



Alex Osuna

Setting up CIFS shares and joining the Active Directory

This IBM® Redpaper discusses setting up CIFS shares and joining the Microsoft® Active Directory®.

Why join an N series storage system to Active Directory?

For resources on a network to be locatable, a mechanism must exist for finding the resources easily. In this case, the directory service Active Directory keeps track of all known resources and responds to requests with a list of available devices and services. Before you can be trusted to query for resources, you must be granted membership in the Active Directory domain.

Active directory works on a container basis. A container can be a domain, organization unit (OU), or computer.

Key benefits for joining an IBM System Storage™ N series system to Active Directory include:

- ▶ Controlled security and management through group management; that is, group policy objects (GPOs) and access control lists (ACLs) placed on objects and organization units (OUs)
- ▶ Single-sign-on and pass-through authentication for users
- ▶ Interoperability by extending control beyond the native Windows® environment through the Microsoft management interface by providing a read-only computer management view of:
 - Shared folders, shares, sessions, and open files
 - Local users and groups to the N series storage system

Data ONTAP

Data ONTAP® is a proprietary operating system developed by Network Appliance™; it is not based on the Windows operating system. Consequently, the current Data ONTAP operating

system requires additional rights assigned to the user or to the precreated device object when an administrator or administrator equivalent account is not used. When the computer object has successfully joined the Active Directory domain, the user account credentials will no longer be used and are not stored in any way in the OS. They are used only to allow the N series storage system to become an active member of Active Directory and to write standard properties to the object during the join process (the properties that are written are listed in the next section).

Machines need accounts, too

Every computer running a Windows workstation (Windows NT® 4.0 or higher), Windows Server® operating system, or N series storage system has a computer account. Just as users must have a valid account before being allowed to access a networked resource, it is also requisite that workstations, servers, and other devices that participate in an Active Directory domain have an account, which provides a means for authenticating and auditing computer access to the network and access control, security, and management to domain resources.

Prerequisites

1. Determine the host name of the N series storage system. On the command line, issue the **hostname** command.

```
Data ONTAP (itsotuc2)
login: root
Password:
itsotuc2> Sat Jan  3 14:34:40 MST [telnet_0:info]: root logged in from host:
192
.168.3.242

itsotuc2*> hostname
itsotuc2
```

Figure 1 Issue the hostname command

To determine the IP address of the N series storage system, use the **ifconfig -a** command.

2. Make sure that the N series storage system is licensed for CIFS. To open the FilerView®, open a browser and type:

`http://nserieshostname/na_admin`

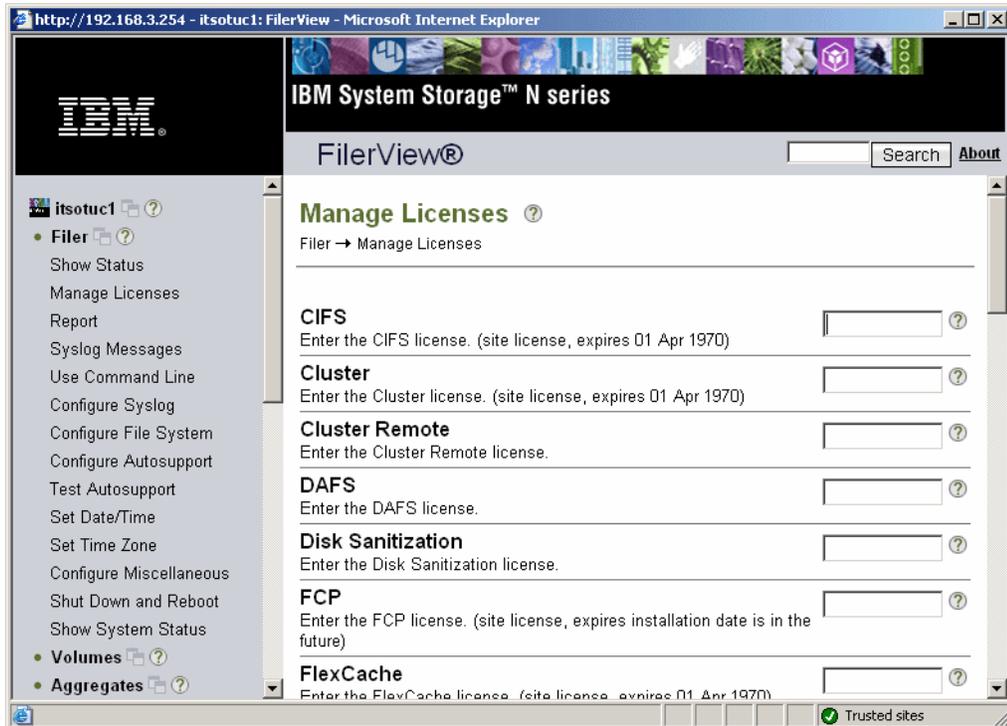


Figure 2 Manage Licenses window

Selecting a user account

In the Active Directory Users and Computers window, select a user account that will be used with precreation of the N series storage system computer object (Figure 3). If you do not already have an appropriate user account, have your Windows administrator create one.

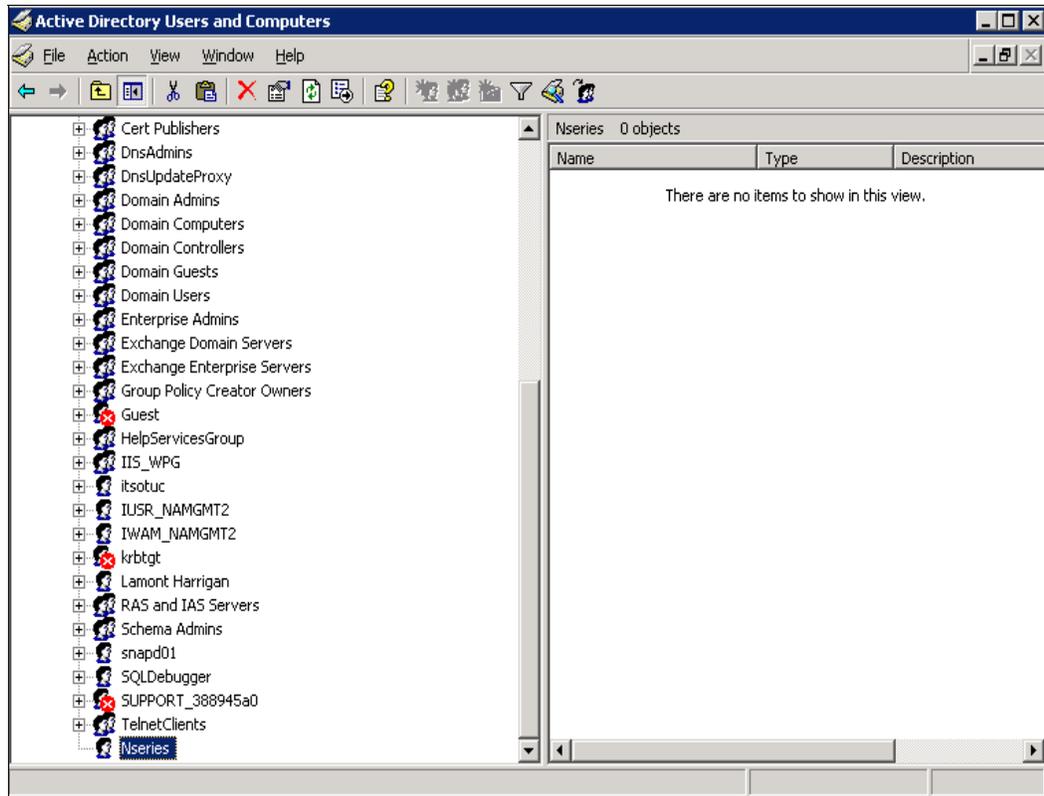


Figure 3 User to be used with creation of N series storage system computer object

Ensuring that the N series storage system acquires minimum operation rights

1. Select **View** from the menu bar, and be sure **Advanced Features** is selected (Figure 4).

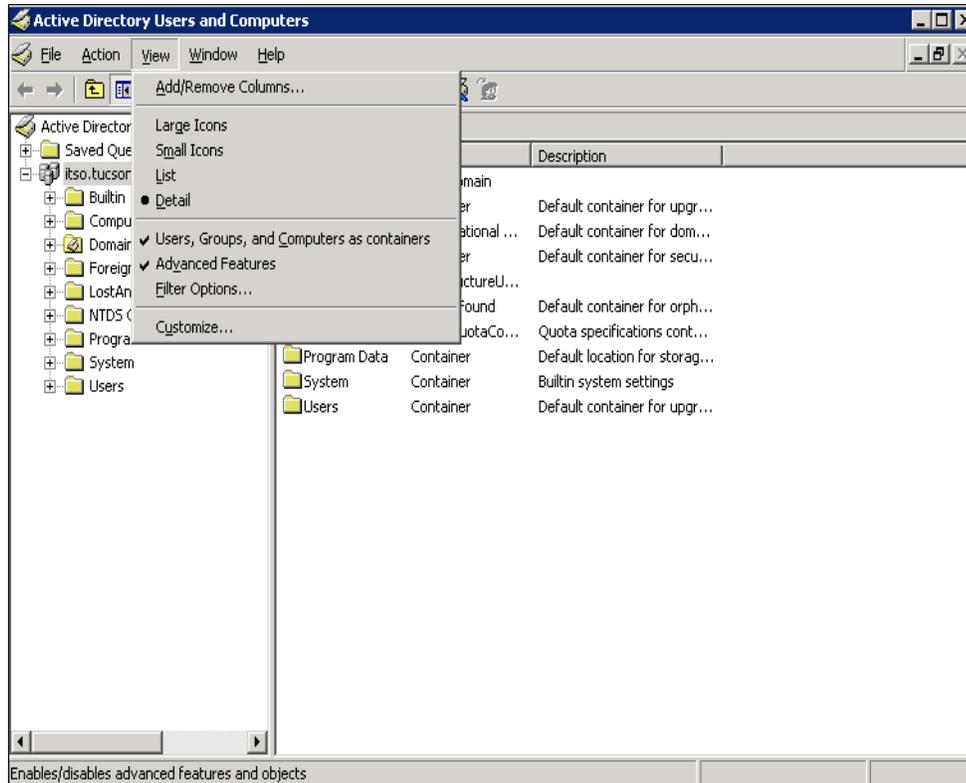


Figure 4 Ensure that Advanced Features is selected

2. Right-click the storage system name and choose **Properties**. Click the **Security** tab (Figure 5).

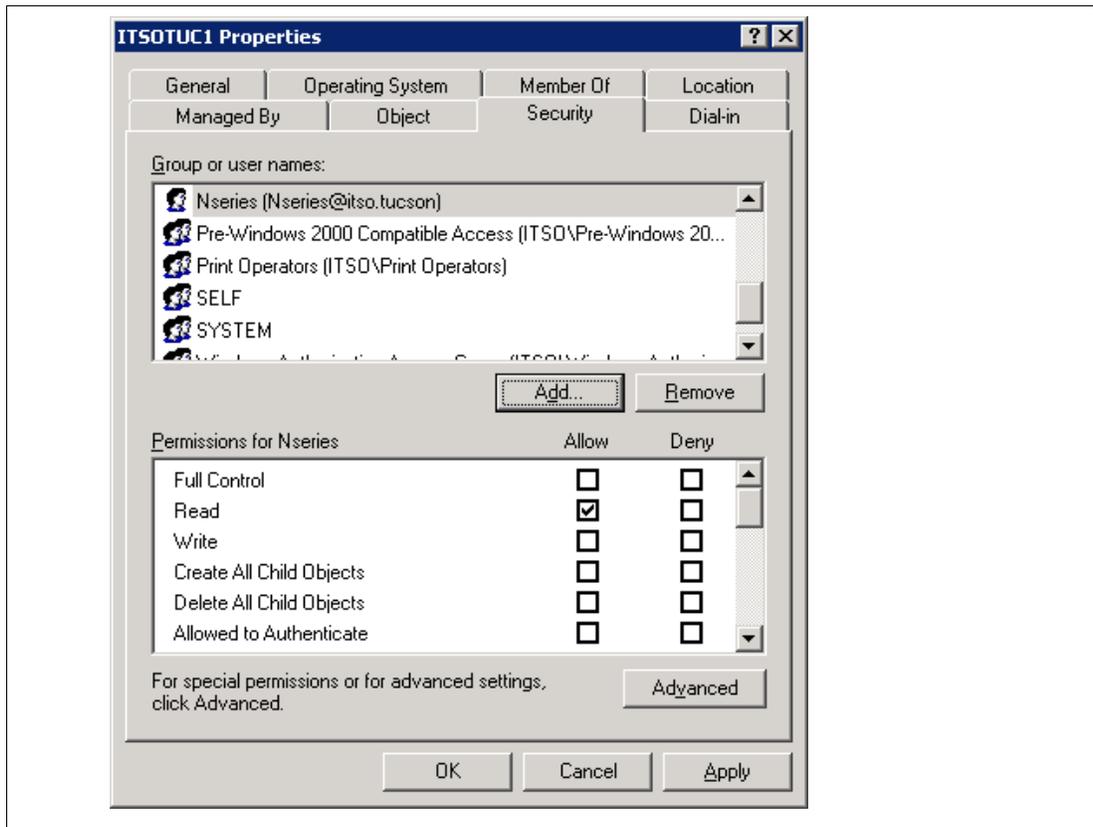


Figure 5 Security tab in Properties dialog

3. In the permissions area, scroll down to be sure that **Change Password** and **Reset Password** are checked (Figure 6).

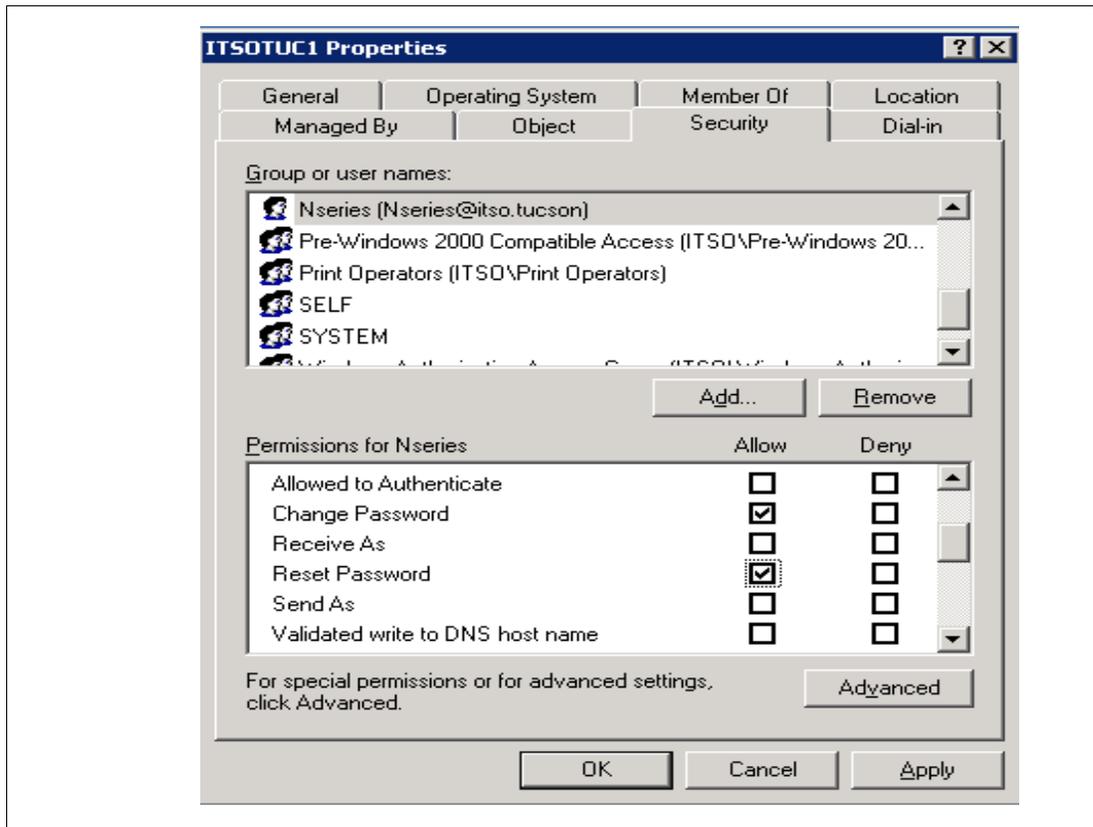


Figure 6 Password permissions

4. Scroll the permissions area again and make sure that **Write Public Information** permission is checked (Figure 7).

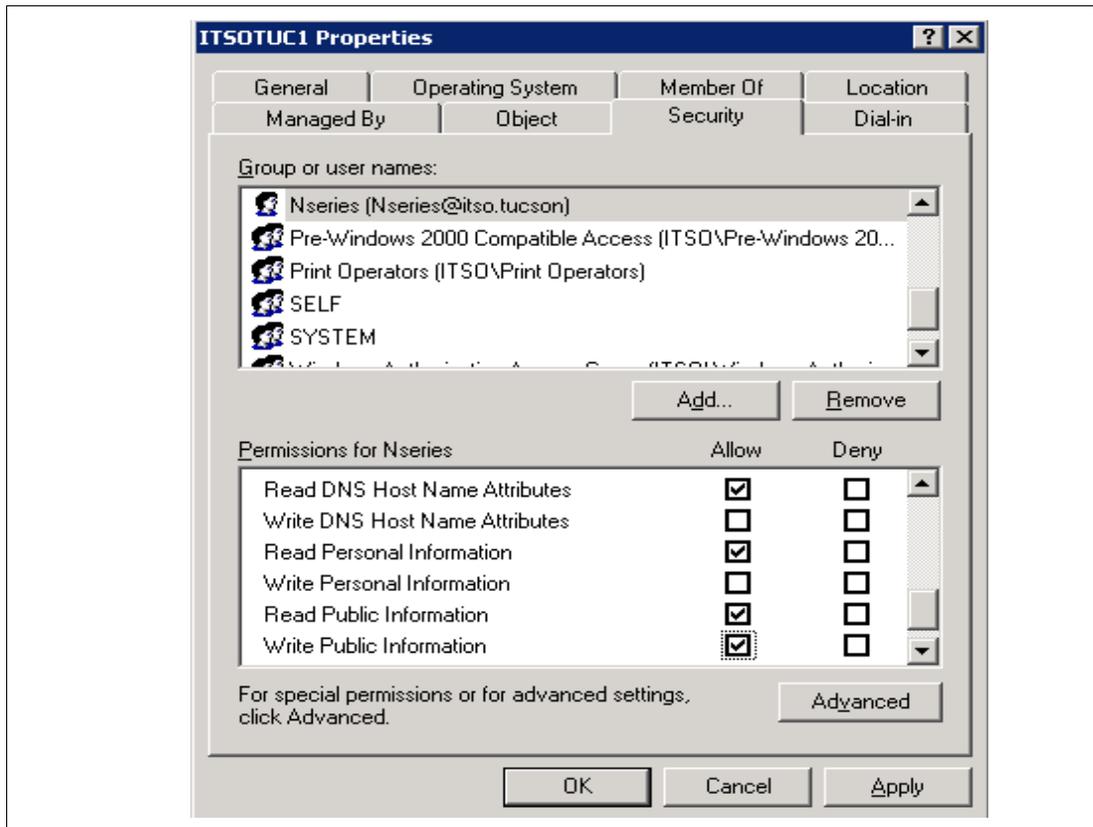


Figure 7 Write Public Information permission

Precreating a computer object

Many Active Directory administrators employ a set of best practices that place strict controls over who can create computer objects. Performing the join as outlined in this section minimizes security risks by eliminating the need for Active Directory administrator rights at the device during the setup process.

You will precreate the computer object using an account with the required privileges, and later use an account with fewer privileges to log on to the computer and issue the appropriate command to complete the join process. Precreating a computer object is the recommended method for joining an N series storage system to Active Directory.

Creating the computer object

For the N series storage system to join the Active Directory, you must create a computer object that references it:

1. Open the Microsoft Management Console (MMC) for Active Directory. Under your domain, right-click **Computer** and select **New** → **Computer** (Figure 8).

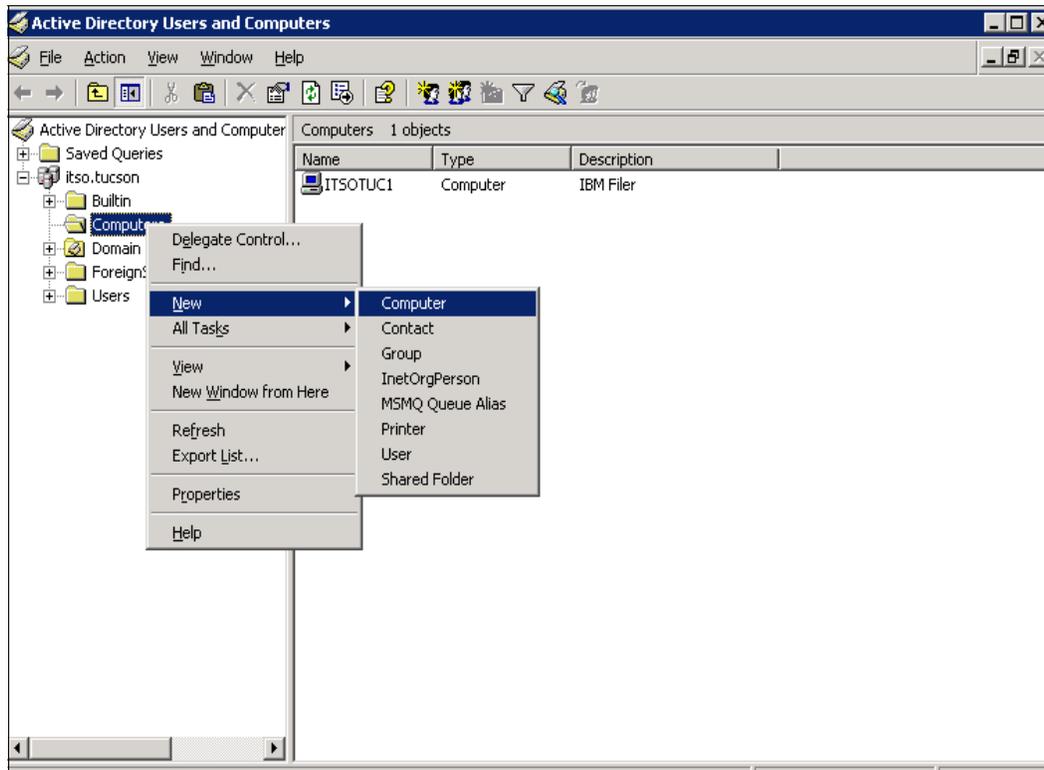


Figure 8 Creating a computer object in Active Directory

- As shown in Figure 9 through Figure 12 on page 11, add a new computer object referencing your N series storage system using the account from “Selecting a user account” on page 4.

Enter a name for the new computer. Click **Change** next to the User or group title. (Figure 9).

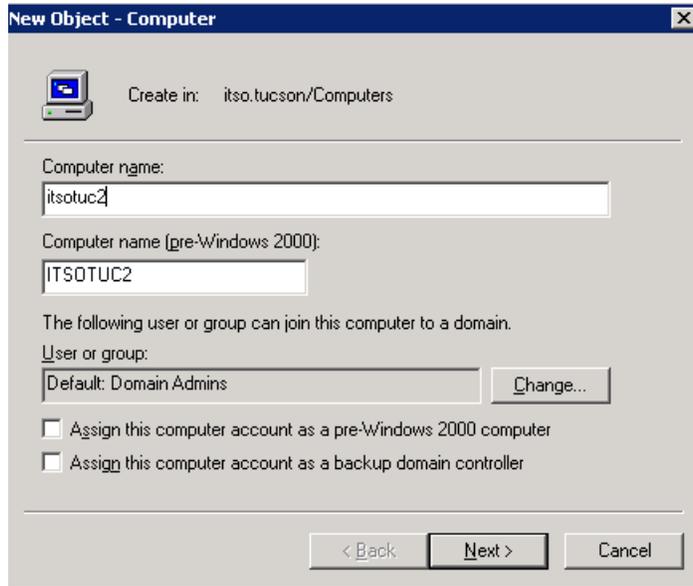


Figure 9 Naming the new computer

- Select the user to manage the N series storage system computer object, (Figure 10) and click **OK**.

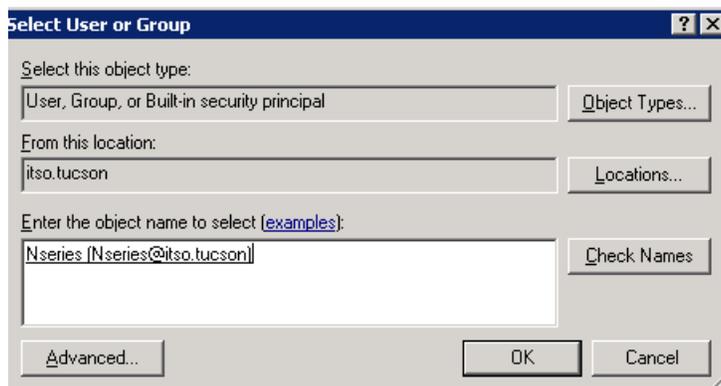


Figure 10 Selecting user for N series storage system computer object

4. Figure 11 shows the result of the user change. Click **Next**.

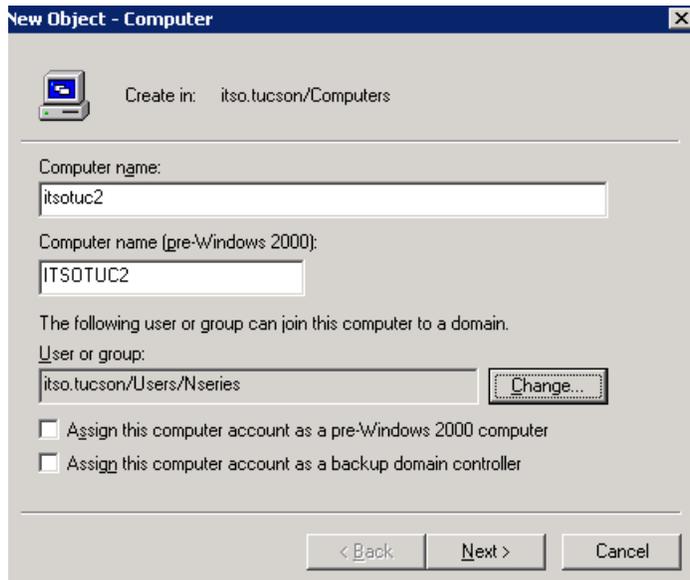


Figure 11 Results of specifying user

5. To create an account for a managed computer, check the box next to **This is a managed computer**, and enter the complete GUID (Figure 12). Click **Next**.

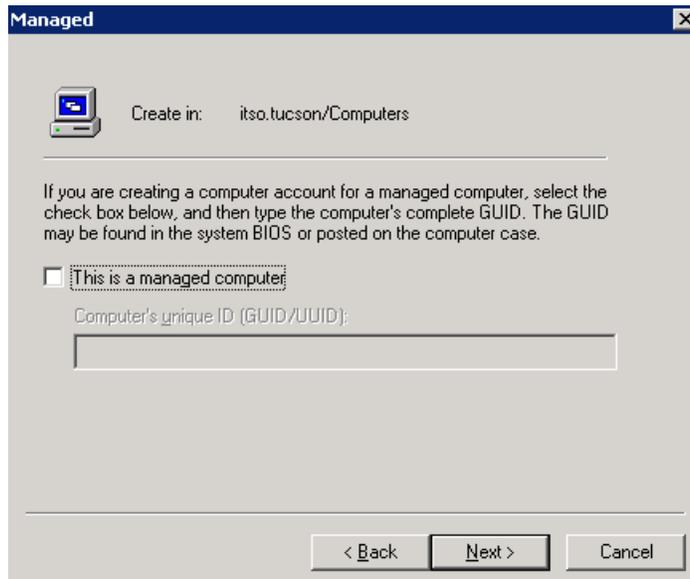


Figure 12 Creating a computer object

6. Confirm your entry and click **Finish** to create the object (Figure 13).

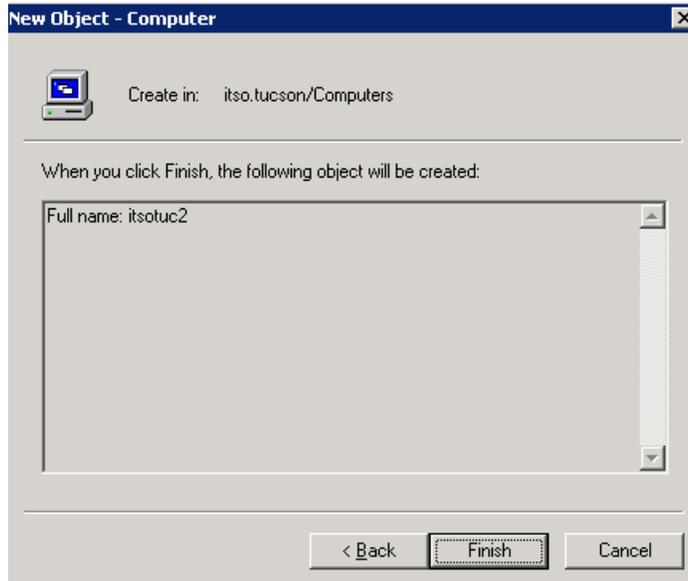


Figure 13 Last step in computer object creation

7. The newly created computer object for the N series storage system should appear in the computer object container of your Active Directory (Figure 14).

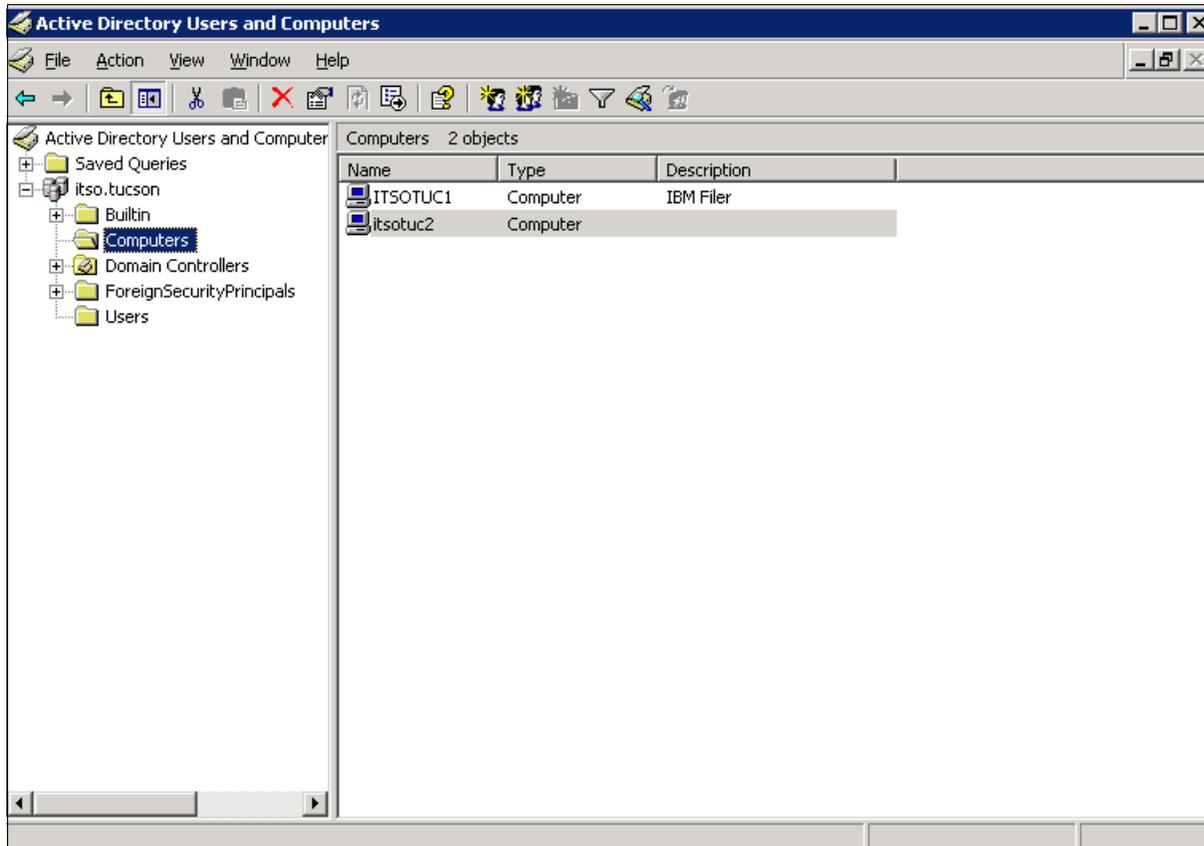


Figure 14 Verification of computer object creation

When the Active Directory join process is complete, a number of properties are written to the computer account, including:

- ▶ DNS host name
- ▶ Several service principal names
- ▶ Object classes
- ▶ Operating system name and version
- ▶ A randomly generated password for this account, set via KPASSWD

Note: This is the only instance in which the N series storage system join process differs from the Microsoft join process. Microsoft uses proprietary RPC calls to change the password, but the N series storage system uses the published KPASSWD APIs to accomplish this task.

Running CIFS setup with the N series storage system

1. In our example, we used the CIFS setup wizard from the command line. Type `cifs setup` to begin (Figure 15).

```
itsotuc2> cifs setup
This process will enable CIFS access to the filer from a Windows(R) system.
Use "?" for help at any prompt and Ctrl-C to exit without committing changes.
```

Figure 15 CIFS setup

2. When asked to confirm changing the account information, type `y` (yes) to continue (Figure 16).

```
          This filer is currently a member of the Windows-style workgroup
          'WORKGROUP'.
Do you want to continue and change the current filer account information? [n]:
y
```

Figure 16 Filer account

3. Type `n` to take the default `no` in answer to WINS visibility (Figure 17).

```
          Your filer does not have WINS configured and is visible only to
          clients on the same subnet.
Do you want to make the system visible via WINS? [n]: n
```

Figure 17 WINS setup

4. Take the default `n` to the NTFS-only question, because you want multiprotocol access (Figure 18).

```
          This filer is currently configured as a multiprotocol filer.
          Would you like to reconfigure this filer to be an NTFS-only filer? [n]: n
```

Figure 18 Protocol setup

5. Keep the name assigned to the N series storage system during initial setup, by taking the default n (Figure 19).

```
The default name for this CIFS server is 'ITS0TUC2'.  
Would you like to change this name? [n]: n
```

Figure 19 Name designation

6. In our example we joined the Active Directory so we selected 1 (Figure 20).

```
Data ONTAP CIFS services support four styles of user authentication.  
Choose the one from the list below that best suits your situation.  
  
(1) Active Directory domain authentication (Active Directory domains only)  
(2) Windows NT 4 domain authentication (Windows NT or Active Directory domains)  
(3) Windows Workgroup authentication using the filer's local user accounts  
(4) /etc/passwd and/or NIS/LDAP authentication  
  
Selection (1-4)? [1]: 1
```

Figure 20 Active Directory selection

7. Specify the Active Directory Domain name itso.tucson (Figure 21).

```
What is the name of the Active Directory domain? []:itso.tucson
```

Figure 21 Active Directory domain

8. Specify the user account that was designated in “Selecting a user account” on page 4 (Figure 22).

```
In order to create an Active Directory machine account for the filer,  
you must supply the name and password of a Windows account with  
sufficient privileges to add computers to the ITS0.TUCSON domain.  
Enter the name of the Windows user []: Nseries
```

Figure 22 Enter the previously selected user

9. Enter the password for the designated user (Figure 23).

```
Password for Nseries:
```

Figure 23 Password entry

10. The setup process recognizes that we preconfigured the computer object and asks whether to reuse this object. Answer yes (Figure 24).

```
CIFS - Logged in as Nseries@ITSO.TUCSON.  
  An account that matches the name 'ITSOTUC2' already exists in Active  
  Directory: 'cn=itsotuc2,cn=computers,dc=itso,dc=tucson'. This is  
  normal if you are re-running CIFS Setup. You may continue by using  
  this account or changing the name of this CIFS server.  
Do you want to re-use this machine account? [y]: y
```

Figure 24 Account reuse option

11. The SMB protocol starts, and asks whether to specify other users to administer the N series storage system. In our example we took the default no. After this response, a confirmation of joining the Active directory appears (Figure 25).

```
CIFS - Starting SMB protocol...  
  Currently the user "ITSOTUC2\administrator" and members of the group  
  "ITSO\Domain Admins" have permission to administer CIFS on this filer.  
  You may specify an additional user or group to be added to the filer's  
  "BUILTIN\Administrators" group, thus giving them administrative  
  privileges as well.  
Would you like to specify a user or group that can administer CIFS? [n]: n  
  
Welcome to the ITSO.TUCSON (ITSO) Active Directory(R) domain.  
  
CIFS local server is running.  
itsotuc2>
```

Figure 25 CIFS setup completion

12. To verify and get more information about the domain you just joined, use the `cifs domaininfo` command (Figure 26).

```
IBM Storage System N3700
itsotuc1*> cifs domaininfo
NetBios Domain:      ITS0
Windows 2000 Domain Name: itso.tucson
Type:                Windows 2000
Filer AD Site:      none

Current Connected DCs:  \\CHRISANTHY
Total DC addresses found: 4
Preferred Addresses:
                    None
Favored Addresses:
                    None
Other Addresses:
                    192.168.3.242   CHRISANTHY   PDC
                    192.168.88.1    PDC
                    9.11.218.250    PDC
                    192.168.110.1   PDC

Not currently connected to any AD LDAP server
Preferred Addresses:
                    None
Favored Addresses:
                    None
Other Addresses:
                    None
itsotuc1*>
```

Figure 26 Output from `cifs domaininfo` command

Should Active Directory be in mixed or native mode?

Note: The terms *mixed mode* and *native mode* refer to functional levels in a Windows 2000 Server. In Windows 2003 Server, the terms mixed and native have been superseded by *Raise Function Level*.

Domain function levels (mixed and native)

There are now four domain levels in which a Windows 2003 Server can operate:

- ▶ Windows 2003 Server. All Windows 2003 Servers, no other domain controllers. However, even at this level, the whole range of clients (including N series storage systems) and member servers can still join the domain.
- ▶ Windows 2003 Server interim. Windows NT 4.0 servers and Windows 2003 Servers (but not Windows Server 2000). This level arises when you upgrade a Windows NT 4.0 PDC to a Windows 2003 Server. Interim mode is important when you have Windows NT 4.0 groups with more than 5000 members. Windows Server 2000 does not allow you to create groups with more than 5000 members.

- ▶ Windows 2000 native. Allows Windows Server 2000 and Windows 2003 Server (but not Windows NT 4.0).
- ▶ Windows 2000 mixed. Allows Windows NT 4.0 BDCs and Windows 2000 Server. Naturally Windows 2000 mixed is the default function level, because it supports all types of domain controllers.

N series storage systems

An N series storage system may be joined to Active Directory whether in mixed, native, interim, or pure Windows 2003 Server mode.

Troubleshooting the domain-joining process

It is not uncommon to encounter errors when during the domain-joining process. This section lists some of the most common challenges when joining the domain.

DNS

To determine whether the IBM N series is joining a Windows NT 4.0 domain or Active Directory, and to locate domain controllers, a key distribution center (KDC used for Kerberos), and other necessary services, CIFS relies on DNS. If DNS is not enabled or is configured incorrectly, the domain-joining phase either will fail or, if a Microsoft Windows Internet-naming server (WINS) is running, assume that the domain being joined is a Windows NT 4.0 domain.

Time synchronization

If time synchronization is not enabled, and the N series storage system's time drifts by more than five minutes from the domain's time, client authentication attempts to the N series storage system will fail until corrected.

Active Directory replication

Based on the size of the Active Directory domain, to propagate a change for a small organization with one site, the replication will usually take less than 15 minutes. For a global company with many sites, the replication might take up to several hours to complete.

Device discovery

The N series storage system performs an intelligent discovery process to locate the most appropriate domain controller (DC) in the network with which to communicate. For its first connection, Data ONTAP attempts to use servers that appear in the CIFS prefdc list (in list order), if configured. (See Figure 27 and Figure 28 on page 18.) If none of these preferred servers is available, or if none is configured, all server addresses are discovered at once, then categorized, prioritized, and cached.

```
itsotuc2> cifs prefdc print
No preferred Domain Controllers configured.
DCs will be automatically discovered.
```

Figure 27 *prefdc list with nothing configured*

```
itsotuc2> cifs prefdc print
Preferred DC ordering per domain:

ITS0:
    1. 192.168.3.242
```

Figure 28 cifs prefdc print with prefdc configured

Preferred addresses are ordered as specified using the **cifs prefdc** command. “Favored” and “other” categories are sorted according to the fastest response. Data ONTAP simultaneously pings all addresses listed in both categories and waits one second for responses.

The **cifs prefdc** command allows control over the order in which Data ONTAP attempts to contact a server. The list is consulted for all Windows service connections, not just domain controllers.

When configuring CIFS on an N series device in a Windows 2000 or 2003 domain, an LDAP query to Active Directory checks to ensure that a computer object with the same name does not already exist. If the name does exist, the setup process makes sure it is not a domain controller. These are precautionary measures that are used to guarantee that no computer object names are duplicated in error.

Conclusion

To locate resources on a network, a mechanism must exist for finding the resources easily. A directory service in this case, Active Directory keeps track of all known resources and responds to requests with a list of currently available devices and services. But before you can be trusted to query for resources, you must be granted membership in the domain. Joining a domain accomplishes two tasks. First, for an N series storage system, it grants the required rights to query Active Directory if it needs to find other resources. Second, it provides a single management interface through MMC for administration of security and users' access levels to the N series storage system.

About the Redpaper author

Alex Osuna is a Project Leader at the International Technical Support Organization in Tucson, Arizona. He writes extensively and teaches IBM classes worldwide about all areas of storage. Before joining the ITSO he was a Systems Engineer with Tivoli®. He has been involved with storage for more than 26 years and the I/T industry for more than 28 years, in service, planning, early ship programs, Advanced Technical Support, and Systems Engineering. He holds more than 10 certifications from IBM, Microsoft, and Red Hat.

Contributors

Piet de Jonge

IBM IT Education Services

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

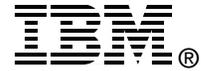
This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Send us your comments in one of the following ways:

- ▶ Use the online **Contact us** review redbook form found at:
ibm.com/redbooks
- ▶ Send your comments in an e-mail to:
redbook@us.ibm.com
- ▶ Mail your comments to:
IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400 U.S.A.



Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM®
Redbooks (logo) ™

System Storage™
Tivoli®

The following terms are trademarks of other companies:

Active Directory, Microsoft, Windows NT, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

NetApp, the Network Appliance logo, the bolt design, DataFabric, FAServer, FilerView, MultiStore, NearStore, NetCache, SecureShare, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapVault, SyncMirror, and WAFL are registered trademarks, and Network Appliance, ApplianceWatch, BareMetal, Camera-to-Viewer, Center-to-Edge, ContentDirector, ContentFabric, Data ONTAP, EdgeFiler, HyperSAN, InfoFabric, NetApp Availability Assurance, NetApp ProTech Expert, NOW, NOW NetApp on the Web, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Smart SAN, SnapCache, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapMigrator, Snapshot, SnapSuite, SohoCache, SohoFiler, The evolution of storage, Vfiler, VFM, Virtual File Manager, and Web Filer are trademarks of Network Appliance, Inc. in the U.S. and other countries.

Other company, product, or service names may be trademarks or service marks of others.