univention
be open.

Univention Corporate Server - Extended Windows integration documentation

Release 5.0

Sep 13, 2023

Contents

1 Advanced Samba documentation

1.1 Operating Samba/AD as a read-only domain controller

Active Directory offers an operating mode called *read-only domain controller* (RODC) with the following properties:

- The data are only stored in read-only format. All write changes must be performed on another domain controller.
- Consequently, replication is only performed in one direction.

A comprehensive description can be found in the Microsoft TechNet Library *AD DS: Read-Only Domain Controllers* [1].

A Samba/AD domain controller can be operated in RODC mode (on a Replica Directory Node for example). Prior to the installation of **univention-samba4**, the Univention Configuration Registry Variable `samba4/role` must be set to `RODC`:

```
$ ucr set samba4/role=RODC
$ univention-install univention-samba4
$ univention-run-join-scripts
```

1.2 Deinstallation of a Samba/AD domain controller

The removal of an Samba/AD domain controller (Active Directory compatible domain controller) is a far-reaching configuration step and should be prepared thoroughly.

If the domain should continue to be provide Active Directory-compatible services, the package **univention-samba4** must remain installed on the Primary Directory Node or a Backup Directory Node system.

Before uninstalling the packages, the domain controller registration must be removed from the Samba/AD database. This can be done with the helper script **purge_s4_computer.py**. It must be run on the Primary Directory Node or a Backup Directory Node system. The query *Really remove Primary Directory Node from Samba/AD?* must be answered with `Yes` and the question *Really remove Primary Directory Node from UDM as well?* must be answered with `No`.

For example:

```
$ /usr/share/univention-samba4/scripts/purge_s4_computer.py --computername=primary
Really remove primary from Samba 4? [y/N]: Yes
If you are really sure type YES and hit enter: YES
Ok, continuing as requested.

[...]
Removing CN=PRIMARY,CN=Computers,$ldap_BASE from SAM database.
Really remove primary from UDM as well? [y/N]: No
Ok, stopping as requested.
```

The Univention S4 connector must be run on the Primary Directory Node or a Backup Directory Node in the domain. After Samba/AD was uninstalled, the Univention S4 connector join script `97univention-s4-connector` should be re-executed on the Primary Directory Node or any Backup Directory Node. This can be done via the Univention Management Console module Domain join[1]:

The FSMO (Flexible Single Master Operations) roles should be checked. In case the roles were provided by the removed DC, they must be transferred, for example:

```
root@backup:~# samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-
↪First-Site-Name,CN=Sites,CN=Configuration,DC=dom
RidAllocationMasterRole owner: CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-
↪First-Site-Name,CN=Sites,CN=Configuration,DC=dom
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-
↪First-Site-Name,CN=Sites,CN=Configuration,DC=dom
DomainNamingMasterRole owner: CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-
↪First-Site-Name,CN=Sites,CN=Configuration,DC=dom
SchemaMasterRole owner: CN=NTDS Settings,CN=PRIMARY,CN=Servers,CN=Default-First-
↪Site-Name,CN=Sites,CN=Configuration,DC=dom

root@backup:~# samba-tool fsmo seize --role=all --force
Will not attempt transfer, seizing...
FSMO transfer of 'rid' role successful
Will not attempt transfer, seizing...
FSMO transfer of 'pdc' role successful
```

(continues on next page)

[1] https://docs.software-univention.de/manual/5.0/en/domain-ldap/domain-join.html#linux-domain-join-umc

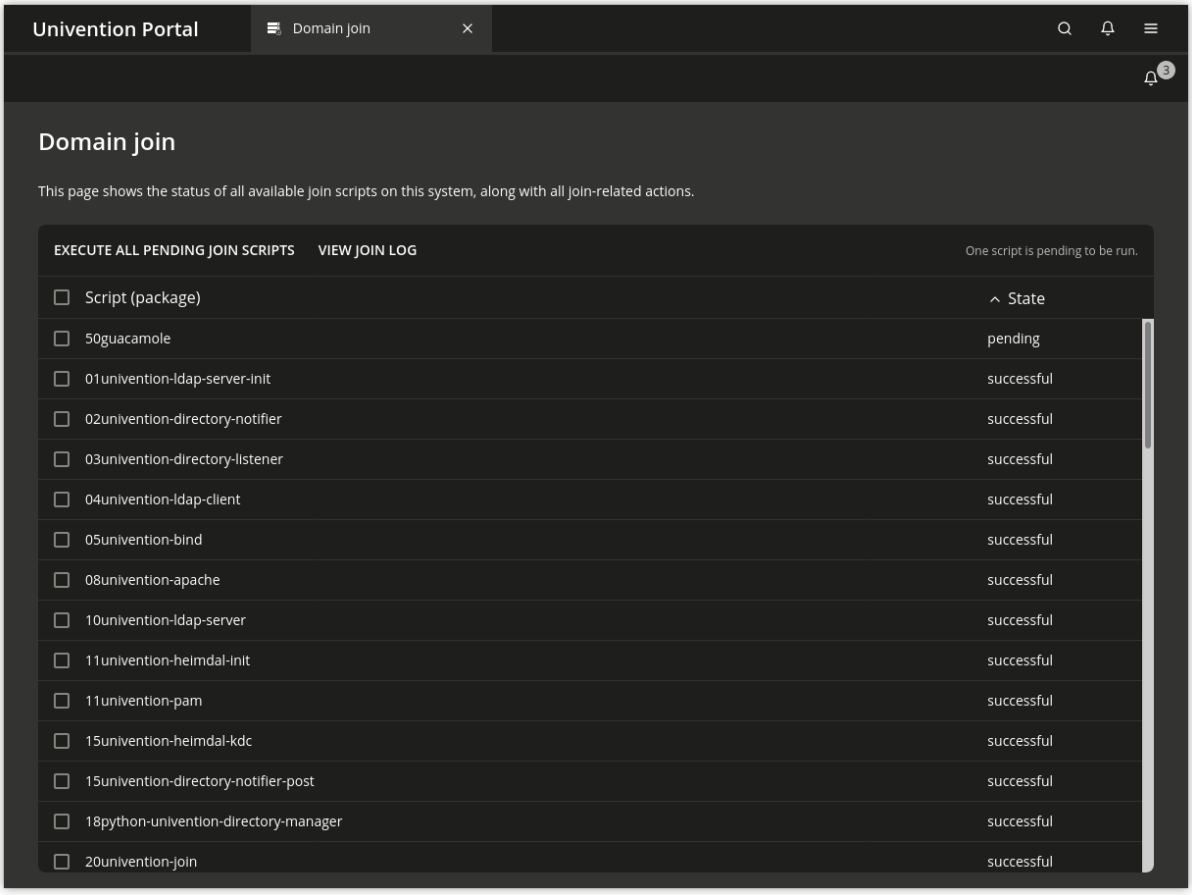

Fig. 1.1: Re-execute S4 connector join script

(continued from previous page)

```
Will not attempt transfer, seizing...
FSMO transfer of 'naming' role successful
Will not attempt transfer, seizing...
FSMO transfer of 'infrastructure' role successful
Will not attempt transfer, seizing...
FSMO transfer of 'schema' role successful
root@backup:~#
```

2 Advanced Active Directory connector documentation

2.1 Synchronization of several Active Directory domains with one UCS directory service

It is possible to synchronize several separate Active Directory domains with one UCS directory service (e.g. to synchronize with an AD forest). One OU (organizational unit) can be defined in LDAP for each AD domain, under which the objects of the respective domains are synchronized. The configuration of further connector instances is not covered by the UMC module.

Several connector instances are started parallel to each other. Each connector instance is operated with a self-contained configuration base. The **prepare-new-instance** script is used to create a new instance, e.g.:

```
$ /usr/share/univention-ad-connector/scripts/prepare-new-instance \
  -a create -c connector2
```

This script creates an additional init script for the second connector instance `/etc/init.d/univention-ad-connector2`, a configuration directory `/etc/univention/connector2` with a copy of the mapping settings of the main connector instance (this can be adapted if necessary) and an array of internal runtime directories.

The additional connector instances are registered in the Univention Configuration Registry Variable `connector/listener/additionalbasenames`.

If SSL is used for the connection encryption, the exported Active Directory certificate must be converted via **openssl** into the required format, for example:

```
$ openssl x509 -inform der -outform pem -in infile.cer -out ad-connector2.pem
```

The filename of the converted certificate then needs to be stored in Univention Configuration Registry:

```
$ univention-config-registry set \
  connector2/ad/ldap/certificate=/etc/univention/ad-connector2.pem
```

If a UCS synchronization is performed towards Active Directory, the replication of the listener module must be restarted after a further connector instance is created. To this end, the following command must be run:

```
$ univention-directory-listener-ctrl resync ad-connector
```

The command line tools which belong to the AD Connector such as **univention-adsearch** support selecting the connector instance with the parameter `-c`.

3 Bibliography

References

[1] *AD DS: Read-Only Domain Controllers*. Microsoft, July 2012. URL: https://technet.microsoft.com/en-us/library/cc732801(v=ws.10).aspx.

Index

C

E

S