Global Information Assurance Certification Paper

Cross Platform Remote Control Authentication using Directory Services and the NetOp Security Server

Albert Caballero
GSEC Practical (v1.4b), option 1
Aug 31, 2004

Abstract

Remote control and administration of machines on a corporate network can be accomplished in a variety of ways and with several different utilities. Many administrators are forced to use a combination of tools to achieve the same end-result because they have computers running Linux, Solaris, or Mac OS X in addition to a large base of Windows PCs and servers. Meeting a company's remote control needs securely, while using many tools, can quickly become a daunting task; considering that different platforms typically use different authentication schemes. For example, Windows may use Active Directory while Unix-based boxes may use password files. Each tool has different set-up requirements and features; adding to the complexity of the configuration. With every additional tool that is used for remote control there are additional threats and vulnerabilities introduced into the system which can increase your overall risk to an unacceptable level, not to mention added administrative challenges.

Some examples of limited remote control programs are Remote Assistant (http://www.microsoft.com/windowsxp/using/helpandsupport/learnmore/remoteassist/intro.mspx) and VNC (http://www.realvnc.com/) that work for basic screen capture; however, they offer little, if anything, when it comes to centralizing or standardizing authentication. They also perform poorly with speed and configurability (see http://www.sans.org/rr/papers/20/721.pdf written by R. Damian Koziel for a great description of the advantages of VNC keeping in mind that centralized authentication or configuration is not possible). Enterprise management suites such as SMS and Tivoli sometimes offer limited remote control with a lot more asset management features but require much more hardware and human resources to effectively manage and implement. Other programs such as Timbuktu (http://www.netopia.com/software/products/tb2/win/index.html) and pcAnywhere (http://sea.symantec.com/content/product.cfm?productid=16) have extensive remote control packages with plenty of features but are limited to Windows only and sometimes lack a means of centrally configuring and managing the authentication and logging of all the hosts. The following pcAnywhere document addresses security and lists different authentication schemes it can integrate with: http://sea.symantec.com/content/displaypdf.cfm?pdfid=1 we would like to be able to manage and configure these settings centrally across a network.

With NetOp Remote Control (www.NetOpUSA.com), an enterprise remote control application, you can centrally authenticate and log all NetOp activity using the NetOp Security Server; which handles all authentication requests from Guests (the client module) to Host's (the server module) across your network. This white paper analyzes how to centrally implement and manage a single authentication scheme for the remote access of all systems including Linux, Solaris, Mac, and Window's machines, using NetOp Remote Control, the NetOp Security Server, and Windows Active Directory.

Introduction

The purpose of the NetOp Security Server (NSS) is to implement role-based access control and administer remote control security with a centralized, fault-tolerant design. The following is a list of terminology that will be used throughout this paper:

- NetOp Guest: The administrator or client module which allows you to remote control any available Host on your network.
- NetOp Host: The server program that must be installed and running on the PC to allow inbound Guest connections on a specific port.
- NSS (NetOp Security Server): This is the central Host module that needs to be running for authentication to occur. Think of it as your domain controller for NetOp Remote Control without which authentication and logging will not work, so redundancy and fault tolerance are usually things to consider.
- Security Manger: The client applications that configure your back end database, your NSS, and let you analyze your solution.
- "The database" An ODBC compliant database that allows you to store security roles and log entries for your entire enterprise. The database must also be available for authentication to occur.

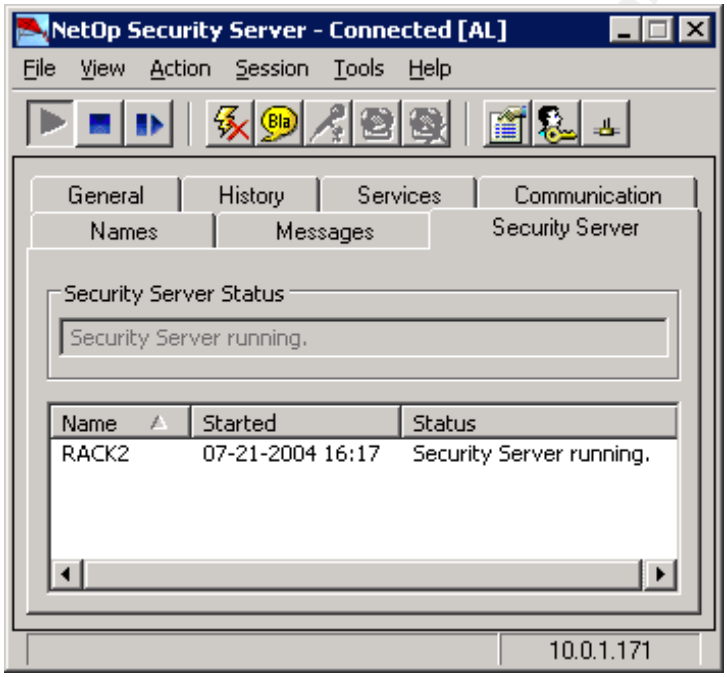
The NSS can require any one of several authentication schemes including Windows security, RSA SecurID, Directory Services, or NetOp authentication. This paper assumes there is a Windows Active Directory environment present where all potential guests have accounts. We want to use these directory services accounts to authenticate all NetOp Guests attempting to remote control any NetOp Host (if there were an RSA SecureID Ace server present we could use that instead).

The first section of this paper will describe the components necessary for the solution. *(Note: A variation of my components section has been posted by Danware Data A/S and Crosstec Corporation on their websites prior to the submission of this paper: http://www.crossteccorp.com/support/resources/NetOp_Security_Server.pdf or http://www.netop.com/_Remote+Control/_NetOp+Remote+Control/_Security+Server)*. The second section will describe a step by step process on how each component is configured, and the last section will test the solution before it is implemented. The purpose of this paper is to identify a process of implementing role-based access control by using the existing users and groups in your Windows Active Directory domain when attempting to remote control non-Windows machines such as Linux, Solaris, and Mac's (and your Window's machines as well of course).

Components

The following solution consists of five components: The NetOp Security Server (NSS) and Security Manager, the database, the NetOp Guest, and the NetOp Host.

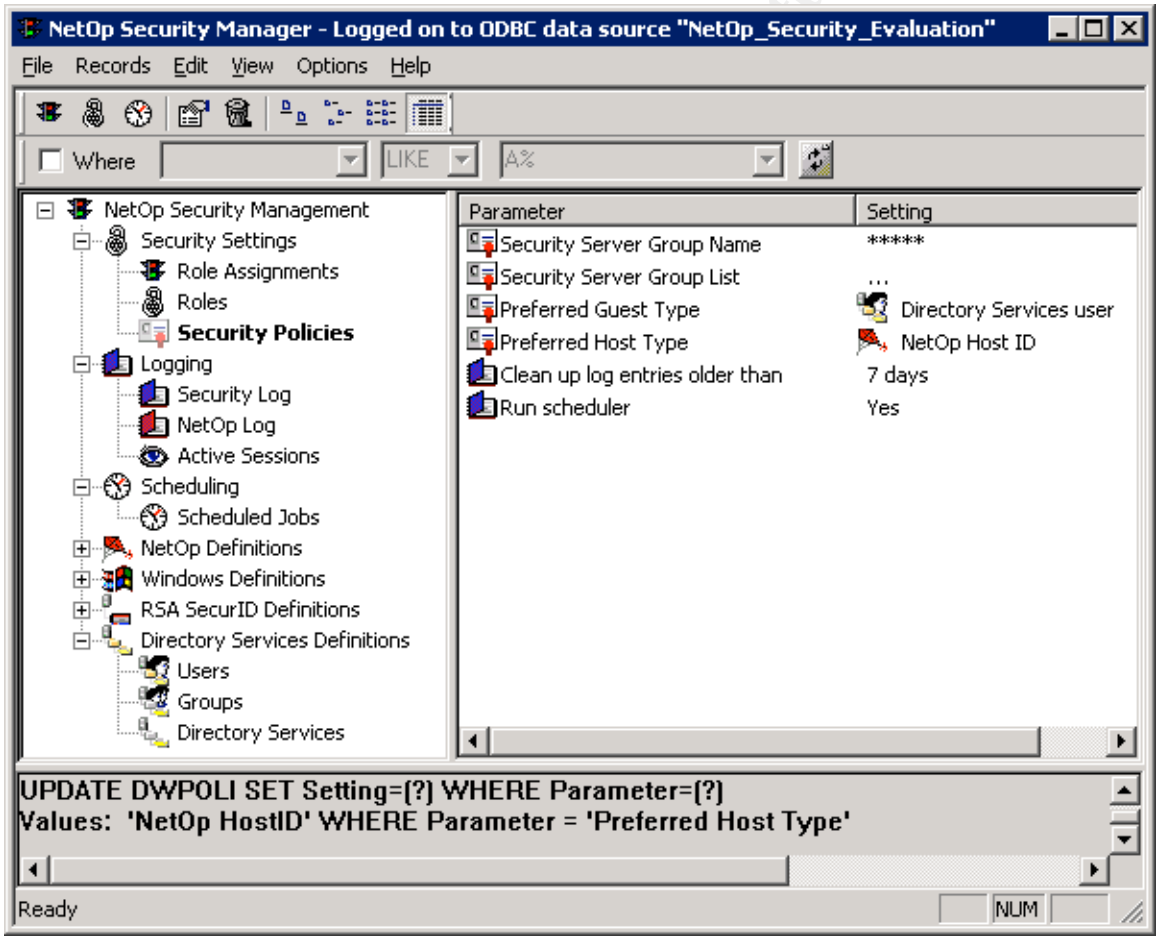
The NetOp Security Server is a Host module that answers queries from other NetOp modules about session permissions and rights across a network. The NSS does this by forwarding these queries to the database where a list of security role assignments defines the access that each Guest has to each Host or group of Hosts on the network. The NSS is also capable of capturing log events of your Window's Hosts and saving them into the same database for centralized management and analysis. It is recommended to use more than one NSS across your network in case of hardware failure or connectivity issues to one of your servers. The NSS can authenticate Guest and Host modules running on a variety of platforms including: Linux, Solaris, Mac OS X, Window's CE, and OS/2 platforms as well as Windows 9x/NT and beyond. All traffic is directed through a single port of your choice. Additionally, all traffic can be encrypted with 256bit AES encryption where a 2048bit Diffie-Hellman key exchange is required.



The NetOp Security Manager is a client application that can add or edit information stored in a database of your choice. It configures how the NetOp Security Servers operate on your network and provides a GUI front-end for the configuration and analysis of your remote control solution. It is where you create security roles, view your logs, and manage your NetOp database. Using role assignments the Security Manager will allow you to assign Host access rights

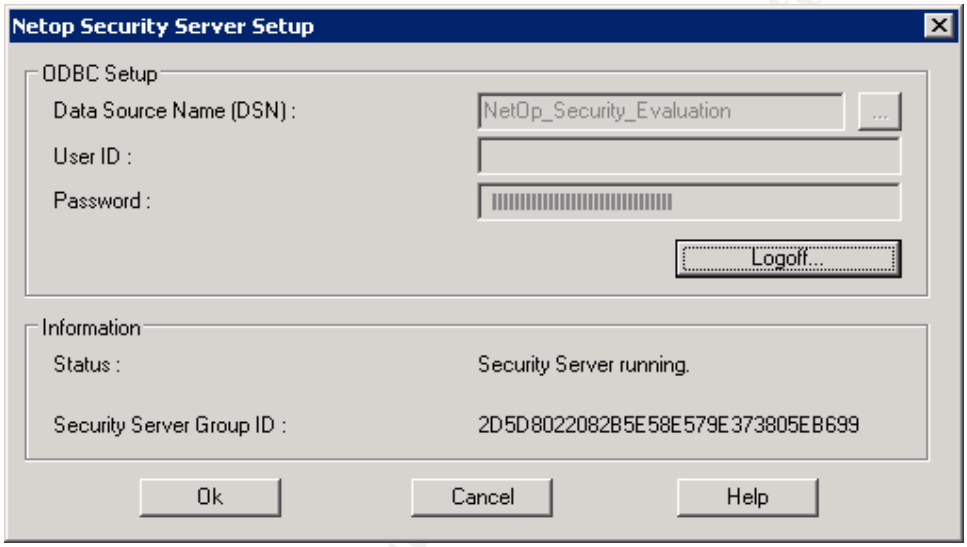
and privileges to Guest modules. It can also be installed as a separate tool on any Windows machine to edit the database remotely.

By assigning security roles to Guest users, each Guest is only allowed to access the Host machines necessary for their daily responsibilities. This way, administrators can rest assured that every connection is authorized and secure. For the CEO, this allows them to receive remote support while at the same time limit what their IT department has access to while connected to his/her machine. This prevents the IT department from accessing any confidential information that may be one the CEO's computer. Additionally, supervisors could be assigned monitoring privileges only to ensure that their employees are staying on task while preventing them from control. Here is a snapshot of the Security policy view of the Security Manager:



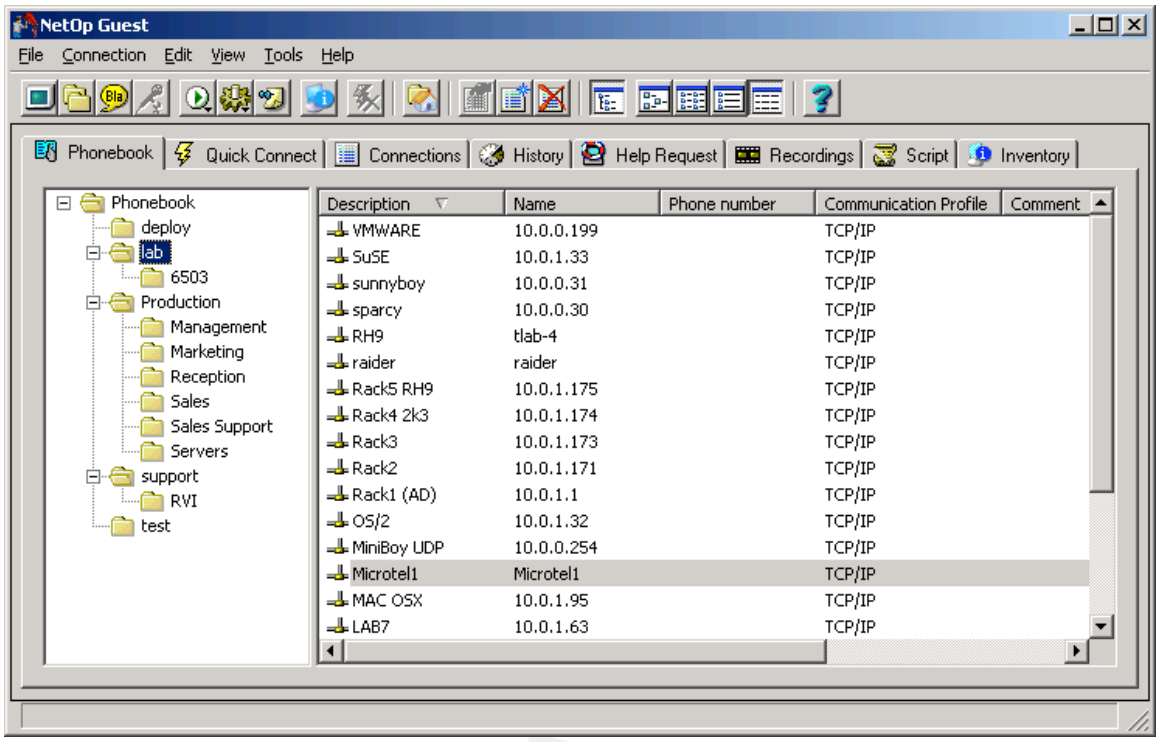
The backend database can be almost any system capable of communicating through the ODBC interface and it has actually been tested with DB2, MS JetEngine, Oracle, and SQL (Danware Knowledge Base article listing the supported databases (http://www.netop.com/tech/support/netop_security_server/supported_databases.htm). By using a standard interface you can use a database system you have

configured on the network with failover and other features making sure the system is available most or all of the time. The database provides input to the NSS's and based on this they will allow or deny NetOp Guests access to NetOp Hosts. During installation it offers to create a local test database, which I would recommend for testing purposes only because this Access database will begin to degrade performance at around 300-500 security roles or Host definitions. Besides, there is no need to test a brand new application on a production database server. Once you have the Data Source ready, the NetOp Security Manager will construct customized default tables for you to start working immediately. The actual NSS program shown above will need to log on to your backend database so it can query for user rights, this is an ideal time to add to the layers of your security by requiring strong authentication to enable a connection. A picture of the database logon dialog of the NSS:



NetOp Guests can initiate sessions with NetOp Hosts. When a Guest program contacts a Host the Guest identifies itself with certain logon credentials. These credentials can be Windows user name, password, and domain name or you can choose to use directory services, RSA SecurID, or NetOp authentication instead. After the server has validated the user name and password, the Host program sends the user name to the NSS together with information about the Host computer. This is important because none of these credentials or definitions are handled locally and this makes the potential compromise of user rights less likely, the attacker must access the central server to edit rights or permissions; not an individual Hosts (see http://www.sans.org/rr/papers/60/483.pdf for 'Potential Vulnerabilities of Timbuktu' by David Batz, which shows vulnerabilities specific to programs that manage authentication and lists of user rights on the Host machine itself via files or registry entries as opposed to a central server). The NSS queries all relevant role assignment records in the database and then returns the Host's information about what the Guest is allowed to do; such as view only, file transfer, chat, or full remote control. Again, all traffic is encrypted and the key exchange is based on the time of day, this means if you do not

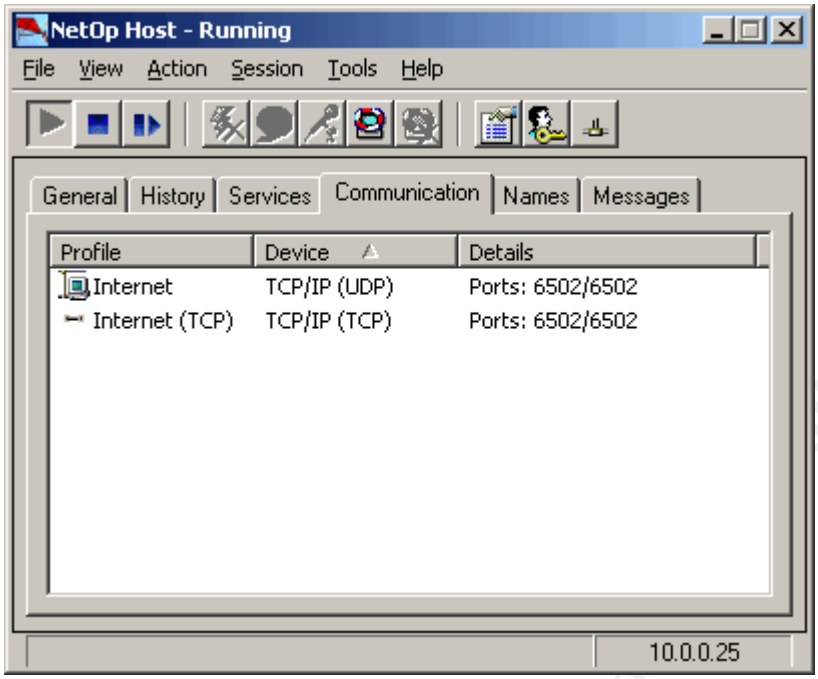
synchronize the time on your network each key will not be unique which could introduce the possible threat of a replay attack. Here is a snapshot of the Guest:



The NetOp Host module can be configured to use the NetOp Security Server or other available security methods such as Windows Active Directory or LDAP. Each individual Host has many security features that can be configured at the time of deployment such as non-default port numbers, logging to multiple locations, IP address filtering, and call-back authentication. This whitepaper concentrates on centralizing authentication for all NetOp Hosts on a LAN not individually securing each Host. A whitepaper that does an excellent job of describing Host-based RC security is “Securing the NetOp Host” written by Robert Rounsavall http://www.crossteccorp.com/support/resources/securing.pdf.

When using the NSS, the Host uses an authentication key pair to secure its relationship with a specific NSS Group ID. Every time a NetOp Guest tries to gain access, the Host will perform a query to the NSS to verify permissions. A Host from a security standpoint can be handled as a computer and/or a person. You can specify an individual workstation as a Host which requires that you enter roles for each workstation individually or you can also group computers that already exist on your network and assign rights based on these groups. When you add a new computer it will automatically be subject to the same NetOp security as other PCs in its own domain or group. It is recommended from the Security Policy view in Security Manager that you set a Host mode where you always ignore a logged-in user and grant rights based on the workstation only. This is especially useful for servers and sensitive PC’s where unexpected accumulated rights can lead to a dangerous outcome.

This is the basic Host interface:



Step by Step

Assuming there are only Windows machines and only one domain, or several domains with a two-way transitive trust it would be easiest to implement Windows Security Management. This means that the users, computers, and groups already exist on your network so you can use them with Security Manager to create your role assignments. In an environment where there are several Windows workgroups, un trusted domains, or cross platform machines such as Mac, Linux, or Solaris boxes you will use NetOp Security Management, Directory Services, or RSA SecurID. NetOp Security Management lets you create Guests and Hosts for role assignments regardless of their OS. This is independent of the authentication that is already set up within your network and quite useful if there is no central server that maintains user accounts for all potential Guests (like vendors, contractors, etc…). The drawback to NetOp Security Management is the same thing that makes it so useful; the fact that it is a stand alone authentication scheme means you must manually create all Guest and Host definitions within the Security Manager before being able to create role assignments. The NSS does provide a utility called AMPlus.exe which allows you to import and export Host and Guest definitions from a comma delimited file but you must still create this file if not exporting from a previous version NSS.

If you already have an ACE server or a directory services solution like Novell or MS Active Directory on your network for authentication then you will go with a hybrid security management solution of Directory Services or RSA Guest definitions and NetOp Host definitions. This lets you take advantage of the user

and group accounts that already exist in your network while allowing you to assign security roles based on Host definitions that you create for the purpose of NetOp. This is the solution we will be implementing. It will allow you to require a NetOp Guest use a Windows AD password before connecting to any Host, even if that Host is a non-Windows machine. We will be assuming that there is an already existing Windows AD domain where all your potential Guest users have an account. You want to require these credentials when one of these Guests attempts to remote control a Host machine that is Windows, Linux, Solaris, or Mac OSX. To accomplish this we will take the following steps:

1. Install the Host on a Linux SUSe 8.0 server.
2. Install the Guest on a Window's XP PC.
3. Prepare the MS SQL backend database to use with the NSS.
4. Install and configure the NetOp Security Server and Security Manager on a Window's 2003 Server (this step is the biggie!).
5. Create Groups and Role Assignments in the Security Manager.

For technical requirements and supported OS's see this link: http://www.netop.com/tech/support/documentation/requirements/requirements_765.htm

Step 1

Most remote control applications will have a guest and a host piece that will need to be installed. You will need to download and install the appropriate NetOp Host package onto each of your Unix based machines. Licensed copies can be downloaded here http://www.netop.com/tech/download/latestbuilds.htm or if you have never used NetOp and want to "try before you buy" you can register and receive a trial version from here: http://www.crossteccorp.com/tryit/index.html

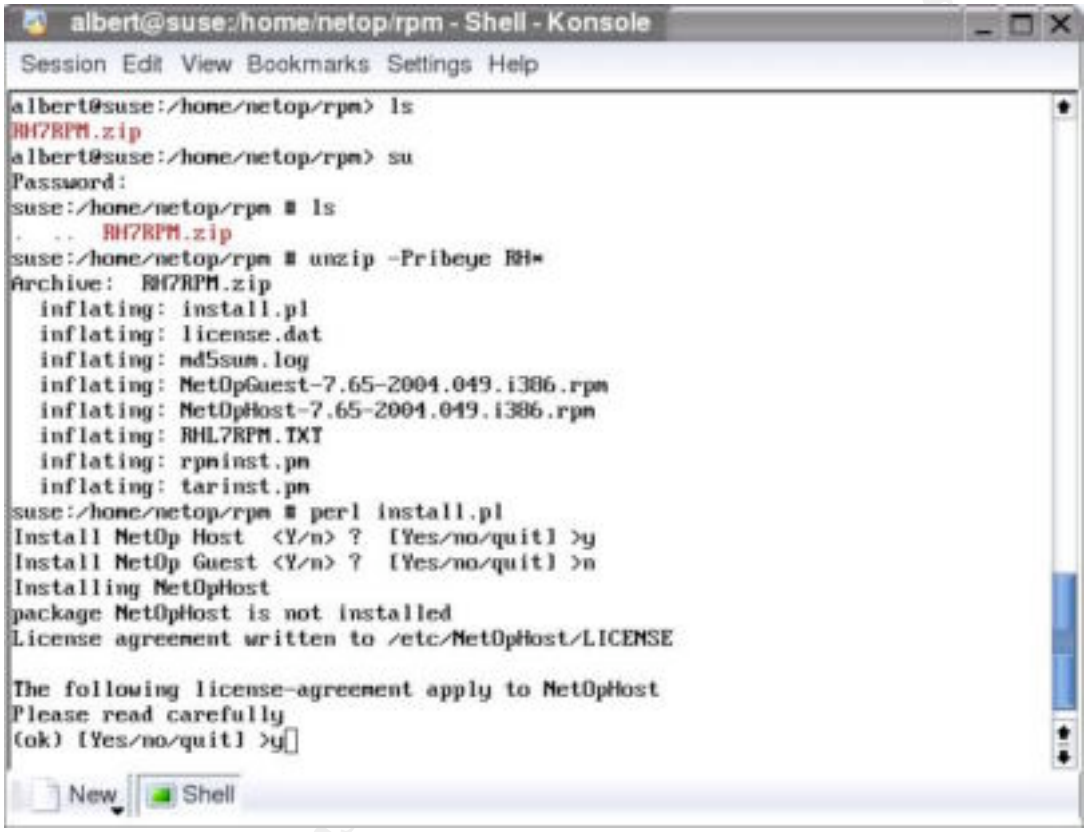
When you download the installation package you must extract the file and run the install script. Based on the download you choose here are the steps from a Linux terminal:

```
#if licensed
su
tar –xvf < package_name >
perl install.pl perl

#if evaluation
su
unzip –P <eval_passwd>
perl install.pl perl
```

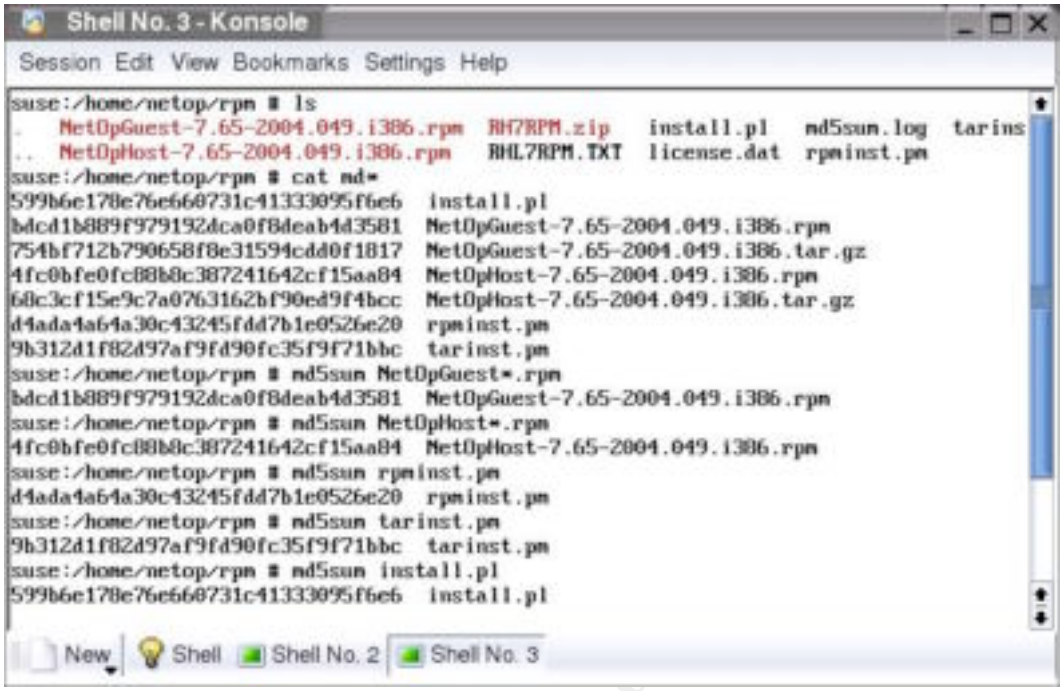
The NetOp Host will then be installed and configured to start at boot time. Once the Host is installed and you have rebooted or restarted the X server you can connect with the NetOp Guest as root. If you run the **NetOpHostGUI** command from a terminal you can configure the Host using the graphical user interface. We will need to configure the Host to use the NSS for authentication instead of the normal UNIX password files later on.

A snapshot of the evaluation installation procedure:

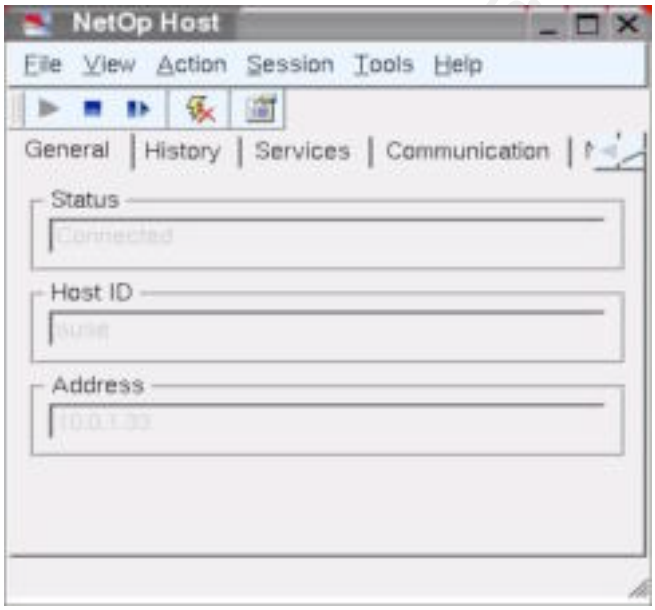


When downloading any software package you should take note if there is a checksum provided by the manufacturer. Before installing the package you should always run the downloaded files through the correct hash algorithm to verify their integrity and if you are able to access two different set of download files from different sources and the hash still checks out then you can be fairly certain that the files are legitimate. Once you have verified the file's integrity then you should use these same files to install on all your Hosts.

Integrity checks using md5 on the SuSE server:



After rebooting or restarting X windows run the **NetOpHostGUI** command from a terminal so you can see the GUI and ultimately configure the Host:

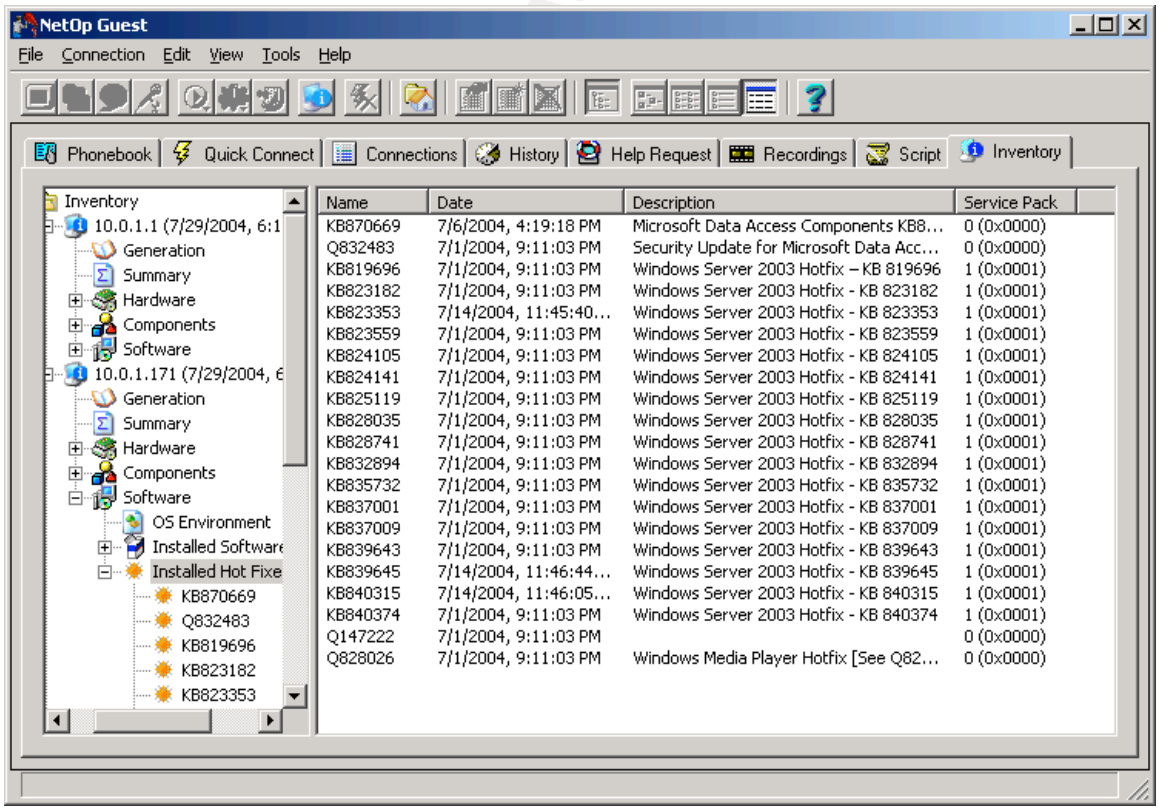


Step 2

In this step you will install the Guest module. The Guest will be used by administrators and will allow the ability to remote control any Host on the network as long as the Guest is authenticated by the NSS. Because we are installing the Guest on a Windows XP box it is a basic Windows installation. There is an Install Shield and a Window's Installer; I'd go with the Install Shield to keep it simple unless you are deploying with GPO's or distribution software like WISE technologies. In either case the install is pretty much the same:

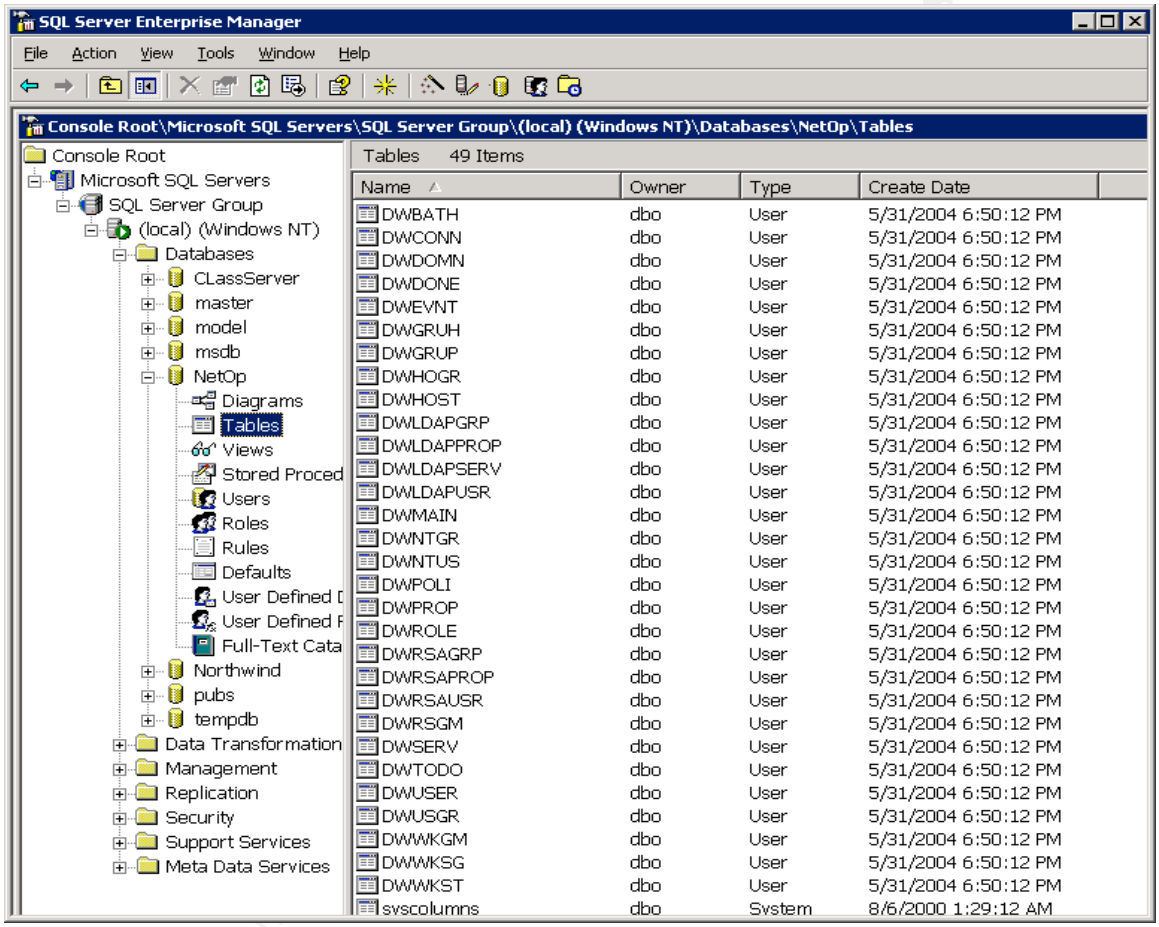
- Download the install files: http://www.netop.com/tech/download/latestbuilds.htm
- Run setup.exe and accept the defaults; here is the Quick Install guide: http://www.crossteccorp.com/support/resources/rc_quick_install.pdf).

It is important that the Guest be a separate piece of software, by design some remote control packages choose to combine the two modules which tends to increase the likelihood of unwanted access to the administrator (Guest) piece by an end user. Furthermore you can use a Closed User Group license that will only allow Guests with the proper serial number to access any particular Host that has the same closed ended serial number. Here's another picture of the Guest application in Inventory:



Step 3

Preparing the database is as simple as creating an empty database for use by the NSS in your server. This database will be populated by the Security Manager with the necessary information the first time it is run. If using MS SQL you would open Enterprise Manager from the programs menu and simply right click on the Databases sections and click New; call it NetOp. This sample db picture already has the default tables necessary for the NSS to be functional:

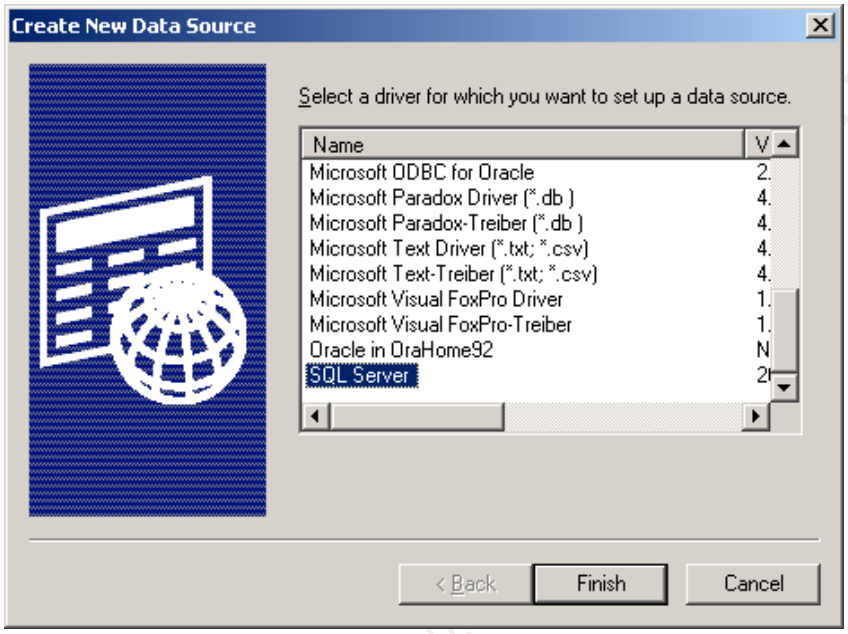


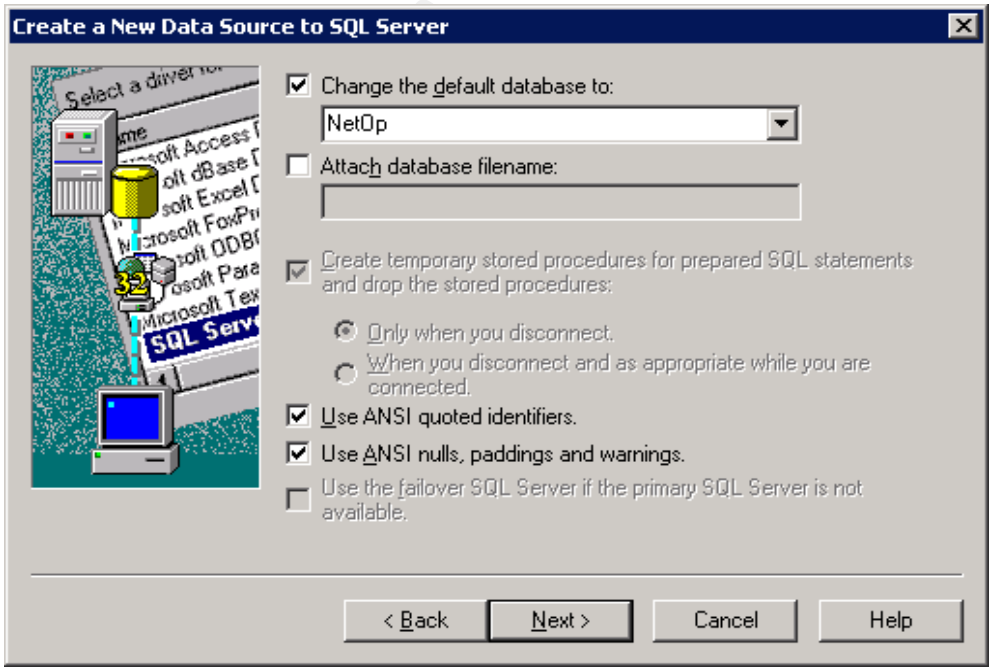
Step 4

We have set the stage by installing a Windows Guest, a non-Windows Host, and creating a database. Now we will install and configure the NSS and the Security Manager. The NSS is exactly like a Host only it must run on an NT based machine. We will be installing the NSS on a Windows 2003 server that is part of an AD domain. Again you can download the installation files (Install Shield or MSI) from the same website provided earlier in this document for Guest and Host. When you choose to install the Host select NetOp Security Server as your choice and both the Security Server and the Security Manager will install and appear under Start>Programs as two individual programs.

You should run the Security Manager first 

, when it runs for the first time it will attempt to create a New Test Database. Click Change and select Machine Data Source then click New. This will walk you through creating a new SQL system data source on your Windows box that must point to the previously created blank database on your SQL server. The DSN can also be created manually via the Data Sources ODBC MMC under Administrative Tools:





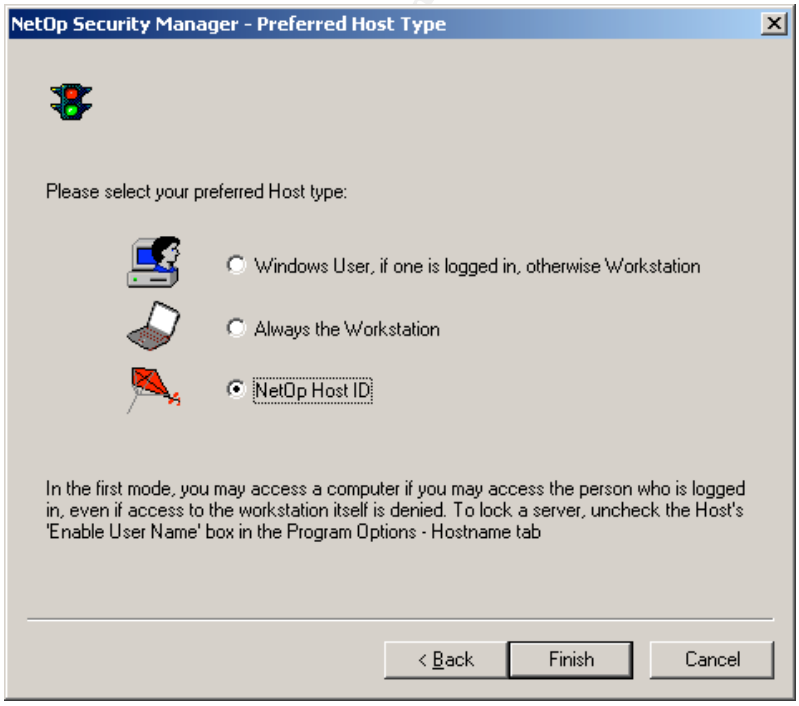
When you get to the end of the wizard click **Finish** and you will now see the name of your Data Source at the Security Manager Log on screen. The Security Manager will start a wizard that will help create the default configuration of the NSS and populate the database with tables. The first screen is the **Group Name** dialog which will have a group name of **NetOp** (it is case sensitive) by default; however, this should be changed to a unique name for your company. Every Group Name will be run through a hash algorithm that will generate a unique public key called your **Group ID**. This public key can be copied from this dialog and should be pasted into a text file that you will refer to later to configure your Hosts. The Guest Access Security settings for each Host that will use the NSS must have the correct public key (Group ID) to connect to the NSS. This is what the Host will use when browsing for available NSS's on your network.

As in all asymmetric encryption models the Private Key (Group Name) should be protected and preferably have considerable length and complexity such as a strong password, although it will not change the length of the hash output itself or its complexity. The public key (Group ID) can be known to all your administrators and users but the private Group Name should remain private.

When using the NSS you will need to decide what type of Guest will be the typical Guest that will be authenticating against or connecting to any particular Host. The **Preferred Guest Type** dialog, which is the next dialog in the wizard, will typically be Windows username and password if you have a pure Window's domain. However because we have cross platform workstations we

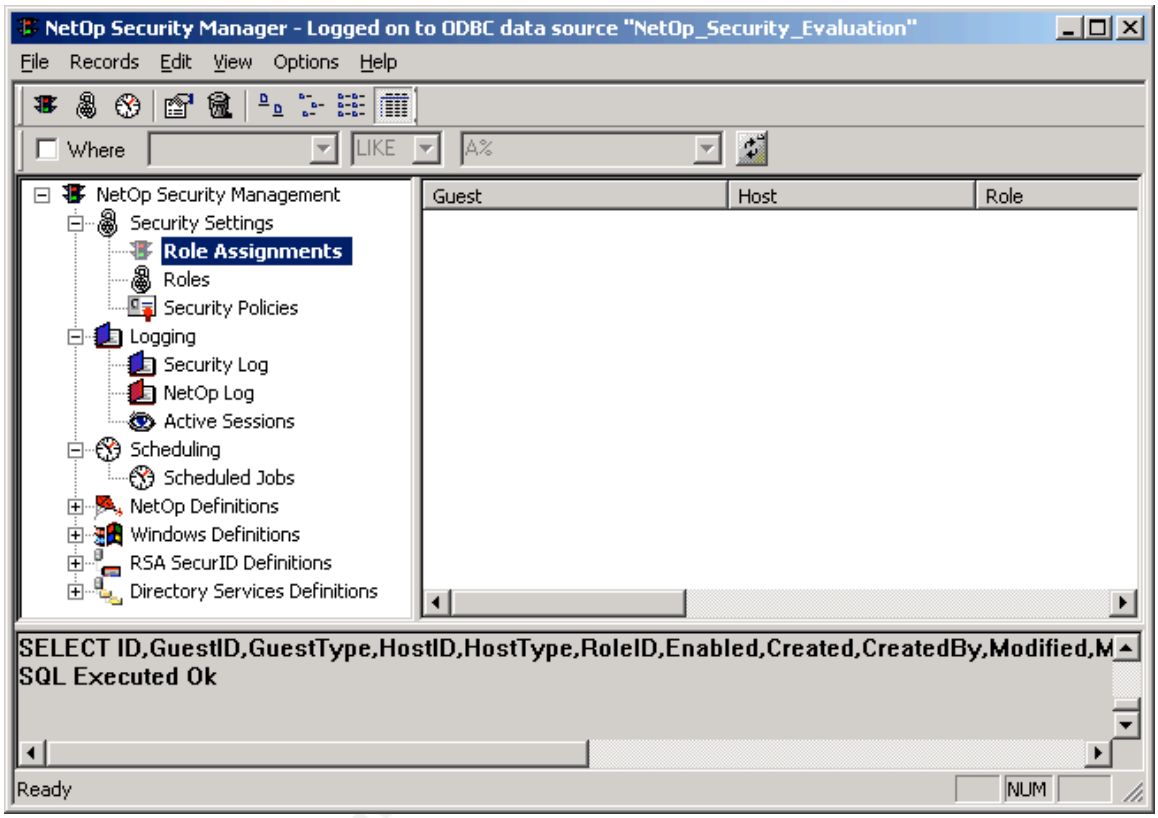
will be selecting Directory Services username and password and we will define our own Hosts which may or may not have computer accounts in the domain (as the case would be with a Linux or Solaris system). Select **Guests enter Directory Services Username and Password**:

Next you will select your **Preferred Host Type.** The Preferred Host Type will determine how you are going to define your workstations. We have non-Windows workstations so we will be using **NetOp Host ID**.



The wizard will now attempt to help you create a Role Assignment, for now **Click Cancel.** We must first create a Directory Service so that our NSS knows where to find and authenticate users/guests. By creating a Directory Service on the NetOp Security Manager you can require all Guests have valid Active Directory credentials before they log on to a Host.

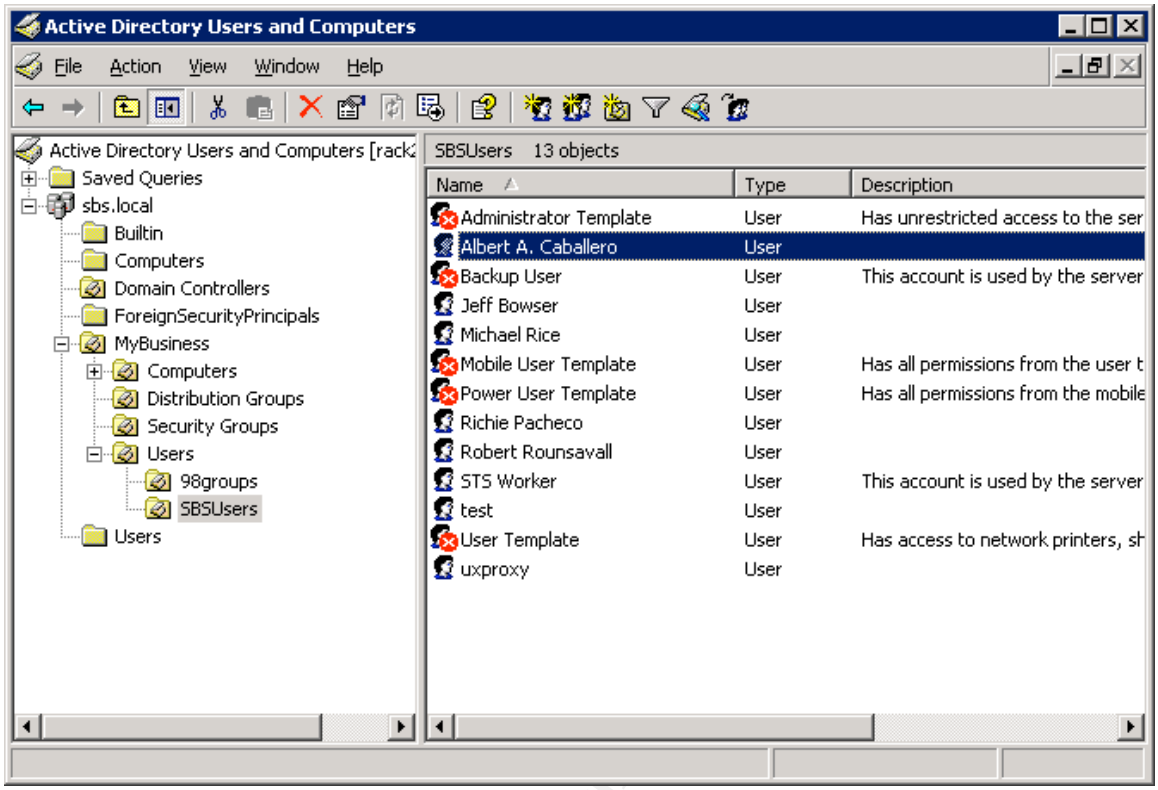
The Security Manager before it's been fully configured:



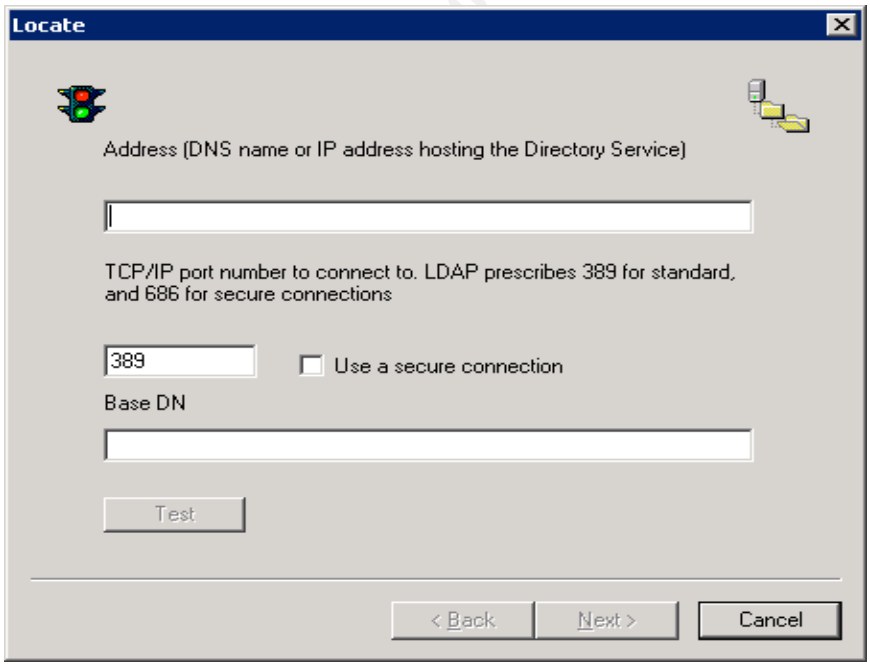
To be able to create the Directory Service in your Security Manager you must have access to the Active Directory Users and Computers MMC on your Windows AD domain so you can verify several pieces of information:

1. Your domain name. In the example below it is sbs.local.
2. The Common Name of a user that you will use for the directory service. This is the user that will be used to query the Active Directory tree. (This is NOT your logon name to the domain; it is the name that actually appears in the Active Directory Users and Computers MMC). In the example below it is Albert A. Caballero; you can also use the Administrator account.
3. You need to know exactly where that user is found. My user is in the sbs.local domain under the MyBusiness>Users>SBSUsers organizational unit. The Administrator user is usually found under the built-in Users Organizational Unit.

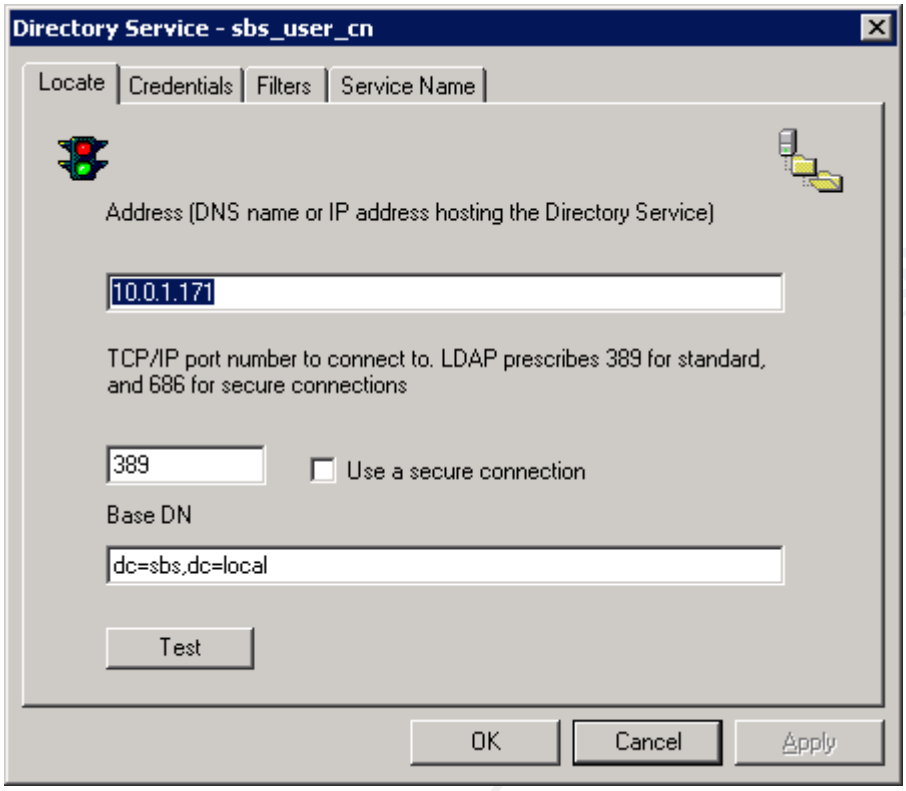
You can see a snapshot of our test active directory structure in the next page.



Go to the Directory Services Definitions view in the Security manager and find Directory Services. On the right side of the windowpane right click and Click **New**. You will be presented the **Locate dialog**:



Fill in the IP address and Base DN of your domain controller and Windows Active Directory domain as shown below:



Click Test and if the test is successful then **Click OK**

Note: The Base DN is your domain name with each section preceded by a DC= and separated by a comma.

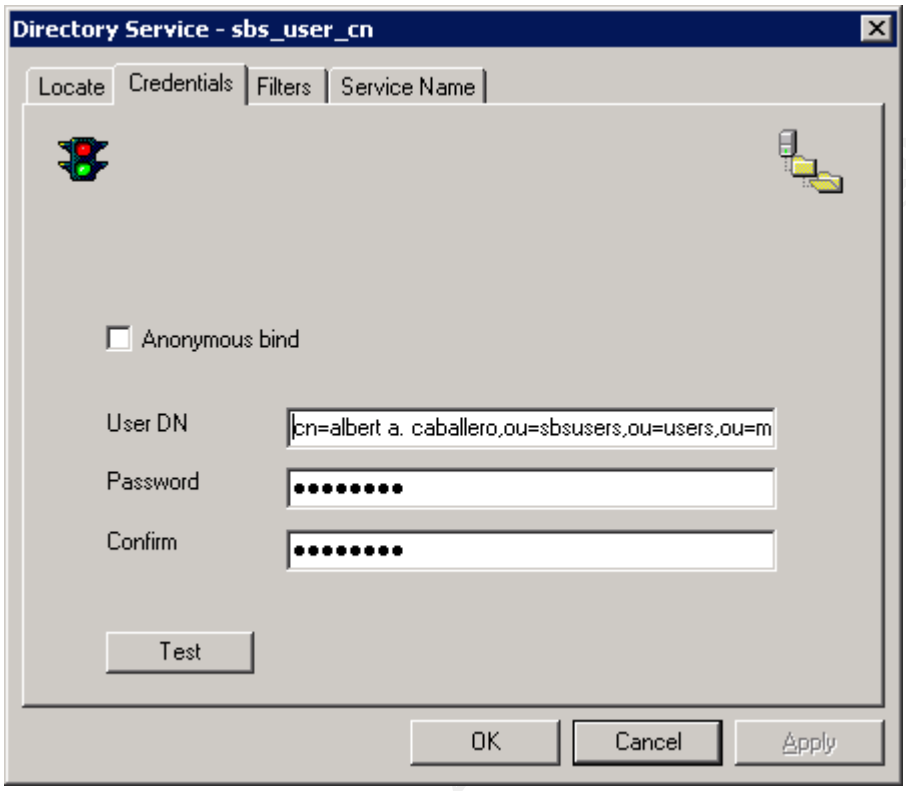
An example Base DN for the domain ad.netop.com would be:
DC=ad,DC=netop,DC=com

For my example where my domain name is sbs.local my Base DN is:
DC=sbs,DC=local

It may be preferable to narrow the search scope to begin at an organizational unit instead of starting at the top of the domain if you have a large directory structure. This would reduce directory lookup time significantly in large enterprises where there may be a lot of domains and OU's with users and computers that will not be using the NSS. We will be using the domain's Base DN for this example; however, if I wanted to start the Guest lookup from the OU SBSUsers instead of the top of the tree my Base DN would look like this:

OU=SBSUsers,DC=sbs,DC=local

Now you are ready to add the user credentials for the Active Directory account used by the NSS to browse the directory tree. This user must have Admin rights on the domain or from within Active Directory Users and Computers they must have been delegated control of the organizational unit inserted in the previous dialog from where you want to be able to add Guest users.



Note: When you specify your User DN in the NetOp Security Server you must use the true Common Name found in the Active Directory Users and Computers MMC not the logon name of the user. In the AD picture at the beginning you see the common name (what NetOp needs) is Albert A. Caballero, this users logon name to the domain happens to be acaballero but this is not what is used when inserting the full User Distinguished Name into this dialog.

The Distinguished Name of the user that I am using is:

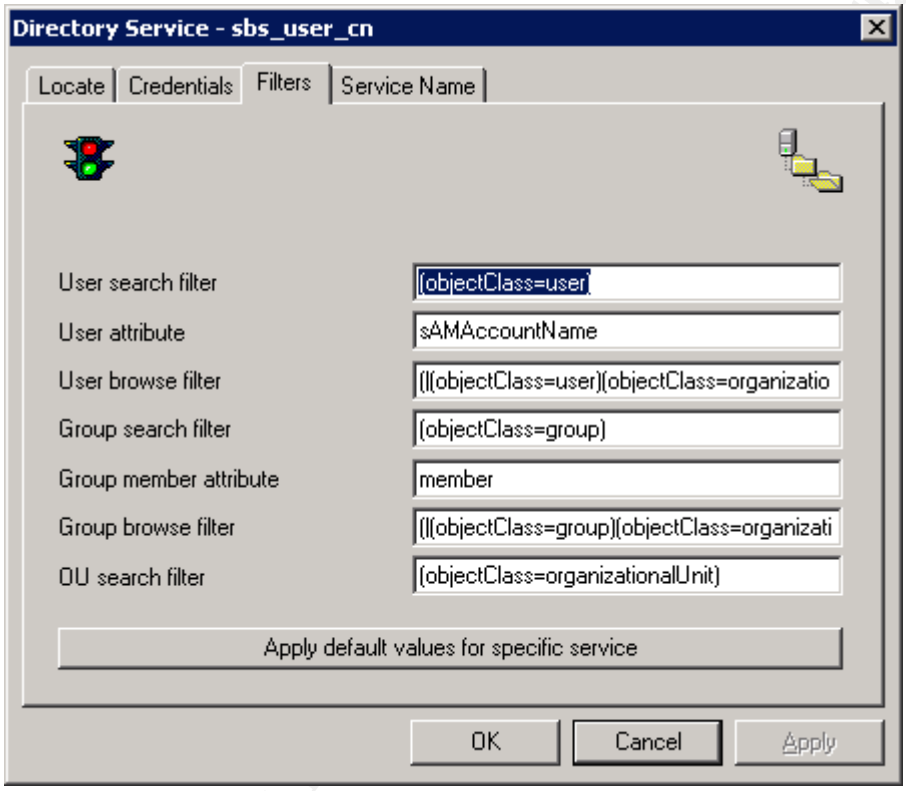
cn=albert a. caballero,ou=sbsusers,ou=users,ou=mybusiness,dc=sbs,dc=local

In most Active Directory domains if the Administrator account exists it is found under the built-in Users container. This Users container is considered a common name not an organizational unit, so for our other example of the ad.netop.com domain the User DN for the Administrator account in the Active Directory would be:

cn=administrator,cn=users,dc=ad,dc=netop,dc=com

Make sure that if you click test you get the following response:

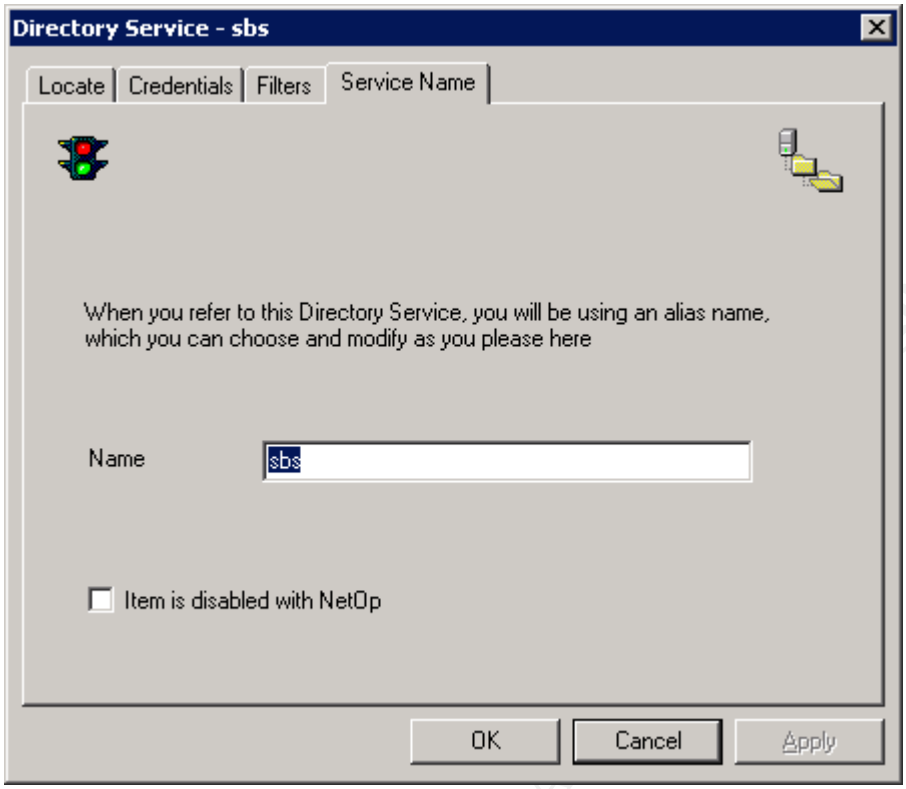
The next dialog is the **Filters** dialog:



There's not much to do in this dialog if you use MS Windows Active Directory as we are doing in this example. When the dialog appears it is empty. Click the "Apply default values for a specific service" and then select Microsoft which should auto populates all the necessary info.

Note: When you click the Apply default values… button you will see a relatively long list of Directory Services. The NSS is designed to be compatible with other directory services server's as well and you can easily pick from any number of directory services such as Novell NDS or eDirectory, Sun ONE Directory Server, NetScape Directory Server, etc... The actual NSS and Security Manager must run on a Windows platform. It is strongly recommended you run the NSS on a server operating system such as NT, 2k, or 2k3 Server for optimum performance.

The next dialog is **Service Name**:

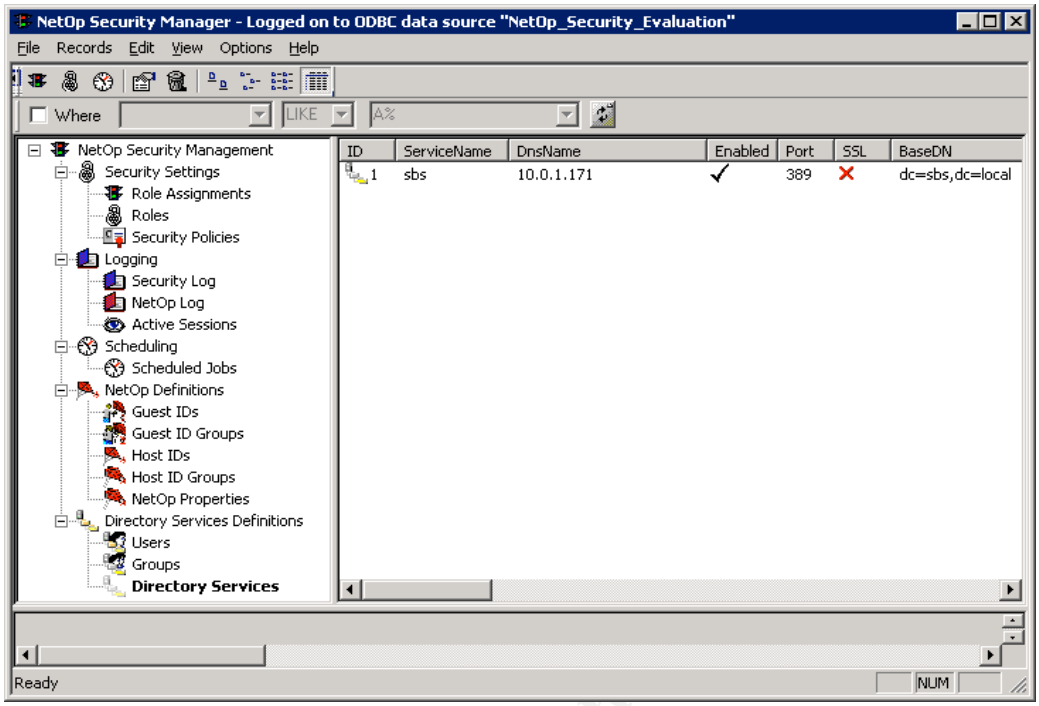


It is considered best practice by the OEM that the Name you insert here, which is just an alias, is the NetBIOS name of the actual domain you are on without the fully qualified extension or names of any parent domains. This is not required but for the sake of user friendliness this is the easiest way to configure your alias name. If the domain is sbs.local the alias given should be **sbs** but does not have to be. For our other example ad.netop.com an alias of **ad** is sufficient if you are following these practices.

Note: This alias name is significant because it is what you need to type into the Directory Server field when you actually get the log on prompt from the NetOp Host on the Guest. This will be addressed again later in the document during the Test Your Solution section.

Click **Finish** and you should have a listing for your newly created Directory Service as shown in the next page. You have the option to use a secure port other than 389 for an SSL connection from NSS to Directory Server if this has been implemented on the server side.

Configured directory service:

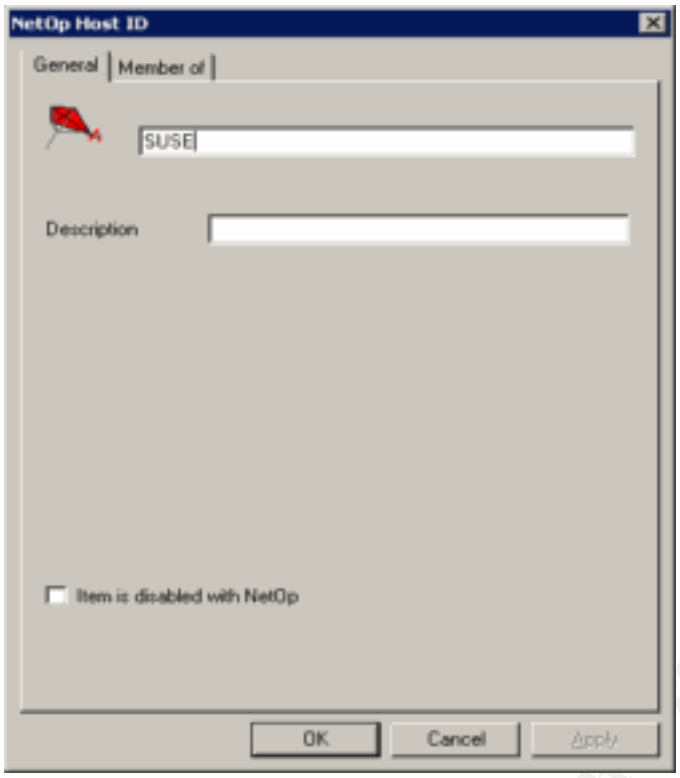


Step 5

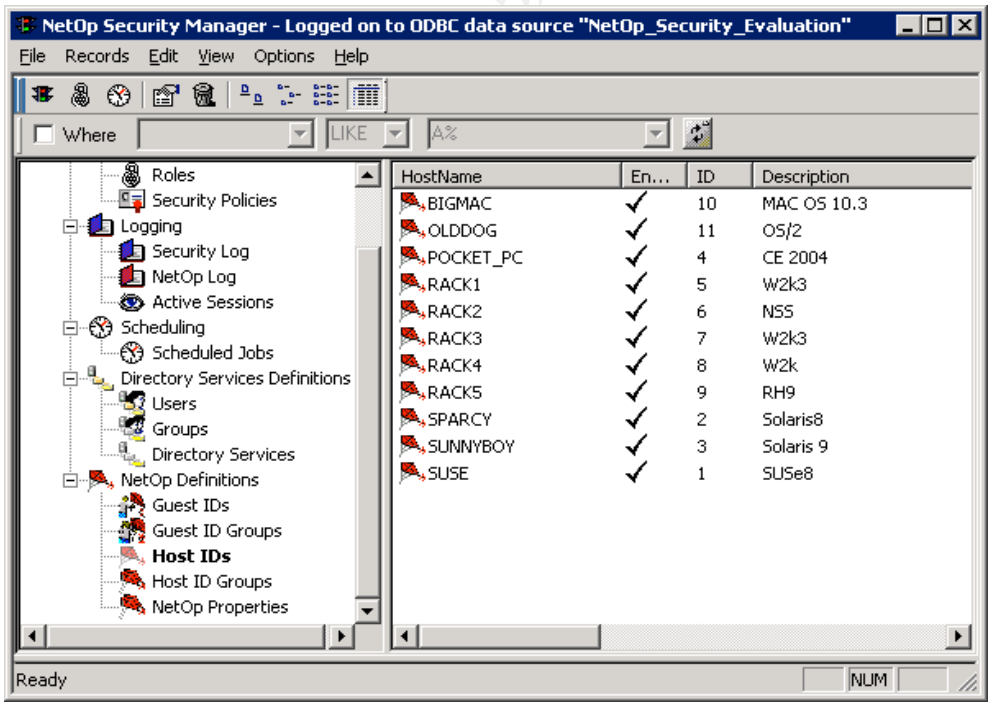
At this point you will begin to insert your Host ID's and groups so that we can create role assignments. Host ID's must be created one by one however they can also be imported into the Security Manager with a small program called Amplus.exe from a comma delimited file. We will then add the Directory Services user's and groups as we add our role assignments because those already exist.

It is good practice to create Host ID groups and insert your Host ID's into those groups so that when you create role assignments you do not have to recreate them for each new Host that is defined. It is always a good idea to assign rights to groups and then put users into groups for ease of manageability this way Guest Access Privileges are at the Host ID Group level and not at the individual Host ID level. New Host ID's can then be added to the Host ID Group's without changing the role assignments or having to add new ones.

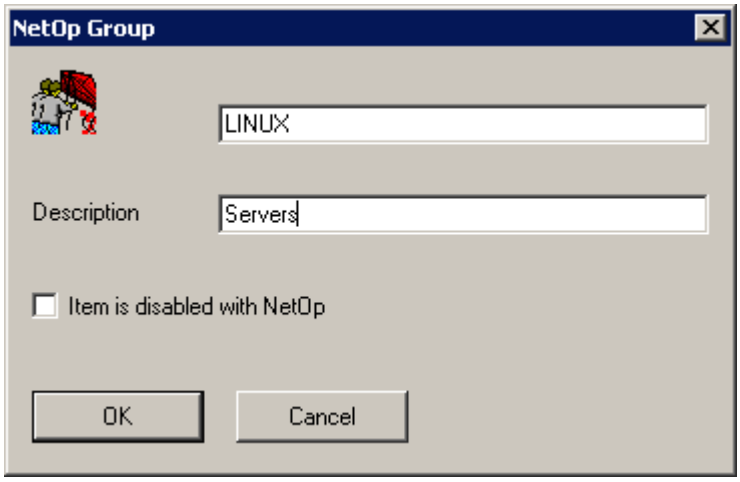
The next step is to add the Host ID of your non-Windows machine under Host ID's. Go to the Host ID's view of the Security Manager, right click, and click **New**. This name can not be random, it must be the computer name that can be resolved by using DNS or a similar naming service or it can be the IP address of the Host if it has a static IP. Usually you would simply add a Host ID and define it with the computer name so you don't have to worry about the IP address changing assuming a DHCP environment. You will be presented the Host ID dialog.



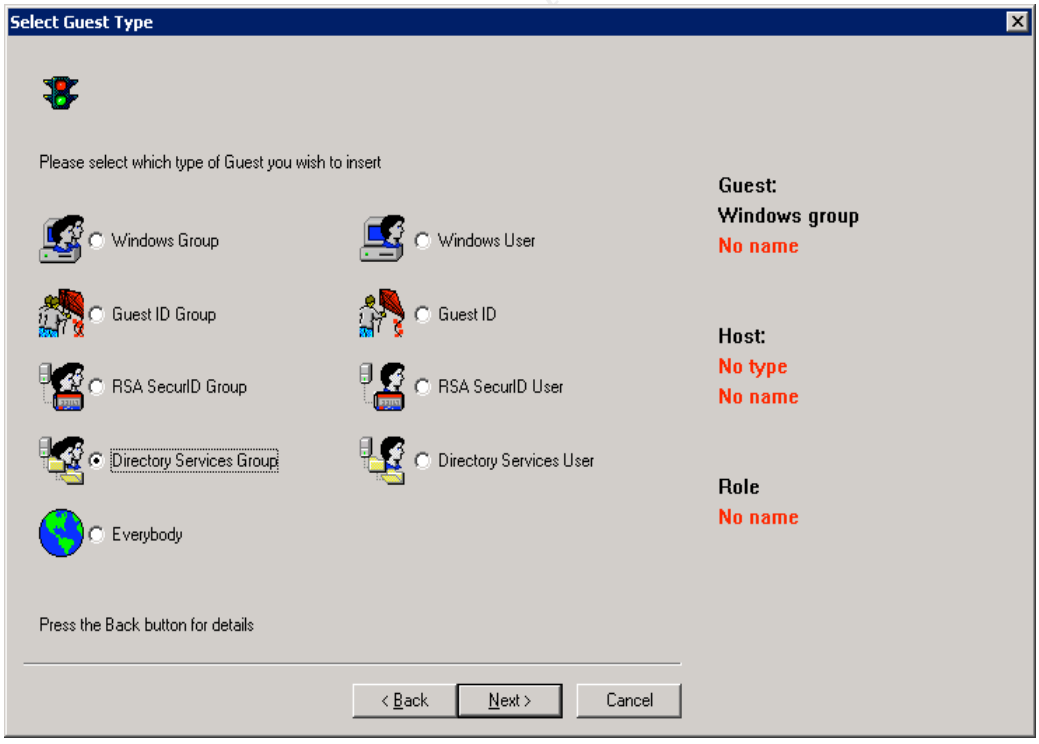
Once you have defined all of your Host ID's (or maybe just a couple for testing) then you can begin to add some Host ID Group's.



Go to the Host ID Group dialog, right click go Click New to create a group.

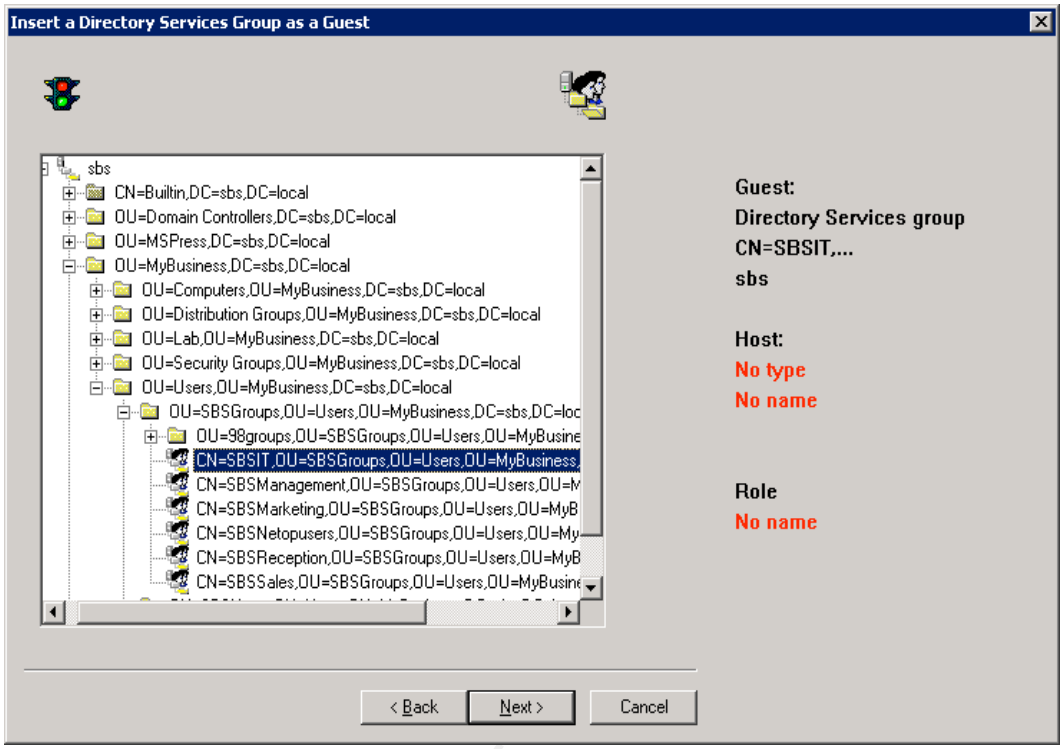


After we have our groups created and all our Hosts designated into the correct groups we can add a role assignment where we will select our Directory Services user group and our newly created Host ID group. This will determine if our configurations are correct. Go to Security Settings>Role Assignments in the Security Manager and in the right pane, right click and click **New**. You will be presented with the following dialog:

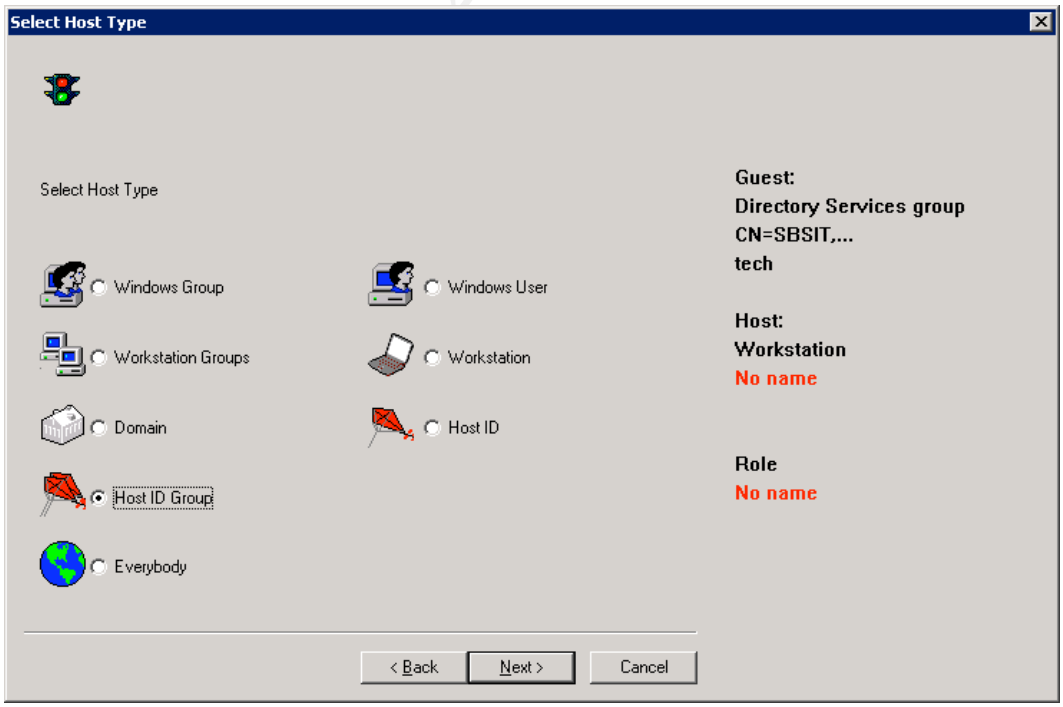


Select Directory Services **Group** and click **Next>**

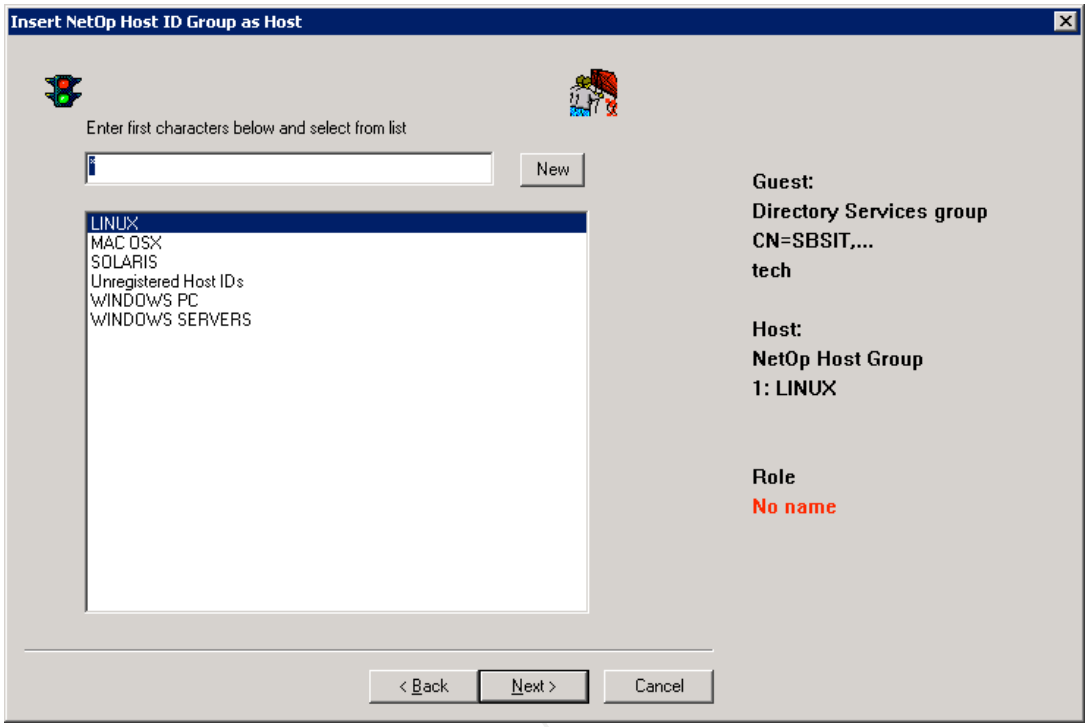
You will be presented with your domain tree if your Directory Service is properly configured and the account used has the correct permissions. Select your Directory Services Group as shown below then Click **Next >**



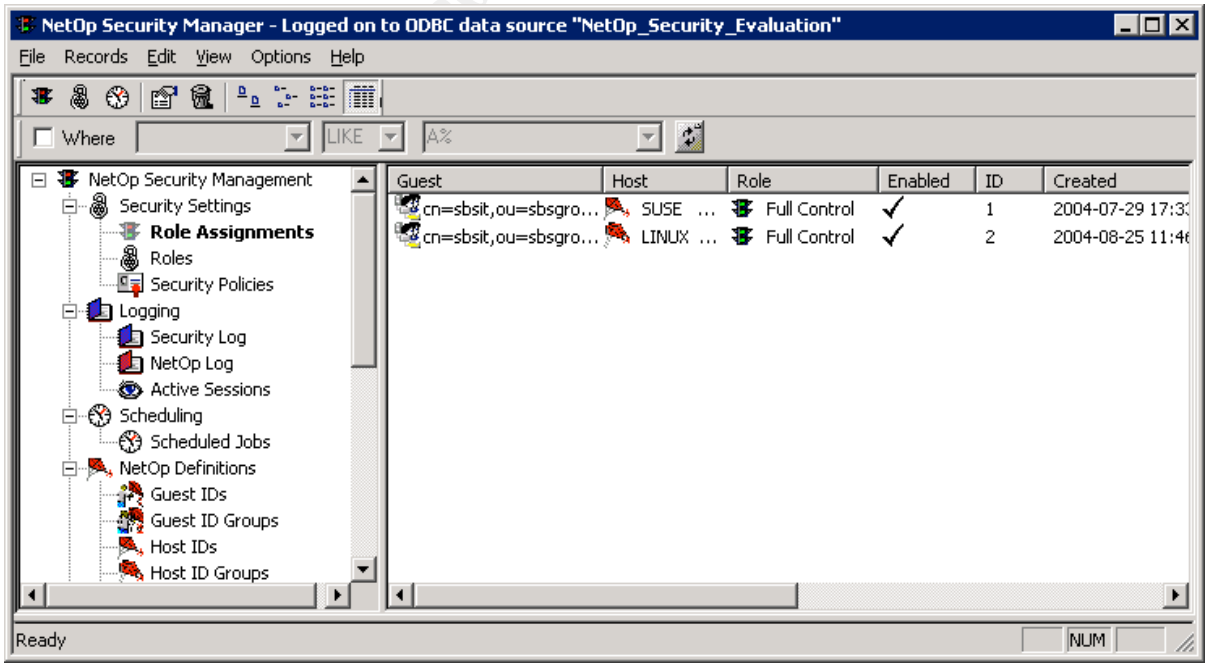
Next select Host ID Group as your Host Type:



And select your Host ID Group from the list (notice the Unregistered Host ID Group, this can be used if you want to avoid defining all your Hosts individually but requires all Guests have the same rights against all Hosts):



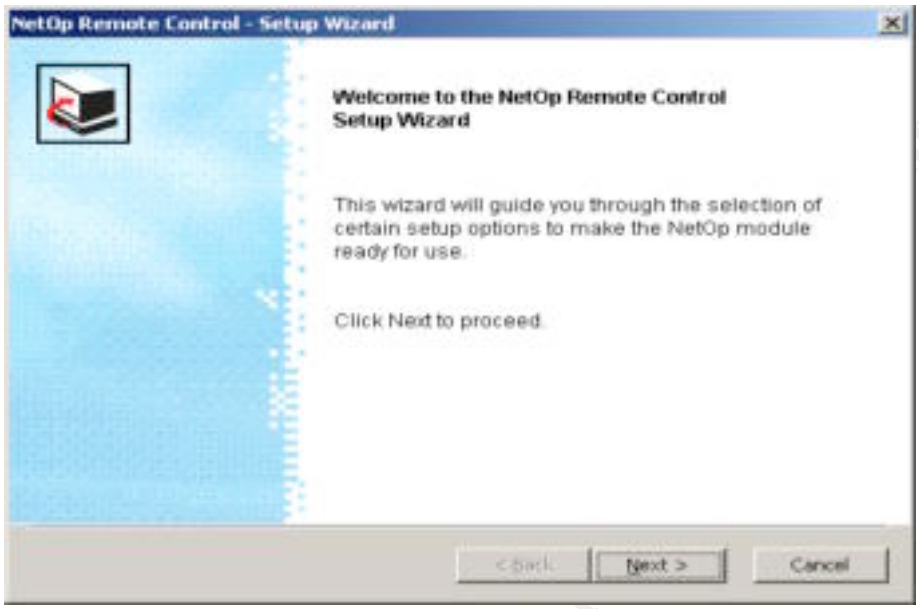
Your Role Assignment is now created:



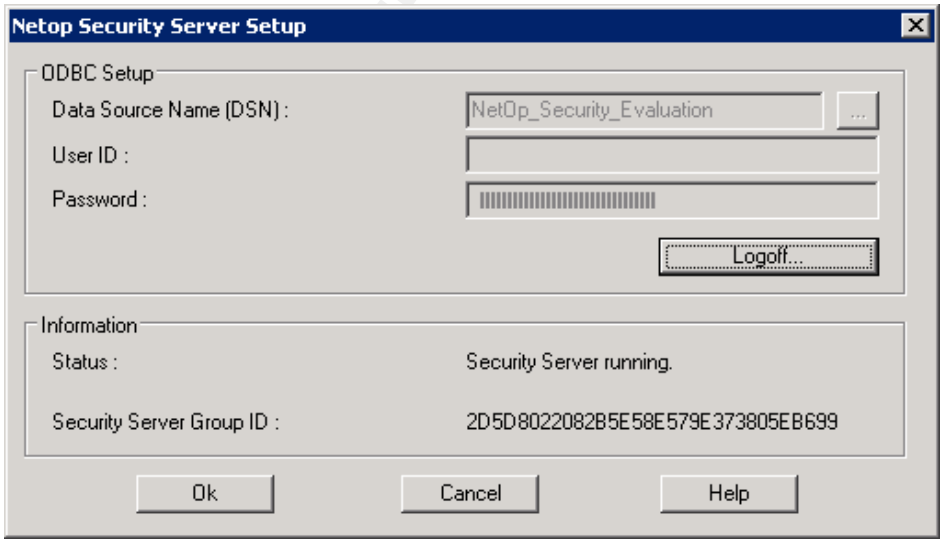
There are no more configurations to be made in the Security Manager.

Start the NSS by going to Start>Programs>Security Server 

. The setup wizard will run and usually choosing the default settings is just fine.



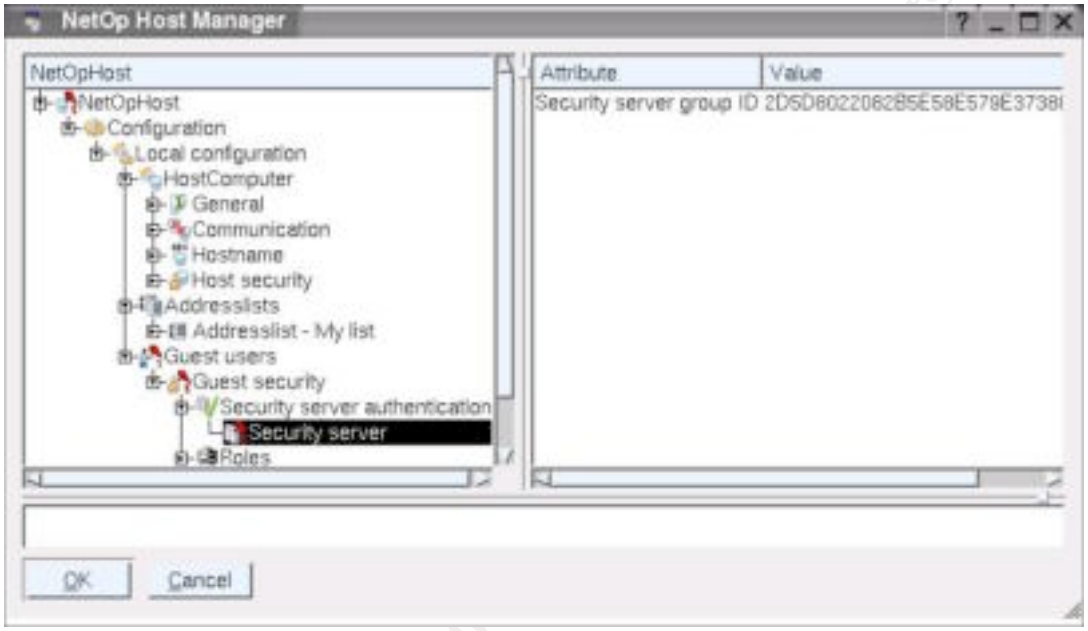
You can set up a single Host to use a directory service as opposed to centralizing it with the NSS. To do this you can refer to this Danware Knowledge Base article: http://www.netop.com/tech/support/documentation/pdf/NRC760-Active-Directory-authentication-via-LDAP.pdf . On the NSS click Tools>Security Server Setup and you will see the following dialog:



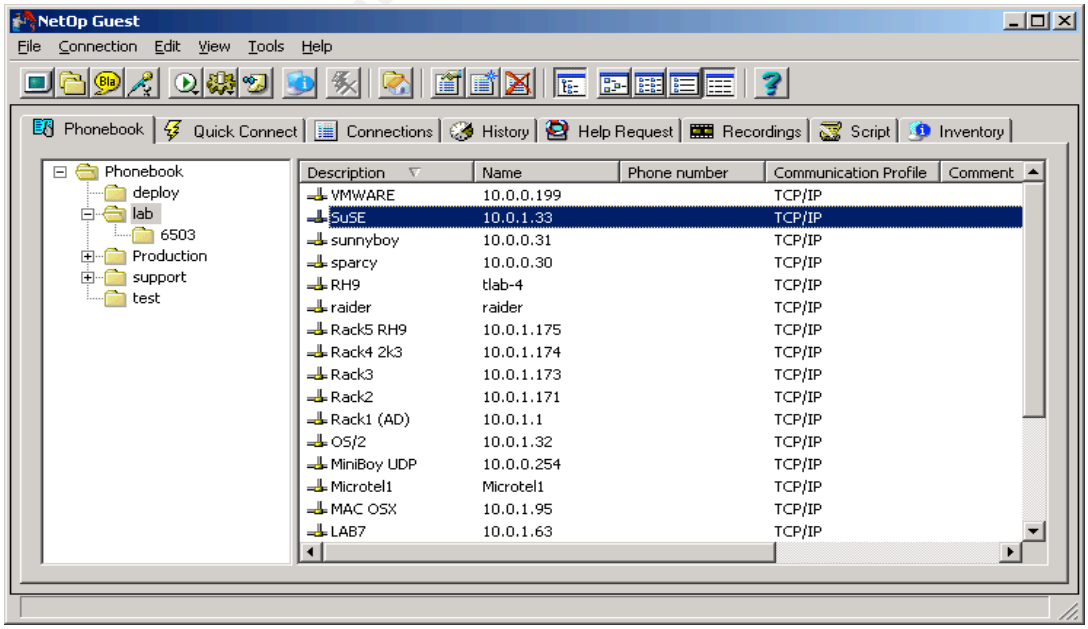
The NSS should now be running and logged into the database configured by the Security Manager. Its now time to validate your solution!

Test Your Solution

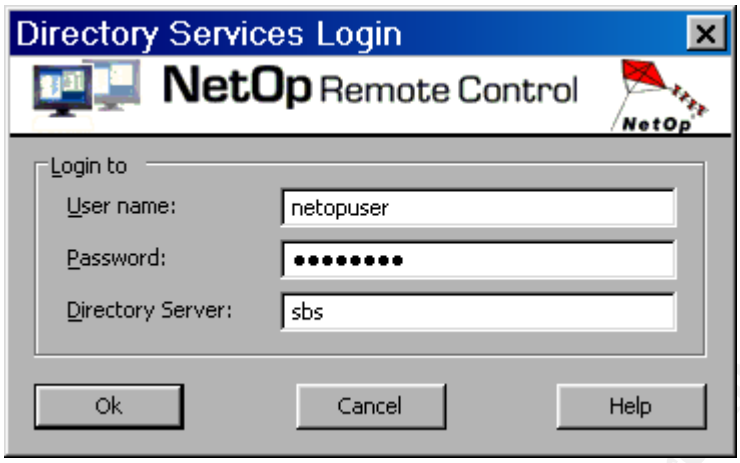
To test our connection from Directory Services Guest to Linux Host the Host must be configured with the public key of the NSS to secure the relationship between server and Host. Under Tools>Guest Access Security type in the NSS Group Name found in the Security policy>Group Name view of the Security Manager. Open a Linux terminal, run NetOpHostGUI and then go to Tools>Options>Security Server authentication and insert the NSS Group ID:



Start the Guest program and go to the Quick Connect or Phonebook tab, insert either the Host ID or IP Address of your Host then click Connect:



At this point you have a Host (in this case a SuSE 8 server) running with a valid IP address on your network as shown above; preferably on the same subnet as the Security Server and the Guest for making the test as straight forward as possible. If all goes well when you attempt to connect to the Host by IP address or name you should get this log in prompt:



- In the User name field enter your directory services Logon Name NOT your User DN or common name for the domain.
- Enter your directory services password.
- Insert the Directory Service **alias** we configured as it appears in the Security Manager NOT your domain name.
- If there is more than one Directory Service defined in your Security Manager you must insert the alias from which the user was added during the Role Assignment. This means that if you have a **sbs** alias and an **ad** alias then you must insert the correct one in this log on box even if you are a member of more than one domain.

Assuming the Security Server is running and the Role Assignment is correct you should be allowed access to this Host according to the rights you have been given by the administrator. We have now enabled our administrator's to use their current Windows user name and password when connecting to a non-Windows machine using NetOp Remote Control. This effectively reduces the amount of tools necessary for administrator's to remotely manage your network and provides a secure way of allowing vendors to provide remote maintenance at the graphical OS level. With accounts you can create and manage via your Window's domain as well as a central database repository for all of your user rights assignments and logs this becomes a highly scalable and robust solution.

For more information please download the Administrator's manual and turn to chapter one that explains the NSS in detail:
http://crosstec1.www.conxion.com/manual.exe

References:

Batz, David. **"Potential Vulnerabilities of Timbuktu Remote Control Software"** SANS Reading Room. Oct. 9, 2002. URL: http://www.sans.org/rr/papers/60/483.pdf (Aug. 5, 2004)

Caballero, Albert. **"NetOp Security Server"** Crosstec Corporation's website. July 6, 2004. URL: http://www.crossteccorp.com/support/resources/NetOp_Security_Server.pdf (Aug. 6, 2004)

Crosstec Corporation. **"NetOp Remote Control and NetOp School"** Crosstec Corporation's corporate website. URL: www.NetOpUSA.com (Aug. 26, 2004)

Crosstec Corporation. **"NetOp Remote Control Quick Install Guide"** Crosstec Corporation's White papers. May 7, 2004. URL: http://www.crossteccorp.com/support/resources/rc_quick_install.pdf (Aug. 30, 2004)

Crosstec Corporation. **"Crosstec's TryIt page"** Crosstec Corporation's website. URL: http://www.crossteccorp.com/tryit/index.html (Aug. 30, 2004)

Crosstec Corporation. **"NetOp Administrator's Manual"** Crosstec Corporation's website. URL: http://crosstec1.www.conxion.com/manual.exe (Aug. 30, 2004)

Danware Data A/S. **"How to configure NetOp Host for AD via LDAP"** Danware Knowledge Base. June 17, 2003. URL: http://www.netop.com/tech/support/documentation/pdf/NRC760-Active-Directory-authentication-via-LDAP.pdf (Aug. 10, 2004)

Danware Data A/S. **"NetOp Security Server Supported Databases"** Danware Knowledge Base. November 5, 2003. URL: http://www.netop.com/tech/support/netop_security_server/supported_databases.htm (July 7, 2004)

Danware Data A/S. **"Technical requirements for NetOp Remote Control Version 7.65"** Danware Knowledge Base. http://www.netop.com/tech/support/documentation/requirements/requirements_765.htm (Aug. 30, 2004)

Danware Data A/S. **"Latest Updates Overview"** Danware Knowledge Base. http://www.netop.com/tech/download/latestbuilds.htm (Aug. 30, 2004)

Koziel, R. Damian. **"Secure Shell Virtual Network Computing"** SANS Reading Room. July 20, 2001. URL: http://www.sans.org/rr/papers/20/721.pdf (Aug. 6, 2004)

Real VNC. **"VNC 4.0 Documentation"** Real VNC's website. URL: http://www.realvnc.com/documentation.html (Aug 26, 2004)

Rounsavall, Robert. **"Securing the NetOp Host"** Crosstec Corporation's White papers. Sept. 2, 2003. URL: http://www.crossteccorp.com/support/resources/securing.pdf (August 2, 2004)

Symantec pcAnywhere. **"Addressing Security with pcAnywhere"** Symantec's Corporate website. URL: http://sea.symantec.com/content/displaypdf.cfm?pdfid=1 (Aug. 6, 2004)

Symantec pcAnywhere. **"Symantec pcAnywhere"** Symantec's Corporate website. URL: http://sea.symantec.com/content/product.cfm?productid=16 (Aug. 26, 2004)

Windows XP Remote Assistant. **"Using Remote Assistance to Get Help When You Need It"** Microsoft's Support Website. URL: http://www.microsoft.com/windowsxp/using/helpandsupport/learnmore/remoteassist/intro.mspx (Aug. 23, 2004)