Rocky Enterprise Linux 9.2 Manual Pages on command 'realmd.conf.5'

$ man realmd.conf.5

REALMD.CONF(5) File Formats REALMD.CONF(5)

NAME

realmd.conf - Tweak behavior of realmd

CONFIGURATION FILE

realmd can be tweaked by network administrators to act in specific ways. This is done by placing settings in a /etc/realmd.conf. This file does not exist by default. The syntax of this file is the same as an INI file or Desktop Entry file. If the file is changed and realmd is running realmd must be restarted to read the new values.

In general, settings in this file only apply at the point of joining a domain or realm. Once the realm has been setup the settings have no effect. You may choose to configure SSSD[1] or Winbind[2] directly.

Only specify the settings you wish to override in the /etc/realmd.conf file. Settings not specified will be loaded from their packaged defaults which can be found in /usr/lib/realmd/realmd-defaults.conf and /usr/lib/realmd/realmd-distro.conf. Only override the settings below.

You may find other settings if you look through the realmd source code. However these are not guaranteed to remain stable.

There are various sections in the config file. Some sections are global topic sections, and are listed below. Other sections are specific to a given realm. These realm specific sections should always contain the domain name in lower case as their section header.

Examples of each setting is found below, including the header of the section it should be placed in. However in the resulting file only include each section once, and combine the various section setting together as lines underneath the section. For example

```
[users]
default-home = /home/%U
default-shell = /bin/bash
```

ACTIVE-DIRECTORY

These options should go in an [active-directory] section of the /etc/realmd.conf file. Only specify the settings you wish to override.

default-client

Specify the default-client setting in order to control which client software is the preferred default for use with Active Directory.

```
[active-directory]
default-client = sssd
# default-client = winbind
```

The default setting for this is sssd which uses SSSD[1] as the Active Directory client. You can also specify winbind to use Samba Winbind[2].

Some callers of realmd such as the realm command line tool allow specifying which client software should be used. Others, such as GNOME Control Center, simplify choose the default.

You can verify the preferred default client softawre by running the following command. The realm with the preferred client software will be listed first.

```
$ realm discover domain.example.com
domain.example.com
  configured: no
  server-software: active-directory
```

client-software: sssd

type: kerberos

realm-name: AD.THEWALTER.LAN

domain-name: ad.thewalter.lan

domain.example.com

configured: no

server-software: active-directory

client-software: winbind

type: kerberos

realm-name: AD.THEWALTER.LAN

domain-name: ad.thewalter.lan

use-ldaps

Use the ldaps port when connecting to AD where possible. In general this option is not needed because realmd itself only read public information from the Active Directory domain controller which is available anonymously. The supported membership software products will use encrypted connections protected with GSS-SPNEGO/GSSAPI which offers a comparable level of security than ldaps. This option is only needed if the standard LDAP port (389/tcp) is blocked by a firewall and only the LDAPS port (636/tcp) is available.

If this option is set to yes realmd will use the ldaps port when reading the rootDSE and call the adcli membership software with the option --use-ldaps. The Samba base membership currently offers only deprecated ways to enable ldaps. Support will be added in realmd when a new way is available.

os-name

(see below)

os-version

Specify the os-name and/or os-version settings to control the values that are placed in the computer account operatingSystem and operatingSystemVersion attributes.

This is an Active Directory specific option.

It is also possible to use the --os-name or --os-version argument

of the realm command to override the default values.

[active-directory]

os-name = Gentoo Linux

os-version = 9.9.9.9.9

SERVICE

These options should go in an [service] section of the /etc/realmd.conf file. Only specify the settings you wish to override.

automatic-install

Set this to no to disable automatic installation of packages via package-kit.

[service]

automatic-install = no

automatic-install = yes

legacy-samba-config

Set this to yes to create a Samba configuration file with id-mapping options used by Samba-3.5 and earlier version.

[service]

legacy-samba-config = no

legacy-samba-config = yes

USERS

These options should go in an [users] section of the /etc/realmd.conf file. Only specify the settings you wish to override.

default-home

Specify the default-home setting in order to control how to set the home directory for accounts that have no home directory explicitly set.

[users]

default-home = /home/%U@%D

default-home = /nfs/home/%D-%U

default-home = /home/%D/%U

The default setting for this is /home/%U@%D. The %D format is replaced by the domain name. The %U format is replaced by the user name.

You can verify the home directory for a user by running the following command.

```
$ getent passwd 'DOMAIN/User'
DOMAIN\user:*:13445:13446:Name:/home/DOMAIN/user:/bin/bash
```

Note that in the case of IPA domains, most users already have a home directory configured in the domain. Therefore this configuration setting may rarely show through.

default-shell

Specify the default-shell setting in order to control how to set the Unix shell for accounts that have no shell explicitly set.

```
[users]
default-shell = /bin/bash
# default-shell = /bin/sh
```

The default setting for this is /bin/bash shell. The shell should be a valid shell if you expect the domain users be able to log in. For example it should exist in the /etc/shells file.

You can verify the shell for a user by running the following command.

```
$ getent passwd 'DOMAIN/User'
DOMAIN\user:*:13445:13446:Name:/home/DOMAIN/user:/bin/bash
```

Note that in the case of IPA domains, most users already have a shell configured in the domain. Therefore this configuration setting may rarely show through.

PATHS

These options should go in an [paths] section of the /etc/realmd.conf file. Only specify the settings you wish to override.

krb5.conf

Path to the Kerberos configuration file, typically /etc/krb5.conf. It can also be the path of a file included by /etc/krb5.conf, e.g. /etc/krb5.conf.d/realmd_settings, if the file does not exist if will be created.

```
[paths]
krb5.conf = /etc/krb5.conf.d/realmd_settings
```

When joining an Active Directory domain realmd will set the default_realm and udp_preference_limit options in the Kerberos configuration:

default_realm = DOMAIN.EXAMPLE.COM

udp_preference_limit = 0

The default_realm option is e.g. needed when trying to resolve enterprise principals and makes it more convenient to request Kerberos tickets for users of the default realm. Instead of specifying the whole principal just kinit username can be used.

With udp_preference_limit = 0 always TCP will be used to send Kerberos request to domain controller. This is useful in Active Directory environments because Kerberos will typically switch to TCP after initially starting with UDP because AD Kerberos tickets are often larger than UDP can handle. Using TCP by default will avoid those extra UDP round trips. Additionally it helps to avoid issues with password changes when the DC does not reply soon enough and the client will send a second UDP request. The DC might reply with a reply error to the second request although the original password change request was successful and the client will no know if the request was successful or not. When using TCP this cannot happen because the client will never send a second request but waits on the connection until the server replies.

Please note that realmd will not remove those options while leaving the domain since they are useful in general. When joining a new domain realmd will of course overwrite default_realm.

REALM SPECIFIC SETTINGS

These options should go in an section with the same name as the realm in the /etc/realmd.conf file. For example for the domain.example.com domain the section would be called [domain.example.com]. To figure out the canonical name for a realm use the realm command:

$ realm discover --name-only DOMAIN.example.com

domain.example.com

...

Only specify the settings you wish to override.

computer-ou

Specify this option to create directory computer accounts in a location other than the default. This currently only works with Active Directory domains.

```
[domain.example.com]
computer-ou = OU=Linux Computers,DC=domain,DC=example,DC=com
# computer-ou = OU=Linux Computers,
```

Specify the OU as an LDAP DN. It can be relative to the Root DSE, or a complete LDAP DN. Obviously the OU must exist in the directory.

It is also possible to use the --computer-ou argument of the realm command to create a computer account at a specific OU.

computer-name

This option only applied to Active Directory realms. Specify this option to override the default name used when creating the computer account. The system's FQDN will still be saved in the dNSHostName attribute.

```
[domain.example.com]
computer-name = SERVER01
```

Specify the name as a string of 15 or fewer characters that is a valid NetBIOS computer name.

It is also possible to use the --computer-name argument of the realm command to override the default computer account name.

user-principal

Set the user-principal to yes to create userPrincipalName attribute for the computer accounts in the realm. The exact value depends on the defaults of the used membership software. To have full control over the value please use the --user-principal option of the realm command, see realm(8) for details.

```
[domain.example.com]
user-principal = yes
```

automatic-join

This option only applies to Active Directory realms. This option is off by default. In Active Directory domains, a computer account can be preset with a known computer account password. This can be used for automatic joins without authentication.

When automatic joins are used there is no mutual authentication between the machine and the domain during the join process.

```
[domain.example.com]
automatic-join = yes
```

automatic-id-mapping

This option is on by default for Active Directory realms. Turn it off to use UID and GID information stored in the directory (as-per RFC2307) rather than automatically generating UID and GID numbers. This option only makes sense for Active Directory realms.

```
[domain.example.com]
automatic-id-mapping = no
# automatic-id-mapping = yes
```

manage-system

This option is on by default. Normally joining a realm affects many aspects of the configuration and management of the system. Turning this off limits the interaction with the realm or domain to authentication and identity.

```
[domain.example.com]
manage-system = no
# manage-system = yes
```

When this option is turned on realmd defaults to using domain policy to control who can log into this machine. Further adjustments to login policy can be made with the realm permit command.

fully-qualified-names

This option is on by default. If turned off then realm user and group names are not qualified their name. This may cause them to conflict with local user and group names.

```
[domain.example.com]
```

```
fully-qualified-names = no
# fully-qualified-names = yes
```

SEE ALSO

realm(8)

AUTHOR

Stef Walter <stef@thewalter.net>

Maintainer

NOTES

1. SSSD

   https://fedorahosted.org/sssd/

2. Winbind

   http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/winbind.html