NetWitness® Platform XDR

NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.4 Migration Guide

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA 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." RSA 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.

July, 2022

Contents

Introduction

This guide provides instructions on how to migrate an existing NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.3 and later.

The migration broadly involves:

- Planning and setting up NetWitness Platform. Contact your account manager for sizing the deployment. For more information on sizing guidelines, see the *Virtual Host Installation Guide*.
- Importing file status, certificate status, and blocked hashes from NetWitness Endpoint 4.4.0.x to NetWitness 11.3 and later.

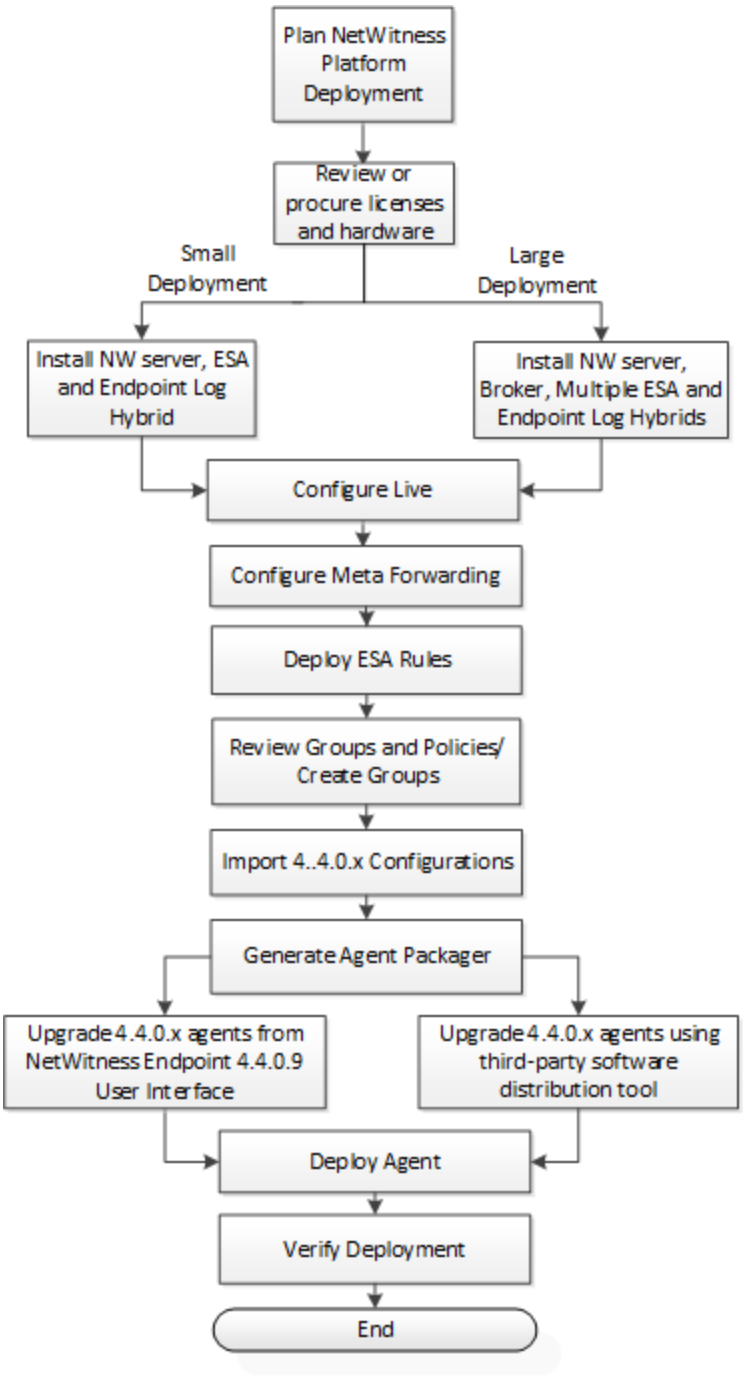
  Note: Endpoint scan and tracking data in the SQL database, users, IIOCs, custom queries, bad certificates, bad domains, bad IPs, and bad file hashes in NetWitness Endpoint 4.4.0.x cannot be migrated.

- Upgrading 4.4.0.x agents to 11.3 and later.

For more information on the new features of NetWitness Endpoint, see the *Release Notes*.

Migration Flowchart

The following flowchart illustrates the migration process:



Note: The instructions for each step is provided in the sections below.

How to Find the List of Documents

If you want to view the NetWitness Platform product documentation, use the following link:
https://community.rsa.com/t5/rsa-netwitness-platform/ct-p/netwitness-documentation/version/11.3

Migrating NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.3 and Later

This topic describes tasks required to migrate NetWitness Endpoint 4.4.0.x to NetWitness 11.3 and later.

Task 1 - Plan your NetWitness Deployment

1. Review the Endpoint architecture and choose one of the following deployments based on number, distribution, and location of endpoints, and data collected from the agents. For more information, see the "NetWitness Endpoint Architecture" topic in the *Deployment Guide*.
   - Small deployment includes NetWitness Server, an Endpoint Log Hybrid, and Event Stream Analysis (ESA).
   - Large deployment includes NetWitness Server, one or more Endpoint Log Hybrids, one or more ESA.

     If you have multiple Endpoint Log Hybrids, install an Endpoint Broker. Once installed, it automatically queries all Endpoint servers in your deployment and provides a consolidated view of all Endpoint servers.

     Note: RSA recommends that you install the Endpoint Broker on the NetWitness Broker host. It is also supported on a separate host, NetWitness Server, and on an Endpoint Log Hybrid.
2. Review existing licenses and hardware, and procure them as required.

   Make sure you have the required hardware for your deployment. For more information, see the "Supported Hardware" topic in the *Physical Host Installation Guide*.

   If you have existing NetWitness Endpoint 4.4.0.x licenses, you do not need to procure a new license. Your existing NetWitness Endpoint 4.4.0.x licenses will be available on myRSA as a NetWitness 11.3 and later license, with a different serial/license number.

   For more information, see the *Licensing Management Guide*.

Task 2 - Set up NetWitness Platform 11.3 and Later

1. Configure the ports on your firewall. For more information, see the "Network Architecture and Ports" topic in the *Deployment Guide*.
2. Install the following NetWitness components:
   - NetWitness Server
   - Endpoint Log Hybrid
   - ESA
   - Endpoint Broker (for more than one Endpoint Log Hybrids)

   For more information, see the *Physical Host Installation Guide*.

3. If you have NetWitness Endpoint 4.4.0.x licenses:
   - With NetWitness - Map your entitlements to the existing license server.
   - Without NetWitness:

     a. Install NetWitness (see Task 2 - Set up NetWitness Platform 11.3 and Later)

     b. Obtain License Server ID

     c. Map entitlements
4. Verify if licenses are reflected on **ADMIN > System > Licenses**.

Task 3 - Configure NetWitness Platform for Endpoints

- Configure your RSA Live account and make sure the File Reputation service is enabled. For more information, see the *Live Services Management Guide*.
- Create users and assign appropriate roles. For more information, see the *System Security and User Management Guide*.
- Configure Endpoint Meta forwarding on Endpoint Log Hybrid. For more information, see the *NetWitness Endpoint Configuration Guide*.
- Deploy ESA rules.

  The existing NetWitness Endpoint 4.4.0.x IIOCs are available as out-of-the-box Application rules and automatically available on installation.

  You must configure the ESA Correlation server with an Endpoint Concentrator and deploy the ESA content for risk score calculation. For more information, see the *ESA Configuration Guide*.
- Review the default Agent Endpoint (EDR) policy and create groups as required. If you want to enable agents for log collection, review and apply the Windows Log policy.

  For more information, see the *NetWitness Endpoint Configuration Guide*.

Task 4 - Import NetWitness Endpoint 4.4.0.x Configurations

Import file status, certificate status, and blocked hashes from NetWitness Endpoint 4.4.0.x to NetWitness Platform. For more information, see Importing NetWitness Endpoint 4.4.0.x Configurations to NetWitness Platform.

Task 5 - Set up Other NetWitness Endpoint 4.4.0.x Configurations

You have to manually set up the following configurations:

- Deploy Blacklisted IP addresses and other feeds that are relevant for your deployment from RSA Live through the NetWitness user interface.

- (Optional) For any other external threat feeds, such as blacklisted IP address, domain, and checksum, that you may want to use to tag endpoint metadata, see the "Create a Custom Feed" topic in the *Live Services Management Guide*.

  For example, to notify an analyst about any communication from a host or file to a certain blacklisted IP address, domain, or hash, create a feed on the Log Decoder, and tag appropriate sessions for investigation and alerting .

- (Optional) Review custom IIOCs and write Endpoint rule. For more information, see the "Custom Endpoint Rule for Risk Scoring" topic in the *NetWitness Endpoint Configuration Guide*.

Task 6 - Deploy Agents

1. Generate an agent packager from NetWitness 11.3 and later.
2. Copy the agent packager (`AgentPackager.zip`) to a Windows machine and generate the 11.3 and later agent installers.
3. Do one of the following to upgrade 4.4.0.x agents to 11.3 and later:
   - If you have NetWitness Endpoint 4.4.0.9 Console Server, copy the agent installers to the NetWitness Endpoint Console Server, and upgrade from the NetWitness Endpoint user interface.
   - If you have 4.4.0.0 or 4.4.0.8, copy the agent installers, and use the third-party software distribution tool.
4. Deploy the agents.

For more information, see the *NetWitness Endpoint Agent Installation Guide*.

Task 7 - Verify the Agent Migration

After the agent migration, verify the following:

- Agents are able to communicate with the Endpoint Server and are listed in the Investigate > Hosts view.
- Perform a scan and make sure that the snapshot details are displayed in the Investigate > Host Details view.
- Hosts metadata is available in Investigate > Navigate and Events view.

  If the Windows Log collection is enabled, make sure that the Windows logs are available in the Navigate and Events view.

- File reputation, file status, risk scores are available in Hosts and Files view.

For detailed information, see the *NetWitness Endpoint Configuration Guide*.

Importing NetWitness Endpoint 4.4.0.x Configurations to NetWitness Platform

You can import file status, certificate status, and blocked hashes from NetWitness Endpoint 4.4.0.x to NetWitness using the MigrationHelper python script.

Note: The MigrationHelper python script must be run only on a Windows host.

You can download the script from RSA Link:

RSA NetWitness > **Downloads** > **RSA NetWitness Platform** > **Version 11.3** > **Tools**.

Prerequisites

To run the python script:

- Install Python 3.6.x or later on a Windows host that can connect to the NetWitness Endpoint 4.4.0.x primary database.
- Install pyodbc by downloading the wheel file from https://pypi.org/project/pyodbc/#files, and run the following command:

  ```
  pip install wheel-file.whl
  ```

- If json and os.path libraries are not available on Python installation, install these libraries by downloading the corresponding wheel file from https://pypi.org/, and run the following command:

  ```
  pip install wheel-file.whl
  ```

Import File and Certificate Status

Note: If the certificate status is graylisted in NetWitness Endpoint, this status is not exported as graylist is not supported for certificates in NetWitness Platform 11.3 and later.

1. Run the `MigrationHelper` python script.

   Note: Run this script from any host that has access to NetWitness Endpoint primary database.

2. Enter the following:
   a. Database server host name or IP address (for example, 10.40.40.10)
   b. Database name (for example, ECATPrimary)
   c. Database credentials
3. Enter the path to store the exported files and press **Enter**. Make sure that the path exist. The file and certificate status are exported to JSON files.
4. Log in to the Context Hub server and copy the exported file to the `/var/netwitness/contexthub-server/data/` directory.
5. On the NW server, run the `nw-shell` command from the command line.

Note: Make sure all Endpoint servers on NetWitness 11.3 and later are online while importing data.

6. Run the `login` command and enter the credentials.
7. Connect to the Context Hub server using the following command:

   ```
   connect --service contexthub-server
   ```

8. Run the following commands to import the file status:

   ```
   cd contexthub/file/status/import
   show
   invoke <file path>/FileStatus.json
   ```

   Note: `<file path>` is the path in the Context Hub server where the file is saved. The Context Hub server is located in the ESA primary host.

9. Run the following commands to import the certificate status:

   ```
   cd contexthub/certificate/status/import
   show
   invoke <file path>/CertificateStatus.json
   ```

   Note: `<file path>` is the path in the Context Hub server where the file is saved. The Context Hub server is located in the ESA primary host.

10. Check the progress of the import in the `/var/log/netwitness/contexthub-server/contexthub-server.log` file.

    Once the import is complete, a message `Imported File status successfully` or `Imported Certificate status successfully` is displayed in the log file.

If you want to unblock the imported 4.4.0.x blocked files:

1. On the NW server, run the `nw-shell` command from the command line.
2. Run the `login` command and enter the credentials.
3. Connect to the Context Hub server using the following command:

   ```
   connect --service contexthub-server
   ```

4. Run the following commands to unblock the file status:

   ```
   cd contexthub/file/status/unblock
   invoke <checksum of blocked file>
   ```