Introduction

Samba AD currently doesn't provide support for SysVol replication. To achive this important feature in a Multi-DC environment, until it's implemented, workarounds are necessary to keep it in sync. This HowTo provides a basic workaround solution based on rsync.

Information on rsync-based replication

This HowTo describes a solution for SysVol replication, that is based on rsync. As the nature of this tool, it is unidirectional. This means, files can only be transfered in one direction. That's why for rsync-based SysVol replicaton, you have to choose one DC, on which you do all modifications (GPO edits, logon script changes, etc.). And all other DCs are retrieving the changes from this host, because modifications on them are overwritten when syncing.

A good choice for this “master” host is the one, that contains the FSMO role “PDC Emulator”, because you can configure the Group Policy Management Console to connect especially to this machine (default), instead of choosing any of your DC. To which machine the GPMC connects, you can define at “Action' / “Change Domain Controller”. There you should select “The domain controller with the Operations Master token for the PDC emulator” (default).

Even if you say the unidirectional replication of rsync is a limitation, it has also many advantages:

- already available on most distributions and can be installed through it's packet manager (if not already installed anyway)
- setup is fast done
- configuration is very easy
- etc.

If you prefer to use rsync through a SSH tunnel, you can adapt the command to your needs. But typically there's no confidential content on the SysVol share. It should be sufficient for most if the transfer is unencrypted. The rsync module on the PDC is also defined as read only, because it is used only as source. So no content can be pushed to it.

Setup the SysVol replication

Setup on the Domain Controller with the PDC Emulator FSMO

role

- Install rsync by using your package manager or compile from source. Make sure, that you use a version that supports extended ACLs!
- If you start your rsync-server through xinetd, you can use the following configuration file (/etc/xinetd.d/rsync):

```
service rsync
{
  disable         = no
  only_from       = 10.12.112.0/24     # Restrict to your DC address(es) or
ranges, to prevent other hosts retrieving the content, too.
  socket_type     = stream
  wait            = no
  user            = root
  server          = /usr/bin/rsync
  server_args     = --daemon
  log_on_failure += USERID
}
```

- Create the file /etc/rsyncd.conf (adapt the path variable to your PDCs SysVol path):

```
[SysVol]
  path = /usr/local/samba/var/locks/sysvol/
  comment = Samba Sysvol Share
  uid = root
  gid = root
  read only = yes
  auth users = sysvol-replication
  secrets file = /usr/local/samba/etc/rsyncd.secret
```

- Create a file /usr/local/samba/etc/rsyncd.secret (permissions must not be world-readable!) with the following content (adapt the password!):

```
sysvol-replication:pa$$w0rd
```

- Restart xinetd

```
# service xinetd restart
```

Setup on all other Domain Controller(s)

- Install rsync by using your package manager or compile from source. Make sure, that you use a version that supports extended ACLs!
- Create a password file /usr/local/samba/etc/rsync-sysvol.secret and fill it with the password you set on the PDC for the sysvol-replication rsync account (permissions of that file must not be world-

readable!):

```
pa$$w0rd
```

For replicating the SysVol folder, run the following command (–dry-run means that no modifications are actually made):

```
 # rsync --dry-run -XAavz --delete-after --password-
file=/usr/local/samba/etc/rsync-sysvol.secret rsync://sysvol-replication@{IP-
of-you-PDC}/SysVol/ /path/to/your/sysvol/folder/
```

Warning: *Make sure that the destination folder is really your SysVol folder, because the command will replicate to the given directory and removes everything in it that isn't also on the source! You could damage your system! So check the output carefully if the replication is doing, what you expect!*

- If everything looks sane, run the command without the –dry-run option and let rsync do the replication.
- To automate synchronisation, you can run the command via cron (e. g. every 5 minutes):

```
 */5 * * * *   rsync --dry-run -XAavz --delete-after --password-
file=/usr/local/samba/etc/rsync-sysvol.secret rsync://sysvol-replication@{IP-
of-you-PDC}/SysVol/ /path/to/your/sysvol/folder/
```

- Repeat these steps on every DC (except your PDC!).

FAQ

- ***How can I get multi-direction replication?:***

This can't be done with rsync, as it can only replicate in one direction. If you try to setup a multi-direction replication process by yourself with a different tool, you have to choose one that is able to replicate extended ACLs, too.

- ***Why can't I simply use a distributed filesystem like GlusterFS, Lustre, etc. for SysVol?:***

A cluster file system with Samba requires CTDB to be able to do it safely. And CTDB and AD DC are incompatible.