Knowledge Base

Redirecting the users and computers containers in Windows Server 2003 domains

PSS ID Number: 324949

Article Last Modified on 8/26/2004

The information in this article applies to:

- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, Standard Edition

This article was previously published under Q324949

SUMMARY

In Windows 2000 and Windows Server 2003 domain controllers, the default containers for users, computers, and groups that are created by using earlier-version application programming interfaces (APIs) are of objectclass CN instead of the more desirable organizational unit class container.

Microsoft recommends that administrators aggressively deploy the best-practice organizational unit structure in all Active Directory domains (see the "More information" section for details). After you upgrade or deploy Windows Server 2003 domain controllers in Windows Server 2003 Domain mode, redirect the default containers that the earlier-version APIs use to create users, computers, and groups to an organizational unit container that the administrator specifies.

MORE INFORMATION

By default, the container for security groups, user accounts and computer accounts in new and upgraded installations of Windows 2000 and Windows Server 2003 is CN=Users and CN=Computers. You cannot apply Group Policy settings on CN-class containers. Therefore, administrators who want to define policy setting for users and computers to be stored in their default container must do so on the root of the domain. To prevent policy settings that are defined on a superior container (the root of the domain) from applying to users and computers in subordinate CN and organizational unit containers, administrators must define complex access control lists (ACLs) on the policy setting in the root of the domain.

The solution for Windows 2000 and Windows Server 2003 domains is to deploy the best-practice organizational unit structure where Users, Computers, Groups, Service Accounts and Admin accounts are each in their own organizational unit. The best-practice organizational unit structure is discussed in the "Creating an Organizational Unit Design" section of the *Best Practice Active Directory Design for Managing Windows Networks* white paper. To view that white paper, visit the following Microsoft Web site:

http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/bpaddsgn

The following list describes the benefits of using the best-practice organizational unit structure:

- It permits administrators to apply Group Policy directly on the containers that are hosting users and computers.
- It permits administrators to match Group Policy to objects of a common objectclass. For example, User or Computer policy settings can be linked directly to organizational units that are hosting user or computer accounts.
- It permits delegated users to apply policy on containers that are not hosting security-sensitive users and groups like Domain Administrators, Schema Administrators, or Enterprise Administrators.
- It can minimize the effect if an organizational unit is accidentally deleted (this assumes that the parent container is correctly protected).
- It permits you to restore users and groups independently of each other in recovery scenarios. User accounts must exist before the restoration of the group. Having users and groups reside in different containers permits you to restore them and mark them as authoritative independently of each other.

Note that the CN=USERS and CN=COMPUTERS containers are computer-protected objects. You cannot (and must not) remove them for backward compatibility purposes although they can be renamed.

The best-practice organizational unit structure works well for storing existing users, computers, and groups in Active Directory because those objects can be moved into the appropriate organizational unit container on

Windows 2000 and Windows Server 2003 domains regardless of its domain or forest functional level. New user accounts, computer accounts, and security groups that are created (in CN=users CN=computers) with earlier-version APIs used by GUI and command-line management tools do not allow administrators to specify a target organizational unit. As a result, these objects will initially be created in the CN=Users and CN=Computers containers until they are moved by the administrator or an administrator-defined script. The following list provides examples of such tools:

- The domain join UI in:
  - Microsoft Windows NT 4.0
  - Microsoft Windows 2000
  - Microsoft Windows XP Professional
  - Microsoft Windows Server 2003

  This operation joins Active Directory domains as member computers.

- The **net user** command.
- The **net computer** command.
- The **net group** command.
- The **netdom add** command where the **/ou** command is either not specified or supported.
- User Manager on Windows NT 4.0-based member computers

Additionally, delegated users do not know what container to create objects in even if the destination organizational unit could be specified.

Microsoft recommends that Administrators upgrade Windows NT 4.0 and Windows 2000 domain controllers to Windows Server 2003 domain controllers and redirect the well-known path for CN=Users and CN=Computers to an organizational unit that the administrator specifies. When you do so, Group Policy settings can apply to containers that are hosting newly created or permanent users and computer accounts.

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 or forest functional level. For the domain functional level, this means that all domain controllers in the domain must be running the Windows Server 2003 operating system.

- If you run the Exchange 2000 **setup /domainprep** command, you receive the error messages that are listed in the "Error Messages That Occur in Exchange 2000 SETUP /DOMAINPREP when CN=Users Is Redirected" section of this article. This issue occurs if the Exchange Enterprise Servers group and Exchange Domain Servers group that are added by Exchange 2000 **setup /domainprep** do not reside in the CN=USERS container. To work around this issue, move the Exchange Enterprise Servers group and the Exchange Domain Servers group that are created by Exchange 2000 **setup /domainprep** from the redirected organizational unit to the CN=Users container. For additional information about Exchange interpretability, click the following article number to view the article in the Microsoft Knowledge Base:

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

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 in either the Active Directory Users and Computers snap-in (Dsa.msc) or the Domains and Trusts (Domains.msc) snap-in. For additional 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 that are created with earlier-version APIs to reside (if the desired OU container does not already exist).

4. Run Redirusr.exe from 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 container-dn
   ```

   Redirusr is installed in the %SystemRoot%\System32 folder on new and upgraded Windows Server 2003-based computers. For example, to change the default location for users created with down-level APIs such as Net User to the OU=Users OU container in the CORP.COM domain, use the following syntax:

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

For additional information about designing group policy infrastructure, visit the following Microsoft Web site:
Designing a Group Policy Infrastructure

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 the Domains and Trusts (Domains.msc) snap-in. For additional 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 reside (if the desired OU container does not already exist).
4. Run Redircmp.exe from 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-dncontainer-dn
   ```

   Redircmp.exe is installed in the %Systemroot%\System32 folder on new and upgraded Windows Server 2003-based 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 CORP.COM domain, use the following syntax:

   ```
   C:\windows\system32>redircomp ou=mycomputers,DC=company,dc=com
   ```

Description of Error Messages

Errors Messages That Occur If the PDC Is Offline

Redircmp and Redirusr modify the **wellKnown** attribute on the primary domain controller (PDC). If the PDC of the domain that is being modified is offline or inaccessible, you receive the following error messages:
D:\>redirusr OU=userOU,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.

   -and-

D:\>redircmp OU=computerOU,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.

Errors Messages That Occur 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:
C:\>redirusr OU=usersou,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: Unwilling To Perform Redirection was NOT successful.

   -and-

C:\>REDIRCMP ou=computersou,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: Unwilling To Perform

Errors Messages That Occur 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:
C:>REDIRCMP OU=computersou,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: Insufficient Rights Redirection was NOT successful.

   -and-

:\>redirusr OU=usersou,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: Insufficient Rights Redirection was NOT successful.

Errors Messages That Occur 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:
C:\>REDIRCMP OU=nonexistantou,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.

  -and-

C:\>redirusr OU=nonexistantou,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.

Errors Messages That Occur in Exchange 2000 SETUP /DOMAINPREP When CN=Users Is Redirected

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

> [HH:MM:SS] Starting Exchange 4417 setup on Windows 2000 5.0.2195.Service Pack 3 at 21:43:31 02/19/2003
> [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

The **wellKnown** attribute that the **redirusr** and **redircmp** commands modify defines the default location that users, computers and groups are created in. You can view the attribute in the root of the domain NC head by using Ldp.exe or Adsiedit.msc. In this example, the Users and Computers organizational units have been redirected to OU=UsersOU and OU=ComputersOU:

```
-----------
Expanding base 'DC=company,DC=com'...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn: DC=company,DC=com
        3> objectClass: top; domain; domainDNS;
        1> distinguishedName: DC=company,DC=com;
        ...
        11> wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:OU=usersou,DC=company,DC=c
                              B:32:AA312825768811D1ADED00C04FD8D5CD:OU=computersou,DC=company,I
                              B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=company,I
                              B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Program Dat
                              B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=company,
                              B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrincipal
                              B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=compa
                              B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=compar
                              B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=company,
```

```
B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=company,DC=com
B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,DC=co
```

REFERENCES

For additional 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

Keywords: kbinfo KB324949
Technology: kbWinServ2003Data kbWinServ2003DataSearch kbWinServ2003Ent kbWinServ2003EntSearch kbWinServ2003Search kbWinServ2003St

---

Send feedback to Microsoft