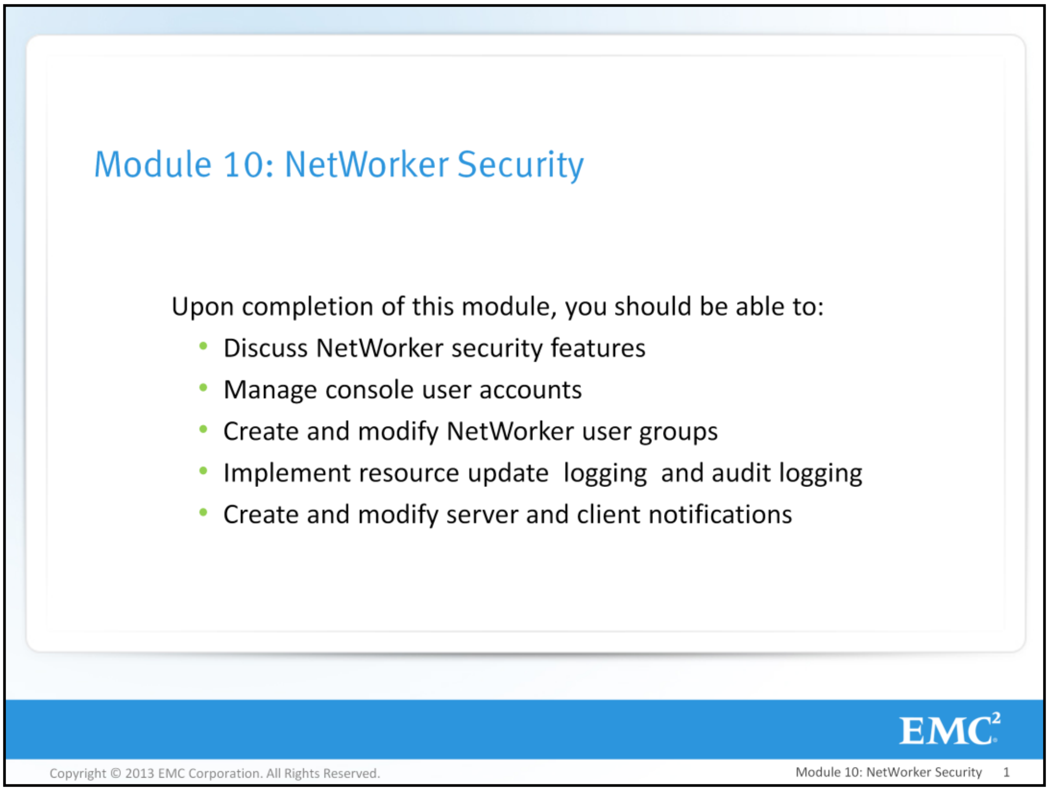
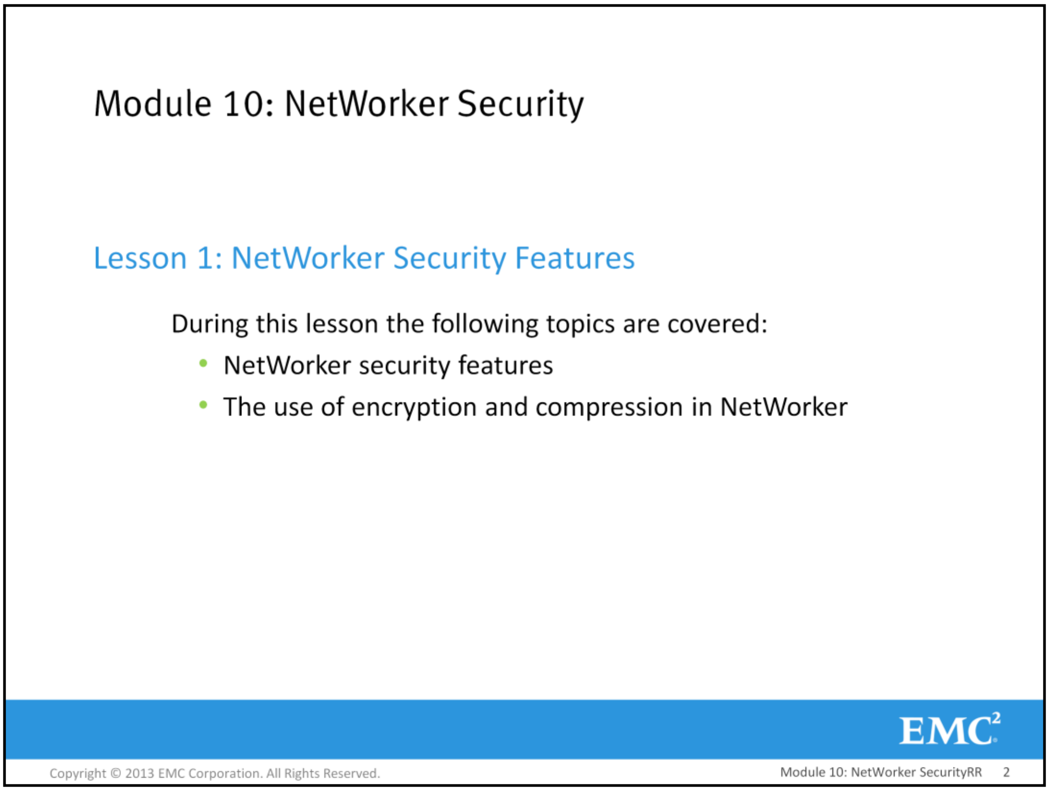


Module 10: NetWorker Security

Upon completion of this module, you should be able to:

- Discuss NetWorker security features
- Manage console user accounts
- Create and modify NetWorker user groups
- Implement resource update logging and audit logging
- Create and modify server and client notifications

This module focuses on the security features of NetWorker. It covers creating and using console user accounts and user groups within a NetWorker environment. We will look at the NetWorker jobs database and audit logging capabilities. The module concludes with a lesson on NetWorker notifications.



Module 10: NetWorker Security

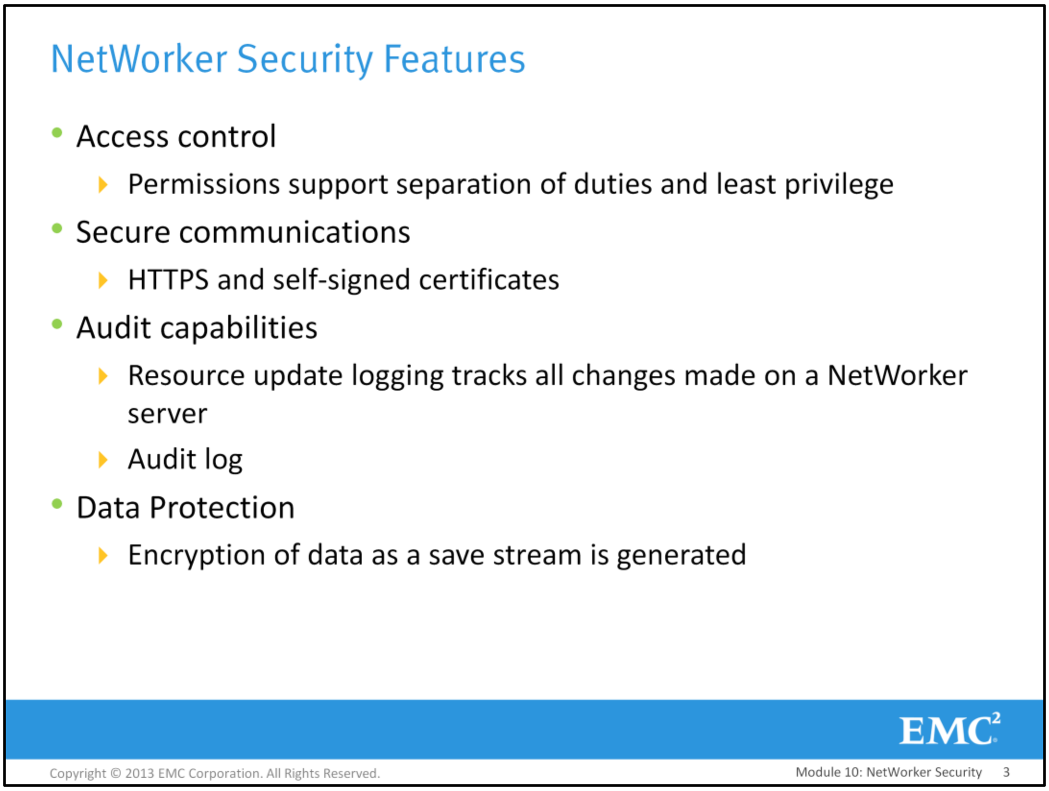
Lesson 1: NetWorker Security Features

During this lesson the following topics are covered:

- NetWorker security features
- The use of encryption and compression in NetWorker

Module 10: NetWorker SecurityRR 2

This lesson focuses on NetWorker security features, including access control, secure communications and audit features. We also examine the use of encryption and compression in NetWorker.



NetWorker Security Features

- Access control
  - Permissions support separation of duties and least privilege
- Secure communications
  - HTTPS and self-signed certificates
- Audit capabilities
  - Resource update logging tracks all changes made on a NetWorker server
  - Audit log
- Data Protection
  - Encryption of data as a save stream is generated

Module 10: NetWorker Security 3

Security is an important component of NetWorker and is accomplished in a number of ways.

NetWorker server security is implemented through the use of user groups and role-based authorization.

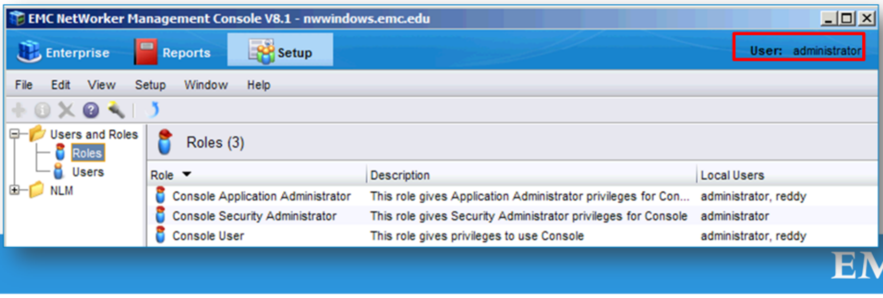
Logins to the NetWorker infrastructure are protected by HTTPS and the use of self-signed certificates for authentication between NetWorker clients and NetWorker storage nodes.

Resource update logging provides for the tracking of all resource changes made on a NetWorker server. This information is useful for accountability where there are multiple NetWorker administrators, for security in the event of a system intrusion and for general auditing of modifications. NetWorker 8 introduces the audit log property setting for every NetWorker client, storage node, and server, and must be configured on a per client basis. It is modifiable only by security or full administrator. Auditable security events include authentication attempts, privilege checks and resource creation and deletion. Multiple systems can send their audit data to the same audit log server providing centralized audit capabilities.

Security for backup data can be provided through the use of encryption. When enabled, the data is encrypted on the client as the save stream is generated.

Access Control

- Console security is implemented through the use of user accounts.
- The role assigned to a user defines the user's privileges.
- There are three console user roles: Console Security Administrator, Console Application Administrator, and Console User.
- The default user account, administrator, is assigned initially to all three roles.

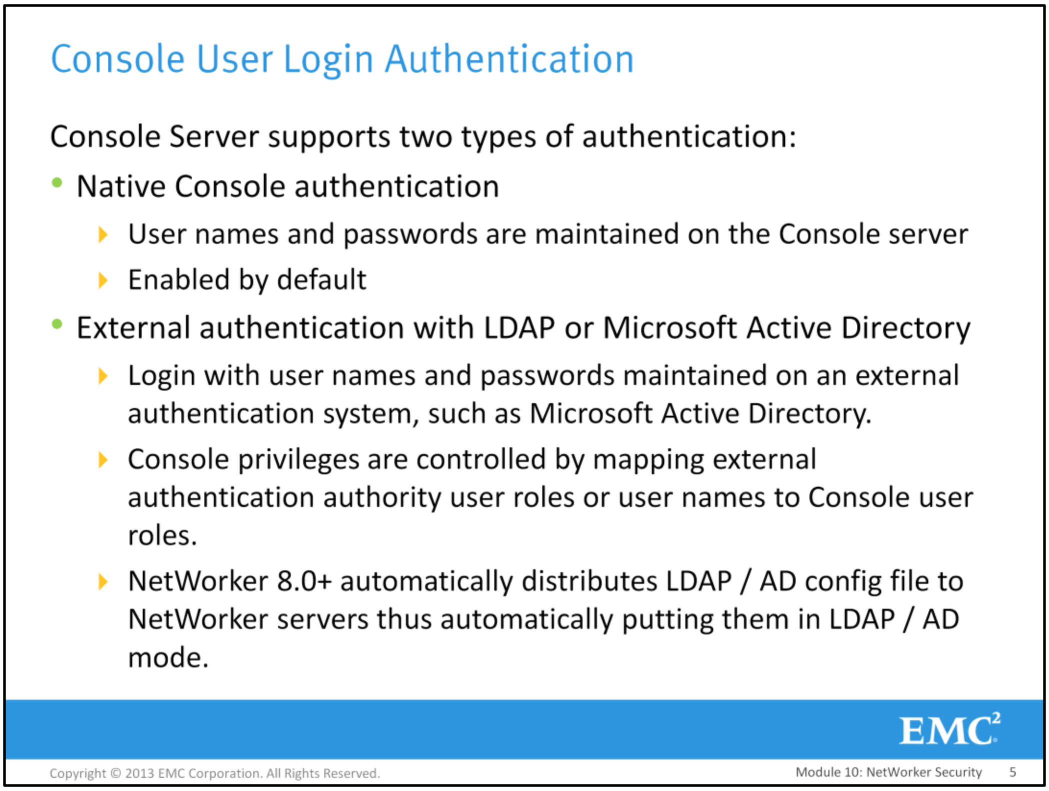


Role	Description	Local Users
Console Application Administrator	This role gives Application Administrator privileges for Con...	administrator, reddy
Console Security Administrator	This role gives Security Administrator privileges for Console	administrator
Console User	This role gives privileges to use Console	administrator, reddy

Access to NetWorker Console functionality is implemented through the use of user accounts. The role assigned to a user account determines the tasks the user can perform in Console. The roles cannot be deleted and the privileges of each role cannot be changed.

There are three Console user roles: Console Security Administrator, Console Application Administrator, and Console User. When Console is first launched, the default user account, administrator, is assigned to all three Console user roles.

User Role	Privileges
Console Security Administrator	•Add, delete and modify Console users •Configure login authentication •Control user access to managed applications •All tasks available to Console User
Console Application Administrator	•Configure Console system options •Set retention policies for reports •View custom reports •Specify the NetWorker server to backup the Console database •Specify a NetWorker License Manager server •Run the Console Configuration wizard •All tasks available to Console User
Console User	All tasks except for those tasks explicitly mentioned for the Console Security Administrator and the Console Application Administrator.



Console User Login Authentication

Console Server supports two types of authentication:

- Native Console authentication
  - User names and passwords are maintained on the Console server
  - Enabled by default
- External authentication with LDAP or Microsoft Active Directory
  - Login with user names and passwords maintained on an external authentication system, such as Microsoft Active Directory.
  - Console privileges are controlled by mapping external authentication authority user roles or user names to Console user roles.
  - NetWorker 8.0+ automatically distributes LDAP / AD config file to NetWorker servers thus automatically putting them in LDAP / AD mode.

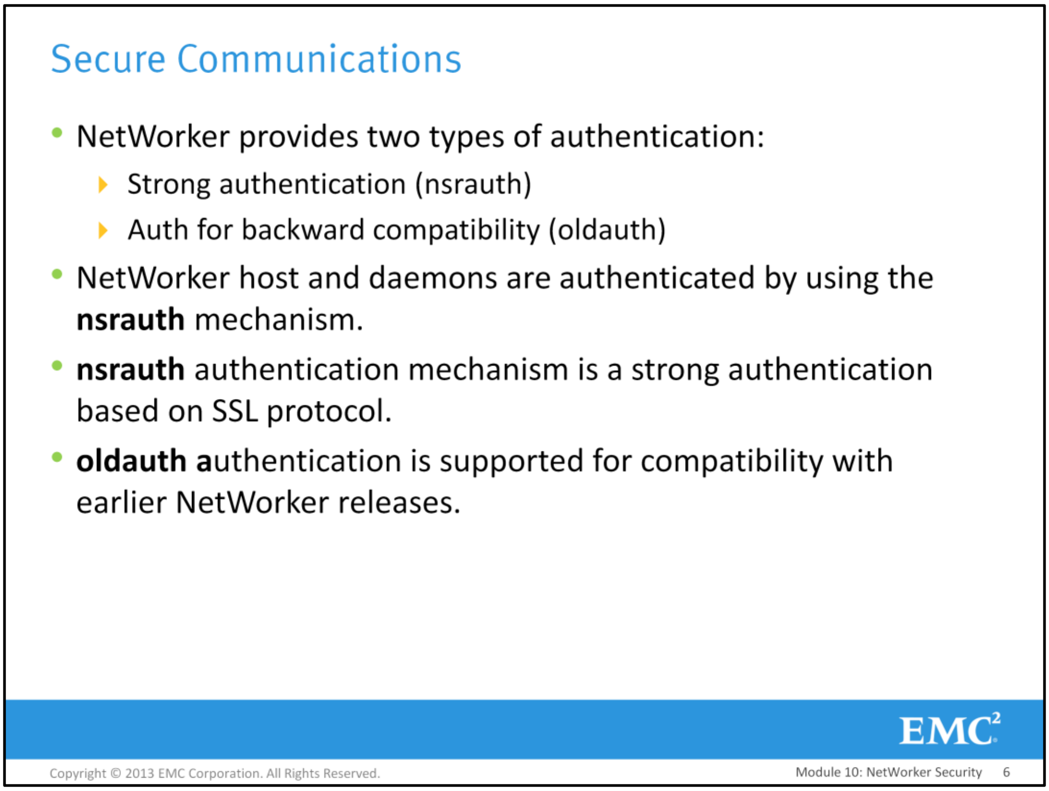
Module 10: NetWorker Security 5

Authentication is a user name/password system that is used to grant user access to the NetWorker Management Console server. Console can leverage an external repository such as LDAP or Microsoft Active Directory in addition to its own internal authentication system.

With native Console authentication, user names and passwords are maintained on the Console server. Native NetWorker Management Console authentication is enabled by default.

With external authentication, user names and passwords are maintained and authenticated by an external LDAP v3 compliant or a Microsoft Active Directory (AD) server. When configured for external authentication, console login and user privileges are controlled by mapping LDAP/AD user roles and user names to Console user roles. There is no requirement to maintain user names and passwords in Console. However, when the LDP or AD user connects to a NetWorker server, the privileges assigned to the user on the NetWorker server are based on the LDAP user/group entries in the external roles attribute of the User Group resource on the NetWorker server.

With NetWorker version 8.0 software or higher, NetWorker automatically distributes the LDAP or AD configuration file from the Console server to the NetWorker servers that are managed by the Console server. This automatically puts the managed NetWorker servers in LDAP or AD mode.



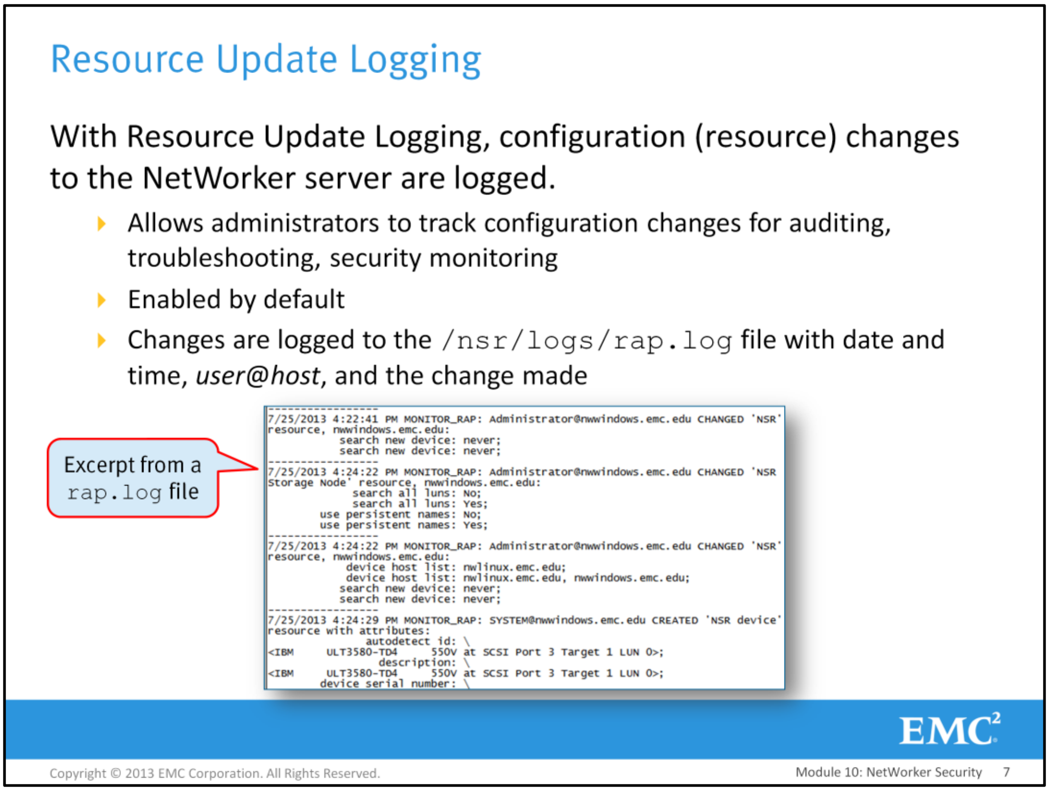
Secure Communications

- NetWorker provides two types of authentication:
  - Strong authentication (nsrauth)
  - Auth for backward compatibility (oldauth)
- NetWorker host and daemons are authenticated by using the **nsrauth** mechanism.
- **nsrauth** authentication mechanism is a strong authentication based on SSL protocol.
- **oldauth a**uthentication is supported for compatibility with earlier NetWorker releases.

NetWorker provides two types of authentication: **nsrauth** and **oldauth**.

The **nsrauth** authentication mechanism is enabled by default and is strong authentication based on the secure socket layer protocol which is provided by the OpenSSL library. Each NetWorker host has a `nsrexecd` service which provides authentication services. Each `nsrexecd` has its own private key and self-signed certificate for authentication. The private key is generated by `nsrexecd` when it starts up or one can be loaded from a file. The corresponding self-signed certificate is generated by the private key. GSS is required for the following NetWorker functionalities: client configuration wizard, filesystem browse from client configuration, and software distribution.

For compatibility with earlier NetWorker releases, oldauth authentication is supported. If two hosts cannot authenticate by using strong authentication, you can enable authentication by using oldauth. One can specify the minimum authentication strength that is allowed for any host relationship. Refer to the *EMC NetWorker Administration Guide* for details on configuring minimum authentication strengths.



Resource Update Logging

With Resource Update Logging, configuration (resource) changes to the NetWorker server are logged.

- Allows administrators to track configuration changes for auditing, troubleshooting, security monitoring
- Enabled by default
- Changes are logged to the `/nsr/logs/rap.log` file with date and time, *user@host*, and the change made

Excerpt from a `rap.log` file

```
-----------------
7/25/2013 4:22:41 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR'
resource, nwwindows.emc.edu:
           search new device: never;
           search new device: never;
-----------------
7/25/2013 4:24:22 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR
Storage Node' resource, nwwindows.emc.edu:
             search all luns: No;
             search all luns: Yes;
        use persistent names: No;
        use persistent names: Yes;
-----------------
7/25/2013 4:24:22 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR'
resource, nwwindows.emc.edu:
            device host list: nwlinux.emc.edu;
            device host list: nwlinux.emc.edu, nwwindows.emc.edu;
           search new device: never;
           search new device: never;
-----------------
7/25/2013 4:24:29 PM MONITOR_RAP: SYSTEM@nwwindows.emc.edu CREATED 'NSR device'
resource with attributes:
               autodetect id: \
<IBM     ULT3580-TD4     550V at SCSI Port 3 Target 1 LUN 0>;
                 description: \
<IBM     ULT3580-TD4     550V at SCSI Port 3 Target 1 LUN 0>;
        device serial number: \
```

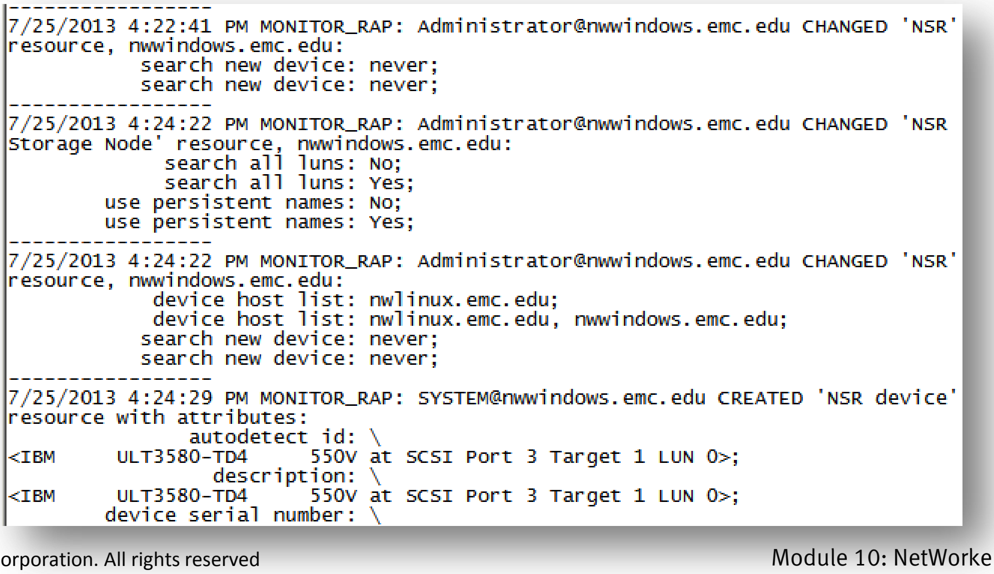
EMC²

Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 7

Resource Update Logging allows you to track all resource changes made on a NetWorker server. Any change made to a NetWorker resource, as well as the creation or deletion of a resource, is logged to the text file `~/nsr/logs/rap.log` on the NetWorker server. Each log entry includes a time stamp of the change, the login name of the user making the change, and specific information about the attribute and attribute values that were changed. This information is useful for accountability if there are multiple NetWorker administrators, for security in the event of a system intrusion, and for general auditing of NetWorker modifications. Resource update logging is enabled/disabled by setting the **Monitor RAP** attribute of the Server (NSR) resource. By default it is **Enabled**.

Here is an excerpt from a `rap.log` file:

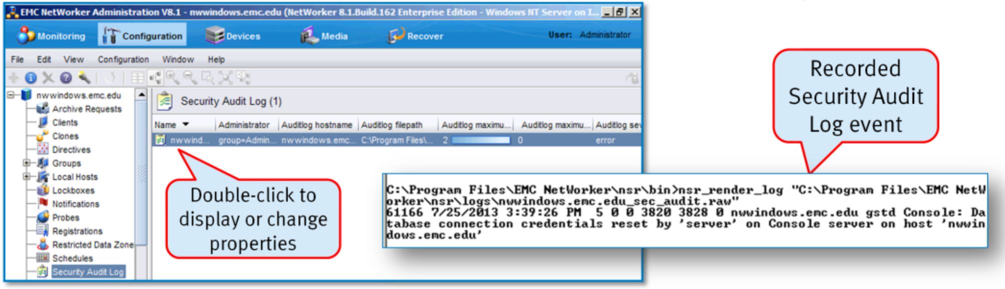


```
-----------------
7/25/2013 4:22:41 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR'
resource, nwwindows.emc.edu:
           search new device: never;
           search new device: never;
-----------------
7/25/2013 4:24:22 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR
Storage Node' resource, nwwindows.emc.edu:
             search all luns: No;
             search all luns: Yes;
        use persistent names: No;
        use persistent names: Yes;
-----------------
7/25/2013 4:24:22 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR'
resource, nwwindows.emc.edu:
            device host list: nwlinux.emc.edu;
            device host list: nwlinux.emc.edu, nwwindows.emc.edu;
           search new device: never;
           search new device: never;
-----------------
7/25/2013 4:24:29 PM MONITOR_RAP: SYSTEM@nwwindows.emc.edu CREATED 'NSR device'
resource with attributes:
               autodetect id: \
<IBM     ULT3580-TD4     550V at SCSI Port 3 Target 1 LUN 0>;
                 description: \
<IBM     ULT3580-TD4     550V at SCSI Port 3 Target 1 LUN 0>;
        device serial number: \
```

Security Audit Logging

Centralized audit mechanism for recording security related events that occur in a NetWorker datazone

- NetWorker 8.0 and later feature
- Automatically enabled for all clients at software installation
- Client processes send audit messages to the nsrlogd daemon where the messages are recorded in the security audit log file
- Any client in the datazone can be configured to host nsrlogd



Name	Administrator	Auditlog hostname	Auditlog filepath	Auditlog maximu...	Auditlog maximu...	Auditlog se
nwwind...	group=Admin...	nwwindows.emc...	C:\Program Files\...	2	0	error

Double-click to display or change properties

Recorded Security Audit Log event

```
C:\Program Files\EMC NetWorker\nsr\bin>nsr_render_log "C:\Program Files\EMC NetW
orker\nsr\logs\nwwindows.emc.edu_sec_audit.raw"
61166 7/25/2013 3:39:26 PM  5 0 0 3820 3828 0 nwwindows.emc.edu gstd Console: Da
tabase connection credentials reset by 'server' on Console server on host 'nwwin
dows.emc.edu'
```

EMC²

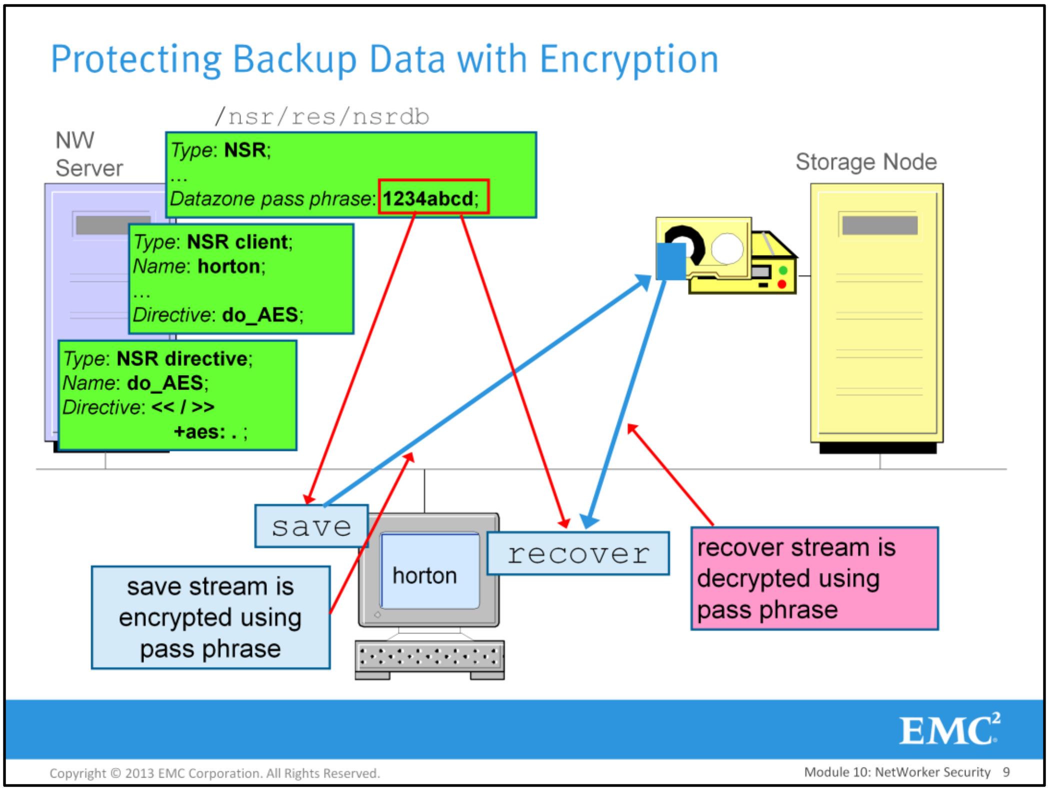
Beginning with NetWorker 8, NetWorker provides a centralized logging feature for recording security related events occurring in a NetWorker datazone. Each client is automatically configured to use security audit logging by default when NetWorker 8.0 and above software is installed. Examples of events that can be recorded include authentication attempts, account privilege changes and authorization changes.

The NSR auditlog resource is used to configure security audit logging. The resource on the NetWorker server is mirrored to all 8.0 and later clients in the datazone. Client processes send audit messages to the nsrlogd daemon where they are recorded in the security audit log file. This file is located in the ~/nsr/logs directory and is read using the nsr_render_logs utility. The security audit logging configuration can only be changed by users with security or full administrator privileges.

The nsrlogd daemon runs on the NetWorker server by default. The configuration can be changed to specify a client of the NetWorker server that will run the daemon. Also, by hosting the nsrlogd on the NMC server, multiple NetWorker systems can send their audit data to the same audit log server.

Please see the *EMC NetWorker Administration Guide* for more information about the security audit logging feature including examples of various audit logging configurations.

Note: The audit log is not a replacement for the RAP log.



Protecting Backup Data with Encryption

/nsr/res/nsrdb

Type: **NSR**;
…
Datazone pass phrase: **1234abcd**;

Type: **NSR client**;
Name: **horton**;
…
Directive: **do_AES**;

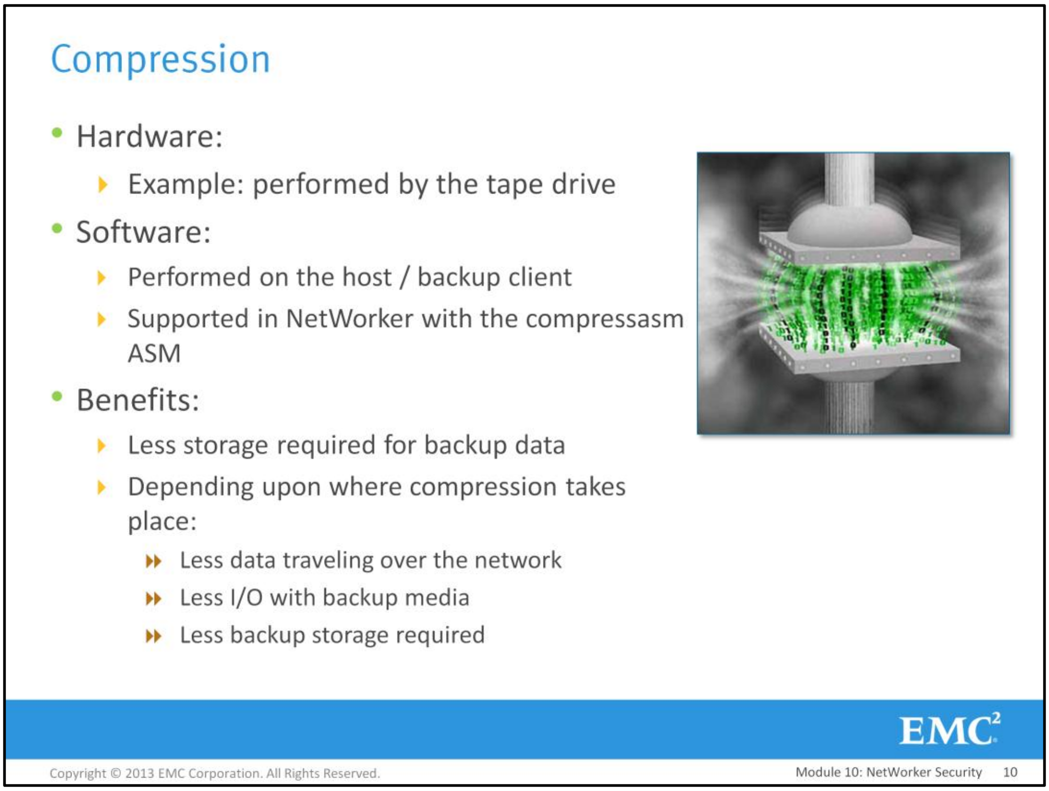
Type: **NSR directive**;
Name: **do_AES**;
Directive: **<< / >>**
+aes: . ;

save stream is encrypted using pass phrase

recover stream is decrypted using pass phrase

Module 10: NetWorker Security 9

Windows and UNIX backup data can be encrypted using the NetWorker aes Application Specific Module, ASM. The aes ASM provides 256-bit data encryption. During a backup of a client using the aes ASM, the NetWorker server provides the value assigned to the *Datazone pass phrase* to the client being backed up. This pass phrase is used to encrypt the data on the client as the save stream is generated. If the *Datazone pass phrase* attribute has no value, the default pass phrase is used. During recovery of encrypted data, the value of the *Datazone pass phrase* attribute is used for decryption. If decryption fails, another attempt to decrypt the data is made using the default pass phrase. If that decryption fails, the recovery will fail. If the current *Datazone pass phrase* was created after the backup was performed, the user must provide the pass phrase that was in effect at the time of the backup.



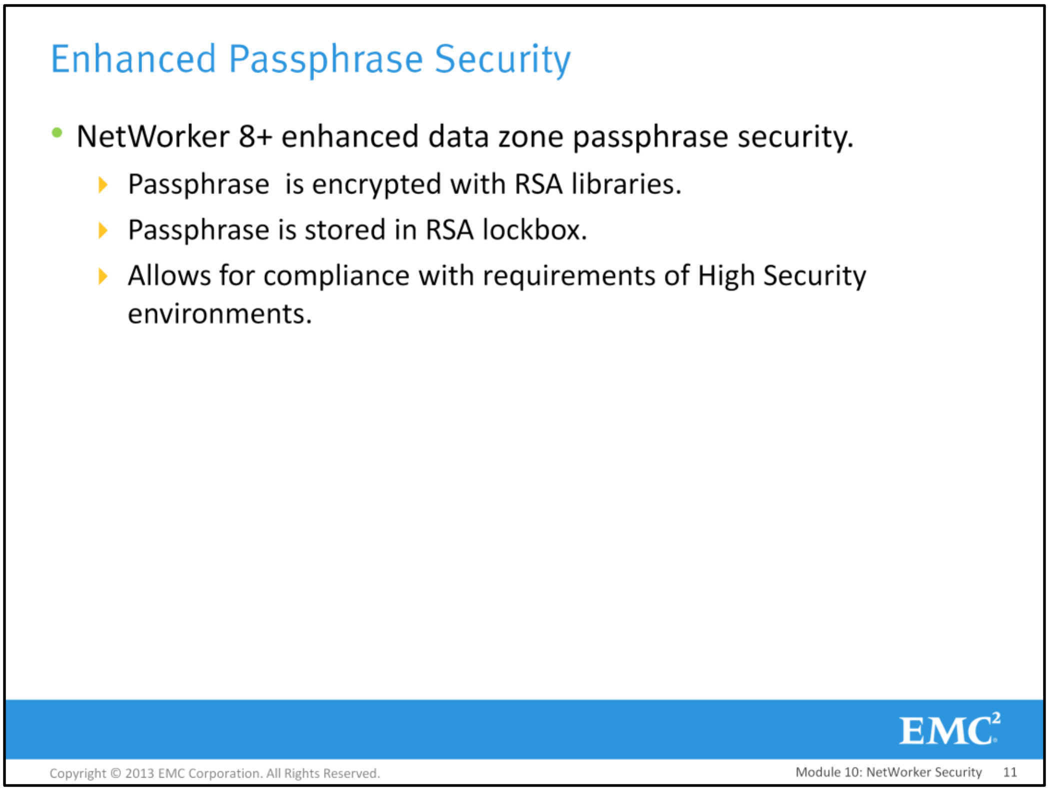
Compression

- Hardware:
  - Example: performed by the tape drive
- Software:
  - Performed on the host / backup client
  - Supported in NetWorker with the compressasm ASM
- Benefits:
  - Less storage required for backup data
  - Depending upon where compression takes place:
    - Less data traveling over the network
    - Less I/O with backup media
    - Less backup storage required

Data compression is the process of encoding information using fewer bits than the original representation. The primary goal and benefit of compression is to reduce the amount of storage media consumed by data. Depending upon where the compression takes place there could be additional benefits including sending less data across the network to backup storage and improving performance through less I/O with backup media.

Compression can be performed at two levels, hardware or software. Hardware compression is compression that is done at the hardware level, such as in a tape drive or in a hardware expansion board. It’s usually done at the backup device, so the data travels from the backup client through the LAN uncompressed, and is compressed right before it is written to the backup media. Tape drive hardware compression is very efficient and uses no additional CPU cycles on any component of the backup infrastructure.

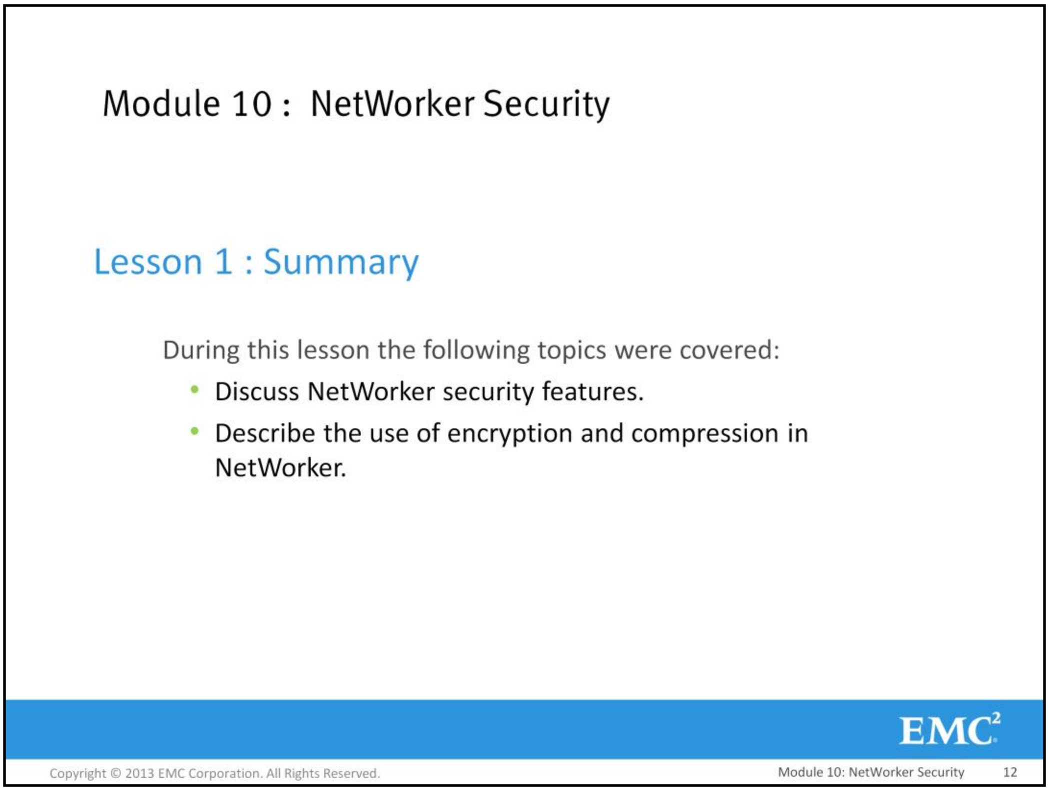
Software compression is compression that is done at the host level using CPU cycles and memory of the host, such as in a backup client. Software compression places an overhead on the host due to the processing requirements to accomplish compression. When software compression takes place at the backup client level, data travels compressed through the LAN, thus reducing the overall bandwidth taken, and is then written to the backup media. Compressed data must be decompressed in order to be used and this may also entail additional processing. NetWorker enables compression of data during backup processing through the use of the compressasm ASM. Alternatively, a preconfigured directive applicable to a client’s operating system can be used.



Enhanced Passphrase Security

- NetWorker 8+ enhanced data zone passphrase security.
  - Passphrase is encrypted with RSA libraries.
  - Passphrase is stored in RSA lockbox.
  - Allows for compliance with requirements of High Security environments.

Previously released versions of NetWorker store the data zone passphrase in encrypted format in the central NetWorker database. Beginning with NetWorker 8.0, data zone passphrases are now encrypted using RSA libraries and are stored in an RSA lockbox. The enhanced security of the data zone passphrase allows for compliance with the highest security requirements.



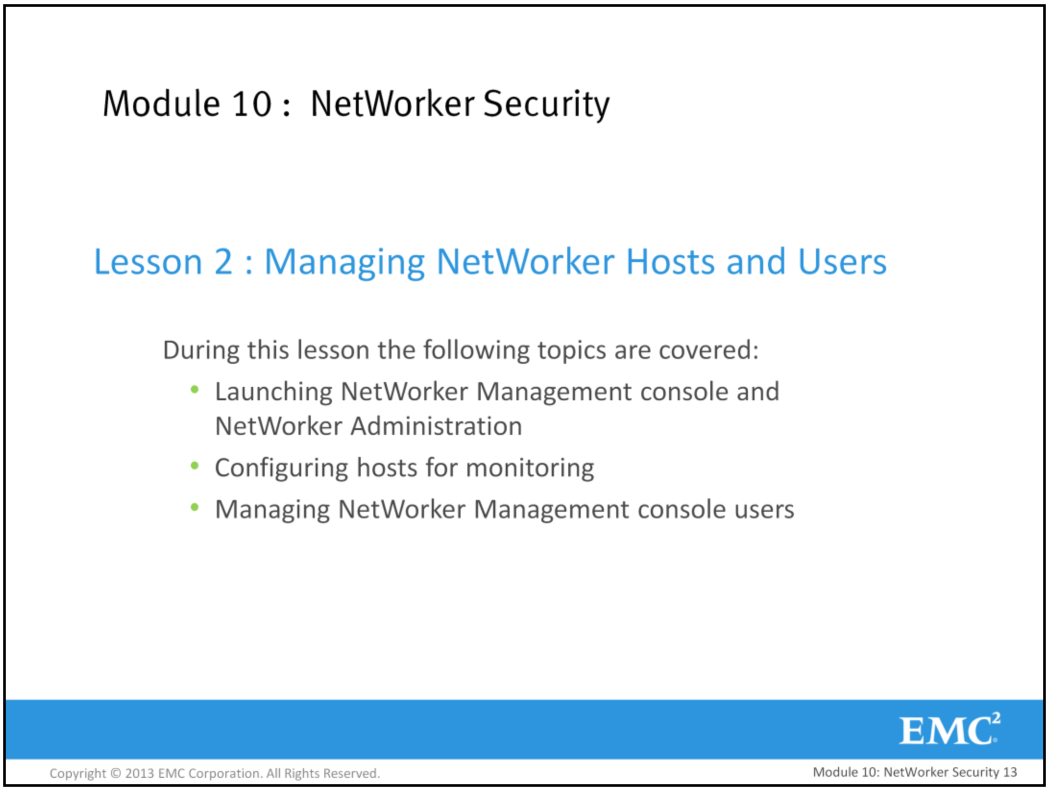
Module 10 : NetWorker Security

Lesson 1 : Summary

During this lesson the following topics were covered:

- Discuss NetWorker security features.
- Describe the use of encryption and compression in NetWorker.

This lesson focused on NetWorker security features, including access control, secure communications and audit features. We also examined the use of encryption and compression in NetWorker.



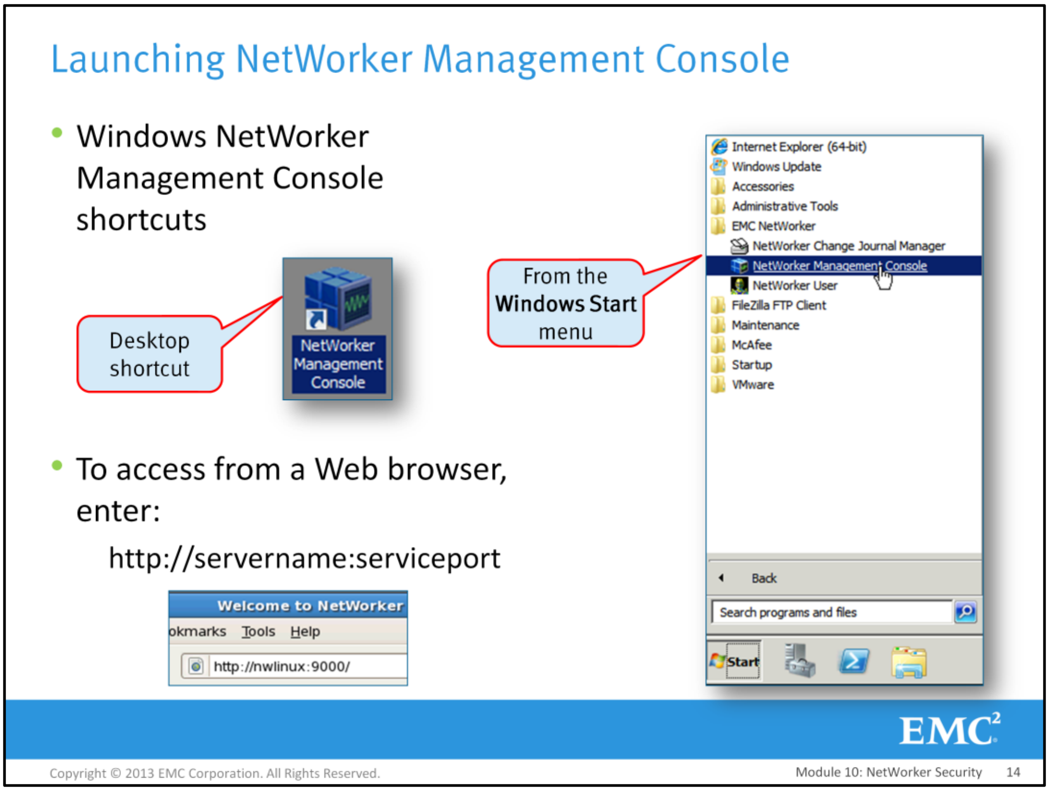
Module 10 : NetWorker Security

Lesson 2 : Managing NetWorker Hosts and Users

During this lesson the following topics are covered:

- Launching NetWorker Management console and NetWorker Administration
- Configuring hosts for monitoring
- Managing NetWorker Management console users

This lesson covers how to launch the NetWorker administration GUI interfaces, configure hosts in NMC and configure NetWorker Management console users.



Launching NetWorker Management Console

- Windows NetWorker Management Console shortcuts
- To access from a Web browser, enter:

  http://servername:serviceport

Desktop shortcut

From the **Windows Start** menu

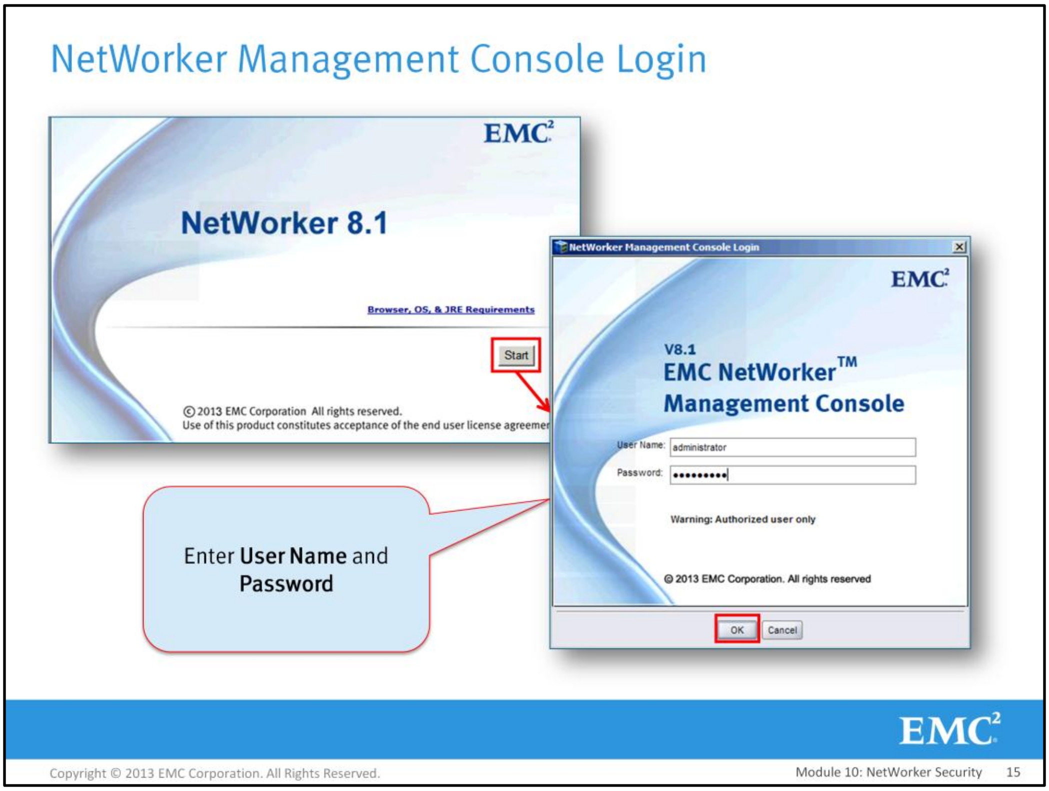
Copyright © 2013 EMC Corporation. All Rights Reserved. Module 10: NetWorker Security 14

NetWorker Management Console, NMC, provides access to each managed NetWorker server in an environment for NetWorker administration functions including configuring clients, devices and other resources, and scheduling, running, and monitoring backups. With NMC, NetWorker can be administered from any host having a supported web browser. For example, you can administer a UNIX NetWorker server from a Windows machine and vice versa. The URL used to connect to the NetWorker Management Console server is:

http://console_server:http_service_port

where console_server is the host name of the console server and http_service_port is the port number for the embedded web server that was specified during the Console server installation. The default HTTP port is 9000.

To start the NMC on a Windows platform, click the program shortcut on the desktop or in the Windows Start menu.



NetWorker Management Console Login

EMC²
NetWorker 8.1
Browser, OS, & JRE Requirements
Start
© 2013 EMC Corporation All rights reserved.
Use of this product constitutes acceptance of the end user license agreemer
NetWorker Management Console Login
EMC²
V8.1
EMC NetWorker™
Management Console

User Name: administrator

Password: ••••••••••

Warning: Authorized user only

© 2013 EMC Corporation. All rights reserved

Enter **User Name** and **Password**

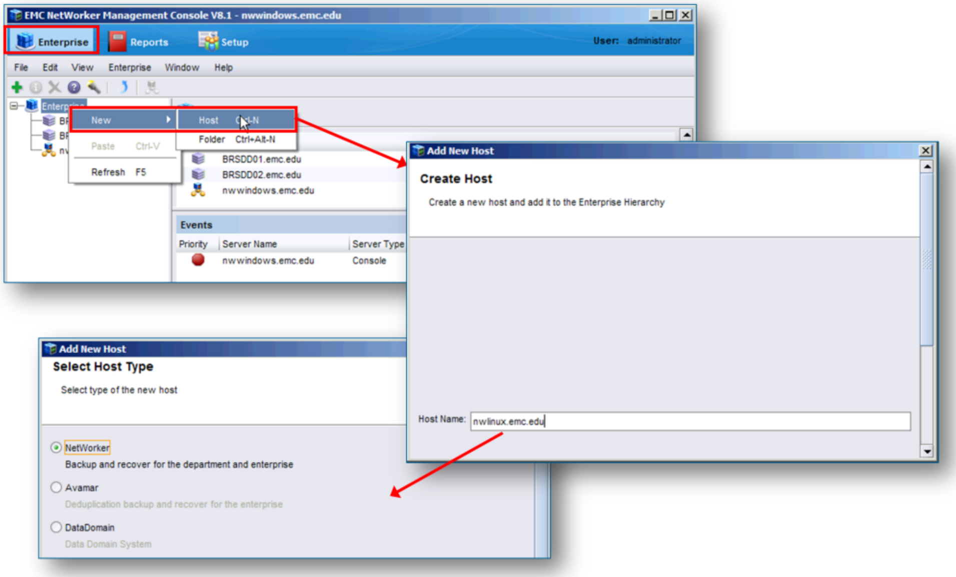
Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 15

A supported version of Java Runtime Environment (JRE) must be installed on the Console client. JRE, which includes Java Web Start, must be installed in order to download and run the Console client properly. Upon launching the Console client, you are notified if an appropriate version of JRE is not installed. Follow instructions for downloading and installing a supported version of JRE from the Java web site. After installing JRE, close and restart the browser.

When NetWorker Management Console is launched, a login screen is displayed to the user. A user cannot run NMC unless a valid User Name and Password combination is provided.

Managing Multiple NetWorker Servers



	BRSDD01.emc.edu	
	BRSDD02.emc.edu	
	nwwindows.emc.edu	

Events

Priority	Server Name	Server Type
●	nwwindows.emc.edu	Console

Create Host

Create a new host and add it to the Enterprise Hierarchy

Host Name: nwlinux.emc.edu

Select Host Type

Select type of the new host

● NetWorker
Backup and recover for the department and enterprise

○ Avamar
Deduplication backup and recover for the enterprise

○ DataDomain
Data Domain System

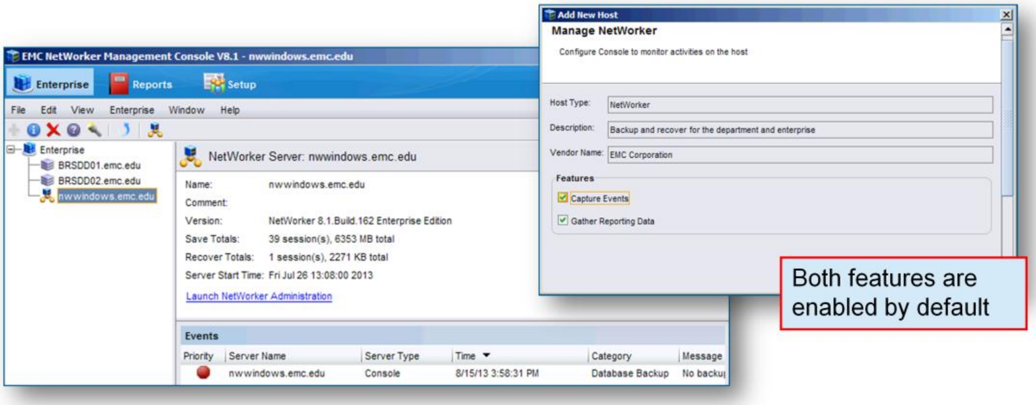
You can configure a NetWorker Management Console server to manage multiple NetWorker servers and other hosts. To display a list of NetWorker servers managed by the Console server, go to the **Enterprise** view. In the left pane, a hierarchical list of managed hosts, including NetWorker servers, is displayed.

To add a new host to the Console, right-click **Enterprise** in the left pane and select **New**. Managed host types include NetWorker, Avamar and Data Domain.

Setting Information Gathering Features

Information gathering is configurable for each NetWorker server:

- When **Capture Events** is enabled:
  - Console receives event notifications from the NetWorker server
- When **Gather Reporting Data** is enabled:
  - Data from the NetWorker server is incorporated into Console reports


EMC NetWorker Management Console V8.1 - nwwindows.emc.edu
Enterprise
Reports
Setup
File Edit View Enterprise Window Help
Enterprise
BRSDD01.emc.edu
BRSDD02.emc.edu
nwwindows.emc.edu
Launch NetWorker Administration
Add New Host

NetWorker Server: nwwindows.emc.edu

Name: nwwindows.emc.edu
Comment:
Version: NetWorker 8.1.Build.162 Enterprise Edition
Save Totals: 39 session(s), 6353 MB total
Recover Totals: 1 session(s), 2271 KB total
Server Start Time: Fri Jul 26 13:08:00 2013

Events

Priority	Server Name	Server Type	Time	Category	Message
●	nwwindows.emc.edu	Console	8/15/13 3:58:31 PM	Database Backup	No backu

Manage NetWorker

Configure Console to monitor activities on the host

Host Type: NetWorker
Description: Backup and recover for the department and enterprise
Vendor Name: EMC Corporation

Features
☑ Capture Events
☑ Gather Reporting Data

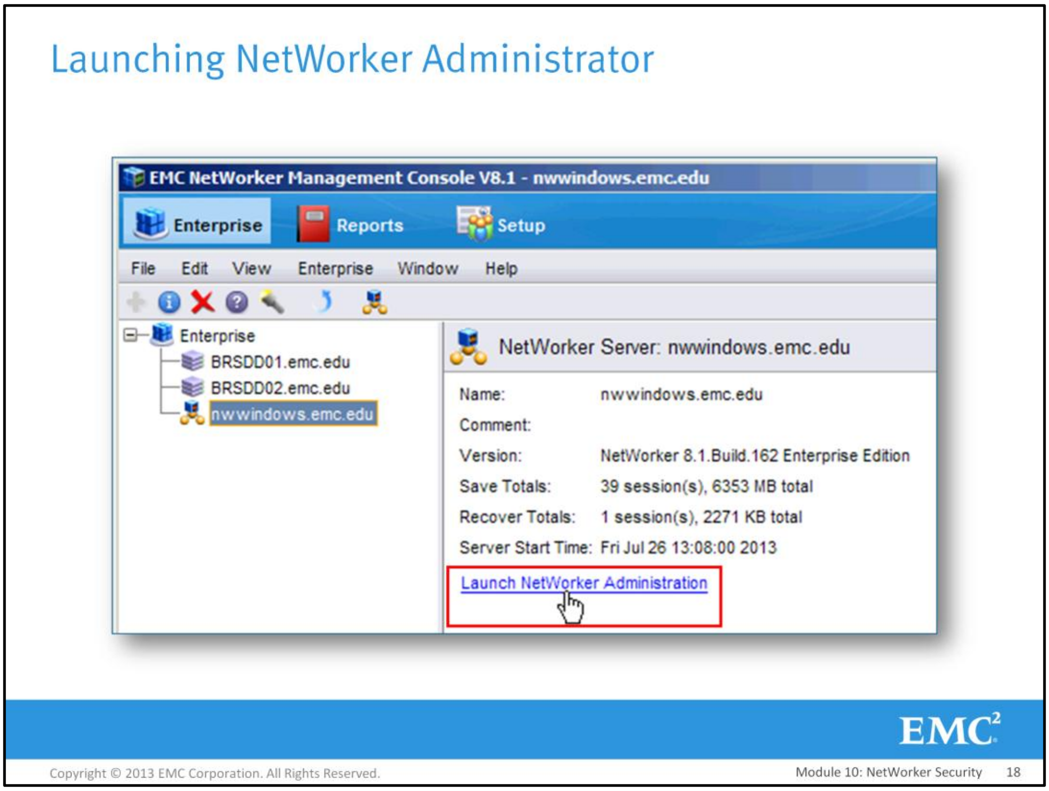
Both features are enabled by default

Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 17

By default, when a host is selected in the left pane of the ***Enterprise*** view, NetWorker displays information about that host in the right pane. When you add a new host, you can choose whether or not to capture events and gather reporting data about that host. Selecting **Capture Events** allows events such as disabled licenses and pending media requests to be displayed in the Console ***Events*** window. Selecting **Gather Reporting Data** allows the Console server to accumulate data retrieved from the NetWorker server jobs database to be used when creating reports.

After the host is created, these selections can be changed from the Properties menu of the host.



Launching NetWorker Administrator

NetWorker Server: nwwindows.emc.edu

Name: nwwindows.emc.edu

Comment:

Version: NetWorker 8.1.Build.162 Enterprise Edition

Save Totals: 39 session(s), 6353 MB total

Recover Totals: 1 session(s), 2271 KB total

Server Start Time: Fri Jul 26 13:08:00 2013

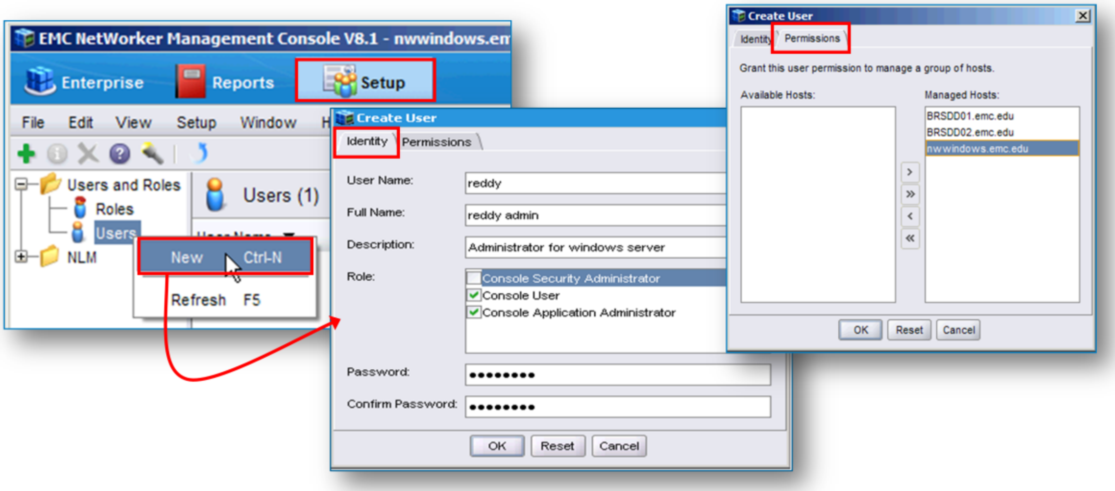
Copyright © 2013 EMC Corporation. All Rights Reserved. Module 10: NetWorker Security 18

To configure, monitor and manage a datazone for a NetWorker server, launch the NetWorker Administration interface from the NMC ***Enterprise*** window by clicking the **Launch NetWorker Administration** link.

Note: If the NetWorker server and the NMC server are on different hosts, the Administrator list attribute on the NetWorker server must include the appropriate NMC accounts before connecting to a NetWorker server.

Managing Console Users

- Configure additional Console accounts to manage specific NetWorker servers or perform specific Console tasks
- By default, Console users can view all managed NetWorker servers



User Name: reddy
Full Name: reddy admin
Description: Administrator for windows server
Role:
☐ Console Security Administrator
☑ Console User
☑ Console Application Administrator
Password: ••••••••
Confirm Password: ••••••••

Grant this user permission to manage a group of hosts.

Available Hosts:

Managed Hosts:
BRSDD01.emc.edu
BRSDD02.emc.edu
nwwindows.emc.edu

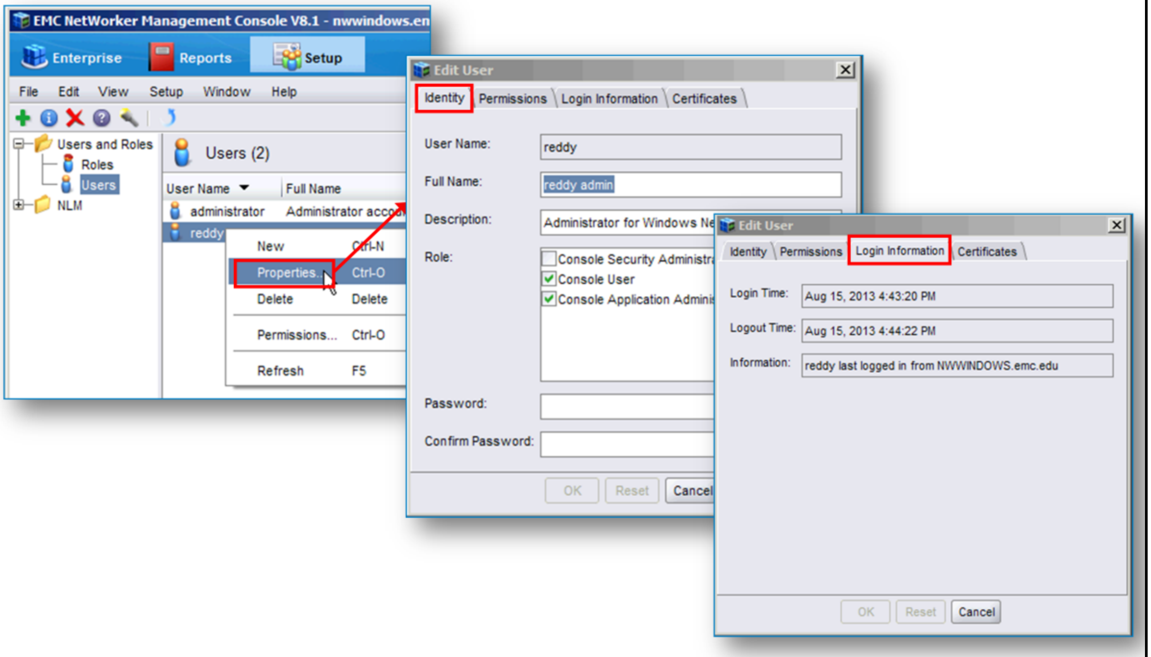
The Console server's **Setup** window is used to configure and manage user accounts. To add a new user, right-click **Users** in the left pane, then select **New**. In the **Identity** tab, enter the user name, description and password. Select the role(s) to be given to this user.

In the **Permissions** tab, select the NetWorker servers the account is allowed to view. In Console, the user can manage data, such as reports and events, only for the servers to which it is given permission. Whether or not this user account can administer a particular NetWorker server is determined by the NetWorker server's Administrator list.

A user must belong to the Console Security Administrator role to add new Console users.

All requests issued to a NetWorker server from the Console GUI come from "user=*user*, host=*console_server*". For example, if the Console server hostname is **cs1** and you are logged into a NMC account named **reddy**, the NetWorker server's Administrator list **must** contain **user=reddy,host=cs1** to allow administration privileges.

Modifying a Console User



User Name: reddy

Full Name: reddy admin

Description: Administrator for Windows Ne

Role:
☐ Console Security Administr
☑ Console User
☑ Console Application Admini

Password:

Confirm Password:

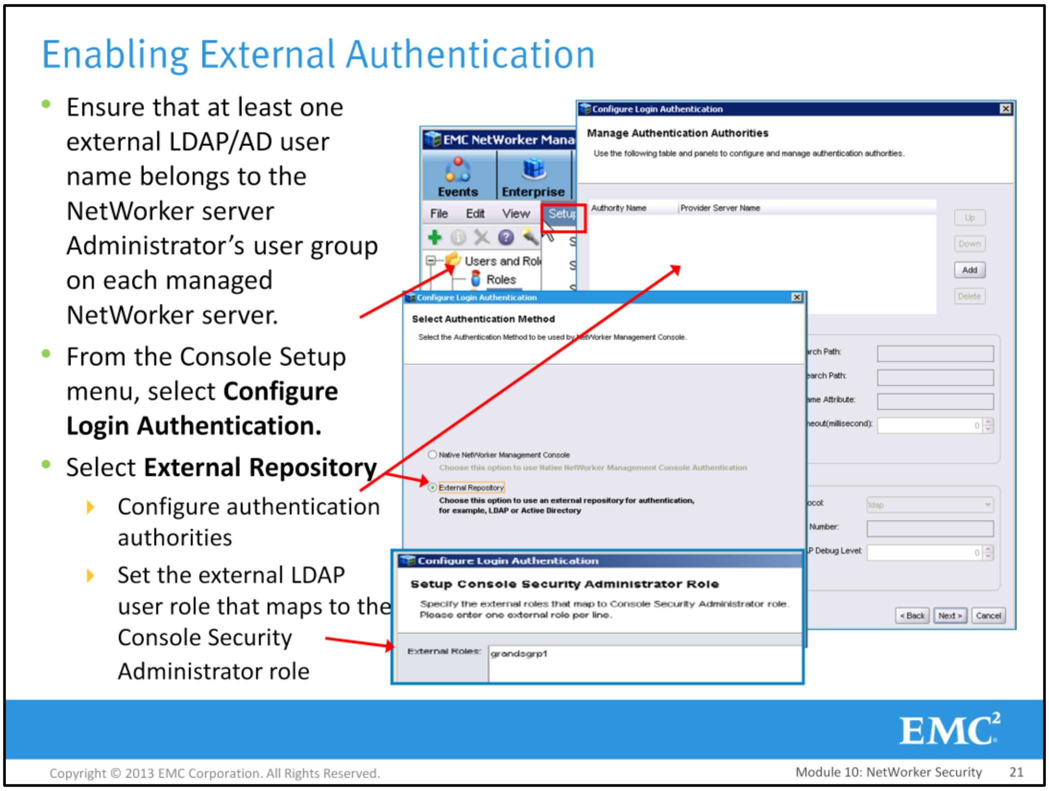
Login Time: Aug 15, 2013 4:43:20 PM

Logout Time: Aug 15, 2013 4:44:22 PM

Information: reddy last logged in from NWWINDOWS.emc.edu

You can change a user's configuration, such as an assigned role or a managed server. This is done within the **Setup** window by clicking **Users** in the left pane, right-clicking the user in the right pane, and then selecting **Properties** from the menu. In the **Identity** tab of the resulting **Edit User** window, you can change the full name, description, roles and password for the selected user. In the **Permissions** tab, you can modify the servers that the user can access. The **Login Information** tab provides details about the last user login.

Note: To assign roles and edit permissions, the user must belong to the Console Security Administrator role.



Enabling External Authentication

- Ensure that at least one external LDAP/AD user name belongs to the NetWorker server Administrator’s user group on each managed NetWorker server.
- From the Console Setup menu, select **Configure Login Authentication.**
- Select **External Repository**
  - Configure authentication authorities
  - Set the external LDAP user role that maps to the Console Security Administrator role

Configure Login Authentication

Manage Authentication Authorities

Use the following table and panels to configure and manage authentication authorities.

Authority Name	Provider Server Name

Configure Login Authentication

Select Authentication Method

Select the Authentication Method to be used by NetWorker Management Console.

○ Native NetWorker Management Console

Choose this option to use Native NetWorker Management Console Authentication

● External Repository

Choose this option to use an external repository for authentication, for example, LDAP or Active Directory

Configure Login Authentication

Setup Console Security Administrator Role

Specify the external roles that map to Console Security Administrator role. Please enter one external role per line.

External Roles: grandsgrp1

Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 21

To enable external authentication:

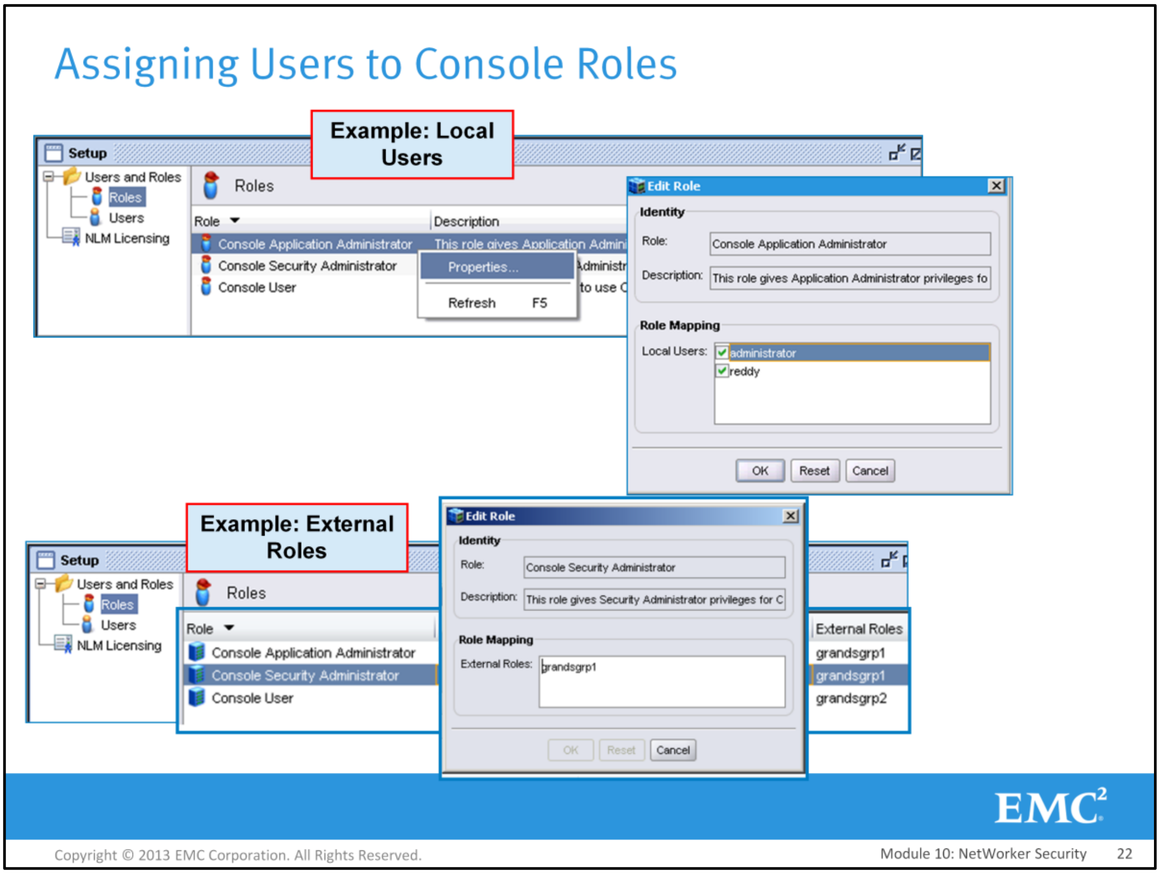
First, ensure that at least one external LDAP user name belongs to the NetWorker server Administrator’s user group on each managed NetWorker server.

Next, select **Configure Login Authentication** from the **Console Setup** window, **Setup** menu. Enter information about your authentication authority on the **Manage Authentication Authorities** window. Then, in the **Setup Console Security Administrator Role** window, enter the LDAP user roles or user names that will be mapped to the Console Security Administrator role. The LDAP user that was added to the NetWorker server Administrator’s list must be added to the Console Security Administrator role. After restarting Console, you can log in to the Console server using an LDAP user name and password belonging to the mapped LDAP role.

<u>Note</u>: A user must belong to the Console Security Administrator role to perform this function.

In LDAP mode, the user name Administrator is not allowed to log in even if it is defined in LDAP.

When using LDAP authentication, when a user logs in for the first time, a user object is automatically created on the Console server. You can also create user objects before users log in for the first time. Enter the LDAP user name and full name. In the ***Permissions*** tab, select the hosts that the user can manage.



Assigning Users to Console Roles

Example: Local Users

Edit Role

Identity

Role: Console Application Administrator

Description: This role gives Application Administrator privileges fo

Role Mapping

Local Users: ☑ administrator ☑ reddy

Example: External Roles

Edit Role

Identity

Role: Console Security Administrator

Description: This role gives Security Administrator privileges for C

Role Mapping

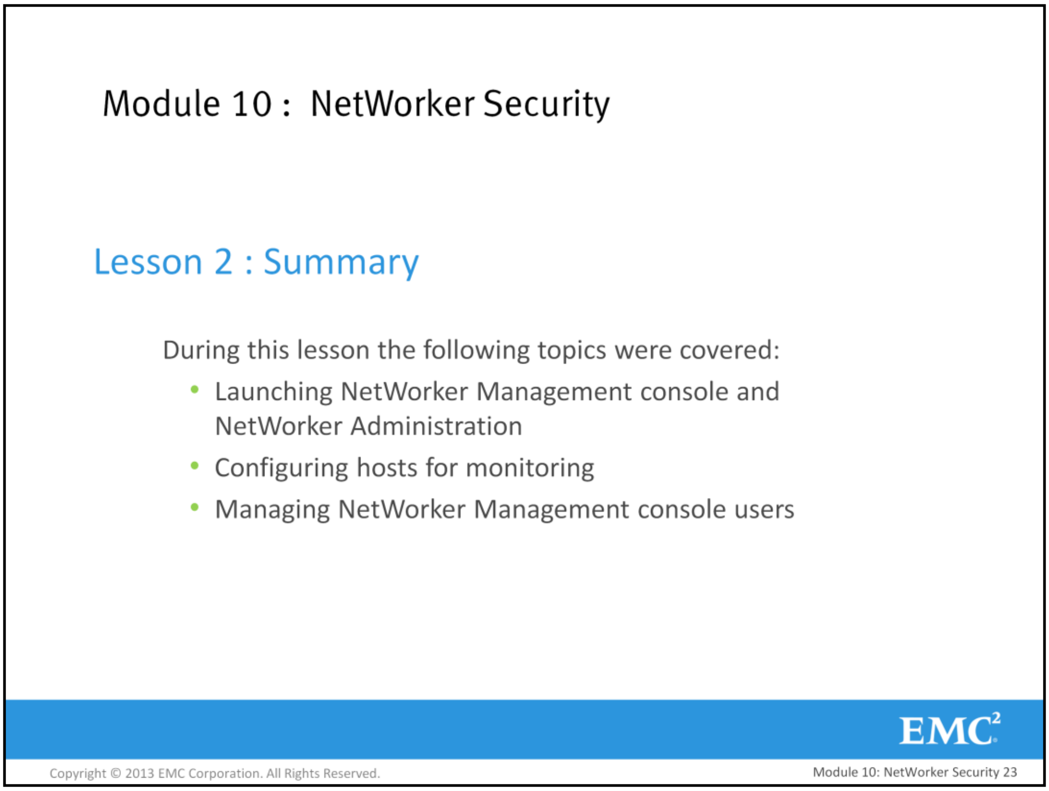
External Roles: grandsgrp1

Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 22

To map users (both local and external) to a Console server role, click **Roles** in the left pane of the **Setup** window and then right-click the role in the right pane. Then, select **Properties** from the menu. In the **Edit Role** window, select the users that map to the role.

Note: To assign roles, the user must belong to the Console Security Administrator role.



Module 10 : NetWorker Security

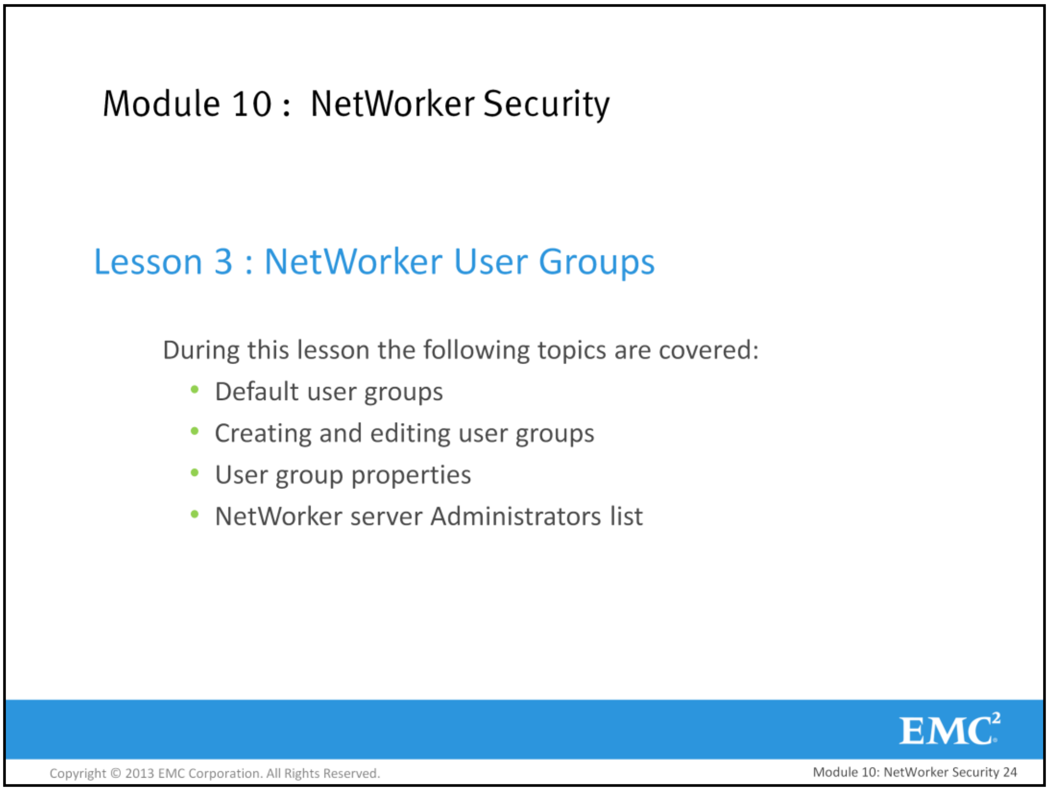
Lesson 2 : Summary

During this lesson the following topics were covered:

- Launching NetWorker Management console and NetWorker Administration
- Configuring hosts for monitoring
- Managing NetWorker Management console users

EMC²

This lesson covered how to launch the NetWorker administration GUI interfaces, configure hosts in NMC and configure NetWorker Management console users.



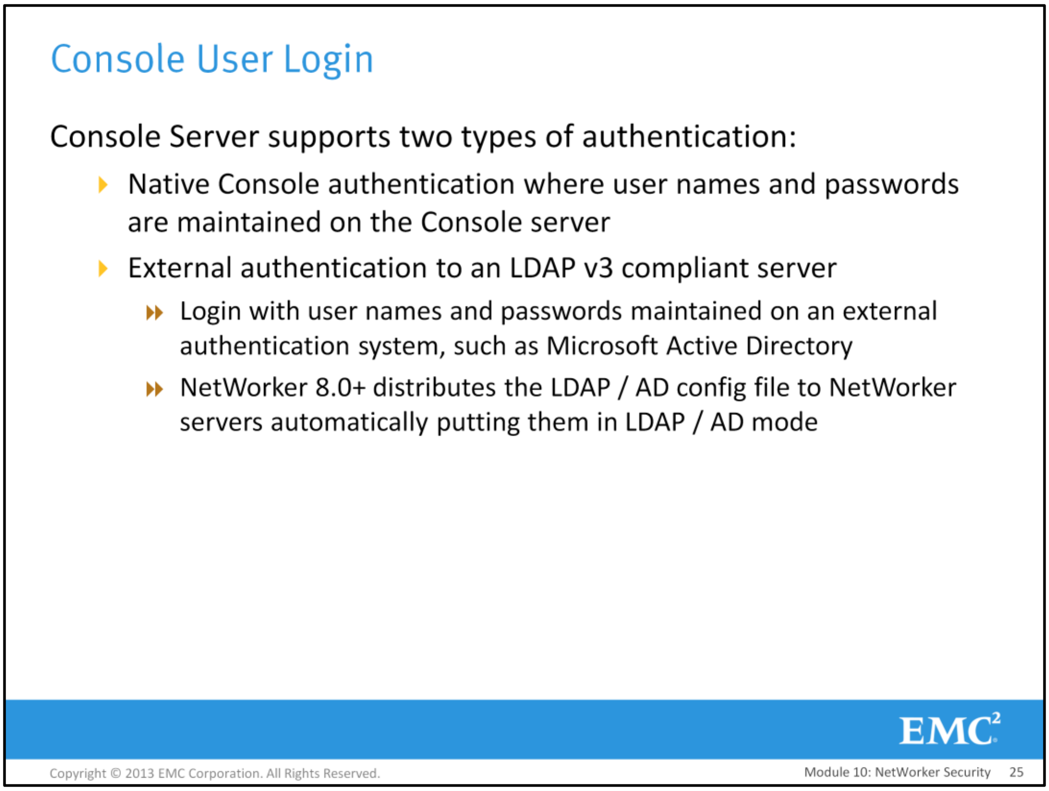
Module 10 : NetWorker Security

Lesson 3 : NetWorker User Groups

During this lesson the following topics are covered:

- Default user groups
- Creating and editing user groups
- User group properties
- NetWorker server Administrators list

This lesson covers user groups within a NetWorker environment. Specific topics include a review of the default, built-in user groups, creating and editing user groups, and user group properties. Finally, the NetWorker server Administrators list is covered.



Console User Login

Console Server supports two types of authentication:

- Native Console authentication where user names and passwords are maintained on the Console server
- External authentication to an LDAP v3 compliant server
  - Login with user names and passwords maintained on an external authentication system, such as Microsoft Active Directory
  - NetWorker 8.0+ distributes the LDAP / AD config file to NetWorker servers automatically putting them in LDAP / AD mode

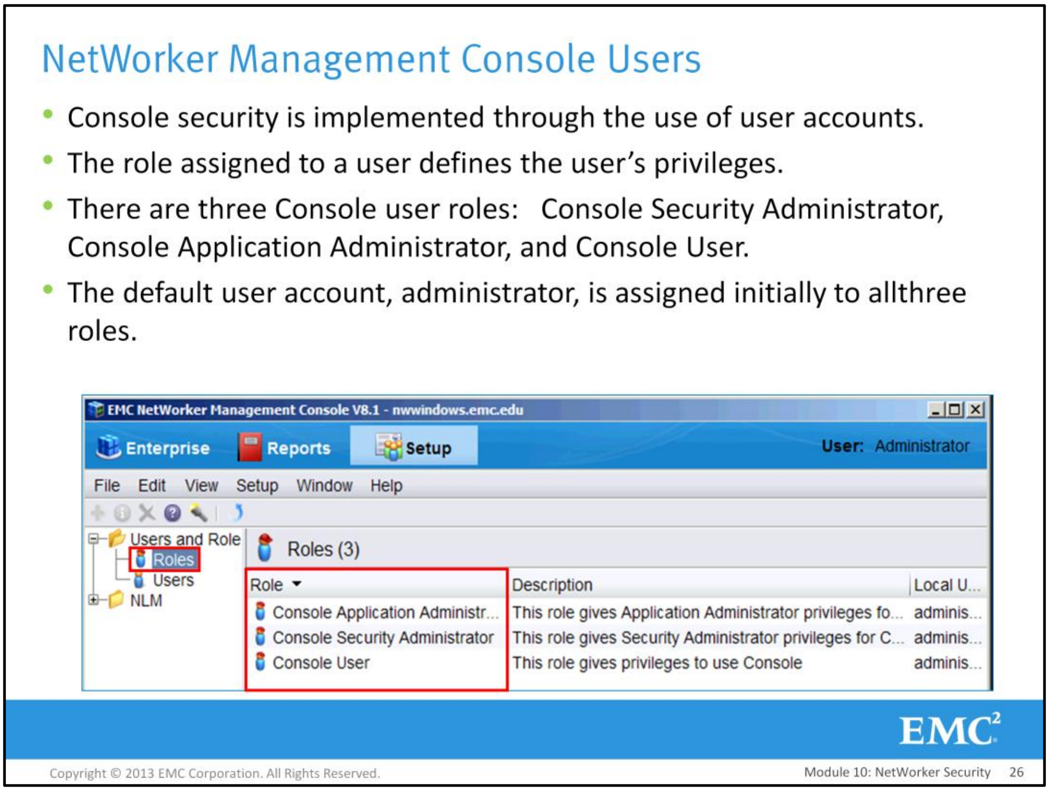
Access to NetWorker Console functionality is implemented through the use of user accounts. The role assigned to a user account determines the tasks the user can perform in Console. The roles cannot be deleted and the privileges of each role cannot be changed.

Authentication is a user name/password system that is used to grant user access to the NetWorker Management Console server. Console can leverage an external repository such as LDAP or Microsoft Active Directory in addition to its own internal authentication system.

With native Console authentication, user names and passwords are maintained on the Console server. Native NetWorker Management Console authentication is enabled by default.

With external authentication, user names and passwords are maintained and authenticated by an external LDAP v3 compliant server. When configured for external LDAP login authentication, console login is controlled by mapping LDAP user roles and user names to console user roles.

With NetWorker version 8.0 software or higher, NetWorker automatically distributes the LDAP or AD configuration file from the Console server to the NetWorker servers that are managed by the Console server. This automatically puts the NetWorker servers in LDAP or AD mode.



NetWorker Management Console Users

- Console security is implemented through the use of user accounts.
- The role assigned to a user defines the user's privileges.
- There are three Console user roles: Console Security Administrator, Console Application Administrator, and Console User.
- The default user account, administrator, is assigned initially to allthree roles.

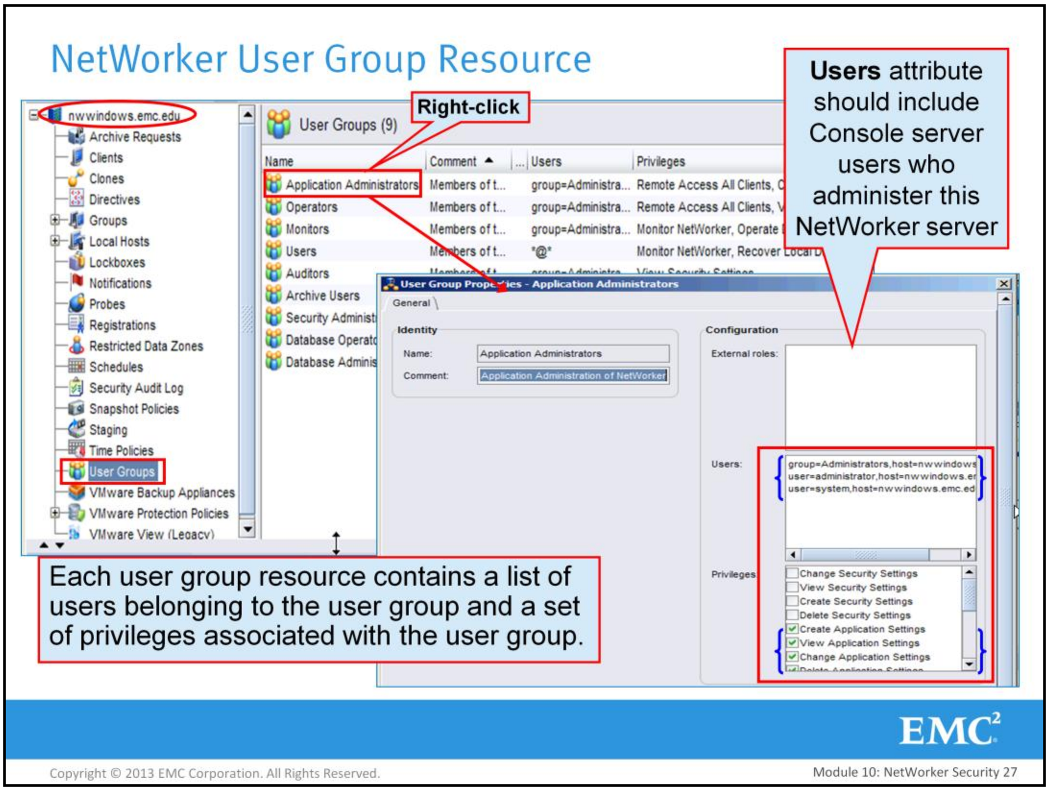
Role	Description	Local U...
Console Application Administr...	This role gives Application Administrator privileges fo...	adminis...
Console Security Administrator	This role gives Security Administrator privileges for C...	adminis...
Console User	This role gives privileges to use Console	adminis...

Access to NetWorker Console functionality is implemented through the use of user accounts. The role assigned to a user account determines the tasks the user can perform in Console. The roles cannot be deleted and the privileges of each role cannot be changed.

There are three Console user roles: Console Security Administrator, Console Application Administrator, and Console User. When Console is first launched, the default user account, administrator, is assigned to all three Console user roles.

User Role	Privileges
Console Security Administrator	•Add, delete, and edit users •Configure login authentication •Control user access to managed applications •All tasks available to Console User
Console Application Administrator	•Configure Console system options •Set retention policies for reports •View custom reports •Specify the NetWorker server to backup the Console database •Specify a NetWorker License Manager server •Run the Console Configuration wizard •All tasks available to Console User
Console User	All tasks except for those tasks explicitly mentioned for the Console Security Administrator and the Console Application Administrator.

NetWorker User Group Resource



Right-click

Name	Comment	Users	Privileges
Application Administrators	Members of t...	group=Administra...	Remote Access All Clients, C
Operators	Members of t...	group=Administra...	Remote Access All Clients, V
Monitors	Members of t...	group=Administra...	Monitor NetWorker, Operate
Users	Members of t...	*@*	Monitor NetWorker, Recover Local D
Auditors	Members of t...	group=Administra...	View Security Settings
Archive Users			
Security Administ			
Database Operato			
Database Adminis			

Users attribute should include Console server users who administer this NetWorker server

User Group Properties - Application Administrators

Identity

Name: Application Administrators

Comment: Application Administration of NetWorker

Configuration

External roles:

Users:
group=Administrators,host=nwwindows
user=administrator,host=nwwindows.er
user=system,host=nwwindows.emc.ed

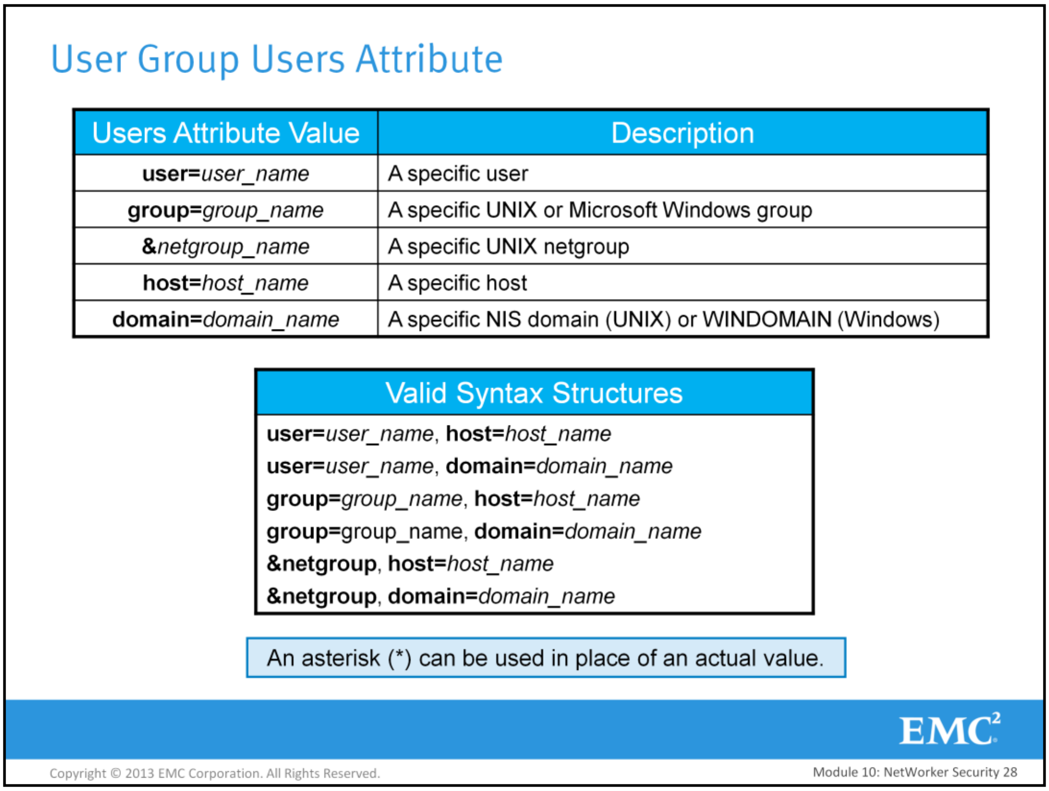
Privileges:
□ Change Security Settings
□ View Security Settings
□ Create Security Settings
□ Delete Security Settings
☑ Create Application Settings
☑ View Application Settings
☑ Change Application Settings
☑ Delete Application Settings

Each user group resource contains a list of users belonging to the user group and a set of privileges associated with the user group.

Module 10: NetWorker Security 27

NetWorker server security is implemented through the use **Role-based authorization** implemented through the use of user groups. When NetWorker is installed, there are nine preconfigured user groups that users can be assigned to based on their administrative role.

Each user group has a specific set of privileges associated with it, defined by the **Privileges** attribute. Specific users or sets of users are associated with a user group via the **Users** attribute. The syntax of an entry in the **Users** attribute can take one of several forms, which are discussed on the following page.



User Group Users Attribute

Users Attribute Value	Description
user=*user_name*	A specific user
group=*group_name*	A specific UNIX or Microsoft Windows group
&*netgroup_name*	A specific UNIX netgroup
host=*host_name*	A specific host
domain=*domain_name*	A specific NIS domain (UNIX) or WINDOMAIN (Windows)

Valid Syntax Structures
user=*user_name*, **host=***host_name*
user=*user_name*, **domain=***domain_name*
group=*group_name*, **host=***host_name*
group=group_name, **domain=***domain_name*
&netgroup, **host=***host_name*
&netgroup, **domain=***domain_name*

An asterisk (*) can be used in place of an actual value.

Module 10: NetWorker Security 28

Assigning a user or group of users to a user group is accomplished by entering pairs of *name=value* entries in the **Users** attribute. Here are some possible examples:

- A user with the name of **sally**, logged into the host named **astro1**.

  ```
  user=sally, host=astro1
  ```

- All users on the host named **astro1**.

  ```
  user=*, host=astro1
  ```

- A user with the name of **sally**, logged in on any host.

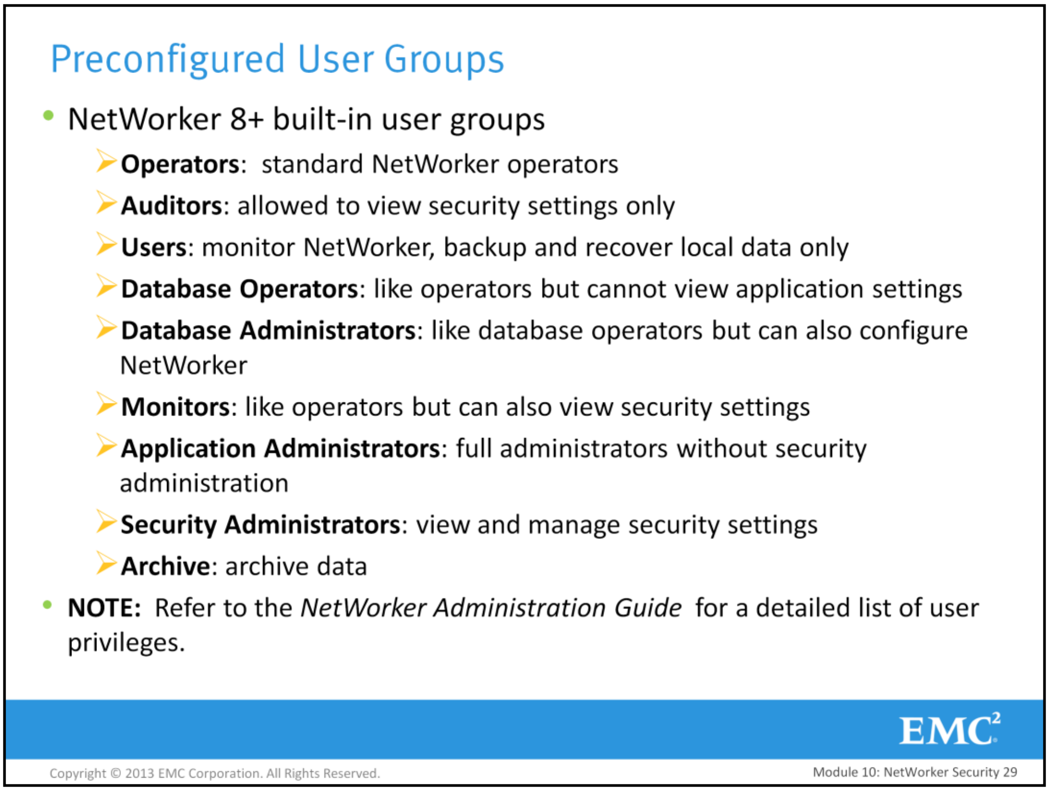
  ```
  user=sally, host=*
  ```

- Any user belonging to the **Administrators** group in the WINDOMAIN **finance.com**.

  ```
  group=Administrators, domain=finance.com
  ```

The set of syntaxes shown in the slide is not an exhaustive list. The syntax “*@*” is also valid but is discouraged because it can be ambiguous. For example, if there is a user named **bubba** and a group named **bubba**, `bubba@*` would include both the user and all members of the group. See the *EMC NetWorker Administration Guide* for a more complete description of the syntax.

Note: When used as a value, an asterisk (*) means all possible values.



Preconfigured User Groups

- NetWorker 8+ built-in user groups
  - **Operators**: standard NetWorker operators
  - **Auditors**: allowed to view security settings only
  - **Users**: monitor NetWorker, backup and recover local data only
  - **Database Operators**: like operators but cannot view application settings
  - **Database Administrators**: like database operators but can also configure NetWorker
  - **Monitors**: like operators but can also view security settings
  - **Application Administrators**: full administrators without security administration
  - **Security Administrators**: view and manage security settings
  - **Archive**: archive data
- **NOTE:** Refer to the *NetWorker Administration Guide* for a detailed list of user privileges.

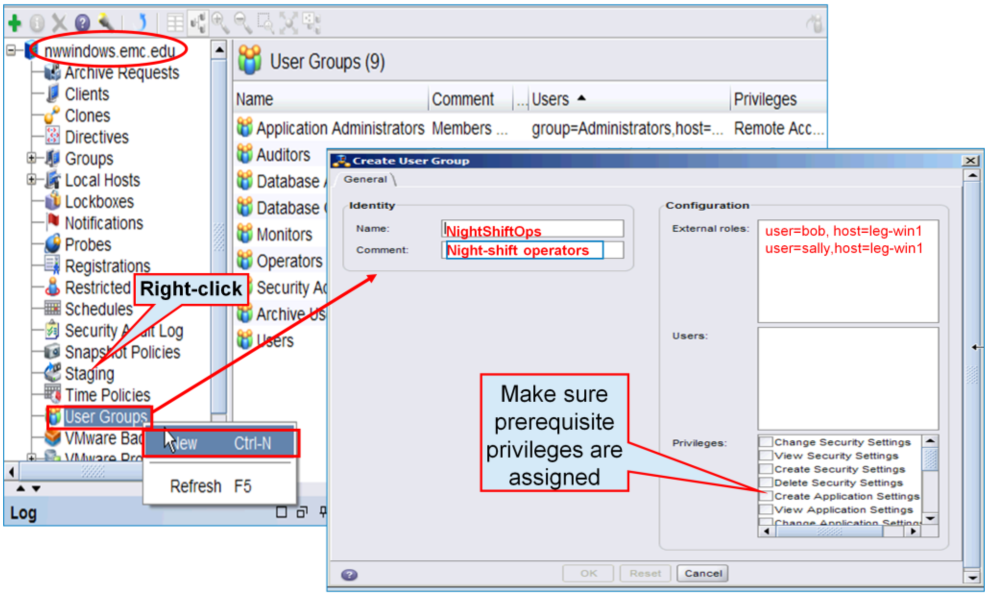
Module 10: NetWorker Security 29

User groups provide the ability to assign a group of NMC, LDAP, and AD users with a defined set of privileges to perform NetWorker operations. NetWorker provides the preconfigured user groups listed on the slide. The preconfigured user groups cannot be deleted. Additional groups, however, can be created by the administrator to meet the needs of the environment.

Prior to the NetWorker 8.0 software, a single Administrators group was created. Modifications to the users in the Administrators user group were automatically reflected in the **Administrator** attribute of the server resource. In NetWorker 8.0 and later, the Administrator user group is replaced by three new administrator user groups and user group membership changes are not reflected in the Administrator attribute of the server resource.

For a detailed description of all user privileges that can be assigned to a user group within NetWorker, refer to the *EMC NetWorker Administration Guide.*

Creating a New User Group Resource



Right-click

User Groups (9)

Name	Comment	Users	Privileges
Application Administrators	Members ...	group=Administrators,host=...	Remote Acc...
Auditors			
Database /			
Database (			
Monitors			
Operators			
Security Ac			
Archive Us			
Users			

Create User Group

General

Identity

Name: NightShiftOps

Comment: Night-shift operators

Configuration

External roles: user=bob, host=leg-win1
user=sally,host=leg-win1

Users:

Privileges:
- □ Change Security Settings
- □ View Security Settings
- □ Create Security Settings
- □ Delete Security Settings
- □ Create Application Settings
- □ View Application Settings
- □ Change Application Settings

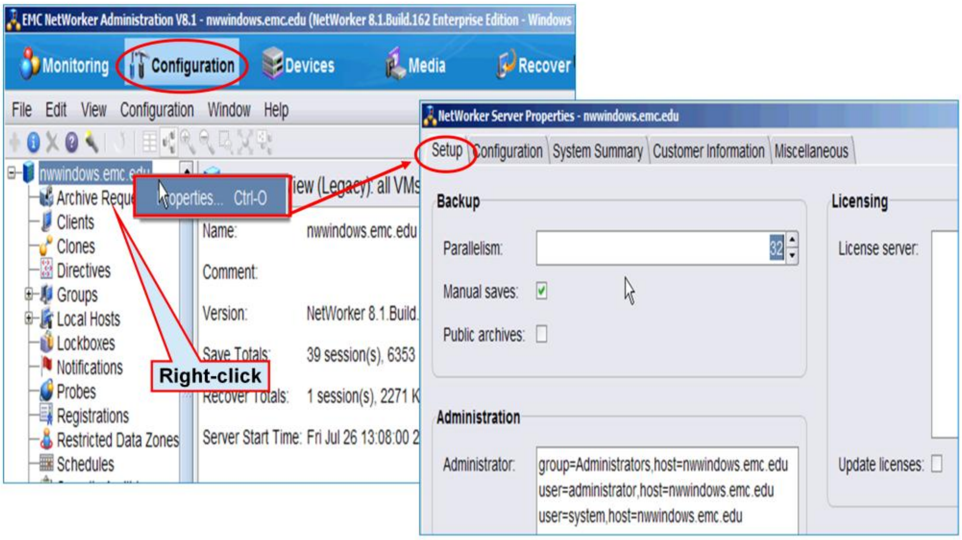
Make sure prerequisite privileges are assigned

Module 10: NetWorker Security 30

As mentioned previously, additional user groups can be created as needed. This is convenient if there are specific users that you would like to assign specific NetWorker duties to but do not fit into the predefined categories.

Since administration of NetWorker is performed using the Management Console, a user assigned to a user group will almost always be a Console user. In the example in the slide, **bob** and **sally** are accounts created within the Console server, nwserver.emc.edu. Creation of Console user accounts is discussed in the module, *Administering the NetWorker Management Console Server*.

NetWorker Server Administrator List



Name: nwwindows.emc.edu

Comment:

Version: NetWorker 8.1.Build.

Save Totals: 39 session(s), 6353

Recover Totals: 1 session(s), 2271 K

Server Start Time: Fri Jul 26 13:08:00 2

Parallelism: 32

Manual saves: ☑

Public archives: □

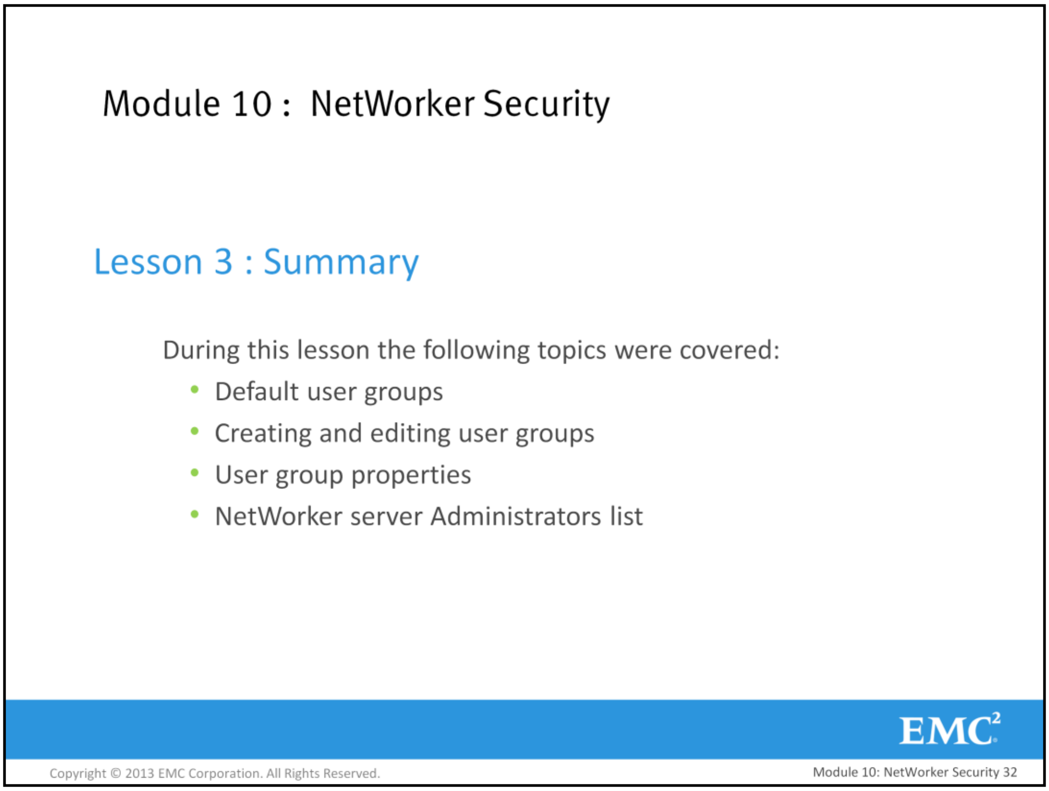
License server:

Update licenses: □

Administrator: group=Administrators,host=nwwindows.emc.edu
user=administrator,host=nwwindows.emc.edu
user=system,host=nwwindows.emc.edu

Module 10: NetWorker Security 31

Administrators is an attribute in the NSR (server) resource which contains a list of users or groups that are allowed to add, delete, and update all NetWorker resources. From NetWorker 8.0 on, the users no longer map to the administrator's NetWorker user group, as was the case in previous versions of NetWorker.



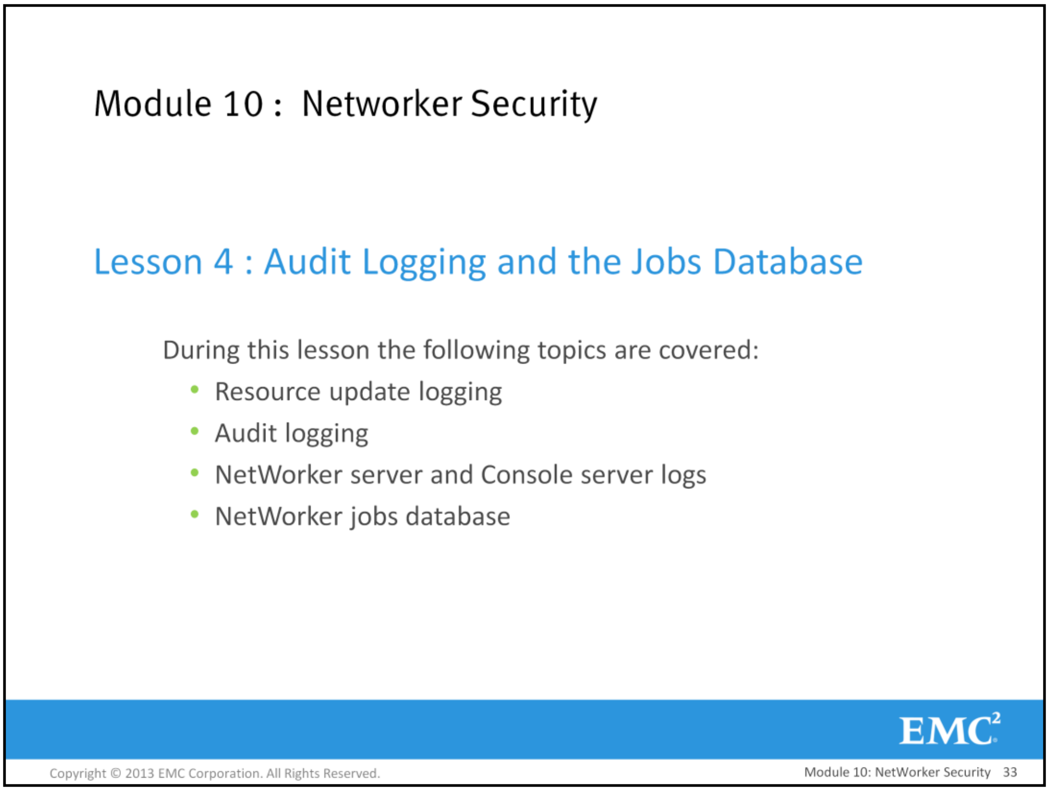
Module 10 : NetWorker Security

Lesson 3 : Summary

During this lesson the following topics were covered:

- Default user groups
- Creating and editing user groups
- User group properties
- NetWorker server Administrators list

This lesson covered user groups within a NetWorker environment. Specific topics include a review of the default, built-in user groups, creating and editing user groups, and user group properties. Finally, the NetWorker server Administrators list is covered.



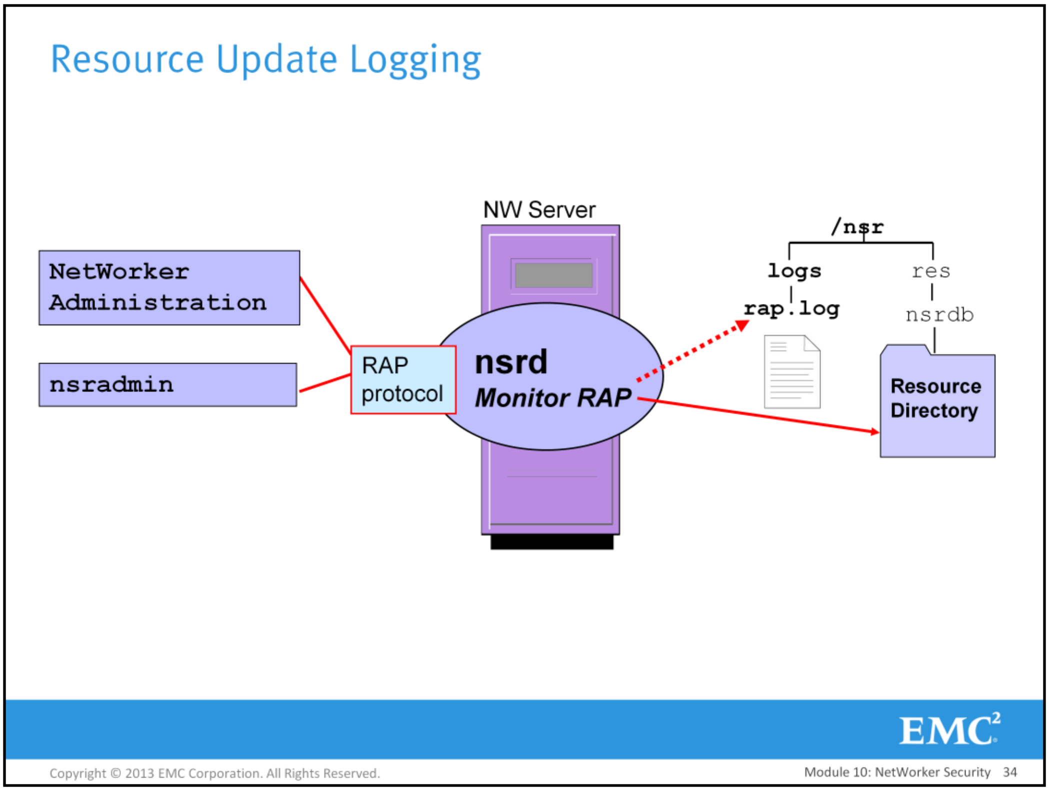
Module 10 : Networker Security

Lesson 4 : Audit Logging and the Jobs Database

During this lesson the following topics are covered:

- Resource update logging
- Audit logging
- NetWorker server and Console server logs
- NetWorker jobs database

This lesson discusses the NetWorker jobs database, resource update logging and audit logging capabilities.



Resource Update Logging

NetWorker Administration

nsradmin

RAP protocol

NW Server

nsrd

Monitor RAP

/nsr

logs

rap.log

res

nsrdb

Resource Directory

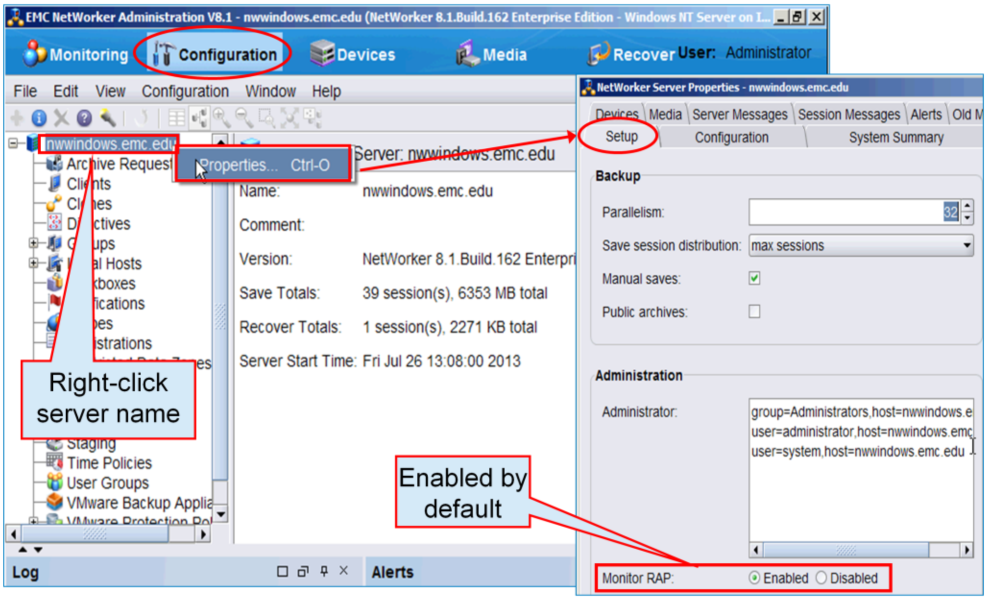
EMC²

Resource update logging is enabled/disabled by setting the **Monitor RAP** attribute of the Server (NSR) resource. By default it is **Enabled**.

`nsrd` is responsible for managing all NetWorker server resources. Resource information is transmitted via the Resource Administration Platform (RAP) protocol between `nsrd` and the NetWorker Administration GUI and `nsradmin` administrative interfaces .

Note: There are several NetWorker client resources, such as NSR Port Range, that are managed by `nsrexecd` and therefore excluded from the resource update logging feature. These resources are maintained in the directory `/nsr/res/nsrladb`, which exists on all NetWorker clients.

Enabling Resource Update Logging



EMC NetWorker Administration V8.1 - nwwindows.emc.edu (NetWorker 8.1.Build.162 Enterprise Edition - Windows NT Server on I...

User: Administrator

Server: nwwindows.emc.edu

Name: nwwindows.emc.edu

Comment:

Version: NetWorker 8.1.Build.162 Enterpri

Save Totals: 39 session(s), 6353 MB total

Recover Totals: 1 session(s), 2271 KB total

Server Start Time: Fri Jul 26 13:08:00 2013

NetWorker Server Properties - nwwindows.emc.edu

Backup

Parallelism: 32

Save session distribution: max sessions

Manual saves: ☑

Public archives: □

Administration

Administrator:
group=Administrators,host=nwwindows.e
user=administrator,host=nwwindows.emc
user=system,host=nwwindows.emc.edu

Monitor RAP: ● Enabled ○ Disabled

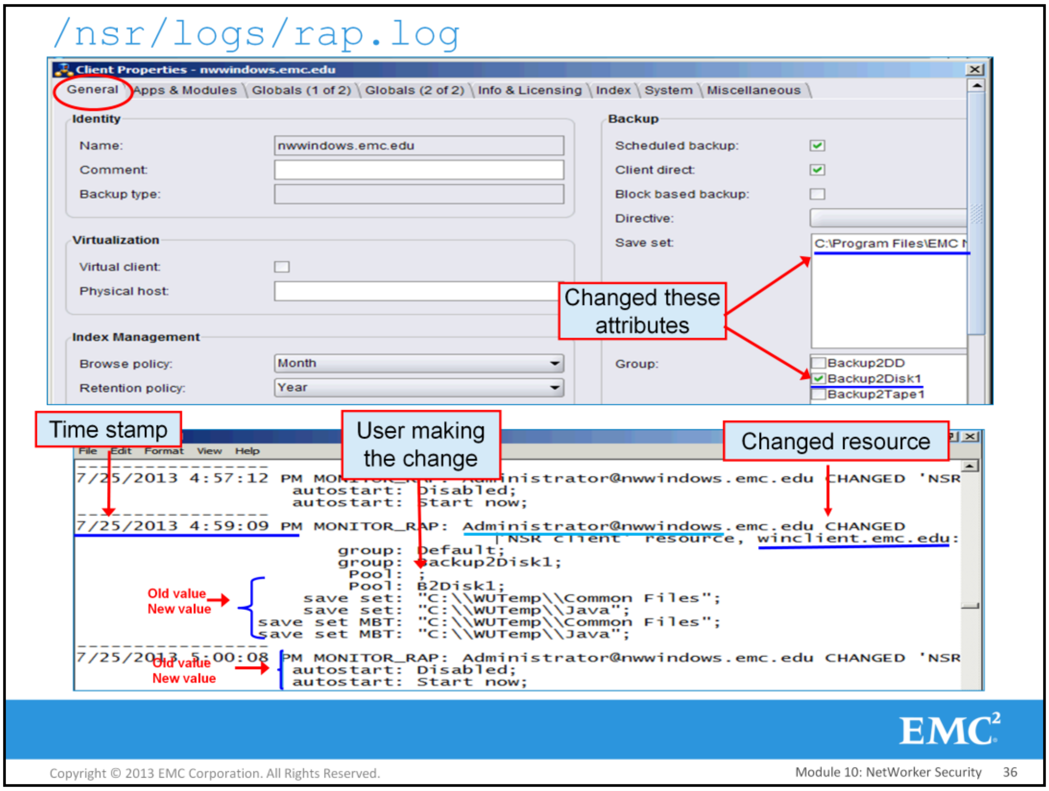
Right-click server name

Enabled by default

EMC²

The NetWorker server resource contains the **Monitor RAP** attribute used to enable or disable the resource update logging feature. The default value of the attribute is **Enabled**.

Note: This attribute is hidden by default. To display the **Monitor RAP** attribute, enable diagnostic mode (**View > Diagnostic Mode**).



/nsr/logs/rap.log

Client Properties - nwwindows.emc.edu

General | Apps & Modules | Globals (1 of 2) | Globals (2 of 2) | Info & Licensing | Index | System | Miscellaneous

Identity

Name: nwwindows.emc.edu

Comment:

Backup type:

Virtualization

Virtual client: □

Physical host:

Index Management

Browse policy: Month

Retention policy: Year

Backup

Scheduled backup: ☑

Client direct: ☑

Block based backup: □

Directive:

Save set: C:\Program Files\EMC N

Group: □ Backup2DD
☑ Backup2Disk1
□ Backup2Tape1

```
-------------------
7/25/2013 4:57:12 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR
                     autostart: Disabled;
                     autostart: Start now;
-------------------
7/25/2013 4:59:09 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED
                                  'NSR client' resource, winclient.emc.edu:
                         group: Default;
                         group: Backup2Disk1;
                          Pool: ;
                          Pool: B2Disk1;
                      save set: "C:\\WUTemp\\Common Files";
                      save set: "C:\\WUTemp\\Java";
                  save set MBT: "C:\\WUTemp\\Common Files";
                  save set MBT: "C:\\WUTemp\\Java";
-------------------
7/25/2013 5:00:08 PM MONITOR_RAP: Administrator@nwwindows.emc.edu CHANGED 'NSR
                     autostart: Disabled;
                     autostart: Start now;
```

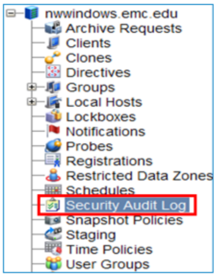
Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 36

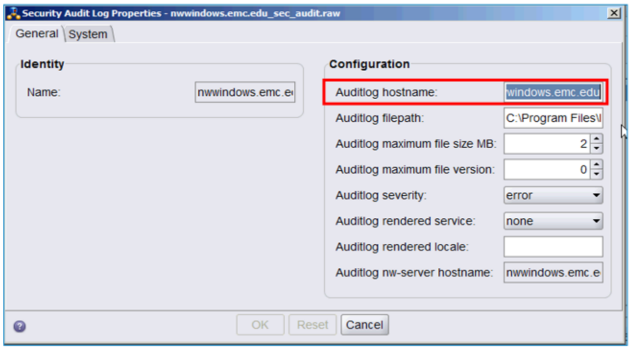
`/nsr/logs/rap.log` is a text file on the NetWorker server and contains an entry for each resource change (creation/deletion/modification) made on the NetWorker server. For each resource modification, there are three or more lines of information written to the file.

Line	Content
Line 1	A string of hyphens (----------). This is used to separate log entries.
Line 2	A time stamp of when the change was made. The string "MONITOR_RAP:" is followed by the *user@host* performing the change. CHANGED, CREATED, or DELETED specifies what action was performed and is followed by the NSR resource type that was affected.
Remaining lines	The details of the modification. If the type of action is CHANGED, the old value is displayed followed by the new value. If the action is CREATED or DELETED, all the resource's attributes and attribute values are displayed.

NetWorker Audit Log



- Audit Log enhancements
  - Property of every NW client, storage node, server
    - Must be configured on per-client bases
  - Modifiable only by the security or full admin
  - Not a replacement for RAP log
  - Auditable security events
    - Authentication attempts, Privilege checks, Resource creation/deletion
    - Can control verbosity
  - Audit log does not have to be on NW server, it can be on a secure system
    - System must have NW client installed
  - Multiple systems can send data to the same audit log server
    - Example: all clients within a datazone can log to the same system



Security Audit Log Properties - nwwindows.emc.edu_sec_audit.raw

Identity

Name: nwwindows.emc.e

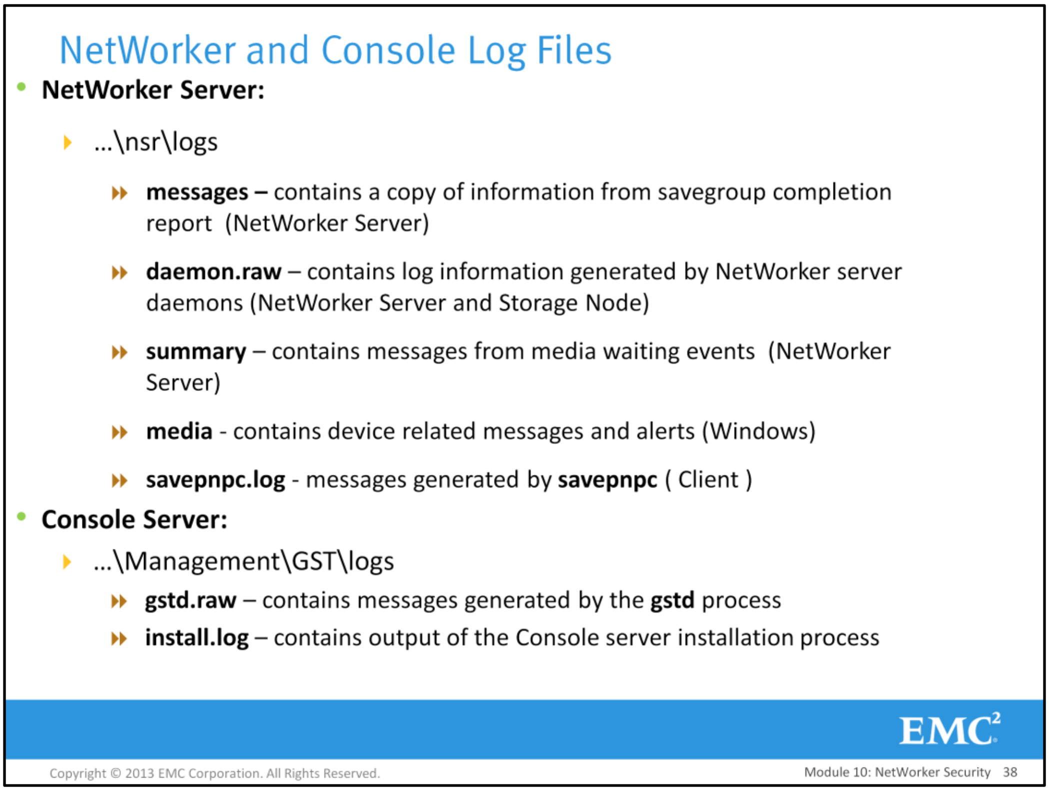
Configuration

Auditlog hostname: windows.emc.edu
Auditlog filepath: C:\Program Files\
Auditlog maximum file size MB: 2
Auditlog maximum file version: 0
Auditlog severity: error
Auditlog rendered service: none
Auditlog rendered locale:
Auditlog nw-server hostname: nwwindows.emc.e

EMC²

NetWorker 8 introduced the audit log property setting for every NetWorker client, storage node, and server, and must be configured on a per client basis. It is modifiable only by security or full administrator.

The audit log is not a replacement for the RAP log and does not have to necessarily be located on the NetWorker server. It can be on a separate secure system but the secure system must have the NetWorker client installed. Multiple systems can send their audit data to the same audit log server.



NetWorker and Console Log Files

- **NetWorker Server:**
  - ...\nsr\logs
    - **messages –** contains a copy of information from savegroup completion report (NetWorker Server)
    - **daemon.raw** – contains log information generated by NetWorker server daemons (NetWorker Server and Storage Node)
    - **summary** – contains messages from media waiting events (NetWorker Server)
    - **media** - contains device related messages and alerts (Windows)
    - **savepnpc.log** - messages generated by **savepnpc** (Client)
- **Console Server:**
  - ...\Management\GST\logs
    - **gstd.raw** – contains messages generated by the **gstd** process
    - **install.log** – contains output of the Console server installation process

Module 10: NetWorker Security 38

Logs for NetWorker server operations are located in …`\nsr\logs` on the NetWorker server and include:

messages : Primarily contains a copy of the information contained in savegroup completion reports.

daemon.raw : Contains log information generated by all the NetWorker server daemons as well as some messages generated by running `nsrck` and `savegrp`. This log is the most useful for performing troubleshooting tasks.

summary : Contains messages from media waiting events such as tape mount requests.

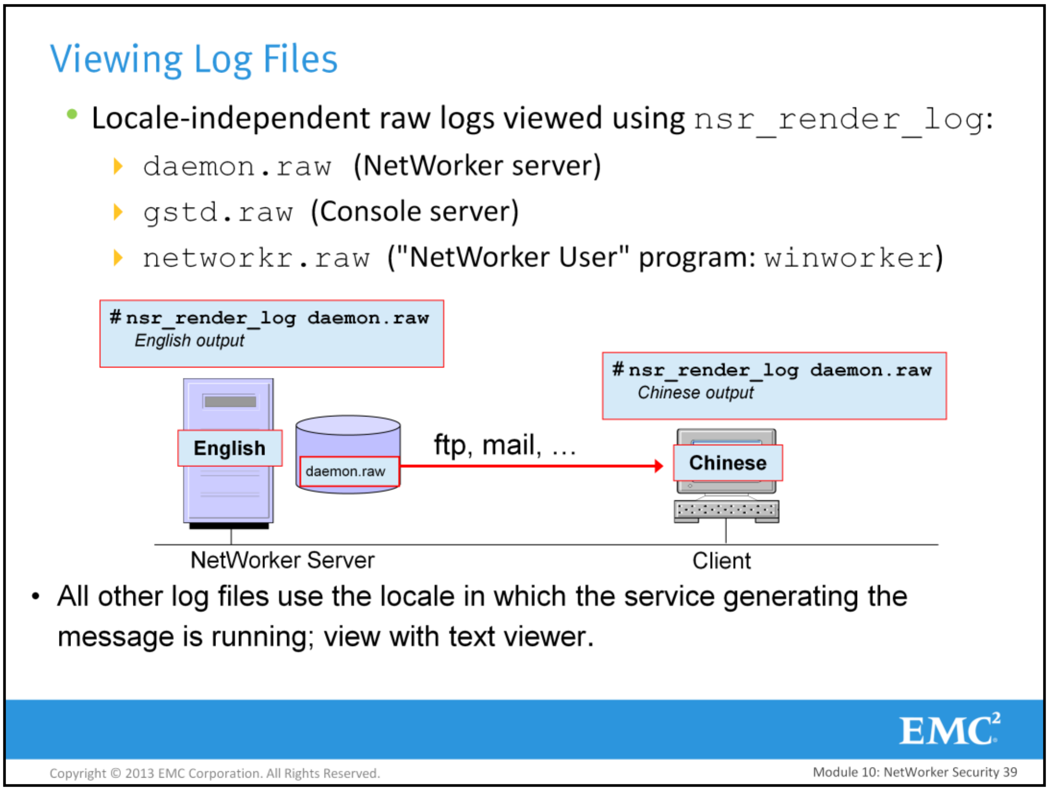
Media : Contains device-related messages such as file system full (AFTD) and cleaning notices

savepnpc : Contains messages generated by `savepnpc`.

Logs for the NetWorker Management Console server are located in …`\Management\GST\logs` and include:

gstd.raw: Contains messages generated by the `gstd` process.

install.log : Contains output of the NetWorker Management Console installation process. One or more installation log files are created when the Console software is installed. These logs are useful for troubleshooting a problem with the Console software and for tracking decisions made during installation, such as the HTTP service port chosen for the web interface.



Viewing Log Files

- Locale-independent raw logs viewed using `nsr_render_log`:
  - `daemon.raw` (NetWorker server)
  - `gstd.raw` (Console server)
  - `networkr.raw` ("NetWorker User" program: `winworker`)

```
# nsr_render_log daemon.raw
```

English output

```
# nsr_render_log daemon.raw
```

Chinese output

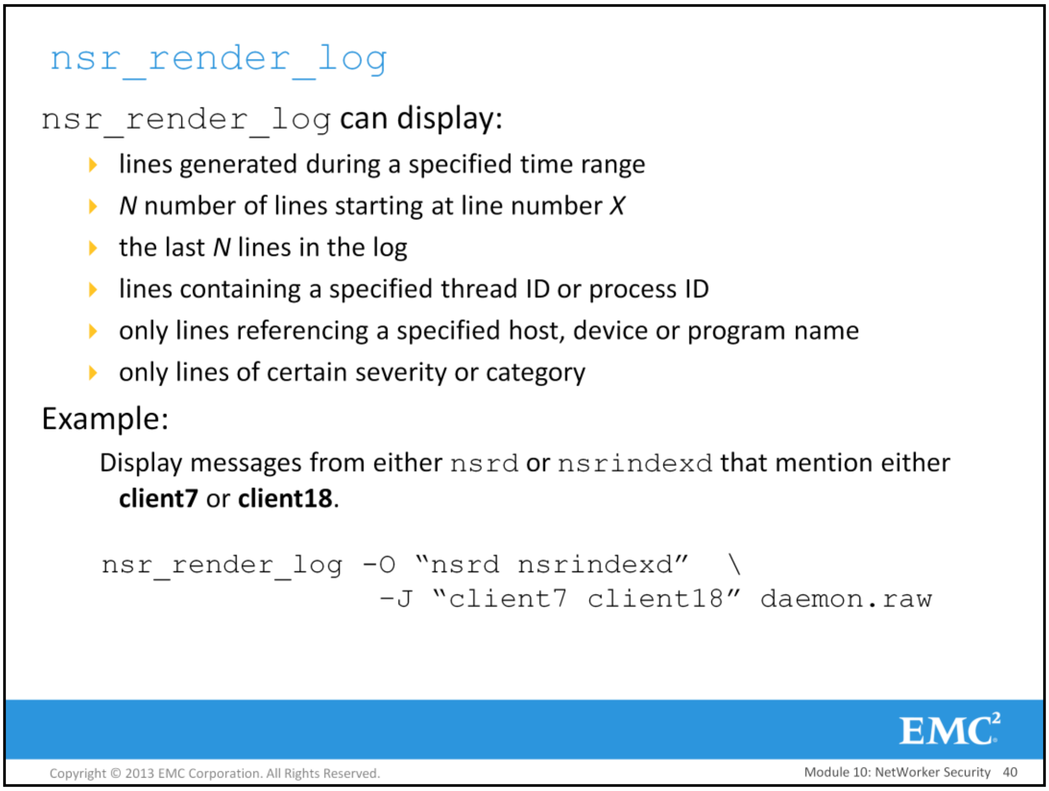
- All other log files use the locale in which the service generating the message is running; view with text viewer.

Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 39

Several NetWorker log files, identified with the `.raw` extension, are written in tokenized format. The list of files is shown in the slide. The tokens are the same regardless of the locale of the host. When viewing these locale-independent raw logs using the `nsr_render_log` command, the tokens are *rendered* using the locale of the current host. Thus, a log file viewed on an English system will display English text. If the same file is viewed, for example, on a host in the Chinese locale, Chinese output is displayed.

All other log files, as well as messages displayed in the NetWorker Console, use the locale in which the service that is generating the log messages is running. Use a text viewer to view the content of these logs.



nsr_render_log

`nsr_render_log` can display:

- lines generated during a specified time range
- *N* number of lines starting at line number *X*
- the last *N* lines in the log
- lines containing a specified thread ID or process ID
- only lines referencing a specified host, device or program name
- only lines of certain severity or category

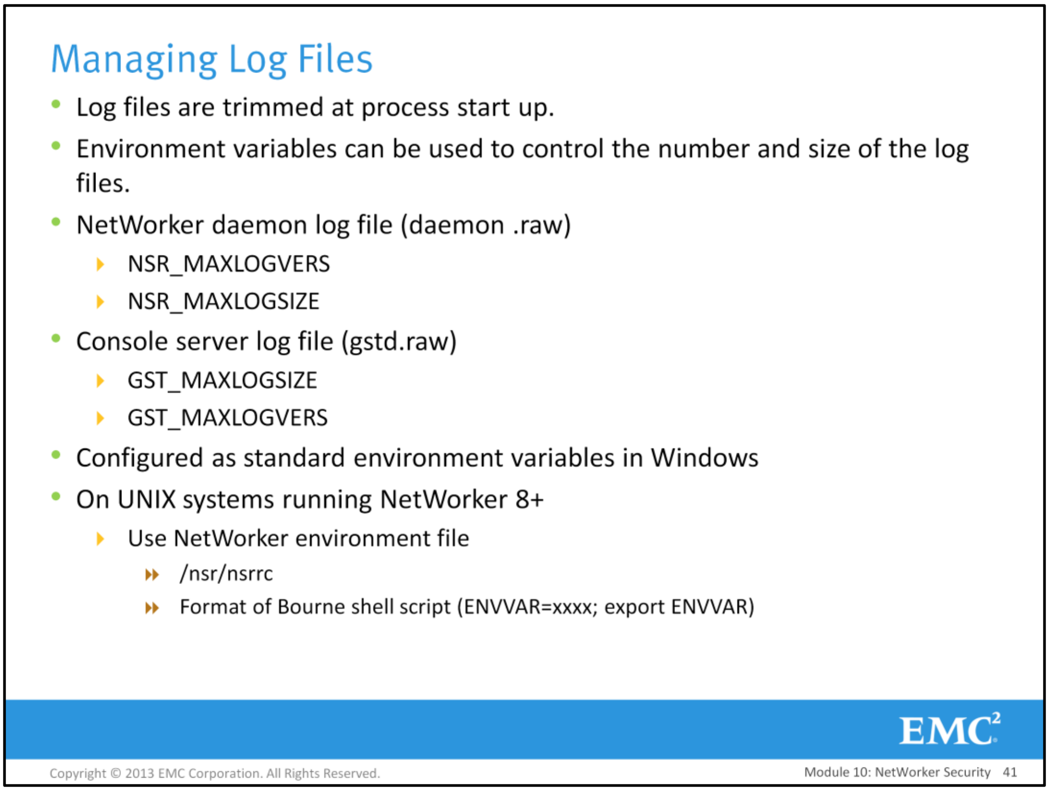
Example:

Display messages from either `nsrd` or `nsrindexd` that mention either **client7** or **client18**.

```
nsr_render_log -O “nsrd nsrindexd”  \
                -J “client7 client18” daemon.raw
```

`nsr_render_log` has many options that allow filtering of output based on specified criteria. If more than one value is specified for a criteria (up to eight values per criteria are allowed) the set of values should be enclosed in quotes. Multiple values for a criteria are OR’d while multiple criteria types are AND’d.

Review the *EMC NetWorker Command Reference Guide* for more information.



Managing Log Files

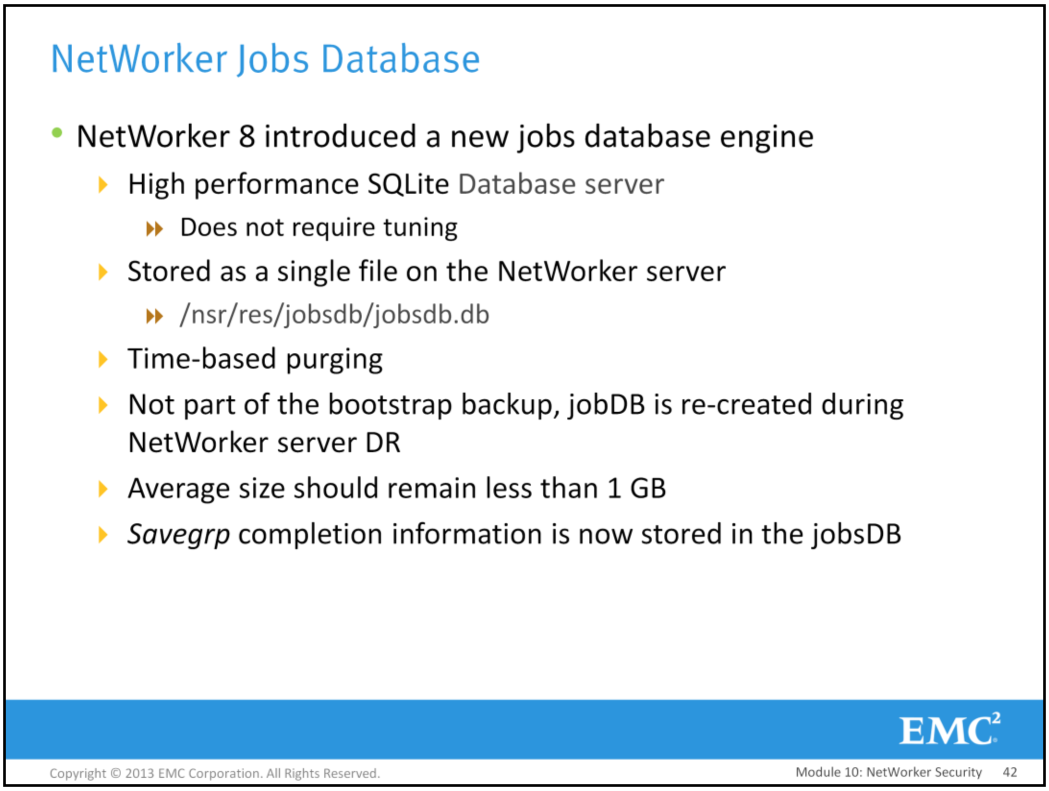
- Log files are trimmed at process start up.
- Environment variables can be used to control the number and size of the log files.
- NetWorker daemon log file (daemon .raw)
  - NSR_MAXLOGVERS
  - NSR_MAXLOGSIZE
- Console server log file (gstd.raw)
  - GST_MAXLOGSIZE
  - GST_MAXLOGVERS
- Configured as standard environment variables in Windows
- On UNIX systems running NetWorker 8+
  - Use NetWorker environment file
    - /nsr/nsrrc
    - Format of Bourne shell script (ENVVAR=xxxx; export ENVVAR)

When the NetWorker server starts (NetWorker Backup and Recover Server in Windows and nsrd in Unix), it checks the size of the `daemon.raw` log file. If the size of the log file has exceeded a maximum size, the current `daemon.raw` file is renamed to `daemon_<date_time>.raw` and a new empty `daemon.raw` is created. Each time the server is restarted, this process is repeated until the maximum number of log versions is reached, at which point the oldest log file is deleted. The default maximum log file size is 2 MB. To change this default value, set the NSR_MAXLOGSIZE environment variable. The maximum number of log files maintained is controlled by an environment variable called NSR_MAXLOGVERS. Its default value is 4.

Whenever the Console service is started (`gstd`), the size of the `gstd` log file is checked. This number is controlled by the GST_MAXLOGSIZE environment variable, with a default maximum size of 1 MB. By default, the maximum number of `gstd` log files is 4. This number is controlled by the GST_MAXLOGVERS environment variable.

On Windows servers these variables are standard operating system variables and should be configured as any other environment variable. On UNIX servers however, NetWorker 8 provides a new environment file that can be used for specifying environment variables. This file is located in `/nsr/nsrrc` and all entries should be formatted in the same way as a Bourne shell script. See the *EMC NetWorker Administration Guide* for details on setting the environment variables.

Note: The `networkr.raw` file is overwritten with the next manual backup or recovery. If the file contains information that you want to save, rename the file or export the information by using the `nsr_render_log` program.

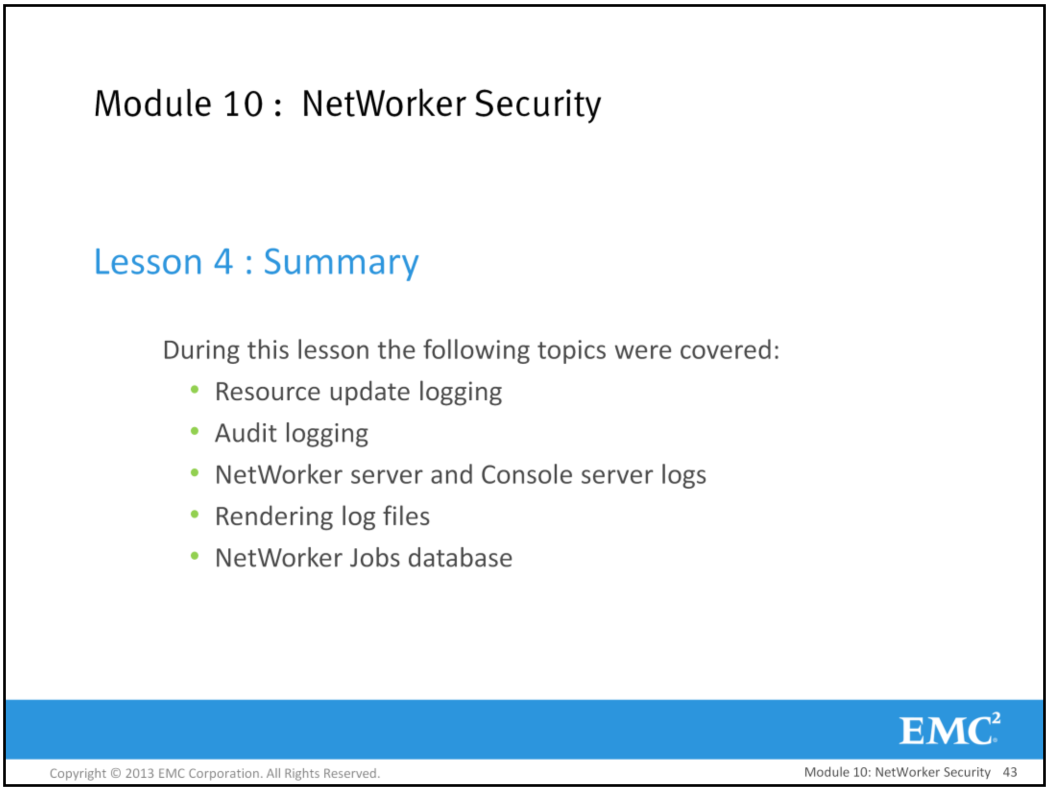


NetWorker Jobs Database

- NetWorker 8 introduced a new jobs database engine
  - High performance SQLite Database server
    - Does not require tuning
  - Stored as a single file on the NetWorker server
    - /nsr/res/jobsdb/jobsdb.db
  - Time-based purging
  - Not part of the bootstrap backup, jobDB is re-created during NetWorker server DR
  - Average size should remain less than 1 GB
  - *Savegrp* completion information is now stored in the jobsDB

Beginning with NetWorker 8, the jobs database has been moved to a new database engine. The new jobs database uses an embedded SQLite database server which is contained within a single file on the NetWorker server. The jobs database is no longer a part of the bootstrap backup and is re-created during NetWorker DR procedure. The average size of the jobs database should remain less than 1 GB in size and is managed using a time-based purging configuration.

Additionally, the savegrp completion information is not stored in RAP and temp files, but is now located in the jobs database.



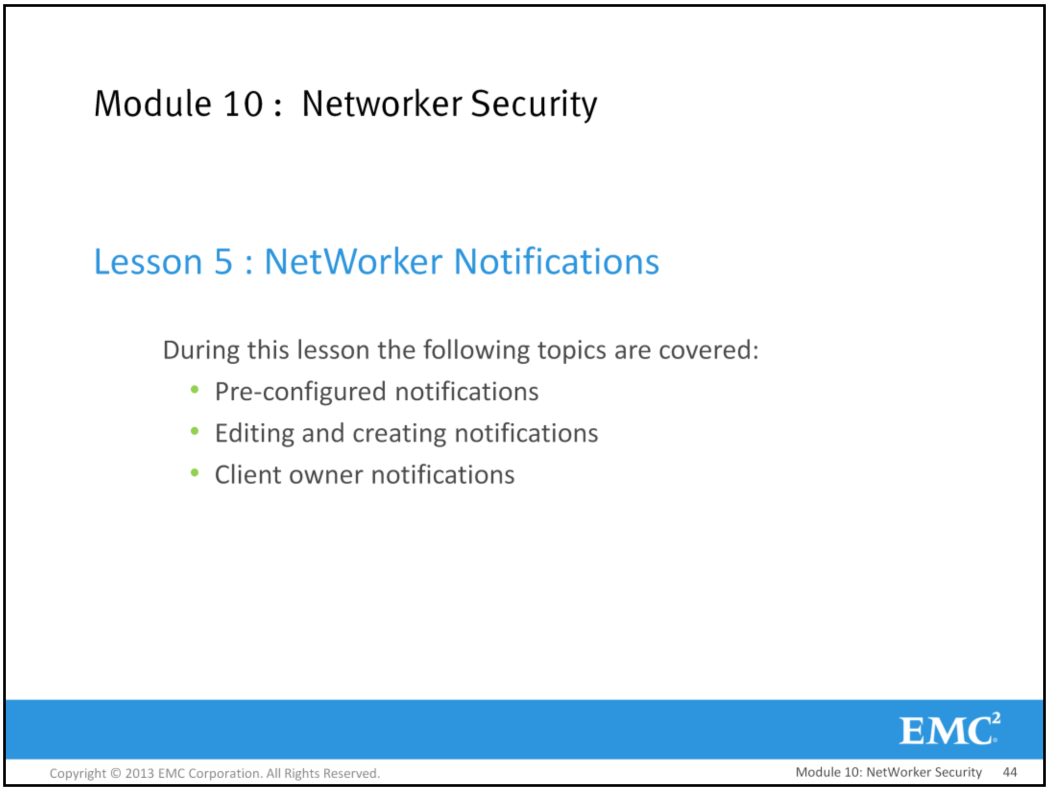
Module 10 : NetWorker Security

Lesson 4 : Summary

During this lesson the following topics were covered:

- Resource update logging
- Audit logging
- NetWorker server and Console server logs
- Rendering log files
- NetWorker Jobs database

This lesson discussed NetWorker log files and the jobs database, including resource update logging and audit logging capabilities, the various logs available for NetWorker and Console servers, and the procedures for rendering the logs.



Module 10 : Networker Security

Lesson 5 : NetWorker Notifications

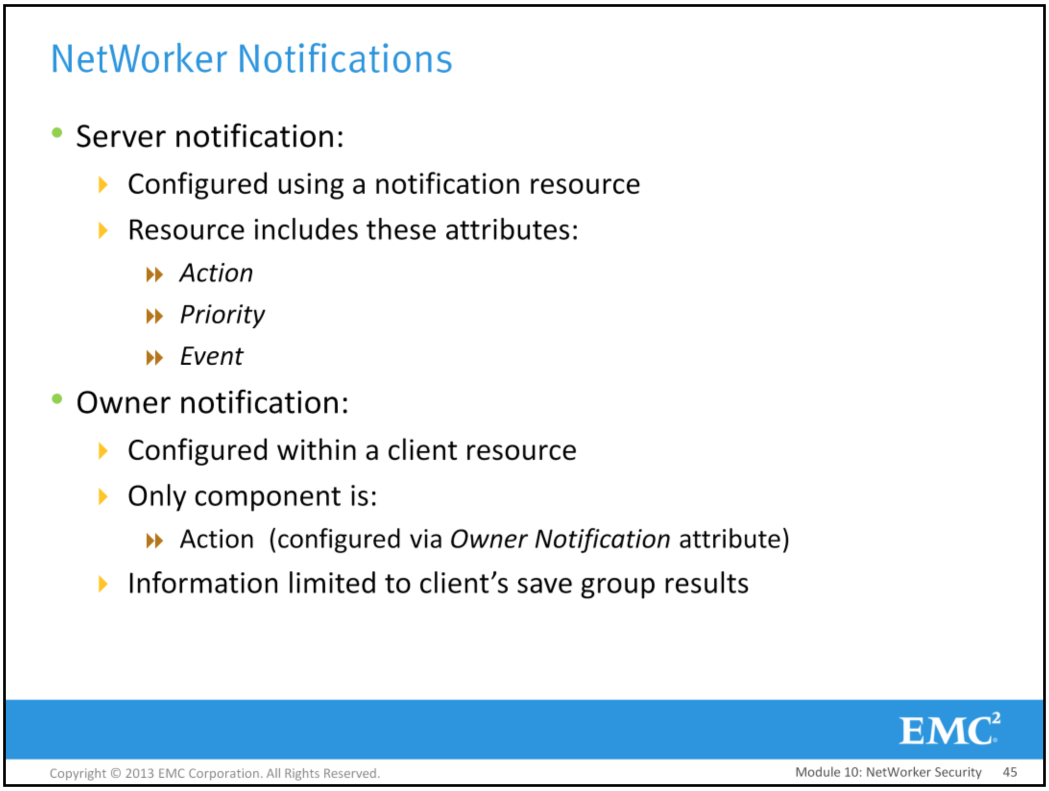
During this lesson the following topics are covered:

- Pre-configured notifications
- Editing and creating notifications
- Client owner notifications

EMC²

Module 10: NetWorker Security 44

This lesson covers NetWorker notifications including pre-configured notifications, procedures for editing and creating notifications, and configuring client owner notifications.



NetWorker Notifications

- Server notification:
  - Configured using a notification resource
  - Resource includes these attributes:
    - *Action*
    - *Priority*
    - *Event*
- Owner notification:
  - Configured within a client resource
  - Only component is:
    - Action (configured via *Owner Notification* attribute)
  - Information limited to client’s save group results

Many NetWorker processes within a data zone notify the NetWorker server (`nsrd`) when they finish performing their assigned task or when they are having difficulty performing a task due to undesirable conditions. These conditions might include:

- There are no appendable volumes available for a backup.
- A NetWorker license has expired or is about to expire.
- A tape drive needs cleaning before data can be written to a volume in the drive.
- An advanced file type device has become full.

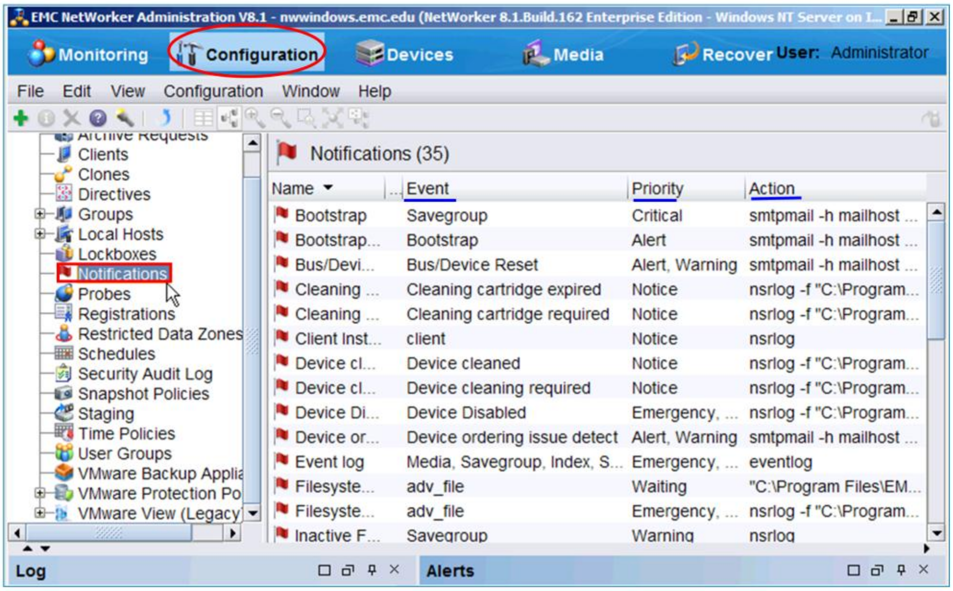
When a process notifies `nsrd` of what is happening, one of multiple priorities is assigned to the notification, depending on the message’s importance. Priorities can range from **informational** where no problem exists, to **critical**, where it is possible that NetWorker is unable to perform a backup.

There are numerous preconfigured NetWorker notification resources that `nsrd` uses, so that when a particular event occurs at a specific priority, `nsrd` can perform some action to either correct the situation or somehow notify the NetWorker administrator that the condition exists.

To customize your NetWorker environment, you can either modify the action performed for existing, preconfigured notifications or you can create your own customized notifications, which usually involves copying an existing notification and modifying the action, resulting in multiple actions being performed for the event.

An owner notification pertains only to the savegroup report for a client and is discussed shortly.

Preconfigured NetWorker Notification Resources

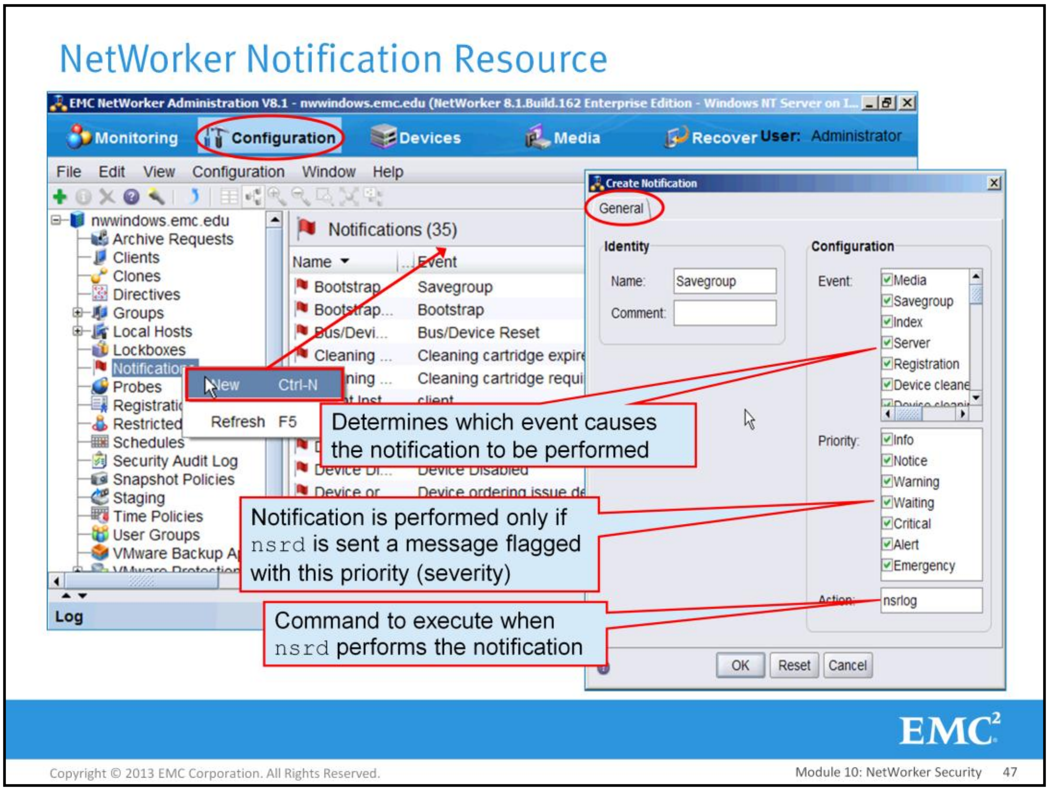


Name	Event	Priority	Action
Bootstrap	Savegroup	Critical	smtpmail -h mailhost ...
Bootstrap...	Bootstrap	Alert	smtpmail -h mailhost ...
Bus/Devi...	Bus/Device Reset	Alert, Warning	smtpmail -h mailhost ...
Cleaning ...	Cleaning cartridge expired	Notice	nsrlog -f "C:\Program...
Cleaning ...	Cleaning cartridge required	Notice	nsrlog -f "C:\Program...
Client Inst...	client	Notice	nsrlog
Device cl...	Device cleaned	Notice	nsrlog -f "C:\Program...
Device cl...	Device cleaning required	Notice	nsrlog -f "C:\Program...
Device Di...	Device Disabled	Emergency, ...	nsrlog -f "C:\Program...
Device or...	Device ordering issue detect	Alert, Warning	smtpmail -h mailhost ...
Event log	Media, Savegroup, Index, S...	Emergency, ...	eventlog
Filesyste...	adv_file	Waiting	"C:\Program Files\EM...
Filesyste...	adv_file	Emergency, ...	nsrlog -f "C:\Program...
Inactive F...	Savegroup	Warning	nsrlog

Module 10: NetWorker Security 46

The slide shows the notifications that are preconfigured when NetWorker is installed. You can customize a notification by changing the action performed when the notification is processed.

For a complete description of the default action of each notification, see the *EMC NetWorker Administration Guide*.



NetWorker Notification Resource

Name	Event
Bootstrap	Savegroup
Bootstrap...	Bootstrap
Bus/Devi...	Bus/Device Reset
Cleaning ...	Cleaning cartridge expire
Cleaning ...	Cleaning cartridge requi
...t Inst...	client
Device Di...	Device Disabled
Device or...	Device ordering issue de

Name: Savegroup

Comment:

Event: ☑Media ☑Savegroup ☑Index ☑Server ☑Registration ☑Device cleane ☑Device cleani

Priority: ☑Info ☑Notice ☑Warning ☑Waiting ☑Critical ☑Alert ☑Emergency

Action: nsrlog

Determines which event causes the notification to be performed

Notification is performed only if nsrd is sent a message flagged with this priority (severity)

Command to execute when nsrd performs the notification

Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 47

A notification's **Event** attribute specifies one or more events which trigger the performing of the notification by `nsrd`. A wide variety of NetWorker events send RPC messages to `nsrd`, keeping the NetWorker server informed about what is taking place.

Each message generated as the result of an event is flagged with a severity level or priority. A notification's **Priority** attribute specifies the severity level(s) at which the message must be flagged for the notification to be performed.

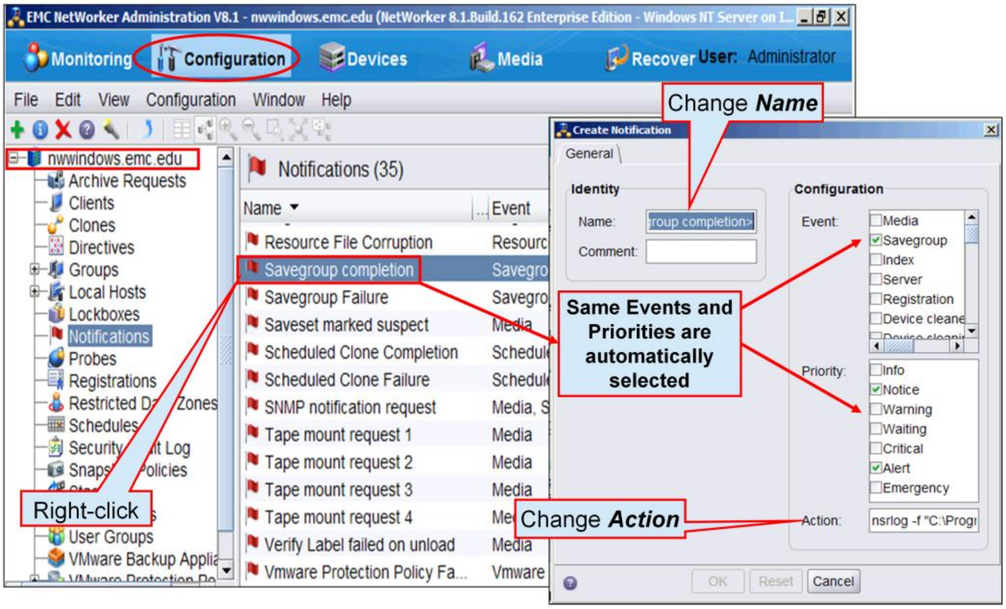
Lastly, the **Action** attribute specifies the command that is executed when a selected event sends a message to `nsrd` at a selected priority. For a NetWorker server running Microsoft Windows, NetWorker provides the following commands that are commonly used in notifications:

- `nsrlog` (directs message contents to a log file)
- `nsrlpr` (sends message contents to a printer)
- `smtpmail` (emails message contents to a user)

A UNIX NetWorker server already has the utilities necessary for logging information (the syslog facility and the `logger` command), printing (`lp` or `lpr`), and sending email (`mail` or `mailx`).

Note: Any path name specified in the **Action** attribute that contains a space character must be enclosed in double quotes.

Copying a Notification



Name	Event
Resource File Corruption	Resourc
Savegroup completion	Savegro
Savegroup Failure	Savegro
Saveset marked suspect	Media
Scheduled Clone Completion	Schedul
Scheduled Clone Failure	Schedul
SNMP notification request	Media, S
Tape mount request 1	Media
Tape mount request 2	Media
Tape mount request 3	Media
Tape mount request 4	Me
Verify Label failed on unload	Media
Vmware Protection Policy Fa...	Vmware

Name: roup completion>

Comment:

Event: ☐Media ☑Savegroup ☐Index ☐Server ☐Registration ☐Device cleane

Priority: ☐Info ☑Notice ☐Warning ☐Waiting ☐Critical ☑Alert ☐Emergency

Action: nsrlog -f "C:\Progr

Change *Name*

Same Events and Priorities are automatically selected

Right-click

Change *Action*

EMC²

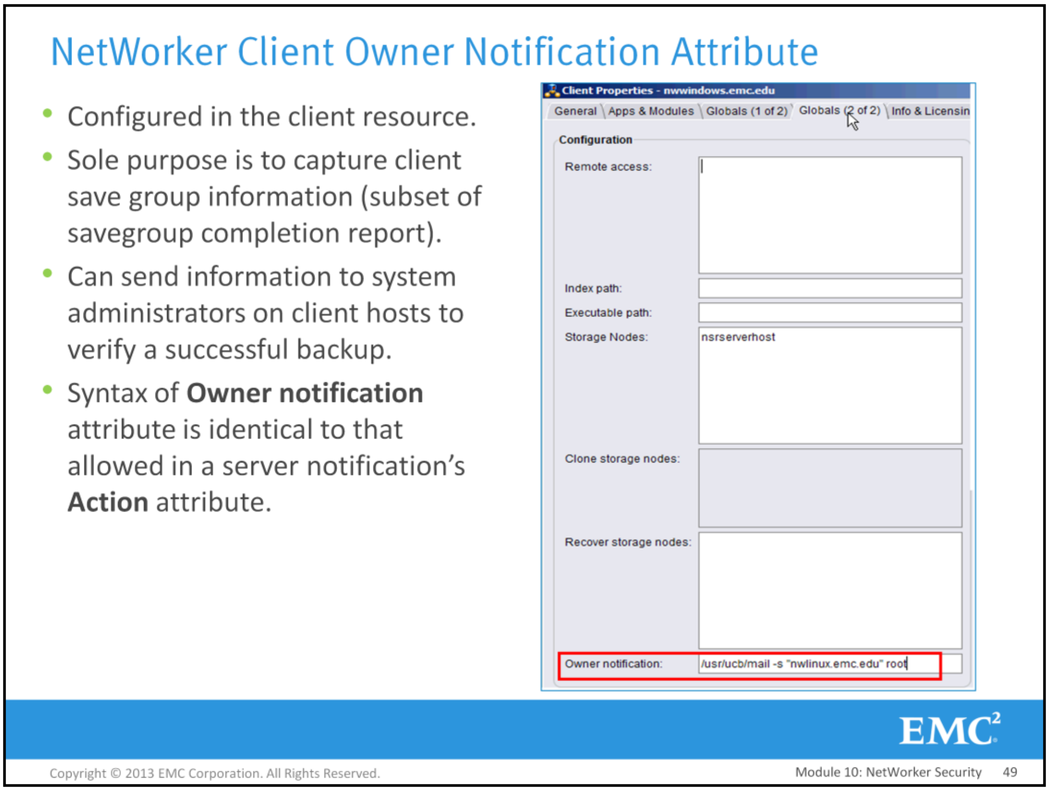
Copyright © 2013 EMC Corporation. All Rights Reserved.

Module 10: NetWorker Security 48

A common reason for creating a new notification is to perform multiple actions for an existing notification without needing to write a customized script. For example, in addition to having the savegroup completion report emailed to the administrator, you may want it appended to the end of a log file. To accomplish this, you have two choices: write a custom script which you enter in the **Action** field of the existing **Savegroup completion** notification or create another notification resource that is configured with the same event and priorities, but with a different action.

In the example in the slide, a new notification is being created by copying the original **Savegroup completion** notification. The new notification is automatically configured with the same event (**Savegroup**), priorities (**Alert** and **Notice**) and action as the original notification. Change the **Name** and **Action** fields to finish defining the new notification.

Now, when `savegrp` finishes and notifies `nsrd` via a message flagged as either “alert” or “notice”, `nsrd` knows that there are two notifications that need to be processed and performs the action specified by each one.



NetWorker Client Owner Notification Attribute

- Configured in the client resource.
- Sole purpose is to capture client save group information (subset of savegroup completion report).
- Can send information to system administrators on client hosts to verify a successful backup.
- Syntax of **Owner notification** attribute is identical to that allowed in a server notification's **Action** attribute.

Client Properties - nwwindows.emc.edu

Remote access:

Index path:

Executable path:

Storage Nodes: nsrserverhost

Clone storage nodes:

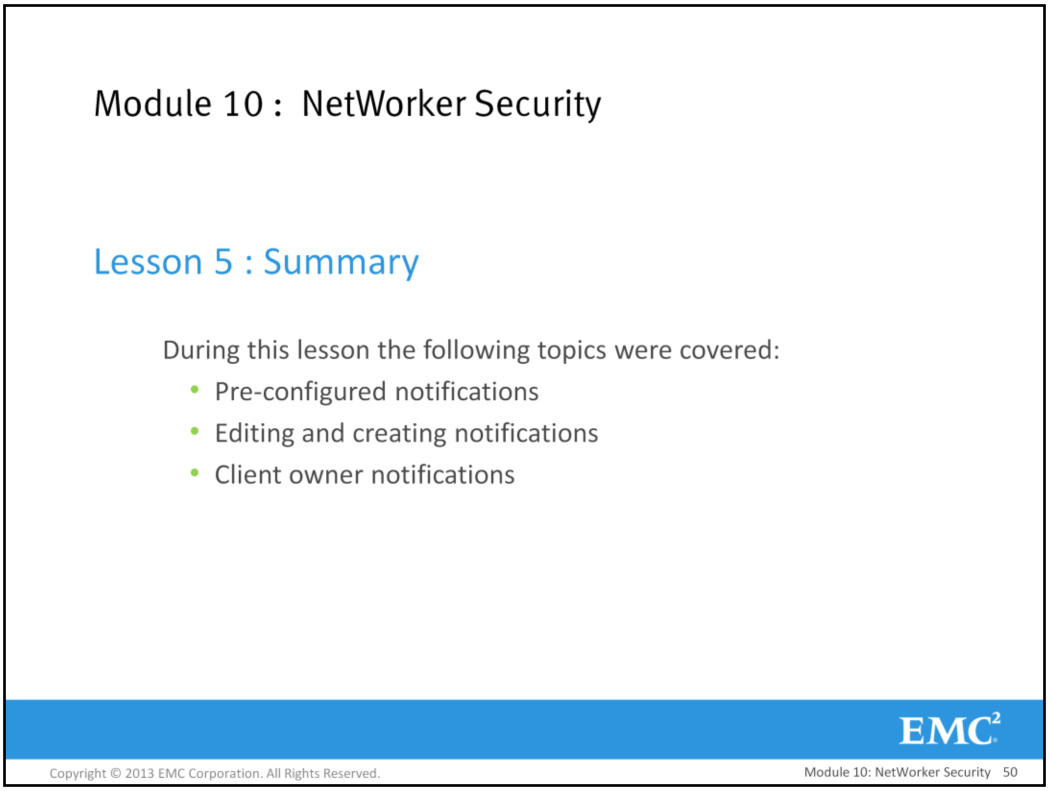
Recover storage nodes:

Owner notification: /usr/ucb/mail -s "nwlinux.emc.edu" root

The **Owner notification** attribute in the client resource is used to specify a command to run on the NetWorker server when the client is backed up in a server-initiated backup (`savegrp`). The command specified receives as its input the portion of the savegroup completion report that pertains to this individual client. This includes all the client's save sets and the client's CFI save set.

This attribute is often used to provide information to the NetWorker client's system administrator, commonly via email, concerning the client's backup status. The information includes:

- The NetWorker group name and summary of the client's backup (success/failures)
- The amount of data backed up in each save set
- The time for each backed up save set
- The number of files in each save set
- Any warning messages that occurred during the backup
- Any failure messages that occurred during the backup



Module 10 : NetWorker Security

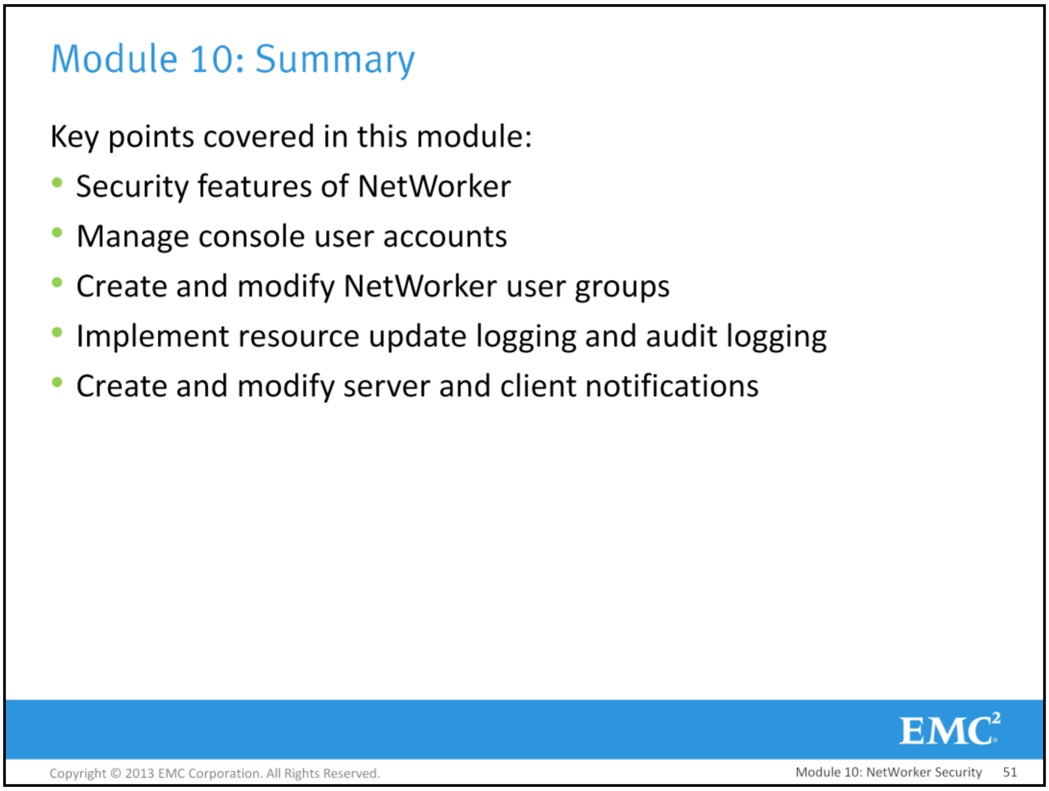
Lesson 5 : Summary

During this lesson the following topics were covered:

- Pre-configured notifications
- Editing and creating notifications
- Client owner notifications

EMC²

This lesson covered NetWorker notifications including pre-configured notifications, procedures for editing and creating notifications, and configuring client owner notifications.



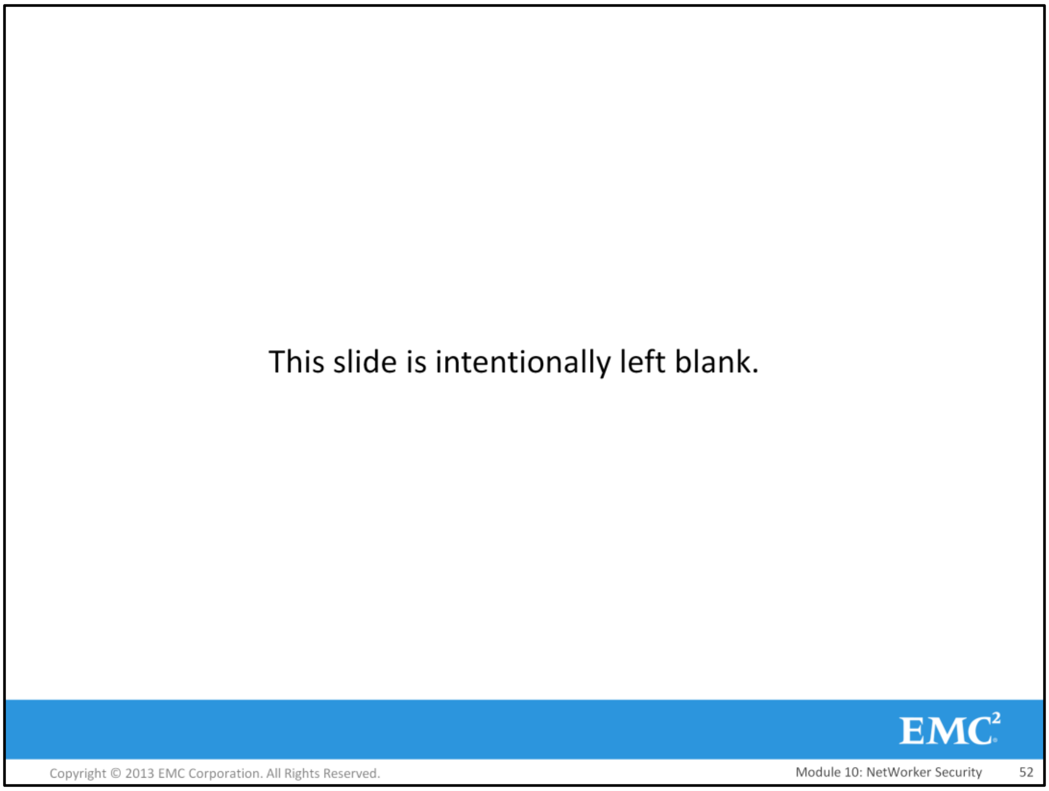
Module 10: Summary

Key points covered in this module:

- Security features of NetWorker
- Manage console user accounts
- Create and modify NetWorker user groups
- Implement resource update logging and audit logging
- Create and modify server and client notifications

EMC²

This module focused on the security features of NetWorker. It covered creating and using user groups within a NetWorker environment. We looked at the NetWorker jobs database and covered the user groups within a NetWorker environment. We discussed the NetWorker notifications including pre-configured notifications, procedures for editing and creating notifications, and configuring client owner notifications.



This slide is intentionally left blank.