

NetDom examples

Sample workstation or member server operations

Adding a workstation or member server to a domain

Add the workstation **mywksta** to the Windows NT 4.0 [domain microsoft](#):

```
NETDOM ADD /d:microsoft mywksta
/ud:mydomain\admin /pd:password
```

Add the workstation **mywksta** to the Windows 2000 domain devgroup.microsoft.com in the [organizational unit \(OU\)](#) Dsys/workstations:

```
NETDOM ADD /d:devgroup.microsoft.com
mywksta /OU:OU=Dsys,OU=Workstations,DC=microsoft,DC=com
```

Note

- If /OU is not specified the account is created in the Computers container.

Joining a workstation or member server to a domain

Join **mywksta** to the devgroup.microsoft.com domain in the Dsys/workstations organizational unit.

```
NETDOM JOIN /d:devgroup.microsoft.com
mywksta /OU:OU=Dsys,OU=Workstations,DC=microsoft,DC=com
```

In addition to adding the computer account to the domain, the workstation is modified to contain the appropriate shared secret to complete the Join operation.

Removing a workstation or member server from a domain

To remove **mywksta** from the mydomain domain and have the workstation be part of a workgroup:

```
NETDOM REMOVE /d:mydomain mywksta
/ud:mydomain\admin /pd:password
```

Moving a workstation or member server from one domain to another

To move **mywksta** from its current domain into the mydomain domain:

```
NETDOM MOVE /d:mydomain mywksta
/ud:mydomain\admin /pd:password
```

If the destination is a Windows 2000 domain, the [SIDHistory](#) for the workstation is updated, retaining the security permissions that the computer account had previously.

Resetting the secure channel for a workstation, member server, or Windows NT 4.0 BDC

To reset the secure channel secret maintained between **mywksta** and devgroup.microsoft.com (regardless of OU):

```
NETDOM RESET /d:devgroup.microsoft.com
mywksta
```

To reset the secure channel between the Windows NT 4.0 PDC for Northamerica and the backup domain controller NABDC:

```
NETDOM RESET /d:Northamerica NABDC
```

Forcing a secure channel session between a member and a specific domain controller

Members may often establish secure channel sessions with non-local domain controllers. To force a secure channel session between a member and a specific domain controller, add the /Server option to the RESET command:

```
NETDOM RESET /d:devgroup.microsoft.com
mywksta /Server:mylocalbdc
```

Verifying a workstation or member server secure channel

To verify the secure channel secret maintained between mywksta and devgroup.microsoft.com:

```
NETDOM VERIFY /d:devgroup.microsoft.com
mywksta
```

Sample domain TRUST operations

Establishing a trust relationship

When used with the TRUST command, the **/d:domain** parameter always refers to the trusted domain.

To have the Windows NT 4.0 resource domain USA-Chicago [trust](#) the Windows NT 4.0 account domain Northamerica:

```
NETDOM TRUST /d:Northamerica USA-Chicago
```

```
/ADD /Ud:Northamerica\admin /Pd:*
/Uo:USA-Chicago\admin /Po:*
```

```
>Password for Northamerica\admin: xxxx
>Password for USA-Chicago\admin: yyyy
```

The user must have credentials for both domains. **/Pd:** can be used to specify the password for Northamerica\admin while **/Po:** can be used to specify the password for USA-Chicago\admin. If passwords are not provided on the command line, the user will be prompted for both.

The **/TWOWAY** option can be appended to specify a bidirectional trust:

```
NETDOM TRUST /d:marketing.microsoft.com
engineering.microsoft.com /ADD /TWOWAY
/Uo:admin@engineering.microsoft.com
/Ud:admin@marketing.microsoft.com
```

Establishing a trust relationship with a non-Windows Kerberos realm

To establish a one-way trust so that Northamerica trusts the non-Windows [Kerberos](#) realm ATHENA:

```
NETDOM TRUST /d:ATHENA Northamerica /ADD /PT:password /REALM
```

The **/d** option specifies the TRUSTED domain and **/REALM** indicates that this is a non-Windows Kerberos realm. The order of the domains is not important and credentials to the Windows 2000 domain can be supplied if needed. Note that verifying a specific trust relationship will usually require credentials unless the user has domain admin privileges on both domains.

To allow the Kerberos realm ATHENA to trust the Northamerica domain:

```
NETDOM TRUST /d:Northamerica ATHENA /ADD
```

To make the trust bi-directional, you can specify **/TWOWAY**.

Changing the trust from ATHENA to Northamerica to transitive (non-Windows Kerberos trusts are created non-transitive)

```
NETDOM TRUST Northamerica /d:ATHENA /TRANS:yes
```

Displaying the transitive state

```
NETDOM TRUST Northamerica /d:ATHENA /TRANS
```

The order of the two domains above is not important (either can be the non-Windows Kerberos domain).

Breaking a trust relationship

To undo the trust that USA-Chicago has for Northamerica,

```
NETDOM TRUST /d:Northamerica USA-Chicago /REMOVE
```

To break a two-way trust relationship

```
NETDOM TRUST /d:marketing.microsoft.com
Engineering.microsoft.com /REMOVE /TWOWAY
/Uo:admin@engineering.microsoft.com
/Ud:admin@marketing.microsoft.com
```

Verifying a specific trust relationship

To verify the one-way trust that USA-Chicago has for Northamerica:

```
NETDOM TRUST /d:Northamerica USA-Chicago /VERIFY
```

To verify a two-way trust between the Northamerica and Europe domains:

```
NETDOM TRUST /d:Northamerica EUROPE /VERIFY /TWOWAY
```

The verify command checks that the appropriate shared secrets are synchronized between the two items involved in the trust.

Resetting a specific trust relationship

To reset the secure channel for the one-way trust between Northamerica and USA-Chicago:

```
NETDOM TRUST /d:Northamerica USA-Chicago
/Ud:Northamerica\admin /RESET
```

The reset command synchronizes the appropriate shared secrets if they are not already synchronized.

Verifying Kerberos functionality

To verify Kerberos authentication between a workstation and a service located in domain devgroup.microsoft.com:

```
NETDOM TRUST /d:devgroup.microsoft.com
```

```
[workstation] /VERIFY /KERBEROS
```

If the workstation parameter is omitted, the current workstation is used.

The NETDOM TRUST command with the /Verify /Kerberos options attempts to get a session ticket for the Kerberos Admin service in the target domain. If successful, it can be concluded that all Kerberos operations (for example [KDC](#) referrals) are operating correctly between the workstation and the target domain.

Note

- The operation can not be executed remotely; it must be run on the workstation being tested.

Sample domain QUERY operations

Viewing domain membership

List all the workstations in the domain Northamerica:

```
NETDOM QUERY /d:Northamerica WORKSTATION
```

List all of the Servers in Northamerica:

```
NETDOM QUERY /d:Northamerica SERVER
```

List all the domain controllers in the domain Northamerica:

```
NETDOM QUERY /d:Northamerica DC
```

List all of the OUs in devgroup.microsoft.com:

```
NETDOM QUERY /d:devgroup.microsoft.com OU
```

List the PDC for Northamerica:

```
NETDOM QUERY /d:Northamerica PDC
```

List the current PDC Emulator for devgroup.microsoft.com:

```
NETDOM QUERY /d:devgroup.microsoft.com FSMO
```

Secure channel batch repair

The QUERY command can be used in conjunction with the /Verify and /Reset options to perform these operations all together. The output of the QUERY command can be piped to the NETDOM VERIFY or NETDOM RESET command.

List all servers and verify secure channel secret:

```
NETDOM QUERY /d:Northamerica SERVER /VERIFY
```

List all workstations and reset any unsynchronized secure channel secrets:

```
NETDOM QUERY /d:Northamerica WORKSTATION /RESET
```

Viewing domain trusts

To view all the direct trust relationships for the domain Northamerica:

```
NETDOM QUERY /d:Northamerica
/Ud:Northamerica\admin DOMAIN /Direct
```

To view all the direct and indirect trust relationships for the domain Northamerica:

```
NETDOM QUERY /d:Northamerica
/Ud:Northamerica\admin DOMAIN
```

To view all trust relationships and check their status:

```
NETDOM QUERY /d:devgroup.microsoft.com
DOMAIN /VERIFY
```

Sample domain TIME operations

Viewing domain controller time status

To verify the current time for all domain controllers in devgroup.microsoft.com:

```
NETDOM TIME /d:devgroup.microsoft.com
```

To verify the time for a specific server:

```
NETDOM TIME /d:devgroup.microsoft.com
dc1.devgroup.microsoft.com
```

Synchronizing time

The /Synch switch may be used to resynchronize a specified domain controller or all domain controllers that are out of synch:

```
NETDOM TIME /d:devgroup.microsoft.com /SYNCH
```

Specifying a domain controller:

```
NETDOM TIME /d:devgroup.microsoft.com  
dc1.devgroup.microsoft.com /SYNCH
```

Renaming the domain name for a Windows NT 4.0 BDC

Changing the name of a Windows NT 4.0 domain is a complex process and requires:

- Renaming the domain name on the Windows NT 4.0 PDC.
- Modifying all Windows NT 4.0 BDCs.
- Rejoining all Members (workstations and servers).
- Deleting and Reestablishing all Trusts.

The following NETDOM syntax is provided to support the modifications necessary to rejoin a BDC to the renamed domain. (step 2 above):

```
NETDOM RENAME /d:newdomainname BDCServer
```

[Windows 2000 Domain Manager \(Netdom.exe\)](#)

[NetDom syntax](#)