# Dell EMC NetWorker

Version 19.1

## Security Configuration Guide

302-005-700
Rev 02
July, 2019

DELL EMC

Copyright © 2014-2019 Dell Inc. or its subsidiaries. All rights reserved.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

# CONTENTS

**Figures** 7

**Tables** 9

**Preface** 11

**Chapter 1 Introduction** 17

**Chapter 2 Access Control Settings** 19
NetWorker Authentication Service 20
NetWorker Authentication Service database 20
Managing authentication 22
Configuring LDAP or AD authentication authorities 22
Querying the LDAP or AD directory from NetWorker Authentication Service 39
Managing the NetWorker Authentication Service local database 42
Harden the Authentication Service on port 9090 51
Increasing the header size of the Apache tomcat 52
Managing the NetWorker Authentication Service options 53
Managing token policies 53
Managing local database password policies 54
Configure CLI options 56
Changing the NetWorker Authentication Service port 57
How user authentication and authorization works in NMC and NetWorker 58
Modifying authentication methods for NetWorker servers in NMC 59
User authorization 60
Changing the NetWorker Authentication Service hostname and port number 82
How user authentication and authorization works in NWUI 84
Disabling SSLv3 cipher connectivity to the PostgresSQL database on the NMC server 85
Component access control 86
Component authentication 86
Removing SHA1 credentials from database 100
Procedure to recreate SHA1 and SHA2 credentials 101
Component authorization 102
Generate self signed certificate 105
Enabling two factor authentication for AD and LDAP users 105

**Chapter 3 Log Settings** 107
NetWorker log files 108
NetWorker Server log files 108
NMC server log files 111

NetWorker Client log files....112
View log files....114
Raw log file management....118
Monitoring changes to the NetWorker server resources....121
Configuring logging levels....122
NetWorker Authentication Service logs....131
NetWorker Authentication Service log files....131
NetWorker Authentication Service server log file management....132
CLI log file management....133

**Chapter 4 Communication Security Settings 135**
Port usage and firewall support....136
Service ports....136
Connection ports....137
Special considerations for firewall environments....137
Configuring TCP keepalives at the operating system level....138
Determining service port requirements....139
NetWorker client service port requirements....140
Service port requirements for NetWorker storage nodes....140
Service port requirements for the NetWorker server....141
Service port requirements for NMC Server....143
Configuring service port ranges in NetWorker....143
Determine the available port numbers....143
Configuring the port ranges in NetWorker....143
Configuring the service ports on the firewall....146
How to confirm the NMC server service ports....151
Determining service port requirement examples....152
Troubleshooting....157

**Chapter 5 Data Security Settings 161**
AES encryption for backup and archive data....162
Creating or modifying the lockbox resource....162
Defining the AES pass phrase....163
Configuring the client resource to use AES encryption....164
Configure encryption for a client-initiated backup....164
Recover encrypted data....165
Federal Information Processing Standard compliance....167
Data integrity....168
Verifying the integrity of the backup data....168
Verifying the integrity of the NetWorker server media data and client file indexes....169
Data erasure....170
NetWorker server media database and index data management....170
Manually erasing data on tape and VTL volumes....171
Manually erasing data from an AFTD....171
Security alert system settings....172
Monitoring changes to NetWorker server resources....172
Security audit logging....172

**Chapter 6 Hardening the NetWorker 187**
Security Hardening For The NetWorker Management Console....188
Enabling the Modules Required To Harden Apache httpd....188
**Enable Apache httpd directives**....188
Enabling HTTPS....189

Configuring gconsole file to Enable HTTPS .....191
Replacing Default Tomcat Web Pages..... 191
Security Hardening For The NetWorker Authentication Tomcat Service.. 192
Hardening the NSR Tomcat Services..... 192
Hardening TLS Protocol..... 193
Hardening Supported Ciphers..... 193
Hardening the NSR Tomcat Shutdown Port.....194
Harden the Authentication Service on port 9090 ..... 194

# FIGURES


1 NetWorker Authentication Service Database hierarchy.....22
2 External Authority pane in the NMC Console.....24
3 Create External Authentication Authority.....24
4 User properties in ADSI Edit.....30
5 Group properties in ADSI Edit.....30
6 User properties in LDAPAdmin.....33
7 Group properties in LDAPAdmin.....33
8 Copying the group DN.....63
9 Configuring the External Roles attribute.....63
10 Copying the group DN.....64
11 Configuring the External Roles attribute.....65
12 Copying the group DN.....77
13 Copying the group DN.....77
14 WinPE registry key to troubleshoot recoveries.....130
15 Default port usage across NetWorker.....136
16 Uni-directional firewall with storage nodes.....153
17 Bi-directional firewall with Data Domain appliance.....155
18 The audit log server manages a single data zone.....175
19 The NMC server is the audit log server for multiple data zones.....176
20 Each NetWorker server in a data zone is the audit log server.....177
21 Security Audit Log resource.....184

# TABLES


1 Revision history ..... 11
2 Style conventions ..... 13
3 Configuration options ..... 26
4 Default password policy requirements ..... 55
5 NetWorker Authentication Service CLI options ..... 56
6 NMC user roles and associated privileges ..... 60
7 Allowed Operations for each NetWorker privilege ..... 69
8 Privileges associated with each NetWorker User Group ..... 73
9 Operations that require entries in the servers file ..... 102
10 NetWorker Server log files ..... 108
11 NMC server log files ..... 111
12 Client log files ..... 112
13 Message types ..... 116
14 Raw log file attributes that manage log file size ..... 119
15 Raw log file attributes that manage the log file trimming mechanism ..... 119
16 NetWorker Authentication Service log files ..... 131
17 Setting TCP parameters for each operating system ..... 138
18 Standard NetWorker Client port requirements to NetWorker server ..... 140
19 Additional service port requirements for Snapshot clients ..... 140
20 Service port requirements for storage nodes ..... 141
21 NetWorker server program port requirements ..... 142
22 Port requirements to NMC server to each NetWorker client ..... 143
23 nsrports options ..... 145
24 Port requirements for NetWorker communications with applications ..... 146
25 Levels available for the nsrck process ..... 170
26 Security event resources and attributes - resource database (RAP) ..... 177
27 Security event resources and attributes - NetWorker client database ..... 179
28 Message types ..... 183
29 Auditlog rendered service attributes ..... 184

# Preface

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

**Note:** This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website https://www.dell.com/support.

## Purpose

This document provides an overview of security settings available in the NetWorker product.

## Audience

This document is part of the NetWorker documentation set, and is intended for use by system administrators who are responsible for setting up and maintaining NetWorker and managing a secure network.

## Revision history

The following table presents the revision history of this document.

**Table 1** Revision history

| Revision | Date | Description |
|---|---|---|
| 02 | July 10, 2019 | Added a chapter on hardening NetWorker. |
| 01 | May 20, 2019 | First release of the document for NetWorker 19.1. |

## Related documentation

The NetWorker documentation set includes the following publications, available on the Support website:

- *NetWorker E-LAB Navigator*
  Provides compatibility information, including specific software and hardware configurations that NetWorker supports. To access E-LAB Navigator, go to https://elabnavigator.emc.com/eln/elnhome.
- *NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *NetWorker Network Data Management Protocol (NDMP) User Guide*
  Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *NetWorker Cluster Integration Guide*
  Contains information related to configuring NetWorker software on cluster servers and clients.
- *NetWorker Installation Guide*

Provides information on how to install, uninstall, and update the NetWorker software for clients, storage nodes, and servers on all supported operating systems.

- *NetWorker Updating from a Previous Release Guide*
  Describes how to update the NetWorker software from a previously installed release.
- *NetWorker Release Notes*
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *NetWorker Data Domain Boost Integration Guide*
  Provides planning and configuration information on the use of Data Domain devices for data deduplication backup and storage in a NetWorker environment.
- *NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Describes how to design, plan for, and perform a step-by-step NetWorker disaster recovery.
- *NetWorker Snapshot Management Integration Guide*
  Describes the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on storage arrays.
- *NetWorkerSnapshot Management for NAS Devices Integration Guide*
  Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.
- *NetWorker Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- *NetWorker VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *NetWorker REST API Getting Started Guide*
  Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *NetWorker REST API Reference Guide*
  Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- *NetWorker 19.1 with CloudBoost 19.1 Integration Guide*
  Describes the integration of NetWorker with CloudBoost.
- *NetWorker 19.1 with CloudBoost 19.1 Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker and Cloud Boost, secure deployment, and physical security controls needed to ensure the secure operation of the product.

- NetWorker Management Console Online Help
  Describes the day-to-day administration tasks performed in the NetWorker Management Console and the NetWorker Administration window. To view the online help, click **Help** in the main menu.
- NetWorker User Online Help
  Describes how to use the NetWorker User program, which is the Windows client interface, to connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

### Special notice conventions that are used in this document

The following conventions are used for special notices:

**NOTICE** Identifies content that warns of potential business or data loss.

**Note:** Contains information that is incidental, but not essential, to the topic.

### Typographical conventions

The following type style conventions are used in this document:

**Table 2** Style conventions

| | |
|---|---|
| **Bold** | Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window. |
| *Italic* | Used for full titles of publications that are referenced in text. |
| `Monospace` | Used for:<br>• System code<br>• System output, such as an error message or script<br>• Pathnames, file names, file name extensions, prompts, and syntax<br>• Commands and options |
| *Monospace italic* | Used for variables. |
| **`Monospace bold`** | Used for user input. |
| [ ] | Square brackets enclose optional values. |
| \| | Vertical line indicates alternate selections. The vertical line means or for the alternate selections. |
| { } | Braces enclose content that the user must specify, such as x, y, or z. |
| ... | Ellipses indicate non-essential information that is omitted from the example. |

You can use the following resources to find more information about this product, obtain support, and provide feedback.

### Where to find product documentation

- https://www.dell.com/support
- https://community.emc.com

### Where to get support

The Support website https://www.dell.com/support provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to https://www.dell.com/support.
2. In the search box, type a product name, and then from the list that appears, select the product.

### Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

### Live chat

To participate in a live interactive chat with a support agent:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

### Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.

**Note:** To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To get the details of a service request, in the `Service Request Number` field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

### Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network https://community.emc.com. Interactively engage with customers, partners, and certified professionals online.

## How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

# CHAPTER 1

# Introduction

NetWorker is a heterogeneous backup application that addresses data protection challenges. The centralized management capabilities of NetWorker provides effective data protection for file systems, enterprise applications, storage arrays, and NAS filers to a variety of target devices.

This guide provides an overview of security configuration settings available in NetWorker, secure deployment, and physical security controls needed to ensure the secure operation of the product.

This guide is divided into the following sections:

**Access Control Settings**

Access control settings enable the protection of resources against unauthorized access. This chapter provides an overview of the settings available in the product to ensure a secure operation of the product and describes how you can limit product access by end-users or by external product components.

**Log Settings**

A log is a chronological record that helps you to examine the sequence of activities surrounding or leading up to an operation, procedure, or event in a security-related transaction from beginning to end. This chapter describes how to access and manage the logs files available in NetWorker.

**Communication Security Settings**

Communication security settings enable the establishment of secure communication channels between NetWorker components, NetWorker components and external systems, and NetWorker components and external components. This chapter describes how to ensure NetWorker uses secure channels for communication and how to configure NetWorker in a firewall environment.

**Data Security Settings**

Data security settings enable you to define controls that prevent unauthorized access and disclosure of data permanently stored by NetWorker. This chapter describes the settings available to ensure the protection of the data handled by NetWorker.

# CHAPTER 2

# Access Control Settings

Access control settings enable the protection of resources against unauthorized access. This chapter describes settings you can use to limit access by end-user or by external product components.


- NetWorker Authentication Service ..... 20
- NetWorker Authentication Service database ..... 20
- Managing authentication ..... 22
- Managing the NetWorker Authentication Service options ..... 53
- How user authentication and authorization works in NMC and NetWorker ..... 58
- How user authentication and authorization works in NWUI ..... 84
- Disabling SSLv3 cipher connectivity to the PostgresSQL database on the NMC server ..... 85
- Component access control ..... 86
- Generate self signed certificate ..... 105
- Enabling two factor authentication for AD and LDAP users ..... 105

# NetWorker Authentication Service

The NetWorker Authentication Service is a web-based application that runs within an Apache Tomcat instance. NetWorker 9.0 and later requires you to install and configure the NetWorker Authentication Service application on the NetWorker server. The *NetWorker Installation Guide* describes how to install and configure the NetWorker Authentication Service.

NetWorker Authentication Service provides a NetWorker environment with token-based authentication and Single Sign On (SSO) support. Token-based authentication enables users to securely connect to the NetWorker Management Console (NMC) server, the NetWorker server, and to perform secure backup and recovery operations.

When a NetWorker or NMC operation requires authentication, the requesting process contacts the NetWorker Authentication Service to verify the credentials of the user account that started the request. When the NetWorker Authentication Service successfully verifies the user, the application issues a time-limited, signed, and encrypted SAML token to the requesting process. All the NetWorker components that require authentication can use the token to verify the user, until the token expires.

For example, the following steps occur when you log in to an NMC server and use the NMC GUI to connect to a NetWorker server:

1. When you log in to the NMC server, the NMC server contacts the NetWorker Authentication Service to verify the user credentials. User credentials include the tenant, domain, username, and password of the specified user account.
2. The NetWorker Authentication Service compares the user credentials with user information that is stored in the local user database, or contacts the external authentication authority to verify the details.
3. If the user verification succeeds, the NetWorker Authentication Service generates a token for the user account and sends the token to the NMC server.
4. The NMC server log in attempt succeeds.
5. The NMC server looks up the user role membership for the user to determine the level of authorization that the user has on the NMC server.
6. The user tries to connect to a NetWorker server.
7. If the NMC user role that is assigned to the user has the rights to manage the selected NetWorker server, the NMC server provides the token information about the user to the NetWorker server, with each request.
8. The NetWorker server compares the information that is contained in the token with contents of the External roles attribute in each configured User Group to determine the level of authorization that the user has on the NetWorker server. NetWorker allows or denies the user request, depending on the level of authorization that is assigned to the user.
9. If the token has expired, the NetWorker server displays an appropriate error message to the user. The user must contact the NetWorker Authentication Service to acquire a new token, and then retry the operation.

# NetWorker Authentication Service database

The NetWorker Authentication Service uses an H2 database to store configuration information.

The NetWorker Authentication Service local database is divided into four major components:

**Note:** You can use the NetWorker Management Console or the `authc_mgmt` command line tool to perform all the configurations.

- Internal authentication authority settings (Local users and groups)—Defines information about local user accounts and groups. The NetWorker Authentication Service creates a built-in local administrator account during the installation process. When you install the NMC server software, the NMC installation process creates a default service account `svc_nmc_`*nmc_server_name*.
- External authentication authority configuration settings—Defines information about the LDAP and AD servers that the NetWorker Authentication Service can use to authenticate user access.
- Access permissions—Defines access permissions for users to manage the local database. Currently, two levels of permissions exist for users: FULL_CONTROL and Everyone. To configure the access permissions, use the `authc_config` command line tool.
- Service options—Defines the options for the NetWorker Authentication Service, for example, token and user options such as password policy configurations.

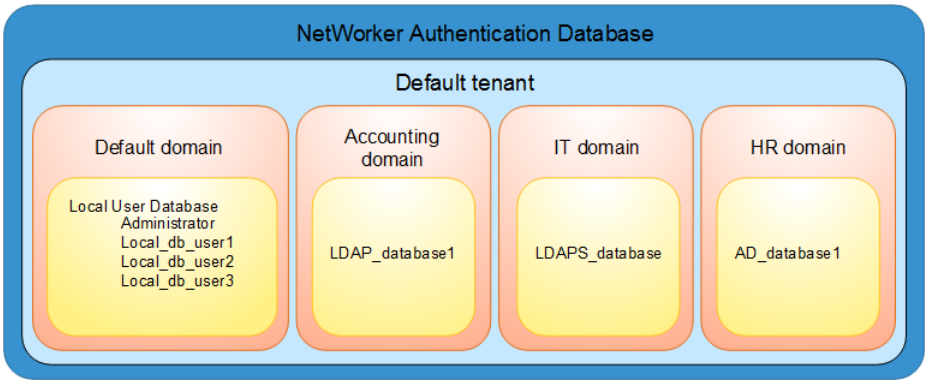
The NetWorker Authentication Service database provides a hierarchical security model for users and groups, which enables you to define access levels, authentication, and authorization in a multi-tenant configuration. The NetWorker Authentication Service provides the following organizational hierarchy:

- Tenant—Top-level organizational container for the NetWorker Authentication Service. Each external authentication authority in the local database is assigned to a tenant. A Tenant can contain one or more Domains but the domain names must be unique within the tenant. NetWorker Authentication Service creates one built-in tenant name Default, which contains the Default domain. Creating multiple tenants helps you to manage complex configurations. For example, service providers with restricted datazones (RDZ) can create multiple tenants to provide isolated data protection services to tenant users.
- Domain—An organizational container that contains one external authentication authority configuration. NetWorker Authentication Service creates one built-in domain name Default, which contains the local user database.
- Configuration— A configuration name and ID that uniquely identifies one tenant, domain, and external authority mapping.

The following figure provides an example of a NetWorker Authentication Service database with the following hierarchy:

- Three external authentication authority configurations:
  - LDAP_database1 contains the configuration information for an LDAP directory.
  - LDAPS_database contains the configuration information for an LDAPS directory.
  - AD_database1 contains the configuration information for an AD directory.
- Four domains, the Default domain, the three user-defined domains, the Accounting domain, the IT domain, and the HR domain.
- One tenant, the Default tenant.

**Figure 1** NetWorker Authentication Service Database hierarchy




# Managing authentication

The NetWorker Authentication Service is a web-based application that provides authentication services to other applications.

The NetWorker Authentication Service maintains a local user database to verify the credentials of a user account. You can also configure the NetWorker Authentication Service to use an external authority database, for example LDAP or AD. When you configure an external authority database, the NetWorker Authentication Service communicates directly with an LDAP or AD server to authenticate users.

You can use command line tools to configure and manage the authentication.

**Note:** If the `authc` server is installed in Java-9, and in case you try to execute the `authc` command/ script using Java-8, you will not be allowed to execute the script. This issue is most likely to occur when you have both Java-8 and Java-9 running on the setup.

To resolve this issue you can perform either of the following:

- Include Djavax.net.ssl.trustStorePassword=XXXXX in CLI script.
- Copy key keystore.password and value from authc-server.app.properties to authc-server.cli.properties.

## Configuring LDAP or AD authentication authorities

When you configure the NetWorker Authentication Service to authenticate users by using an external authentication authority, you can log in to the NMC server with a local user account or with a username and password that is managed by Lightweight Directory Access Protocol (LDAP), Lightweight Directory Access Protocol over SSL (LDAPS), or a Microsoft Active Directory server (AD). The NMC and NetWorker servers do not authenticate the user against the LDAP authority. The NMC server requests user validation from the NetWorker Authentication Service. The NetWorker Authentication Service performs a look-up to determine the LDAP or AD group that the authenticated user belongs to in the external authority. When authentication succeeds, the NetWorker Authentication Service issues a token to the NMC server. Activities that you perform in the Console window and the NetWorker Administration window uses the token information to ensure that the user can perform only the activities that the user has the appropriate privileges to perform.

**Note:** Nested AD group user login is not supported.

## Using NMC Console to configure LDAP, AD, or LDAPS authentication to manage NetWorker servers

On NetWorker servers, you can use the NMC **Console** window to configure the NetWorker Authentication Service to authenticate users in an AD or LDAP directory. After creating an AD or LDAP provider, you can also edit the external authority within the **Console**.

### About this task

**Note:** The LDAP Configuration wizard is only supported from the NetWorker 18.1 release.

### Procedure

1. (Optional) Create a tenant in the local database for the external authority. If you do not create a tenant, the configuration uses the Default tenant, which has an ID of 1. To create a tenant, type the following command:

   ```
   authc_config -u administrator -p "password" -e add-tenant -D
   "tenant-name=name" -D "tenant-alias=alias" -D "tenant-details=
   tenant_description"
   ```

   where:

   - *name* is the name of the tenant, without spaces. The maximum number of characters is 256. Specify ASCII characters in the tenant name only.
   - *alias* is alias of the tenant name. The maximum number of characters is 256.
   - *tenant_description* is a user-defined description of the tenant. The maximum number of characters is 256.

   **Note:** For multiple authentication providers of the same protocol, you cannot share the same tenant ID.

2. Connect to the NMC server with a NetWorker Authentication Service administrator account.

   The Console window opens with three tabs—Enterprise, Reports, and Setup.

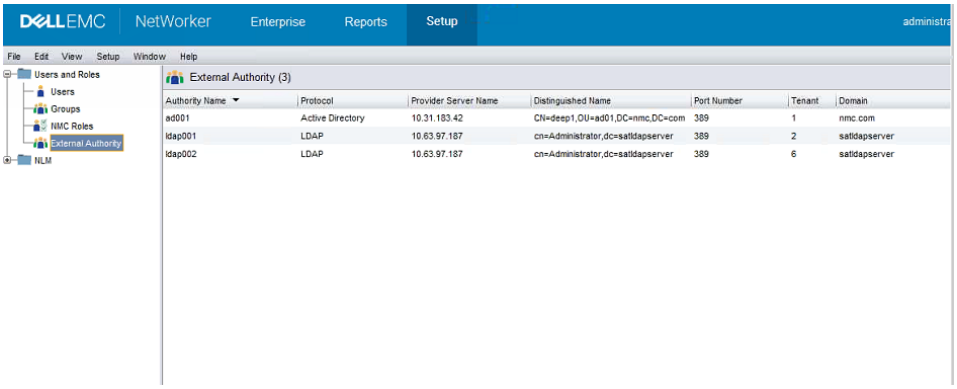
3. Click **Setup**.

   The **Users and Roles** window appears.

4. In the left navigation pane, select **Users and Roles** > **External Authority**.

   The **External Authority** pane displays in the right of the **Console** window.

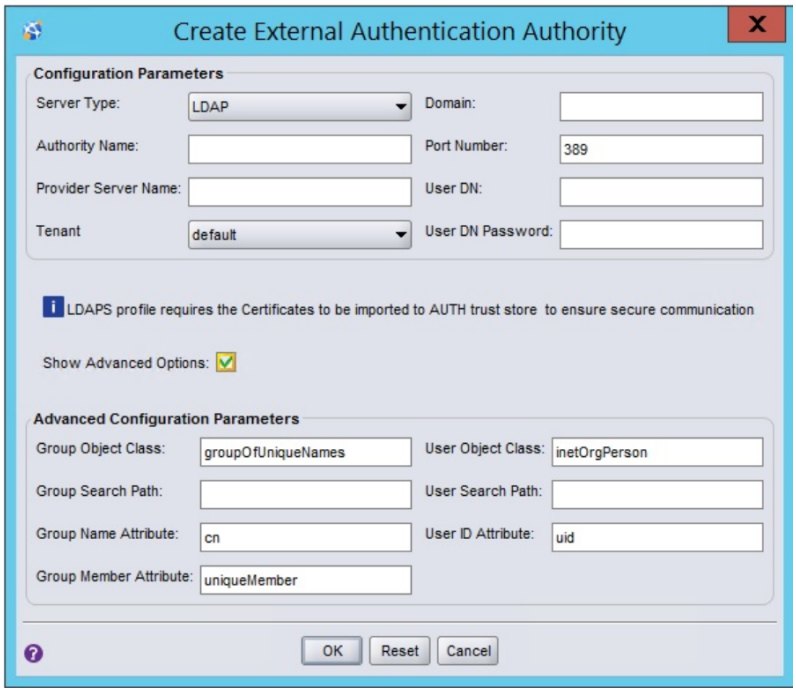
**Figure 2** External Authority pane in the NMC Console




5. Right-click in the External Authority pane and select **New** from the drop-down.

   The **Create External Authentication Authority** dialog displays.

   **Figure 3** Create External Authentication Authority




6. In the **Configuration Parameters** pane, select either the **LDAP**, **Active Directory**, or **LDAP over SSL** from the **Server type** drop-down. **LDAP** is selected by default.

   The fields in the **Advanced Configuration Parameters** pane, which appear when you select the **Show Advanced Options** checkbox, populate automatically with default values based on the Server type selected.

7. In the **Configuration Parameters** pane, provide the **Authority Name**, **Domain**, and the IP address of the server or the host name in the **Provider Server Name** field, and then select a tenant from the **Tenant** drop-down.

   Ensure that the **Authority Name** and **Domain** do not contain white spaces within the name, and that the name contains all ASCII characters is less than 256 characters.

> **Note:** Use only FQDN in case of LDAPS configuration.

8. In the **Configuration Parameters** pane, if you are not using the default port 389, type the correct **Port Number**.
9. In the **Configuration Parameters** pane, for the **User Group** field, type the name of a user account that has full read access to the LDAP or AD directory in the format " CN=XXXX,OU=YYYY", and then type the **User DN password**. XXXX is the common name and YYYY is the organizational unit name. Alternatively, if there is no OU configured, you can specify the CN and DC components instead. The NMC Property Help provides more information and examples for the **User Group** field.
10. If any of the default values populated in the **Advanced Configuration Parameters** fields do not match your LDAP/LDAPS/AD server configuration, change the values accordingly. If these values do not match your configuration, the provider creation process fails.
11. Click **OK**.

    > **Note:** All fields in the **Configuration Parameters** pane of the dialog are mandatory. If you click **OK** and any of these fields is missing, NMC displays an error message.

    Validation of the provider occurs during the connection attempt with the server. If the domain or FQDN could not be validated, then an error will be logged in NMC.

#### Results

After creating a provider, you can double-click on the entry in the **External Authority** pane to view the properties of the provider. The **Edit External Authentication Authority** dialog displays.
Within this dialog, you can modify any of the read/write fields. Note that the **Authority Name** and **Tenant** fields will be greyed out. You can only modify these fields when you create the provider in the **Create External Authentication Authority** dialog.

When you change any of the fields and click **OK**, a prompt appears requesting you to re-enter the password. After a message displays indicating that the change was successful, close the **Edit External Authentication Authority** dialog and then re-open to view the change.

> **Note:** After you log in as an AD or LDAP user, ensure that you do not change the **Group Search Path** and the **User Search Path** values. If you change the **Group Search Path** and the **User Search Path** values, the earlier saved values are lost, and you cannot access information related to users, groups, and so on.

## Using authc_config to configure LDAP, AD, or LDAPS authentication to manage NetWorker servers

You can also use the `authc_config` command on NetWorker 9.0 and later servers to configure the NetWorker Authentication Service to authenticate users in an AD or LDAP directory.

#### Before you begin

By default, the `authc_config` command is in the `/opt/nsr/authc-server/bin` on Linux and `C:\Program Files\EMC NetWorker\nsr\authc-server\bin` on Windows.

### Procedure

1. (Optional) Create a tenant in the local database for the external authority, and then determine the tenant ID assigned to the tenant. If you do not create a tenant, the configuration uses the Default tenant, which has an ID of 1. Perform the following steps:

   a. To create a tenant, type the following command:

   ```
   authc_config -u administrator -p "password" -e add-tenant -D
   "tenant-name=name" -D "tenant-alias=alias" -D "tenant-details=
   tenant_description"
   ```

   where:

   - *name* is the name of the tenant, without spaces. The maximum number of characters is 256. Specify ASCII characters in the tenant name only.
   - *alias* is alias of the tenant name. The maximum number of characters is 256.
   - *tenant_description* is a user-defined description of the tenant. The maximum number of characters is 256.

   b. To determine the tenant ID assigned to the tenant, type the following command:

   ```
   authc_config -u administrator -p "password" -e find-tenant -D
   "tenant-name=tenant_name"
   ```

   **Note:** You require the tenant ID to configure the LDAP or AD authentication authority in the local database.

2. From a command prompt on the NetWorker server, type the following command:

   ```
   authc_config -u administrator -p "password" -e add-config -D
   "tenant-id=tenant_id" -D options....
   ```

   **Note:** Ensure that you have a space before each -D. If you do not have a space before the -D switch, `authc_config` appends the -D to the previous option value and ignores the option value to which the -D is associated with.

   The following table provides more information about each configuration option.

**Table 3** Configuration options

| Options for 9.x and later | Equivalent 8.2 and earlier option name | Description |
|---|---|---|
| -D "config-tenant-id=*tenant_id*" | N/A | Required. The ID of the tenant that you created for the LDAP or AD configuration in the local database. By default, NetWorker Authentication Service creates one tenant that is called Default with a tenant ID of 1. |

**Table 3** Configuration options (continued)

| Options for 9.x and later | Equivalent 8.2 and earlier option name | Description |
|---|---|---|
| -D "config-active-directory=*y/n*" | N/A | Optional. A yes or no value that specifies if the external authority is AD. When you set this option to<br>`y` for an AD configuration, NetWorker Authentication Service uses Microsoft specific enhancements for LDAP to perform optimized queries.<br>Default value: NO |
| -D "config-name=*authority_name*" | N/A | Required. A descriptive name, without spaces for the LDAP or AD configuration.<br>The maximum number of characters is 256. Specify ASCII characters in the config name only. |
| -D "config-server-address=*protocol://hostname_or_ip_address*:*port#/base_dn*" | protocol<br>serverName<br>portNumber | Required. A string that specifies the protocol, hostname, or IP address of the LDAP or AD server, the LDAP port number, and the base DN.<br>The base DN specifies the base suffix from which all the operations originate.<br>For the protocol, specify LDAP for LDAP or AD authorities and LDAPS for LDAPS.<br>**Note:** Use only FQDN in case of LDAPS configuration. |
| -D "config-domain=*domain_name*" | N/A | Required. A descriptive name, without spaces for the domain attribute in the local database. It is recommended that you specify the domain name that is used by the LDAP or AD authority.<br>The maximum number of characters is 256. Specify ASCII characters in the domain name only. |
| -D "config-user-dn=cn=*name*,dc=*domain_component1*,dc=*domain_component2...*" | bindDn | Required. The full distinguished name (DN) of a user account that has full read access to the LDAP or AD directory. |
| -D "config-user-dn-password=*password*" | bindPassword | Required. The password of the bind account. |
| -D "config-user-search-path=*user_search_path*" | userSearchPath | Required. The DN that specifies the search path that the authentication service should use when searching for users in the LDAP or AD hierarchy. Specify a search path that is relative to the base DN that you specified in the config-server-address option. For example, for AD, specify `cn=users`. |
| -D "config-user-id-attr=*user_ID_attribute*" | userIdAttribute | Required. The user ID that is associated with the user object in the LDAP or AD hierarchy. For LDAP, |

**Table 3** Configuration options (continued)

| Options for 9.x and later | Equivalent 8.2 and earlier option name | Description |
|---|---|---|
| | | this attribute is commonly `uid`. For AD, this attribute is commonly `sAMAccountName`. |
| -D "config-user-object-class=*user_object_class*" | userObjectClass | Required. The object class that identifies the users in the LDAP or AD hierarchy. For example, `inetOrgPerson`. |
| -D "config-group-search-path=*group_search_path*" | groupSearchPath | Required. A DN that specifies the search path that the authentication service should use when searching for groups in the LDAP or AD hierarchy. Specify a search path that is relative to the base DN that you specified in the **config-server-address** option. |
| -D "config-group-name-attr=*group_name_attribute*" | groupNameAttribute | Required. The attribute that identifies the group name. For example, `cn`. |
| -D "config-group-object-class=*group_object_class*" | groupObjectClass | Required. The object class that identifies groups in the LDAP or AD hierarchy.<br>• For LDAP, use `groupOfUniqueNames` or `groupOfNames`.<br>• For AD, use `group`. |
| -D "config-group-member-attr=*group_member_attribute*" | groupMemberAttribute | Required. The group membership of the user within a group.<br>• For LDAP:<br>▪ When the Group Object Class is `groupOfNames` the attribute is commonly `member`.<br>▪ When the Group Object Class is `groupOfUniqueNames` the attribute is commonly `uniquemember`.<br>• For AD, the value is commonly `member`. |
| -D "config-user-search-filter=*user_search_filter_name*" | N/A | Optional. The filter that the NetWorker Authentication Service can use to perform user searches in the LDAP or AD hierarchy. RFC 2254 defines the filter format. |
| -D "config-group-search-filter=*group_search_filter_name*" | N/A | Optional. The filter that the NetWorker Authentication Service can use to perform group searches in the LDAP or AD hierarchy. RFC 2254 defines the filter format. |
| -D "config-search-subtree=y/n" | N/A | Optional. A yes or no value that specifies if the external authority should perform subtree searches.<br>Default value: **No** |

**Table 3** Configuration options (continued)

| Options for 9.x and later | Equivalent 8.2 and earlier option name | Description |
|---|---|---|
| -D "config-user-group-attr=*user_group_attribute* " | N/A | Optional. This option supports configurations that identify the group membership for a user within the properties of the user object. For example, for AD, specify the attribute `memberOf`<br>**Note:** When you define this attribute, NetWorker Authentication Service does not have to browse the entire hierarchy to determine group membership for a user. |
| -D "config-object-class=*object_class*" | N/A | Optional. The object class of the external authentication authority. RFC 4512 defines the object class.<br>Default value: **objectclass**. |

**After you finish**

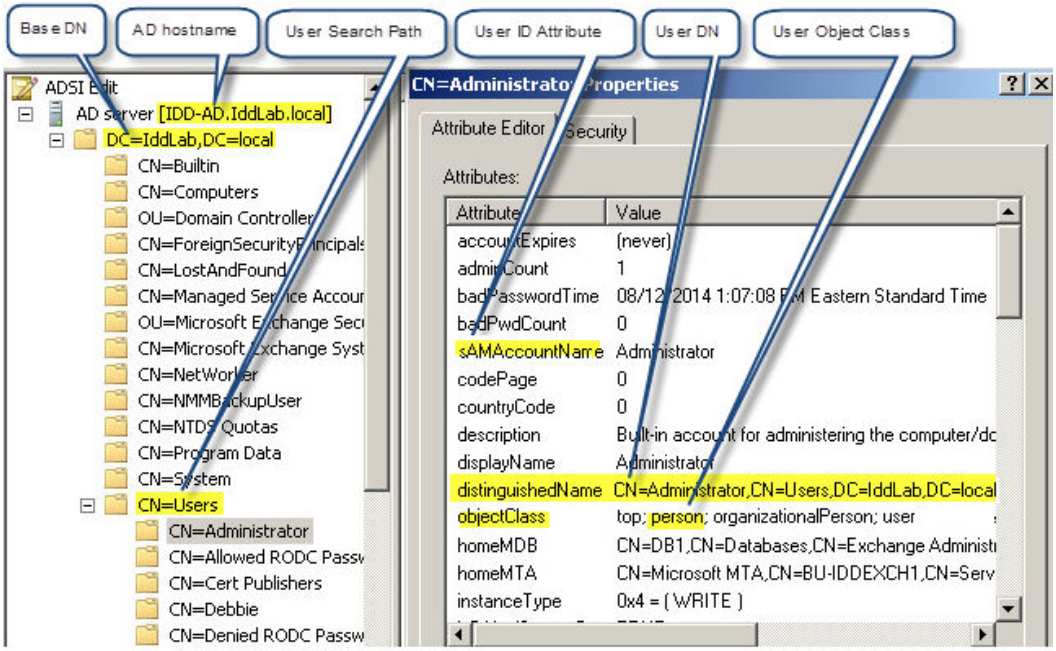
After you configure the NetWorker Authentication Service to use LDAP authentication, configure the NMC and NetWorker server to authorize the users.

## Example: Configuring an AD authority for user authentication in NMC and NetWorker

In this example, the Active Directory Services Interfaces Editor (ADSI Edit) program is used to view the properties of the AD configuration.

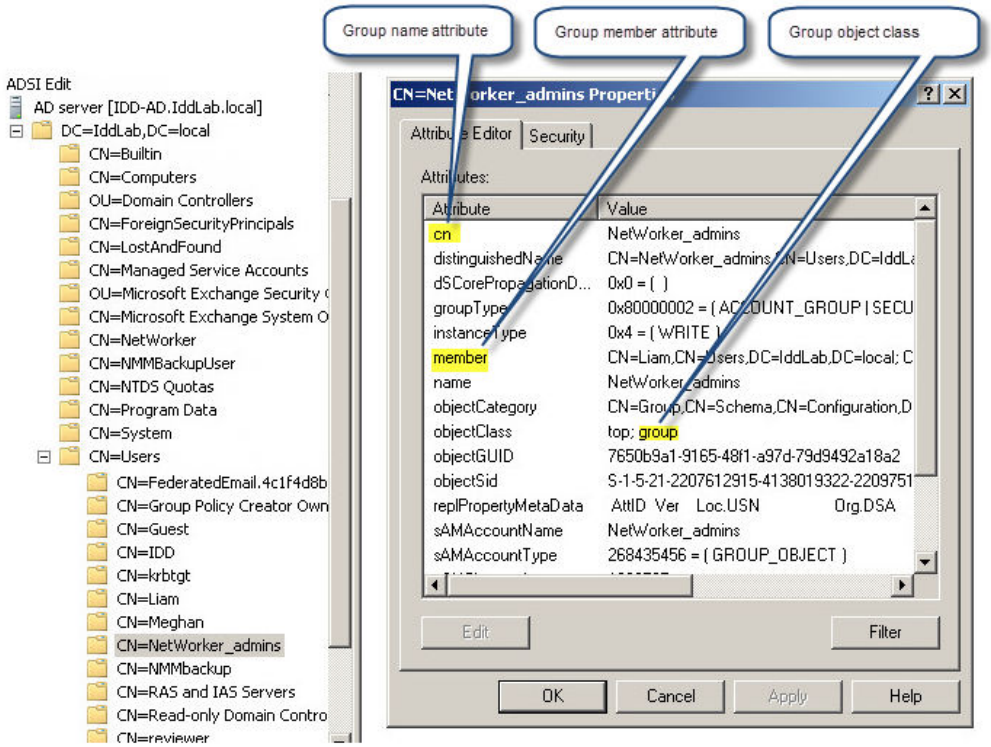
The following figure provides an example of the key user attributes to use when configuring an AD authority.

**Figure 4** User properties in ADSI Edit




The following figure provides an example of the key group attributes that you use when you configure the AD authority.

**Figure 5** Group properties in ADSI Edit




NetWorker provides a template file that you can modify with the configuration values that are specific to your environment, and then run to configure AD authentication.

The location and name of the file differs on Windows and Linux:

- AD template file:
  - Windows—`C:\Program Files\EMC NetWorker\nsr\authc-server\scripts\authc-create-ad-config.bat.template`
  - Linux—`/opt/nsr/authc-server/scripts/authc-create-ad-config.sh.template`

To use the template file, perform the following steps:

1. Use a text editor to open the file.
2. Replace the variables enclosed in <> with the values that are specific to your configuration. The following output provides an example of the contents of the file after substituting the attributes for your configuration:

```
authc_config -u administrator -p "1.Password" -e add-config
-D "config-tenant-id=33"
-D "config-name=iddconfig"
-D "config-server-address=ldap://idd-ad.iddlab.local:389/
dc=iddlab,dc=local"
-D "config-domain=idddomain"
-D "config-user-dn=cn=administrator,cn=users,dc=iddlab,dc=local"
-D "config-user-dn-password=1.Password"
-D "config-user-group-attr=memberof"
-D "config-user-id-attr=sAMAccountName"
-D "config-user-object-class=person"
-D "config-user-search-filter="
-D "config-user-search-path=cn=users"
-D "config-group-member-attr=member"
-D "config-group-name-attr=cn"
-D "config-group-object-class=group"
-D "config-group-search-filter="
-D "config-group-search-path="
-D "config-object-class=objectclass"
-D "config-active-directory=y"
-D "config-search-subtree=y"
```

   **Note:** In this example, to restrict NMC and NetWorker servers access to only users in the NetWorker_admins group, you must configure the NMC Roles on the NMC server and the User Groups resource on the NetWorker server. The section "User authentication and authorization" provides more information.

3. Save the file, and then remove the `.template` extension.
4. Use the `authc_mgmt` command with the `-e query-ldap-users` option along with the query-domain and query-tenant options to confirm that you can successfully query the AD directory:

```
authc_mgmt -u administrator -p "Password1" -e query-ldap-users -D
"query-tenant=IDD" -D
"query-domain=ldapdomain"
```

   Output similar to the following appears:

```
The query returns 15 records.
```

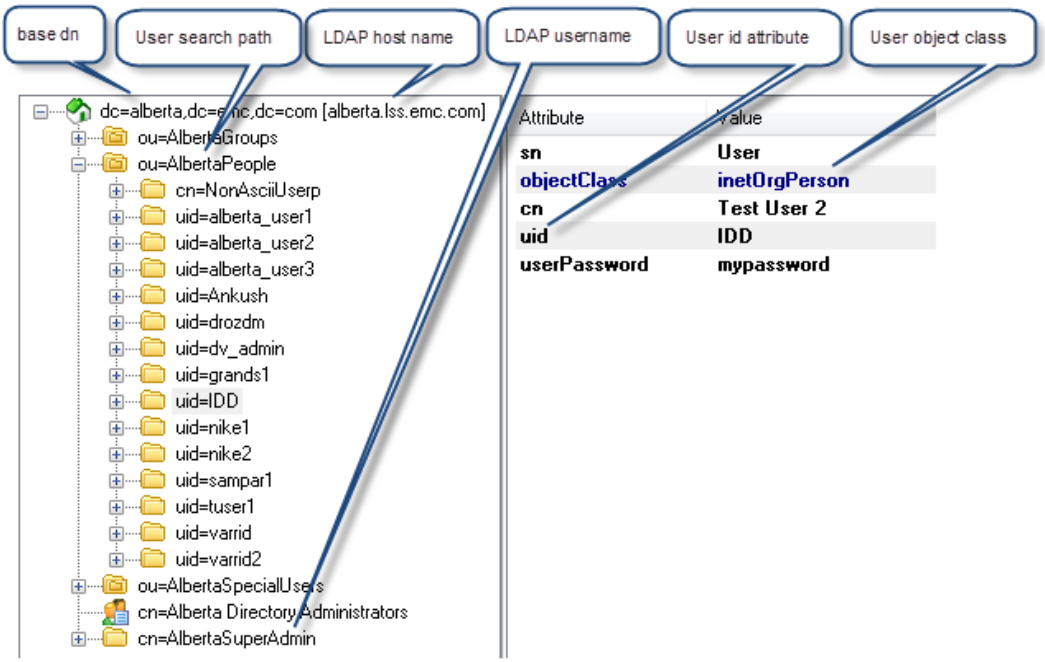
```
User Name Full Dn Name
alberta_user1
uid=alberta_user1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
alberta_user3
uid=alberta_user3,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
alberta_user2
uid=alberta_user2,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
drozdm uid=drozdm,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
tuser1
cn=NonAsciiUserp,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
tuser1 uid=tuser1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
grands1
uid=grands1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
varrid uid=varrid,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
dv_admin
uid=dv_admin,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
varrid2
uid=varrid2,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
Ankush uid=Ankush,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
IDD uid=IDD,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
nike1 uid=nike1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
nike2 uid=nike2,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
sampar1
uid=sampar1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
```

## Example: Configuring an LDAP authority for user authentication in NMC and NetWorker

In this example, a third party LDAP management tool, LDAPAdmin, is used to view the properties of the LDAP configuration.

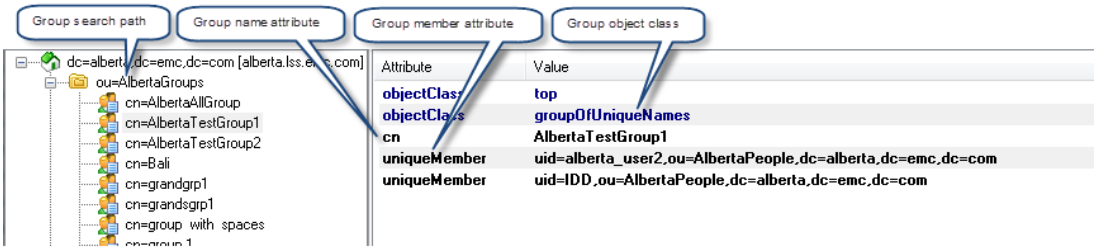
The following figure provides an example of the key user attributes to use when configuring an LDAP authority.

**Figure 6** User properties in LDAPAdmin




The following figure provides an example of the key group attributes that you use when configuring the LDAP authority.

**Figure 7** Group properties in LDAPAdmin




NetWorker provides a template file that you can modify with the configuration values that are specific to your environment, and then run to configure AD authentication.

The location and name of the file differs on Windows and Linux:

- LDAP template file:
  - Windows—`C:\Program Files\EMC NetWorker\nsr\authc-server\scripts\authc-create-ldap-config.bat.template`
  - Linux—`/opt/nsr/authc-server/scripts/authc-create-ldap-config.sh.template`

To use the template file, perform the following steps:

1. Use a text editor to open the file.
2. Replace the variables enclosed in <> with the values that are specific to your configuration. The following output provides an example of the contents of the file after substituting the attributes for your configuration:

```
authc_config -u administrator -p "Password1" -e add-config
-D "config-tenant-id=33"
-D "config-name=ldapconfig"
-D "config-server-address=ldap://alberta.lss.emc.com:389/
dc=lss,dc=emc,dc=com"
-D "config-domain=ldapdomain"
-D "config-user-
dn=cn=AlbertaSuperAdmin,dc=alberta,dc=emc,dc=com"
-D "config-user-dn-password=AlbertaPassword"
-D "config-user-group-attr=uniquemember"
-D "config-user-id-attr=uid"
-D "config-user-object-class=inetorgperson"
-D "config-user-search-path=ou=AlbertaPeople"
-D "config-group-member-attr=uniquemember"
-D "config-group-search-path=ou=AlbertaGroups"
-D "config-group-name-attr=cn"
-D "config-group-object-class=groupofuniquenames"
```

3. Save the file, and then remove the `.template` extension.
4. Execute the script file.
5. To confirm that you can successfully query the LDAP directory, use the `authc_mgmt` command with the *-e query-ldap-users* option:

```
authc_mgmt -u administrator -p "Password1" -e query-ldap-users -D
"query-tenant=IDD" -D
"query-domain=ldapdomain"
```

Output similar to the following appears:

```
The query returns 15 records.
User Name Full Dn Name
alberta_user1
uid=alberta_user1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
alberta_user3
uid=alberta_user3,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
alberta_user2
uid=alberta_user2,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
drozdm uid=drozdm,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
tuser1
cn=NonAsciiUserp,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
tuser1 uid=tuser1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
grands1
uid=grands1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
varrid uid=varrid,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
dv_admin
uid=dv_admin,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
varrid2
uid=varrid2,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
```

```
Ankush uid=Ankush,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
IDD uid=IDD,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
nike1 uid=nike1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
nike2 uid=nike2,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
sampar1
uid=sampar1,ou=AlbertaPeople,dc=alberta,dc=emc,dc=com
```

## Configuring LDAPS authentication

Before you configure the NetWorker Authentication Service to use LDAPS, you must store the CA certificate from the LDAPS server in the Java trust keystore.

### About this task

Perform the following steps on the NetWorker server.

### Procedure

1. Display a list of current trusted certificates in the trust keystore:

   ```
   java_path/bin/keytool -list -keystore
   java_path/lib/security/cacerts -storepass
   "password"
   ```

   where:

   - *java_path* is `/opt/nre/java/latest` on UNIX if NRE is installed. *java_path* is `/usr/java/latest` if NRE is not installed.
   - *java_path* is `C:\Program Files\NRE\Java` on Windows if NRE is installed. *java_path* is `C:\Program Files\Java` if NRE is not installed.
   - *"password"* is the Java trust keystore password.
     **Note:** By default the password is set to *changeit*.

2. (Optional) If the keystore contains expired trusted Java certificates for the LDAPS server, delete the certificates:

   ```
   java_path/bin/keytool -delete -alias
   LDAPS_server -keystore
   java_path/lib/security/cacerts -storepass
   "password"
   ```

   where:

   - *LDAPS_server* is the hostname of the LDAPS server.
   - *"password"* is the Java trust keystore password.

   **Note:** The time on NetWorker server must be in sync with the LDAPS server.

3. To obtain a copy of the CA certificate from the LDAPS server, use the `openssl` command:

   ```
   openssl s_client -showcerts -connect
   LDAPS_server:636
   ```

   where:

- *LDAPS_server* is the hostname of the LDAPS server.
- The `openssl` command may display two certificates. The last certificate is usually the CA certificate.

**Note:** By default, a Windows host does not include the `openssl` program. The OpenSSL website describes how to obtain an `openssl` program from a third party provider.

**Note:** Use only FQDN in case of LDAPS configuration.

4. Copy the CA certificate, including the -----BEGIN CERTIFICATE----- header and the -----END CERTIFICATE----- footer into a text file.

   For example:

```
-----BEGIN CERTIFICATE-----
aklfhskfadljasdl1340234234ASDSDFSDFSDFSDFSD
....
-----END CERTIFICATE-----
```

   **Note:** The `openssl` command may display two certificates. The second certificate is usually the CA certificate.

   To verify if the certificate is valid, run the following command:

```
openssl s_client -connect <LDAPS server:636> -
CAfile<certificate>
```

5. Add the certificate to the Java trust keystore:

```
java_path/bin/keytool -import -alias
LDAPS_server -keystore
java_path/lib/security/cacerts -storepass
"password" -file
certificate_file
```

   where:

   - *LDAPS_server* is the hostname of the LDAPS server.
   - *java_path* is `/opt/nre/java/latest` on UNIX if NRE is installed. *java_path* is `/usr/java/latest` if NRE is not installed.
   - *java_path* is `C:\Program Files\NRE\Java` on Windows if NRE is installed. *java_path* is `C:\Program Files\Java` if NRE is not installed.

6. When prompted to trust the certificate, type `Yes`, and then press **Enter**.
7. Restart the NetWorker server after importing the new certificate into the `cacerts store` file.

   **Note:** This step is mandatory in order for the newly imported certificate to get honored by the Authentication Service.

8. To configure LDAPS authentication authority in the NetWorker Authentication Service, use the `authc_config` command.

   For example:

```
authc_config -u administrator -p "1.Password" -e add-config
-D "config-tenant-id=33"
-D "config-name=LDAPS"
```

```
-D "config-domain=IDDS"
-D "config-server-address=ldaps://ldaps.emc.com:636"
-D "config-user-dn=cn=Directory Manager"
-D "config-user-dn-password=1.Password"
-D "config-user-id-attr=uid"
-D "config-user-object-class=inetOrgPerson"
-D "config-user-search-path=ou=People,dc=talisman-ds6,dc=com"
-D "config-group-member-attr=uniqueMember"
-D "config-group-name-attr=cn"
-D "config-group-object-class=groupOfUniqueNames"
-D "config-group-search-path=ou=Group,dc=talisman-ds6,dc=com"
-D "config-object-class=objectclass"
-D "config-active-directory=n"
-D "config-search-subtree=y"
```

```
Configuration LDAPS is created successfully.
```

**Note:** When you define the *config-server-address* option, ensure that you specify ldaps as the protocol and the appropriate LDAPS port number.

9. To confirm that you can successfully query the LDAP directory, use the `authc_mgmt` command with the **`-e query-ldap-users`** option. For example:

```
authc_mgmt -u administrator -p "1.Password" -e query-ldap-users
-D "query-tenant=IDD" -D "query-domain=IDDS"
```

Output similar to the following appears:

```
The query returns 12 records.
User Name Full Dn Name
Konstantin uid=Konstantin,ou=People,dc=talisman-ds6,dc=com
Katherine uid=Katherine,ou=People,dc=talisman-ds6,dc=com
Victoryia uid=Victoryia,ou=People,dc=talisman-ds6,dc=com
Patrick uid=Patrick,ou=People,dc=talisman-ds6,dc=com
Liam uid=Liam,ou=People,dc=talisman-ds6,dc=com
Meghan uid=Meghan,ou=People,dc=talisman-ds6,dc=com
```

## Troubleshooting LDAPS configuration

### Timestamp check failed

During LDAPS configuration, when you run `authc_config`, the following error occurs even when the certificate is not expired:

```
Error executing command. Failure: 400 Bad Request. Server message:
Failed to verify configuration LDAPS: An SSL handshake error occurred
while attempting to connect to LDAPS server: timestamp check failed.
```

### Workaround

- Ensure that the date and time on the NetWorker server is in sync with the LDAP server.

- Verify if the certificate is a valid one by running the **`openssl s_client -connect <LDAPS server:636> -CAfile <certificate>`** command. If the command returns the following message:

  ```
  Verify return code: 10 (certificate has expired)
  ```

  This message means that the certificate has expired and cannot be used. The `notAfter` field shows the validity of this certificate. Due to differences noticed in the output of the `keytool` command, it is recommended that you use the OpenSSL tool.

## Troubleshooting external authentication configuration issues

When the configuration for an external authentication authority is not correct, `authc_config` command may fail with an error message. Review this section for a summary of common error messages and possible resolutions.

### Error executing command. Failure: 400 Bad Request. Server message: Failed to verify configuration *config_name*: Authentication error occurred while accessing the naming or directory service: [LDAP: error code 49 - Invalid Credentials]

This error message appears when the external authentication authority cannot successfully validate the user credentials that were specified in the external authentication authority configuration.

To resolve this issue, correct the value defined in the *config-user-dn* or *config-user-dn-password* option.

### Error executing command. Failure: 400 Bad Request. Server message: Failed to verify configuration *config_name*: Error occurred while attempting to connect to a remote server '*hostname:port*'. Connection refused: connect

This error messages appears when the NetWorker Authentication Service cannot connect to the LDAP or AD server by using the port number specified in the *config-server-address* option in the external authentication authority configuration.

To resolve this issue, correct the port number defined in the *config-server-address* option.

### Error executing command. Failure: 400 Bad Request. Server message: Failed to verify configuration *config_name*: Cannot resolve host

This error messages appears when the NetWorker Authentication Service cannot resolve the host name of the LDAP or AD server specified in the *config-server-address* option in the external authentication authority configuration.

To resolve this issue, perform the following tasks:

- Ensure that the NetWorker server can resolve the hostname and IP address of the LDAP or AD server, and that the LDAP or AD server can resolve the hostname and IP address of the NetWorker server.
- Ensure that the hostname or IP address that you specified in the *config-server-address* option is correct.

### Error executing command. Failure: 400 Bad Request. Server message: Failed to verify configuration *config_name*: Error occurred while attempting to resolve component name '*component_name*'

This error message appears when the external authentication authority cannot successfully validate the user or group search path that was specified in the external authentication authority configuration.

To resolve this issue, correct the value defined in the *config-user-search-path* or *config-group-search-path* option.

**Error executing command. Failure: 400 Bad Request. Server message: Failed to verify configuration *config_name*: Error occurred while attempting to resolve component name '*component*'**

This error message appears when the external authentication authority cannot successfully validate the base DN specified in the *config-server-address*.

To resolve this issue correct the base DN value that is defined in the *config-server-address* option.

## Querying the LDAP or AD directory from NetWorker Authentication Service

Use the `authc_mgmt` command to perform queries of the LDAP or AD directory.

**Before you begin**

By default, the `authc_mgmt` command is in the `/opt/nsr/authc-server/bin` on Linux and `C:\Program Files\EMC NetWorker\nsr\authc-server\bin` on Windows.

**Procedure**

1. To display a list of existing configuration and determine the configuration ID for the external authority in the local database, use the `authc_config` with the *-e find-all-configs* option:

   ```
   authc_config -u username -p "password" -e find-all-configs
   ```

   For example:

   ```
   authc_config -u administrator -p "Password1" -e find-all-configs

   The query returns 1 records.
   Config Id Config Name
   40 iddconfig
   ```

2. To determine the properties of the provider configuration, use the `authc_config` with the *-e find-config* option:

   ```
   authc_config -u username -p "password" -e find-config -D
   "config-id=config_id"
   ```

   For example, to display information about the iddconfig configuration, type:

   ```
   authc_config -u administrator -p "Password1" -e find-config -D
   "config-id=40"
   Config Id : 40
   Config Tenant Id : 33
   Config Name : iddconfig
   Config Domain : idddomain
   Config Server Address : ldap://idd-ad.iddlab.local:389/
   dc=iddlab,dc=local
   Config User DN :
   cn=administrator,cn=users,dc=iddlab,dc=local
   Config User Group Attribute : memberof
   Config User ID Attribute : cn
   Config User Object Class : person
   Config User Search Filter :
   ```

```
Config User Search Path : cn=users
Config Group Member Attribute: member
Config Group Name Attribute : cn
Config Group Object Class : group
Config Group Search Filter :
Config Group Search Path :
Config Object Class : objectclass
Is Active Directory : true
Config Search Subtree : true
```

3. To determine the tenant name that is associated with the tenant, use the `authc_config` with the *-e find-tenant* option:

   **authc_config -u *username* -p *"password"* -e find-tenant -D "tenant-id=*tenant_id*"**

   For example, to display information about a tenant with tenant ID 33, type:

   ```
   authc_config -u administrator -p "Password1" -e find-tenant -D "tenant-id=33"
   Tenant Id : 33
   Tenant Name : IDD
   Tenant Alias : IDD-alias
   Tenant Details:
   ```

   To view all the available operations, use the **authc_config -help** command.

4. To query the external authority database, use the `authc_mgmt` command with one of the query options:

   **authc_mgmt -u *username* -p *"password"* -e *operation* -D "query-tenant=*tenant_name*" -D "query-domain=*local_database_domain_name*"**

   where *operation* is one of the following:

   - **query-ldap-users**—Specify this operation to generate a list of users in the external authority database.
   - **query-ldap-groups**—Specify this operation to generate a list of groups in the external authority database.
   - **query-ldap-users-for-group**—Specify this operation to generate a list of users in a specified group.
   - **query-ldap-groups-for-user**—Specify this operation to a display the group membership for the specified user.
     To view all the available operations, use the **authc_mgmt -help** command.

   For example, to display the group membership for a specific user in the iddconfig, perform the following steps:

   a. If the username is not known, to determine the username, use the `authc_mgmt` command with the *-e query-ldap-users* option. For example, type:

      `authc_mgmt` **-u administrator -p "1.Password" -e query-ldap-users -D "query-tenant=IDD" -D "query-domain=idddomain"**

      Output similar to the following appears:

      ```
      The query returns 7 records.
      User Name Full Dn Name
      ```

```
Administrator
cn=Administrator,cn=Users,dc=iddlab,dc=local
Konstantin cn=Konstantin,cn=Users,dc=iddlab,dc=local
Katherine cn=Katherine,cn=Users,dc=iddlab,dc=local
Viktoryia cn=Viktoryia,cn=Users,dc=iddlab,dc=local
Patrick cn=Patrick,cn=Users,dc=iddlab,dc=local
Liam cn=Liam,cn=Users,dc=iddlab,dc=local
Meghan cn=Meghan,cn=Users,dc=iddlab,dc=local
```

b. To determine the group membership for a user, use the `authc_mgmt` command with the *-e query-ldap-groups-for-user* option. For example, to display the group membership for the user **`Konstantin`**, type:

```
authc_mgmt -u administrator -p "Password1" -e query-ldap-
groups-for-user -D query-tenant=idd -D query-domain=idddomain
-D user-name=Konstantin
```

```
The query returns 1 records.
Group Name Full Dn Name

NetWorker cn=NetWorker,dc=iddlab,dc=local
```

## Troubleshooting external authentication authority configuration issues with authc_mgmt

When the configuration for an external authentication authority is not correct, `authc_mgmt` commands fail. Review this section for a summary of common error messages and possible resolutions.

### Error executing command. Failure: 400 Bad Request. Server message: Failed to verify configuration LDAPS: An SSL handshake error occurred while attempting to connect to LDAPS server: timestamp check failed

This error message is seen during an authc_config operation. You must ensure that the following requirements are met from the NetWorker server:

- Ensure that the date and time on NetWorker server is in sync with the LDAP server.
- Verify if the certificate is a valid one by running the **`openssl s_client -connect -CAfile`** command. If the command returns a "`Verify return code: 10 (certificate has expired)`" message, it means that the certificate has expired and cannot be used. The `notAfter` field shows the validity of the certificate.

### Error executing command. Failure: 400 Bad Request. Server message: Failed to perform LDAP task *task*: Authentication error occurred while accessing the naming or directory service: [LDAP: error code 49 - Invalid Credentials]

This error message appears when the external authentication authority cannot successfully validate the user credentials that were specified in the external authentication authority configuration.

To resolve this issue, correct the value defined in the *config-user-dn* or *config-user-dn-password* option.

For example, to update the value in the *config-user-dn-password* option in the *iddconfig* configuration, type the following command:

```
authc_config -u administrator -p "1.Password" -e update-config -D
config-id=1 -D "config-user-dn-password=MyPassword1"
Configuration iddconfig is updated successfully.
```

### Error executing command. Failure: I/O error on POST request for "*host*":Connection to *host* refused; nested exception is org.apache.http.conn.HttpHostConnectException: Connection to *host* refused

This error messages appears when the NetWorker Authentication Service cannot connect to the LDAP or AD server by using the port number specified in the *config-server-address* option in the external authentication authority configuration.

To resolve this issue, correct the port number defined in the *config-server-address* option.

For example, to update the *config-server-address* value in the *config-server-address* in the *iddconfig* configuration, type the following command:

```
authc_config -u administrator -p "1.Password" -e update-config -D
config-id=1 -D "config-server-address:ldap://idd-ad.iddlab.local:389/
dc=iddlab,dc=local"
Configuration iddconfig is updated successfully.
```

### Error executing command. Failure: 400 Bad Request. Server message: Failed to perform LDAP task *task*: Cannot resolve host 'hostname'

This error messages appears when the NetWorker Authentication Service cannot resolve the host name of the LDAP or AD server specified in the *config-server-address* option in the external authentication authority configuration.

To resolve this issue, perform the following tasks:

- Ensure that the NetWorker server can resolve the hostname and IP address of the LDAP or AD server, and that the LDAP or AD server can resolve the hostname and IP address of the NetWorker server.
- Ensure that the hostname or IP address that you specified in the *config-server-address* option is correct.

If required, update the *config-server-address* value. For example, to update the *config-server-address* value in the *config-server-address* in the *iddconfig* configuration, type the following command:

```
authc_config -u administrator -p "1.Password" -e update-config -D
config-id=1 -D "config-server-address:ldap://idd-ad.iddlab.local:389/
dc=iddlab,dc=local"
Configuration iddconfig is updated successfully.
```

## Managing the NetWorker Authentication Service local database

When you install and configure the NetWorker Authentication Service, you define the password for the administrator account for the NetWorker Authentication Service. The NetWorker Authentication Service maintains a local database of users and groups, which enables you to access the NetWorker Authentication Service securely.

A NetWorker Authentication Service administrator can use the following tools to manage the local database:

- To manage local database user accounts and groups, use the NMC GUI or the NetWorker Authentication Service `authc_mgmt` CLI tool.
  User names and group names cannot include spaces. The maximum number of characters for a user name or group name is 64.

> **Note:** A non-administrator account can use `authc_mgmt` to change their password.

- To manage local database permissions or local database password policies, use the NetWorker Authentication Service `authc_config` CLI tool.

## Using NMC to manage users and groups in the local database

Use NMC to create, delete, and modify users and groups in the local database.

### NMC service account

When you log in to the NMC server for the first time the configuration wizard creates a service account for the NMC server in the authentication service database.

The username of the service account is in the format **svc_nmc_*nmc_server_name***. The NMC server uses this account for interprocess communications between the NMC server and managed NetWorker server. For example, the NMC server uses the service account to gather reporting data.

It is recommended that you do not modify the properties of the service account.

If you delete the NMC service account, an error similar to the following appears in the `gstd.raw` file: `Unable to get token for service account of NMC server from authentication service..`

To recreate the NMC service account, perform the following steps:

1. Log in to the NMC server as a Console Security Administrator. The NetWorker Authentication Service administrator account is a Console Security Administrator.
2. On the **NMC Console** window, click **Setup**.
3. On the **Setup** window, from the **Setup** menu, select **Configure Service Account**.
4. Click **OK**.

### Using NMC to create or modify user accounts in the local user database

Perform the following steps to create users in the NetWorker Authentication Service local database.

**Before you begin**

Log in to the NMC server as a Console Security Administrator. The NetWorker Authentication Service administrator account is a Console Security Administrator.

**Procedure**

1. From the **Console** window, click **Setup**.
2. Perform one of the following steps:
   - To create a new user, right-click in the **Users** window pane, and then select **New**.
   - To modify an existing user, right-click the user account, and then select **Properties**.
3. For new users only, in the **User Name** field, specify the name for the user account, without spaces.

   The maximum number of allowed characters is 64.
4. (Optional) Specify information in the **First Name**, **Last Name**, **Email**, and **Description** fields.

5. In the **Groups** field, select the required NetWorker Authentication Service groups.
6. In the **NMC Role** field, select the roles that the user has on the NMC server. The NMC roles define the access level that the user has on the NMC server.

   **Note:** To manage users, the Console Security Administrator role requires that the user account to also be a member of the Administrators group. If you do not add a user with the Console Security Administrator role to an administrator group, the user can only manage NMC Roles.

7. In the **Password** and **Confirm Password** fields, specify a password for the user that meets the password policy settings that are defined for the environment.

   The default password policy requires that the password meets the following minimum requirements:

   - Nine characters long
   - One uppercase letter
   - One lowercase letter
   - One special character
   - One numeric character

   **Note:** Managing local database password policies on page 54 describes how to change the default password policy requirements.

8. (Optional) Enable or disable the **Password Never Expires** option.

   When you do not select this option, the default password expiration policy is 90 days.

9. (Optional) To force the user to change the password at the next log in try, enable the **Password Change Required** option.
10. (Optional) On the **Permissions** tab, define the NetWorker server hosts that the user can manage. The **Available Hosts** field provides a list of NetWorker server that this user cannot manage. The **Managed Hosts** field provides a list of NetWorker servers that the user can manage. To modify the list of NetWorker servers that the user can manage, use the **Add**, **Add All**, **Remove**, and **Remove All** buttons.

    **Note:** By default, a user can manage all the NetWorker servers in the Enterprise.

11. Click **OK**.

## Using NMC to delete a local database user

This section describes how to remove local database users.

### Before you begin

Log in to the NMC Server as a Console Security Administrator. The NetWorker Authentication Service administrator account is a Console Security Administrator.

### About this task

**Note:** The NetWorker Authentication Service requires the existence of at least one enabled user that is a member of a local group with FULL_CONTROL permission. To provide full control access to a group, type the following command:

```
authc_config -e add-permission -u username -p "password" -D
permission-name=permission -D permission-group-dn=group_dn-
patterns -D permission-group-dn-patterns=group_dn_pattern
```

**Procedure**

1. From the **Console** window, click **Setup**.
2. In the left pane, select **Users**.
3. Right-click the user, and then select **Delete**.
4. To confirm the deletion, click **Yes**.

   If the user had saved customized reports, a dialog box prompts for the username to reassign to those reports. Otherwise, you can delete the reports.

## Using authc_mgmt to manage users and groups in the local database

To manage users and group in the local database, use the `authc_mgmt` command. By default, the `authc_config` command is in the `/opt/nsr/authc-server/bin` on Linux and `C:\Program Files\EMC NetWorker\authc-server\bin` on Windows.

### Creating groups

To create a new group, use the *-e add-group* option:

```
authc_mgmt -u administrator -p "password" -e add-group -D "group-
name=group_name" [-D "group-details=description"] [-D "group-
users=userID1, userID2..."]
```

**Note:** Do not include spaces in the group name.

For example, to create a group that is named test, type the following command:

```
authc_mgmt -u administrator -p "1.Password" -e add-group -D "group-
name=test" -D "group-details=New local database group"
```

Group is created successfully.

### Viewing group information

To view information about a specific group, use the *-e find-group* option:

```
authc_mgmt -u administrator -p "password" -e find-group -D group-
name=group_name
```

To display information about a group named test, type the following command:

```
authc_mgmt -u administrator -p "1.Password" -e find-group -D "group-
name=test"
Group Id : 132
Group Name : test
Group Details: New local database group
Group DN : cn=test,cn=Groups,dc=bu-
iddnwserver2,dc=IddLab,dc=local
Group Users : []
```

**Note:** You specify the group ID value when you create a user or add a user to an existing group.

### Creating users

To create a user, use the *-e add-user* option:

```
authc_mgmt -u administrator -p "password" -e add-user -D "user-
name=user_name" [-D "user-password=password"] [-D "user-first-
name=firstname"] [-D "user-last-name=last_name"] [-D "user-
details=description" [-D "user-email=email_address"] [-D "user-
groups=group_ID1,group_ID2..."] [-D "user-enabled=yes_or_no"
```

**Note:** Do not include spaces in the user name.

For example, to create a user account `PatD` and add the account to a group named test, type:

```
authc_mgmt -u administrator -p "1.Password" -e add-user -D "user-
name=PatD" -D "user-password=Password1" -D "user-first-name=Patrick" -
D "user-last-name=Dunn" -D "user-details=test user" -D "user-
groups=132" -D "user-enabled=yes"
User PatD is created successfully.
```

### Displaying a list of users

To display a list of users, use the *-e find-all-users* option:

```
authc_mgmt -u administrator -p "password" -e find-all-users

The query returns 2 records.
User Id User Name
1000 administrator
1001 svc_nmc_bu-iddnwserver2
```

### Updating personal user account information

To update the personal information for an existing user, use the *-e update-user* option:

```
authc_mgmt -u administrator -p "password" -e update-user -D "user-
name=user_name" -D "option=value"
```

For example, to update the email address for the user account `PatD`, type the following command:

```
authc_mgmt -u administrator -p "1.Password" -e update-user -D "user-
name=PatD" -D "user-email=patd@emc.com"
User PatD is updated successfully.
```

### Displaying personal information for a user account

To display personal information about an existing user, use the *-e find-user* option:

```
authc_mgmt -u administrator -p "password" -e find-user -D "user-
name=user_name"
```

For example, to view details about the user account `PatD`, type:

```
authc_mgmt -u administrator -p "1.Password" -e find-user -D "user-
name=PatD"
User Id : 1064
User Name : PatD
User Domain :
User First Name: Patrick
User Last Name : Dunn
User Email : patd@emc.com
User Details : test user
```

```
User DN : cn=PatD,cn=Users,dc=bu-
iddnwserver2,dc=IddLab,dc=local
User Enabled : true
User Groups : [132]
```

### Updating user options

To update user options for a specific user, use the *-e update-user-options* option:

```
authc_mgmt -u administrator -p "password" -e update-user-options -D
"user-options-userid=userid_for_user" -D "option_name=value"
```

For example, to set the *user-must-change-password* option for the user *Patd*, type:

```
authc_mgmt -u administrator -p "1.Password" -e update-user-options -D
"user-options-userid=1064" -D "user-
options-password-must-change=true"
The user options for user 1,064 is updated successfully.
```

The user cannot manage the NetWorker Authentication Service until the password is changed. For example:

```
authc_mgmt -u patd -p "1.Patrick2" -e find-all-user-options
Error executing command. Failure: 401 Unauthorized. Server
message: Unauthorized access: user Patd must change password
```

The `authc_mgmt` UNIX man page and the *NetWorker Command Reference Guide* provides detailed information about all the configuration options.

## Using authc_config to manage local database permissions

NetWorker Authentication Service has two types of user access permissions to the local database, FULL_CONTROL and Everyone. By default, a new local user has "Everyone" access to the local database. NetWorker Authentication Service allows you to assign FULL_CONTROL permissions to a local or LDAP/AD group. Users in a group with full control access can manage and configure local database resources. A user with "Everyone" access can only update user information about their user account and query the NetWorker Authentication Service for API version and certificate information.

To provide full control access to a group, type the following command:

```
authc_config -e add-permission -u username -p "password" -D
permission-name=permission -D permission-group-dn=group_dn-patterns -D
permission-group-dn-patterns=group_dn_pattern
```

For example, to add the FULL_CONTROL permission to a local group called **authgroup**, perform the following steps:

1. To determine the Group DN, use *-e find-group* option:

   ```
   authc_mgmt -e find-group -u administrator -p "1.Password" -D group-
   name=authgroup
   ```

   ```
   Group Id : 164
   Group Name : authgroup
   Group Details:
   Group DN : cn=authgroup,cn=Groups,dc=bu-
   iddnwserver2,dc=IddLab,dc=local
   Group Users : PatD
   ```

2. Use the *-e add-permission* option to add the FULL_CONTROL permission to the authgroup:

```
authc_config -e add-permission -u administrator -p "1.Password" -D
permission-name=FULL_CONTROL -D permission-group-
dn=cn=authgroup,cn=Groups,dc=bu-iddnwserver2,dc=IddLab,dc=local
Permission FULL_CONTROL is created successfully
```

3. To confirm the properties of the group, use the *-e find-all-permissions* option:

```
authc_config -e find-all-permissions -u administrator -p
"Password1"


Permission Id Permission Name Group DN Pattern Group DN
1 FULL_CONTROL ^cn=Administrators,cn=Groups.*$
2 FULL_CONTROL cn=authgroup,cn=Groups,dc=bu-iddnw...
```

**Note:** The output abbreviates the Group DN Pattern and Group DN values. Use the *find-permission* option to see the complete value information.

The UNIX man page and the *NetWorker Command Reference Guide* provides detailed information about how to use `authc_config` to manage permissions.

## Changing the password for a local user

By default, the NetWorker Authentication Service password policy enforces password expiration for local user accounts. A NetWorker Authentication Service administrator can change the password for any local user. A non-administrator user can only change their own password.

### About this task

Use the `authc_mgmt` tool to change the password for a local database user. The command to change the password differs, depending on the user that changes the password.

- To change the password for the administrator account, or for a non-administrator user to change their password, use the *-e update-password* option:

  ```
  authc_mgmt -u username -p "current_password" -e update-password -D
  password-new-value="new_password"
  ```

  where:

  - *"username"* is the name of the user whose password you want to change, or local administrator account.
  - *"current_password"* is the current password for the username that you specified.
  - *"new_password"* is the new password for the username that you specified.

  For example, to change the password for the local administrator account, type the following command:

  ```
  authc_mgmt -u administrator -p "1.Password" -e update-password -D
  password-new-value="1.Updated2"
  ```

  **Note:** To change the password without typing the new password in the command string, do not include the *-D password-new-value="new_password"*

option. The command will prompt you for the new password and will not display the characters.

- To use the administrator account to change the password for any user, use the *-e update-user* option with the *-D user-name* and *-D user-password* options:

  ```
  authc_mgmt -u administrator -p "current_password" -e update-user -D
  user-name=username -D user-password="new_password"
  ```

  where:

  - *"current_password"* is the password for the administrator account.
  - *"username"* is the name of the user whose password you want to change.
  - *"new_password"* is the new password that you want to set for the user.

  For example, to change the password for a local user who is named `Noelle` to `".Mynewpass1"`, type the following command:

  ```
  authc_mgmt -u administrator -p "1.Password" -e update-user -D user-
  name=Noelle -D user-password=".Mynewpass1"
  ```

## Resetting the administrator password

To reset the administrator password, create a JSON file on the NetWorker server that contains the new password in a Base64 encoded format.

**Procedure**

1. To determine the Base64 password value for the new password, use Base64 encoding utilities:

   - On Windows, perform the following steps:

     a. Create a text file and specify the password value in clear text, on one line.
     For example, create a password file that is called *mypassword_in.txt* with the password value *"1.Password".*

     b. To create a Base64 encoded password for the password value that is defined in the *mypassword_in.txt* file, use the `certutil.exe` utility. For example:

     ```
     certutil.exe -encode mypassword_in.txt mypassword_out.txt
     ```

     where *mypassword_out.txt* is the name of the output file that contains the Base64 encoded password.

     Output similar to the following appears:

     ```
     Input Length = 10
     Output Length = 74
     CertUtil: -encode command completed successfully.
     ```

     The contents of the *mypassword_out.txt* file contains the following encoded text for the password value *"1.Password"*:

     ```
     -----BEGIN CERTIFICATE-----
     MS5QYXNzd29yZA==
     -----END CERTIFICATE-----
     ```

     where the Base64 encoded password is *MS5QYXNzd29yZA==*.

   - To create the Base64 encoded password on Linux, use the `base64` utility.

For example, to create the Base64 encoded password for a password value of *"1.Password"*, type:

```
echo -n "1.Password" | base64
```

The command displays the encoded text for the password value **"1.Password"**: MS5QYXNzd29yZA==

2. Use a text editor to open the `authc-local-config.json.template` file, which is located in the `C:\Program Files\EMC NetWorker\nsr\authc-server\scripts` folder on Windows and the `/opt/nsr/authc-server/scripts` directory on Linux.
3. In the template file, perform the following steps:
   a. Replace the *your_username* variable with the name of the administrator account for which you want to reset the password.
   b. Replace the *your_encoded_password* variable with the base64 encoded password value.

   For example, to reset the password for the user account administrator with a password of *"1.Password "*, the modified file appears as follows:

```
{
"local_users": [
{
"user name": "administrator",
"password": "MS5QYXNzd29yZA=="
}]
}
```

4. Rename the `authc-local-config.json.template` file to `authc-local-config.json`.
5. Copy the `authc-local-config.json` file to the `Tomcat conf` folder.

   By default, the conf folder is `/nsr/authc/conf` on Linux and `C:\Program Files\EMC NetWorker\authc-server\tomcat\conf` on Windows.

6. Change privileges on the `authc-local-config.json` file:

```
chmod 755 /nsr/authc/conf/authc-local-config.json
```

   If you do not change the privileges, the `authc-server.log` displays an error indicating that you do not have the necessary permissions to open the file.

7. On the NetWorker server, stop, and then start the services:
   - For Windows, type the following commands from a command prompt:

```
net stop nsrexecd

net start nsrd
```

     **Note:** If the NetWorker server is also the NMC server, start the NMC server service. Type the following commands: **`net start gstd`**

   - For Linux, type the following commands:

```
/etc/init.d/networker stop
/etc/init.d/networker start
```

   When the NetWorker Authentication Service starts, the startup process checks for the `authc-local-config.json`. If the file exists and the password

adheres to the minimum password policy requirements defined for a password, the NetWorker Authentication Service resets the password. Review the `authc-server.log` file for errors.
By default, the `authc-server.log` file is located in `/nsr/authc/logs` on Linux and `C:\Program Files\EMC NetWorker\authc\tomcat\logs` on Windows.

> **Note:** The startup process automatically deletes the `authc-local-config.json` file to ensure that the password is not reset the next time that you restart the NetWorker Authentication Service.

8. To confirm that you can connect to the NetWorker Authentication Service with the new password, use the `authc_mgmt` command.

   For example:

```
authc_mgmt -u administrator -p "1.Password" -e find-all-users


The query returns 2 records.
User Id User Name
1000 administrator
1001 svc_nmc_bu-iddnwserver2
```

## Harden the Authentication Service on port 9090

Perform the following steps to harden the Authentication Service on port 9090:

**Procedure**

1. On the NetWorker server, stop the NetWorker services.
2. Edit the `server.xml` file with a text editor.

   The location of the file differs on Windows and Linux:

   - Windows: `C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat\conf`
   - Linux: `/nsr/authc/conf`

3. Search for the string `Connector port = 9090`.

```
<Connector port="9090"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="/nsr/authc/conf/authc.keystore " keystorePass="$
{keystore.password}"
keyAlias="emcauthctomcat" keyPass="${tckey.password}"
clientAuth="false" sslProtocol="TLS"
sslEnabledProtocols="TLSv1.2, TLSv1.1, TLSv1"
ciphers="TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
```

```
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_GCM_SHA384" />
```

4. Remove the specific TLS versions and ciphers.
   - Hardening TLS Protocol- Your organization may require that certain TLS protocols are disabled and not used. This hardening can be done by editing the **sslEnabledProtocols** and removing the TLS settings that are not needed. The following is set by default:

     ```
     sslEnabledProtocols="TLSv1.2, TLSv1.1, TLSv1"
     ```

     To disable TLS 1.0 and TLS 1.1, update to indicate the following:

     ```
     sslEnabledProtocols="TLSv1.2"
     ```

   - Hardening Supported Ciphers- Your organization may require that certain ciphers are disabled and not used. This hardening can be done by editing the ciphers setting and removing the cipher settings that are not needed. The following is set by default:

     ```
     ciphers="TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
     TLS_RSA_WITH_AES_128_CBC_SHA,
     TLS_RSA_WITH_AES_128_CBC_SHA256,
     TLS_RSA_WITH_AES_128_GCM_SHA256,
     TLS_RSA_WITH_AES_256_CBC_SHA,
     TLS_RSA_WITH_AES_256_CBC_SHA256,
     TLS_RSA_WITH_AES_256_GCM_SHA384"
     />
     ```

5. Save the `server.xml` file.
6. On the NetWorker server, start the NetWorker services.

## Increasing the header size of the Apache tomcat

If you have configured external authority properly(LDAP) and not able to login to VMware backup and recovery plugin with AD, then you must consider increasing the header size.

**About this task**

Perform the following steps to increase the header size of Apache tomcat:

**Procedure**

1. On the NetWorker server, stop the NetWorker services.
2. Edit the server.xml file with a text editor.

   The location of the file differs on Windows and Linux.

   - Windows- `C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat\conf`

- Linux- `/nsr/authc/conf`

3. Search for the string maxHttpHeaderSize="131072"
4. Change the value to maxHttpHeaderSize="10485760"
5. Save the server.xml file.
6. On the NetWorker server, start the NetWorker services.

# Managing the NetWorker Authentication Service options

You can manage how NetWorker Authentication Service implements password policies and tokens. You can also perform queries for general information about the NetWorker Authentication Service.

## Managing token policies

Use the `authc_config` command to manage NetWorker Authentication Service. Token policies allow you to configure the expiration timeout for a token and the acceptable time difference for the token start timestamp. NetWorker Authentication Service allows you to configure two token options TokenStartTimeDeltaInMinutes and TokenTimeoutInMInutes.

### TokenStartTimeDeltaInMinutes

Defines the maximum time difference in minutes that the NetWorker server accepts when validating the start time of a token. The default value is -5. Use this value to ensure that when the NetWorker server validates the token start time, the service does not reject the token because of unsynchronized clocks in the NetWorker datazone.

**Note:** The `TokenStartTimeDeltaInMinutes` parameter is case sensitive.

To modify the *TokenStartTimeDeltaInMinutes* property, use the *-e add-option* option:

```
authc_config -u username -p "password" -e add-option -D option-
name=TokenStartTimeDeltaInMinutes -D option-value=time_in_minutes
```

For example, to change the *TokenStartTimeDeltaInMinutes* to -15, perform the following steps:

1. To change the default value, use the *-e add-option* option:

   ```
   authc_config -u administrator -p "Password1" -e add-option -D
   option-name=TokenStartTimeDeltaInMinutes -D option-value=-15
   ```

   ```
   Option TokenStartTimeDeltaInMinutes is created successfully.
   ```

2. To confirm the change, use the *-e find-option*:

   ```
   authc_config -u administrator -p "Password1" -e find-option -D
   option-name=TokenStartTimeDeltaInMinutes
   ```

   ```
   Option Id: 2
   Name : TokenStartTimeDeltaInMinutes
   Value : -15
   ```

### TokenTimeoutInMinutes

The SAML token expiration timeout in minutes. The default value is 480 minutes (8 hours).

**Note:** The `TokenTimeoutInMIintes` parameter is case sensitive.

To modify the *TokenTimeoutInMIintes* property, type the following command:

```
authc_config -u username -p "password" -e add-option -D option-name=TokenTimeoutInMinutes -D option-value=time_in_minutes
```

For example, to change the *TokenTimeoutInMinutes* to 12 hours (720 minutes), perform the following steps:

1. To change the default value, use the *-e add-option* option:

   ```
   authc_config -u administrator -p "Password1" -e add-option -D option-name=TokenTimeoutInMinutes -D option-value=720
   ```

   ```
   Option TokenTimeoutInMinutes is created successfully.
   ```

2. To confirm the change, use the *-e find-option* option :

   ```
   authc_config -u administrator -p "Password1" -e find-option -D option-name=TokenTimeoutInMinutes
   ```

   ```
   Option Id: 3
   Name : TokenTimeoutInMinutes
   Value : 720
   ```

## Modifying the token expiration timeout interval in NMC

NMC provides you with the ability to change the token expiration timeout interval. NetWorker enforces the new interval after the current token expires.

**Before you begin**

Log in to the NMC server as a Console Security Administrator. The NetWorker Authentication Service administrator account is a Console Security Administrator.

**Procedure**

1. On the toolbar, click **Setup**.
2. From the **Setup** menu, select **Configure Authentication Service Token Timeout**.
3. In the **Token Timeout** box, specify a period in hours or days.
4. Click **OK**.

   **Note:** If you change the **Token Timeout** value, you must restart the `gstd` service.

# Managing local database password policies

Use the `authc_config` command to control the password policy requirement for user accounts.

The following table provides a summary of the default password policy requirements for users in the local database.

**Table 4** Default password policy requirements

| Password policy option | Description |
|---|---|
| PasswordMinLengthCharacters | Minimum number of required characters in a password. The default value is 9. |
| PasswordMaxLengthCharacters | Maximum number of characters that are allowed for a password. The default value is 126. |
| PasswordMinAlphabeticCharacters | Minimum number of required alphabetic characters in a password. The default value is 2. |
| PasswordMinLowerCaseCharacters | Minimum number of required lowercase characters in a password. The default value is 1. |
| PasswordMinUpperCaseCharacters | Minimum number of required uppercase characters in a password. The default value is 1. |
| PasswordMinNumericalCharacters | Minimum number of required numeric characters in a password. The default value is 1. |
| PasswordMinSpecialCharacters | Minimum number of required special characters in a password. The default value is 1. |
| PasswordSpecialCharacters | List of the characters that the NetWorker Authentication Service considers special, to satisfy the PasswordMinSpecialCharacters password policy requirement. Default special characters include the following list: !@#$%^&*()_-+=~{}[]<>?/`:;',.\|\" |
| PasswordExpirationDays | Maximum number of days that a user can use a password before the user must change the password. The default value is 90. |
| PasswordHistoryCount | Maximum number of passwords that the NetWorker Authentication Service remembers for a user account, to ensure that the user does not reuse a stored password. The default value is 8. |

To control the password policy requirement for user accounts, perform the following steps:

- To modify password policy requirements, type the following command:

  **authc_config -u *username* -p "*password*" -e add-option -D option-name=*option* -D option-value=*value***

  where *option* is one of the password policy options in the previous table.

  For example, to change the default password expiration policy from 90 days to 30 days, type:

  **authc_config -e add-option -u administrator -p "1.Password" -D "option-name=PasswordExpirationDays" -D "option-value=30"**

  ```
  Option PasswordExpirationDays is created successfully.
  ```

- To review a list of all the options that have been modified from the default value, type:

  **authc_config -u *username* -p "*password*" -e find-all-options**

  For example:

```
authc_config -u administrator -p "1.Password" -e find-all-options
The query returns 1 records.
Option Id Name
1 PasswordExpirationDays
```

> **Note:** The `find-all-options` operation does not display options that you have not changed from the default values.

- To review the details about a specific option that has been modified from the default value, type:

  **`authc_config -u`** ***`username`*** **`-p`** ***`"password"`*** **`-e find-option -D option-id=`**`option_id`

  where *option_id* is the option ID value that appears in the `find-all-options` output for the password policy option.

  For example, to display the details about the PasswordExpirationDays option, type:

```
authc_config -u administrator -p "1.Password" -e find-option -D
"option-id=1"
Option Id: 1
Name : PasswordExpirationDays
Value : 30
```

## Configure CLI options

To define default argument values for commonly used options or the settings that are required by the `authc_mgmt` and `authc_config` commands, modify the `authc-cli-app.properties` file. When you define default argument values in the `authc-cli-app.properties`, you do not have to specify the option when you use the `authc_mgmt` and `authc_config` commands.

- UNIX—The `authc-cli-app.properties` file is located in the `/opt/nsr/authc-server/conf` folder.
- Windows—The `authc-cli-app.properties` file is located in the `C:\Program Files\EMC NetWorker\nsr\authc-server\conf` directory.

The following table summarizes the arguments that you can define for the CLI commands.

**Table 5** NetWorker Authentication Service CLI options

| Argument | Purpose |
|---|---|
| admin_service_default_protocol | Defines the web protocol to use when you connect to the NetWorker Authentication Service. The default value is https. |
| admin_service_default_url | Defines the url to use when you connect to the NetWorker Authentication Service. The default value is localhost. |
| admin_service_default_port | Defines the port number to use when communicating with the NetWorker Authentication Service. The default value is 9090. |
| admin_service_default_tenant | Defines the tenant to use, to validate the username that you specify with the CLI command. When you use this option, you do not require the -t argument to define a username that is not in the Default tenant. |

**Table 5** NetWorker Authentication Service CLI options (continued)

| Argument | Purpose |
|---|---|
| admin_service_default_domain | Defines the default domain to use to validate the username that you specify with the CLI command. When you use this option, you do not require the -d argument to define a username that is not in the Default domain. |
| admin_service_default_user | Defines the username that runs the CLI command. When you use this option, you do not require the -u argument with the CLI commands. |
| admin_service_default_password | Defines the password of the user that runs the CLI command. When you use this option, you do not require the -p argument with the CLI commands. |

## Changing the NetWorker Authentication Service port

Perform the following steps to change the port that the NetWorker Authentication Service uses for communication.

**Procedure**

1. On the NetWorker server, stop the NetWorker services.
2. Edit the `server.xml` file with a text editor.

   The location of the file differs on Windows and Linux:

   - Windows: `C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat\conf`
   - Linux: `/nsr/authc/conf`

3. Search for the string `Connector port`.
4. Modify the connector port value.

   Ensure that you specify an unused port that is in the range of 1024-49151.

   For example, to change the port to 9091, the connector port entry would appear as follows:

   ```
   <Connector port="9091"
   protocol="org.apache.coyote.http11.Http11NioProtocol"
   SSLEnabled="true"
   ```

5. Save the `server.xml` file.
6. Edit the `authc-server-app.json` file with a text editor.

   The location of the file differs on Windows and Linux:

   - Windows: `C:\Program Files\EMC NetWorker\authc-server\conf`
   - Linux: `/opt/nsr/authc-server/conf`

7. Search for the string `port`.
8. Modify the port value.

   For example, to change the port to 9091, the port entry would appear as follows:

```
"port" : "9091"
```

9. Save the `authc-server-app.json` file.
10. On the NetWorker server, start the NetWorker services.

# How user authentication and authorization works in NMC and NetWorker

User authentication settings control the processes that the NetWorker Management Console (NMC) and the NetWorker software applications use to verify the identity that is claimed by a user. User authorization settings control the rights or permissions that are granted to a user and enable access to resources managed by NetWorker and the NMC server.

## NMC server authentication and authorization

When you use a web browser on a host (NMC client) to connect to the NMC Server, ensure that you log in with a valid username and password. Specify the username in one of the following formats:

- For LDAP/AD authentication: *domain\username*
- For local user database authentication: *username*
- For tenant configurations: *tenant\domain\username*

The http daemon on the NMC server downloads the Java client to the NMC client. You do not require a secure http (https) connection because only the Java client transfers information and performs authentication between the NMC server and NMC client. The NMC server contacts the NetWorker Authentication Service to validate the user log in credentials. When the NetWorker Authentication Service successfully validates the credentials, the application issues an authentication token for the user, to the NMC server. The NMC server caches the token.

To set the level of access that the user has to the NMC server, assign NMC roles to an LDAP or AD user or group. NMC roles define the NMC activities that a user is authorized to perform.

## NetWorker Administration authentication and authorization

When the user tries to establish a connection to the NetWorker server by opening the **NetWorker Administration** window, the NMC server confirms that the user has access permissions to manage the NetWorker server. If the user has the appropriate permissions, the NMC server sends the token to the NetWorker server. You can restrict or grant access to a NetWorker server by settings permissions on the NetWorker server for the authenticated user. NetWorker uses the token of the user that you specified when you logged in to the NMC GUI to authenticate and authorize the operations that are performed in the **NetWorker Administration** window. The privileges that are assigned to an authenticated user on the NetWorker server are based on the entries present in the Users or External roles attribute of the User Group resources on the NetWorker server. User group membership defines which NetWorker activities the user is authorized to perform. When you use token-based authentication, NetWorker uses the External roles attribute in the User group resource to determine user membership. When you do not use token-based authentication, NetWorker uses the User attribute in the User group resource to determine membership.

Operations that you perform in the NMC GUI always use token-based authentication. The privileges that are assigned to the user to perform NMC server operations, for example adding new local database users are determined by user or group membership in External roles attribute of the NMC Roles resources.

NMC server authorization on page 60 provides more information about NMC roles.

Operations that you perform in the NetWorker Administration GUI always use token-based authentication. As a result, NetWorker uses the users and groups that are specified in the External roles attribute of a User Group to determine the privileges that are assigned to the user that begins the operation.

User group management on page 74 provides more information about the User Group resource.

### Client-initiated backup and recovery authentication and authorization

To use token-based authentication with a command line (CLI) backup or recovery operation on a NetWorker host, first run the `nsrlogin` command. When you run the `nsrlogin` command, the NetWorker host contacts the NetWorker Authentication Service to validate the user log in credentials. When the NetWorker Authentication Service successfully validates the credentials, the application issues an authentication token to the NetWorker host for the user account that you used to run the command. The NetWorker host caches the token and confirms that the user account has the appropriate privileges to perform the operation. The user account can perform secure client-initiated backup and recovery operations with the authenticated user until the token expires or a user runs the `nsrlogout` command.

**Note:** When you do not use the `nsrlogin` command to enable token-based authentication, NetWorker uses the NetWorker 8.2.x and earlier authentication method. This authentication method relies on operating system authentication to validate the user privileges.

### Token expiration

The token policies that are defined in the NetWorker Authentication service database determine how long a token remains valid:

- When the token for a CLI authenticated user expires, in-progress user-initiated operations complete, but the user cannot start new operations until a new token is issued to the user. To issue a new token for a CLI operation, the user must run the `nsrlogin` command again.
- When the token expires while a user is connected to the **NetWorker Administration** window, a token expiration message appears and the connection to the NetWorker server closes. A prompt appears requesting that the user specify their password and generate a new token. After a new token is issued, the user can re-establish the connection to the NetWorker server.
- When the token expires while a user is connected to the NMC GUI, a token expiration message appears and the user is prompted to specify their password and generate a new token. After a new token is issued, the user can use the NMC GUI.

Troubleshooting authorization errors and NetWorker server access issues on page 81 provides more information about how to resolve token expiration messages that appear on a NetWorker server.

## Modifying authentication methods for NetWorker servers in NMC

You can restrict or grant access to a NetWorker server based on the authenticated user. Requests to NetWorker servers through the NetWorker Administration window always come from the NMC server. The privileges that are assigned to an authenticated user on the NetWorker server are based on the entries present in the Users or External roles attribute of the User Group resources on the NetWorker server.

The NMC server controls how an authenticated user accesses a managed NetWorker server. When you enable the **User Authentication for NetWorker** system option on the NMC server, you can grant and restrict NetWorker server access and privileges to individual user accounts. When you disable the **User Authentication for NetWorker** option, access requests to a NetWorker server appear to come from the `gstd` process owner on the NMC server. All NMC users that access the NetWorker server are granted the same access and privilege rights that are assigned to the `gstd` process owner account.

The NMC server enables the **User Authentication for NetWorker** system option by default. When you enable the option, the NMC server software creates a separate network connection from the NMC server to a NetWorker server for each NMC user that has an **Administration** window open to that server. Additional network connections might require access to additional firewall service ports.

When you do not set the **User Authentication for NetWorker** system option, there is only one network connection from the NMC server to the managed NetWorker server.

### Modifying the User Authentication for NetWorker system option

Use these steps to define how the NetWorker Management Console (NMC) server controls the user account that requests NetWorker server access.

**Before you begin**

Log in to the NMC Server as a Console Security Administrator. The NetWorker Authentication Service administrator account is a Console Security Administrator.

**Procedure**

1. From the **Console** window, click **Setup**.
2. From the **Setup** menu, select **System Options**.
3. Set the **User authentication for NetWorker** option:
   - When you enable this option, the username of the authenticated user determines the level of user access to the NetWorker server.
   - When you disable this option, the user ID of the gstd process owner determines the level of user access to the NetWorker server.
4. Click **OK**.

## User authorization

User authorization settings control the rights or permissions that are granted to a user and enable access to a resource managed by NetWorker.

### NMC server authorization

The user role that you use to connect to the NMC server determines the level of access to the NMC server.

The NMC server restricts user privileges that are based on three authorization roles. You cannot delete the roles or change the privileges that are assigned to each role.

**Table 6** NMC user roles and associated privileges

| User role | Privileges |
|---|---|
| Console Security Administrator | • Add, delete, and modify NetWorker Authentication Service local database users. |

**Table 6** NMC user roles and associated privileges (continued)

| | |
|---|---|
| | • Control user access to managed applications, such as a NetWorker server.<br>**Note:** By default, NMC assigns the Console Security Administrator role to the NetWorker Authentication Service local database administrator. |
| Console Application Administrator | • Configure NMC system options.<br>• Set retention policies for reports.<br>• View custom reports.<br>• Specify the NetWorker server to back up the NMC database.<br>• Specify a NetWorker License Manager server.<br>• Run the **Console Configuration** wizard.<br>• All tasks available to a Console User role. |
| Console User | All tasks except for those tasks that are explicitly mentioned for the Console Security Administrator and the Console Application Administrator.<br>Tasks include:<br>• Add and delete hosts and folders.<br>• Add and delete Managed applications for NetWorker and Data Domain.<br>• Create and delete their own reports.<br>• Set features for Managed Applications.<br>• Manage a NetWorker server with the appropriate privilege levels.<br>• Dismiss events. |

## Configuring NetWorker Authentication Service local user access to the NMC server

After you create new users in the NetWorker Authentication Service database, assign the user to an NMC role to enable user access to the NMC server.

### Procedure

1. Connect to the NMC server with a NetWorker Authentication Service administrator account.
2. Click **Setup**.

   The **Users and Roles** window appears.
3. In the left navigation pane, select **Users and Roles** > **NMC Roles**.
4. In the **NMC Roles** window, right-click the role, and then select **Properties**.
5. In the **Local Users** section, select the users.
6. Click **OK**.
7. Connect to the NMC server with the user account.

Troubleshooting login errors on page 65 provides information about how to troubleshoot login issues.

## Configuring authentication in NMC

After you create users in the NetWorker Authentication Service database or configure the NetWorker Authentication Service to use an external authority for authentication, configure the NMC server to enable user access.

**Procedure**

1. Connect to the NMC server with a NetWorker Authentication Service administrator account.
2. Click **Setup**.

   The **Users and Roles** window appears.
3. In the left navigation pane, select **Users and Roles** > **NMC Roles**. In the **NMC Roles** window, right-click the role, and then select **Properties**.
4. For local database users only, in the **Local Users** section, select the users.
5. For LDAP and AD users, in the **External Roles** attribute, specify the DN of the LDAP/AD users or group that require privileges to the NMC server.

   Click **OK**, and then close the NMC GUI.
6. Connect to the NMC server. When you are prompted for a username and password, specify the credentials for a user that is in the hierarchy of the DN that you specified in the **External Roles** attribute.

   For the username, use the following format:

   ***tenant_name\domain_name\user_name***

   where:

   - *tenant_name* is the name of the tenant that you specified when you configured the external authentication authority configuration on the NetWorker Authentication Service. If you use the Default tenant, you are not required to specify the tenant name.
   - *domain_name* is the name of the domain that you specified when you configured the external authentication authority configuration on the NetWorker Authentication Service.
   - *user_name* is the name of the user in the LDAP or AD directory, which you added to the External Roles attribute or is a member of the group that you added to the External Roles attribute.

For example, to specify an AD account that is named Liam in an external authentication authority that you configured in an authentication service domain that is called IDDdomain and a tenant that is called IDD, specify the following username: **IDD\IDDdomain\Liam**.

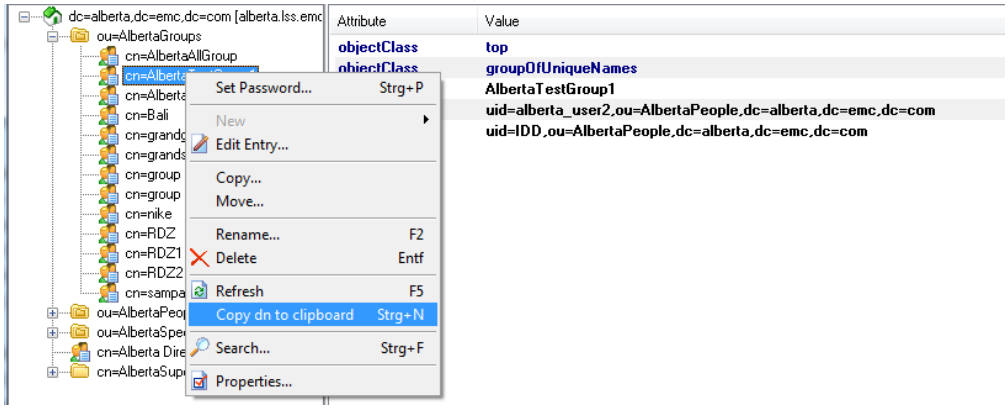
Troubleshooting login errors provides information about how to troubleshoot login issues.

**Example: Configure the External Roles attribute for LDAP authentication**

To add the AlbertaTestGroup1 LDAP group to the Console Security Administrators group on the NMC server, perform the following steps.

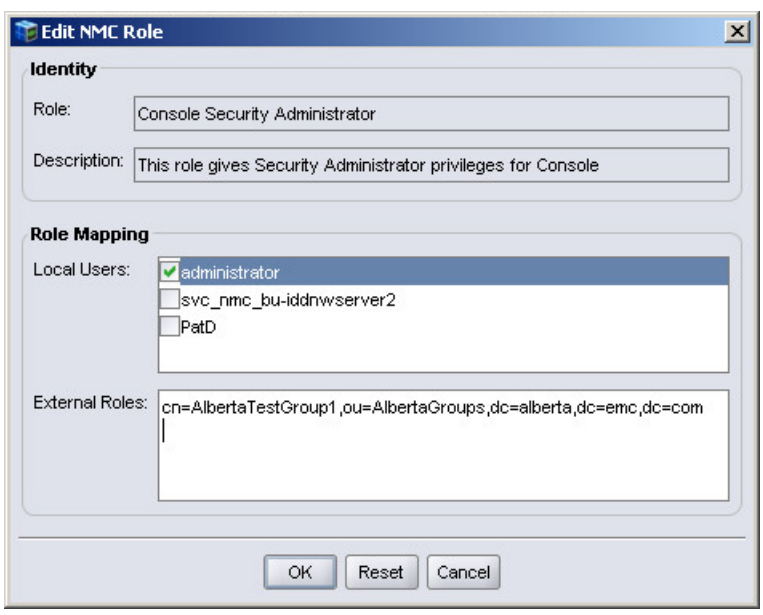
1. To connect to the LDAP server, use LDAP Admin.
2. Navigate to the LDAP group, right-click on the group name, and then select **Copy dn to clipboard**. The following figure provides an example of the LDAP Admin window.

**Figure 8** Copying the group DN




3. Connect to the NMC server with the NetWorker Authentication Service administrator account.
4. On the **Setup** window select **Users and Roles** > **NMC Roles** > **Console Security Administrator**.
5. In the **External Roles** attribute, paste the group dn value. The following figure provides an example of the group dn entry for the AlbertaTestGroup1 group.

**Figure 9** Configuring the External Roles attribute

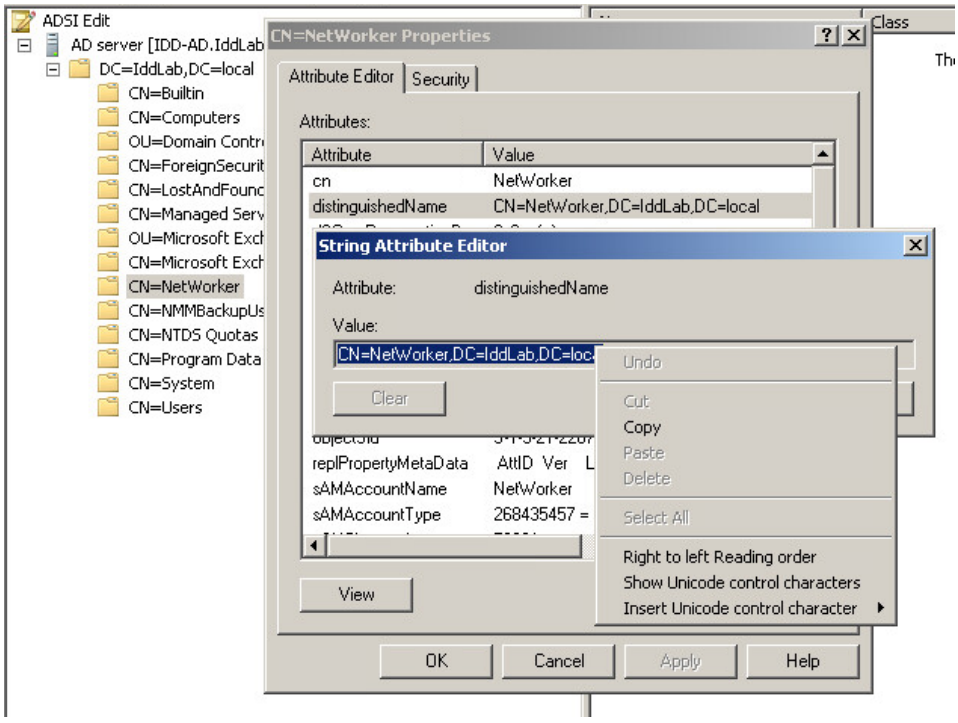


**Example: Configure the External Roles attribute for AD authentication**

To add an AD group that is named NetWorker to the Console Security Administrators group on the NMC server, perform the following steps.

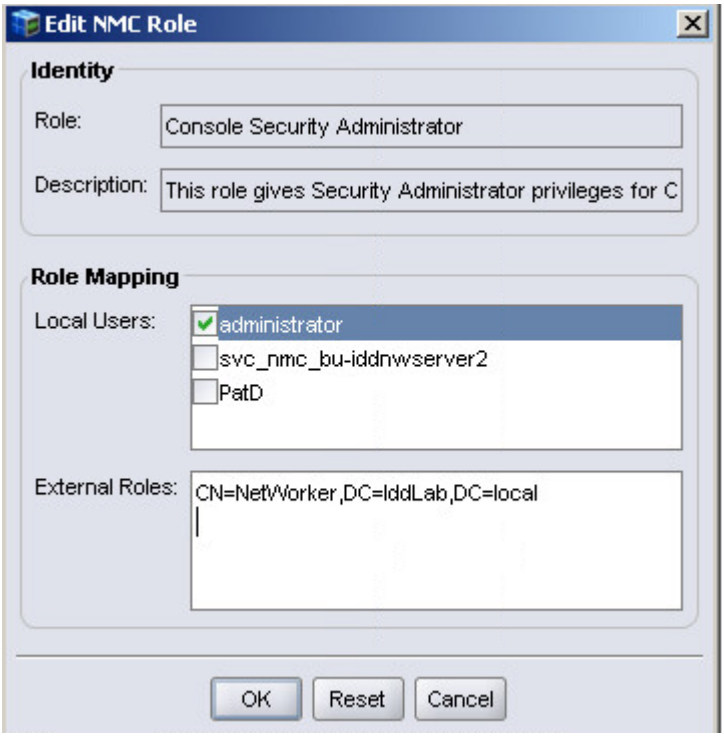
1. To connect to the AD directory, use ADSI Edit.
2. Navigate to the AD group, right-click the group name, and then select **Properties**.
3. On the **Attribute Editor** window, select **distinguishedName** from the attribute list, and then select **View**.
4. On the **String Attribute Editor** window, with the entire dn highlighted, right-click in the value field, and then select **Copy**. The following figure provides an example of copying the group DN in the ADSI Editor.

   **Figure 10** Copying the group DN




5. Click **Cancel**, and then close ADSI Editor.
6. Connect to the NMC server with the NetWorker Authentication Service administrator account.
7. On the **Setup** windows select **Users and Roles** > **NMC Roles** > **Console Security Administrator**.
8. In the **External Roles** attribute, paste the group DN value. The following figure provides an example of the group DN entry for the NetWorker group.

**Figure 11** Configuring the External Roles attribute




## Troubleshooting login errors

This section provides a list of possible causes and resolutions for NMC login error messages.

### You do not have privileges to use NetWorker Management Console

Appears when a valid LDAP or AD account tries to log in to the NMC server, but the account is not assigned a Console role.

### Could not authenticate this username and password, try again!

Appears when you try to log in to the NMC server with:

- An unrecognized username or an incorrect password. To resolve this issue, use the correct username and password combination for the configured NMC server authentication method.
- An AD user that has the **User must change password at next login** option enabled. To resolve this issue, change the password before trying to log in to the NMC server.
- A user that is not enabled in the NetWorker Authentication Service local user database.

## Server authorization

The NetWorker server provides a mechanism to authorize users that perform operations from a command prompt and from the NMC GUI.

### Configuring local user access to managed NetWorker servers

By default, the local database administrator is an administrator of each NetWorker server that is managed by the NMC server.

#### About this task

To provide local users and groups with administrator access to managed NetWorker servers, perform the following steps.

#### Procedure

1. Connect to the NMC server with the NetWorker Authentication Service administrator account.
2. Click **Enterprise**.
3. Right-click the NetWorker server, and then select **Launch Application**.
4. On the **NetWorker Administration** window, select **Servers**.
5. In the left navigation pane, select **User Groups**.
6. On the **User Groups** window, right-click **Security Administrators**, and then select **Properties**.
7. In the **Configuration** group box, click the + sign beside **External Roles**, and then select the users or groups to add to the **External Roles** attribute.

   The external roles attribute automatically gets populated with the selected users or groups.
8. Click **OK**.
9. On the **User Groups** window, right-click **Application Administrators**, and then select **Properties**.
10. In the **Configuration** group box, click the + sign beside **External Roles**, and then select the users or groups to add to the **External Roles** attribute.
11. Click **OK**.
12. Close the **NetWorker Administration** and **NMC** windows.
13. Connect to the NMC server with an LDAP or AD user, and then connect to the NetWorker server.
14. Confirm that you can view server resources, for example Directives.

### Configuring LDAP and AD user access to managed NetWorker servers

By default, the local database administrator is an administrator of each NetWorker server that is managed by the NMC server.

#### About this task

To provide LDAP/AD users and groups with administrator access to managed NetWorker servers, perform the following steps.

#### Procedure

1. Connect to the NMC server with the NetWorker Authentication Service administrator account.

2. Click **Enterprise**.
3. Right-click the NetWorker server, and then select **Launch Application**.
4. On the **NetWorker Administration** window, select **Servers**.
5. In the left navigation pane, select **User Groups**.
6. On the **User Groups** window, right-click **Security Administrators**, and then select **Properties**.
7. In the **External Roles** attribute, paste the dn of the user or group that you copied from the Console Security Administrator role.
8. Click **OK**.
9. On the **User Groups** window, right-click **Application Administrators**, and then select **Properties**.
10. In the **External Roles** attribute, paste the dn of the user or group that you copied from the Console Security Administrator role.
11. Click **OK**.
12. Close the **NetWorker Administration** and **NMC** windows.
13. Connect to the NMC server with an LDAP or AD user, and then connect to the NetWorker server .
14. Confirm that you can view server resources, for example Directives.

## Restricting managed server view for a user

By default the NMC server adds the default administrator account to the Security Administrators user group on each NetWorker server that is managed by the NMC server.

### Before you begin

Log in to the NMC server with an account that has the Console Security Administrator role.

### About this task

To restrict the NetWorker servers that a user can view and manage, modify the privileges that are assigned to the user account.

**Note:** If this user account has console security administrator privileges, the NMC server by default grants permission to all hosts and editing is disabled.

### Procedure

1. From the **Console** window, click **Setup**.
2. In the left pane, click **Users**.
3. Right-click a user, then select **Permissions**. The **Edit User** window appears and the **Permissions** tab displays.
4. To grant the user privileges to view various hosts, use the arrow keys to select the allowed hosts.
5. Click **OK**.

### Results

When you restrict the NMC view for a user, then you limit what a user can see in the NMC windows:

- In the **Enterprise** window—The user sees all the hierarchy folders, but only the allowed NetWorker servers appear in the folders.
- In the **Events** window—The user sees only events from allowed NetWorker servers.
- In the **Reports** window—The user only sees reporting data from allowed NetWorker servers and as a result, reports can vary among users. For example, a shared backup summary report entitled "Building C Backups" displays different data for different users (even when each user runs the report simultaneously) when the privileges of the users include different NetWorker servers. This applies to all report types.

  **Note:** A NetWorker server only appears in a list of reports when there is data available on which to report.
- In the **Setup** window:
  - The user sees properties for all users, in addition to its own properties and privileges.
  - The user can modify its own properties, but not privileges. Only the Console Security Administrator can view and modify user privileges.

## NetWorker user groups

User Groups provide you with the ability to assign local database, LDAP, and AD users privileges to perform operations on a NetWorker server.

The tasks that a user can perform on a NetWorker server depend on user group membership and the privileges that are assigned to the user group. Two attributes in the User Groups resource define user membership for a user group:

- External Roles—Defines membership for users in the local user database, LDAP directory, and AD directory. NetWorker uses this attribute to validate user authorization for operations that require token-based authentication, including CLI commands that are authenticated with a token generated by the `nsrlogin` command.
- Users—Defines membership for operating system users that perform operations outside of the **NetWorker Administration** window. For example:
  - CLI commands, such as `nsradmin`, `save`, and `recover`, that are not authenticated with the `nsrlogin` command.
  - NetWorker Modules, such as NetWorker Module for Database Applications and NetWorker Module for Microsoft Applications.

Using nsrlogin for authentication and authorization on page 79 describes how to use the `nsrlogin` command to provide token-based authentication to CLI operations.

### User group privileges

User privileges define the NetWorker operations and tasks that local database, AD, and LDAP users can perform on a NetWorker server. You can modify the privileges that are associated with a User Group, with the exception of the Application Administrators user group and the Security Administrators user group. The following table provides a summary of the available privileges and the operations that each privilege enables for a user.

**Table 7** Allowed Operations for each NetWorker privilege

| NetWorker privilege | Allowed operations |
|---|---|
| **Change Security Settings** | The ability to modify:<br>• User groups<br>• Security Audit log resource<br>• Server resource<br>**Note:** The **Change Security Settings** privilege requires that you also set the following prerequisite privileges: **View Security Settings**, **Create Security Settings**, and **Delete Security Settings**. |
| **View Security Settings** | The ability to view:<br>• User groups<br>• Audit log resource<br>• Server resource |
| **Create Security Settings** | The ability to create user group resources.<br>**Note:** The **Create Security Settings** privilege requires that you also set the following prerequisite privileges: **View Security Settings**, **Change Security Settings**, and **Delete Security Settings**. |
| **Delete Security Settings** | The ability to delete user created user groups. You cannot delete preconfigured user groups.<br>**Note:** The **Delete Security Settings** privilege requires that you also set the following prerequisite privileges: **View Security Settings**, **Change Security Settings**, and **Delete Security Settings**. |
| **Remote Access All Clients** | The ability to:<br>• Remotely browse and recover data that are associated with any client.<br>• View all client resources configuration attributes.<br>This privilege supersedes the users who are defined in the **Remote Access** attribute of a client resource.<br>**Note:** The **Remote Access All Clients** privilege requires that you also set the following prerequisite privileges: **Operate NetWorker**, **Monitor NetWorker**, **Operate Devices and Jukeboxes**, **Backup Local Data**, and **Recover Local Data**. |
| **Configure NetWorker** | The ability to configure resources that are associated with the NetWorker server, storage nodes, and clients. For example creating, editing, and deleting resources. |

**Table 7** Allowed Operations for each NetWorker privilege (continued)

| NetWorker privilege | Allowed operations |
|---|---|
| | This privilege does not enable users to configure user group resources.<br>**Note:** The **Configure NetWorker** privilege requires that you also set the following prerequisite privileges: **Operate NetWorker**, **Monitor NetWorker**, **Operate Devices and Jukeboxes**, **Backup Local Data**, and **Recover Local Data**. |
| **Operate NetWorker** | The ability to perform NetWorker operations, such as:<br>• Reclaim space in a client file index.<br>• Set a volume location or mode.<br>• Query the media database and client file indexes.<br>**Note:** The **Operate NetWorker** privilege requires that you also set the following prerequisite privileges: **Monitor NetWorker**, **Operate Devices and Jukeboxes**, **Backup Local Data**, and **Recover Local Data**. |
| **Monitor NetWorker** | The ability to:<br>• Monitor NetWorker operations, including device status, savegroup status, and messages.<br>• View media database information.<br>• View NetWorker configuration information (except the security settings that are described in the Change Security Settings privilege).<br>A user does not require this privilege to back up and recover local data, but the privilege helps users to monitor messages and other information. |
| **Operate Devices and Jukeboxes** | The ability to:<br>• Perform device and autochanger operations, for example, mounting, unmounting, and labeling volumes.<br>• View device status and pending messages.<br>• View information in the media database.<br>**Note:** The **Operate Devices and Jukebox** privilege requires that you also set the **Monitor NetWorker** privilege. |
| **Recover Local Data** | The ability to:<br>• Recover data from the NetWorker server to the local client.<br>• View most client configuration attributes.<br>• Query client save sets and browse the client file index. |

**Table 7** Allowed Operations for each NetWorker privilege (continued)

| NetWorker privilege | Allowed operations |
|---|---|
| | This privilege enables a user to view information about other clients and does not override file-based privileges.<br><br>Users can only recover files with the user privileges for that operating system. To perform save set or NDMP recoveries, users with the privilege must log in to the local host as root (UNIX) or administrator (Windows). |
| **Backup Local Data** | The ability to:<br>• Manually back up data from their local client to the NetWorker server.<br>• View most attributes in the client's configuration.<br>• Query the client save sets and browse the client file index.<br><br>This privilege does not enable a user to view information about other clients and does not override file-based privileges.<br><br>Users can only back up files with the user privileges for that operating system. To run the `nsrpolicy` command or to perform NDMP backups, users with this privilege must log in to the local hosts as root (UNIX) or administrator (Windows). To allow scheduled backups to operate correctly, the root user (UNIX) or administrator (Windows) on the client has this privilege automatically. |
| **View Application Settings** | The **View Application Settings** privilege:<br>• Provides the ability to view NetWorker resources including: Archive Requests, Clients, Devices, Directives, Policies, Jukeboxes, Labels, Licenses, Notifications, Pools, Schedules, Staging, and Storage Nodes.<br>• Allows user group members to view the status of operations.<br>• Does not allow user group members to view the Server, User groups, or Security Audit Log resources.<br><br>**Note:** The **View Application Settings** privilege requires that you also set the following prerequisite privileges: **Change Application Settings**, **Create Application Settings**, and **Delete Application Settings**. |
| **Change Application Settings** | The **Change Application Settings** privilege:<br>• Provides the ability to change NetWorker resources including: Archive Requests, Clients, Devices, Directives, Jukebox, Label, License, Notification, Policies, Pool, Schedule, Staging, and Storage Nodes.<br>• Allows user group members to view the status of operations. |

**Table 7** Allowed Operations for each NetWorker privilege (continued)

| NetWorker privilege | Allowed operations |
|---|---|
| | • Does not allow user group members to change the Server, User group, or Security Audit Log resources.<br>Note: The **Change Application Settings** privilege requires that you also set the following prerequisite privileges: **Change Application Settings**, **Create Application Settings**, and **Delete Application Settings**. |
| **Create Application Settings** | The **Create Application Settings** privilege:<br>• Provides the ability to create NetWorker resources including: Archive Requests, Clients, Devices, Directives, Policies, Jukeboxes, Labels, Licenses, Notifications, Pools, Schedule, Staging, and Storage Node.<br>• Allows user group members to view the status of operations.<br>• Does not allow user group members to change the Server, User groups, or Security Audit Log resources.<br>Note: The **Create Application Settings** privilege requires that you also set the following prerequisite privileges: **Change Application Settings**, **Create Application Settings**, and **Delete Application Settings**. |
| **Delete Application Settings** | The **Delete Application Settings** privilege:<br>• Provides the ability to delete NetWorker resources including: Archive Requests, Clients, Devices, Directives, Jukeboxes, Labels, Licenses, Notifications, Policies, Pool, Schedule, Staging, and Storage Node.<br>• Allows user group members to view the status of operations.<br>• Does not allow user group members to change the Server, User groups, or Security Audit Log resources.<br>Note: The **Delete Application Settings** privilege requires that you also set the following prerequisite privileges: **Change Application Settings**, **Create Application Settings**, and **Delete Application Settings**. |
| **Archive Data** | The ability to archive data. The NetWorker application administrator must have configured NetWorker for a user with this privilege to run this operation. Only the client resource that pertains to the client that issues the archive command is viewable. |
| **Backup Remote Data** | Allows users to remotely back up data. |
| **Recover Remote Data** | Allows users to recover data for a back up performed on another server. |

### Preconfigured user groups

By default, NetWorker provides preconfigured user groups with specific privileges. You cannot delete preconfigured user groups.

The following table provides a summary of the preconfigured user groups and the default privileges associated with each user group.

**Note:** By default, the NetWorker Authentication Service administrator group is automatically added to the preconfigured Application Administrators and Security Administrators user groups on the local NetWorker server.

**Table 8** Privileges associated with each NetWorker User Group

| NetWorker user group | Associated privileges | |
|---|---|---|
| Security Administrators | • View Security Settings<br>• Change Security Settings | • Create Security Settings<br>• Delete Security Settings |
| Application Administrators | • Remote Access All Clients<br>• Configure NetWorker<br>• Operate NetWorker<br>• Monitor NetWorker<br>• Operate Devices and Jukeboxes<br>• Recover Local Data<br>• Recover Remote Data | • Backup Local Data<br>• Backup Remote Data<br>• Create Application Settings<br>• View Application Settings<br>• Change Application Settings<br>• Delete Application Settings<br>• Archive Data |
| Monitors | • Monitor NetWorker<br>• Operate Devices and Jukeboxes<br>• Recover Local Data<br>• Recover Remote Data | • Backup Local Data<br>• Backup Remote Data<br>• Create Application Settings<br>• View Application Settings<br>• Archive Data |
| Operators | • Remote Access All Clients<br>• View Application Settings<br>• Operate NetWorker<br>• Monitor NetWorker<br>• Operate Devices and Jukeboxes | • Recover Local data<br>• Recover Remote Data<br>• Backup Local Data<br>• Backup Remote Data<br>• Archive Data |
| Auditors | • View Security Settings | |
| Users | • Monitor NetWorker<br>• Recover Local Data | • Backup Local Data |
| Database Operators | • Remote Access All Clients | • Recover Local Data |

**Table 8** Privileges associated with each NetWorker User Group (continued)

| NetWorker user group | Associated privileges | |
|---|---|---|
| | • Operate NetWorker<br>• Monitor NetWorker<br>• Operate Devices and Jukeboxes | • Recover Remote Data<br>• Backup Local Data<br>• Backup Remote Data<br>• Archive Data |
| Database Administrators | • Remote Access All Clients<br>• Configure NetWorker<br>• Operate NetWorker<br>• Monitor NetWorker<br>• Operate Devices and Jukeboxes | • Recover Local Data<br>• Recover Remote Data<br>• Backup Local Data<br>• Backup Remote Data<br>• Archive Data |

**User group management**
Users assigned to the Create Security Settings and Change Security Settings NetWorker privileges can manage and modify user groups.

The Security Administrators user groups contain these privileges by default.

**Modifying user group privileges**
You can change privileges that are associated with a user group, with the exception of the Application Administrators and Security Administrators user groups.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**Procedure**

1. From the **Administration** window, click **Server**.
2. Click **User Groups**.
3. Right-click the user group to edit, and then select **Properties**.

   The **Properties** dialog box appears.
4. In the **Privileges** field, select or unselect the privileges as required.
5. Click **OK**.

   **Note:** If you select a privilege without selecting dependent privileges, then an error message appears.

**Creating or modifying user groups**
Use the NMC GUI to create user group resources.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**Procedure**

1. From the **Administration** window, click **Server**.
2. Click **User Groups**.

3. For new user groups only, right-click **User Group**, and then select **Create**.
4. To modify a user group, right-click the user group, and then select **Properties**.
5. In the **Name** attribute, type a name for the user group.

   **Note:** You cannot modify the name of an existing user group.

6. In the **External roles** attribute, specify the dn of the users and groups.

   Modifying NetWorker user group membership for NMC on page 76 provides more information.

7. In the **Privileges** attribute, select the privileges to assign to the user group.
8. Click **OK**.

### Copying user groups

Use NMC to copy a User Group.

#### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

#### Procedure

1. From the **Administration** window, click **Server**.
2. Click **User Groups**.
3. Right-click the user group to edit, and then select **Copy**.

   The **Create User Group** dialog box appears, and contains the same information as the user group that was copied, except for **Name** attribute.

4. In the **Name** attribute, type a name for the new user group.
5. Edit the other attributes as appropriate, and then click **OK**.

### Deleting user groups

Use the NMC GUI to delete User Groups.

#### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

#### Procedure

1. From the **Administration** window, click **Server**.
2. Click **User Groups**.
3. Right-click the user group to edit, and then select **Delete**.
4. When prompted, to confirm the deletion, click **Yes**.

   **Note:** You cannot delete a preconfigured user group.

### Modifying user group membership

By default, the user group provides Backup Local Data and Recover Local Data privileges to all operating system users and all users in the local database group Users. You can modify the group membership of existing user groups to restrict the operations that users can perform.

Before you change existing user group membership, review the following information:

- Operations that are performed within NMC and the **NetWorker Administration** window use token-based authentication and authorize user privileges that are

based on the user membership that is defined in the **External Roles** attribute of a user group.

- Operations that you perform within the NMC and the **NetWorker Administration** window do not use the **Users** attribute to determine the level of authorization that is assigned to a user.
- Use the **External Roles** attribute to manage local database, LDAP, AD user, and group membership.

  **Note:** When you restrict user group membership to users and groups in the **External Roles** attribute only, use the `nsrlogin` command to authenticate the user before you run NetWorker CLI commands.
- NetWorker module applications, such as NMDA and NMM do not use token-based authentication and rely on GSS to authenticate OS users. Use the **User** attribute to manage OS user and group membership for GSS authentication.

  **Note:** When a user belongs to many operating system groups, the total number of characters for all the group names can exceed the buffer size that NetWorker users to store the group names. NetWorker excludes characters and group names that exceed the buffer size. If you add a group to **Users** attribute that is not in the buffer for a userid, NetWorker does not consider the user to be a member of the User Group.

**Modifying NetWorker user group membership for NMC**

Use the External roles field in the User Group resource to manage local database, LDAP, and AD user and group access to the NetWorker server.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Security Administrators user group on the NetWorker server.

**Procedure**

1. On the **Administration** window, click **Server**.
2. Click **User Groups**.
3. Right-click the user group, and then select **Properties**.
4. Modify the **External roles** attribute. To add NetWorker Authentication Service local database users or groups, click the + sign, and then select the users or groups. When you add an LDAP or AD user or group, specify the distinguished name (DN).

   The following sections provide more information about how to get the dn for the user or group in an AD or LDAP external authentication authority, and how to add the NMC service account.

   **Note:** It is recommended that you specify usernames when your user accounts are a member of a large number of groups.

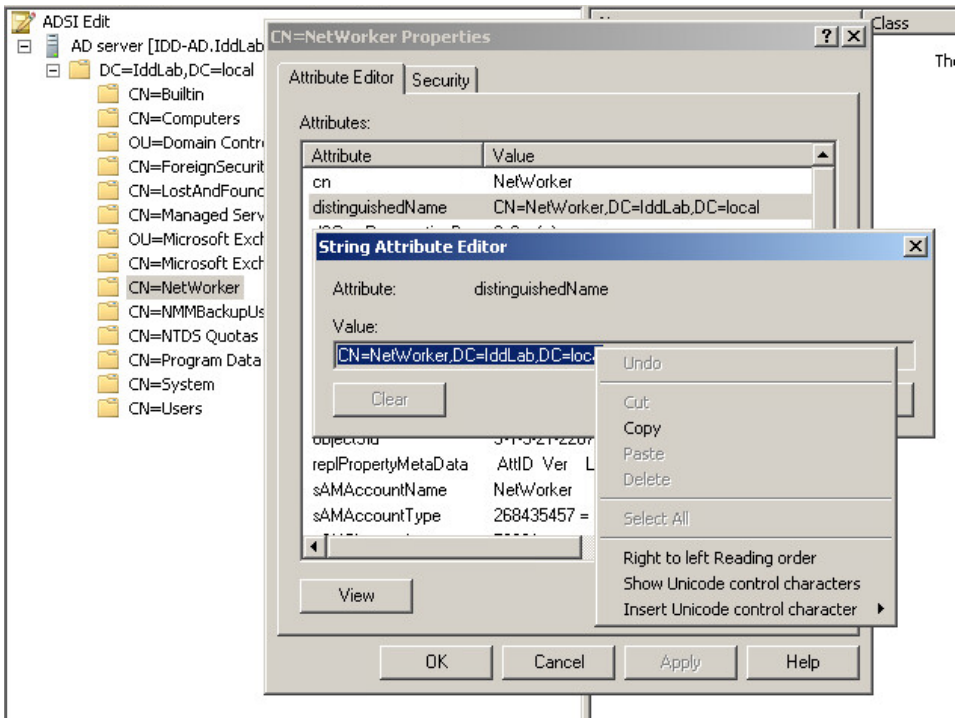
**Example: Adding AD group to the External roles attribute**

The following example uses ADSI Edit, a Windows tool that allows you to view information about users and groups in AD directory service. Microsoft TechNet provides the most up to date information about how to use ADSI Edit.

1. To connect to the AD directory, use ADSI Edit.
2. Navigate to the AD group, right-click the group name, and then select **Properties**.
3. On the **Attribute Editor** window, select **distinguishedName** from the attribute list, and then select **View**.

4. On the **String Attribute Editor** window, with the entire dn highlighted, right-click in the value field, and then select **Copy**. The following figure provides an example of copying the group DN in the ADSI Editor.

**Figure 12** Copying the group DN



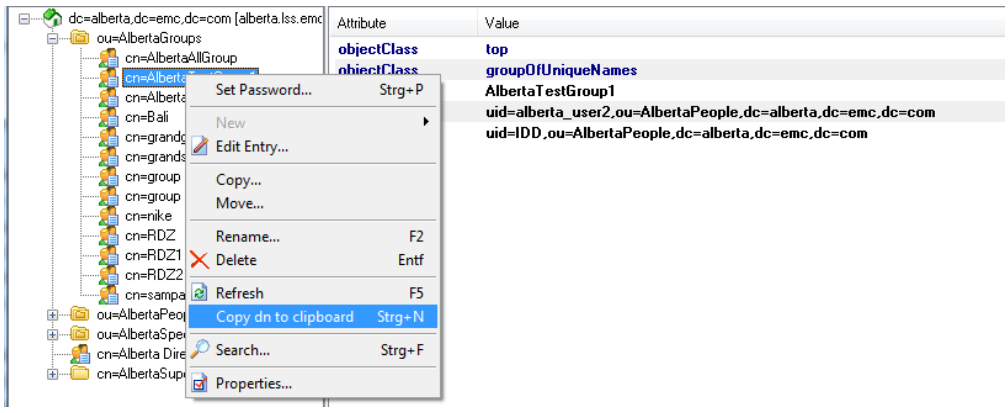

5. Click **Cancel**, and then close ADSI Editor.
6. Paste the dn value for the group into the **External roles** attribute.

### Example: Adding LDAP group to the External Roles attribute

The following example uses LDAP Admin, a third party tool that allows you to view information about users and groups in the LDAP directory service.

1. To connect to the LDAP server, use LDAP Admin.
2. Navigate to the LDAP group, right-click on the group name, and then select **Copy dn to clipboard**. The following figure provides an example of the LDAP Admin window.

**Figure 13** Copying the group DN



3. Close the LDAP Admin window.
4. Paste the dn value for the group into the **External roles** attribute.

```
authc_mgmt -u administrator -p "Password1" -e query-ldap-users -D

"query-tenant=IDD" -D

"query-domain=ldapdomain"
```

**Example: Adding a local database group to the External Roles attribute**

1. To view information about a specific group, use the *-e find-group* option:

```
authc_mgmt -u administrator -p "password" -e find-group -D group-
name=group_name
```

2. To display information about a group named test, type the following command:

```
authc_mgmt -u administrator -p "1.Password" -e find-group -D
"group-name=test"
Group Id : 132
Group Name : test
Group Details: New local database group
Group DN : cn=test,cn=Groups,dc=bu-
iddnwserver2,dc=IddLab,dc=local
Group Users : []
```

3. Copy the value in the *Group DN* attribute.
4. Paste the *Group DN* value into the **External roles** attribute.

**Modifying user group membership for OS users and groups**

Use the Users attribute in the User Group resource to manage OS user and group access to the NetWorker server.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**Procedure**

1. From the **Administration** window, click **Server**.
2. Click **User Groups**.
3. Right-click the user group, and then select **Properties**.
4. In the **Users** field, specify the NMC user. Specify the username with the following syntax: ***name=value***`[,`***name=value***`, ...]`

   where *name* is one of the following:

   - user
   - group
   - host
   - domain
   - domainsid
   - domaintype (either NIS or WINDOMAIN)

For example, to specify a user who is named patrick on a host that is named jupiter, enter this line in the **Users** attribute: `user=patrick,host=jupiter` or `user=patrick,host=jupiter.emc.com`

> **Note:** The formats user@host, host and user, and similar formats are ambiguous as to whether host or domain is intended. It is recommended that you use the name=value format.

This example shows what to enter to provide NetWorker administrative privileges to the following:

In the **Users** field, type the following information:

- The user *root* from any host.
- The user *operator* from the hosts *mars* and *jupiter* .
- Any users, valid hosts for the users, and valid domains for the users and host that are included in the netgroup *netadmins*. For example:

```
user=root
user=operator,host=jupiter
user=operator,host=mars.emc.com
&netadmins
```

Consider the following information:

- If the value has spaces, then surround the value in quotation marks, for example: `domain="Domain Admins"`
- When you specify a netgroup name, precede the name with an ampersand (&).
- You can use wildcards in place of a value. However, use wildcards with caution because they can compromise the enterprise security.
- You can specify local and global Windows domain names and groups. For example, the Administrators group and Domain Admins group.
- When you log in to the NetWorker server with a domain account, you can only specify a global group.
- When you log in to the NetWorker server locally, you can only specify local groups.
- When you log in to the NetWorker server with a domain account but the NetWorker server cannot contact the AD server to verify the username, use multiple names and values to ensure that NetWorker assigns the correct users or groups the appropriate privileges. For example, `user=meghan`, `domain=Engineering` or `group=development`, `domainsid=S-1-5-32-323121-123`

> **Note:** It is recommended that you specify usernames when your user accounts are a member of a large number of groups.

## Using nsrlogin for authentication and authorization

When you configure the NetWorker Authentication Service to use LDAP/AD authentication, you modify the **External Roles** attribute in the **User Group** resource to assign privileges to LDAP and AD users. As a result, NetWorker command line operations and NetWorker module operations might fail due to insufficient privileges. To resolve this issue, use the `nsrlogin` command to contact the NetWorker Authentication Service and authenticate a user. When user authentication succeeds, the NetWorker Authentication Service issues a token to the NetWorker host for the

user, which provides CLI operations with token-based authentication until the token expires.

### Before you begin

Ensure that the user that the NetWorker Authentication Service validates has the appropriate User Group privileges to run the CLI commands.

### About this task

Perform the following steps on a NetWorker Client on which you initiate the CLI commands, or the requesting host.

### Procedure

1. To validate a user and generate a token for the user, use the `nsrlogin` command:

   **`nsrlogin [-s NetWorker_server] [-H authentication_host] [-P port] [-t tenant] [-d logindomain] -u username [-p "password"]`**

   where:

   - **`-s NetWorker_server`**—Specifies the name of the NetWorker Server. Use this option when you use the `nsrlogin` command on a NetWorker host that is not the NetWorker Server.
   - **`-H authentication_host`**—Specifies the name of the NetWorker Authentication Service host. Use this option when you use the `nsrlogin` command on a NetWorker host that is not the NetWorker Server. This option is only required when you do not use the **`-s`** option.
   - **`-P port`**—Specifies the NetWorker Authentication Service port number. Use this option when you do not use the **`-s`** option and when the NetWorker Authentication Service does not use the default port number 9090 for communications.
   - **`-t tenant`**— Specifies the tenant name that the NetWorker Authentication Service should use to verify the username and password. When you omit this option, NetWorker Authentication Service uses the Default tenant to verify the user credentials.
   - **`-d logindomain`**—Specifies the domain name that the NetWorker Authentication Service should use to verify the username and password with an external authentication authority. When you omit this option, the NetWorker Authentication Service uses the local user database to verify the user credentials.
   - **`-u username`**—Specifies the username that the NetWorker Authentication Service should validate to generate a token.
   - **`-p "password"`**—Specifies the password that the NetWorker Authentication Service should use to verify the username. If you do not specify the password, the `nsrlogin` command prompts you to provide the password.

   For example, to generate a token for user *Konstantin* in the *idddomain* domain and the *idd* tenant, type the following command:

   ```
   nsrlogin -s bu-idd-nwserver2 -d idddomain -u Konstantin -p
   "1.Password"
   ```

   ```
   Authentication succeeded.
   ```

When the NetWorker Authentication Service successfully validates the user, the service issues an authentication token to the requesting host.

2. At the command prompt, type the NetWorker command.

   If the validated user does not have the appropriate privileges to run the command, an error message appears or the command does not return the expected result. For example, when you try to perform an operation with a user account that does not have the required privilege, a message similar to the following appears:

   ```
   Permission denied, user must have the 'Operate NetWorker'
   privilege'.
   ```

### Results

The CLI command uses the authenticated token, until the token expires. By default the token expiration period is 480 minutes or 8 hours. When the token expires and the user tries to run a CLI command, the command fails with a permissions error and a message similar to the following appears to indicate that the token has expired:

```
Security token has expired
```

To resolve this issue, run the `nsrlogin` command again to generate a new authenticated token.

**Note:** To revoke the user token and enable the CLI commands to use the **Users** attribute in the Usergroups resources to authenticate users, use the `nsrlogout` command. The `nsrlogout` UNIX man page and the *NetWorker Command Reference Guide* provides detailed information about the `nsrlogout` command.

## Troubleshooting authorization errors and NetWorker server access issues

This section provides a list of possible causes and resolutions for error messages that are related to NetWorker Server authorization issues.

### Insufficient permissions

This message is displayed when the user that you used to log in to the NMC server is a member of many operating system groups and you try to perform NetWorker operations.

When a user belongs to many groups, the total number of characters in the group names can exceed the buffer size that NetWorker allots for the group names. NetWorker excludes characters and group names that exceed the buffer size.

To resolve this issue, edit the Usergroup resource to which the user belongs, and then specify the DN for the user in the **External Roles** field.

### Token has expired

This message is displayed when the NMC GUI is open and the token expires for the authenticated user.

To resolve this issue:

1. Click **OK**. The **Enter Credentials** window is displayed.
2. In the **Enter Credentials** window, specify the user password, and then click **OK**. The NetWorker Authentication Service validates the user credentials and, if the validation succeeds, generates a new session token.

### Unable to connect to server: Unable to set user privileges based on user token for SYSTEM: security token has expired

This message is displayed when the **NetWorker Administration** window is open and the token expires for the authenticated user.

To resolve this issue:

1. Click **OK**. The **NetWorker Administration** window closes.
2. In the Console GUI, select the NetWorker server, and then select **Launch NetWorker Administration**. The **Enter Credentials** window is displayed.
3. In the **Enter Credentials** window, specify the password of the user, and then click **OK**. The NetWorker Authentication Service validates the user credentials and if the validation succeeds, generates a new token for the session.

### Unable to query resource database: security token has expired

This message is displayed when you run a CLI tool as an authenticated user but the user token has expired.

To resolve this issue, run the `nsrlogin` command to generate a new token for the user.

### Unable to connect to server: Unable to authenticate with server "server-name": Authentication error

This issue is seen if the NMC (gstd) service and NetWorker server (nsrd) service are installed on separate hosts. When you log in to NMC and click the tabs and options the error: “Unable to connect to server: Unable to authenticate with server networker-server: Authentication error: why = Server rejected credentials” is displayed. This issue arises due to peering conflict or incorrect permission settings.

To resolve the issue, clear the peering information:

1. Run the following command on theNetWorker Server:

```
nsradmin -p nsrexec
p type: nsr peer information; name: nmc-server-name
delete
yes
```

2. Run the following command on the NMC server:

```
nsradmin -p nsrexec
p type: nsr peer information; name: nmc-server-name
delete
yes
```

**Note:** The hostname is case sensitive. You must use the hostname that is displayed in the NMC console.

If the issue persists, then run the following command on the NetWorker Server:

```
nsrauthtrust -H nmc-server-name -P 9090
nsraddadmin -H nmc-server-name -P 9090
```

## Changing the NetWorker Authentication Service hostname and port number

When you install the NMC server software, you specified the hostname of the NetWorker Authentication Service and the port number that the service uses for

communication. Perform the following steps to change the host that provides user authentication to the NMC server.

**Procedure**

1. Connect to the NMC server with an Administrator account on Windows or the root account on UNIX.
2. Stop the EMC `gstd` process:
   - Linux—`/etc/init.d/gstd stop`
   - Windows—Stop the **EMC GST Database Service** service.
3. From a command prompt, to change the NetWorker Authentication Service host that is used by the NMC server, type the `gstauthcfg` command.

   The location of the `gstauthcfg` command is not in the path by default and differs on Linux and Windows:
   - Linux—`/opt/lgtonmc/bin`
   - Windows—`C:\Program Files\EMC NetWorker\Management\GST\bin`

   For example:

   `gstauthcfg` **-c -t -h *New_authentication_service_hostname* -p *port_number***

   **Note:** The default port number is 9090.
4. Start the EMC `gstd` process:
   - Linux: `/etc/init.d/gstd start`
   - Windows: Start the **EMC GST Database Service** service.
5. To establish the trust, type the following command on each NetWorker Server that is not local to the NetWorker Authentication Service that NMC uses for authentication:

   `nsrauthtrust` **-H *Authentication_service_host* -P *Authentication_service_port_number***

   where:
   - The location of the `nsrauthtrust` command differs on Linux and Windows:
     - Linux—`/usr/sbin`
     - Windows—`C:\Program Files\EMC NetWorker\nsr`
   - *Authentication_service_host* is the hostname of the NetWorker Server that authenticates the NMC Server host.
   - *Authentication_service_port_number* is the port number used by the NetWorker Authentication Service. The default port number is 9090.

   For example:

   **`nsrauthtrust -H nwserver.corp.com -P 9090`**
6. Grant the NetWorker Authentication Service user groups access to the NetWorker Server, by typing the `nsraddadmin` command:

```
nsraddadmin -H Authentication_service_host -P
Authentication_service_port_number
```

For example:

```
nsraddadmin -H nwserver.corp.com -P 9090
```

The `nsraddadmin` command updates the following user groups:

- Application Administrator—Adds the distinguished name (DN) of the NetWorker Authentication Service Administrators group.
- Security Administrator—Adds the DN of the NetWorker Authentication Service Administrators group.
- Users—Adds the DN of the NetWorker Authentication Service Users group.

7. Connect to the NMC server GUI with a user that has the NMC Console Security Administrator role.
8. When prompted to create a service account for the NMC server in the NetWorker Authentication Service database, click **OK**.

   **Note:** If you do not create the service account, the NMC server cannot monitor events or gather reporting data from the managed NetWorker servers.

# How user authentication and authorization works in NWUI

User authentication settings control the processes that the NetWorker Web UI (NWUI) and the NetWorker software applications use to verify the identity that is claimed by a user. User authorization settings control the rights or permissions that are granted to a user and enable access to resources managed by NetWorker.

**Note:** The NetWorker Management Web UI uses the NetWorker credentials for authentication.

## NWUI server authentication and authorization

Specify the username in one of the following formats:

- For LDAP/AD authentication: *domain/username*

  **Note:** LDAP over SSL is supported.
- For local user database authentication: *username*
- For tenant configurations: *tenant/domain/username*

The NetWorker Web UI uses the NetWorker role based access control configuration to define the access level available to the user.

The login process uses JWT token based authentication, which is three way communication between AUTHC, Web UI and REST APIs.

VM File-level recovery requires that the user possesses administrative privileges.

A non-administrator user can perform VM Image-level recoveries using the NWUI, if the user is associated with a user group, which has the following privileges:

- Remote Access All Clients
- Operate NetWorker
- Monitor NetWorker

- Operate Devices and Jukeboxes
- Recover Local Data
- Backup Local Data

**Note:**

- You can access the NetWorker Web Management UI using HTTPS. The application uses self signed certificates.
- If the NetWorker Management Web UI is idle for 15 minutes, then a warning message appears on the screen. If there is no activity for 30 seconds, you are logged out.

### NWUI administration authentication and authorization

NetWorker user groups section describes how to configure user groups on a NetWorker server.

For more information on configuring user groups, see NetWorker user groups

Component access control settings define how to control external and internal system or component access to the product. NetWorker provides you with the ability to restrict remote program executions or client-tasking rights on a NetWorker host using different component authorization levels.

For more information on component access control, see Component access control

# Disabling SSLv3 cipher connectivity to the PostgresSQL database on the NMC server

**Procedure**

1. Connect to the NetWorker Management Console (NMC) server.
2. Edit the `postgresql.conf` file. The file is in the following locations:
   - Windows: `C:\Program Files\EMC NetWorker\Management\nmcdb\pgdata\`
   - Linux: `/nsr/nmc/nmcdb/pgdata/`
3. Search for the string ssl_ciphers.

   By default you see: `ssl_ciphers = 'ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH' # allowed SSL ciphers`
4. Update the ssl_ciphers parameter to:

   `ssl_ciphers = 'TLSv1.2:HIGH:!SSLv3:!NULL:!ADH:!MEDIUM:!LOW:!EXP:!MD5:!RC4:!3DES:@STRENGTH'`
5. Save the file.
6. Restart the `EMC gstd service/gstd` daemon.

# Component access control

Component access control settings define how to control external and internal system or component access to the product.

## Component authentication

NetWorker hosts and daemons use the nsrauth mechanism to authenticate components and users, and to verify hosts. The nsrauth GSS authentication mechanism is a strong authentication that is based on the Secure Sockets Layer (SSL) protocol.

**Note:** HP-UX depends on the OpenSSL library available on the operating system. OpenSSL 0.9.8e or later is required for NetWorker modules to function correctly.

Following version SSLv3, SSL was renamed to Transport Security Layer (TLS) starting with TLSv1. For Windows, nsrauth uses the SSL/TLS protocol that is implemented by RSA BSAFE. For UNIX and Linux, nsrauth uses the SSL/TLS protocol that is implemented by the OpenSSL library. NetWorker 9.1 and later uses TLSv1.2. Earlier NetWorker versions that have not been updated use TLSv1.0.

The `nsrexecd` service on each NetWorker host provides the component authentication services. The first time the nsrexecd process starts on a host, the process creates the following unique credentials for the host:

- 2048-bit RSA private key
- 1024-bit RSA private key, for backward compatibility
- Self-signed certificate or public key
- NW Instance ID
- my hostname

NetWorker stores these credentials in the NSRLA resource found in the local NetWorker client database, nsrexec. These credentials are known as local host authentication credentials. NetWorker uses the local host authentication credentials to uniquely identify the host, to other NetWorker hosts in the datazone.

When a NetWorker host communicates with other NetWorker hosts, the nsrauth process creates an NSR Peer Information resource in the nsrexec database of the target host that contains local host authentication credentials for the initiating host. When a NetWorker host starts a session connection to another host, the following steps occur:

1. The `nsrexecd` daemon on the initiating host contacts the `nsrexecd` daemon on the target host.
2. The `nsrexecd` daemon on the initiating host sends the local host authentication credentials to the target host.
3. The target host compares the local host authentication credentials with the information that is stored in the local NSR Peer Information resource:
   - If the information provided by the initiating host matches the information that is stored in the **NSR Peer Information** resource on the remote host, the nsrexecd daemon creates a session key and establishes an SSL connection between the two hosts. NetWorker uses AES-256 bit encryption to encrypt the data that is exchanged between the two hosts.

- If the information provided by the initiating host does not match the information that is stored in the **NSR Peer Information** resource on the remote host, the remote host requests the certificate from the initiating host:
  - If the certificate provided by the initiating host matches the certificate that is stored on the remote host, the nsrexecd daemon creates a session key and establishes an SSL connection between the two hosts. NetWorker uses AES-256 bit encryption to encrypt the data that is exchanged between the two hosts.
  - If the certificate provided by the initiating host does not match the certificate that is stored on the remote host, NetWorker drops the connection between the two hosts.
- If the remote host does not contain a **NSR Peer Information** resource for the initiating host, the remote host uses the information that is provided by the initiating host to create a **NSR Peer Information** resource. NetWorker uses the session key to establish an SSL connection between the two hosts. Component authentication uses the AES-256 bit encryption method.

**Note:** For compatibility with earlier NetWorker releases, NetWorker supports oldauth authentication. It is recommended that you use nsrauth authentication and only enable oldauth authentication when two hosts cannot authenticate by using nsrauth. The oldauth authentication method is not secure. Modifying the authentication methods used by NetWorker hosts on page 88 provides more information.

## Configuring access privileges to the NetWorker client database

To modify access to the client database (nsrexec), use the `nsradmin` program to edit the administrators list.

### Before you begin

Perform the following steps on the target host as the root user on a UNIX host or as an administrator user on a Windows host.

### About this task

By default, the administrator attribute provides access to the following users:

- On a UNIX or Linux host, any root user on any host to modify the nsrexec database attributes.
- On a Windows host, any user in the administrators group can modify the nsrexec database attributes.

To modify attributes for a host by using the **Local Hosts** resource in the NetWorker Management Console (NMC) UI, the administrator attribute of the target host must contain the account that starts the gstd service on the NMC server.

### Procedure

1. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

2. Set the query to the NSRLA resource:

   ```
   . type: NSRLA
   ```

3. Display the NSRLA resource and view the current settings for the *administrator* attribute:

   ```
   print
   ```

4. Update the value of the administrator attribute to include the owner of the gstd process on the NMC server:

   **`append administrator:"user=`*`gstd_owner`*`,host=`*`NMC_host`*`"`**
   where:

   - *gstd_owner* is the user account that starts the gstd daemon on UNIX or the EMC GST service on Windows. By default, the process owner is the SYSTEM user on Windows and is the root user on UNIX.
   - *NMC host* is the hostname of the NMC server.

   For example, to add the *SYSTEM* account on a Windows NMC server that is named *win.emc.com* to a UNIX NetWorker client named *unix.emc.com*, type:

   ```
   append administrator: root,
   "user=root,host=unix.emc.com","user=SYSTEM,host=win.emc.com"
   ```

5. To confirm the change, type **`Yes`**.
6. To exit the `nsradmin` program, type **`Quit`**.

## Modifying the authentication methods used by NetWorker hosts

NetWorker enables you to restrict the authentication methods available for communication between NetWorker hosts and define the priority of authentication methods that are used by NetWorker hosts. Use the Host Managements window in NMC or the `nsradmin` command to modify the authentication method that is used by NetWorker hosts.

### Using NMC to manage the authentication method

To manage the authentication method that is used by a host use the Known Hosts section of the Host Management window in NMC.

#### Before you begin

The account that you use to connect to the NetWorker server must have permission to access the NSRLA database on the target host.

#### Procedure

1. On the **Administration** window, select **Hosts**.

   The **Hosts Management** window appears.
2. In the **Hosts** pane, right-click the target host, and then select **Configure Local Agent**.
3. On the **Advanced** tab, in the **Auth Methods** attribute, specify the authentication methods that other NetWorker hosts (peer hosts) can use when initiating a connection.

   To specify the **Auth Methods** value, use the following format:

   ***`IP_Address[mask], authentication_method[/ authentication_method]...`***

   where:

   - *IP_Address[mask]* is a single IP address, a single host name, or an IP address and netmask range. You can specify the number of bits for the mask value or use the full subnet mask address.
   - *authentication_method* is **nsrauth**, for strong authentication or **oldauth** for legacy authentication.

> **Note:** When you specify more than one authentication method, NetWorker attempts to communicate with the first method in the list. If the first method fails, then NetWorker will attempt to communicate by using the second method in the list.

For example:

- To configure host mnd.emc.com to only use nsrauth when communicating with the host, type:

  ```
  mnd.emc.com,nsrauth
  ```

- To configure all hosts on the 137.69.168.0 subnet to only use nsrauth when communicating with the host, type:

  ```
  137.69.160.0/24, nsrauth
  ```

- To configure all hosts in the datazone to use nsrauth when communicating with the host except for a host with the IP address 137.69.160.10, which should try oldauth first, type the following two lines:

  ```
  137.69.160.10, oldauth/nsrauth
  ```

  ```
  0.0.0.0, nsrauth
  ```

4. Click **OK**.
5. On the target host, restart the NetWorker services or daemons.

## Using nsradmin to manage the authentication method

Use the `nsradmin` program to manage the authentication method that is used by a host.

### Before you begin

Connect to the target host with an account that has administrator access to the NSRLA database. You must configure access privileges to the NetWorker client database.

### Procedure

1. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

2. Set the query type to the **NSR Peer Information** resource:

   ```
   . type: nsrla
   ```

3. Display the current value for the **auth methods** attribute:

   ```
   show auth methods
   ```

   ```
   print
   ```

4. Update the **auth methods** attribute, by using the following format:

   ```
   update auth methods: "IP_Address[mask],authentication_method[/
   authentication_method]"
   ```

   where:

- *IP_Address[mask]* is a single IP address, a single host name, or an IP address and netmask range. You can specify the number of bits for the mask value or use the full subnet mask address.
- *authentication_method* is **nsrauth**, for strong authentication or **oldauth** for legacy authentication.

  **Note:** When you specify more than one authentication method, NetWorker attempts to communicate with the first method in the list. If the first method fails, then NetWorker will attempt to communicate by using the second method in the list.

For example:

- To configure host mnd.emc.com to only use the nsrauth when communicating with the host, type:

  ```
  update auth methods: "mnd.emc.com,nsrauth"
  ```

- To configure all hosts on the 137.69.168.0 subnet to only use the nsrauth when communicating with the host, type:

  ```
  update auth methods: 137.69.160.0/24,nsrauth
  ```

- To configure all hosts in the datazone to use the nsrauth when communicating with the host except for a host with the IP address 137.69.160.10 which should try oldauth first, type the following two lines:

  ```
  update auth methods: 137.69.160.10,oldauth/nsrauth
  0.0.0.0,nsrauth
  ```

## Maintaining the NSRLA resource

The NSRLA resource in the nsrexec database contains unique information that identifies a NetWorker host to other NetWorker hosts.

Use NMC or the `nsradmin` command to export and import the NSRLA resource. Use the `nwinstcreate` program to create a customized private key and certificate.

### Exporting the local host credentials

Export the local host credentials for a host to ensure that you have a copy of the unique credential information. If data loss or corruption of the NSRLA resource occurs, you can import the local host credentials and restore the original local host credentials to the NSRLA resource.

**Exporting the local host credentials by using NMC**

Connect to the NetWorker server with NMC and export the local host credentials.

**Before you begin**

The account that you use to connect to the NetWorker server must have permission to access the NSRLA database on the target host.

You cannot use NMC to export the local host credentials for a NetWorker host that does not have an existing client resource that is configured on the NetWorker server.

**Procedure**

1. On the **Administration** window, select **Hosts**.

   The **Hosts Management** window appears.

2. In the **Hosts** pane, right-click the target host, and then select **Configure Local Agent**.
3.

On the **Advanced** tab, in the **NW instance info operations** attribute, select **Export**.

4. In the **NW instance info file** attribute, specify the path and name of the file that contains the exported information.

   For Windows paths, use a forward slash (/) when you specify the path. For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.

5. Click **OK**.

### Results

NetWorker exports the local host credential information to the file you specify, on the target host.

**Note:** If you do not specify a path to the file, NetWorker creates the export file in the `C:\Windows\system32` directory on a Windows host and in the `/nsr/cores/nsrexecd` directory on a UNIX host.

### Exporting the local host credentials by using nsradmin

Use the `nsradmin` program to export the local host credentials.

### Before you begin

Connect to the target host with an account that has administrator access to the NSRLA database. You must configure access privileges to the NetWorker client database.

### Procedure

1. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

2. Set the query type to NSRLA:

   ```
   . type: NSRLA
   ```

3. Configure the **NW instance info operations** attribute and the **NW instance info file** attribute to export the resource information:

   ```
   update "NW instance info operations: export", "NW instance info
   file: pathname_filename"
   ```

   For example, to export the information to the `/home/root/export.txt` file on a UNIX host, type:

   ```
   update NW instance info operations: export; NW instance info
   file: /home/root/export.txt
   ```

   For Windows paths, use a forward slash (/) when you specify the path.
   For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.

### Results

NetWorker exports the local host credential information to the file you specify, on the target host.

## Create a custom certificate and private key for a host

NetWorker automatically creates certificate and private keys for each NetWorker host. However, you can create a certificate and a private key for a host manually.

You might want to do this in special cases, such as when the company policy stipulates that a host must use a certificate and private key that a trusted random number generation utility creates. You can import the new certificate and key information to the NSRLA resource of the host and import the information into the NSR peer information resource on each host within the enterprise. NetWorker supports self-signed certificates. A certificate that is signed by a certificate authority (CA) cannot be imported.

### Creating a custom certificate and private key

Use the `nwinstcreate` command to create a custom certificate and private key.

#### About this task

Perform the following steps from a command prompt on the host that uses the custom certificate and private key. You can import the custom file into the NSRLA resource on the local host or you can import the custom file into the **NSR Peer Information** resource for the host, on other hosts in the datazone.

#### Procedure

1. Start the `nwinstcreate` program:

   ```
   nwinstcreate -ix
   ```

2. On the `Enter the file name to save NetWorker identify information into` prompt, specify the name of the file to save the custom certificate and private key or accept the default file name and location.
3. On the `Enter a unique NetWorker instance name to identify your machine` prompt, specify an instance name or accept the default value (hostname of the machine).

   NetWorker uses the specified value in the *my hostname* attribute by default.
4. On the `Enter the NetWorker instance id` prompt, specify a unique value to identify the host or accept the default value.
5. On the `Enter the file containing the private key` prompt, specify the path and file name of a PEM formatted file that contains the private key for this host. If the organization does not have a private key, leave the prompt blank and NetWorker generates the private key for the host.
6. On Windows hosts only, ensure that the Windows Local System Account (System) has read, write, and modify privileges for the file that contains the custom certificate and key.

## Importing local host credentials

If you used the `nwinstcreate` program to export the local host credentials for the host or you created custom credentials, then you can use NMC or `nsradmin` to import the information into the NSRLA resource on a host.

When NSRLA corruption occurs and the `nsrexecd` program creates new local host credentials on a host, the nsrauth process rejects all connection attempts between the host and all other hosts in the datazone that have communicated with the host before the corruption. The nsrauth process rejects the connection because information in the **NSR Peer Information** resource for the host differs from the new local host credentials that the host provides when it tries to establish a connection. To resolve

this issue, import a copy of the local host credentials for the host into the local NSRLA resource. This workaround ensures that the local host credentials for the host match the information that is stored in the **NSR Peer Information** resource on all other hosts in the datazone. Resolving conflicts between the local host credentials and NSR Peer Information resource on page 98 describes how to resolve this issue if an exported copy of the local host credential information is not available.

**Importing local host credentials by using NMC**

Connect to the NetWorker server with NMC and import the local host credentials.

**Before you begin**

The account that you use to connect to the NetWorker server must have permission to access the NSRLA database on the target host.

**Procedure**

1. Copy the file that contains the exported local host credentials to the target host.
2. On UNIX platforms, ensure that the root user has read and write permissions for the credential file.

   For example: `chmod 600` ***`export_file_name`***
3. On the **Administration** window, select **Hosts**.

   The **Hosts Management** window appears.
4. In the **Hosts** pane, right-click the target host, and then select **Configure Local Agent**.
5. On the **Advanced** tab, in the **NW instance info operations** attribute, select **Import**.
6. In the **NW instance info file** attribute, specify the path and name of the file that contains the exported information.

   For Windows paths, use a forward slash (`/`) when you specify the path.
   For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.
7. Click **OK**.

**Results**

NetWorker imports the local host credential information to the target host.

**Importing localhost credentials by using nsradmin**

Use the `nsradmin` program to import local host credentials from a file into the NSRLA resource of a host.

**Before you begin**

Connect to the target host with an account that has administrator access to the NSRLA database. You must configure access privileges to the NetWorker client database.

**Procedure**

1. Copy the file that contains the exported local host credentials to the target host.
2. On UNIX platforms, ensure that the root user has read and write permissions for the credential file.

   For example: `chmod 600` ***`export_file_name`***

3. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

4. Set the query type to NSRLA:

   ```
   . type: NSRLA
   ```

5. Configure the **NW instance info operations** attribute and the **NW instance info file** attribute to import the resource information:

   ```
   update NW instance info operations: import; NW instance info
   file: pathname_filename
   ```

   For example, to export the information to the `/home/root/mnd_credentials.txt` file on a UNIX host, type:

   ```
   update NW instance info operations: import; NW instance info
   file: /home/root/mnd_credentials.txt
   ```

   For Windows paths, use a forward slash (`/`) when you specify the path.For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.
   For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.

6. When prompted to update the resource, type **`Yes`**.
7. Exit the `nsradmin` program:

   ```
   quit
   ```

## Maintaining nsrauth authentication credentials

This section describes how to maintain the local host credentials and the NSR Peer Information resource.

### Creating the NSR Peer Information resource manually

When a NetWorker host begins a connection with another host for the first time, NetWorker automatically creates an NSR Peer Information resource for the beginning host in the nsrexec database on the target host. NetWorker uses the information that is contained in the NSR Peer Information resource to verify the identity of the beginning host on subsequent authentication attempts. Manually create the NSR Peer Information resource on the target client before the two hosts communicate for the first time, to eliminate the possibility that an attacker could compromise this process.

**Creating the NSR Peer Information resource manually by using NMC**
Connect to the NetWorker server with NMC to create a new NSR Peer Information resource for a host.

**Before you begin**

The account that you use to connect to the NetWorker server must have permission to access the NSRLA database on the target host.

Review the contents of the file that contains the exported local host credentials for the host and make note of the values in the **Name**, **My hostname**, and **NW Instance ID** attributes.

### Procedure

1. Copy the file that contains the exported local host credentials to the target host.
2. To connect to the NetWorker server, use the NMC.
3. On the **View** menu, select **Diagnostic mode**.
4. On the **Administration** window, select **Hosts**.

   The **Hosts Management** window appears.
5. Right-click the target host, and then select **Host Details**.
6. In the **Certificates** pane, right-click, and then select **New**.
7. On the **Create certificate** window, in the **Change certificate** list box, select **Load certificate from file**.
8. In the **Name** field, type the *Name* value from the credential file.
9. In the **Instance ID** field, type the *NW Instance ID* value from the credential file.
10. In the **Peer Hostname** field, type the *My Hostname* value from the credential file.
11. In the **Change certificate** list box, select **Load certificate from file**.
12. In the **Certificate file to load** attribute, specify the path and name of the file that contains the exported local host credentials.

    For Windows paths, use a forward slash (`/`) when you specify the path. For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.
13. On UNIX platforms, ensure that the root user has read and write permissions for the credential file.

    For example: `chmod 600` ***`export_file_name`***
14. Click **OK**.

### Creating the NSR Peer Information by using nsradmin

Use the `nsradmin` program on a host to create an NSR Peer Information resource for a host.

### Before you begin

Connect to the target host with an account that has administrator access to the NSRLA database. You must configure access privileges to the NetWorker client database.

### Procedure

1. Copy the file that contains the exported local host credentials to the target host.
2. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexecd
   ```
3. Create the **NSR Peer Information** resource:

   ```
   create type: NSR Peer Information; name:hostname; NW Instance:
   nw_instance_id; peer hostname: my_hostname
   ```

   where:

- *hostname* is value that appears in the **Name** attribute in the credential file.
- *NW_instance_id* is the value that appears in the **NW Instance ID** attribute in the credential file.
- *my_hostname* is the value that appears in the **My hostname** attribute in the credential file.

4. When prompted to create the resource, type `Yes`.
5. Set the current query to the new **NSR Peer Information** resource:

   ```
   . type: NSR Peer Information; name: hostname
   ```

6. Update the new **NSR Peer Information** resource to use the exported certificate:

   ```
   update: change certificate: load certificate from file;
   certificate file to load: pathname_filname
   ```

   For Windows paths, use a forward slash (`/`) when you specify the path. For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.

7. When prompted to update the resource, type `Yes`.
8. Display the hidden properties:

   ```
   option hidden
   ```

9. Display the new **NSR Peer Information** resource:

   ```
   print . type: NSR Peer Information;name: hostname
   ```

## Deleting the NSR Peer Information resource

When the local host credentials for a NetWorker host change, authentication attempts from the host to other hosts fail because the credential information stored in the target host does not match the local host credential information that is provided by the initiating host.

Use the `nsradmin` program or the **Local Host** window in NMC to delete the **NSR Peer Information** resource for the initiating host on the target host. The next time the initiating host attempts to connect to the target host, the nsrauth authentication process will use the current local host credentials to create a new **NSR Peer Information** resource for the initiating host.

### Deleting the NSR Peer Information resource by using NMC

Use NMC to connect to the NetWorker server and delete the NSR Peer Information resource for a NetWorker host.

#### Before you begin

The account that you use to connect to the NetWorker server must have permission to access the NSRLA database on the target host.

**Note:** You cannot use NMC to delete the **NSR Peer Information** resource for a NetWorker host that does not have an existing client resource that is configured on the NetWorker server.

#### Procedure

1. On the **Administration** window, select **Hosts**.

The **Hosts Management** window appears.

2. Right-click the NetWorker host with the **NSR Peer Information** resource that you want to delete, and then select **Host Details**.

   **Note:** The NetWorker host does not appear in the **Local Hosts** section when a client resource does not exist on the NetWorker server.

   The **Certificate** window displays a list of NSR Peer Information resources stored in the nsrexec database on the host.

3. In the **Certificate** pane, right-click the certificate that you want to delete, and then select **Delete**.
4. When prompted to confirm the delete operation, select **Yes**.

   If you receive the error, `User username on machine hostname is not on administrator list`, you cannot modify the resource until you configure the NSRLA access privileges on the target host. The section "Configuring NSRLA access privileges" provides more information.

### Results

The target host creates a new NSR Peer Information resource for the initiating host the next time that the initiating host attempts to establish a connection with the target host.

**Deleting the NSR Peer Information resource by using nsradmin**

To delete the NSR Peer Information resource for the initiating host, use the `nsradmin` command on the target host.

### Before you begin

Connect to the target host with an account that has administrator access to the NSRLA database. You must configure access privileges to the NetWorker client database.

### Procedure

1. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

2. Set the query type to the **NSR Peer Information** resource of the initiating host:

   ```
   . type: nsr peer information;name:initiating_host_name
   ```

   For example, if the hostname of the initiating host is pwd.corp.com, type:

   ```
   . type: nsr peer information;name: pwd.corp.com
   ```

3. Display all attributes for the **NSR Peer Information** resource:

   ```
   show
   ```

4. Print the attributes for the **NSR Peer Information** resource and confirm that the name and peer hostname attributes match the hostname of the initiating host:

   ```
   print
   ```

5. Delete the `NSR Peer Information` resource:

   ```
   delete
   ```

6. When prompted to confirm the delete operation, type `y`.
7. Exit the `nsradmin` program:

   ```
   quit
   ```

#### Results

The target host creates a new NSR Peer Information resource for the initiating host the next time that the initiating host attempts to establish a connection with the target host.

## Resolving conflicts between the local host credentials and NSR Peer Information resource

After two NetWorker hosts successfully authenticate each other, the target host creates an NSR Peer Information resource to store the local host credentials of the initiating host. The target host uses attributes that are stored in the NSR Peer Information resource to validate connection requests from the target host. When unexpected data loss or corruption occurs in the NSRLA resource of the initiating host, the nsrexecd process creates new local host credentials. When a host with new local host credentials attempts to connect another host, the target host rejects the connection request if an NSR Peer Information resource exists for the initiating host because the credentials do not match the contents of the NSR Peer Information resource.

When the local host credentials change for a host, all target hosts that have had a prior connection with the host rejects a connection attempt. To resolve this issue, type the following command to remove **NSR Peer Information** resources from the nsrexec database:

```
nsradmin -s NetWorker_server -p nsrexec -C -y "NSR peer information"
```

where you specify the `-s NetWorker_server` option when you type the command from the target host.

Alternately, perform the following steps:

- Manually delete the **NSR Peer Information** resource for the initiating host in the NetWorker client database of each target host.

  **Note:** If the NetWorker server is the initiating host, delete the **NSR Peer Information** resource on each host in the datazone.
- Import a backup copy of the local host credentials on the initiating host.

### Importing localhost credentials into the NSR Peer Information resource

Use the `nsradmin` program or the Local Host window in NMC to import the private key and certificate into the NSR Peer Information resource for the initiating host, on the target host.

The next time the initiating host attempts to connect to the target host, the nsrauth authentication process uses the imported local host credentials to create a new **NSR Peer Information** resource for the initiating host.

#### Importing localhost credentials by using NMC

Use NMC to connect to the NetWorker server and import the certificate and private key into the NSR Peer Information resource for a NetWorker host.

#### Before you begin

The gstd process owner must have permission to update the nsrexec database on the target host. You must configure access privileges to the NetWorker client database.

### Procedure

1. On the **Administration** window, select **Configuration**.
2. In the left navigation pane, expand the NetWorker server, and then expand the **Local Hosts** resource.
3. Right-click the target host, and then select **Configure Local Agent**.
4. Select the NetWorker host with the **NSR Peer Information** resource that you want to modify.
5. In the **Certificate** window, right-click the certificate that you want to delete, and then select `Properties`.
6. On the **Create certificate** window, in the **Change certificate** list box, select **Load certificate from file**.
7. In the **Certificate file to load** attribute, specify the path and name of the file that contains the exported local host credentials.

   If you receive the error, `User username on machine hostname is not on administrator list`, you cannot modify the resource until you configure the NSRLA access privileges on the target host. The section "Configuring NSRLA access privileges" provides more information.
8. Click **OK**.

## Importing localhost credentials by using nsradmin

Use `nsradmin` to import the certificate and private key into the NSR Peer Information resource for a NetWorker host.

### Before you begin

Connect to the target host with an account that has administrator access to the NSRLA database. You must configure access privileges to the NetWorker client database.

### Procedure

1. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

2. Set the query type to the **NSR Peer Information** resource of the initiating host:

   ```
   . type: nsr peer information;name:initiating_host_name
   ```

   For example, if the hostname of the initiating host is pwd.corp.com, type:

   ```
   . type: nsr peer information;name: pwd.corp.com
   ```

3. Display hidden resources:

   ```
   option hidden
   ```

4. Print the attributes for the **NSR Peer Information** resource and confirm that the name and peer hostname attributes match the hostname of the initiating host:

   ```
   print
   ```

5. Update the new **NSR Peer Information** resource to use the exported certificate:

```
update: change certificate: load certificate from file;
certificate file to load: pathname_filname
```

For Windows paths, use a forward slash (/) when you specify the path. For example, when the `mnd_credentials.txt` file is in `c:\users`, specify: `c:/users/mnd_credentials.txt`.

6. When prompted to update the resource, type **Yes**.
7. Display the hidden properties:

```
option hidden
```

8. Display the new **NSR Peer Information** resource:

```
print . type: NSR Peer Information;name: hostname
```

## Generating a new host certificate key

Use NMC to create a new host certificate key for a NetWorker host.

### Before you begin

The account that you use to connect to the NetWorker server must have permission to access the NSRLA database on the target host.

### Procedure

1. On the **Administration** window, select **Hosts**.

   The **Hosts Management** window appears.
2. In the **Hosts** pane, right-click the target host, and then select **Configure Local Agent**.
3. Select the **Advanced** tab.
4. From the **NW Instance Info Operations** attribute list, select **New Keys**.
5. Click **OK**.

### Results

NetWorker generates a new certificate for the NetWorker host. Delete all existing **Peer Information** resources for the host, on other NetWorker hosts. Deleting the NSR Peer Information resource on page 96 describes how to delete the resource.

# Removing SHA1 credentials from database

In order to communicate with clients of older and newer versions, the nsrexecd process generates both SHA1 and SHA2 credentials. However, in certain cases, SHA1 credentials are not required as only new version of clients are present in the datazone. To address this issue, a new (hidden) option `delete SHA1 certificates` is introduced in the `nsradmin` NSRLA resource that helps the user to delete SHA1 credentials if not used.

### Before you begin

Use the `nsradmin` program to delete SHA1 credentials.

The account that you use to connect to the NetWorker server must have permission to access the NSRLA database on the target host.

### Procedure

1. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

2. Set the query type to NSRLA:

   ```
   . type: NSRLA
   ```

3. Display hidden resources:

   ```
   option hidden
   ```

4. Print the attributes for the NSRLA resource:

   ```
   print
   ```

5. Update the attribute *delete sha1 certificates* : `Yes`.

   ```
   update delete sha1 certificates:Yes;
   ```

6. When prompted to update the resource:

   type `Yes`

   This deletes the credentials from database.

7. Verify by displaying the NSRLA resource again:

   ```
   print
   ```

## Procedure to recreate SHA1 and SHA2 credentials

### About this task

When a new client (pre-9.1.1) is added in the datazone then SHA1 credentials are required for communicating with the new hosts. To achieve this revert *delete sha1 certificates* to `No`.

Perform the following steps to recreate the SHA1 and SHA2 credentials:

### Procedure

1. Connect to the nsrexec database:

   ```
   nsradmin -p nsrexec
   ```

2. Set the query type to NSRLA:

   ```
   .type: NSRLA
   ```

3. Display hidden resources:

   ```
   option hidden
   ```

4. Print the attributes for the NSRLA resource:

   ```
   print
   ```

5. Update the attribute *delete sha1 certificates*: `No`.

   ```
   update delete sha1 certificates:No;
   ```

6. When prompted to update the resource:

   type `Yes`

7. Stop and re-start the nsrexecd process or import the certificates from the host. For more information refer to the topic Importing local host credentials.

## Component authorization

NetWorker provides you with the ability to restrict remote program executions or client-tasking rights on a NetWorker host.

You can also:

- Define users that can access the data of a NetWorker host and recover the data to a different NetWorker host.
- Restrict client-initiated backups to the NetWorker server.
- Configure the NetWorker server to prevent the start up of new save and recover sessions.

### Restricting remote program executions and client-tasking rights

When a NetWorker host requests the right to perform a task on another NetWorker host, the destination host compares the name of the requesting host to the list of hostnames that are specified in the servers file on the destination NetWorker host. If the hostname of the requesting host is not in the `servers` file, then the requesting host does not have client-tasking rights and the destination host rejects the request.

The following table provides a list of tasks that require client-tasking rights.

**Table 9** Operations that require entries in the servers file

| Operation | Entries required in the client servers file |
|---|---|
| Archive request | Add the FQDN or shortname of the NetWorker server. |
| Scheduled backup | Add the FQDN or shortname of the NetWorker server.<br>For a clustered NetWorker server, add the long or shortname of the virtual NetWorker and all physical nodes. |
| Remote directed recovery | Add the FQDN or shortname of the administering client to the `servers` file on the destination client. |
| NDMP DSA backup | Add the FQDN or shortname of the NetWorker client that starts the backup.<br>**Note:** For NDMP, the servers file resides in the NetWorker Server. |

**Note:** Before adding the FQDN or shortname to the NetWorker server file, ensure that the host name resolution for FQDN or short name is working correctly.

The software installation process on Windows and Solaris allows you to specify a list of hosts to add to the `servers` file. To change the servers file after the installation completes or to specify hosts on operating systems that do not allow you to configure the file during the installation process, use a text editor to edit the `servers` file. The `servers` file resides in the following locations:

- On UNIX and Mac NetWorker hosts:`/nsr/res`
- On Windows NetWorker hosts:*`NetWorker_installation_path`*`\res`

When you add a NetWorker host to the `servers` file, ensure that you perform the following tasks:

- Specify the FQDN or shortname for the host.
- Specify one hostname on each line.

- Restart the nsrexecd service on the host, after you save the file.

**Note:** If the `servers` file is empty or does not exist, then any NetWorker host has client-tasking rights to the host.

On UNIX computers, you can start the `nsrexecd` daemon with the *-s servername* option to assign client-tasking rights to a host. The use of the *-s* option to start the `nsrexecd` daemon supersedes the use of the servers files to restrict client-tasking rights.

## Configuring remote recover access rights

You can control client recover access through the Client resource. The Remote Access attribute displays the user accounts that are able to recover save sets from the NetWorker host to different NetWorker host. Add or remove user names depending on the level of security the files require.

### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

### About this task

Only the users who are specified in the **Remote Access** attribute and the following user accounts can perform remote or directed recoveries of the target client data:

- The root user on a target UNIX host.
- Member of the local 'Administrators' group on a target Windows host.
- Members of the 'Application Administrator' user group on the NetWorker Server.
- Members of a NetWorker Server user group that has the 'Change Security Settings' privilege.

The *NetWorker Administration Guide* describes how to configure and perform remote and directed recoveries.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the left navigation pane, select **Clients**.
3. Right-click the client, and then select **Properties**.
4. On the **Globals (2 of 2)** tab, in the `Remote Access` attribute, specify the user accounts that you want to have remote recover access to the client, in one of the following formats:
   - `user=`*username*
   - *username*`@`*hostname*
   - *hostname*
   - `host=`*hostname*
   - `user=`*username*`, host=`*hostname*

   **Note:** If you enter a *hostname* or *host=hostname* in the **Remote Access** attribute, then any user on the specified host can recover the files for the client. To enter a username without specifying the host, type `user=`*username*.
5. Click **OK**.

## Restrict backup and recover access to the NetWorker server

You can configure the NetWorker server to allow or prevent manual save operations, accept or reject new save sessions, and accept or reject new recovery sessions.

### Restricting manual save operations

Use the manual saves attribute in the NSR resource to allow or prevent client-initiated backups to the NetWorker server. This option is enabled by default.

#### Before you begin

Connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

#### Procedure

1. From the **Administration** window, click **Server**.
2. In the left navigation pane, right-click the NetWorker server, and then select **Properties**.
3. On the **General** tab, clear **Manual saves**.

#### Results

Users cannot use the `save` command or the NetWorker User application (Windows clients only) to perform backups from any NetWorker host to the NetWorker server.

### Rejecting new save sessions

You can configure the NetWorker server to reject new save sessions from an in-progress manual or scheduled backup. For example, the NetWorker server can reject new save sessions and allow routine NetWorker Server maintenance, such as a server restart, to occur without cancelling in-progress backup operations during the shutdown process. By default, the NetWorker server is configured to accept new save sessions. Perform the following steps to prevent the NetWorker server from accepting new save sessions.

#### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

#### Procedure

1. From the **Administration** window, click **Server**.
2. In the left navigation pane, right-click the NetWorker server, and then select **Properties**.
3. On the **Security** tab, in the **Accept new sessions** attribute, select **No**.

### Rejecting new recover and clone sessions

You can configure the NetWorker server to reject new recover and clone sessions. For example, NetWorker can reject recover sessions and allow routine NetWorker Server maintenance, such as a server restart, to occur without cancelling in-progress recover operations during the shutdown process. By default the NetWorker server is configured to accept new recover sessions. Perform the following steps to prevent the NetWorker server from accepting new recover sessions.

#### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

### Procedure

1. From the **Administration** window, click **Server**.
2. In the left navigation pane, right-click the NetWorker server, and then select **Properties**.
3. On the **Security** tab, in the **Accept new recover sessions** attribute, select **No**.

# Generate self signed certificate

### About this task

Ensure the following:

- The owner and issuer details are correct.
  - Owner: CN=gst
  - Issuer: CN=gst
- The certificate must be valid for a year.
- The certificate must be of type x509.
- The private key must be generated separately.

### Procedure

1. Generate a new certificate and private key using your certificate generator or OpenSSL.

   **`openssl req -x509 -nodes -sha512 -days 365 -newkey rsa:2048 -keyout server.key -out server.crt`**

   **Note:** `server.rct` is the certificate name and `server.key` is the private key.

2. Stop the `gstddb` service.
3. Create a copy of the existing `server.crt` and `server.key` files, located in the `C:\Program Files\EMC NetWorker\Management\nmcdb\pgdata` directory.
4. Replace the existing `server.crt` and `server.key` files with the new files.
5. Start `gstddb` service.

# Enabling two factor authentication for AD and LDAP users

You can use NMC to enable two factor authentication for AD and LDAP users.

### Procedure

1. On Linux, modify the `/opt/nsr/admin/gst_linux.sh` script and add the following at the beginning of the script:

   ```
   GST_LDAP_USING_2FA="true"
   export GST_LDAP_USING_2FA
   ```

2. On Windows, do the following to set the environment variable:

   a. Browse to **Control Panel** > **System and Security** > **System** > **Advanced Settings**.

b. On the **General** tab, click **Environment Variables**.

c. In the **System variables** section, click **New**.

d. In the **Variable** name field, type: `GST_LDAP_USING_2FA`, and in the **Variable** value field, type: True. Click **OK**.

3. Log in to NMC as an Administrator.
4. From the NMC**Console** window, click **Setup**.
5. In the left pane, select **Users**.

   a. Right-click the service account (for example, svc_nmc_*), and then select **Properties**.

   b. On the **Groups** window, select **Administrators** and click **OK** to add the service account user as a part of this group.

6. Restart the EMC GST service:

   - Linux: `/etc/init.d/gstd start`
   - Windows: Start the **EMC GST** service

7. Configure AD and LDAP users. The *NetWorker Security Configuration Guide* provides information on configuring AD and LDAP users.
8. Connect to the NMC server with an LDAP or AD user.

# CHAPTER 3

# Log Settings

This chapter describes how to access and manage the logs files available in NetWorker.


- NetWorker log files.....108
- NetWorker Authentication Service logs.....131

# NetWorker log files

This section provides an overview of the log files that are available on NetWorker hosts and the NMC server.

## NetWorker Server log files

This section provides a summary of the log files available on a NetWorker Server and log file management.

**Table 10** NetWorker Server log files

| Component | File name and default location | Description |
|---|---|---|
| NetWorker Server daemons | UNIX: `/nsr/logs/daemon.raw`<br>Windows: `C:\Program Files\EMC NetWorker\nsr\logs\daemon.raw` | Main NetWorker log file.<br>Use the `nsr_render_log` program to view the contents of the log file. |
| Client fix | UNIX:<br>• `/nsr/logs/client_fix`<br>• `/nsr/logs/client_fix.raw`<br>Windows:<br>• `C:\Program Files\EMC NetWorker \nsr\logs\client_fix`<br>• `C:\Program Files\EMC NetWorker \nsr\logs\client_fix.raw` | Contains status information that is related to the use of the `nsr_client_fix` command. |
| NetWorker Server generated syslog messages and `daemon.notice` | UNIX:<br>OS log file that is defined by system log configuration file.<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr \logs\messages` | Contains general NetWorker error messages. |
| NetWorker Servergenerated syslog<br>messages `local0.notice` and `local0.alert` | Log file name and location that is defined by the system log configuration file. | UNIX only, OS log file.<br>**Note:** NetWorker does not modify the `syslog.conf` file to configure `local0.notice` and `local0.alert`. Vendor specific documentation describes how to configure `local0.notice` and `local0.alert` |
| **Disaster recovery** command line wizard, `nsrdr` program | UNIX:<br>`/nsr/logs/nsrdr.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr \logs\nsrdr.log` | Contains detailed information about the internal operations that are performed by the `nsrdr` program. NetWorker overwrites this file each time you run the `nsrdr` program. |

**Table 10** NetWorker Server log files (continued)

| Component | File name and default location | Description |
|---|---|---|
| Index log | UNIX:<br>`/nsr/logs/index.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\index.log` | Contains warnings about the size of the client file index and low disk space on the file system that contains the index files. By default, the **Index size** notification on the NetWorker Server sends information to the log file. |
| Hypervisor | UNIX:<br>`/nsr/logs/Hypervisor/hyperv-flr-ui/hyperv-flr-ui.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\hyperv-flr-ui\hyperv-flr-ui.log` | Contains status information about the Hyper-V FLR interface. |
| VMware protection policies | UNIX:<br>`/nsr/logs/Policy/`*VMware_protection_policy_name*<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\Policy\`*VMware_protection_policy_name* | Contains status information about VMware Protection Policy actions. NetWorker creates a separate log file for each action. |
| Policies | UNIX:<br>`/nsr/logs/policy.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\policy.log` | Contains completion information about VMware Protection Policies. By default, the **VMware Protection Policy Failure** notification on the NetWorker Server sends information to the log file. |
| Snapshot management | UNIX:<br>`/nsr/logs/nwsnap.raw`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\nwsnap.raw /nsr/logs/nwsnap.raw` | Contains messages that are related to snapshot management operations. For example, snapshot creation, mounting, deletion, and rollover operations. Use the `nsr_render_log` program to view the contents of the log file. |
| Migration | UNIX:<br>`/nsr/logs/migration`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\migration` | Contains log files that provide detailed information about the migration of attributes in an 8.2.x and earlier resources during an update of the NetWorker Server. The *NetWorker Installation Guide* provides more information about all the migration log files. |

**Table 10** NetWorker Server log files (continued)

| Component | File name and default location | Description |
|---|---|---|
| Media management | UNIX:<br>`/nsr/logs/media.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\media.log` | Contains device related messages. By default, the device notifications on the NetWorker Server send device related messages to the `media.log` file on the NetWorker Server and each Storage Node. |
| Recovery Wizard | UNIX:<br>`/nsr/logs/recover/`*recover_config_name_YYYYMMDDHHMMSS*<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs\recover\`*recover_config_name*_YYYYMMDDHHMMSS | Contains information that can assist you in troubleshooting recovery failures. NetWorker creates a log file on the NetWorker Server for each recover job. |
| Package Manager log | UNIX:<br>`/nsr/logs/nsrcpd.raw`<br>Windows:<br>`C:\Program Files\EMC NetWorker\logs\nsrcpd.raw` | Contains information that is related to the Package Manager and the `nsrpush` command. Use the `nsr_render_log` program to view the contents of the log file. |
| Rap log | UNIX:<br>`/nsr/logs/rap.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\logs\rap.log` | Records configuration changes that are made to the NetWorker Server resource database. |
| Security Audit log | UNIX:<br>`/nsr/logs/`*NetWorker_server*`_sec_audit.raw`<br>Windows:<br>`C:\Program Files\EMC NetWorker\logs\`*Networker_server*`_sec_audit.raw` | Contains security audit related messages. |

## NMC server log files

This section provides a summary of the log files available on an NMC server.

**Table 11** NMC server log files

| Component | File name and default location | Description |
|---|---|---|
| NMC server log files | Linux:<br>`/opt/lgtonmc/management/logs/gstd.raw`<br>Windows:<br>`C:\Program Files\EMC NetWorker\Management\logs\gstd.raw` | Contains information that is related to NMC server operations and management. Use the `nsr_render_log` program to view the contents of the log file. |
| NMC server database conversion | Linux:<br>`/opt/lgtonmc/logs/gstdbupgrade.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\Management\logs\gstdbupgrade.log` | Contains the results of the NMC server database conversion that is performed during an upgrade operation. |
| NMC web server | Linux:<br>`/opt/lgtonmc/management/logs/web_output`<br>Windows:<br>`C:\Program Files\EMC NetWorker\Management\logs\web_output` | Contains messages for the embedded Apache httpd web server on the NMC server. |
| NMC server database log files | Linux:<br>`/opt/lgtonmc/management/nmcdb/pgdata/db_output`<br>Windows:<br>`C:\Program Files\EMC NetWorker\Management\nmcdb\pgdata\db_output` | Contains messages for the embedded PostgreSQL database server on the NMC server. |

## NetWorker Client log files

This section provides a summary of the log files available on a NetWorker Client.

**Table 12** Client log files

| Component | File name and default location | Description |
|---|---|---|
| NetWorker Client daemons | UNIX:<br>`/nsr/logs/daemon.raw`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\logs \daemon.raw /nsr/logs/ daemon.raw` | Main NetWorker log file.<br>Use the `nsr_render_log` program to view the contents of the log file. |
| User log | `C:\Program Files\EMC NetWorker\logs \networkr.raw` | For Windows only, contains a record of every file that was part of an attempted manual backup or recovery operation that is started by the NetWorker User program. Subsequent manual backup or recover operations overwrite the file. Use the `nsr_render_log` program to view the contents of the log file. |
| Windows Bare Metal Recovery (BMR) | The following files in the `X:\Program Files\EMC NetWorker\nsr\logs\` directory:<br>`ossr_director.raw` | Contains the recovery workflow of the `DISASTER_RECOVERY:\` and any errors that are related to recovering the save set files or Windows ASR writer errors. Use the `nsr_render_log` program to view the contents of the log file. |
| | `recover.log` | Contains the output that is generated by the NetWorker `recover.exe` program and error messages that are related to critical volume data recovery. |
| | `winPE_wizard.log` | Contains workflow information that is related to the **NetWorker BMR** wizard user interface. |
| | `winpe_nw_support.raw` | Contains output from the `winpe_nw_support.dll` |

**Table 12** Client log files (continued)

| Component | File name and default location | Description |
|---|---|---|
| | | library. The output provides information about communications between the **NetWorker BMR** wizard and the NetWorker Server.<br><br>Use the `nsr_render_log` program to view the contents of the log file. |
| | `winpe_os_support.log` | Contains output information that is related to Microsoft native API calls. |
| CloudBoost - NetWorker Client | The following log files in the<br><br>`/nsr/logs/cloudboost`<br><br>directory:<br><br>`MagFS.log.ERROR.`*`date-timestamp.pid`*`.txt`<br><br>`MagFS.log.FATAL.`*`date-timestamp.pid`*`.txt`<br><br>`MagFS.log.INFO.`*`date-timestamp.pid`*`.txt` | These files appear on a client direct-enabled NetWorker Client and contain information about data stored on a CloudBoost device. The severity of the message determines which log file that error message is written to.<br><br>The maximum size of the log files are 100 MB.<br>Before a client direct backup, the `save` process checks the size of the file. When the maximum size is reached, `save` starts an automatic trimming mechanism, which renames and compresses the log file. The maximum number of versions for a file is 10. When the number of renamed log files reaches the maximum version value, NetWorker removes the oldest log when a new version of the log file is created.<br><br>**Note:** The Troubleshooting manual backups section of the *NetWorker Administration Guide* describes how to use the *CB_LOG_DIR_LOCATION* environment variable to change the default log file location. |

**Table 12** Client log files (continued)

| Component | File name and default location | Description |
|---|---|---|
| CloudBoost - CloudBoost Appliance | The following log files in the `/nsr/logs/cloudboost` directory:<br>`MagFS.log.ERROR.`*`date-timestamp.pid`*`.txt`<br>`MagFS.log.FATAL.`*`date-timestamp.pid`*`.txt`<br>`MagFS.log.INFO.`*`date-timestamp.pid`*`.txt` | These files appear on the CloudBoost appliance and contain information about operations performed on a CloudBoost device. The severity of the message determines which log file that error message is written to.<br>The maximum size of the log files are 100 MB. When the maximum size is reached, the `nsrmmd` process starts an automatic trimming mechanism, which renames and compresses the log file. The maximum number of versions for a file is 10. When the number of renamed log files reaches the maximum version value, NetWorker removes the oldest log when a new version of the log file is created. |

## View log files

NetWorker sends messages to two types of logs. Plain text log files that are saved with the `.log` extension and unrendered log files that are saved with the `.raw` extension.

The `.log` files and the messages that appear in NMC use the locale setting of the service that generates the log message. To view the contents of `.log` files, use any text editor. Before you can view `.raw` files in a text editor, render the `.raw` file into the locale of the local computer. You can use the `nsr_render_log` command manually render the raw log files or you can configure NetWorker to render the log files at runtime.

The `nsr_render_log` command renders internationalized NetWorker log files in to the current locale of the host that the user uses to run the program. All other log files, as well as messages displayed in NMC, use the locale of the service that is generating the log message. The `nsr_render_log` program is non-interactive. Use command line options to specify the log file that you want to view and the format of the output. The `nsr_render_log` program sends the results to `stdout`. You can redirect and save the output to a file.

## Rendering a raw file manually

The `nsr_render_log` program is non-interactive. When you use the `nsr_render_log` program to render the contents of the `.raw` file to the locale of the host where you run the command, `nsr_render_log` prints the output to `stdout`. You can redirect this output to a file and view the output in a text editor.

### Before you begin

The `bin` subdirectory in the NetWorker installation directory contains the `nsr_render_log` program. If the `bin` directory is not in the search path of the host where you run the command, include the full path when you use the `nsr_render_log` program. If you do not run the `nsr_render_log` command from the directory that contains the `.raw` file, include the path to the `.raw` file.

### About this task

The `nsr_render_log` program supports a number of options that allow you to filter the contents of a `.raw` file and render the contents into an easy to read format.

### Procedure

- To render a raw file into a format similar to a `.log` file and redirect the output to a text file, type: `nsr_render_log -c -empathy` ***raw_filename*** `1>`***output_filename*** `2>&1`

  where:

  - *raw_filename* is the name of the unrendered file. For example, `daemon.raw`
  - *output_filename* is the name of the file to direct the output to
  - `-c` suppresses the category
  - `-m` suppresses the message ID
  - `-e` suppresses the error number
  - `-a` suppresses the activity ID
  - `-p` suppresses the process ID
  - `-t` suppresses the thread ID
  - `-h` suppresses the hostname
  - `-y` suppresses the message severity

- To render a `.raw` file from a remote machine, type: `nsr_render_log -c -empathy -R` ***hostname raw_filename*** `1>`***output_filename*** `2>&1`

  where:

  - *hostname* is the name of the host that contains the `.raw` file.
  - *raw_filename* is the name of the unrendered file. For example, `daemon.raw`
  - *output_filename* is the name of the file to direct the output to
  - `-c` suppresses the category
  - `-e` suppresses the error number
  - `-m` suppresses the message ID
  - `-p` suppresses the process ID
  - `-a` suppresses the activity ID

- `-t` suppresses the thread ID
- `-h` suppresses the hostname
- `-y` suppresses the message severity

- To render a `.raw` file and only view log file messages for a specific device, type: `nsr_render_log -c -empathy -F` ***devicename raw_filename*** `1>`***output_filename*** `2>&1`

  where *devicename* is the name of the device.

- To render only the most recently logged messages, type: `nsr_render_log -c -empathy -B` ***number raw_filename*** `1>`***output_filename*** `2>&1`

  where *number* is the number of lines that you want to render.

  The *NetWorker Command Reference Guide* provides detailed information about the `nsr_render_log` program and the available options.

- To render a `.raw` file and only view certain messages severities, type: `nsr_render_log -c -empath -Y` ***message_severity*** `1>`***output_filename*** `2>&1`

  where *message_severity* is one of the severity types listed in the following table.

  **Table 13** Message types

| Type | Description |
|---|---|
| Informational | Information that may be useful, but does *not* require any specific action. |
| Warning | A temporary problem that NetWorker software may resolve or prompt you to resolve. |
| Notification | An event has occurred that generated a message. |
| Error | Errors that you are required to resolve. |
| Critical | Errors that you are required to resolve, to ensure successful NetWorker operations. |
| Severe | Errors that cause NetWorker services to become disabled or dysfunctional. |

  The UNIX man page and the *NetWorker Command Reference Guide* provides detailed information about the `nsr_render_log` program and the available options.

## Rendering raw log files at runtime

You can instruct the NetWorker software to render the `daemon.raw` and `gstd.raw` files into the locale of the host at runtime, in addition to creating locale-independent log files. This allows you to view the log file in a text editor without using the `nsr_render_log` program to render the file first.

### Before you begin

Log in to the NetWorker host with the root (UNIX) or Administrator (Windows) user account.

### About this task

To instruct the NetWorker software to render logs in the locale of the computer hosting the file, set the **runtime rendered log file** attribute in the NSRLA database.

For backward compatibility with previous releases of the NetWorker software, runtime rendered log files contain the following attributes:

- Message ID
- Date and time of message
- Rendered message

**Procedure**

1. To access the NSRLA database, from a command prompt, use the `nsradmin` program:

   ```
   nsradmin -p nsrexec
   ```

2. Set the resource type to NSR log:

   ```
   . type: NSR log
   ```

3. Display a list of all log file resources:

   ```
   print
   ```

   For example, on a Windows NMC server, output similar to the following appears:

   ```
   nsradmin> print
   type: NSR log;
   administrator: Administrators,
   "group=Administrators,host=bu-iddnwserver.iddlab.local";
   owner: NMC Log File;
   maximum size MB: 2;
   maximum versions: 10;
   runtime rendered log: ;
   runtime rollover by size: Disabled;
   runtime rollover by time: ;
   name: gstd.raw;
   log path: \
   "C:\\Program Files\\EMC NetWorker\\Management\\GST\\logs\
   \gstd.raw";

   type: NSR log;
   administrator: Administrators,
   "group=Administrators,host=bu-iddnwserver.iddlab.local";
   owner: NetWorker;
   maximum size MB: 2;
   maximum versions: 10;
   runtime rendered log: ;
   runtime rollover by size: Disabled;
   runtime rollover by time: ;
   name: daemon.raw;
   log path: \
   "C:\\Program Files\\EMC NetWorker\\nsr\\logs\\daemon.raw";
   ```

4. Define the log resource that you want to edit:

   ```
   . type: NSR log; name: log_file_name
   ```

   For example, to select the `daemon.raw` file, type the following:

```
. type: NSR log; name: daemon.raw
```

5. To define the path and file name for the rendered log file, use the **Runtime rendered log** attribute.

   For example, to save rendered messages to the file `rendered.log` in the default NetWorker logs directory on a Windows host, type:

   ```
   update runtime rendered log: "C:\\Program Files\\EMC NetWorker\
   \nsr\\logs\\rendered.log"
   ```

6. When prompted to confirm the update, type: **y**
7. Verify that the attribute value update succeeds:

   ```
   nsradmin> print

   type: NSR log;
   administrator: root, "user=administrator,host=bu-
   iddnwserver.iddlab.local";
   owner: NetWorker;
   maximum size MB: 2;
   maximum versions: 10;
   runtime rendered log:C:\\Program Files\\EMC NetWorker\\nsr
   \\logs\\daemon.log ;
   runtime rollover by size: Disabled;
   runtime rollover by time:;
   name: daemon.raw;
   log path: C:\\Program Files\\EMC NetWorker\\Management\
   \GST\\logs\\daemon.raw;
   ```

8. Exit the `nsradmin` program.

## Raw log file management

The NetWorker software manages the size and the rollover of the raw log files.

NetWorker automatically manages the `nwsnap.raw` and `nsrcpd.raw` files in the following ways:

- `nwsnap.raw`: Before a process writes messages to the `nwsnap.raw` file, the process checks the size of the `.raw` file. The process invokes the trimming mechanism when the size of the log file is 100 MB or larger. Snapshot management supports up to 10 `.raw` file versions.
- `nsrcpd.raw`: When the NetWorker daemons start on the machine, the startup process checks the size of the raw file. The startup process runs the trimming mechanism when the size of the log file is 2 MB or larger. Package Manager supports 10 raw file versions.

NetWorker enables you to customize the maximum file size, maximum number of file versions, and the runtime rollover of the `daemon.raw`, `gstd.raw`, `networkr.raw`, and *`Networker_server_`*`sec_audit.raw` files. Use the `nsradmin` program to access the NSRLA database, and modify the attributes that define how large the log file becomes before NetWorker trims or renames the log file.

The following table describes the resource attributes that manage the log file sizes.

**Table 14** Raw log file attributes that manage log file size

| Attribute | Information |
|---|---|
| Maximum size MB | Defines the maximum size of the log files.<br><br>Default: 2 MB |
| Maximum versions | Defines the maximum number of the saved log files.<br><br>When the number of copied log files reaches the maximum version value,<br>NetWorker removes the oldest log when a new copy of the log file is created.<br><br>Default: 10 |
| Runtime rollover by size | When set, this attribute invokes an automatic hourly check of the log file size.<br><br>When you configure the runtime rendered log attribute, NetWorker<br>trims the runtime rendered log file and the associated `.raw` file simultaneously.<br><br>Default: disabled |
| Runtime rollover by time | When set, this attribute runs an automatic trimming of the log file at the<br>defined time, regardless of the size. The format of the variable is<br>HH:MM (hour:minute).<br><br>When you configure the runtime rendered log attribute, NetWorker trims the<br>runtime rendered log file and the associated `.raw` file simultaneously.<br><br>Default: undefined<br><br>**Note:** After setting this attribute, restart NetWorker services for the change to take effect. |

How the trimming mechanism trims the log files differs depending on how you define the log file size management attributes. The following table summarizes the trimming behavior.

**Table 15** Raw log file attributes that manage the log file trimming mechanism

| Attribute configuration | Trimming behavior |
|---|---|
| When you configure runtime rollover by time or runtime rollover by size | • NetWorker copies the contents of the existing log file to a new file with the naming convention:*daemondate_time.raw*<br>• NetWorker truncates the existing `daemon.raw` to 0 MB. |

**Table 15** Raw log file attributes that manage the log file trimming mechanism (continued)

| Attribute configuration | Trimming behavior |
|---|---|
| | **Note:** When this mechanism starts on a NetWorker Server that is under a heavy load, this process may take some time to complete. |
| When you do not configure runtime rollover by time or runtime rollover by size | • NetWorker checks the log file size when the `nsrexecd` process starts on the computer.<br>• When the log file size exceeds the size that is defined by the maximum size MB attribute, NetWorker renames the existing log file to *`log_file_name_date_time.raw`* then creates a new empty log file.<br>**Note:** When the `nsrd` daemon or NetWorker Backup and Recover Server service runs for a long time, the size of the log file can become much larger than the value defined by maximum size MB. |

## Managing raw log file size for the daemon.raw, networkr.raw, and gstd.raw files

To configure the NetWorker software to rollover the `.raw` file by time, perform the following steps.

### Procedure

1. Log in to the NetWorker host with root on UNIX or Administrator on Windows.
2. To access the NSRLA database, use the `nsradmin` program:

   ```
   nsradmin -p nsrexec
   ```

3. Set the resource type to NSR log:

   ```
   . type: NSR log
   ```

4. Display a list of all log file resources:

   ```
   print
   ```

   For example, on a Windows NMC server, output similar to the following appears:

   ```
   nsradmin> print
   type: NSR log;
   administrator: Administrators,
   "group=Administrators,host=bu-iddnwserver.iddlab.local";
   owner: NMC Log File;
   maximum size MB: 2;
   maximum versions: 10;
   runtime rendered log: ;
   runtime rollover by size: Disabled;
   ```

```
runtime rollover by time: ;
name: gstd.raw;
log path: \
"C:\\Program Files\\EMC NetWorker\\Management\\GST\\logs\
\gstd.raw";

type: NSR log;
administrator: Administrators,
"group=Administrators,host=bu-iddnwserver.iddlab.local";
owner: NetWorker;
maximum size MB: 2;
maximum versions: 10;
runtime rendered log: ;
runtime rollover by size: Disabled;
runtime rollover by time: ;
name: daemon.raw;
log path: \
"C:\\Program Files\\EMC NetWorker\\nsr\\logs\\daemon.raw";
```

5. Define the log resource that you want to edit:

   **. type: NSR log; name: log_file_name**

   For example, to select the `gstd.raw` file, type the following:

   **. type: NSR log; name: gstd.raw**

6. Update the **runtime rollover by time** attribute with the time that you want to rollover the log file.

   For example, to configure the `gstd.raw` file to rollover at 12:34 AM, type:

   **update runtime rollover by time: "00:34"**

7. When prompted to confirm the update, type: **y**
8. Verify that the attribute value update succeeds:

```
nsradmin> print

type: NSR log;
administrator: root, "user=administrator,host=bu-
iddnwserver.iddlab.local";
owner: NMC Log File;
maximum size MB: 2;
maximum versions: 10;
runtime rendered log: ;
runtime rollover by size: Disabled;
runtime rollover by time: "00:34";
name: gstd.raw;
log path: C:\\Program Files\\EMC NetWorker\\Management\
\GST\\logs\\gstd.raw;
```

9. Exit the `nsradmin` program.

## Monitoring changes to the NetWorker server resources

The Monitor RAP (resource allocation protocol) attribute in the NSR resource enables you to track configuration modifications to the NetWorker server resources and

attributes. The NetWorker server records these changes in the `rap.log` file, which is located in the *`NetWorker_install_dir`*`\logs` directory. Each entry in the `rap.log` file consists of the user action, the name of the user that performed the action, the name of the source computer, and the time of the change. NetWorker logs sufficient information in the `rap.log` file to enable an administrator to undo any changes. The Monitor RAP attribute is enabled by default. To disable the attribute setting, perform the following steps.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**About this task**

**Note:** In NetWorker 8.0 and later, the Security Audit Log feature provides the NetWorker server and the NMC server with the ability to log specific security audit events that are related to their operations.

**Procedure**

1. From the **Administration** window, select **Server**.
2. From the **View** menu, select **Diagnostic mode**.
3. Right-click the NetWorker server name in the left navigation pane, and then select **Properties**.
4. On the **General** tab, select the **Disabled** button for the **Monitor RAP** attribute.

# Configuring logging levels

This section describes how to modify the logging levels of the NetWorker and NMC processes to troubleshoot issues.

## Setting the troubleshoot level for NetWorker daemons

How you configure the NetWorker daemons to run in troubleshoot mode depends on the daemon.

On a NetWorker server, you can configure the `nsrctld` and `nsrexecd` to start in troubleshoot mode. The `nsrctld` daemon starts other daemons, as required. To capture troubleshoot output for the daemons that the `nsrctld` daemon starts use the `dbgcommand`.

On an NMC server, you can start the `gstd` daemon in troubleshoot mode.

### Starting nsrctld and nsrexecd daemons in troubleshoot mode on UNIX

The `nsrctld` daemon is the main process for the NetWorker server. To troubleshoot problems with the NetWorker server process, start the `nsrctld` process in troubleshoot mode. The `nsrexecd` process is the main process for NetWorker client functions. To troubleshoot problems that are related to NetWorker client functions, start the `nsrexecd` process in troubleshoot mode.

**Procedure**

1. Log in to the NetWorker host with the root account, and then stop the NetWorker processes:

   ```
   nsr_shutdown
   ```

2. From a command prompt , start the daemon, and then specify the troubleshoot level.

   For example:

   - To start the `nsrexecd` daemon in troubleshoot mode, type:

     ```
     nsrexecd -D9 1>filename2>&1
     ```

   - To start the `nsrctld` daemon in troubleshoot mode, type the following command:

     ```
     source /opt/nsr/admin/networkerrc; source /opt/nsr/admin/
     nsr_serverrc; nsrctld -D 9 1>filename.log 2>&1
     ```

   Where *filename* is the name of the text file that NetWorker uses to store the troubleshoot messages.

3. After you collect the necessary troubleshoot information, perform the following steps:

   a. Stop the NetWorker processes by using the `nsr_shutdown` command.

   b. Restart the processes by using the NetWorker startup script:

      - On Solaris and Linux, type:

        ```
        /etc/init.d/networker start
        ```

      - On HP-UX, type:

        ```
        /sbin/init.d/networker start
        ```

      - On AIX, type:

        ```
        /etc/rc.nsr
        ```

## Starting the NetWorker daemons in troubleshoot mode on Windows

The NetWorker Backup and Recovery service starts the `nsrctld` process, which is the main process for a NetWorker server. To troubleshoot problems with the NetWorker server process, start the `nsrctld` process in troubleshoot mode. The NetWorker Remote Exec service starts the `nsrexecd` process which is the main process for NetWorker client functions. To troubleshoot problems that are related to NetWorker client functions, start the `nsrexecd` process in troubleshoot mode.

**Procedure**

1. Open the Services applet, `services.msc`.
2. Stop the NetWorker Remote Exec service.

   On a NetWorker server, this also stops the **NetWorker Backup and Recover** service.

3. To put a `nsrexecd` process in troubleshoot mode:

   a. Right-click the **NetWorker Remote Exec** service, and then select **Properties**.

   b. In the **Startup Parameters** field, type `-D` *x*.

      where x is a number between 1 and 99.

   c. Click **Start**.

4. To put the `nsrd` process in troubleshoot mode:
   a. Right-click the NetWorker Backup and Recover service, and then select **Properties**.
   b. In the **Startup Parameters** field, type `-D` *x*.

      where *x* is a number between 1 and 99.
   c. Click **Start**.

**Results**

NetWorker stores the troubleshoot information in the `daemon.raw` file.

**After you finish**

After you capture the troubleshoot information, stop the NetWorker services, remove the *-D* parameter, and then restart the services.

## Starting the NMC server daemon in troubleshoot mode

When you can access the NMC GUI, use the Debug Level attribute in the System Options window to start the `gstd` daemon in troubleshoot mode.

When you cannot access the NMC GUI, use environment variables to start the `gstd` daemon in troubleshoot mode.

### Starting the NMC server daemon in troubleshoot mode using NMC

The `gstd` daemon is the main NMC server process. To troubleshoot NMC GUI issues, start the `gstd` daemon in troubleshoot mode.

**Before you begin**

Log in to the NMC server with an administrator account.

**Procedure**

1. In the NMC Console, select **Setup**.
2. On the **Setup** menu, select **System Options.**
3. In the **Debug Level** field, select a number between 1 and 20.

**Results**

NMC stores the troubleshoot information in the `gstd.raw` file.

**After you finish**

After you capture the troubleshoot information, stop the NetWorker services, set the **Debug Level** to 0, and then restart the services.

### Starting the NMC server daemon in troubleshoot mode using environment variables

Use environment variable to put the `gstd` daemon in troubleshoot mode when you cannot access the NMC GUI.

### Setting the GST debug environment variable on Windows

To set the GST troubleshoot environment variable on Windows, use the Control Panel system applet on the NMC server.

**Procedure**

1. Browse to **Control Panel** > **System and Security** > **System** > **Advanced Settings**.
2. On the **General** tab, click **Environment Variables.**

3. In the **System variables** section, click **New**.
4. In the **Variable name** field, type: `GST_DEBUG`
5. In the **Variable value** field, type a number between 1 and 20.
6. Stop, and then start the **EMC gstd** service.

**Results**

NMC stores the troubleshoot information in the `gstd.raw` file.

**After you finish**

After you capture the troubleshoot information, stop the **EMC gstd** service, remove the environment variable from the startup file, and then restart the **EMC gstd** service.

**Setting the GST troubleshoot environment variable on UNIX**

Use a borne shell script to put the `gstd` daemon in troubleshoot mode.

**Procedure**

1. Modify the file permissions for the `gst` startup file. By default, the file is a read-only file.

   The file location varies depending on the operating system:

   - Solaris and Linux: `/etc/init.d/gst`
   - AIX: `/etc/rc.gst`

2. Edit the file and specify the following at beginning of the file:

   ```
   GST_DEBUG=x
   export GST_DEBUG
   ```

   where *x* is a number between 1 and 20.

3. Stop, and then restart the `gstd` daemon:

   - Solaris and Linux: Type:

     ```
     /etc/init.d/gst stop
     ```

     then

     ```
     /etc/init.d/gst start
     ```

   - AIX: Type:

     ```
     /etc/rc.gst start
     ```

     then

     ```
     /etc/rc.gst stop
     ```

**Results**

NMC stores the troubleshoot information in the `gstd.raw` file.

**After you finish**

After you capture the troubleshoot information, stop the `gstd` daemon, remove the environment variable from the startup file, and then restart the `gstd` daemon.

### Using the dbgcommand program to put NetWorker process in troubleshoot mode

Use the `dbgcommand` program to generate troubleshoot messages for NetWorker daemons and processes without the stopping and starting the NetWorker daemons. You can also use the `dbgcommand` program to produce troubleshoot information for a process that another process starts. For example, use the `dbgcommand` to put the `nsrmmd` process in troubleshoot mode.

#### Procedure

1. From a command prompt on the NetWorker host, determine the process id (PID) of the daemon or process that you want to troubleshoot.
   - On Windows: To determine the PID, use the **Task Manager**.
     **Note:** If you do not see the PID for each process on the **Process** tab, browse to **View** > **Select Columns**, and then select **PID (Process Identifier)**
   - On UNIX, use the `ps` command. For example, to get a list of all the NetWorker processes that start with *nsr*, type `ps -ef | grep nsr`.
2. From a command prompt, type:

   ```
   dbgcommand -p PID -Debug=x
   ```

   where:

   - *PID* is the process id of the process.
   - *x* is a number between 0 and 9.

   **Note:** 0 turns off troubleshoot.

#### Results

NetWorker logs the process troubleshoot information in the `daemon.raw` file.

#### After you finish

To turn off troubleshoot, type:

```
dbgcommand -p PID -Debug=0
```

## Running individual clients in a group in troubleshoot mode

Modify the backup command attribute for a Client resource to send verbose backup information to the `daemon.raw` file, for individual clients in a group.

#### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

#### Procedure

1. From the **Administration** window, click **Protection**.
2. In the left navigation pane, click **Clients**.
3. Right-click the client, and then select **Modify Client Properties**.
4. On the **Apps & Modules** tab, in the **Backup command** attribute, type:

   ```
   save -Dx
   ```

where *x* is a number between 1 and 99.

5. Click **OK**.

**Results**

At the scheduled time, NetWorker logs troubleshoot information for the client backup in the `daemon.raw`.

**After you finish**

When the group backup operations complete, edit the properties of the client and clear the **Backup Command** field.

## Running client-initiated backups in troubleshoot mode from the command line

Use the `save` program to perform a client-initiated backup from the command line.

**About this task**

On the host you want to backup, type the following command:

```
save -Dx file_sytem_objects
1>filename 2>&1
```

where:

- *x* is a number between 1 and 99.
- *file_sytem_objects* is the name of the files or directory to backup.
- *filename* is the name of the file that stores the troubleshoot information.

**Note:** The *NetWorker Command Reference Guide* provides detailed information about all the available backup options and how to use the `save` command.

## Running Recoveries in troubleshoot mode

You can configure NetWorker to log verbose output for recoveries when you Recovery wizard, perform Windows disaster recoveries and by using the `recover` command.

### Run Recovery wizard recover jobs in debug mode

You can run recover jobs that you created in the Recovery wizard by using the Recovery wizard or by using the `nsrtask` program from the command line.

**Running a recovery job in troubleshoot mode**
To send verbose recovery information to the recovery log file, set the troubleshoot level of a recovery job.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**Procedure**

1. On the **Administration** window, click **Recover**:
   - To modify a scheduled recover job, select the job in the **Configured Recovers** section, and then select **Properties**.
   - To configure a new recover job, select **New**.

   **Note:** You cannot modify an expired or failed to recover job.

2. To create or modify the recover job, use the Recovery wizard. On the **Select the Recovery Options** window, select **Advanced Options**.
3. In the **Debug level** attribute, select a troubleshooting level between 0 and 9.
4. Complete the remaining steps in the Recovery Wizard.

**Results**

NetWorker logs the troubleshoot recovery information to the recover log file.

**Running a recovery job in troubleshoot mode by using nsrtask**

Use the `nsrtask` command to run a recovery job that is created by the **Recovery** wizard, from a command prompt.

**Procedure**

1. On the NetWorker server, type: `nsradmin`.
2. From the `nsradmin` prompt:
   a. Set the resource attribute to the **Recover** resource:

      ```
      . type: nsr recover
      ```

   b. Display the attributes for the **Recover** resource that you want to troubleshoot:

      `print name:`**`recover_resource_name`**

      where **`recover_resource_name`** is the name of the **Recover** resource.

   c. Make note of the values in the **recover**, **recovery options**, and **recover stdin** attributes. For example:

      ```
      recover command: recover;
      recover options: -a -s nw_server.corp.com -c
      mnd.corp.com -I - -i R;
      recover stdin:
      "<xml>
      <browsetime>
      May 30, 2013 4:49:57 PM GMT -0400
      </browsetime>
      <recoverpath>
      C:
      </recoverpath>
      </xml>";
      ```

      where:

      - *nw_server.corp.com* is the name of the NetWorker server.
      - *mnd.corp.com* is the name of the source NetWorker client.

3. Confirm that the `nsrd` process can schedule the recover job:
   a. Update the **Recover** resource to start the recover job:

      `update: name: `*`recover_resource_name;`*`start time: now`

      where *recover_resource_name* is the name of the **Recover** resource.

   b. Exit the `nsradmin` application
   c. Confirm that the `nsrtask` process starts.

      If the `nsrtask` process does not start, the review the `daemon.raw` file on the NetWorker server for errors.

4. To confirm that the NetWorker server can run the `recover` command on the remote host, on the NetWorker server type the following command:

   `nsrtask -D3 -t 'NSR Recover'` *recover_resource_name*

   where *recover_resource_name* is the name of the **Recover** resource.
5. When the `nsrtask` command completes, review the `nsrtask` output for errors.
6. To confirm that the Recovery UI sends the correct recovery arguments to the `recover` process:
   a. On the destination client, open a command prompt.
   b. Run the recover command with the recover options that the **Recover** resource uses.

      For example:

      ```
      recover -a -s nw_server.corp.com -c mnd_corp.com -I - -i
      R
      ```

   c. At the **Recover** prompt, specify the value in the `recover stdin` attribute. Do not include the " ," or the ";" that appears with the recover stdin attribute.

      If the `recover` command appears to stop responding, then review the `daemon.raw` file for errors.

   d. When the `recover` command completes, review the recover output for errors. If the `recover` command fails, then review the values that are specified in the **Recover** resource for errors.
7. To review the details of the Recover job, use the `jobquery` command. From a command prompt on the NetWorker server, type: `jobquery`
8. From the `jobquery` prompt, perform one of the following steps:
   - Set the query to the **Recovery** resource and display the results of all recovery jobs for a **Recovery** resource:

     `print name:` ***recover_resource_name***

     where *recover_resource_name* is the name of the Recover resource.
   - Set the query to a particular jobid and display the results of the job.

     `print job id:` ***jobid***

     Where *jobid* is the jobid of the Recover job that you want to review.

   **Note:** Review the `daemon.raw` file on the NetWorker server to obtain the jobid for the recovery operation.

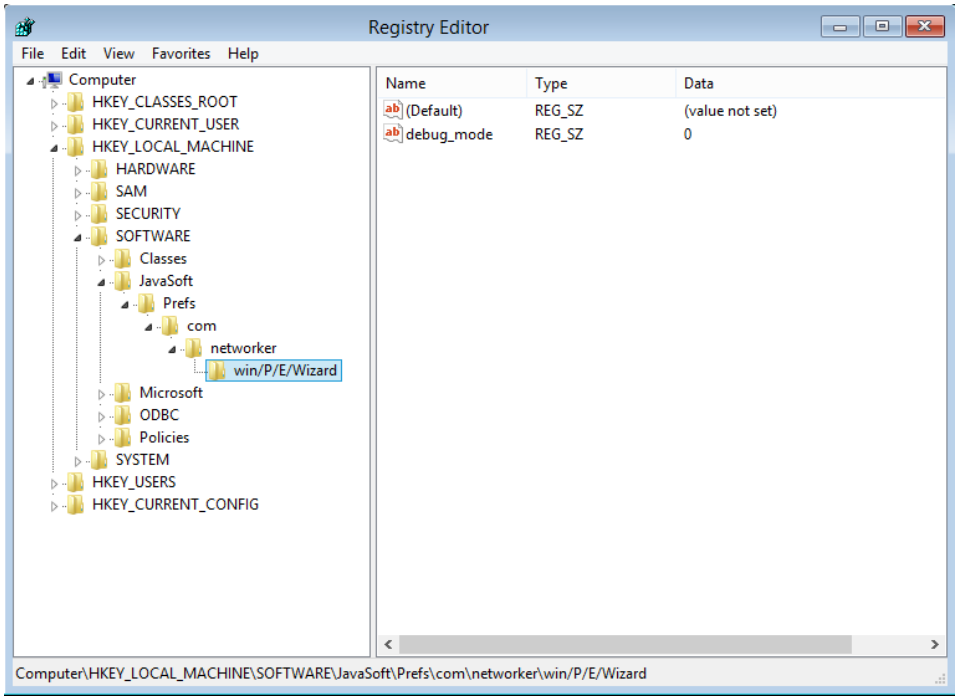
## Running Windows BMR recoveries in troubleshoot mode

Use the WinPE registry to troubleshoot recoveries that are performed with the **BMR Recovery** wizard.

### Procedure

1. From a command prompt, type: `regedit`
2. In the Registry Editor, browse to `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\com\networker\win/P/E/Wizard`

**Figure 14** WinPE registry key to troubleshoot recoveries




3. Change the **Data** value in the *debug_mode* attribute from `0` to `1`.
4. Start the BMR Recovery wizard.

### Results

The BMR Recovery Wizard logs the troubleshoot information that is related to the following in the `X:\Program Files\EMC NetWorker\nsr\logs\WinPE_Wizard.log` file.
After you collect the troubleshoot information, to turn off troubleshoot mode, modify the data value for the *debug_mode* attribute from `1` to `0`.

## Running client-initiated recoveries in troubleshoot mode from the command line

To perform a client started backup from the command line, use the `recover` program with the *-D* option.

### About this task

For example, on the host you want to recover the data to, type the following command:

```
recover -Dx file_sytem_objects 1>filename 2>&1
```

where:

- *x* is a number between 1 and 99.
- *file_sytem_objects* is the name of the files or directory to recover.
- *filename* is the name of the file that stores the troubleshoot information.

**Note:** The *NetWorker Command Reference Guide* provides detailed information about all the available recovery options and how to use the `recover` command.

# NetWorker Authentication Service logs

This section provides an overview of the log files that are available for the NetWorker Authentication Service.

## NetWorker Authentication Service log files

This section provides a summary of the log files available for the NetWorker Authentication Service.

**Table 16** NetWorker Authentication Service log files

| Component | File name and default location | Description |
|---|---|---|
| Installation log | Linux:<br>`/opt/nsr/authc-server/logs/install.log`<br>Windows:<br>`C:\Users\`*`username`*`\AppData\Local\Temp\NetWorker_`*`date_seq_num`*`_AuthC..log` | Contains information about the installation of NetWorker Authentication Service. |
| `authc_mgmt` and `authc_config` | Linux:<br>`$HOME/authc-cli.log`<br>Where *$HOME* is the home folder for the currently logged in user. For example, when the root user runs the command, the file location is `/root/authc-cli.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\authc-server\logs\authc-cli.log` | Contains a list of error messages that appeared when a user ran the `authc_mgmt` and `authc_config` tools. |
| Authentication server log | Linux:<br>`/nsr/authc/logs/authc-server.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\authc\tomcat\logs\authc-server.log` | Main authentication service log file. |
| Audit log | Linux:<br>`/nsr/authc/logs/authc-server-audit.log`<br>Windows:<br>`C:\Program Files\EMC NetWorker\nsr\authc\tomcat\logs\authc-server-audit.log` | Contains security audit messages for the NetWorker Authentication Service. |
| Tomcat Access logger | Linux:<br>`/nsr/authc/logs/localhost_access_log.`*`date`*`.txt`<br>Windows: | Contains access information for the embedded Apache httpd web server. |

**Table 16** NetWorker Authentication Service log files (continued)

| Component | File name and default location | Description |
|---|---|---|
| | `C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat\logs\localhost_access_log.date.txt` | |
| Apache Catalina log | Linux: `/nsr/authc/tomcat/logs/catalina.out` Windows: `C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat\logs\catalina.date.log` | Contain messages for the Apache Tomcat core component. |

Refer to the Apache website for detailed information about the Apache Tomcat log files.

## NetWorker Authentication Service server log file management

NetWorker Authentication Services uses the Apache log4j API to manage log files. To modify how NetWorker Authentication Services manage the `authc-server.log` log file, edit the `log4j.properties` file:

- UNIX: The `log4j.properties` file is located in `/nsr/authc/webapps/auth-server/WEB-INF/classes`.
- Windows: The file is located in `C:\Program Files\EMC\authc-server\tomcat\webapps\auth-server\WEB-INF\classes`.

This section describes how to modify the commonly used log attributes in the `log4j.properties` file. Apache documentation provides more detailed information about each attribute in the `log4j.properties` file.

**Note:** After you make changes to the `log4j.properties` file, you must stop and start the NetWorker Authentication Service daemon to reset the configuration settings.

### Modifying the logging level

The *log4j.rootLogger=* attribute defines the level of logging that the NetWorker Authentication Service writes to the log files and where the messages appear. By default, the NetWorker Authentication Service sets the logging level to *warn* and messages appear in the log files, stdout, and in the Java application, There are five standard log levels: *debug*, *info*, *warn*, *error*, and *fatal*.

To change the logging level to *error*, modify the *log4j.rootLogger=* attribute to appear as follows: `log4j.rootLogger=error, stdout, app`

### Modifying the maximum log file size

The *log4j.appender.app.MaxFileSize* attribute defines the maximum size of the `authc-server.log` file. When the log file reaches the maximum size, NetWorker Authentication Service renames the log file for archival purposes and creates log file. By default, NetWorker Authentication Service sets the maximum size to 100 KB.

To increase the size of the log file to 2MB, modify the *log4j.appender.app.MaxFileSize* attribute to appear as follows: `log4j.appender.app.MaxFileSize=2MB`

### Modifying the number of rollover log files

The *log4j.appender.app.MaxBackupIndex* attribute defines the number of `authc-server.log` rollover log files that the NetWorker Authentication Service

maintains. When the size of the `authc-server.log` reaches the maximum file size value, NetWorker Authentication Service copies the contents of the log file to a new log file with the naming convention `authc-server`*`date`*`.log`. By default, NetWorker Authentication Service maintains one rollover log file.

To increase the number of rollover log files to 4, modify the *log4j.appender.app.MaxBackupIndex* attribute to appear as follows: `log4j.appender.app.MaxBackupIndex=4`

## CLI log file management

NetWorker Authentication Services uses the Apache log4j API to manage log files. To modify how NetWorker Authentication Services manage the CLI log file, edit the `authc-cli-log4j.properties` file. On UNIX, the `authc-cli-log4j.properties` file is located in `/opt/nsr/authc-server/conf`. On Windows, the file is located in `C:\Program Files\EMC NetWorker\nsr\authc-server\conf`.

This section describes how to modify the commonly used log attributes in the `log4j.properties` file. Apache documentation provides more detailed information about each attribute in the `log4j.properties` file.

**Note:** After you make changes to the `authc-cli-log4j.properties` file, you must stop and start the NetWorker Authentication Service daemon to reset the configuration settings.

### Modifying the logging level

The *log4j.rootLogger=* attribute defines the level of logging that the NetWorker Authentication Service writes to the log files and where the messages appear. By default, the NetWorker Authentication Service sets the logging level to *warn* and messages appear in the log files, stdout, and in the Java application, There are five standard log levels: *debug*, *info*, *warn*, *error*, and *fatal*.

To change the logging level to *error*, modify the *log4j.rootLogger=* attribute to appear as follows: `log4j.rootLogger=error, stdout, app`

### Modifying the maximum log file size

The *log4j.appender.app.MaxFileSize* attribute defines the maximum size of the `authc-cli.log` file. When the log file reaches the maximum size, NetWorker Authentication Service renames the log file for archival purposes and creates a log file. By default, NetWorker Authentication Service sets the maximum size to 100 KB.

To increase the size of the log file to 2MB, modify the *log4j.appender.app.MaxFileSize* attribute to appear as follows: `log4j.appender.app.MaxFileSize=2MB`

### Modifying the number of rollover log files

The *log4j.appender.app.MaxBackupIndex* attribute defines the number of `authc-cli.log` rollover log files that the NetWorker Authentication Service maintains. When the size of the `authc-cli.log` reaches the maximum file size value, NetWorker Authentication Service copies the contents of the log file to a new log file with the naming convention `authc-cli`*`date`*`.log`. By default, NetWorker Authentication Service maintains one rollover log file.

To increase the number of rollover log files to 4, modify the *log4j.appender.app.MaxBackupIndex* attribute to appear as follows:
`log4j.appender.app.MaxBackupIndex=4`

# CHAPTER 4

# Communication Security Settings

This chapter describes how to ensure NetWorker uses secure channels for communication and how to configure NetWorker in a firewall environment.


- Port usage and firewall support ..... 136
- Special considerations for firewall environments ..... 137
- Determining service port requirements ..... 139
- Configuring service port ranges in NetWorker ..... 143
- Configuring the service ports on the firewall ..... 146
- Determining service port requirement examples ..... 152
- Troubleshooting ..... 157

# Port usage and firewall support

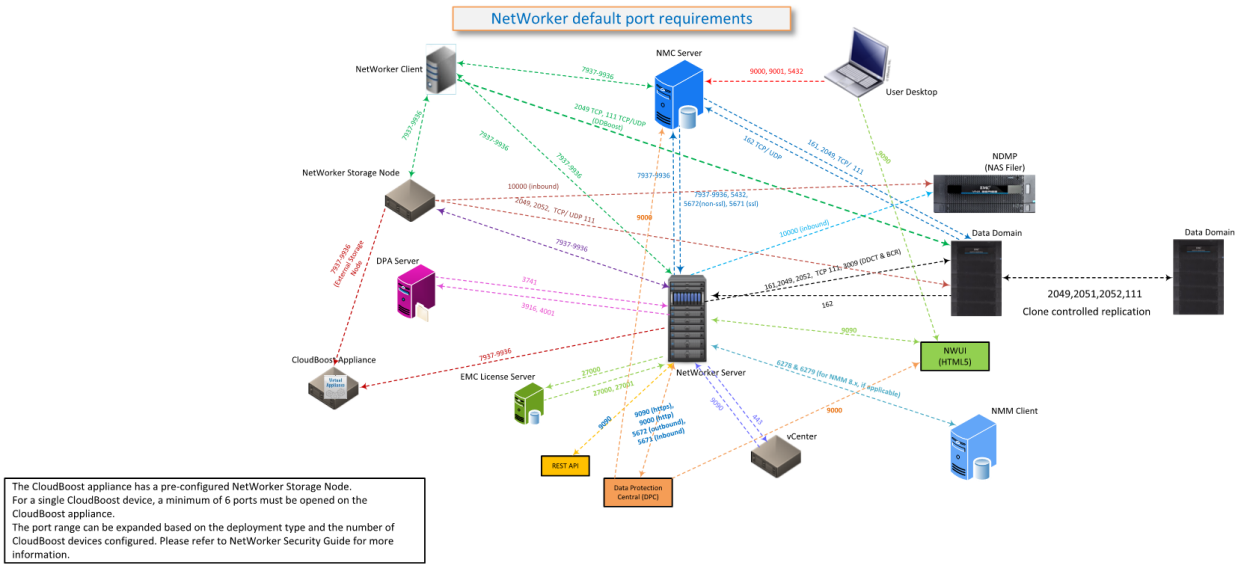
NetWorker uses a direct socket connection to communicate and move data across the network to the required service with minimal overhead. While NetWorker opens some ports for TCP and UDP, NetWorker only requires TCP ports. UDP ports are optional.

NetWorker uses two types of ports:

- Service ports.
- Connection ports.

The following diagram illustrates the default port usage of service and connection ports across NetWorker.

**Figure 15** Default port usage across NetWorker




**Note:** The CloudBoost appliance has a pre-configured NetWorker storage node. For a single CloudBoost device, open a minimum of six ports on the CloudBoost appliance. You can further expand the port range based upon the deployment type and the number of CloudBoost devices configured. The "Communication Security Settings" chapter provides additional information.

## Service ports

The service ports are also known as inbound, destination, or listening ports. The TCP server processes that run on each NetWorker host use service ports to listen for inbound connections. The service ports are meant to provide specific services on the ports that are reserved for them.

NetWorker uses two types of service ports:

- Fixed ports—NetWorker uses two fixed ports: TCP/7937 and TCP/7938. Include these ports in the service port range of each NetWorker host. NetWorker uses these ports to start connections.
- Variable ports—NetWorker dynamically opens ports. A NetWorker host can allocate any port in the defined service port range and the NetWorker daemons select the dynamic ports within that range randomly. The default range is 7937-9936 and you can narrow or expand this range.

To increase security in the environment, reduce the variable ports range to specify only the minimum number of service ports that the NetWorker software requires. The minimum value depends on the installation type and the number of hosted NetWorker devices. NetWorker stores the service port range for a host in the NSR Local Agent (NSRLA) resource in the NetWorker client database (nsrexec). The service ports can be modified using the `nsrports` command.

## Connection ports

Connection ports are also known as outbound ports, source ports, or communication ports. NetWorker processes use connection ports to connect to a service. The NetWorker software requires one connection port for any type of communication between the client, storage node, and server.

NetWorker uses a default range, 0-0, to indicate that the NetWorker software allows the operating system to select the port for TCP clients. Port 0-0 indicates that any available port from the operating system can be used for outbound communication. The operating system reserves connection ports for short-term use and reuses the ports as needed. The operating system might allow you to configure the dynamic port range, for example, by using the `netsh` program on Windows. NetWorker does not require changes to this range and it is recommended that you use the default dynamic port range.

The use of the default port range does not cause security concerns. It is recommended that you do not change the range for any NetWorker hosts in the datazone. NetWorker performance problems or random malfunctions can occur when the range is too narrow. The connection ports can be modified using the `nsrports` command.

# Special considerations for firewall environments

You can configure some firewall products to close an open connection that is inactive for a defined period of time. NetWorker uses persistent connections between daemons to transfer information as efficiently as possible.

Connections open at the start of communication, and close when the communication finishes. For example, a running backup may have connections open with the following daemons:

- nsrmmd, to send the backup data.
- nsrindexd, to send the client file index information.
- nsrjobd, to send control and status information.

NetWorker connections between hosts can remain idle for periods of time that exceed the idle timeout value on the firewall, and as a result, the firewall ends the connection. For example, the status connection to nsrjobd is frequently idle during a backup. When there are no error messages to report, the connection does not have traffic until the backup completes and NetWorker generates the success message.

To prevent the firewall from closing a NetWorker connection prematurely, configure the firewall to not close idle connections. If you cannot eliminate the firewall timeout, then configure the datazone to send a keepalive signal between the hosts at an interval that is shorter than the timeout period defined on the firewall. Configure the keep alive signal at the operating system level.

When you configure TCP keepalives within NetWorker, NetWorker does not send a keepalive signal across some connections, for example, between the save and nsrmmd processes. It is recommended that you configure TCP keepalive signals at the operating system level to ensure all connections do not close prematurely. It is not

recommended to reduce the *TIME_WAIT* and *CLOSE_WAIT* intervals on a host to reduce the demand for connection or service ports. When the intervals are too low, the port for a process might close while NetWorker is resending data packets to the process. In some situations, a new instance of a process connects to the port and incorrectly receives the data packet, which might corrupt the new process.

## Configuring TCP keepalives at the operating system level

You can change the TCP KeepAlive parameters temporarily on UNIX or permanently on UNIX and Windows operating systems. Restart all NetWorker services after you change the TCP KeepAlive parameters.

Firewall configurations commonly define a 1 hour idle timeout. It is recommended that you set the `Wait Time Before Probing` and `Interval Between Retry Probes` parameters to 57 minutes. The exact value that you use to define these parameters depend what unit of measure the operating system uses.

For example:

```
57 min = 3420 seconds = 6840 half seconds = 3420000
milliseconds
```

**Note:** If the firewall time out is shorter than the common 1 hour value, further decrease these values. The network overhead as a result of enabling TCP KeepAlive is minimal.

The following table summarizes the `Wait Time Before Probing` and `Interval Between Retry Probes` parameters for each operating system.

**Table 17** Setting TCP parameters for each operating system

| Operating system | Temporary setting | Permanent setting |
|---|---|---|
| AIX | # `no -o tcp_keepidle = 6840`<br># `no -o tcp_keepintvl = 6840`<br>where the TCP parameter value is defined in half-seconds. | `/etc/rc.net` |
| HP-UX | # `ndd -set /dev/tcp tcp_time_wait_interval 3420000`<br># `ndd -set /dev/tcp tcp_keepalive_interval 3420000`<br>where the TCP parameter value is defined in milliseconds. | `/etc/rc.config.d/nddconf` |
| Linux | # `sysctl -w net.ipv4.tcp_keepalive_time = 3420`<br># `sysctl -w net.ipv4.tcp_keepalive_intvl = 3420` | Add the `net.ipv4.tcp_parameter=`*tcp_value* commands to the `/etc/sysctl.conf` file, then issue the following command:<br>RHEL: `chkconfig sysctl on` |

**Table 17** Setting TCP parameters for each operating system (continued)

| Operating system | Temporary setting | Permanent setting |
|---|---|---|
| | where the TCP parameter value is defined in seconds. | SLES: `chkconfig boot.sysctl on` |
| Solaris | # `ndd -set /dev/tcp tcp_time_wait_interval 3420000`<br># `ndd -set /dev/tcp tcp_keepalive_interval 3420000`<br>where the TCP parameter value is defined in milliseconds. | Add the `ndd` commands to the `/etc/rc2.d/S69inet` file. |
| Windows | Not applicable | Modify the following registry keys:<br>`HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime`<br>DWORD=3420000<br>`HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveInterval`<br>DWORD=3420000 |

# Determining service port requirements

Before you modify the service port range on the NetWorker host or on a firewall, determine the minimum number of required service ports for the NetWorker host.

The number of ports that the NetWorker software daemons and processes require for communication depends on the NetWorker installation type. This section describes how to calculate the minimum number of service ports that are required for each NetWorker installation type (Client, Storage Node, Server, or NMC Server) and how to view or update the service port range value.

When the datazone uses an external firewall, open the service port range in the firewall for TCP connections. Some operating systems enable personal firewall software on a host by default. For example, Windows 7 enables Windows Firewall and Red Hat Linux 6 enables iptables. The NetWorker installation process on Windows adds firewall rules to the Windows firewall for NetWorker. The NetWorker installation process on UNIX does not add firewall rules to a personal firewall. When you use personal firewall software on a UNIX host, create the firewall rules for the NetWorker software manually.

When the NetWorker software interacts with other applications in the environment, for example, a Data Domain appliance, define additional service ports on a firewall.

# NetWorker client service port requirements

This section describes the port requirements for standard, NDMP, and Snapshot clients.

## Service port requirements for a standard NetWorker client

A standard NetWorker client requires a minimum of 4 TCP service ports to communicate with the NetWorker server. Snapshot services require two additional ports.

The following table summarizes the TCP service port requirements and the RPC program number for each program on a NetWorker client.

**Table 18** Standard NetWorker Client port requirements to NetWorker server

| RPC program number | Port number | Daemon/program |
|---|---|---|
| TCP/390113 | TCP/7937 | nsrexecd/nsrexec |
| TCP/390113 | TCP/7938 | nsrexecd/portmap |
| TCP/390435 | Dynamic TCP port from the service port range | nsrexecd/res_mirror |
| TCP/390436 | Dynamic TCP port from the service port range | nsrexecd/gss_auth |

## Service port requirements for an NDMP client

An NDMP client that sends data to an NDMP device requires access to TCP ports through the firewall only.

The service port range in the NSRLA database on the host does not require modifications.

## Service port requirements for Snapshot clients

When you configure a snapshot backup each Snapshot client requires 2 TCP ports for the PowerSnap service, in addition to the 4 standard client ports.

The following table summarizes the two additional ports that a Snapshot client requires.

**Table 19** Additional service port requirements for Snapshot clients

| RPC program number | Port number | Daemon/program |
|---|---|---|
| TCP/390408 (Snapshot services) | Dynamic TCP port from the service port range | nsrpsd |
| TCP/390409 (Snapshot services) | Dynamic TCP port from the service port range | nsrpsd/nsrsnapckd |

# Service port requirements for NetWorker storage nodes

When you calculate the service port requirements for a storage node, only consider the devices that the storage node manages. To accommodate growth in the environment and the addition of new devices, It is recommended that you allocate

extra service ports for the NetWorker storage node. The minimum number of service ports that a storage node requires is 5. This number includes the four TCP service ports that are required for a NetWorker client and one service port for the storage management process, nsrsnmd. NetWorker requires additional ports and the amount differs for each device type used.

Use the following formulas to calculate storage node port requirements:

- For NDMP-DSA devices: `5 + #backup_streams`
- For tape devices: `5 + #devices + #tape_libraries`
- For AFTD or Data Domain Boost devices: `5 + #nsrmmds`

where:

- *#devices* is the number of devices that are connected to the storage node.
- *#tape_libraries* is the number of jukeboxes that the storage node accesses. The storage node has one nsrlcpd process for each jukebox.
- *#nsrmmds* is the sum of the **Max nsrmmd count attribute** value of each device that the NetWorker storage node manages.

The following table summarizes the port requirements specific to the storage node programs.

**Table 20** Service port requirements for storage nodes

| RPC program number | Port number | Daemon/program |
|---|---|---|
| TCP/390111 | Dynamic TCP port from the service port range. | nsrnsmd |
| TCP/390429 | Dynamic TCP port from the service port range. | nsrlcpd |
| TCP/390104 | Dynamic TCP port from the service port range. Total port number depends on device type. | nsrmmd |

**Note:** In enterprise environments that require the restriction of unattended firewall ports for security reasons, configure the storage node attributes **mmds for disabled devices** and **Dynamic nsrmmds unselected (static mode)** to prevent a listener from starting an inactive nsrmmd port. The *NetWorker Administration Guide* provides more information.

## Service port requirements for the NetWorker server

The NetWorker server requires a minimum of 15 service ports.

Additional ports are required when the NetWorker server manages devices. Additional port requirements differ for each device type used.

To determine the service port range, use the following calculation:

- For NDMP-DSA or SnapImage devices: `14 + #backup_streams`
- For tape devices: `14 + #devices + #tape_libraries`
- For AFTD or Data Domain Boost devices: `14 +#nsrmmds`

where:

- *#devices* is the number of devices that are connected to the storage node.

- *#tape_libraries* is the number of jukeboxes that the storage node accesses. The storage node has one nsrlcpd process for each jukebox.
- *#nsrmmds*is the sum of the **Max nsrmmd count** attribute value of each device that the NetWorker storage node manages.

To accommodate growth in the environment and the addition of new devices, allocate extra service ports for the NetWorker server.

**Note:** The Software Configuration wizard requires one service port. The port is dynamic and closes when the wizard closes. If you use the Software Configuration wizard, add one additional port to the service port range.

The following table summarizes the port requirements specific to the Server programs.

**Table 21** NetWorker server program port requirements

| RPC program number | Port number | Daemon/program |
|---|---|---|
| TCP/390103 | Dynamic TCP port from the service port range | nsrd |
| TCP/390109 | User-defined UDP | nsrd/nsrstat<br>**Note:** Optional, NetWorker uses this port for internal communications. For example, automatic discovery and initial ping (is alive) checks of the NetWorker server. Backup and recovery operations do not use this port. NetWorker does not require this port through an external firewall. |
| TCP/390105 | Dynamic TCP port from the service port range | nsrindexd |
| TCP/390107 | Dynamic TCP port from the service port range | nsrmmdbd |
| TCP/390437 | Dynamic TCP port from the service port range | nsrcpd |
| TCP/390433 | Dynamic TCP port from the service port range | nsrjobd/jobs |
| TCP/390439 | Dynamic TCP port from the service port range | nsrjobd/rap |
| TCP/390438 | Dynamic TCP port from the service port range | nsrlogd |
| TCP/390430 | Dynamic TCP port from the service port range | nsrmmgd |

**Note:** If you restrict unattended firewall for security reasons, then use the storage node attributes **mmds for disabled devices** and *Dynamic nsrmmds unselected (static mode)* to prevent a listener from starting on an inactive `nsrmmd` port.

## Service port requirements for NMC Server

The minimum service port range for the NMC server to communicate with the NetWorker server is the same as a standard NetWorker client.

The NMC server also requires two TCP service ports to communicate with the each NetWorker client. The following table summarizes the TCP service port requirements and the RPC program number for each program on a the NMC server.

**Table 22** Port requirements to NMC server to each NetWorker client

| RPC program number | Port number | Daemon/program |
|---|---|---|
| TCP/390113 | TCP/7937 | nsrexecd/nsrexec |
| TCP/390113 | TCP/7938 | nsrexecd/portmap |

# Configuring service port ranges in NetWorker

After you determine the service port requirements for a NetWorker host, you must confirm which port numbers are available between each host, and then configure the port range on each NetWorker host and on the firewall.

## Determine the available port numbers

Before you define ports in the service ports attribute for a NetWorker host, determine the current service port allocations for the host by using the `netstat -a` command.

After you determine which ports are available, you can decide which ports to allocate for NetWorker host communications. Before you select the ports, consider the following information:

- The service port range for each NetWorker host must contain port 7937 and 7938. The `nsrexecd` daemon reserves these ports and you cannot change the ports numbers.
- It is recommended that you select ports within the default range of 7937-9936.
- To avoid conflicts with other daemons or services on the host, do not assign ports under 1024.

## Configuring the port ranges in NetWorker

The service ports attribute in the NSRLA resource defines which TCP ports that the NetWorker process can listen on and connect to.

To define the service port on each NetWorker host in the datazone, use NMC or the `nsrports` command.

### Enabling updates of the NSR system port ranges resource

The nsrexec database on each NetWorker host has its own administrators list. By default, only users that login to the NetWorker host locally can update the NSR system port ranges resource. Perform the following steps to add users to the

administrator list of the NSR system port ranges resource and enable remote updates of the attribute.

**Procedure**

1. Connect to the target NetWorker host.
2. To connect to the nsrexec database, from a command prompt, use the `nsradmin` program:

   ```
   nsradmin -p nsrexec
   ```

3. Display the current administrators list:

   ```
   p NSR system port ranges
   ```

   In this example, only the local users can update the attributes in the NSR system port ranges resource:

   ```
   nsradmin> p NSR system port ranges
   type: NSR system port ranges;
   service ports: 7937-9936;
   connection ports: 0-0;
   administrator: *@localhost;
   ```

4. Update the administrator attribute to include a remote account:

   ```
   update administrator: *@localhost, username@system
   ```

   For example, if you connect to the NMC server with the NMC administrator from the NMC client *mnd.mydomain.com*, type:

   ```
   update administrator: *@localhost,
   administrator@mnd.mydomain.com
   ```

5. When prompted, type **y**.
6. Exit the `nsradmin` program:

   ```
   quit
   ```

## Configuring the port ranges in NetWorker by using NMC

Use the NMC to view and modify the current port ranges for each NetWorker host.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**Procedure**

1. On the **Configuration** window, select **Hosts**.
2. In the **Known Hosts** window, right-click the NetWorker host, and then select **Configure Ports.**
3. On the **General** tab, review the value in the **Administrators** attribute:
   - If you see the message:

     ```
     No privilege to view administrator list then the account
     that you used to log in to the NMC server does not have
     permission to modify the port ranges.
     ```

Enabling updates of the NSR system port ranges resource on page 143 describes how to provide user accounts with the ability to modify the service port attribute.

- If you see accounts in the **Administrators** attribute, then update the **Service ports** attribute with the calculated service port range. For multiple ranges, type one range per line.

4. In the **Service ports** attribute, specify the calculated service port range. For multiple ranges, type one range per line.

   **Note:** It is recommended that you do not change the **Connection ports** attribute from the default value 0-0.

5. Click **Ok**.
6. On the NetWorker host, stop, and then start the NetWorker services or daemons.

## Configuring the port ranges in NetWorker by using nsrports

To view and modify the current port ranges for each NetWorker host from a command prompt, use the `nsrports` program.

### About this task

**`nsrports -s target_hostname[-S|-C]range`**

**Table 23** nsrports options

| Option | Description |
|---|---|
| -s *target_hostname* | Optional. Use this option when updating the port range for a remote NetWorker host. Enabling updates of the NSR system port ranges resource on page 143 describes how to enable remote access of the NSR system port ranges resource. |
| -S *range* | Sets the service port range to the value specified by range. The default range is 7937-7941. If the range is not a consecutive set of ports, use a space to separate the port values. |
| -C *range* | Sets the connection port range to the value specified by range. It is recommended that you do not change the connection ports attribute from the default value 0-0. |

For example, to modify the service port attribute in the NSR system port ranges resource on *myclient.emc.com*, perform the following steps:

### Procedure

1. Display the current port range:

   ```
   nsrports -s myclient.emc.com
   ```

   ```
   Service ports: 7937-7940
   Connection ports: 0-0
   ```

2. Update the service port range. Separate multiple port ranges with a space. For example:

   ```
   nsrports -s myclient.emc.com -S 7937-7938 7978-7979
   ```

> **Note:** If you do not have permission to update the NSR system port ranges attribute, an error message similar to the following appears: `nsrexecd: User 'username' on machine 'hostname' is not on 'administrator' list`. Enabling updates of the NSR system port ranges resource on page 143 describes how to enable user access to update the **NSR system port ranges** resource.

3. Confirm the service port attribute updated successfully. For example:

```
nsrports -s myclient.emc.com
```

```
Service ports: 7937-7938 7978-7979
Connection ports: 0-0
```

4. On *myclient.emc.com*, stop, and then start the NetWorker services or daemons.

# Configuring the service ports on the firewall

To enable communication between the NetWorker host and other applications, configure additional firewall rules.

The NetWorker software may communicate with other applications on ports outside of the service port range, for example, to communicate with a Data Domain or Avamar **Utility** node. The following table summarizes the firewall requirements for each NetWorker installation type and applications.

**Table 24** Port requirements for NetWorker communications with applications

| Source host | Destination host | Protocol | Ports to open on the firewall |
|---|---|---|---|
| NetWorker client | NetWorker server | TCP | 9090. The default port used to communicate with the NetWorker Authentication Service.<br>Port range determined in NetWorker client service port requirements on page 140. |
| NetWorker client | NetWorker Storage Node | TCP | Port range determined in NetWorker client service port requirements on page 140. |
| NetWorker client | NMC server | TCP | Port range determined in NetWorker client service port requirements on page 140. |
| NetWorker client | Data Domain | TCP<br>TCP/UDP | 2049, 2052<br>111 (Portmapper) |
| NetWorker client | Avamar - all nodes | TCP | 27000 |

**Table 24** Port requirements for NetWorker communications with applications (continued)

| Source host | Destination host | Protocol | Ports to open on the firewall |
|---|---|---|---|
| | | TCP | 29000 (For SSL only) |
| NetWorker client | Avamar Utility Node | TCP | 28001 |
| NetWorker storage node | NetWorker client | TCP | Port range determined in NetWorker client service port requirements on page 140. |
| NetWorker storage node | NetWorker server | TCP | 9090. The default port used to communicate with the NetWorker Authentication Service.<br>Port range determined in Service port requirements for NetWorker storage nodes on page 140. |
| NetWorker storage node | Data Domain | TCP<br>TCP/UDP | 2049, 2052<br>111 (Portmapper) |
| NetWorker storage node | ESX Cluster | TCP | 902 |
| NetWorker storage node | vCenter server | TCP | 443 |
| NetWorker storage node (NDMP-DSA) | NetWorker server | TCP | Port range determined in Service port requirements for NetWorker storage nodes on page 140. |
| NetWorker server | ATMOS server | | 80, 443 |
| NetWorker server | EMC Licensing Server | TCP | 27000 |
| NetWorker server | NDMP filer | TCP | 10000<br>**Note:** When a NetWorker server uses Windows Firewall, manually create an inbound rule in for the `nsrdsa_save` program to allow communications over TCP port 10000. |
| NetWorker server | NetWorker client | TCP | Port range determined in NetWorker client service |

**Table 24** Port requirements for NetWorker communications with applications (continued)

| Source host | Destination host | Protocol | Ports to open on the firewall |
|---|---|---|---|
| | | | port requirements on page 140. |
| NetWorker server | NetWorker Storage Node | TCP<br>UDP | Port range determined in Configuring service port ranges in NetWorker.<br>**Note:** Open the 2 required UDP service ports on the firewall for TCP connections but there is no need to allow UDP connections through the firewall. |
| NetWorker server | Data Domain | TCP<br>TCP<br>TCP/UDP<br>TCP | 2049, 2052<br>111 (portmapper)<br>161 (Port used by SNMPd to query the Data Domain system)<br>3009 (Port used by Data Domain Cloud Tier device, and Backup Capacity Reporting (BCR), for the REST API |
| NetWorker server | Avamar **Utility** Node | TCP | 7937, 7938<br>2 ports in range 7939-9936 |
| NetWorker server | DPA | TCP | 3916, 4001 |
| NetWorker server | vCenter server | TCP<br>TCP 9090 (inbound) | 443<br>Port range determined in NetWorker client service port requirements on page 140 |
| NetWorker server | VMware Backup Appliance (EBR/VBA) | TCP | 8543<br>Port range determined in NetWorker client service port requirements on page 140. |
| NetWorker server | NMC server | TCP | Port range determined in NetWorker client service |

**Table 24** Port requirements for NetWorker communications with applications (continued)

| Source host | Destination host | Protocol | Ports to open on the firewall |
|---|---|---|---|
| | | | port requirements on page 140. |
| NetWorker server | NetWorker Module for Microsoft Applications (NMM) client | TCP | 6278 (Control port)<br>6279 (Data port)<br>For Hyper-V FLR Support:<br>10000 (HTTP)<br>11000 (Secure HTTPS)<br>10099 (Cache Service)<br>10024 (Persistence Service) |
| NMM client | NetWorker server | TCP | 6278 (Control port)<br>6279 (Data port) |
| NMM client | NMM Proxy Recovery Agent - target Virtual machines for recoveries | TCP | 50000<br>**Note:** This port is required for Hyper-V FLR recoveries only. |
| NMM Proxy Recovery Agent | NMM client | TCP | 50000<br>**Note:** This port is required for Hyper-V FLR recoveries only. |
| Avamar Utility Node | NetWorker client | TCP | 28002 |
| NMC server | NetWorker server | TCP | 9090. The default port used to communicate with the NetWorker Authentication Service.<br>**Note:** If you specified a different port when you configured the NetWorker Authentication Service, specify that port number.<br>5672 (Message queue adaptor)<br>**Note:** The AMQP clients interact with |

**Table 24** Port requirements for NetWorker communications with applications (continued)

| Source host | Destination host | Protocol | Ports to open on the firewall |
|---|---|---|---|
| | | | the Message Bus on port 5672, and it must be open. It is the default port (non-SSL). Port 5671 must be opened for SSL ports.<br><br>Port range determined in Service port requirements for NMC Server on page 143. |
| NMC server | NetWorker client | TCP | Port range determined in Service port requirements for NMC Server on page 143. |
| NMC server | Data Domain | TCP<br><br>TCP | 161 (Port used by SNMPd to query the Data Domain system)<br><br>162 (Port used by SNMPtrapd to capture Data Domain SNMP traps) |
| NMC Client | NMC server | TCP<br><br>TCP<br><br>UDP | 9000 (Port used by HTTPd to download the Console user interface)<br><br>9001 (Port used to perform RPC for calls from the Console Java client to the Console server)<br><br>5432 (Port used by Tabular Data Stream (TDS) for database queries)<br><br>You can modify default ports values. How to confirm the NMC server service ports on page 151 provides more information. |
| DPA | NetWorker server | TCP | 3741 |
| DPA | Data Domain | TCP | 22 |

**Table 24** Port requirements for NetWorker communications with applications (continued)

| Source host | Destination host | Protocol | Ports to open on the firewall |
|---|---|---|---|
| | | TCP/UDP | 161 (Port used by SNMPd to query the Data Domain system) |
| DPA | Avamar Utility Node | TCP | 5555 |
| Data Domain | NMC server | TCP/UDP | 162 (Port used by SNMPtrapd to capture Data Domain SNMP traps) |
| Data Domain | DPA | TCP/UDP | 162 (Port used by SNMPtrapd to capture Data Domain SNMP traps) |
| EMC Licensing Server | NetWorker server | TCP | 27000<br>27001 |
| VMware Backup Appliance (VBA/EBR) | NetWorker server | TCP | 8080<br>Port range determined in NetWorker client service port requirements on page 140. |

## How to confirm the NMC server service ports

The NMC server installation process prompts you to define the service ports that the NMC server will use.

To confirm the defined port numbers, review the `gstd.conf` file and look for the following lines:

- http_svc_port = *http_service_port*
- clnt_svc_port = *client_service_port*
- int db_svc_port = *client_db_port*
- authsvc_port=*auth_service_port*

where *http_service_port*, *client_service_port*, *client_db_port*, and *auth_service_port* are port numbers.

By default:

- HTTP service port is 9000.
- Client service port used to make RPC calls is 9001.
- The client database port is 5432.
- NetWorker Authentication Service port is 9090.

If you change the port values in the `gstd.conf` file, then you must restart the `gstd` daemon.

**Note:** The `gstd.conf` file is located in the *`NMC_install_dir`*`/opt/lgtonmc/etc` on UNIX and *`NMC_install_dir`*`\GST\etc` on Windows.

# Determining service port requirement examples

This section provides three examples to determine firewall port requirements. In each example, the NetWorker Server resides in the secure network.

Each example uses the following IP addresses and hostnames:

192.167.10.101 client_A
192.167.10.102 client_B
192.167.10.103 client_C
192.167.10.104 client_D
192.167.10.105 client_E
192.167.10.106 client_F
196.167.10.124 storage_node_X
192.167.10.125 storage_node_Y
192.167.10.127 storage_node_Z
192.167.10.126 NW_server

## Calculating service port ranges for a bi-directional firewall configuration

In this example:

- The **Service port** attribute on each client specifies a minimum of four service ports, for example: 7937–7940.
  **Note:** To simplify the configuration, configure each client to use the same four service port numbers.
- The firewall must allow outbound traffic, to the IP address of each NetWorker Client, on each of the service ports that are defined in the Service port attribute on the NetWorker Client. Because each client can specify the same port numbers, the firewall only needs to allow four ports for each client IP address. These port numbers can be a subset of the port numbers that are used by the NetWorker Server, as in this example.
- In pseudo syntax, the firewall rule for the service ports would look like this:

```
TCP, Service, src 192.167.10.*, dest 192.167.10.101, ports
7937-7940, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.102, ports
7937-7940, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.103, ports
7937-7940, action accept
...
```

In the previous pseudo syntax, the firewall configuration allows:

- Incoming service connections to the IP address of the NetWorker server on ports 7937–7958, from the IP addresses of each storage node, client, and any other host on the subnet.
- Connections to the IP addresses for each storage node on ports 7937–7948, and to each client IP address on ports 7937–7940. Ensure that you configure each

NetWorker host with the appropriate port range, then restart the NetWorker services for each host.

This is the most stringent configuration possible, but difficult to maintain.

To simplify the configuration and administration of the datazone, assign a range of 22 ports, 7937–7958 to each host, and then configure the firewall to allow traffic to these ports on any host, from any host.

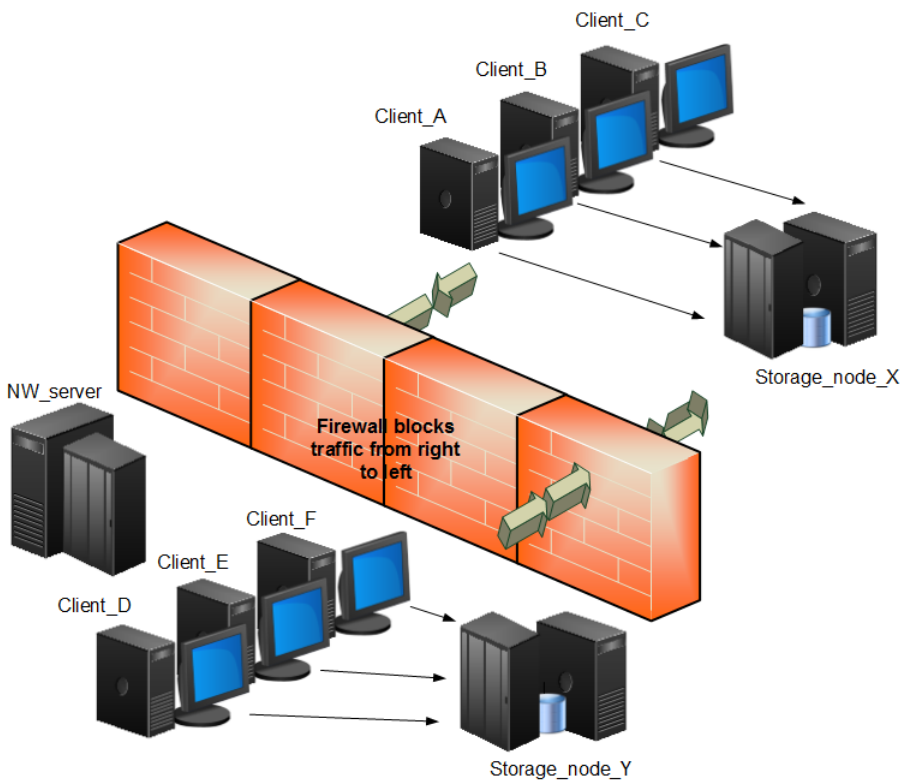
In pseudo syntax, the firewall rule for the service ports would look like this:

```
TCP, Service, src 192.167.10.*, dest 192.167.10.*, ports
7937-7958, action accept
```

## Calculating service ports for a uni-directional firewall environment with storage nodes

This example describes how to apply the basic rules of service port calculations to a sample network. In this example, there is one NetWorker **Storage** node on either side of the firewall. Clients D, E, and F in the secure network back up data to the storage node in the secure network. Clients A, B, and C in the insecure network back up data to the storage node in the insecure network. The firewall protects each host in the secure network. The firewall does not protect hosts in the insecure network. The firewall blocks network traffic from insecure to secure.

**Figure 16** Uni-directional firewall with storage nodes




This example requires you to only open service ports for the NetWorker Server on the firewall to allow inbound traffic. Calculate the service port requirements for the NetWorker Server with this formula:

- The **Service port** attribute on each client specifies a minimum of four service ports, for example: 7937–7940.

  **Note:** To simplify the configuration, configure each client to use the same four service port numbers.

- The firewall must allow outbound traffic, to the IP address of each NetWorker Client, on each of the service ports that are defined in the Service port attribute on the NetWorker Client. Because each client can specify the same port numbers, the firewall only needs to allow four ports for each client IP address. These port numbers can be a subset of the port numbers that are used by the NetWorker Server, as in this example.
- In pseudo syntax, the firewall rule for the service ports would look like this:

```
TCP, Service, src 192.167.10.*, dest 192.167.10.101, ports
7937-7940, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.102, ports
7937-7940, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.103, ports
7937-7940, action accept
...
```

This example requires you to only open service ports for the NetWorker Server on the firewall to allow inbound traffic. Calculate the service port requirements for the NetWorker Server with this formula:

14 +*(num devices)*+*(num libraries)* + 1 *(client push)*= 14 + 6 + 1 +1 = 22

In this example:

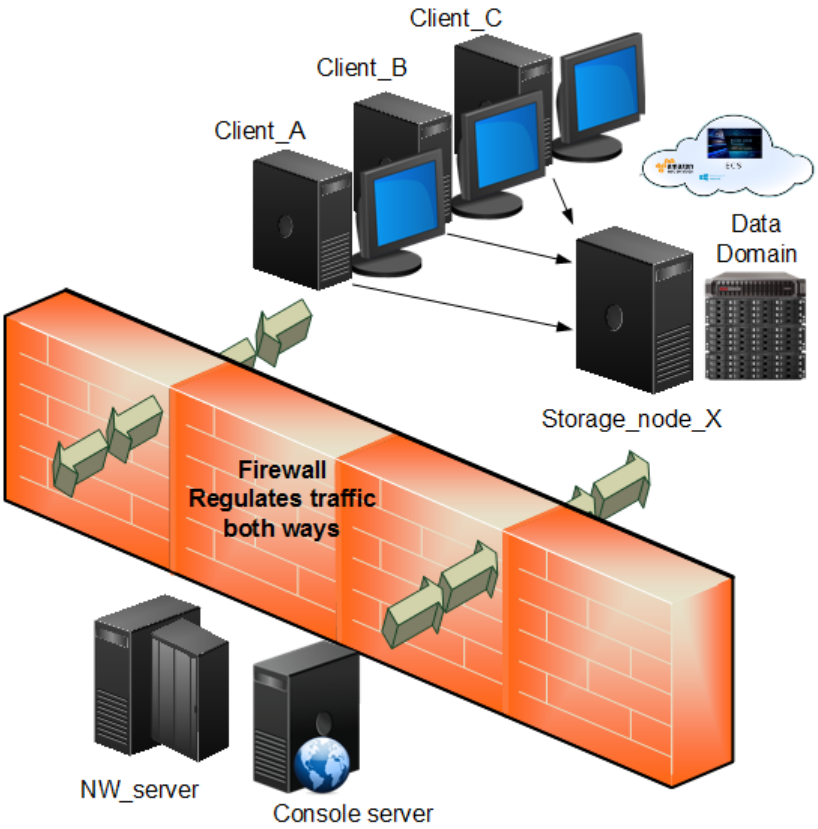
- The **Service ports** attribute of the NetWorker Server contains the range: 7937-7958.
- The firewall must allow inbound traffic to the IP address of the NetWorker Server on each service port with the exception of the UDP port. In this example, 22 ports in the range of 7937 to 7958 must allow inbound traffic to the NetWorker server.
- In pseudo syntax, the firewall rule for the service ports would look like the following:

```
TCP, Service, src 192.167.10.*, dest 192.167.10.126, ports
7937-7958, action accept
```

### Calculating service ports in a bi-directional firewall environment with Data Domain

This example shows how to apply the basic rules to a sample network with clients A, B and C, one storage node X, and a Data Domain appliance in an insecure network, which uses Data Domain Cloud Tier devices. The NetWorker server and NMC server are in a secure network. A single firewall separates the secure network from the insecure network. The NetWorker server has a tape library and six drives. The client sends backup data to the Data Domain appliance and each client acts as an NMC client.

**Figure 17** Bi-directional firewall with Data Domain appliance




## System port requirements for the NetWorker Server

Calculate the service port requirements for the NetWorker Server with this formula:

```
14 + (num devices) + (num libraries) = 14 + 6 + 1 = 21 service
ports
```

In this example:

- Configure the **Service port** attribute on the NetWorker Server to use a minimum of 21 service ports, for example: 7937–7957.
- Configure the firewall to allow inbound traffic, to the IP address of the NetWorker Server:
  - On the 21 service ports that are specified in Service port attribute of the NetWorker Server. The UDP port is not required.
  - On TCP ports 2049 and 2052 for Data Domain connectivity.
  - On TCP ports 111 and 161 for Data Domain connectivity.
- Configure the firewall to allow outbound traffic from the IP address of the NetWorker server on TCP port 3009.

In pseudo syntax, the firewall rules for the service ports would look like the following:

```
TCP, Service, src 192.167.10.*, dest 192.167.10.126, ports
7937-7957, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.126, ports
2049, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.126, ports
2052, action accept
```

```
TCP, Service, src 192.167.10.*, dest 192.167.10.126, ports 111,
action accept
UDP, Service, src 192.167.10.*, dest 192.167.10.126, ports 111,
action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.126, ports 161,
action accept
UDP, Service, src 192.167.10.*, dest 192.167.10.126, ports 161,
action accept
TCP, Service, src 192.167.10.126, dest 192.167.10.*, ports
3009, action accept
```

### Service port requirements for the NetWorker storage node

The storage node is in the insecure network and uses a Data Domain appliance. There are two Data Domain devices and each device uses a **Max nsrmmd count** value of 4. The **Dynamic nsrmmds** attribute is enabled on the storage node.

Calculate the service port requirements for the NetWorker storage node with this formula: 5 + 8 = 13 service ports.

In this example:

- The **Service port** attribute on the NetWorker storage node must specify a minimum of 13 service ports, for example: 7937–7949.
- The firewall must allow outbound traffic, from the NetWorker server to the IP address of the NetWorker storage node:
  - On the 13 service ports that are specified in the **Service port** attribute of the NetWorker storage node.
  - On TCP ports 2049 and 2052 for Data Domain connectivity.
  - On TCP/UDP port 111 for Data Domain connectivity.

In pseudo syntax, the firewall rules for the service ports would look like the following:

```
TCP, Service, src 192.167.10.126, dest 192.167.12.125, ports
7937-7949, action accept
TCP, Service, src 192.167.126.*, dest 192.167.10.125, ports
2049, action accept
TCP, Service, src 192.167.126.*, dest 192.167.10.125, ports
2052, action accept
TCP, Service, src 192.167.126.*, dest 192.167.10.125, ports
111, action accept
UDP, Service, src 192.167.126.*, dest 192.167.10.125, ports
111, action accept
```

### Service port requirements for the NetWorker Client

There are NetWorker clients in the insecure network. Each client requires four service ports. Two ports must be 7937 and 7938.

In this example:

- The **Service port** attribute on each client specifies a minimum of four service ports, for example: 7937–7940.

  **Note:** To simplify the configuration, configure each client to use the same four service port numbers.
- The firewall must allow outbound traffic, to the IP address of each NetWorker client, on the four service ports that are defined in the **Service port** attribute of

the NetWorker client. These port numbers can be a subset of the port numbers that the NetWorker server uses.

- In pseudo syntax, the firewall rules for the service ports would look like the following:

```
TCP, Service, src 192.167.10.*, dest 192.167.10.101, ports
7937-7940, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.102, ports
7937-7940, action accept
TCP, Service, src 192.167.10.*, dest 192.167.10.103, ports
7937-7940, action accept
```

# Troubleshooting

This section contains solutions to some common problems encountered when you configure NetWorker in a firewalled environment.

### Backups appear to stop responding or slow down dramatically

When you configure a firewall to drop packets outside an allowed range, but the firewall configuration does not allow for proper NetWorker connectivity:

- NetWorker will not get proper notification that a connection is not possible.
- The socket connections might not close correctly and remain in a TCP FIN_WAIT state. As a result, NetWorker requires more ports for client connectivity.

To avoid these issues, configure the firewall to reject packets outside the allowed range. When the firewall rejects packets, NetWorker receives an immediate notification of any connection failures and the remaining operations continue.

If you cannot configure the firewall to reject packets, reduce the TCP timeout values on the NetWorker server's operating system to reduce the impact of the problem. The *NetWorker Performance Optimization Planning Guide* describes how to change TCP timeout values.

### Cannot bind socket to connection port range on system hostname

This message appears in the savegroup messages or in stdout during manual operations when there are insufficient connection ports available and NetWorker cannot establish a connection.

To resolve this issue, ensure that the **Connection port** attribute in the NSR System Port ranges resource is 0-0 on the host that is specified by hostname.

### Failed to bind socket for service_name service: Can't assign requested address

This message appears when a NetWorker daemon cannot register to a port within the service port range because all ports are in use by other daemons and processes.

To resolve this issue, increase port range in the Service ports attribute in the NSR System port ranges resource on the NetWorker host and make a corresponding change in the firewall rules.

### Service is using port port_number which is outside of configured ranges: range

This message appears in the **Logs** window when a NetWorker daemon attempts to register to a port that is not within the service port range. This can occur because the port requirements of the NetWorker host exceed the number of service ports that are defined in the range.

To resolve this issue, increase port range in the Service ports attribute in the NSR System port ranges resource on the NetWorker host and make a corresponding change in the firewall rules.

**Note:** Communications between NetWorker processes on the same host do not follow defined rules. For example, the NetWorker server daemons communicate internally outside of the defined port range. Do not configure a firewall to limit the range for TCP traffic inside a single system.

### Connection refused

This message appears when the NetWorker host cannot establish a portmapper connection on port 7938.

To resolve this issue, ensure that the NetWorker software can register an RPC portmapper connection on port 7938.

### Connection reset by peer

This message appears when the connection between two NetWorker hosts closes prematurely.

To resolve this issue, configure the datazone to send a keep alive signal between the hosts at an interval that is shorter than the time out period defined on the firewall. Special considerations for firewall environments on page 137 describes how to configure the TCP keep alive signal.

### Unable to obtain a client connection to nsrmmgd (version #) on host hostname

This message appears on a Windows host when the Windows firewall Allow list on the NetWorker server does not contain the nsrmmgd process.

When this error message appears:

- A library that is configured on the NetWorker storage node will not enter “ready” state.
- Multiple nsrlcpd processes are started on the storage node.

To resolve this issue, ensure that the firewall is turned on, then add the nsrmmgd process to the Allow list of the Windows firewall on the NetWorker server host.

### nsrndmp_save: data connect:failed to establish connection

This message appears during an NDMP-DSA backup when a Windows NetWorker server uses Windows firewall, but an inbound rule for port 10000 does not exist.

To resolve this issue, perform the following steps:

1. Log in to the NetWorker server as a Windows administrator.
2. In the Windows Firewall application, on the **Advanced** properties select **Inbound Rules** > **New Rule**.
3. Select **Program**, and then click **Next**.
4. Select **This Program Path**.
5. Click **Browse**. Select the binary `nsrdsa_save.exe`, and then click **Next**.
6. Select **Allow the connection**, and then click **Next**.
7. Leave the default Profiles selections enabled, and then click **Next**.
8. Provide a name for the rule, and then click **Finish**.
9. Edit the new rule.
10. On the **Protocols and Ports** tab, perform the following steps:

a. From the **Protocol type** list box, select **TCP**.

b. From the **Local Port** list box, select **Specific Ports**. Specify port number `10000`.

c. Click **OK**.

### Unable to execute savefs job on host hostname: Remote system error - No route to host

This message appears during a scheduled backup when the NetWorker server can reach the client but cannot contact the nsrexecd process to start the savefs process.

To resolve this issue, ensure that you configure the following:

- Any external firewall between the two hosts to allow communication on the required service ports.
- A personal firewall on the client, for example, `iptables` on Linux, to allow communication between the two hosts on the required service ports.

### Modifying the port number of the NetWorker portmapper service

NetWorker contains a fully functional RPC portmapper service within the client daemon `nsrexecd`. The service runs by default on port 7938, and is used almost exclusively throughout NetWorker.

To modify the port number, perform the following steps:

1. On the NetWorker host, edit the `services` file. The services file is located in the following directory:
   - On UNIX and Linux — `/etc/services`
   - On Windows—`%WINDIR%\system32\drivers\etc\services`
2. Add the following entries:
   ```
   nsrrpc 7938/tcp lgtomapper #EMC NetWorker RPC
   nsrrpc 7938/udp lgtomapper #EMC NetWorker RPC
   ```
   Replace the port number with the desired port. Ensure that you choose a new port that is not already in use.
3. On the host, restart the NetWorker services.

### An error occurred while validating user credentials. Verify that NetWorker Authentication Service is running

This error message appears when the NMC server cannot validate user credentials with the NetWorker Authentication Service. The firewall configuration prevents the NMC server from contacting the NetWorker Authentication Service on the NetWorker server.

To resolve this issue, ensure that the firewall rules allow communication between the NMC server and NetWorker server on the port that you configured for the NetWorker Authentication Service. The default port is 9090.

# CHAPTER 5

# Data Security Settings

This chapter describes the settings available to ensure the protection of the data handled by NetWorker.


- AES encryption for backup and archive data ..... 162
- Federal Information Processing Standard compliance ..... 167
- Data integrity ..... 168
- Data erasure ..... 170
- Security alert system settings ..... 172

# AES encryption for backup and archive data

You can encrypt backup and archive data on UNIX and Windows hosts with the AES Application Specific Module (ASM). The AES ASM provides 256-bit data encryption. NetWorker encrypts the data based on a user-defined pass phrase, which you can securely store and retrieve from a lockbox.

The NetWorker software includes a preconfigured global directive that enables you to encrypt backup and archive data with the AES ASM. To use AES, modify the default NetWorker lockbox resource, set the datazone pass phrase for the NetWorker server, and then apply the AES directive to clients in the datazone. Do not use AES encryption to:

- Backup files that are encrypted by Encrypting File System (EFS). NetWorker reports the backup successful, but a recovery fails with the following message:

  ```
  recover: Error recovering <filename>. The RPC call completed
  before all pipes were processed
  ```

  The *NetWorker Administration Guide* provides more information about NetWorker interoperability with EFS.
- Backup a client that sends data to an encryption-enabled cloud device. Backup speeds decrease because the encryption functions occur twice.

## Creating or modifying the lockbox resource

By default, NetWorker creates a lockbox resource for the NetWorker server. The lockbox allows NetWorker to store pass phrases securely and enables you to specify a list of users that can store, retrieve, and delete AES pass phrases.

### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

### About this task

To create or edit the **Lockbox** resource, perform the following steps.

### Procedure

1. On the **Administration** window, click **Server**.
2. In the left navigation pane, click **Lockboxes**.
3. Right-click the lockbox resource for the NetWorker server, and then select one of the following options:
   a. To edit an existing lockbox resource, click **Properties**.
   b. To create a new lockbox resource, click **New**.
4. For a new lockbox resource only, in the **Name** field, type a name for the resource.

   The **Name** must meet the following requirements:

   - Does not contain these characters: \?/*:><\"|;
   - Does not contain only spaces and periods
   - Does not end with a space or a period

5. In the **Users** field, specify the list of users that have access to the AES pass phrases in one of the following formats:
   - `user=username`
   - `username@hostname`
   - `hostname`
   - `host=hostname`
   - `user=username, host=hostname`

   **Note:** If you enter a hostname or `host=hostname` in the **Users** attribute, then any user on the specified host can recover the files for the client. To enter a username without specifying the host, enter `user=username`.

6. Click **OK**.

**Results**

Only users that you specify in the **Users** field can modify the **Datazone pass phrase** attribute in the **NSR** resource.

## Defining the AES pass phrase

NetWorker uses a pass phrase to generate the datazone encryption key that backup and recovery operations use. Specify the AES pass phrase in the NSR resource to enable backup data encryption.

**Before you begin**

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**About this task**

If you do not specify a datazone pass phrase and you configure clients to use the AES directive to encrypt backups, NetWorker uses a default pass phrase. To define the AES pass phrase that NetWorker uses to generate the datazone encryption key, perform the following steps.

**Procedure**

1. On the **Administration** window, click **Server**.
2. In the left navigation pane, right-click the NetWorker server, and then select **Properties**.
3. On the **Configuration** tab in the **Datazone pass phrase** field, specify the pass phrase.

   It is recommended that you specify a pass phrase that meets the following requirements:
   - 9 or more characters in length
   - Contains at least one numeric character
   - Contains at least one uppercase and one lowercase letter
   - Contains at least one special character, for example # or !

4. Click **OK**.

### Results

NetWorker generates the datazone encryption key that is based on the pass phrase. To recover the data, you must know the datazone pass phrase that was in the **Datazone pass phrase** attribute at the time of the backup.

## Configuring the client resource to use AES encryption

To implement AES data encryption, apply the Encryption global directive to individual clients by using the Directives attribute in the Client resource.

### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

### Procedure

1. On the **Administration** window, click **Protection**.
2. In the left navigation pane, select **Clients**.
3. Right-click the client, and then select **Modify Client Properties**.
4. On the **General** tab, from the **Directive** attribute select **Encryption Directive**.
5. Click **OK**.

## Configure encryption for a client-initiated backup

To configure a NetWorker client to use AES encryption, use the NetWorker User program on Windows, or the `save` command.

### Configuring encryption for client-initiated backups on Windows by using NetWorker User

You can use AES to encrypt data that you backup by using the NetWorker User program.

#### Procedure

1. On the Windows host, start the NetWorker User program.
2. On the NetWorker User toolbar, select **Backup**.
3. On the **Options** menu, select **Password**.
4. When prompted, specify a password, and then click **OK**.

   The NetWorker User program creates the `C:\NETWORKR.CFG` file, which contains the password in an encrypted format.
5. On the **Backup** window, mark the files for backup.
6. On the Backup toolbar, select **Encrypt**.

   An E appears in the **Attributes** column for each marked file and directory.
7. Start the backup operation.

#### Results

NetWorker uses AES encryption to back up the data based on the value specified in the **Datazone pass phrase** attribute of the **NSR** resource on the NetWorker server at the time of the backup.

**Note:** To recover the data, NetWorker prompts you for the password that you defined for the backup.

### Configuring AES encryption by using the save command

To perform an AES encrypted backup from the command line, you must create a local AES directive file that the `save` program uses during backup.

**Procedure**

1. On the host, create a directive file.

   On Windows, create a text file named `nsr.dir`. On UNIX, create a text file named `.nsr`.

   You can create the file in any directory on the host.

2. Add the following two lines to the directive file:

   ```
   << / >>
   +aes: *
   ```

3. Save the directive file.
4. Perform the backup by using the `save` command with the *-f* option.

   `save -f` ***full_path_to_directive_file backup_object***
   For example, to back up the directory `c:\data` on a Windows host where you created the `nsr.dir` file in the `c:\directives` folder, type the following command:

   ```
   save -f c:\directive c:\data
   ```

**Results**

The backup operation encrypts the backup data based on the value specified in the **Datazone pass phrase** in the NSR resource, on the NetWorker server.

## Recover encrypted data

You can recover AES encrypted data by using the NMC Recovery Wizard, the NetWorker User program, or the `recover` command.

To decrypt backup data, the recovery operation must use the Datazone pass phrase value that was used to encrypt the backup data. By default, a recovery operation will use the current value of the Datazone pass phrase attribute to recover the data. If the current Datazone pass phrase value differs from the Datazone pass phrase value that was specified at the time of the backup, then the recovery operation fails.

### Recovering AES encrypted data by using NetWorker User

You can use the NetWorker User program to recover AES encrypted data on a Windows host.

**About this task**

To specify the Datazone pass phrase value that was used to encrypt the backup, perform the following steps.

**Procedure**

1. Start the `NetWorker User` program with the following command:

   `winworkr -p` *pass_phrase*....

where *pass_phrase* is the pass phrase that is specified in the **Datazone pass phrase** attribute of the NSR resource on the NetWorker server at the time of the backup.

When you recover data that requires different pass phrases, use additional `-p` *pass_phrase* options to specify each required pass phrase.

2. Confirm that the recover operation successfully recovers the data.

   When you specify an incorrect pass phrase:

   - NetWorker creates 0kb files but does not recover the data into the files.
   - The recover output reports a message similar to the following:

     ```
     Invalid decryption key specified
     ```

## Recovering AES encrypted data by using the NMC Recovery wizard

You can use the NMC Recovery wizard to recover AES encrypted data. The *NetWorker Administration Guide* describes how to use the NMC recovery wizard.

### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

### About this task

To specify the Datazone pass phrase value that was used to encrypt the backup, perform the following additional steps on the **Select the Recovery Options** window of the NMC Recovery wizard:

### Procedure

1. Select **Advanced Options**.
2. In the **Pass phrases** field, specify the pass phrase(s) used at the time of the backup.

## Recovering AES encrypted data by using the recover command

Use the `recover` command to run recover AES encrypted data from a command line.

### Before you begin

Perform the following steps with the root account on UNIX or an administrator account on Windows.

### Procedure

1. To specify a pass phrase, use the -p option with the `recover` command. For example:

   **`recover -a -p`** ***`pass_phrase filesystem_object`***

   where:

   - *pass_phrase* is the pass phrase that is specified in the **Datazone pass phrase** attribute of the NSR resource on the NetWorker server at the time of the backup. When you recover data that requires different pass phrases, use additional **`-p`** ***`pass_phrase`*** options to specify each required pass phrase.
   - *filesystem_object* is the full path to the data that you want to recover.

2. Confirm that the recover operation successfully recovers the data.

   When you specify an incorrect pass phrase:

   - NetWorker creates 0kb files but does not recover the data into the files.
   - The recover output reports a message similar to the following:

     ```
     Invalid decryption key specified
     ```

# Federal Information Processing Standard compliance

NetWorker 9.1.1 and later running on Linux and Windows has been updated to prevent operation when either:

- The pre-configured cryptographic SSL library has been modified or corrupted.
- The cryptographic library being used is not in the approved FIPS 140-2 set.

As a result, NetWorker 9.1.1 and later running on Linux and Windows qualifies as Federal Information Processing Standard (FIPS) 140-2 compliant.

As with prior versions of NetWorker running on Linux and Windows version 9.1.1 and later ships with, and is pre-configured by Dell EMC to use, encryption algorithms that are in the approved FIPS 140-2 set.

Federal Information Processing Standard (FIPS) 140-2 compliant encryption algorithms are used for:

- Encryption in-flight
- TLS/SSL handshaking in `nsrauth` workflows
- libCURL interfaces
- AESASM (client side encryption Application Specific Module)
- Storing of secrets, for example, passwords

**Note:**

NetWorker clients running on Linux on PowerPC do not utilize FIPS compliant libraries.

In NetWorker on Linux, by default the FIPS mode is set to *disabled*. To enable FIPS mode operation on NetWorker on Linux, create a file `/nsr/debug/fipsenable`, and restart NetWorker services. On Windows, NetWorker always utilizes FIPS mode, and you cannot switch to non-FIPS mode.

The disablement of FIPS mode does not change the encryption algorithms that are used by NetWorker. The encryption algorithms are consistent between FIPS and non-FIPS modes.

NetWorker Module for Databases and Applications (NMDA) for MySQL running on Linux does not utilize FIPS compliant encryption libraries, and is not supported on Linux client platforms where FIPS mode is enabled.

# Data integrity

NetWorker enables you to verify the integrity of the backup data and the integrity of the NetWorker server databases.

## Verifying the integrity of the backup data

Use the Auto media verify attribute for a pool resource or the Verify files option in the NetWorker User program to automatically verify the data that NetWorker writes to a volume.

### Configuring auto media verify for a pool

Media pools provide you with the ability to do direct backups to specific devices. When you label a volume, you specify the pool for the volume. To configure NetWorker to automatically verify that the data that is written to media is valid, enable the Auto media verify attribute for the Pool resource.

#### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

**Note:** This option cannot be modified for 'Default' pools.

#### Procedure

1. On the **Administration** window, click **Media**.
2. In the left navigation pane, select **Media Pools**.
3. On the **Media Pools** window, right-click the pool, and then select **Properties.**
4. On the **Configuration** tab, select **Auto media verify**.
5. Click **OK**.

### Configuring verify files in NetWorker User

The Verify files feature compares the file types, file modification times, file sizes, and file contents. The feature does not verify other system attributes, such as read-only, archive, hidden, system, compressed, and file access control list (ACL). Use the Verify files feature to ensure that backup data on the NetWorker server matches the data on the local disk.

#### Before you begin

#### About this task

**Note:** The Verify files feature is not available for NetWorker clients on UNIX.

#### Procedure

1. Connect to the NetWorker host as an administrator.
2. In the **NetWorker User** program, from the **Operation** menu, select **Verify Files**.
3. Select the data that you want to verify.
4. From the **View** menu, select **Required volumes**.

   The **Required Volumes** window appears with the list of volumes that contain the data that you want to verify. Mount the volumes in devices.

5. Click **Start**.

   The **Verify Files** status window appears and provides the progress and results of the Data Verification process. The output displays data mismatch messages to alert you to any detected data changes since the backup.

**Results**

Verification also determines if a hardware failure kept the NetWorker server from completing a successful backup. The Verify files feature provides a way to test the ability to recover data.

The following output provides an example where the Verify Files process verifies four files, and reports that one file, `recover_resource.txt` has changed since the backup:

```
Verify Files
Requesting 4 file(s), this may take a while...
Verify start time: 28/10/2013 3:46:36 PM
Requesting 1 recover session(s) from server.
91651:winworkr: Successfully established AFTD DFA session for
recovering save-set ID '4285011627'.
C:\data\mnd.raw
C:\data\pwd.txt
C:\data\lad.txt
32210:winworkr: DATA MISMATCH FOR C:\data\recover_resource.txt.
C:\data\
Received 4 file(s) from NSR server `bu-iddnwserver'
Verify completion time: 28/10/2013 3:46:48 PM
```

## Verifying the integrity of the NetWorker server media data and client file indexes

NetWorker provides you with the ability to manually check the integrity and consistency of the media database and client file index by using the `nsrim` and `nsrck` commands.

### Using nsrim to check media database consistency

Use the `nsrim -X` command to check the consistency of the data structures of the save set with the data structures of the volume.

**About this task**

**Note:** The `nsrim -X` process will also perform media database maintenance tasks. NetWorker server media database and index data management on page 170 provides more information.

### Using nsrck to check consistency of the client file index

NetWorker uses the `nsrck` program to check the consistency of the client file index save set records.

When the NetWorker server starts, the `nsrindexd` program starts the `nsrck` process to perform consistency checks. You can also manually start the `nsrck` program to check the consistency of the client file indexes.

For example: `nsrck -L` ***x*** `[-C` ***client_name***`]`

where:

- `-c` *client_name* is optional. When you use the -C option, `nsrck` performs consistency checks on client file index for the specified client.
- *x* is the consistency check level. The following table provides more information.

**Table 25** Levels available for the nsrck process

| Level | Description |
|---|---|
| 1 | Validates the online file index header, merging a journal of changes with the existing header. Moves all save set record files and the corresponding key files to the appropriate folder under the `C:\Program Files\EMC NetWorker\nsr\index\`*`client_name`*`\db6` folder on Windows hosts or the `/nsr/index/`*`client_name`*`/db6` directory on UNIX hosts. |
| 2 | Performs a level 1 check and checks the online file index for new and cancelled saves. Adds new saves to the client file index, and removes cancelled saves. |
| 3 | Performs a level 2 check and reconciles the client file index with the media database. Removes records that have no corresponding media save sets. Removes all empty subdirectories under `db6` directory. |
| 4 | Performs a level 3 check and checks the validity of the internal key files for a client file index. Rebuilds any invalid key files. |
| 5 | Performs a level 4 check and verifies the digest of individual save times against the key files. |
| 6 | Performs a level 5 check and extracts each record from each save time, to verify that each record can be extracted from the database. Re-computes the digest of each save time and compares the results with the stored digest. Rebuilds internal key files. |

The UNIX man page and the *NetWorker Command Reference Guide* provides detailed information about how to use the `nsrck` command and the available options.

# Data erasure

During a backup operation, NetWorker stores data in save sets on physical or virtual volumes. NetWorker stores information about the save sets in the media database and client file indexes.

Based on user-defined policies, NetWorker automatically performs media database and client file index management, which expires data on volumes and makes the data eligible for erasure. You can also manually erase data and remove data from the media database and client file indexes.

## NetWorker server media database and index data management

The NetWorker server uses the `nsrim` program to manage and remove data from the media database and client file indexes.

Two NetWorker processes automatically start the `nsrim` process:

- The `savegrp` process, after a scheduled group backup completes.
- The `nsrd` process, when a user selects the **Remove oldest cycle** option in the **NetWorker Administration** window.

The `nsrim` process uses policies to determine how to manage information about save sets in the client file index and media database. When the `savegrp` process starts `nsrim`, NetWorker checks the timestamp of the `nsrim.prv` file. If the timestamp of the file is greater than or equal to 23 hours, then the `nsrim` process performs the following operations:

- Removes entries that have been in a client file index longer than the period specified by the browse policy from the client file index.
- Marks save sets that have existed longer than the period specified by the retention policy for a client as recyclable in the media index.
- Deletes the data that is associated with recyclable save sets from an advanced file type device and removes the save set entries from the media database.
- Marks a tape volume as recyclable when all the save sets on the tape volume are marked recyclable. NetWorker can select and relabel recyclable volumes when a backup operation requires a writeable volume. When NetWorker relabels a recyclable tape volume, NetWorker erases the label header of the volume and you cannot recover the data.

NetWorker relabels a volume at the time of a backup or clone when a set of defined selection criteria is met. Use the **Recycle start** and **Recycle interval** attributes on the **Miscellaneous** tab of a **Pool** resource to schedule automatic volume relabeling for eligible volumes in a pool. The *NetWorker Administration Guide* provides more information.

## Manually erasing data on tape and VTL volumes

To erase all data on a tape volume, relabel the volume.

### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Operators user group.

### Procedure

1. On the **Administration** window, click **Devices**.
2. In the left navigation pane, click **Library**. On the right window, right-click the library, and then select **Label**.

   The **Details** window and **Label Library Media** appear.
3. (Optional) In the **Pool** field, select a different pool.
4. Click **OK**.

   The **Library Operation** window appears, which states that the library operation has started.
5. To track the status of the label operation, on the **Operations** tab, select **Monitoring**.
6. When prompted to overwrite label, click **OK**.

## Manually erasing data from an AFTD

Relabel an AFTD volume to erase all of the data.

### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

### Procedure

1. On the **Administration** window, click **Devices**.
2. In the left navigation pane, select **Devices**.
3. In the **Device** window, right-click on the AFTD device, and then select **Label**.
4. (Optional) in the **Target Media Pool** field, select a different pool.
5. Click **OK**.
6. If prompted to overwrite label, then right-click the label operation in the **Operations Status** window to confirm intent to overwrite the existing volume label with a new label, and then select **Supply Input**.

   A question window appears displaying this message:

   ```
   Label <labelname> is a valid NetWorker label. Overwrite it
   with a new label
   ```

7. Click **Yes**.

# Security alert system settings

NetWorker provides you with the ability to send security notifications, log, and track NetWorker server configuration changes to file, and provides a centralized logging mechanism to log security related events that occur in a NetWorker datazone.

## Monitoring changes to NetWorker server resources

The Monitor RAP (resource allocation protocol) attribute in the NetWorker Server resource tracks both before and after information related to additions, deletions, or modifications to NetWorker server resources and their attributes. NetWorker records these changes in the *NetWorker_install_dir*`\logs\rap.log` file.

### Before you begin

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators or Database Administrators user group.

### About this task

The `rap.log` file records the name of the user that made the change, the source computer, and the time the user made the change. NetWorker logs sufficient information in the `rap.log` file to enable an administrator to undo any changes.

### Procedure

1. In the left navigation pane, right-click the NetWorker server, and then select **Properties**.
2. On the **Administration** window, select **View** > **Diagnostic mode**.
3. On the **General** tab, select **Enabled** or **Disabled** for the **Monitor RAP** attribute.
4. Click **OK**.

## Security audit logging

NetWorker provides a centralized logging mechanism to log security related events that occur in a NetWorker data zone. This mechanism is called security audit logging.

The security audit log feature monitors and reports critical NetWorker events that relate to the integrity of the data zone or host. The security audit log feature does not monitor events that relate to the integrity of a backup.

When you install NetWorker in a data zone, each client is automatically configured to use security audit logging. Any audit logging configuration changes that you set on the NetWorker server are automatically communicated to all NetWorker 8.0 and later clients in the data zone. NetWorker automatically configures existing NetWorker clients to send security audit messages to the `nsrlogd` daemon when you:

- Update the NetWorker server software.
- Create new client resources.

Examples of security audit events that generate security audit messages include:

- Authentication attempts: Successful and unsuccessful attempts to log in to an NMC Server.
- Account management events: Password changes, privilege changes and when users are added to the list of remote administrators.
- Changes to program authorization: Deleting or adding peer certificates and redefining which binaries a user can execute remotely.
- Changes to the `daemon.raw` and audit log configurations.
- Events that can lead to the general compromise or failure of the system.

## Security audit logging overview

NetWorker enables security audit logging by default. NetWorker records security audit messages in the security audit log when the message severity level is at least as severe as the level defined in the NSR security audit log resource.

The NetWorker server contains an NSR auditlog resource. This resource configures security audit logging. The following actions occur when security audit logging is enabled in a datazone:

- NetWorker assigns a severity to each security audit messages.
- NetWorker server mirrors the NSR auditlog resource to NetWorker clients in the datazone. The NetWorker Client database stores the client side security audit log resource. The auditlog resource provides each client with the hostname of the machine that hosts the `nsrlogd` daemon and the types of security audit messages that the client should send to the nsrlogd daemon. The auditlog severity setting in the NetWorker server auditlog resource determines how each client receives the configuration information:
  - When the audit severity level is information, warning, or notice, the NetWorker server broadcasts the auditlog resource to each client when the `nsrd` daemon starts.
  - When the audit severity level is error, severe, or critical, the NetWorker server does not broadcast the auditlog resource to each client when the `nsrd` daemon starts. Instead the NetWorker clients request auditlog resource configuration updates from the last NetWorker server that backed up the client data. This passive method requires that the client has performed at least one backup to the NetWorker server before the client can receive updates to the auditlog resource. By default, the audit severity level is error.
- NetWorker clients process and send audit messages to the `nsrlogd` daemon.
- The `nsrlogd` daemon records the security audit messages to the security audit log file.

## Security audit logging configurations

While you can configure any NetWorker client in the datazone to run the `nsrlogd` daemon, there are certain performance and reliability advantages to using the NetWorker server for this task.

The following sections provide examples of security audit logging configurations and the advantages and disadvantages of each configuration.

### Single data zone: The NetWorker server hosts the nsrlogd daemon

By default, the `nsrlogd` daemon runs on the NetWorker server.

In this configuration, the `nsrlogd` daemon receives security audit messages from:

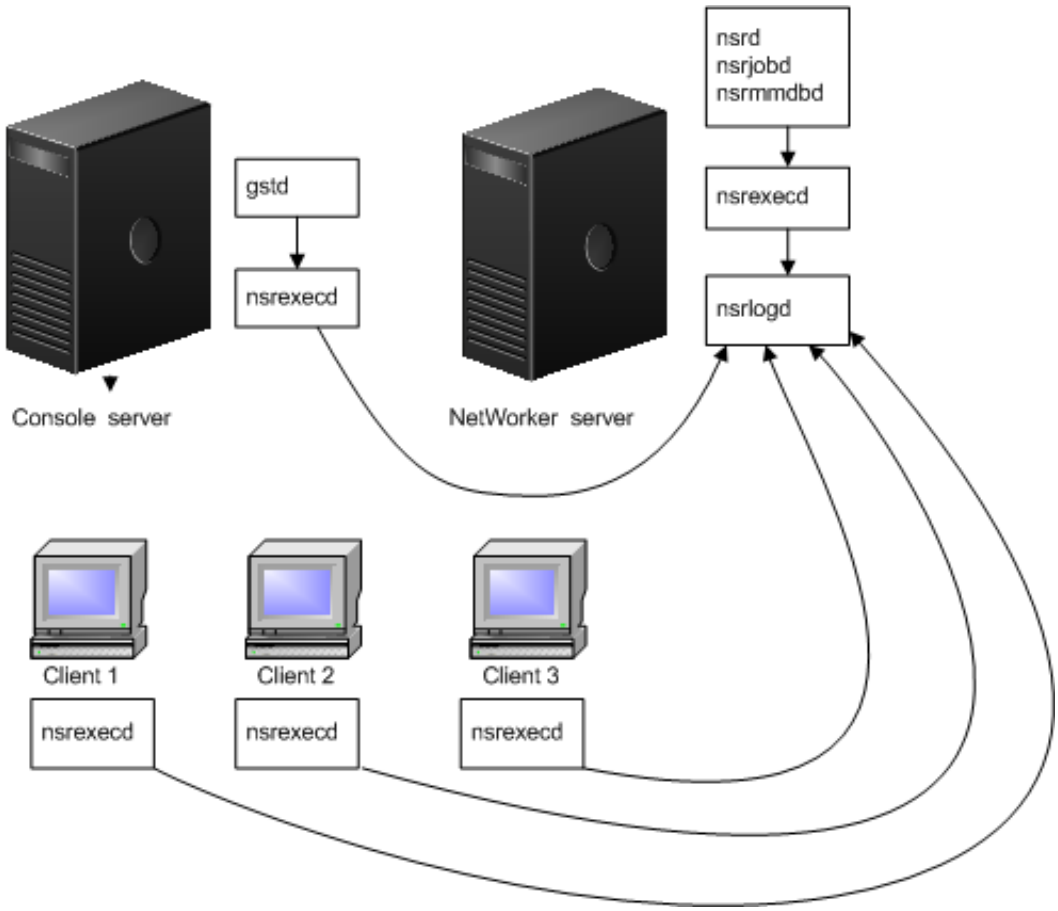
- The `gstd` and `nsrexecd` processes on the NMC server.
- The nsrexecd process on each NetWorker client in the data zone.
- The daemons that run on the NetWorker server.

Advantages:

- The NetWorker server daemons generate the majority of the security audit messages. In this configuration, the audit log messages are not sent over the network and will not increase network traffic.
- Security audit messages from each NetWorker client are sent to the NetWorker server. Additional network ports and routes to other networks are not required to send security audit messages.

The following figure provides an example of this configuration.

**Figure 18** The audit log server manages a single data zone




## Multiple data zones: The NMC server hosts the nsrlogd daemon

In this configuration, the nsrlogd daemon runs on the NMC server and the NMC server manages multiple NetWorker data zones. The NMC server must be configured as a client, on each NetWorker server.

Advantages:

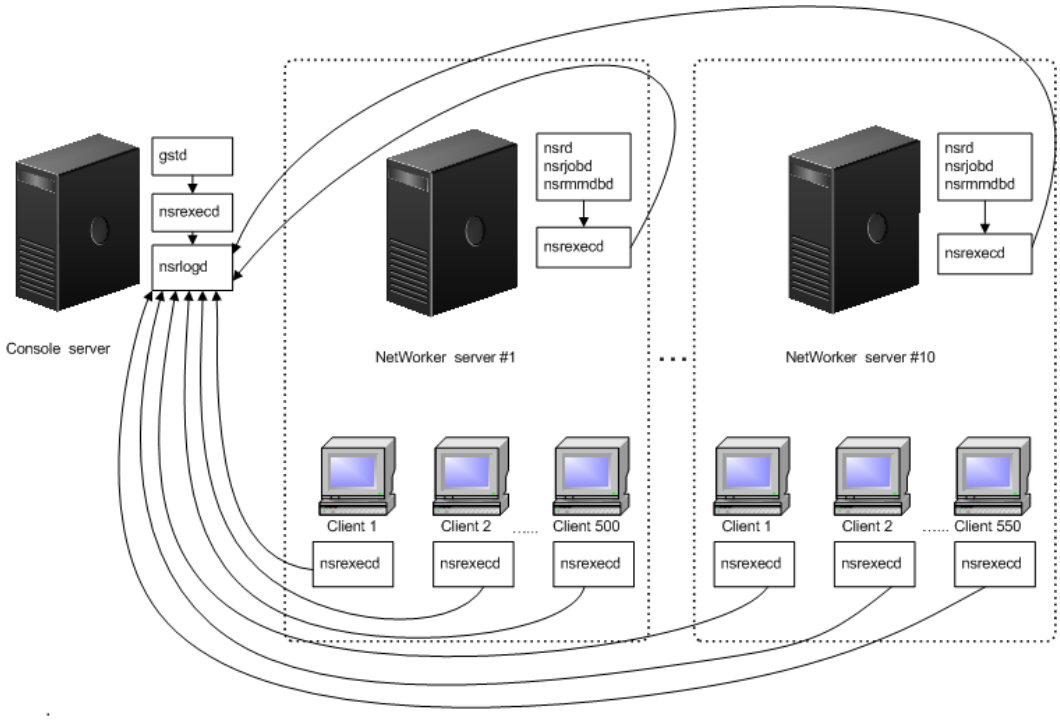
- Centralized logging of the security audit messages. The security audit log for each NetWorker server is stored on the NMC server.

Disadvantages:

- If the nsrlogd daemon is not accessible, either because the daemon fails or because of a message routing difficulty, security related events are not recorded.
- The NetWorker server daemons generate the majority of the security audit messages. In this scenario, the security audit log messages are sent over the network and increase network traffic.
- Each NetWorker host in each datazone must have a route to the NMC server.

The following figure provides an example of this configuration.

**Figure 19** The NMC server is the audit log server for multiple data zones




## Multiple datazones: Each NetWorker server hosts the nsrlogd daemon

In this configuration, each NetWorker server act runs the `nsrlogd` daemon and records the messages for a single data zone.

Each NetWorker client in the datazone sends security audit messages to the NetWorker server.

The NMC server is a client of the NetWorker server in Datazone 1.

Advantages:

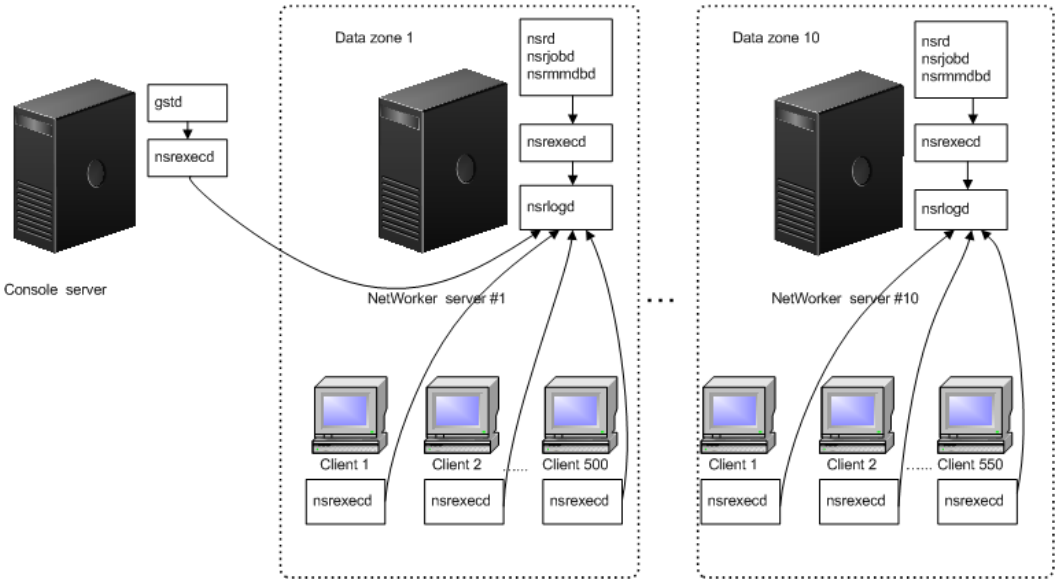
- The NetWorker server daemons generate the majority of the security audit messages. In this configuration, the audit log messages are not sent over the network and do not increase network traffic.
- Security audit messages from each NetWorker client are sent to the NetWorker server. Additional routes in other networks are not required to send security audit messages.

Disadvantages:

- You may not be able to access the security audit logs if the NetWorker server is compromised.
- You must manage multiple security audit logs.

The following figure provides an example of this configuration.

**Figure 20** Each NetWorker server in a data zone is the audit log server




## Security events

The security audit log feature detects and reports configuration changes that can result in inappropriate access or damage to a NetWorker server. NetWorker logs successful and unsuccessful attempts to create and delete security-related resources and modifications of security-related resource attributes in the audit log file.

### Resource database

The following table summarizes which resources and attributes the security audit log monitors in the resource database (RAP).

**Table 26** Security event resources and attributes - resource database (RAP)

| NSR Resource/NMC resource name | Attribute |
|---|---|
| NSR/NSR | Administrator<br>Authentication method<br>Datazone pass phrase |
| NSR Archive request/Archive request | Grooming |
| NSR auditlog /Security Audit log | Administrator<br>Auditlog filepath<br>Auditlog hostname<br>Auditlog maximum file size MB<br>Auditlog maximum file version<br>Auditlog rendered locale<br>Auditlog rendered service |

**Table 26** Security event resources and attributes - resource database (RAP) (continued)

| NSR Resource/NMC resource name | Attribute |
|---|---|
| | Auditlog severity |
| NSR client/Client | Aliases<br>Archive users<br>Backup command<br>Executable path<br>Password<br>Remote access<br>Remote user<br>server network interface |
| NSR Device/Devices | Remote user<br>Password<br>Encryption |
| NSR Data Domain /Data Domain devices | Username<br>Password |
| NSR De-duplication Node /Avamar deduplication node | Remote user<br>Password |
| NSR Hypervisor /Hypervisor | Command<br>Password<br>Proxy<br>Username |
| NSR Lockbox/Lockbox | Client<br>Name<br>Users |
| Notifications | Action |
| NSR Operation Status | command |
| NSR Report Home | Command<br>Mail Program |
| NSR restricted datazone /Restricted Data Zone (RDZ) | External roles<br>Privileges |

**Table 26** Security event resources and attributes - resource database (RAP) (continued)

| NSR Resource/NMC resource name | Attribute |
|---|---|
| | Users |
| Storage Node | Password<br>Remote user |
| Usergroup | External Roles<br>Name<br>Privileges<br>Users<br>Resource identifier |

## NetWorker client database

The following table summarizes which resources and attributes the security audit log monitors in the NetWorker client database (nsrexec).

**Table 27** Security event resources and attributes - NetWorker client database

| Resource | Attribute |
|---|---|
| NSR log | Administrator<br>Log path<br>Maximum size MB<br>Maximum versions<br>Name<br>Owner<br>Runtime rendered log<br>Runtime rollover by size<br>Runtime rollover by time |
| NSR peer information | Administrator<br>Certificate<br>Name<br>NW instance ID<br>Peer hostname |
| NSR remote agent | Backup type<br>Backup type icon |

**Table 27** Security event resources and attributes - NetWorker client database (continued)

| Resource | Attribute |
|---|---|
| | Features<br>Name<br>Product version<br>Remote agent executable<br>Remote agent protocol version |
| NSR system port ranges | Administrator<br>Connection ports<br>Service ports |
| NSRLA | Administrator<br>Auth methods<br>Certificate<br>Disable directed recover<br>Max auth attempts<br>Max auth thread count<br>My hostname<br>Name<br>NW instance ID<br>NW instance info file<br>private key<br>VSS writers |

## Audit message format

The security audit log file contains the timestamp, the category, the program name, and the unrendered message for each security audit message.

Use the `nsr_render_log` program to render the audit log file in to a readable format. For example:

**`nsr_render_log -pathyem`** ***`Security_Audit_ Log_filename`***

```
03/03/12 14:28:39 0 nsrd Failed to modify Resource type: 'NSR
usergroup', Resource name: 'Users' for Attribute: users' by
user: 'administrator' on host: 'nwserver.emc.com'
```

where:

- The TimeStamp is 03/03/12 14:28:39.

- The Category is 0.
- The ProgramName is nsrd.
- The RenderedMessage is `Failed to modify Resource type:` 'NSR usergroup', Resource name: 'Users' for Attribute: 'users' by user: 'administrator' on host: 'nwserver.emc.com'.

## Security audit log messages

This section provides a list of common messages that appear in the security audit log file when you set the severity level to information.

### nsrd Permission denied, user '*username*' on host: '*hostname*' does not have '*privilege1*' or '*privilege2*' privilege to delete this resource - *resource_type*

This message appears when a user attempts to delete a security-related resource but does not have the required privileges on the NetWorker server.

For example:

```
15/08/2014 8:56:31 AM 3 nsrd Permission denied, user 'debbie'
on 'bu-iddnwserver.iddlab.local' does not have 'Delete
Application Settings' or 'Configure NetWorker' privilege to
delete this resource -
NSR client.
```

### nsrd Permission denied, user *'username*' on '*hostname*' does not have '*privilege1*' or '*privilege2*' to create configure this resource - *resource_type*

This message appears when a user attempts to create a security-related resource but does not have the required privileges on the NetWorker server.

For example:

```
15/08/2014 9:11:43 AM 3 nsrd Permission denied, user 'debbie'
on 'bu-iddnwserver.iddlab.local' does not have 'Create
Application Settings' or 'Configure NetWorker' privilege to
create this resource -
NSR client.
```

### nsrd Failed to create Resource type: '*resource_type*', Resource name: '*resource_name*' by user: '*username*' on host: '*hostname*'

This message appears when a user cannot create a security-related resource. For example, if a user attempts to create a new client resource but the client hostname is not valid, a message similar to the following appears:

```
15/08/2014 8:49:57 AM 3 nsrd Failed to create Resource type:
'NSR client', Resource name: 'bu-exch1.lss.emc.com' by user:
'debbie' on host: 'bu-iddnwserver.iddlab.local'
```

### nsrd Permission denied, user '*username*' on host: '*hostname*' does not have *privilege1*' or '*privilege2* privilege to configure this resource - *resource_type*

This message appears when a user attempts to modify a security-related attribute in a resource but does not have the required privileges.

For example:

```
15/08/2014 9:03:45 AM 3 nsrd Permission denied, user 'debbie'
on 'bu-iddnwserver.iddlab.local' does not have 'Configure
```

```
NetWorker' OR 'Change Application Settings' privilege to
configure this resource - NSR client.
```

**nsrd Successfully created Resource type: '*resource_type*', Resource name: '*resource_name*' by user: '*username*' on host: '*hostname*'**

This message appears when a user successfully creates a new security-related resource.

For example:

```
15/08/2014 1:57:54 PM 3 nsrd Successfully created Resource
type: 'NSR notification', Resource name: 'new-notification' by
user: 'administrator' on host: 'bu-iddnwserver.iddlab.local'
```

**gstd Console: User '*username*' failed to login to Console server on host '*hostname*'**

This message appears when you specify an incorrect username or password on the NMC server login window.

For example:

```
14/08/2014 4:36:43 PM 0 gstd Console: User 'root' failed to
login to Console server on host 'bu-iddnwserver.iddlab.local'
```

**gstd Console: User '*username*' successfully logged in to Console server on host '*hostname*'**

This message appears when you successfully log in to the NMC server.

For example:

```
14/08/2014 4:36:49 PM 0 gstd Console: User 'administrator'
successfully logged in to Console server on host 'bu-
iddnwserver.iddlab.local'
```

**gstd Console: User '*username*' logged out of Console server on host '*hostname*'**

This message appears when a user closes the Console window and connection to the Console server.

For example:

```
14/08/2014 4:36:21 PM 0 gstd Console: User 'administrator'
logged out of Console server on host 'bu-
iddnwserver.iddlab.local'
```

## Modifying the security audit log resource

You can modify the audit security log resource on the audit log server. Changes that you make in the resource are automatically copied to each client in the datazone that supports audit logging.

**Before you begin**

Log in to the NMC server as a Console Security Administrator.

**Procedure**

1. Connect to the NetWorker server.
2. On the **Server** window, in the left pane, select **Security Audit log**.
3. Right-click the **Security Audit Log** resource, and then select **Properties**.

4. (Optional) Specify a hostname in the **auditlog hostname** attribute for the NetWorker client that runs the security audit log service, `nsrlogd`.
5. (Optional) In the **auditlog filepath** attribute, specify a valid path on the audit log server.

   This changes the location of the security audit log file. The default location is `/nsr/logs` on a UNIX Audit Log server and *`NetWorker_install_path`* `\nsr\logs` on a Windows Audit Log server.
6. (Optional) In the **auditlog maximum file size (MB)** attribute, change the maximum size of the security audit log.

   When the log file reaches the maximum size, NetWorker renames the security audit log file for archival purposes and creates a security audit log file.

   The default value for the **auditlog maximum file size (MB)** attribute is 2 MB.
7. (Optional) In the **auditlog maximum file version** attribute, change the maximum number of the audit log file versions that NetWorker maintains.

   When the log file version reaches the maximum number, NetWorker removes the oldest archived version of the security audit log file before creating the log file.

   The default value for the **auditlog maximum file version** attribute is 0, which means that NetWorker maintains all versions.
8. (Optional) In the security audit log in the **auditlog severity** attribute, change the audit message severity to increase or decrease the volume of messages that are saved.

   The following severity levels are available.

   **Table 28** Message types

| Type | Description |
|---|---|
| Informational | Information that may be useful, but does *not* require any specific action. |
| Warning | A temporary problem that NetWorker software may resolve or prompt you to resolve. |
| Notification | An event has occurred that generated a message. |
| Error | Errors that you are required to resolve. |
| Critical | Errors that you are required to resolve, to ensure successful NetWorker operations. |
| Severe | Errors that cause NetWorker services to become disabled or dysfunctional. |

   Changes to the attribute apply to each client that generates security related events. For example, if the security audit log severity attribute is Information, all clients send messages with the Information severity level. The Information and Notice level audit messages are very common. If the security audit log records too much or too little detail, then adjust the severity level accordingly.

   **Note:** This field also controls remote client security audit configuration. At the information, notice and warning levels, `nsrd` broadcasts the security configuration to all clients during startup. At other levels, when supported clients request the security configuration from the NetWorker server as

needed, the nsrd daemon does not broadcast security configuration during startup.

9. (Optional) use a third party logging service to send security audit log messages to by using the **auditlog rendered service** attribute.

   The following table describes the available options. Each option enables NetWorker to write unrendered security audit log messages to the `NetWorker_server_sec_audit.raw` file only. To render the log file in to a readable format, use the `nsr_render_log` program.

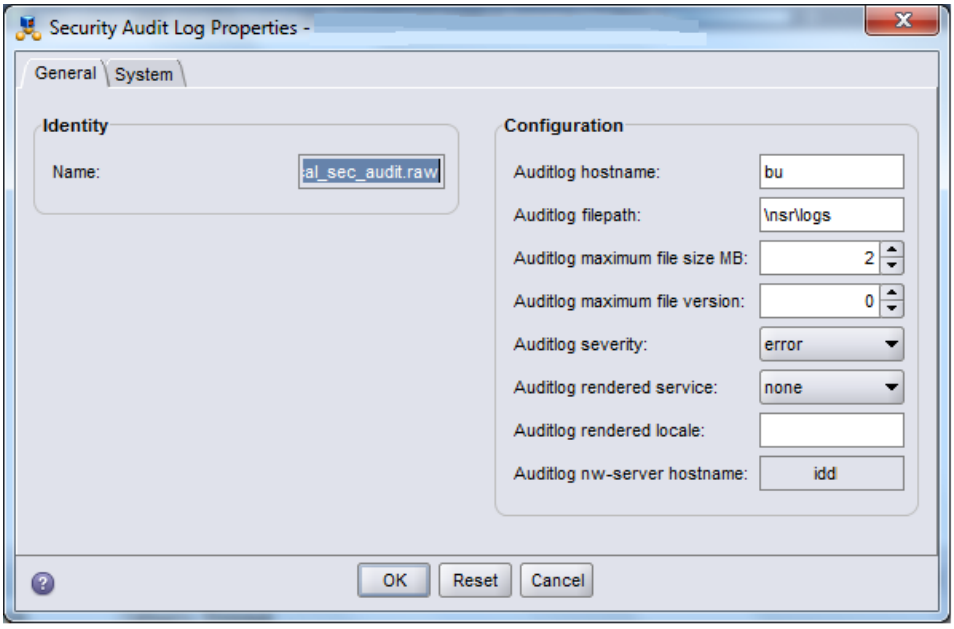
   **Table 29** Auditlog rendered service attributes

| Option | Description |
|---|---|
| None | The default value. |
| Local | Also writes rendered security audit log messages to the `NetWorker_server_sec_audit.raw` file. |
| syslog | Also writes rendered security audit log messages to the UNIX syslog. |
| eventlog | Also writes rendered security audit log messages to the Windows Event Log. |

10. (Optional) In the **auditlog rendered locale** attribute, specify the locale for the rendered audit log file. If this attribute is empty, the default locale en_US is used. The Multi-locale datazone considerations section in the *NetWorker Installation Guide* describes how to install and configure the NetWorker software on a machine that uses a non-English locale.

    The following figure provides an example of the **Security Audit Log Properties** resource.

    **Figure 21** Security Audit Log resource




11. Click **OK**.
12. To ensure that the configuration change completes successfully, review the **Monitoring** > **Log** > window.

For example:

- If the host specified in the auditlog hostname attribute supports security audit logging and the `nsrlogd` daemon is successfully started, a message similar to the following appears:

  ```
  The process nsrlogd was successfully configured on host
  'security_audit_log_hostname' for server
  'NetWorker_server'.
  ```

- If the host specified in the **auditlog hostname** attribute does not support security audit logging or the `nsrlogd` daemon does not start successfully, a message similar to the following appears:

  ```
  The security audit log daemon nsrlogd is probably not
  running. 'Unable to connect to the nsrexecd process on
  host 'client_name'. '355:Program not registered'.'.
  Ensure that the host 'client_name' can be reached. If
  required, restart the host.
  ```

- If a service port is not available on the host that is specified in the **auditlog hostname** attribute, the `nsrlogd` daemon fails to start and a message similar to the following appears:

  ```
  Process nsrlogd was spawned on
  'security_audit_log_hostname', but nsrlogd could not
  open an RPC channel. 'Unable to connect to the nsrlogd
  process on host 'security_audit_log_hostname'.
  '352:Remote system error'
  ```

- If the path specified in the **auditlog filepath** attribute does not exist, a message similar to the following appears:

  ```
  Unable to open the output file '/proc/
  NetWorker_server_sec_audit.raw' for the security audit
  log. No such file or directory
  ```

**Note:** Users that belong to the Security Administrators User Group, but not the Application Administrators User Group cannot see messages in the **Logs** window.

# CHAPTER 6

# Hardening the NetWorker

This chapter describes the configuration changes that are to be done to harden the NetWorker.


- Security Hardening For The NetWorker Management Console.....188
- Security Hardening For The NetWorker Authentication Tomcat Service..... 192
- Harden the Authentication Service on port 9090 .....194

# Security Hardening For The NetWorker Management Console

The NetWorker Management Console contains its own copy of the Apache httpd service. The hardening of the NMC httpd service will require the updating of the httpd.conf file.

The httpd.conf file contains the configuration settings for the service. The files are located in

- Windows: <EMC Networker Installation Directory> \Management\GST\apache \conf
- Linux: <EMC Networker Installation Directory>/opt/lgtonmc/apache/conf

## Enabling the Modules Required To Harden Apache httpd

To harden the Apache httpd service will require the enabling of a number of modules that are disabled by default. You must enable rewrite module, SSL module and mod_headers must be loaded to allow for setting header directives

**Procedure**

1. For the rewrite, SSL and mod_headers module, add the comment and then remove then enable the module by removing “#” from the existing httpd.conf file.

```
# NetWorker Apache Hardening - enable the rewrite module
LoadModule rewrite_module /opt/lgtonmc/apache/modules/
mod_rewrite.so
# NetWorker Apache Hardening - enable the SSL module
LoadModule ssl_module /opt/lgtonmc/apache/modules/mod_ssl.so
#NetWorker Hardening - mod_headers must be loaded to allow
for setting header directives
LoadModule headers_module /opt/lgtonmc/apache/modules/
mod_headers.so
```

## Enable Apache httpd directives

**Before you begin**

Open the `httpd.conf` file and perform the following steps:

**Procedure**

1. Locate "#gstconfig eNd" and above that line, add the following text.

```
# NetWorker Apache Hardening – Disable tracing
TraceEnable off
#Networker Hardening - Remove Apache Server Version Banner
ServerTokens Prod
ServerSignature Off
#NetWorker Hardening - Prevent cross-site scripting
Header set X-XSS-Protection "1; mode=block"
#NetWorker Hardening - prevent common cross-site scripting
attacks
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
#NetWorker Hardening - prevent click jacking
Header always append -X-Frame-Options SAMEORIGIN
```

```
#NetWorker Hardening - prevent MIME sniffing
Header set X-Content-type-Options nosniff

#NetWorker Hardening - HTTP Strict Transport Security
Header set Strict-Transport-Security "max
age=31536000;includeSubDomains;preload"

#NetWorker Hardening - Content Security Policy
Header always set Content-Security-Policy "frame-src 'self';"

#NetWorker Hardening - disable caching
Header always set Cache-Control "no-cache, no-store, must-
revalidate"
Header always set Pragma "no-cache"
#NetWorker Hardening - force server to make page requests
Header always set Expires "-1"
```

## Enabling HTTPS

To enable HTTPS, you can use either self signed or NetWorker generated certificates.

You can enable HTTPS by following one of the method:

1. Redirect HTTP to HTTPS port
2. HTTPS Redirect

### Redirect HTTP to HTTPS port

If you want to preserve http to port 9000, then Redirect HTTP to HTTPS port.

**Before you begin**

To enable HTTPS you will need to have the following three files for configuration:

1. Public key file used to generate the initial certificate.
2. Generated certificate file
3. Chain file that includes the server certificate file

**Procedure**

1. Open the `httpd.conf` file and locate for the line `# gstconfig bEgIn`
2. Choose a port number for which you want https to be supported.

   Uncomment the following lines (remove the #) and update the port number. Do not use the port 9001 or any the port that is in use.

   ```
   <IfDefine !SSL_PORT>
   Define SSL_PORT <choose a port number for which you want
   https to be on>
   </IfDefine>
   ```

   An example to enable SSL on port 9111.

   ```
   <IfDefine !SSL_PORT>
   Define SSL_PORT 9111
   </IfDefine>
   ```

3. Locate the line that defines the current listen port of 9000. Below the line, add `Listen ${SSL_PORT}`

```
Listen 9000
Listen ${SSL_PORT}
```

4. Locate the section that defines the VirtualHost for port 9000 and modify the section as shown below:

   This section enables HTTPS and creates a rewrite rule to redirect requests through port 9000 to the newly created HTTPS port. The section marked as <IP Address of the NMC Console Host> has to be updated with the IP address or name of the NMC host.

```
<VirtualHost *:9000>
ServerName localhost:9000
RewriteEngine On
Rewritecond %{HTTPS} !On
Rewriterule (.*) https://<IP Address of the NMC Console
Host>:${SSL_PORT}/%{REQUEST_URI}
</VirtualHost>
```

5. Locate the section that defines the VirtualHost of the newly created HTTPS port. Update the certificate settings for https, SSL protocol, and the ciphers to be used.

```
<VirtualHost *:${SSL_PORT}>
Servername localhost:${SSL_PORT}
SSLEngine on
SSLCertificateFile "/nsr/certs/<certificate file>"
SSLCertificateKeyFile "/nsr/certs/<public key>"
SSLCACertificateFile "/nsr/certs/”<chain file>"
SSLProtocol ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
SSLCipherSuite
HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4:!SSLv2:!SSLv3:!
TLSv1.0:!TLSv1.1:!ADH:!MEDIUM:!LOW:@STRENGTH
</VirtualHost>
```

## HTTPS Redirect

Use this method if you want to restrict all the requests on port 9000 to https

**Before you begin**

To enable HTTPS you will need to have the following three files for configuration:

1. Public key file used to generate the initial certificate.
2. Generated certificate file
3. Chain file that includes the server certificate file

**Procedure**

1. Open the `httpd.conf` file and locate for the line `# gstconfig bEgIn`
2. Locate the line that defines the current listen port of 9000. Below the line, add `Listen 9000 https`

```
Listen 9000
Listen 9000 https
```

3. Locate the section that defines the VirtualHost for port 9000 and comment the section by adding # as shown below:

```
#<VirtualHost *:9000>
#ServerName localhost:9000
#RewriteEngine On
#Rewritecond %{HTTPS} !On
#Rewriterule (.*) https://<IP Address of the NMC Console
Host>:${SSL_PORT}/%{REQUEST_URI}
#</VirtualHost>
```

4. Locate the section that defines the VirtualHost that contains the HTTPS enablement. Update the certificate settings for https, SSL protocol, and the ciphers to be used.

```
<VirtualHost *:9000>>
Servername localhost:9000
SSLEngine on
SSLCertificateFile "/nsr/certs/<certificate file>"
SSLCertificateKeyFile "/nsr/certs/<public key>"
SSLCACertificateFile "/nsr/certs/”<chain file>"
SSLProtocol ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
SSLCipherSuite
HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4:!SSLv2:!SSLv3:!
TLSv1.0:!TLSv1.1:!ADH:!MEDIUM:!LOW:@STRENGTH
</VirtualHost>
```

## Configuring gconsole file to Enable HTTPS

You must configure the gconsole file to ensure that `gconsole.jnlp` landing page is properly serviced through the HTTPS SSL PORT.

**Procedure**

1. Open the `gconsole.jnlp` file.
   - Windows : <EMC Networker Installation Directory>\Management\GST\web
   - Linux : <EMC Networker Installation Directory >/opt/lgtonmc/web
2. Modify the codebase attribute by changing http to https and replacing the http port with the port number

   For example, `codebase= http://IPADDR_REPLACE_AT_RUNTIME(<IP of server>):9000/` should be changed to `https://IPADDR_REPLACE_AT_RUNTIME(<IP of server>):<SSL_PORT>/`
3. Restart the GST services.

## Replacing Default Tomcat Web Pages

The NetWorker Authentication Tomcat service ships with default Tomcat web pages. There are some security scanners that will generate a security advisory due to these pages when the service is scanned. You can update the service to provide new webpage.

**Procedure**

1. Open the `web.xml` file using a text editor.

   The location of the file:

- Windows: C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat \conf
- Linux: /nsr/authc/conf

2. Locate the line </web-app> and add the following above that line.

```
<error-page>
<error-code>404</error-code>
<location>/error.jsp</location>
</error-page>
<error-page>
<error-code>500</error-code>
<location>/error.jsp</location>
</error-page>
<error-page>
<error-code>400</error-code>
<location>/error.jsp</location>
</error-page>
```

3. Add a new file with the name `error.jsp` in the webapps directory of the distribution.

   The location of the file:

   - Windows: C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat \webapps
   - Linux: /nsr/authc/webapps

4. Using an editor, edit the error.jsp file and add the following content

```
<html>
<head>
<title>NSR Authentication Services Error</title>
</head>
<body> Page Not Found! </body>
</html>
```

# Security Hardening For The NetWorker Authentication Tomcat Service

The NetWorker Authentication Service is a web-based application that runs within an Apache Tomcat instance.

The hardening of the Apache Tomcat service on port 9090 and 11000 involves hardening of NSR tomcat services, TLS protocols, ciphers and connected ports.

## Hardening the NSR Tomcat Services

Perform the following steps to harden the NetWorker Authentication Service used for Authentication, REST API, and FLR UI services.

**Procedure**

1. On the NetWorker server, stop the NetWorker services and open the server.xml file using a text editor.

   The location of the file differs on Windows and Linux

- Windows: C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat \conf
- Linux: /nsr/authc/conf

2. Search for the string Connector port of 9090 and add the following lines in the Connect port setting

```
Server ="NSR SERVICES for <insert customer name> "
SSLEnabled="true"
maxThreads="150"
scheme="https"
secure="true"
xpoweredBy="false"
allowTrace="false"
deployXML="false"
```

An example of the definition of port 9090

```
<Connector port="9090"
protocol="org.apache.coyote.http11.Http11NioProtocol"
Server =" "
SSLEnabled="true"
maxThreads="150"
scheme="https"
secure="true"
xpoweredBy="false"
allowTrace="false"
deployXML="false"
keystoreFile="keystore file" keystorePass="keystore passwd"
keyAlias="emcauthctomcat" keyPass="${tckey.password}"
clientAuth="false"
sslProtocol="TLS"
```

## Hardening TLS Protocol

The hardening of TLS can be done by editing the sslEnabledProtocols and remove the TLS settings that are not needed.

**About this task**

By default the following is set to sslEnabledProtocols="TLSv1.2, TLSv1.1, TLSv1"

**Procedure**

1. To disable TLS 1.0 and TLS 1.1, update to indicate:

   ```
   sslEnabledProtocols="TLSv1.2"
   ```

## Hardening Supported Ciphers

The hardening is done by editing the ciphers setting and removing the cipher that are not needed.

**About this task**

By default the following is set to

```
ciphers="TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SH
A256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC
```

```
_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM
_SHA384,
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384"/>
```

**Procedure**

1. Remove the ciphers that are not required.

## Hardening the NSR Tomcat Shutdown Port

Disable the tomcat shutdown port by setting the shutdown port value to "-1" in the server.xml file . This prevents malicious actors from shutting down Tomcat's web services.

If the port cannot be disabled then set a strong password for shutdown. You can still shutdown tomcat directly on the server itself with the "-1" entry but not remotely through a utility like telnet. Search for “Server port=8005”, you can choose to disable the port, or provide a secure password.

### Disable port

```
<Server port="-1" shutdown="SHUTDOWN">
```

### Strong Password

```
<Server port="8005" shutdown="5hu!dOwN!\">
```

### Hardening the NSR Tomcat Connectors

By default Tomcat publishes two connector types, HTTP AJP non-SSL/TLS HTTP/1.1 8080 and AJP xx Connector 8009. In most configurations Tomcat request/responses will go over HTTP/HTTPS. The AJP connector is generally used for parsing requests through reverse proxies, although still slightly more efficient than HTTP over reverse proxies.

It is often not needed and should be disabled in the server.xml file. Search for Connect port=8009, change `<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />` to `<!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->`

# Harden the Authentication Service on port 9090

Perform the following steps to harden the Authentication Service on port 9090:

**Procedure**

1. On the NetWorker server, stop the NetWorker services.
2. Edit the `server.xml` file with a text editor.

   The location of the file differs on Windows and Linux:

   - Windows: `C:\Program Files\EMC NetWorker\nsr\authc-server\tomcat\conf`
   - Linux: `/nsr/authc/conf`

3. Search for the string `Connector port = 9090`.

```
<Connector port="9090"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="/nsr/authc/conf/authc.keystore " keystorePass="$
{keystore.password}"
keyAlias="emcauthctomcat" keyPass="${tckey.password}"
clientAuth="false" sslProtocol="TLS"
sslEnabledProtocols="TLSv1.2, TLSv1.1, TLSv1"
ciphers="TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_GCM_SHA384" />
```

4. Remove the specific TLS versions and ciphers.
   - Hardening TLS Protocol- Your organization may require that certain TLS protocols are disabled and not used. This hardening can be done by editing the **sslEnabledProtocols** and removing the TLS settings that are not needed. The following is set by default:

     ```
     sslEnabledProtocols="TLSv1.2, TLSv1.1, TLSv1"
     ```

     To disable TLS 1.0 and TLS 1.1, update to indicate the following:

     ```
     sslEnabledProtocols="TLSv1.2"
     ```

   - Hardening Supported Ciphers- Your organization may require that certain ciphers are disabled and not used. This hardening can be done by editing the ciphers setting and removing the cipher settings that are not needed. The following is set by default:

     ```
     ciphers="TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
     TLS_RSA_WITH_AES_128_CBC_SHA,
     TLS_RSA_WITH_AES_128_CBC_SHA256,
     TLS_RSA_WITH_AES_128_GCM_SHA256,
     TLS_RSA_WITH_AES_256_CBC_SHA,
     TLS_RSA_WITH_AES_256_CBC_SHA256,
     TLS_RSA_WITH_AES_256_GCM_SHA384"
     />
     ```

5. Save the `server.xml` file.
6. On the NetWorker server, start the NetWorker services.