Rocky Enterprise Linux 9.2 Manual Pages on command 'realm.8'

$ man realm.8

REALM(8) User Commands REALM(8)

NAME

realm - Manage enrollment in realms

SYNOPSIS

realm discover [realm-name]

realm join [-U user] [realm-name]

realm leave [-U user] [realm-name]

realm list

realm permit [-ax] [-R realm] {user@domain...}

realm deny -a [-R realm]

DESCRIPTION

realm is a command line tool that can be used to manage enrollment in

kerberos realms, like Active Directory domains or IPA domains.

See the various sub commands below. The following global options can be

used:

-i, --install=/path

Run in install mode. This makes realmd chroot into the directory

specified by an absolute path and place files in appropriate

locations for use during an installer. No packages will be

installed or services will be started when running in this mode.

--unattended

Run in unattended mode without prompting for input.

-v, --verbose

Display verbose diagnostics while doing running commands.

DISCOVER

Discover a realm and its capabilities.

$ realm discover

$ realm discover domain.example.com

After discovering a realm, its name, type and capabilities are

displayed.

If no domain is specified, then the domain assigned through DHCP is

used as a default.

The following options can be used:

-a, --all

Show all discovered realms (in various configurations).

--client-software=xxx

Only discover realms for which we can use the given client

software. Possible values include sssd or winbind.

-n, --name

Only show the names of the discovered realms.

--server-software=xxx

Only discover realms which run the given server software. Possible

values include active-directory or ipa.

--membership-software=xxx

Only discover realms for which the given membership software can be

used to subsequently perform enrollment. Possible values include

samba or adcli.

--use-ldaps

See option description in the section called ?JOIN?.

JOIN

Configure the local machine for use with a realm.

$ realm join domain.example.com

$ realm join --user=admin --computer-ou=OU=Special domain.example.com

The realm is first discovered, as we would with the discover command.

If no domain is specified, then the domain assigned through DHCP is used as a default.

After a successful join, the computer will be in a state where it is able to resolve remote user and group names from the realm. For kerberos realms, a computer account and host keytab is created.

Joining arbitrary kerberos realms is not supported. The realm must have a supported mechanism for joining from a client machine, such as Active Directory or IPA.

If the domain has been preconfigured, and unless --user is explicitly specified, an automatic join is attempted first.

Note that the --user, --no-password, and --one-time-password options are mutually exclusive. At most one of them can be specified.

It is generally possible to use kerberos credentials to perform a join operation. Use the kinit command to acquire credentials prior to starting the join. Do not specify the --user argument, the user will be selected automatically from the credential cache. The realm respects the KRB5_CCACHE environment variable, but uses the default kerberos credential cache if it's not present. Not all types of servers can be joined using kerberos credentials, some (like IPA) insist on prompting for a password.

The following options can be used:

--automatic-id-mapping=no

Do not perform UID/GID mapping for users and groups, but expect these identifiers to be present in the domain already.

--client-software=xxx

Only join realms for which we can use the given client software. Possible values include sssd or winbind. Not all values are supported for all realms. By default the client software is automatically selected.

--computer-ou=OU=xxx

The distinguished name of an organizational unit to create the computer account. The exact format of the distinguished name depends on the client software and membership software. You can usually omit the root DSE portion of distinguished name. This is an Active Directory specific option.

--membership-software=xxx

The software to use when joining to the realm. Possible values include samba or adcli. Not all values are supported for all realms. By default the membership software is automatically selected.

--computer-name=xxx

This option only applies 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.

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

--no-password

Perform the join automatically without a password.

--one-time-password=xxxx

Perform the join using a one time password specified on the command line. This is not possible with all types of realms.

--os-name=xxx

The name of the operation system of the client. When joining an AD domain the value is store in the matching AD attribute.

--os-version=xxx

The version of the operation system of the client. When joining an AD domain the value is store in the matching AD attribute.

--server-software=xxx

Only join realms for run the given server software. Possible values include active-directory or ipa.

-U, --user=xxx

The user name to be used to authenticate with when joining the

machine to the realm. You will be prompted for a password.

--user-principal=host/name@REALM

Set the userPrincipalName field of the computer account to this kerberos principal. If you omit the value for this option, then a principal will be set based on the defaults of the membership software.

AD makes a distinction between user and service principals. Only with user principals you can request a Kerberos Ticket-Granting-Ticket (TGT), i.e. only user principals can be used with the kinit command. By default the user principal and the canonical principal name of an AD computer account is shortname$@AD.DOMAIN, where shortname is the NetBIOS name which is limited to 15 characters.

If there are applications which are not aware of the AD default and are using a hard-coded default principal the --user-principal can be used to make AD aware of this principal. Please note that userPrincipalName is a single value LDAP attribute, i.e. only one alternative user principal besides the AD default user principal can be set.

--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. Given that and to lower the initial effort to discover a remote domain realmd does not require a strict certificate check. If the validation of the LDAP server certificate fails realmd will continue to setup the encrypted connection to the LDAP server.

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.

--do-not-touch-config

Run the join operation but do not touch the local configuration of the client except adding new Kerberos keys to the keytab. The purpose of this option is to synchronize the keytab entries with the ones stored in AD or recreate the computer object in AD without changing the local configuration which might contain changes which would get overwritten by a fully leave/join cycle.

If running realm join with this options does not help to fix issues it is recommended to call realm leave followed by realm join to enforce a fresh configuration with default settings. Since this might overwrite manual changes to the related configuration files it is recommend to save those change before running the commands.

This options is only available when joining AD domains.

LEAVE

Deconfigure the local machine for use with a realm.

$ realm leave

$ realm leave domain.example.com

If no realm name is specified, then the first configured realm will be used.

The following options can be used:

--client-software=xxx

Only leave the realm which is using the given client software.

Possible values include sssd or winbind.

--server-software=xxx

Only leave the realm which is using the given server software.

Possible values include active-directory or ipa.

--remove

Remove or disable computer account from the directory while leaving the realm. This will usually prompt for a pasword.

-U, --user

The user name to be used to authenticate with when leaving the realm. You will be prompted for a password. Implies --remove.

--use-ldaps

See option description in the section called ?JOIN?.

LIST

List all the discovered and configured realms.

$ realm list

By default, realms that have been discovered, but not configured (using the join command), are not displayed. Also, by default, the list of realm details displayed is verbose. The options below can be used to change this default behavior

The following options can be used:

--all

Show all discovered realms (whether or not they have been configured).

--name-only

Display only realm names (as opposed to verbose output).

PERMIT

Permit local login by users of the realm.

$ realm permit --all

$ realm permit user@example.com

$ realm permit DOMAIN\\User2

$ realm permit --withdraw user@example.com

The current login policy and format of the user names can be seen by using the realm list command.

The following options can be used:

--all, -a

Permit logins using realm accounts on the local machine according to the realm policy.This usually defaults to allowing any realm user to log in.

--groups, -g

Treat the specified names as groups rather than user login names.

Permit login by users in the specified groups.

--realm, -R

Specify the of the realm to change login policy for.

--withdraw, -x

Remove a login from the list of realm accounts permitted to log into the machine.

DENY

Deny local login by realm accounts.

$ realm deny --all

This command prevents realm accounts from logging into the local machine. Use realm permit to restrict logins to specific accounts.

The following options can be used:

--all, -a

This option should be specified

--realm, -R

Specify the name of the realm to deny users login to.

SEE ALSO

realmd.conf(5)

AUTHOR

Stef Walter <stef@thewalter.net>

Maintainer

realmd 10/14/2022 REALM(8)