



EMC[®] NetWorker[®]

Release 7.5

Security Configuration Guide

P/N 300-008-475

Rev A01

December 8, 2008

This guide contains information on security configurations for EMC[®] NetWorker[®] release 7.5. Topics include:

- ◆ [Access control settings](#) 2
- ◆ [Log settings](#) 4
- ◆ [Communication security settings](#) 6

Access control settings

Access control settings provide protection of resources against unauthorized access.

User authentication

User authentication settings control the process of verifying an identity claimed by a user for accessing the product.

Default accounts

[Table 1 on page 2](#) describes the default login accounts.

Table 1

Login accounts

User account	Description
root@localhost - for NetWorker server on UNIX platforms system@localhost - Windows platforms	User 'root' on the NetWorker server host is automatically added to the Administrator list.
@	All users at all hosts are added to the 'users' attribute of an instance of the 'NSR Usergroup' resource. All privileges associated with that 'NSR Usergroup' instance go to 'all users @ all hosts' with no explicit denial of access.
administrator	Default NMC user. First login procedure forces password change.

Authentication configuration

The NMC Console has two modes of operation: native mode and LDAP mode. By default, NMC user authentication is set to native mode. You can set up user authentication in LDAP mode by using the Configure Login Authentication wizard. You can also revert back to native NetWorker user authentication by using the wizard. *EMC NetWorker Release 7.5 Administration Guide* provides more information about NMC console login authentication.

User authorization

User authorization settings control the privileges that are granted to a user to access a resource managed by the product.

EMC NetWorker Release 7.5 Administration Guide provides more information to set up users and to control user permissions for the Console server.

EMC NetWorker Release 7.5 Administration Guide provides more information to set up users and user groups and to control user permissions for the Console server.

Component access control

Component access control settings define the control over access to the product by external and internal systems or components.

Component authentication

NetWorker hosts and daemons are authenticated by using the **nsrauth** mechanism, which is available for hosts that run NetWorker release 7.3 or later. The NetWorker **nsrauth** authentication mechanism is a strong authentication and is based on the Secure Sockets Layer (SSL) protocol provided by the OpenSSL library or RSA BSAFE SSL, depending on the platform.

Each NetWorker host has a **nsrexecd** service, which provides authentication services. Each **nsrexecd** service has its own private key and self-signed certificate for authentication. The private key is generated by **nsrexecd** when it starts. The private key can also be loaded from a file. The corresponding self-signed certificate is generated by the private key. The private key is RSA and is 1024 bits in length. The encryption method that is used once an SSL session is set up is AES-128. The session information sent over the SSL connection includes:

- ◆ Session keys
- ◆ Session ID
- ◆ User's information
- ◆ User's NetWorker permissions

EMC NetWorker Release 7.5 Administration Guide provides information about configuring **nsrauth** authentication.

Component authorization

NetWorker uses the contents of the `/nsr/res/servers` file for UNIX or the `NetWorker_install_path\res\servers` file for Windows, on each NetWorker client to control the client-tasking rights.

The client-tasking rights are the rights to request the execution of a program on another client and may be any of the following:

- Server that performs an archive request
- Scheduled backup
- Another client that requests a directed recover

If the server file is empty, then any NetWorker host can have tasking rights.

- ◆ Add the names of the additional NetWorker servers to the server file so that the client with the tasking rights can back up to other NetWorker servers.
- ◆ Add the client names to the servers file so that other clients can perform directed recovers to the client with the tasking rights.

You can add the names of NetWorker servers to the server file during a NetWorker software installation. To add additional hosts later, use a text editor and add the hostnames to the server file.

After adding the additional hosts in the server file, restart the nsrexecd on that client for effect on the additional server hosts.

Log settings

A log is a chronological record for system activities that helps to examine the sequence activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

Log files and their descriptions

[Table 2 on page 4](#) shows the log files path.

Table 2

Log files

Component	Location
Server and client daemons	/nsr/logs/daemon.raw
Server-generated syslog messages and daemon.notice	/nsr/logs/messages
Server-generated syslog messages local0.notice and local0.alert	/nsr/logs/summary
NMC gstd logs	<install path>/logs/gstd.raw
NMC Web Server logs	<install path>/logs/web_output
NMC DB logs	<install path>/logs/db_output

Log management and retrieval

This section explains how to view and manage logs.

Viewing log files

For NetWorker release 7.4 and later, the following log files can be viewed by using the non-interactive command line program, `nsr_render_log` (for UNIX and Linux) or `nsr_render_log.exe` (for Microsoft Windows):

- ◆ Daemon log file: `daemon.raw`
- ◆ `gstd` log file: `gstd.raw`
- ◆ NetWorker user log file: `networkr.raw` (for Microsoft Windows only)

EMC NetWorker Release 7.5 Administration Guide provides information about using the `nsr_render_log` program including, filtering output, viewing logs remotely, and rendering logs to the current locale.

Managing log files

The Console server `gstd` log file can be managed with the following environment variables:

- ◆ **GST_MAXLOGSIZE**
Sets the maximum size of the `gstd` log file before a new log file is created at Console server startup time.
- ◆ **GST_MAXLOGVERS**
Sets the maximum number of historical versions of the `gstd` log file that Console retains.
- ◆ **GST_DEBUG**
Sets the level of debugging information written to the `gstd` log file.

EMC NetWorker Release 7.5 Administration Guide provides information to edit Console server environment variables.

The NetWorker server `daemon.raw` log file can be managed with the following environment variables:

- ◆ **NSR_MAXLOGSIZE**
Sets the maximum size of the daemon log file before a new log file is created at NetWorker server startup time.
- ◆ **NSR_MAXLOGVERS**

Sets the maximum number of historical versions of the daemon log file that the NetWorker server retains.

EMC NetWorker Release 7.5 Administration Guide provides information to edit NetWorker server environment variables.

Communication security settings

Communication security settings enable the establishment of secure communication channels between:

- ◆ product components
- ◆ product components and external systems or components.

Port usage

[Table 3 on page 6](#) lists all components, protocols, ports, and services.

Table 3 Port usage

Component	Service	Protocol	Port	Description
Service Port Range		TCP	7937 - 9936	This is the default range of ports that all NetWorker daemons should use when they need to start a service. This range can be configured. Since the daemons may start in any order, there is no guarantee that any one daemon will always use any singular port from this range.
nsrd	RPC	TCP		1 from SPR
nsrindexd	RPC	TCP		1 from SPR
nsrmmdbd	RPC	TCP		1 from SPR
nsrmmgd	RPC	TCP		1 from SPR
nsrjobd	RPC	TCP		1 from SPR
nsrexecd	RPC	TCP	7937, 7938	Plus 2 from SPR. Regardless of SPR, nsrexecd always listens to these two ports. 7938 must be allowed through a firewall, either by NetWorker or another portmapping service, or NetWorker will not work.
nsrlcpd	RPC	TCP		Per instance running.

Table 3 Port usage

Component	Service	Protocol	Port	Description
nsrcmd	RPC	TCP		1 from SPR, per instance running.
NMC Web Server	HTTP	TCP	9000*	Jumpstart to launch NMC
NMC	GSTD	TCP	9001*	Communicates between Java client and main daemon.
NMC SQLAnywhere DB	DB		2638*	Database listening port

Encrypting backup data

Backup and archive data on UNIX and Windows hosts can be encrypted with the AES Application Specific Module (ASM). The AES ASM provides 256-bit data encryption. Backup data is encrypted based on a user-defined pass phrase.

Do not use AES encryption when backing up files that are encrypted using the Microsoft Windows Encrypting File System (EFS).

EMC NetWorker Release 7.5 Administration Guide provides more information.

Copyright © 2008 EMC Corporation. All rights reserved.

EMC 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." EMC CORPORATION 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 EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.