univention
be open.

Univention Corporate Server

Operation of a Samba domain based on Windows NT domain services

Table of Contents

1. Components of a Samba domain 4
2. Installation 5
3. Services of a Samba domain 6
    3.1. Authentication services 6
    3.2. File services 6
    3.3. Print services 6
    3.4. NetBIOS name service 6
    3.5. Name resolution using WINS 7
4. Configuration and management of Windows desktops 8
    4.1. Logon scripts / NETLOGON share 8
    4.2. Configuration of the file server for the home directory 8
    4.3. Roaming profiles 8
5. Trust relationships 10
    5.1. Windows domain trusts Samba domain 10
    5.2. Samba domain trusts Windows domain 10
Bibliography 12

Chapter 1. Components of a Samba domain

NT domains are the predecessor of Active Directory from a technical perspective. This document is predominantly relevant for existing installations which have yet to perform migration to an AD-based domain. Migration from a NT-based Samba domain to a domain with Active Directory services is described in the Univention Wiki [wiki-samba-update]. For new installations, we highly recommend the use of an AD-based domain.

A Samba NT domain is composed of at least one domain controller. Windows clients and member servers can join the trust context of the Samba domain as domain members. Member servers do not provide login services, but may offer file and print services, for example. In addition to a member server domain join of Windows Server systems, Samba can also act as a member server.

Domain joining of Windows clients and Microsoft Windows member servers is described in chapter *Domain services / LDAP directory* of the UCS manual [ucs-handbuch].

Microsoft Windows domain controllers cannot join the Samba domain.

Chapter 2. Installation

Samba as a NT domain controller can be installed on all UCS domain controllers by installing the software package ***univention-samba***. (`univention-run-join-scripts` command must be run after installation). Additional information can be found in chapter *Software deployment* of the UCS manual [ucs-handbuch].

A Samba member server can be installed on UCS member servers from the Univention App Center with the application *Windows-compatible fileserver*. Alternatively, the software package ***univention-samba*** can be installed (`univention-run-join-scripts` command must be run after installation). Additional information can be found in chapter *Software deployment* of the UCS manual [ucs-handbuch].

Chapter 3. Services of a Samba domain

3.1. Authentication services

Feedback

User logins can only be performed on Microsoft Windows systems joined in the Samba domain. Domain joins are documented in the chapter *Domain services / LDAP directory* of the UCS manual [ucs-handbuch].

The user passwords are saved in the UCS LDAP. Users are authenticated against the LDAP directory when logging into the domain with their username and password, and can then access all the shared resources of the domain without having to enter their username and password again. Computers with any kind of Windows operating systems are authenticated in the same way as in Windows NT domains, via the `NTLMv2` protocol.

3.2. File services

Feedback

A file server provides files over the network and allows concentrating the storage of user data on a central server.

The file services integrated in UCS support the provision of shares using the CIFS protocol. Insofar as the underlying file system supports Access Control Lists (ACLs) (can be used with ext3, ext4 and XFS), the ACLs can also be used by Windows clients.

Samba supports the CIFS protocol and the successor SMB2 to provide file services. Using a client which supports SMB2 (as of Windows Vista, i.e., Windows 7/8 too) improves the performance and scalability.

The protocol can be configured using the Univention Configuration Registry variable `samba/max/protocol`. It must be set on all Samba servers and then all Samba server(s) restarted.

- **NT1** configures CIFS (supported by all Windows versions)
- **SMB2** configures SMB2 (supported as of Windows Vista/Windows 7)
- **SMB3** configures SMB3 (supported as of Windows 8) (currently not covered by Univention support)

3.3. Print services

Feedback

Samba offers the possibility of sharing printers set up under Linux as network printers for Windows clients. The management of the printer shares and the provision of the printer drivers is described in chapter *Print services* of the UCS manual [ucs-handbuch].

3.4. NetBIOS name service

Feedback

NetBIOS is a network protocol for host names and for network communication of Windows clients. It is primarily used for NT-compatible domains; the name resolution in Active Directory is based on DNS. Samba provides NetBIOS functions with the `nmbd` system service.

NetBIOS computer names can have a maximum of 13 characters. The NetBIOS name of a UCS system corresponds to the host name by default.

In a native Active Directory environment, there are no NetBIOS services provided as standard. In an AD environment based on Samba, however, it is activated. This can be deactivated with the Univention Configuration Registry variable `samba4/service/nmb`.

3.5. Name resolution using WINS

Feedback

Similar to DNS in TCP/IP networks, the *Windows Internet Name Service (WINS)* is used for resolving NetBIOS names into IP addresses. In addition, WINS provides information on the services of the hosts.

WINS is used in NT-compatible Samba domains; in Samba AD domains, the name resolution generally occurs primarily via DNS (WINS is also available).

WINS support is activated on the master domain controller in the default setting and can also be operated on another server by setting the Univention Configuration Registry variable `windows/wins-support`. WINS can only be operated without adjustments on one Samba server in the domain; distribution across several servers requires the setup of WINS replication. Information on the commissioning of the WINS replication can be found in the Univention Support database at SDB 1107.

The WINS server can be assigned to Windows clients via a *DHCP-NetBIOS* policy, see chapter *IP and network management* of the UCS manual [ucs-handbuch].

http://sdb.univention.de/1107

Chapter 4. Configuration and management of Windows desktops

4.1. Logon scripts / NETLOGON share

Feedback

The NETLOGON share serves the purpose of providing logon scripts in Windows domains. The logon scripts are executed following after the user login and allow the adaptation of the user's working environment. Scripts have to be saved in a format which can be executed by Windows, such as *bat*.

The directory `/var/lib/samba/netlogon` is set up as the Samba share *NETLOGON*.

In the default setting, all adjustments are made in the `/var/lib/samba/netlogon/` directory on the master domain controller and synchronized hourly on all domain controllers with Samba installed via the `rsync` tool.

The Univention Configuration Registry variable `samba/logonscript` is available for defining a global logon script for all users. If this variable is set on a Samba server, then all users logging into this Samba server have the specified logon script assigned. The logon script can also be assigned user-specifically in the Univention Management Console.

4.2. Configuration of the file server for the home directory

Feedback

As standard, the home directory of each user is shared by Samba and connected with the *I:* drive after login in Windows.

The Univention Configuration Registry variable `samba/homedirserver` can be used to specify the server on which the home directories should be stored; the Univention Configuration Registry variable `samba/homedirpath` can be used to specify the directory. These values will then be valid for all the users.

It it also possible to make individual assignment in the user settings in the Univention Management Console with the setting **Windows home path**, e.g., **`\\ucs-file-server\smith`**.

If instead of the user's UNIX home directory, a different UNIX directory is to be displayed as the home directory on the Windows drive, then this server and the home directory need to be entered in the **Windows home path** entry field.

4.3. Roaming profiles

Feedback

Samba supports roaming profiles, i.e., user settings are saved on a central server. This directory is also used for storing the files which the user saves in the *My Documents* folder. Initially, these files are stored locally on the Windows computer and then synchronized onto the Samba server when the user logs off.

If the profile path is changed in the Univention Management Console, then a new profile directory will be created. The data in the old profile directory will be kept. These data can be manually copied or moved to the new profile directory. Finally, the old profile directory can be deleted.

The user profiles are saved in the `windows-profiles\<Windows-Version>` subdirectory on the Samba server that the user logged on to.

Univention Configuration Registry variable `samba/profileserver` can be used to specify another server and `samba/profilepath`to specify another directory. These settings must be set on all Samba domain controllers.

In the user management of the Univention Management Console, the input field **Windows profile directory** can be set to configure a different path or another server for the profile directory for the user.

Roaming profiles can be deactivated by configuring the Univention Configuration Registry variables `samba/profilepath` and `samba/profileserver` to *local* and restarting the Samba server. The UMC setting from the input field **Windows profile directory** must also be set empty.

Chapter 5. Trust relationships

Trust relationships between domains make it possible for users from one domain to log on to computers from another domain.

Trust settings are not supported by in Samba domains based on Active Directory.

If a Windows domain trusts a Samba domain, there is also the possibility to log on to the Samba domain alongside the Windows domain when logging on to computers belonging to the Windows domain.

If a Samba domain trusts a Windows domain, users from the Windows domain enter the user name *<name-of-windows-domain>+<username>* when logging on to a Linux computer belonging to the Samba domain.

When setting up and using the trust relationship the domain controllers of both domains must be able to reach each other over the network and identify each other using broadcasts or WINS.

Two steps generally need to be performed to establish a trust relation:

- A domain trust account needs to be created in the "trusted" domain.
- The trust relation needs to be established in the "trusting" domain. This is done by logging in to the "trusting" domain with administrative privileges and running the tool for domain trust administration provided by the domain controller (Microsoft Windows or Samba) to establish an "outgoing" trust (as it is called in the Microsoft terminology). The credentials of the trust account for the "trusted" domain need to be entered. This trust account is required by the "trusting" domain for name resolution in the "trusted" domain.

Trust relations can be configured unidirectional or bidirectional. Technically a bidirectional trust is simply realized as two unidirectional trusts; one in each direction.

The terminology of unidirectional trusts depends on the perspective of either the "trusting" or the "trusted" domain. From the perspective of the "trusting" domain the trust is called "outgoing". From the perspective of the "trusted" domain the trust is called "incoming".

Further information on the configuration of trust relationships on Microsoft Windows can be found in [windows-trust].

5.1. Windows domain trusts Samba domain

Feedback

A *Domain Trust Account* with a name reflecting the NetBIOS name of the Windows domain and a password issued for the account must be created in the computer management module of Univention Management Console The password quality requirements which may apply to Windows domains must be observed.

Trust settings can only be set up on domain controllers.

An outgoing trust relationship must be created on the Windows PDC.

The trust relationship between the Windows domain and the Samba domain can be removed by deleting the trust relationship on the Windows PDC and the domain trust account in the Univention Management Console.

5.2. Samba domain trusts Windows domain

Feedback

The following steps are used to set up the trust setting on a slave domain controller as a *root* user:

The ***winbind*** package must be installed. Winbind maps UNIX IDs to Windows users and groups

An incoming trust relationship must be created on the Windows PDC.

If Univention Firewall is used, replies to NetBIOS broadcasts need to be allowed:

```
echo "iptables -I INPUT 1 -p udp --sport 137 -j ACCEPT" \
    >> /etc/security/packetfilter.d/50_local.sh
/etc/init.d/univention-firewall restart
```

The trust relationship is now initiated and Winbind restarted. This command must be run on all Samba login servers:

```
net rpc trustdom establish <Windows domain>
net setauthuser -UAdministrator (enter the Windows Administrator
 password)
ucr set samba/winbind/rpc/only=yes
/etc/init.d/winbind restart
ucr set auth/methods="krb5 ldap unix winbind"
/etc/init.d/nscd restart
```

The following command can be used to check that the trust relationship has been added correctly:

```
net rpc trustdom list
```

Bibliography

[ucs-handbuch] Univention GmbH. 2015. *Univention Corporate Server - Manual for users and administrators*. https://docs.software-univention.de/manual-4.2.html.

[wiki-samba-update] Univention GmbH. 2013. *Univention Wiki - Migration from Samba 3 to Samba 4*. http://wiki.univention.de/index.php?title=Migration_from_Samba_3_to_Samba_4.

[windows-trust] Microsoft Support. 2007. *How to establish trusts with a Windows NT-based domain in Windows Server 2003*. https://support.microsoft.com/en-us/kb/325874.