Redirecting the users and computers containers in Active Directory domains

Summary

In a default installation of an Active Directory domain, user accounts, computer accounts, and groups are put in CN=objectclass containers instead of being put in a more desirable organizational unit class container. Similarly, user accounts, computer accounts, and groups that were created by using earlier-version APIs are put in the CN=Users and CN=computers containers.

This article describes how to use the redirusr and redircmp utilities to redirect user, computer, and group accounts that were created by earlier-version APIs so that they are put in admin-specified organizational unit containers.

Important Some applications require specific security principals to be located in default containers like CN=Users or CN=Computers. Verify that your applications have such dependencies before you move them out of the CN=users and CN=computes containers.

More Information

Users, computers, and groups that are created by earlier-version APIs place objects in the DN path that is specified in the **WellKnownObjects** attribute that is located in the domain NC head. The following code example shows the relevant paths in the

Properties

Article ID: 324949 - Last Review: Sep 17, 2009 - Revision: 1

WellKnownObjects attribute from the CONTOSO.COM domain NC head.

Dn: DC=CONTOSO,DC=COM

```
wellKnownObjects (11):
B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quot
B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft
B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program D
B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSe
B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted O
B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastru
B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFo
B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC
B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Co
B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers
B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=
```

Examples of operations that use earlier-version APIs that reply on the paths that are defined in the **WellKnownObjects** attribute include the following.

Operation	Operating system versions
Domain Join UI	Windows NT version4.0 Windows 2000 Windows XP Professional Windows XP

	Ultimate Windows Server 2003 Windows Server 2003 R2 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2
NET COMPUTER	All versions
NET GROUP	All versions
NET USER	All versions
NETDOM ADD, where the **/ou** command is either not specified or supported	All versions

It is helpful to make the default container for user, computer, and security groups an organizational unit for several reasons, including the following:

- Group policies can be applied on organizational unit containers but not on CN class containers, where security principals are put by default.

- The "best practice" is to arrange security principals into an organizational unit hierarchy that mirrors your organizational structure, geographic layout, or administration model.

If you are redirecting the CN=Users and CN=Computers folders, be aware of the following issues:

- The target domain must be configured to run in the Windows Server 2003 domain functional level or higher. For the 2003 domain functional level, this means that:
  - Windows Server 2003 ADPREP /FORESTPREP or newer

  - Windows Server 2003 ADPREP /DOMAINPREP or newer

- All domain controllers in the target domain must run Windows Server 2003 or newer.
- Windows Server 2003 domain functional level or higher must be enabled.

- Unlike CN=USERS and CN=COMPUTERS, organizational unit containers are subject to accidental deletions by privileged user accounts, including administrators.

  CN=USERS and CN=COMPUTERS containers are system-protected objects that cannot, and must not, be removed for backward compatibility. However, they can be renamed. Organizational units, on the other hand, are subject to accidental tree deletions by administrators.

  Windows Server 2003 versions of the Active Directory Users & Computers snap-in can follow the steps in "Protect an Organizational Unit from Accidental Deletion."

  Windows Server 2008 and newer versions of the Active Directory Users and Computers snap-in feature a "Protect object against accidental deletion" check box that you can click to select when you create a new organizational unit container. You can also select this check box on the **Object** tab of the **Properties** dialog box for an existing organizational unit container.

  A scripted option is documented in "Script to Protect Organizational Units (OUs) from Accidental Deletion."

- Exchange 2000 and 2003 setup /domainprep fails with errors. This issue is documented in the following Microsoft Knowledge Base articles:
  - 260914 Domainprep utility does not work if Exchange Enterprise Servers group and Exchange

Domain Servers group moved to a new container

- 818470 Exchange Server 2003 Setup returns error code 0x80072030 when you run setup.exe /domainprep

Redirecting CN=Users to an administrator-specified organizational unit

1. Log on with domain administrator credentials in the z domain where the CN=Users container is being redirected.

2. Transition the domain to the Windows Server 2003 domain functional level or newer in either the Active Directory Users and Computers snap-in (Dsa.msc) or the Domains and Trusts (Domains.msc) snap-in. For more information about increasing the domain functional level, click the following article number to view the article in the Microsoft Knowledge Base:

   322692 How to raise domain and forest functional levels in Windows Server 2003

3. Create the organizational unit container where you want users who are created with earlier-version APIs to be located, if the organization unit container that you want does not already exist.

4. Run the Redirusr.exe file at the command prompt by using the following syntax, where **container-dn** is the distinguished name of the organizational unit that will become the default location for newly created user objects created by down-level APIs:

   c:\windows\system32\redirusr <DN path to alternate OU>

   Redirusr is installed in the %SystemRoot%\System32 folder on Windows Server 2003-based or newer computers. For example, to change the default location for users who are created with down-level APIs such as Net User to the

OU=MYUsers OU container in the CONTOSO.COM domain, use the following syntax:

c:\windows\system32>redirusr ou=myusers,DC=contoso,dc=com

Redirecting CN=Computers to an administrator-specified organizational unit

1. Log on with Domain Administrator credentials in the domain where the CN=computers container is being redirected.

2. Transition the domain to the Windows Server 2003 domain in the Active Directory Users and Computers snap-in (Dsa.msc) or in the Domains and Trusts (Domains.msc) snap-in.For more information about increasing the domain functional level, click the following article number to view the article in the Microsoft Knowledge Base:

   322692 How to raise domain and forest functional levels in Windows Server 2003

3. Create the organizational unit container where you want computers that are created with earlier-version APIs to be located, if the desired organizational unit container does not already exist.

4. Run the Redircmp.exe file at a command prompt by using the following syntax, where **container-dn** is the distinguished name of the organizational unit that will become the default location for newly created computer objects that are created by down-level APIs:

   redircmp container-dn container-dn

   Redircmp.exe is installed in the %Systemroot%\System32 folder on Windows Server 2003-based or newer computers. For example, to change the default location for a computer that is created with earlier-version APIs such as Net User to the OU=mycomputers container in the CONTOSO.COM domain, use the following syntax:

   C:\windows\system32>redircmp ou=mycomputers,DC=contoso,dc=com

   Note When Redircmp.exe is run to redirect the

CN=Computers container to an organizational unit that is specified by an administrator, the CN=Computers container will no longer be a protected object. This means that the Computers container can now be moved, deleted, or renamed. If you use ADSIEDIT to view attributes on the CN=Computers container, you will see that the **systemflags** attribute was changed from -1946157056 to 0. This is by design.

Description of error messages

Error messages that you receive if the PDC is offline

Redircmp and Redirusr change the **wellKnownObjects** attribute on the primary domain controller (PDC). If the PDC of the domain that is being changed is offline or inaccessible, you receive the following error messages.

Error message 1

```
D:\>redirusr OU=userOU,DC=udc,dc=jkcertcontoso,dc=loc com
Error, could not locate the Primary Domain Controller for the current domain: The specified domain either does not exist or could not be contacted. Redirection was NOT successful.
```

Error message 2

```
D:\>redircmp OU=computerOU,DC=contoso,dc=com
DC=udc,dc=jkcert,dc=loc
Error, could not locate the Primary Domain Controller for the current domain: The specified domain either does not exist or could not be contacted. Redirection was NOT successful.
```

Error messages that you receive if the domain functional level is not Windows Server 2003

If you try to redirect the users or computer organizational unit in a domain that has not transitioned to the Windows Server 2003 domain functional level, you receive the following error messages.

Error message 1

```
C:\>redirusr
OU=usersou,DC=contoso,dc=comDC=company,DC=com
```

```
Error, unable to modify the wellKnownObjects attribute. Verify
that the domain functional level of the domain is at least
Windows Server 2003: Unwilling To Perform Redirection was NOT
successful.
```

Error message 2

```
C:\>REDIRCMP
ou=computersou,DC=contoso,dc=comdc=company,dc=com

Error, unable to modify the wellKnownObjects attribute. Verify
that the domain functional level of the domain is at least
Windows Server 2003: Unwilling To Perform
```

Error messages that you receive if you log on without the required permissions

If you try to redirect the users or computer organizational unit by using incorrect credentials in the target domain, you may receive the following error messages.

Error message 1

```
C:>REDIRCMP
OU=computersou,DC=contoso,dc=comDC=company,DC=com

Error, unable to modify the wellKnownObjects attribute. Verify
that the domain functional level of the domain is at least
Windows Server 2003: Insufficient Rights Redirection was NOT
successful.
```

Error message 2

```
:\>redirusr
OU=usersou,DC=contoso,dc=comDC=company,DC=com

Error, unable to modify the wellKnownObjects attribute. Verify
that the domain functional level of the domain is at least
Windows Server 2003: Insufficient Rights Redirection was NOT
successful.
```

Error messages that you receive if you redirect to an organizational unit that does not exist

If you try to redirect the users or computer organizational unit to an organizational unit that does not exist, you may receive the following error messages.

Error message 1

```
C:\>REDIRCMP OU=nonexistantou,DC=contoso,dc=com
dc=rendom,dc=com

Error, unable to modify the wellKnownObjects attribute. Verify
that the domain functional level of the domain is at least
Windows Server 2003: No Such Object Redirection was NOT
successful.
```

Error message 2

```
C:\>redirusr OU=nonexistantou,DC=contoso,dc=com
DC=company,DC=com

Error, unable to modify the wellKnownObjects attribute. Verify
that the domain functional level of the domain is at least
Windows Server 2003: No Such Object Redirection was NOT
successful.
```

Error messages that you receive in Exchange 2000 "setup /domainprep" when CN=Users is redirected

If Exchange 2000 and Exchange 2003 **setup /domainprep** is unsuccessful, you receive the following error message:

```
Setup failed while installing sub-component Domain-level
permissions with error code 0x80072030) (please consult the
installation logs for a detailed description). You may cancel the
installation or try the failed step again. (Retry / Cancel)
```

The following data appears in the Exchange 2000 Setup log that is parsed with log parser. Exchange 2003 should be similar.

```
[HH:MM:SS] Completed DomainPrep of Microsoft Exchange
2000 component
[HH:MM:SS] ScGetExchangeServerGroups (K:\admin\src\libs
\exsetup\dsmisc.cxx:301) Error code 0X80072030 (8240): There
is no such object on the server.
[HH:MM:SS] ScCreateExchangeServerGroups (K:\admin\src\libs
\exsetup\dsmisc.cxx:373) Error code 0X80072030 (8240): There
is no such object on the server.
```

[HH:MM:SS] CAtomPermissions::ScAddDSObjects (K:\admin \src\udog\exsetdata\components\domprep \a_permissions.cxx:144) Error code 0X80072030 (8240): There is no such object on the server.
[HH:MM:SS] mode = 'DomainPrep' (61966) CBaseAtom::ScSetup (K:\admin\src\udog\setupbase\basecomp \baseatom.cxx:775) Error code 0X80072030 (8240): There is no such object on the server.
[HH:MM:SS] Setup encountered an error during Microsoft Exchange Domain Preparation of DomainPrep component task. CBaseComponent::ScSetup (K:\admin\src\udog \setupbase\basecomp\basecomp.cxx:1031) Error code 0X80072030 (8240): There is no such object on the server.
[HH:MM:SS] CBaseComponent::ScSetup (K:\admin\src\udog \setupbase\basecomp\basecomp.cxx:1099) Error code 0X80072030 (8240): There is no such object on the server.
[HH:MM:SS] CCompDomainPrep::ScSetup (K:\admin\src\udog \exsetdata\components\domprep\compdomprep.cxx:502) Error code 0X80072030 (8240): There is no such object on the server.
[HH:MM:SS] CComExchSetupComponent::Install (K:\admin \src\udog\BO\comboifaces.cxx:694) Error code 0X80072030 (8240): There is no such object on the server.
[HH:MM:SS] Setup completed

References

For more information, click the following article numbers to view the articles in the Microsoft Knowledge Base:

818470 Exchange Server 2003 Setup returns error code 0x80072030 when you run setup.exe /domainprep

260914 Domainprep utility does not work if Exchange Enterprise Servers group and Exchange Domain Servers group moved to a new container

Script to protect organizational units from accidental deletion:

http://gallery.technet.microsoft.com/ScriptCenter/en-us /c307540f-bd91-485f-b27e-995ae5cea1e2

For more information about how to design a Group Policy

infrastructure, visit the following Microsoft Web site:

http://technet2.microsoft.com/windowsserver/en/library/c75e3e6f-c322-4220-b205-46c6e9ba76741033.mspx