Active Directory Domain Services
Administration of Different Clients, a SAN and a Cluster File System
Software Installation Guide
Active Directory Domain Services

This Software Installation Guide informs you about how to install and configure the applications to administer several clients with the operating systems Windows, Mac and Linux (Red Hat Enterprise Linux 6.x), a SAN, and the cluster file system StorNext by Quantum via a single Active Directory.

This document deals with the following topics:

- Installation of the Active Directory Domain Services on page 1-2
  - Configuring the Server on page 1-2
  - Configuring the Server for Unix/Linux-based Operating Systems on page 1-11
- Joining a Windows Client to the Active Directory on page 1-13
- Joining a Mac OS Client to the Active Directory on page 1-16
- Joining a Linux Client (RHEL 6.x) to the Active Directory on page 1-20

This document provides only a part of the information needed to install the Active Directory and joining all clients to it. It does not deal with e.g. all variations of operating systems or detailed configurations that have to be made in specific files. The various operating systems or versions may require different setups. Profound skills and experience in system and domain administration are mandatory. If you are not sure about the correct installation or in case of malfunctions, please contact the DVS service department.

To complete the tasks described in the following, some user entries are required. For this follow the information in this document and/or the instructions given on the screen.

The domain controller is provided by Windows Server 2008 which includes the Active Directory and the DNS server. It is required to have Windows Server 2008 installed on your system. Under Red Hat Linux the latest Samba version should be installed in addition.

Once a direct access from client to storage is made via Fibre Channel, it can only be restricted manually.
1 Installation of the Active Directory Domain Services

Install the Active Directory Domain Services as detailed below and observe the following in particular:

---

**NOTICE**

**Disconnection due to time difference between clients**

A difference of more than five minutes between the clients’ local clocks may disconnect the respective client.

*To ensure a connection of clients to the Active Directory, it is necessary to set all clients’ local clocks to the same time of day.*

---

**Information**

It is recommended to use only one network card or, in case of several network cards, to limit the IP addresses that the server has to listen on for DNS queries to only a specific one.

---

1.1 Configuring the Server

A static IP address has to be assigned to the server first, otherwise the installation of the Active Directory will not work. If you haven’t done this yet, perform the following:

1. Go to **Start >> Control Panel >> Network and Sharing Center.**

2. Click through the respective options until you arrive at the internet protocol properties.
3. Enter the static IP address that has to be assigned to the server in the respective field.

The local host (127.0.0.1) can be assigned as DNS server. After the installation of the DNS server this would happen automatically.

Now the installation of the Active Directory can be performed on the server:

4. Navigate to **Start >> Execute** and enter `dcpromo` in the command line. To confirm press [Enter] on your keyboard.

This will start the installation wizard of the Active Directory Domain Services (ADDS) as follows:
5. Click on the button **NEXT** to continue in the standard installation mode.

6. Select the option to create a new domain in a new forest and press the button **NEXT** to continue.
7. Enter the name for the root domain in the forest.

The picture above shows an example for a possible naming.

8. Press the button **NEXT** to continue.

9. Set the forest’s functional level to e.g. **Windows Server 2008** and press the button **NEXT** to continue.
The window to set additional domain controller options will appear on the screen:

10. Select the following check boxes if selectable and/or not selected yet:
   - DNS server (mandatory, usually selected as default when no DNS server has been installed before)
   - Global Catalog (usually selected as default when it is the first domain controller in the forest)

    The check box **Read-only domain controller** is disabled in this case.

11. Press **NEXT** to continue.

    At this point an error message may appear if a second network card configured as DHCP is active. IPV6 should be deactivated as well.
Excursus: Dealing with the Network Error Message

To correct the cause for the error message it is necessary to e.g. limit the IP addresses to a specific one. This happens on the server. Perform the following:

1. Navigate to **Start >> Programs >> Administrative Tools >> DNS** and then to the window providing the properties.

The following will appear on the screen:

![Image of DNS properties window](image)

2. Go to the tab **Interfaces**, select **Only the following IP addresses** and enter the respective IP address the server has to listen on for DNS queries in the respective entry field. Press the button **OK**.

With this the cause for the error message should be resolved. You can now go back to the installation wizard of the Active Directory to continue with the installation.
Continuing the Installation of the ADDS

If only one network card is active, the limitation of IP addresses is not necessary. Instead of performing the steps described in the excursus, you can continue with the installation. The following window will appear on the screen:

12. Enter or browse to the location for the database folder, the log files and the SYSVOL folder and press the button NEXT to continue.
13. Enter an administrator password for the restore mode in the following window and continue with **NEXT**. This password will be used to start ADDS in Directory Service Restore Mode (DSRM) for tasks that must be performed offline.

The last window that appears before the installation begins, is a summary of all options that have been selected.

14. Press the button **NEXT** to initiate the installation process of the Active Directory.

Several windows will be displayed on the screen that indicate the state of the installation process.

15. Do not perform any commands, wait until you see the following on the screen:
16. Press the button **FINISH** to continue.

It is necessary to restart the server. In the following window the system will prompt you to do so.

17. Click on the button **RESTART NOW** to restart the server and, by doing so, applying the configurations to it.

Now a user account has to be created on the server to ensure the LDAP access.

18. Navigate to **Start >> Programs >> Administrative Tools >> Active Directory Users and Computers.**

19. Click through the options until you arrive at the window shown in the figure below:
20. Set the user name and the password in the respective entry fields.

In this example the user’s name has been set Idapreader. It is important to assign a safe password and to ensure that it does not expire. The other options have to be set as shown in the figure above.

After having finished all the steps as described above, the Active Directory should now be installed. Now the server configurations for the Unix/Linux-based clients have to be made.

### 1.2 Configuring the Server for Unix/Linux-based Operating Systems

Before a Mac OS or Linux client can be joined to the Active Directory the roles have to be assigned first. To do so, the Identity Management for Unix is required which can be added as follows on the server:

1. Navigate to Start >> Programs >> Administrative Tools >> Server Manager and expand Roles in the tree pane.

You will see the following on your screen:
2. Select **Identity Management for UNIX** and click **Add Role Services** in the ‘Role Services’ section. This will open the window ‘Add Role Services’.

3. Select the Identity Management for UNIX role services that you want to install on the ‘Select Role Services’ page by clicking in the respective check box. Press the button **NEXT** to continue. This will open the installation wizard.

4. If the wizard prompts you to install any other role services that are required by Identity Management for UNIX components, click **YES**.

5. After verifying your selections on the ‘Confirm Installation Selections’ page, click **INSTALL**. This will initiate the installation.

6. Click **CLOSE** when the installation is completed, and press **YES** to restart the server. After having restarted the server all installed configurations should apply.
2 Joining a Windows Client to the Active Directory

To make a Windows client available in the Active Directory and enable the user(s) to log in, the system must be added to the Active Directory. Therefore, the domain controller and the DNS must be installed correctly. The operating systems Windows 7 Home Premium and Basic cannot be joined to the domain. It is required to use Professional, Enterprise or Ultimate. To join a Windows client to the Active Directory perform the following on the client:

1. Navigate to **Start >> Control Panel >> System** and click on the option **Change settings**.
   This will open the following window:
2. Select the tab **Computer Name** and click on the button **CHANGE...**

The following window will appear on the screen:

3. Enter the name of the computer, e.g. `pc1` in the respective entry field.
4. Enter the name of the domain, e.g. dvssan.local in the entry field under the selected point **Domain** and press the button **OK**. This will initiate the search for the domain controller.

When the domain controller has been found, a login window appears on the screen.

5. Enter the administrator name and the password and press the button **OK**. The system will display a message to confirm your login and prompt you to restart.

After having performed a restart the Windows client should be joined to the Active Directory.
3 Joining a Mac OS Client to the Active Directory

After all necessary settings have been made on the server, the client can be joined to the ADDS. This happens directly on the client.

To join the Mac OS client to the Active Directory perform the following:

1. Navigate to **System Preferences >> Network**.

The window for the network configuration will appear on the screen as follows:

2. Press the button **ADVANCED...** on the lower right.

3. Add the DNS to the search domains and press the button **OK**.
4. Now go back to the 'System Preferences' window and select Accounts. Press the button Edit... in the 'Accounts' window. You will see the window 'Directory Utility' as shown in the figure below:

5. Select the line Active Directory in the listing box under Name and press the button showing a pencil to the lower left, below the listing box. This will open the 'Directory Utility' editing window where you can enter the Active Directory forest and domain. The figure below shows an example:
6. Select the following check boxes in the tab **User Experience** if not selected yet:
   - Create mobile account at login
   - Use UNC path from Active Directory to derive network home location
   - Default user shell

7. When having selected the check boxes, go to the tab **Mappings** by clicking on it.

8. Select the following check boxes if not selected yet:
   - Map UID to attribute
   - Map user GID to attribute
   - Map group GID to attribute

9. Enter the following in the entry fields to the right of the check boxes:
   - uidNumber to the right of **Map UID to attribute**
   - gidNumber to the right of **Map user GID to attribute**
   - gidNumber to the right of **Map group GID to attribute**

10. Click on the button **BIND...** in the middle right of the 'Directory Utility' window to join the Mac OS client to the Active Directory.

This will open a login window with a request for the domain administrator name and password.

11. Enter the requested data and press **OK**.
With this the Mac client should be joined to the Active Directory.

To check if all steps have worked successfully perform the following:

12. Go back to the 'System Preferences' window and select **Accounts**.

13. Press the button **Edit...** in the 'Accounts' window.
You will see the window 'Directory Utility' as shown in the figure below:
14. Click on **DIRECTORY EDITOR** to the top left of the window.

In the middle left of the window you will see a listing of all joined clients to the Active Directory. By selecting **Users** or **Groups** next to the drop-down list **Viewing**, the display can be adjusted to your requirements. If the Mac client appears in the listing, the steps performed as described above should have worked successfully.

Before a user can log in on the client some configurations have to be made. This is to ensure working with the correct access rights when writing data on the SAN via Fibre Channel.

The default setting for the umask on Mac OS systems is 022. That means, only the holder of the file has read and write permissions. The group has only read permissions. To assign write permissions to the group, two files (`launchd-user.conf` and `launchd.conf`) have to be created in the `/etc` directory to set the umask 002 for the users.

The figure below shows an example:

```bash
sh-3.2$ cd /etc
sh-3.2$ ls -al
launchd-user.conf launchd.conf localtime locat
sh-3.2$ ls -al
launchd-user.conf launchd.conf localtime locat
sh-3.2$ ls -al launchd
-rw-r--r-- 1 root wheel 11 Aug 30 09:05 launchd-user.conf
-rw-r--r-- 1 root wheel 11 Aug 30 09:06 launchd.conf
sh-3.2$ cat launchd-user.conf
umask 002

sh-3.2$ cat launchd.conf
umask 002

sh-3.2$ 
```

Finally, the mount point must be defined and the so called sticky bit assigned to the group. This is necessary, to ensure that always the same and wanted group writes on the storage.

15. To set the sticky bit in the mounted directory enter the command:

```
Chmod -R g+s.
```
### Joining a Linux Client (RHEL 6.x) to the Active Directory

To join a Linux (RHEL 6.x) client with Samba to the Active Directory and configure it properly, the standard installation of a Red Hat Linux Enterprise and the latest Samba version are necessary. Sometimes it is required to deinstall the previously installed versions before installing the latest programs. In addition a static IP address should be assigned. This all has to be performed directly on the client.

To join a Linux (RHEL 6.x) client with Samba to the Active Directory, the following data files need to be configured:

- `resolv.conf`
- `nsswitch.conf`
- `krb5.conf`
- `smb.conf`
- `ns1cd.conf`
- `pam_ldap.conf`
- `ldap.conf`

To validate if the Active Directory and Samba are connected the following commands can be used:

- `wbinfo -u`
- `wbinfo -g`
- `getent group`
- `getent passwd`

These commands can be used when Linux has been joined to the domain and the LDAP client has been configured appropriately. For this, the DNS has to be connected to the Linux client.

In addition, the Linux client and the DNS server must be synchronized. The command to set the time of a Linux Client is:

```
ntpdate name-of-ntp-server
```

The runlevel, in this case level 5, must be adjusted for Samba and Winbind. If this doesn’t happen, the services will not initiate automatically when rebooting the system the next time. This can be performed manually by using symbolic links or the command line tool `chkconfig` as follows:

```
chkconfig smb on
```
chkconfig winbind on

Furthermore, it must be checked if Windbind exists or is linked correctly and therefore the `nsswitch.conf` is able to work as shown below:

```
[root@system /]# ldconfig -v | grep winbind
    libnss_winbind.so.2 -> libnss_winbind.so.2
```

After a restart of both services the communication with the Active Directory should be set up. Perform the following:

1. Restart both services.
2. Enter the command `kinit` to issue a ticket.
3. Enter the command `klist` to view the ticket.

If joining the client to the domain has been finished successfully, the first permissions can be set as follows:

```
kinit Administrator@DVSSAN.LOCAL
nen ads join -U Administrator
```

To ensure that the client has been joined correctly, the output should look as follows:

```
... 
[root@system /]# getent group
nsccd:x:28:
ldap:x:55:
screen:x:84:
Domain Admins:*:10001:
Domain Users:*:10000:

[root@system /]# getent passwd
nsccd:x:28:28:NSCD Daemon:/sbin/nologin
nslcd:x:65:55:LDAP Client User:/sbin/nologin
test123:*:10009:10000:test123:/home/test123:/bin/sh
ldapreader:*:10001:10000:ldapreader:/home/ldapreader:/bin/sh
test321:*:10012:10000:test321:/home/test321:/bin/sh
```
testuser:*:10013:10000:Testuser:/home/testuser:/bin/sh

[root@system /]# wbinfo -g
domain computers
domain controllers
schema admins
enterprise admins
cert publishers
domain admins
domain users
domain guests
group policy creator owners
ras and ias servers
allowed rodc password replication group
denied rodc password replication group
read-only domain controllers
enterprise read-only domain controllers
dnsadmins
dnsupdateproxy

# wbinfo -u
administrator
guest
krbtgt
test123
ldapreader
test321
testuser
...

The necessary information are read out of the file *krb5.conf*.
Access rights for groups, users and others are assigned in octal notation. The assignment of access rights should be considered thoroughly. Access restrictions are possible on group as well as on user level. In addition, it is possible to set the group which should be used to generate the data.
To give users the ability of logging in locally the files `/etc/pam.d/ system-auth` and `password-auth` have to be configured. This can be performed manually or via the user interface:

1. Navigate to **System >> Administration >> Authentication**.

2. Configure the files so that the authentication happens via kerberos.

   The mapping of groups and users happens via LDAP, so no local database is needed.

Before a user can log in on the client some configurations have to be made. This is to ensure working with the correct access rights when writing data on the SAN via Fibre Channel. The file is `.bashrc` as indicated in the figure below:

At the bottom of the file the read and write permissions of the group have to be set. By default the umask is set to 022 that gives the group read but no write permissions.

3. Set the umask to 002 to give the group read and write permissions.

   This ensures that all users write data with the same access rights to the SAN. This is especially necessary when data is shared with other users in the same group.
Joining a Linux Client (RHEL 6.x) to the Active Directory