a correct resolution of the hostname to its IP:

```
127.0.0.1     localhost.localdomain      localhost
10.99.0.2     DC2.samdom.example.com     DC2
```

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

- Remove any previous existing installation of Samba on the host.
- If your AD forest is Windows driven, further checks are required:

  The following commands can be run from any Windows domain computer.

  - Check the Forest functional level:

```
> dsquery * "CN=Partitions,CN=Configuration,DC=samdom,DC=example,DC=com" -scope base -attr msDS-Behavior-Version
  msDS-Behavior-Version
  4
```

    Minimum suported level: 2003 native (level 2)
    Maximum suported level: 2008 R2 (level 4)

  - Check the directory schema version:

```
> dsquery * "CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com" -Scope Base -attr objectVersion
  objectVersion
  69
```

    Samba <= 4.4.x: The maximum Forest schema supported is: 47 (Server 2008 R2)
    Samba >= 4.5.x: The maximum Forest schema supported is: 69 (Server 2012 R2)

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 version of Samba, noting that not all distributions currently ship Samba packages with Active Directory Domain Controller capabilities. One reason 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.

Preparing the host for the domain join

Local DNS server

By default, the first Domain Controller in a domain automatically acts as a DNS server for AD based zones. For failover reasons, it is recommended to have at least two DC's providing AD DNS services. If you plan to use BIND as the DNS backend on the new Domain Controller, you have to configure BIND as backend for Samba AD before you start your DC the first time. It's a good idea to finish this task now. If you decided to run the internal or no DNS server on this host, no further steps are required.

DNS resolving

Many things in an Active Directory, not only the join process, rely on DNS. Therefore it is required that the new host is able to resolve AD DNS zones. To accomplish this, we use a DNS server on one of your existing Domain Controllers.

On Linux and Unixes, you usually configure DNS settings in /etc/resolv.conf:

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

Some tools like NetworkManager may overwrite manual changes in that file. Please consult your distributions documentation for configuring name resolution.

To verify a correct name resolution, try resolving the hostname of one of your existing Domain Controllers:

```
# host -t A DC1.samdom.example.com
DC1.samdom.example.com has address 10.99.0.1
```

Kerberos

Kerberos, which is also a very important part in an AD, needs to be configured next. Add the following content to /etc/krb5.conf:

```
[libdefaults]
    dns_lookup_realm = false
    dns_lookup_kdc = true
    default_realm = SAMDOM.EXAMPLE.COM
```

To verify the correct setup, use "kinit" to obtain a Kerberos ticket:

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

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

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

Valid starting       Expires              Service principal
24.09.2015 19:56:55  25.09.2015 05:56:55  krbtgt/SAMDOM.EXAMPLE.COM@SAMDOM.EXAMPLE.COM
        renew until 25.09.2015 19:56:53
```

Join the existing domain as a Domain Controller

Before you start, make yourself familiar with the possible parameters and options of the join process:

```
# samba-tool domain join --help
```

If your new Domain Controller has multiple network interfaces, the following two "samba-tool" options are required to prevent it 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 join ..... --option="interfaces=lo eth0" --option="bind interfaces only=yes"
```

Join the existing domain (parameter explanation below):

```
# samba-tool domain join samdom.example.com DC -Uadministrator --realm=SAMDOM.EXAMPLE.COM --dns-backend=SAMBA_INTERNAL
Finding a writeable DC for domain 'samdom.example.com'
Found DC dc1.samdom.example.com
Password for [WORKGROUP\administrator]:
workgroup is SAMDOM
realm is samdom.example.com
checking sAMAccountName
Adding CN=DC2,OU=Domain Controllers,DC=samdom,DC=example,DC=com
Adding CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdom,DC=example,DC=com
Adding CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdom,DC=example,DC=com
Adding SPNs to CN=DC2,OU=Domain Controllers,DC=samdom,DC=example,DC=com
Setting account password for DC2$
Enabling account
Calling bare provision
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
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Provision OK for domain DN DC=samdom,DC=example,DC=com
Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[402/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[804/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[1206/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[1550/1550] linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[402/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[804/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[1206/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[1608/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[1618/1618] linked_values[38/0]
Replicating critical objects from the base DN of the domain
Partition[DC=samdom,DC=example,DC=com] objects[100/100] linked_values[23/0]
Partition[DC=samdom,DC=example,DC=com] objects[387/287] linked_values[23/0]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=samdom,DC=example,DC=com
Partition[DC=DomainDnsZones,DC=samdom,DC=example,DC=com] objects[41/41] linked_values[0/0]
Replicating DC=ForestDnsZones,DC=samdom,DC=example,DC=com
Partition[DC=ForestDnsZones,DC=samdom,DC=example,DC=com] objects[19/19] linked_values[0/0]
Committing SAM database
Sending DsReplicaUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
Setting up secrets database
Joined domain SAMDOM (SID S-1-5-21-469703510-2364959079-1506205053) as a DC
```

Parameter explanations:

- Domain: AD Domain Name
- Server Role: "DC" for Domain Controller
- Username: Account that is allowed to join new Domain Controllers. Typically it is at least the Domain Administrator.
- Realm: Kerberos Realm written in upper case.

- DNS backend: Supported DNS backends are the Samba internal DNS server and BIND9_DLZ. We used the default - the internal DNS - in our above example. Even though it's the default, we used this parameter to show users how to set a different DNS backend. The internal DNS 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 choose BIND9_DLZ as the 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! Given that this is at least your second DC in your AD forest, you can also choose NONE here. However, for failover reasons it is recommended to have at least two AD DNS servers in your network.
- Site: If you have setup Active Directory Sites, it's possible to join a new DC directly into a specified AD site by using the "--site=SITE" parameter.

Check DNS entries

This is a very important step, so don't skip it!

For a working replication, it is required that all DC related DNS records were added to the DNS zones during the join. Check, if they are existing and if not (Bug #10928 (https://bugzilla.samba.org/show_bug.cgi?id=10928)), add them manually.

Adaptations for the BIND DNS backend

Skip this step, if you're not using BIND as DNS backend

Workaround: Fix keytab permissions

This fix is only required, if joining the domain with a Samba version prior to 4.4. Wrong keytab permissions will prevent BIND updating your AD DNS zones. One of the results will be that "samba_dnsupdate" can't add important DNS entries, that clients query to locate the new Domain Controller!

Fix permissions on the "dns.keytab" file, to allow BIND to read this file:

```
# chmod 640 /usr/local/samba/private/dns.keytab
# chgrp named /usr/local/samba/private/dns.keytab
```

Note: If you use Samba packages, make sure that the account BIND uses, is able to access the dns.keytab file. Some package installations set too restrictive permissions on higher folders.

Enable the correct BIND9_DLZ module

Samba is shipped with BIND9_DLZ modules for different BIND versions. You have to enable the right one in /usr/local/samba/private/named.conf (uncomment the right one and comment the others):

```
dlz "AD DNS Zone" {
    # For BIND 9.8.0
    database "dlopen /usr/local/samba/lib/bind9/dlz_bind9.so";

    # For BIND 9.9.0
    # database "dlopen /usr/local/samba/lib/bind9/dlz_bind9_9.so";

    # For BIND 9.10.0
    # database "dlopen /usr/local/samba/lib/bind9/dlz_bind9_10.so";
};
```

The example above enables the module for BIND 9.8.x (default).

GID mappings of built-in groups

If you are using a version of Samba before 4.2.0, or are using the builtin winbind instead of the separate winbindd, there are issues with GID mappings of built-in groups. The GIDs of groups owning files and directories in the SYSVOL folder may differ between Domain Controllers, as Samba doesn't replicate these GIDs! From Samba version 4.2.0, the separate winbindd daemon is used instead of the built-in winbind and this is able to display the built-in group names instead of just the GID number.

If you are using a Samba version before 4.2.0 or are using the built-in winbind, you will need to use the following workaround:

NOTE: Only do this if you are running a version of Samba before 4.2.0 or are using the built-in winbind.

- Create a hot-backup of "idmap.ldb" on one of your other Samba Domain Controllers:

```
# tdbbackup -s .bak /usr/local/samba/private/idmap.ldb
```

- Move the created backup file "/usr/local/samba/private/idmap.ldb.bak" to "/usr/local/samba/private/" on the new joined Domain Controller and remove the .bak suffix, to replace the existing file.
- Reset the ACLs on the local SYSVOL folder of the new joined Domain Controller:

```
# samba-tool ntacl sysvolreset
```

Start Samba

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.

Directory replication

A few minutes after you have started Samba, connections with other DCs will be established automatically.

```
# samba-tool drs showrepl
Default-First-Site-Name\DC2
DSA Options: 0x00000001
DSA object GUID: c14a774f-9732-4ec2-b9fa-2156c95c4e48
DSA invocationId: 7bdb135c-6868-4dd9-9460-33dea4b6b87b

==== INBOUND NEIGHBORS ====

CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ Thu Sep 24 20:08:46 2015 CEST was successful
                0 consecutive failure(s).
                Last success @ Thu Sep 24 20:08:46 2015 CEST

DC=DomainDnsZones,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
                0 consecutive failure(s).
                Last success @ Thu Sep 24 20:08:45 2015 CEST

CN=Configuration,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ Thu Sep 24 20:08:46 2015 CEST was successful
                0 consecutive failure(s).
                Last success @ Thu Sep 24 20:08:46 2015 CEST

DC=ForestDnsZones,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
                0 consecutive failure(s).
                Last success @ Thu Sep 24 20:08:45 2015 CEST

DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
                0 consecutive failure(s).
                Last success @ Thu Sep 24 20:08:45 2015 CEST

==== OUTBOUND NEIGHBORS ====

CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=DomainDnsZones,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

CN=Configuration,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ NTTIME(0) was successful
```

```
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=ForestDnsZones,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
        Connection name: fb03f58b-1654-4a02-8e11-f0ea120b60cc
        Enabled        : TRUE
        Server DNS name : DC1.samdom.example.com
        Server DN name  : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdo
                TransportType: RPC
                options: 0x00000001
Warning: No NC replicated for Connection!
```

Depending on your replication settings it may take a few minutes until all connections are established. So please be patient! On the long shot that the outbound connections aren't established automatically - not even after several minutes - you can force the replication (generally not necessary!). See samba-tool drs replicate.

Note: The message "Warning: No NC replicated for Connection!" can be safely ignored. See FAQ: Message: Warning: No NC replicated for Connection!

Start BIND

Skip this step if not using BIND9_DLZ as DNS backend.

Check that the DNS partitions are already replicated:

```
# samba-tool drs showrepl
...
==== INBOUND NEIGHBORS ====
...
DC=DomainDnsZones,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
                0 consecutive failure(s).
                Last success @ Thu Sep 24 20:08:45 2015 CEST
...
DC=ForestDnsZones,DC=samdom,DC=example,DC=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: 4a6bd92a-6612-4b15-aa8c-9ec371e8994f
                Last attempt @ Thu Sep 24 20:08:45 2015 CEST was successful
                0 consecutive failure(s).
                Last success @ Thu Sep 24 20:08:45 2015 CEST
```

If replication is working, start BIND.

Testing the local DNS

Skip this step, if you have choosen "NONE" as DNS backend during the join.

To test that the local DNS is working properly, run the following commands on the new DC, to query the local DNS

```
$ host -t A dc1.samdom.example.com localhost
Using domain server:
Name: localhost
Address: 127.0.0.1#53
Aliases:

dc1.samdom.example.com has address 10.99.0.1
```

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

Best practice: DNS configuration on DCs

It is not just on Workstations that you should configure at least two AD DNS servers. On Domain Controllers it is even more important, because if just one DNS is configured and that one fails, services relying on DNS, such as directory replication, will also fail!

A best practice for DNS configuration on DCs is, that you don't define the IP of the local DNS as the first nameserver. This could lead into problems like DNS islanding (http://retrohack.com/a-word-or-two-about-dns-islanding) .

Example configuration:

/etc/resolv.conf on DC1:

```
nameserver 10.99.0.2       # IP of the other DC as first entry
nameserver 10.99.0.1       # IP of this DC as second entry
search samdom.example.com
```

/etc/resolv.conf on DC2:

```
nameserver 10.99.0.1       # IP of the other DC as first entry
nameserver 10.99.0.2       # IP of this DC as second entry
search samdom.example.com
```

If you have more than two DCs, you can configure the nameserver IPs in crosswise direction. However you shouldn't set the local DNS as first entry!

SYSVOL replication

At the current stage of Samba, SYSVOL replication isn't implemented. Until it is, if you make any changes on that share, you will have to keep them in sync on all your Domain Controllers. An example of how to achieve this in an easy and automated way between Samba DCs, can be found in the Rsync based SYSVOL replication workaround documentation. For a workaround with a Windows DC, see Robocopy based SysVol replication workaround.

Some pages on the internet recommend using a distributed filesystem like GlusterFS, Lustre, etc. to automatically mirror the content of the SYSVOL share. **The Samba team strongly advises not to do this, because a cluster file system, used with Samba, requires a CTDB setup, that is not compatible with the Samba Active Directory Domain Controller!**

Testing directory replication

To check that replication is working correctly between your Domain Controllers, try adding/modifying e. g. a user on one DC using either the Samba command line tools (samba-tool, ldbedit) or the Windows GUI admin tools. Then check that the changes shows up within a few seconds on the new Domain Controller.

ldapcmp

An alternative to compare two directories is samba-tool ldapcmp.

Troubleshooting

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