Using Microsoft Active Directory (AD) with EonNAS 3000 and 5000 in Windows Server 2008

Application Note

Abstract

This application note describes how to use Microsoft Active Directory (AD) service with EonNAS 3000 and 5000 systems in Windows Server 2008 environments.

Table of Contents

Product Models Covered by This Document

This document applies to the following product models:

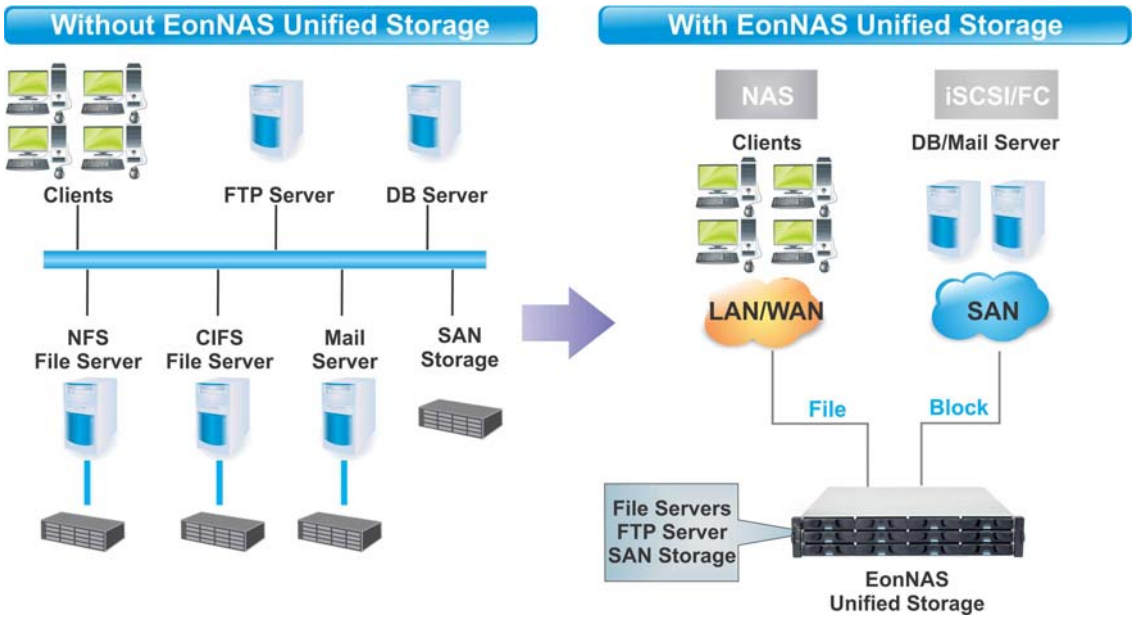
- **EonNAS 3210**
- **EonNAS 3220**
- **EonNAS 3230**
- **EonNAS 5120**

For more information regarding individual product models, please visit www.infortrend.com.

EonNAS Family of Unified Storage Systems

IT environments often feature multiple types of storage infrastructures to accommodate various types of data and achieve different service levels. The scattered boxes for DAS (Direct-Attached Storage), SAN (Storage Area Network) and NAS (Network-Attached Storage) configurations lead to poor utilization and complicated management.

Infortrend EonNAS simultaneously serves file and block-based applications with a unified storage platform, and features easy management, optimized resource utilization, high availability, flexible scalability and competitive price/performance. In addition, EonNAS offers a comprehensive set of advanced software features at no additional costs. EonNAS systems help businesses effectively meet diverse and changing data demand while staying within budget.



Using Microsoft Active Directory (AD) with EonNAS 3000 and 5000 Systems in Windows Server 2008

Microsoft Active Directory (AD) in Windows Server environments is a directory service designed for data management and resource distribution on network environments. Microsoft AD allows storing and sharing data, configuring storage parameters, and managing account information from a central location.

Using Microsoft AD with EonNAS 3000 and 5000 systems offers the following benefits:

- **Simplified account management**
  The same Microsoft AD account name and password can be used for EonNAS; there is no need to manage separate sets of account information.
- **Consolidated access control**
  Read/write rights to shared directories on the network can be controlled from the EonNAS.
- **Enhanced security**
  EonNAS can also benefit from the enhanced data protection protocol integrated in Microsoft AD.

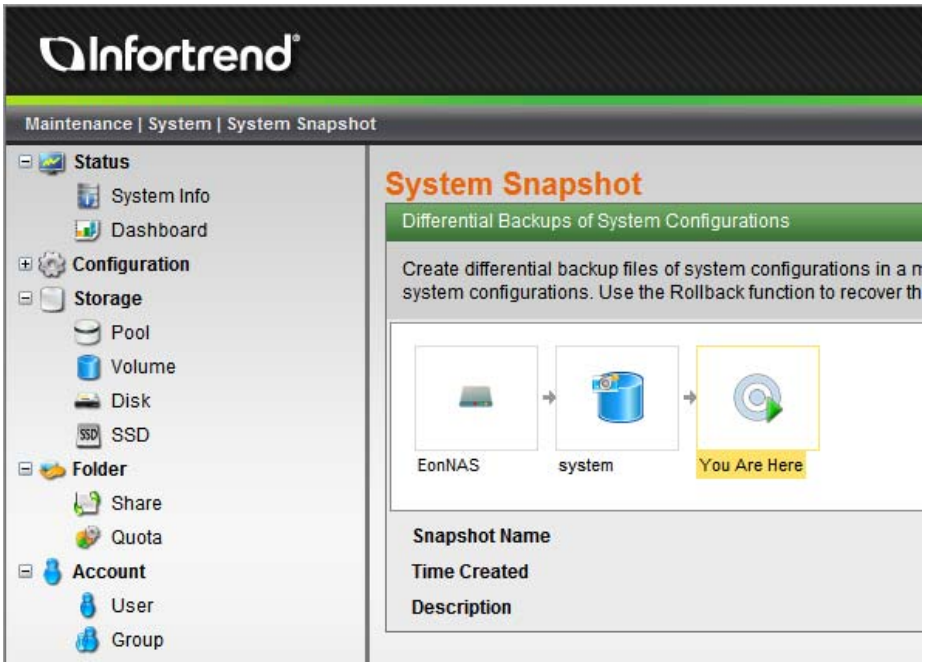
The EonNAS 3000 and 5000 systems are compatible with Microsoft AD for Windows Server 2003 R2 and Windows Server 2008. The following procedures show how to use EonNAS systems with Microsoft AD in Windows 2008.

Step 1: Preparing the Environment

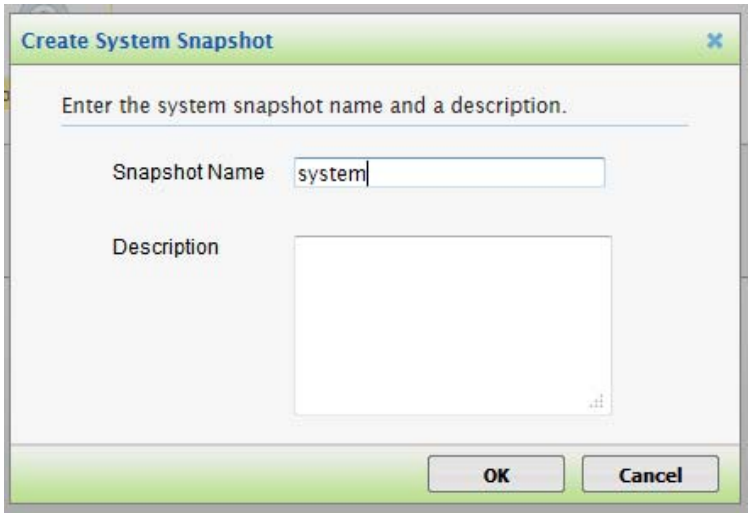
1.1 Take an EonNAS system snapshot.

This snapshot image will be of use in case the EonNAS system encounters errors during user import.

Go to *Maintenance* > *System* > *System Snapshot*.

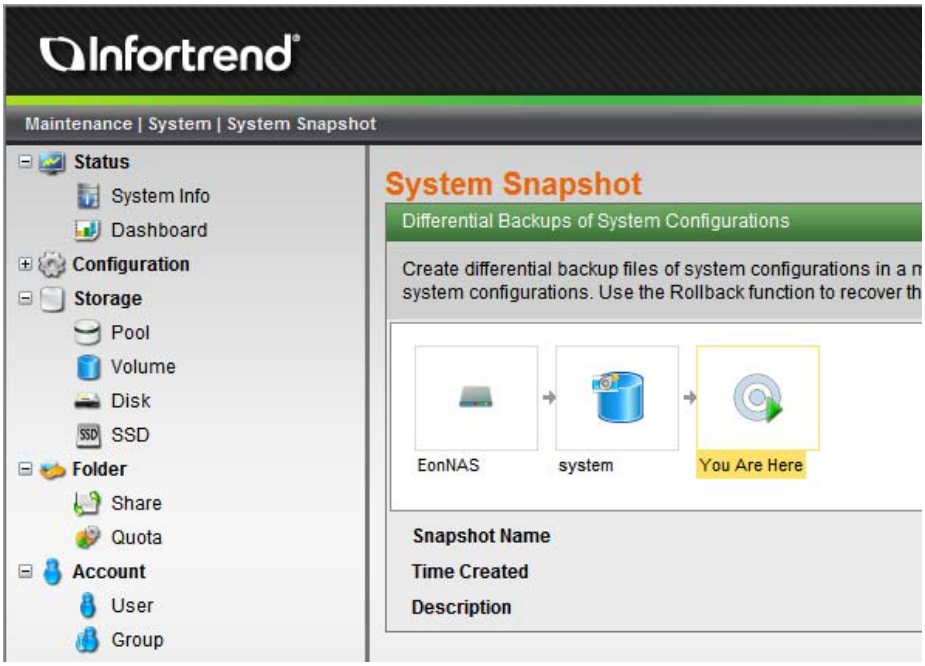


Click on *Take Snapshot*. Enter a snapshot name and add a description.



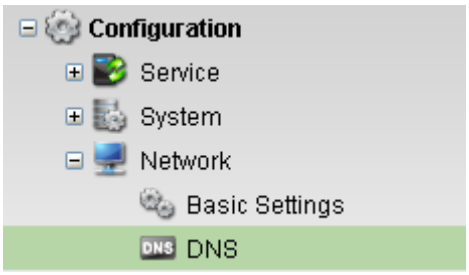
Click on *OK*.

After creation, the snapshot can be found in the system snapshot list.



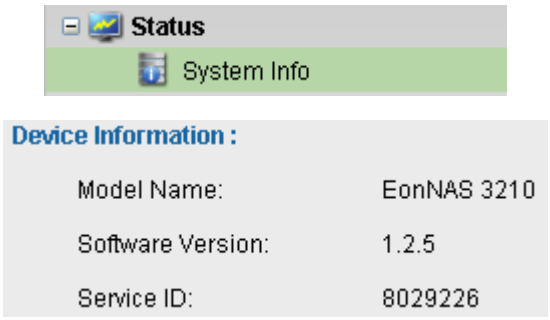
In the event this system snapshot has to be used (system recovery), this recovery will require a short amount of downtime in the form of an EonNAS system reboot. Make sure to properly plan this recovery so that the reboot downtime does not interfere with business applications. For more information about system recovery, please refer to the Appendix.

1.2 Check the NAS DNS IP; this should be the AD server IP address. To check the DNS server IP address, go to *Configuration* > *Network* > *DNS* in the EonNAS GUI.



1.3 The EonNAS and AD server should be synchronized, with a time difference of no more than 5 minutes. To check the date/time settings of the EonNAS, go to *Configuration* > *System* > *Date/Time* in the EonNAS GUI.

1.4 The older EonNAS software version 1.1.15 can not support AD domain names exceeding two levels (for example, abc.foo.com features three levels so the user will not able to add this). To check the software version, go to *Status* > *System Info* in the EonNAS GUI.



1.5 Conduct a Test Run

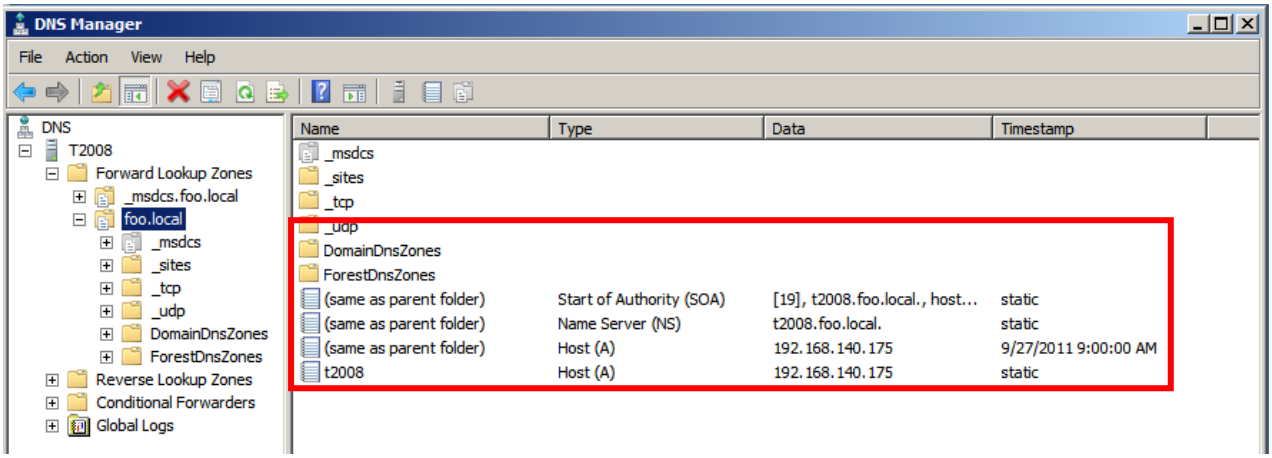
Prepare a test AD server to conduct a practice run before doing the configurations on the operational AD server. In this way, users can ensure that the configurations highlighted in this document work in their specific environments and avoid any damage from unexpected errors that may occur when doing these configurations for the first time.

Step 2: Verifying AD Server DNS

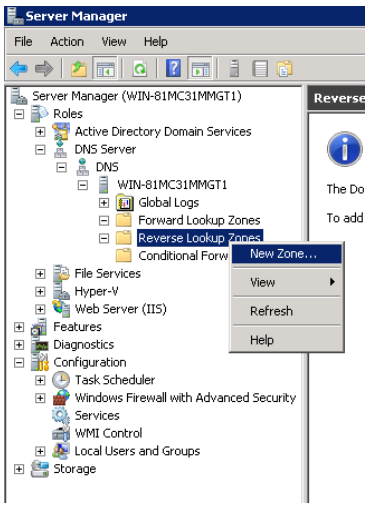
2.1 Open *DNS Manager* by going to *Start* > *Administrative Tools* > *DNS*.

Check the AD server IP settings as well as the *Forward Lookup Zones* and *Reverse Lookup Zones.*

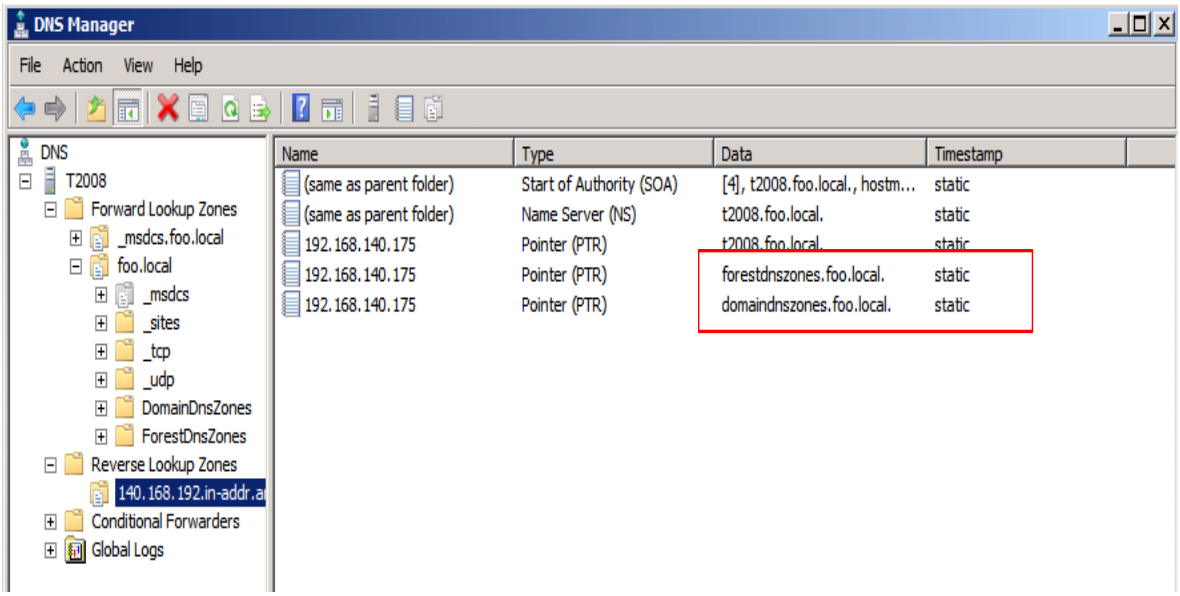
Ensure that the *Forward Lookup Zone* includes *Domaindnszones* and *Forestdnszones*.



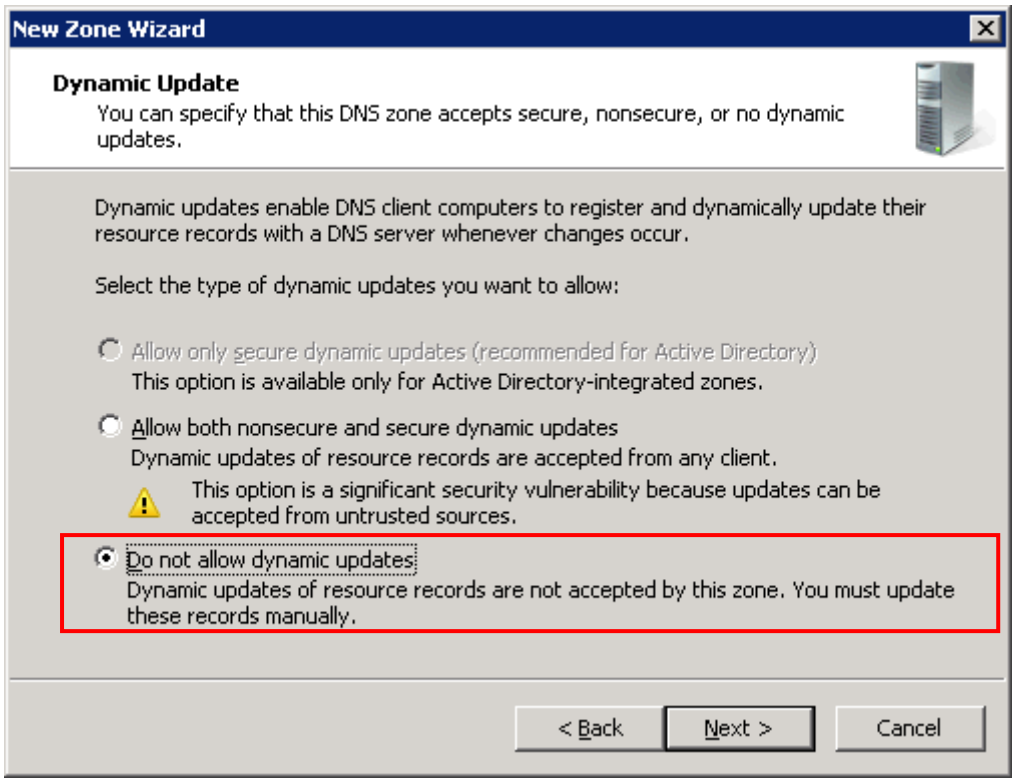
Add a zone in *Reverse Lookup Zones* by right-clicking and selecting *New Zone*, as shown below.



The zone should include *domaindnszones* and *forestdnszones*.



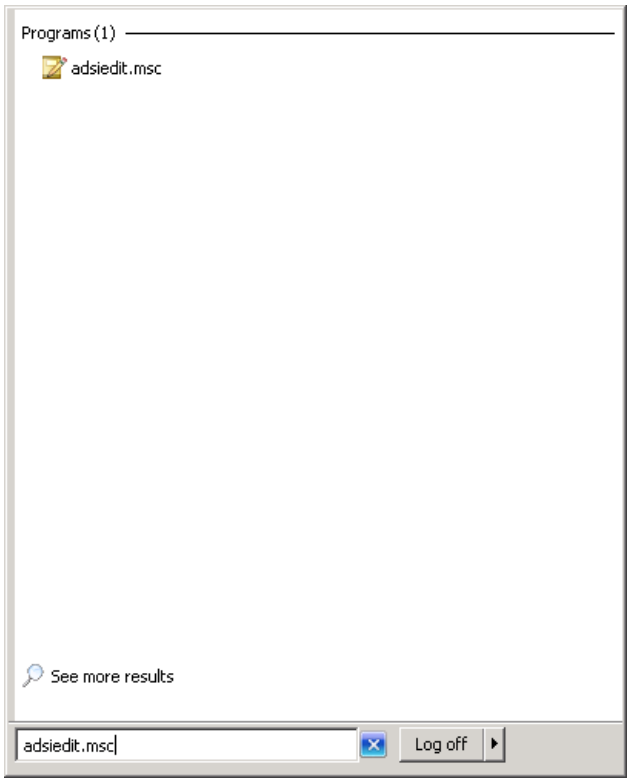
In addition, towards the end of the zone configuration process, the following wizard pops up. In this *New Zone Wizard*, make sure that you do not allow dynamic updates.



2.2 Add *Unix Attribute* tab into the AD server user page by executing the following:

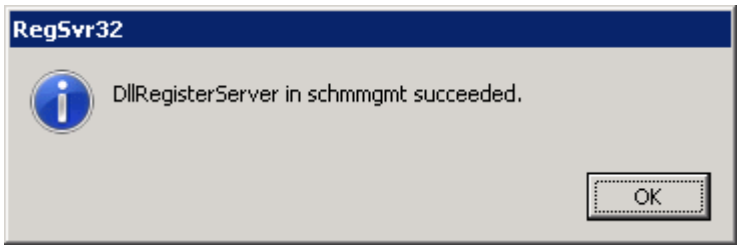
Execute *regsvr32 adsiedit*

Execute *adsiedit.msc*



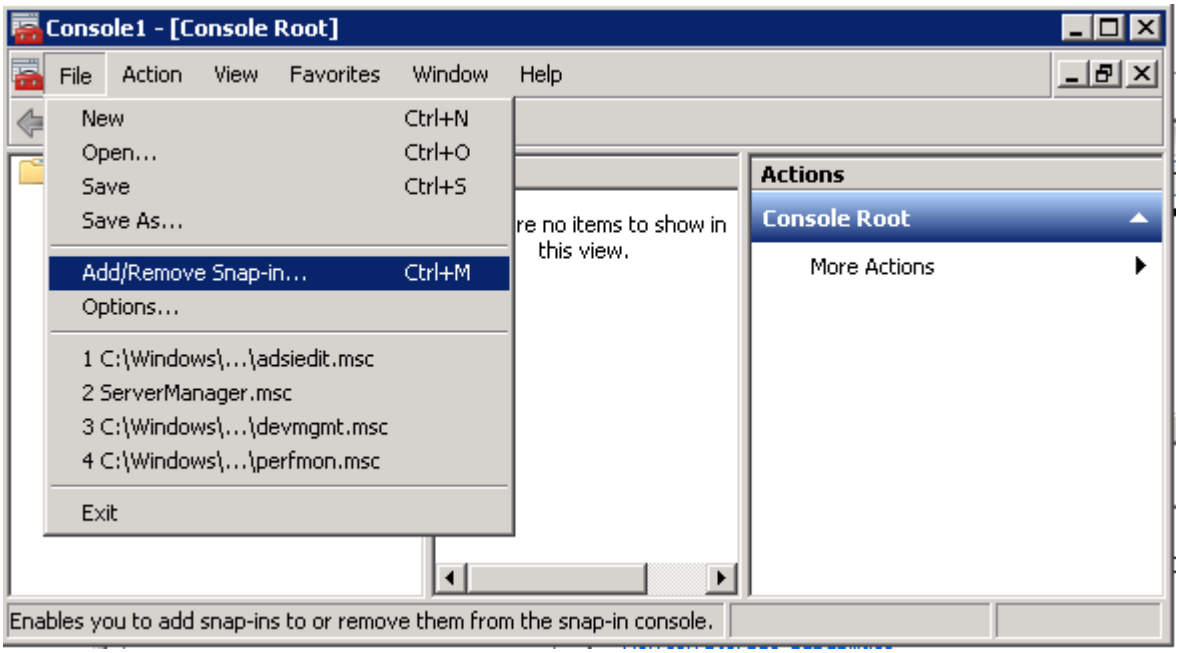
2.3 Add *Schema Management MMC Snap-in* and *Active Directory Schema* into the *Console Root*.

When doing this for the first time, please execute the command *regsvr32 schmmgmt* and click *OK*.

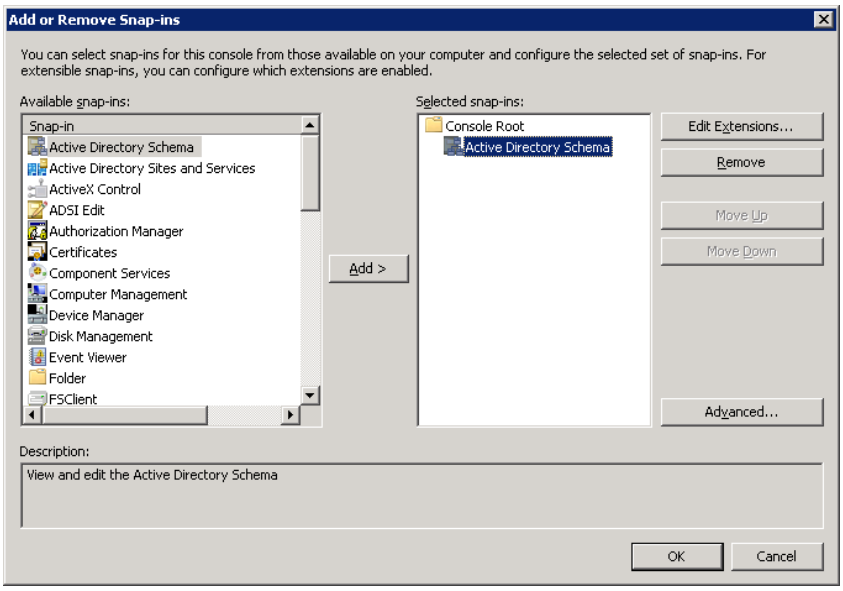


Execute *mmc /a.*

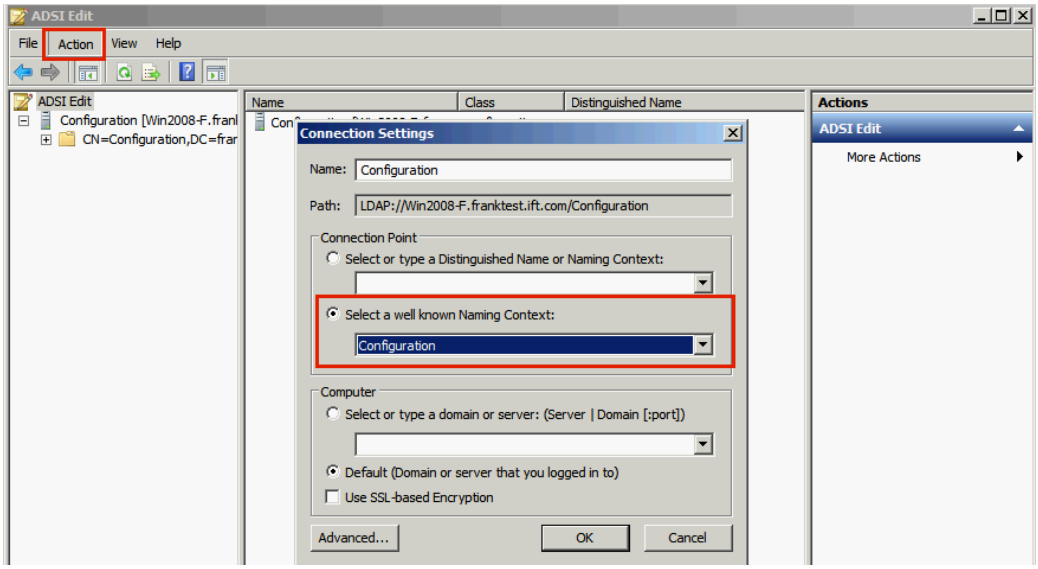
In the console that pops up, click on *Add/Remove Snap-in*.

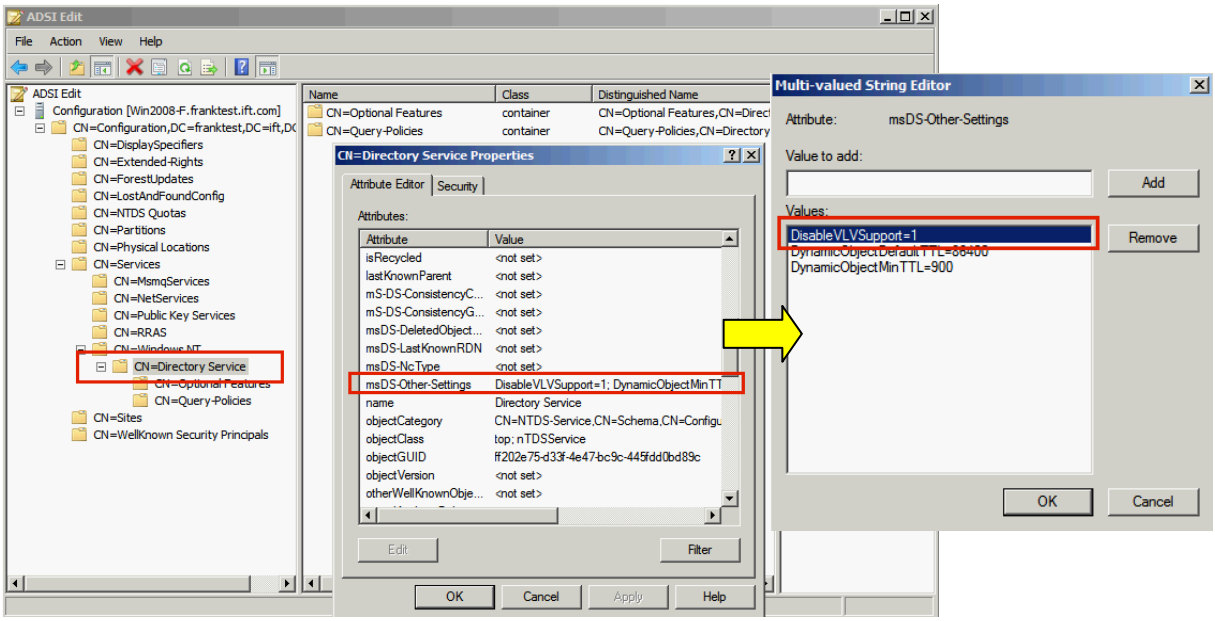


Add *Active Directory Schema* into the *Console Root* by selecting it in the left-side box and moving it to the right-side box by clicking on *Add* >, as shown below.



2.4 In the *ADSI Edit* window, set the attribute value of *DisableVLVSupport* from 0 to 1 by following the steps shown in the screenshots below.





Step 3: Installing Microsoft Patches for Windows Server 2008 (for 2008 and 2008 SP1)

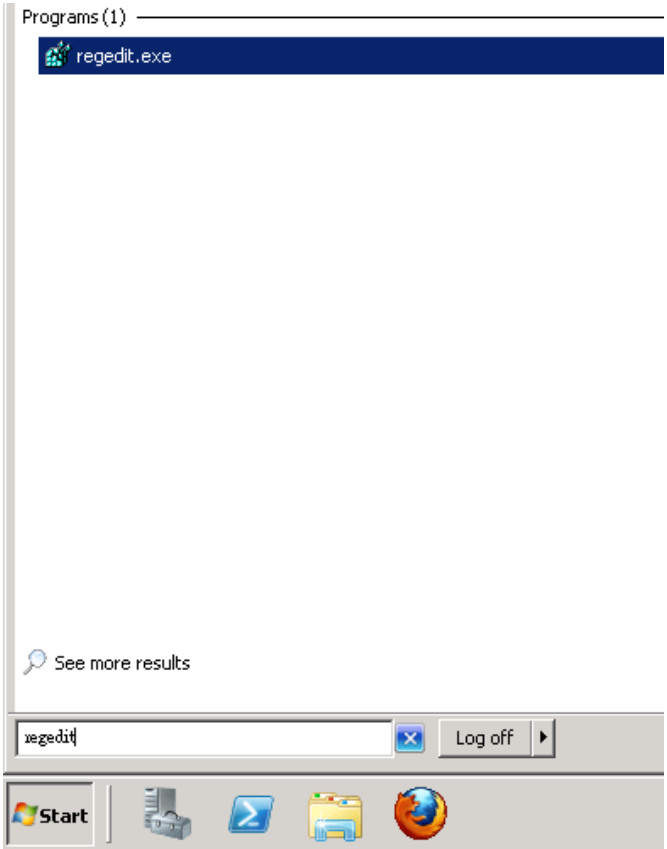
Install the following patches for Windows Server 2008 and 2008 SP1 to fix errors.

http://support.microsoft.com/kb/951191

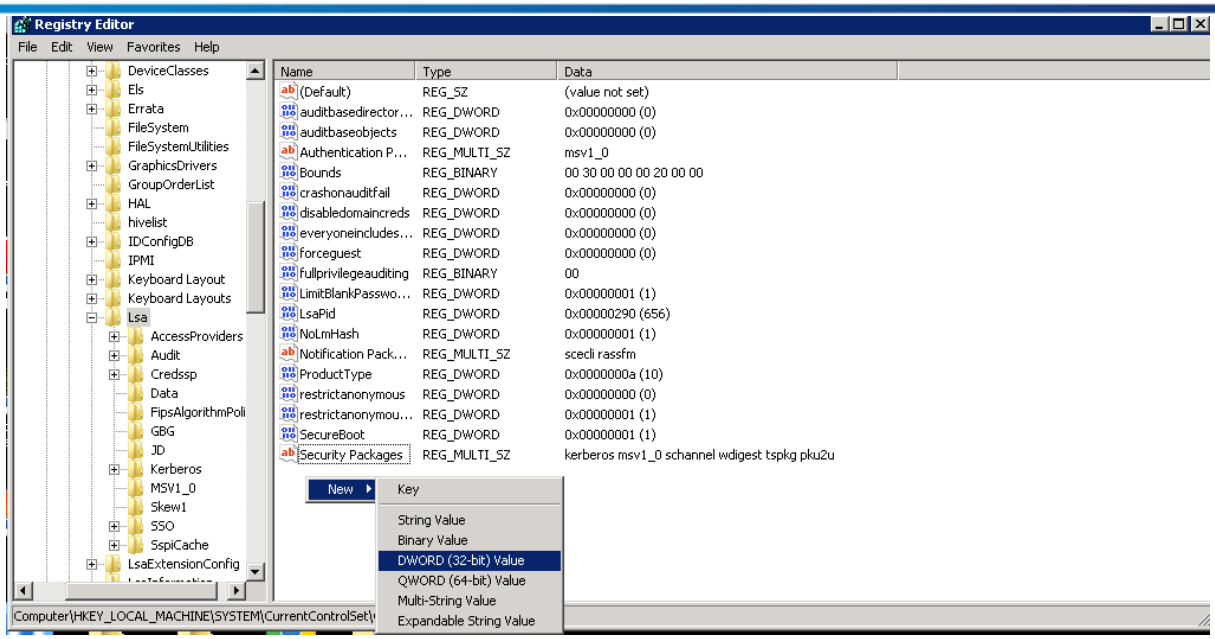
http://support.microsoft.com/kb/957441

Step 4: Modifying Registry in Windows 2008 AD (for 2008 SP2 and 2008 R2)

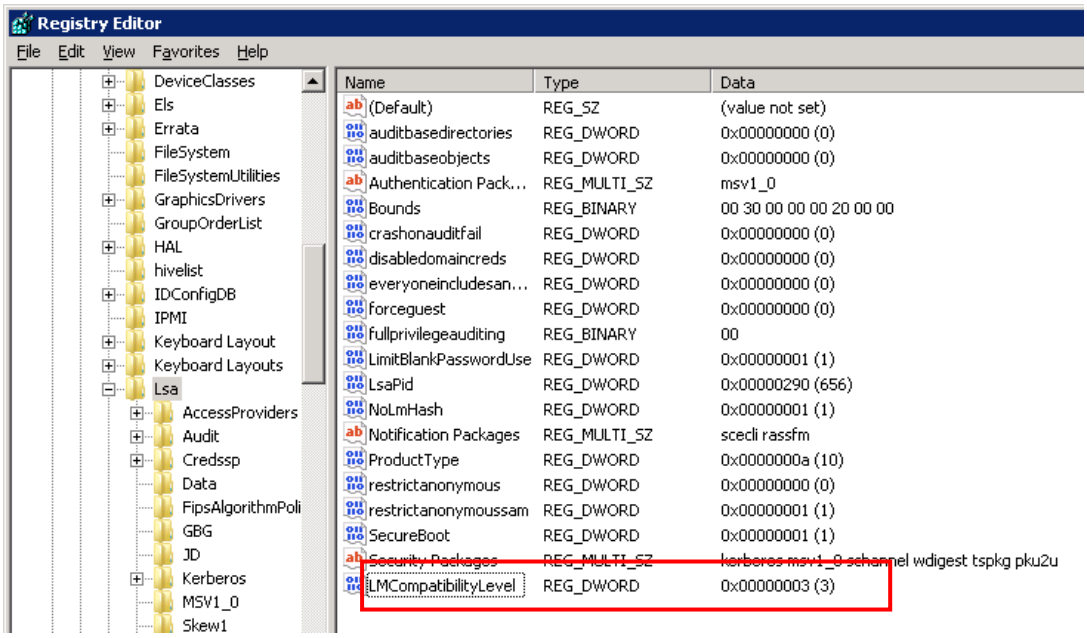
Modify several values in the registry by going to the *Registry Editor* using the command *regedit*.



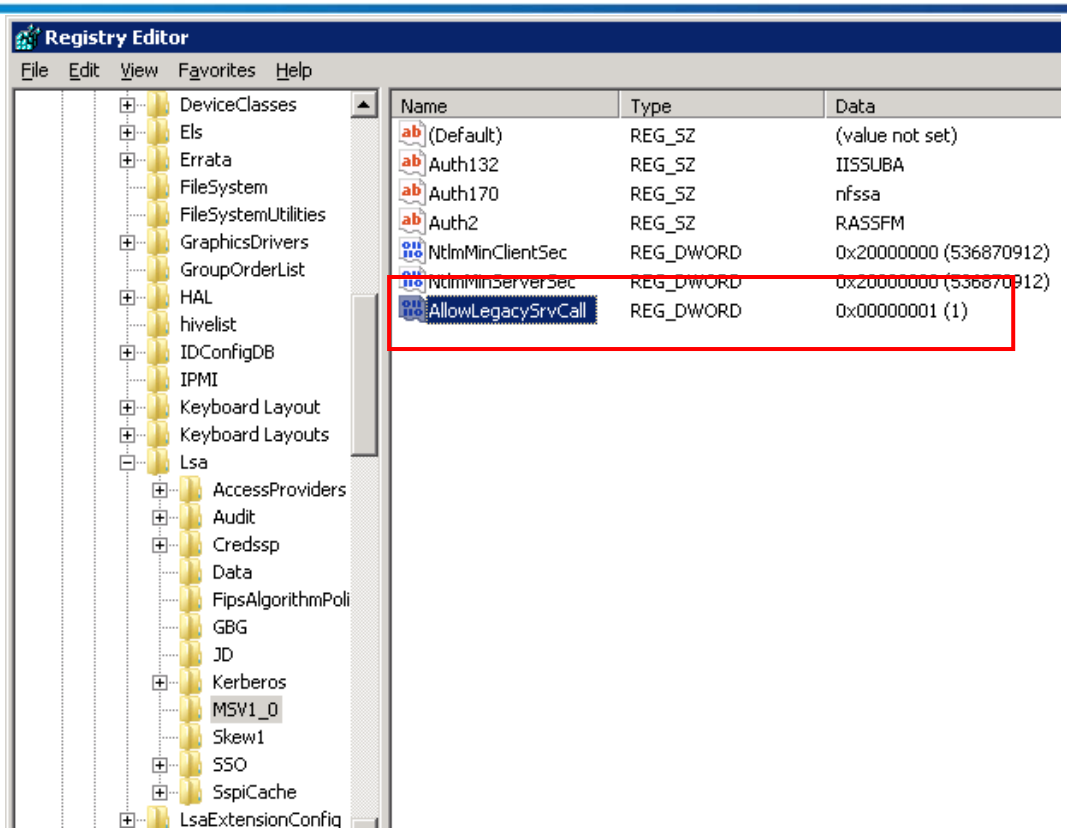
Go to the *Lsa* menu, and select *DWORD (32-bit) Value* after right-clicking on blank space.



Make sure that the *LMCompatibilityLevel* value is 00000003, as shown below.

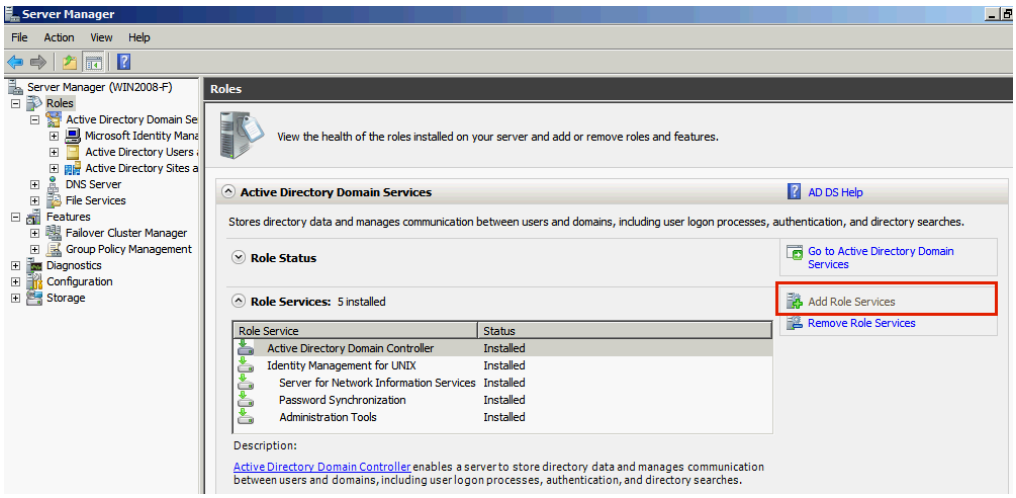


In the *MSV1_0* menu, make sure that the value of *AllowLegacySrvCall* is 00000001, as shown below.

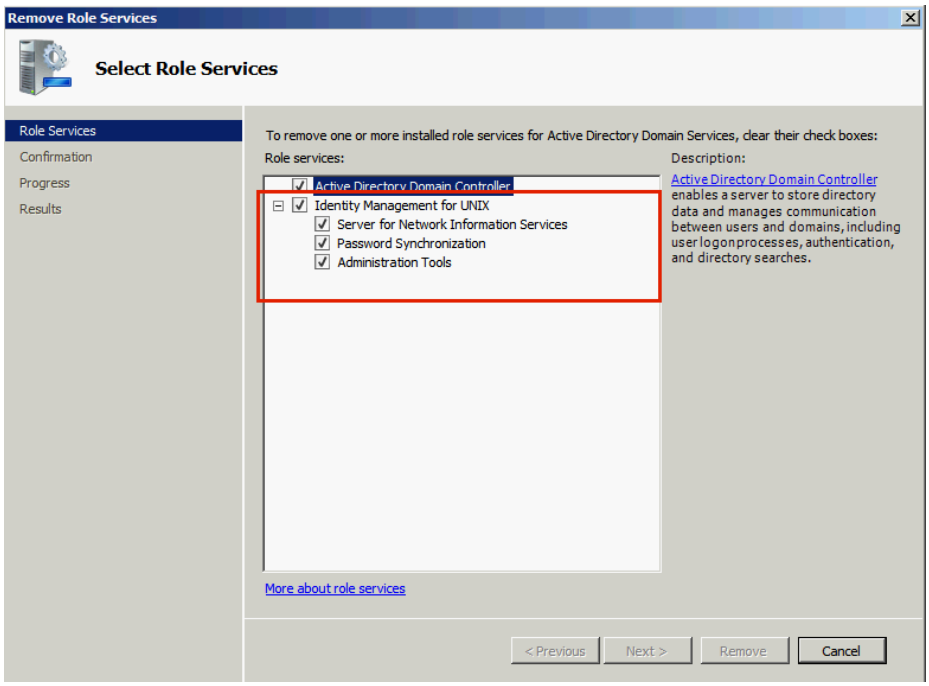


Step 5: Installing Identity Management for UNIX

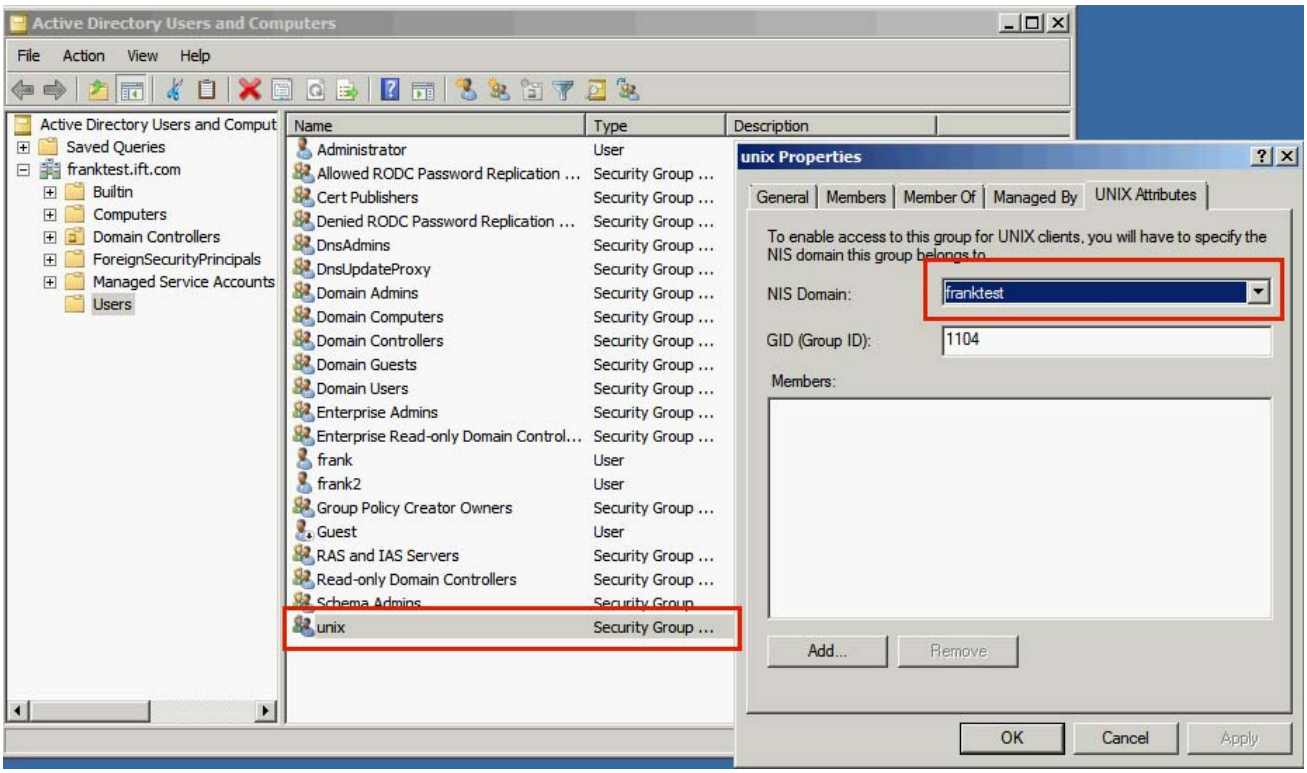
5.1 Go to *Server Manager* > *Roles* and click on *Add Role Services*.



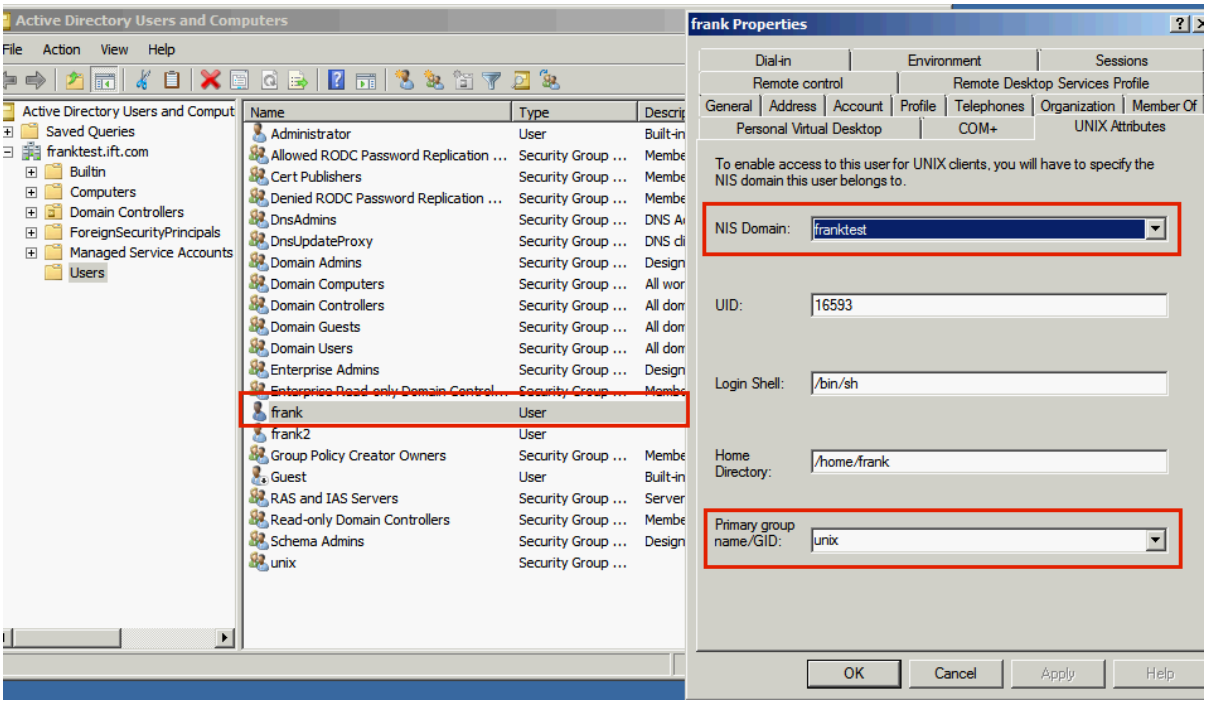
5.2 Check all the options in the next window and click *Next*.



5.3 Select the *unix* security group in *Active Directory Users and Computers* and go to the *Unix Attributes* tab. Choose the *NIC Domain* for your AD.



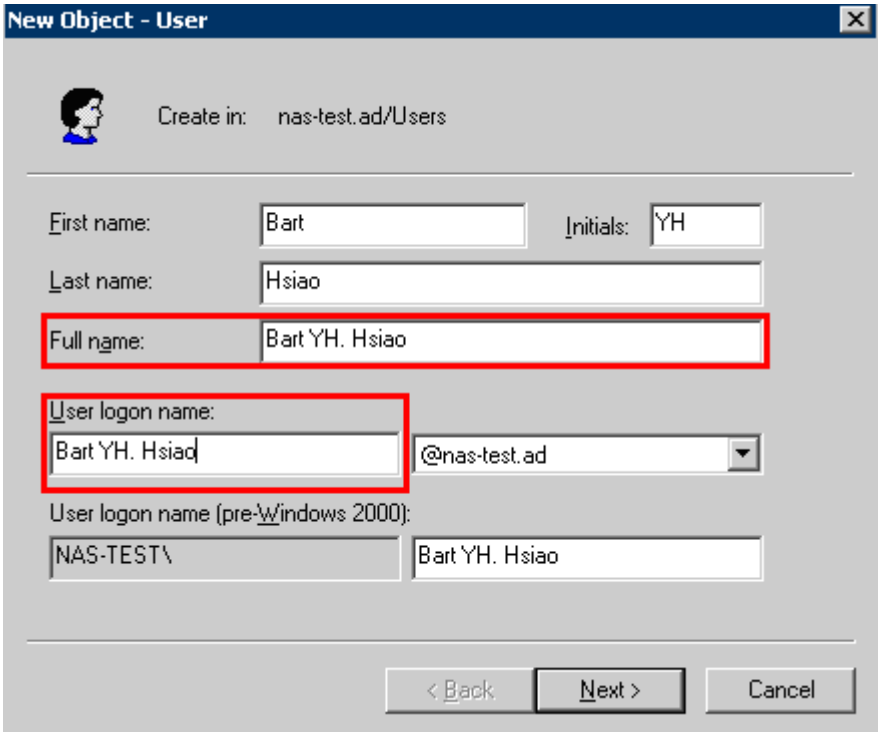
After setting up the UNIX attributes, add user accounts into configured group and NIS domain, as shown in the screenshots below.



Step 6: Configuring AD User Account Settings for Import into EonNAS

AD user accounts have to meet the following criteria:

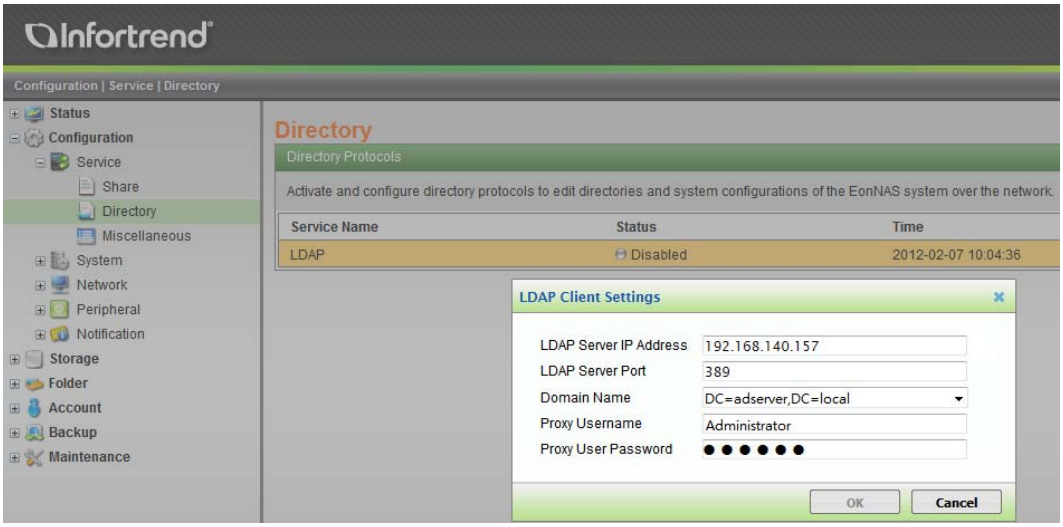
- AD *user logon name* needs to be the same as the *full name.*



- The user logon name length should be less than 20 characters.
- The user logon name can not include the following invalid characters: /\[]:;|=,+*?<>@”

Step 7: Adding AD server to EonNAS

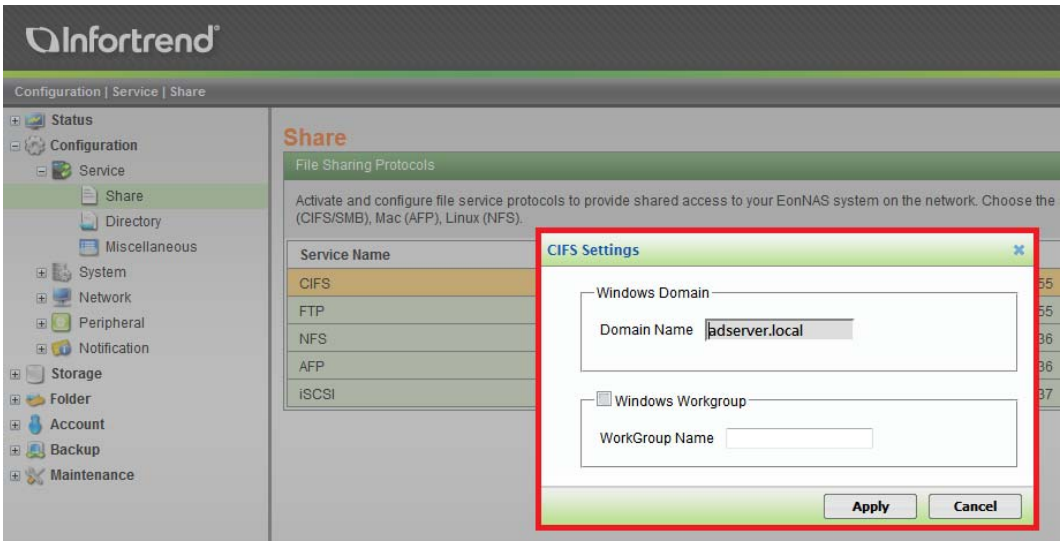
7.1 In the EonNAS GUI, go to *Configuration* > *Service* > *Directory*, select the LDAP service and click on *Edit*. Configure the settings and click *OK* after finishing the settings.



- **LDAP Server IP Address**: Specifies the AD server IP address.
- **LDAP Server Port**: Specifies the server port. This parameter will be assigned automatically according to the IP address.
- **Domain Name**: Specifies the AD server domain name. This parameter will be assigned automatically according to the IP address.
- **Proxy Username**: Specifies the AD server admin username.
- **Proxy User Password**: Specifies the AD server admin password.

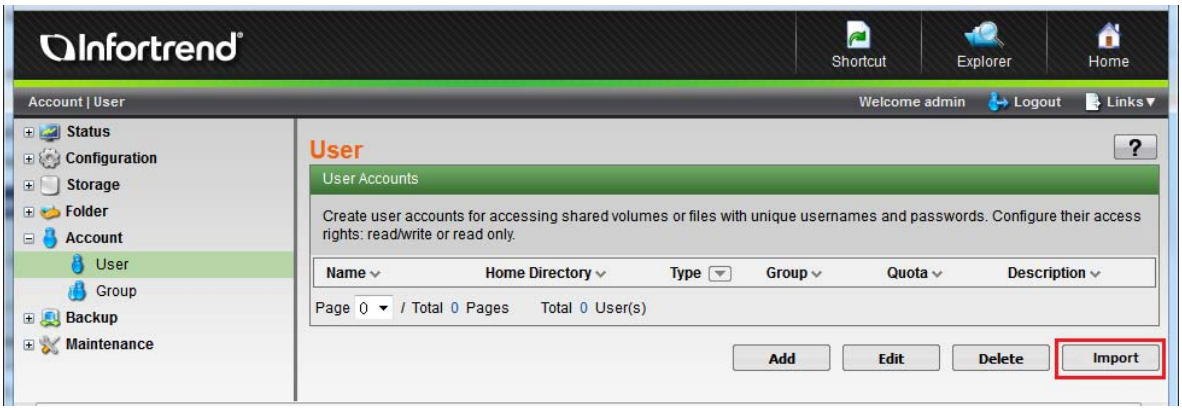
When LDAP configuration is successful, the AD has been added to the EonNAS system.

7.2 Go to *Configuration* > *Service* > *Share* to check CIFS settings and confirm the Windows domain name.



Step 8: Importing Users from AD Server

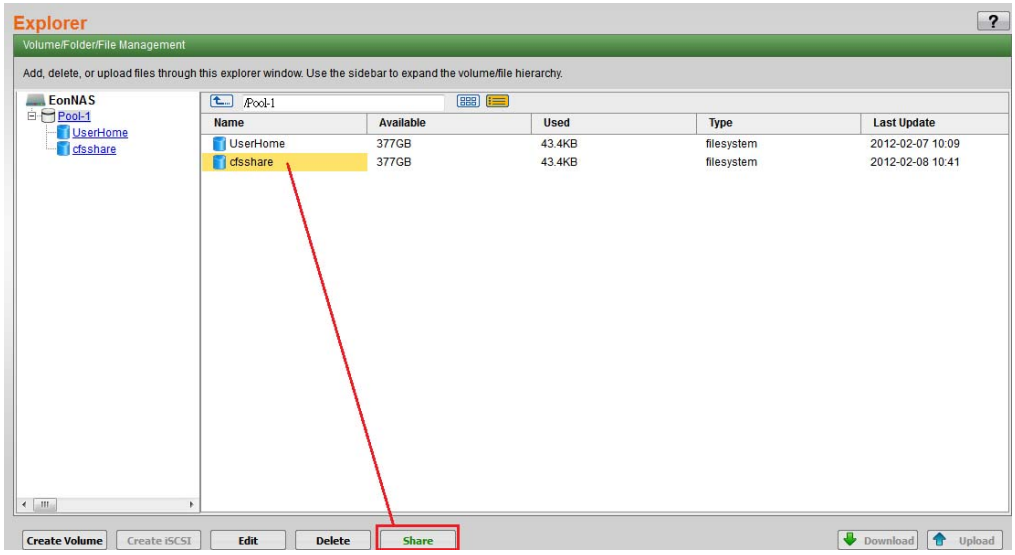
Go to *Account* > *User* and click on *Import*.



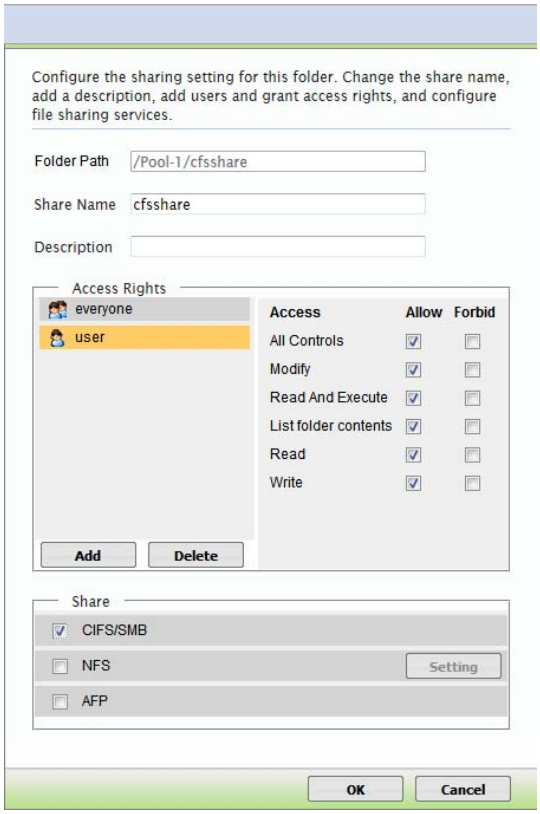
Ensure the AD users are imported from the AD server.

Step 9: Allowing Users to Access Folders

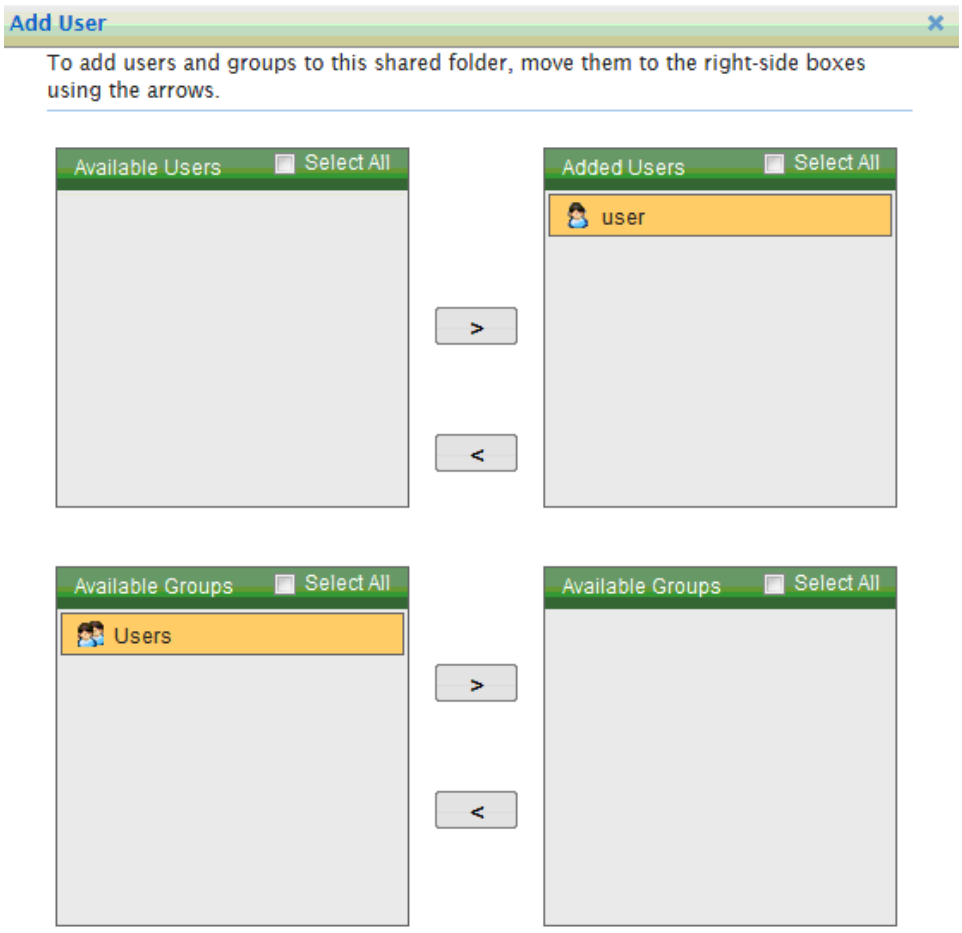
9.1 Go to *Explorer* in the EonNAS GUI and select the folder to be shared. Click on *Share*.



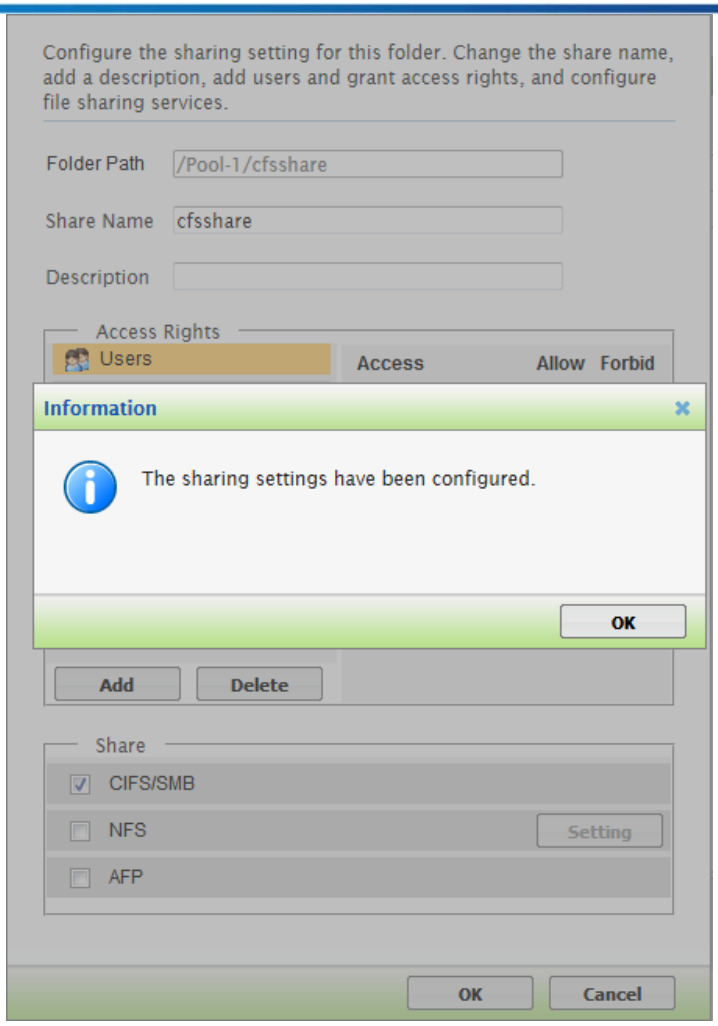
9.2 Add users that will have permission to access this folder by clicking on *Add*.



9.3 To add users and/or groups, move them to the right-side boxes using the arrow signs.



9.4 After configuring the share settings, click *OK* button to apply the modifications.



9.5 After that, go back to Windows Server 2008 and verify whether the share folder access rights are the same as on the EonNAS system. To do so, find the relevant network disk, right-click and select *Properties*. The share folder access settings can be found in the *Security* tab.

Appendix

EonNAS System Recovery Procedure

If the system encounters errors during import, recover (rollback) the system as follows using the system snapshot image mentioned above.

Go to *Maintenance* > *System* > *System Snapshot*. Select the snapshot image for recovery and click on *Rollback*.