NetWitness® Platform

Version 12.5.1

Windows Legacy Collection

NETWITNESS

Platform

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.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November, 2024

Contents

NetWitness Legacy Windows Collection Update and Installation Instructions

NetWitness Legacy Windows collection collects event data from multiple Windows Event Source domains.

It supports collection from:

- Windows 2003 and earlier event sources
- NetApp ONTAP host evt files

IMPORTANT: This document is applicable only for upgrades to versions 12.5.1 and above. For versions 12.5 and below, please refer to the Windows Legacy Collection guide for 12.5.

This document contains the following sections:

Setup Requirements

This section provides the NetWitness Legacy Windows Collector Setup requirements.

To set up the NetWitness ® Platform Legacy Windows Collector, you need:

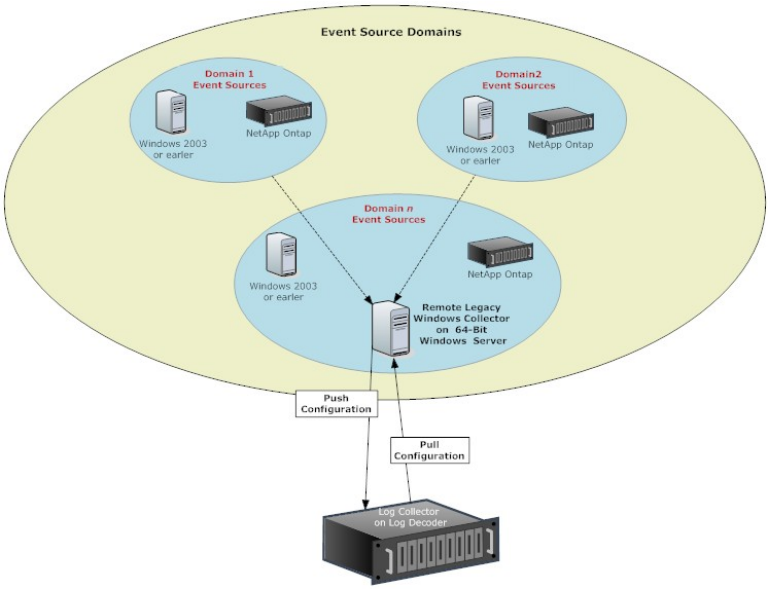
- Any of the following physical or virtual systems that can access the desired event source domains for collection:

Note: Windows Server 2012 has reached its end-of-life and is no longer supported by Microsoft. We strongly recommend upgrading to a later version to avoid potential performance issues and ensure continued security and support.

- Windows 2012 Server, or
- Windows 2016 Server, or
- Windows 2019 Server, or
- Windows 2022 server

- A minimum of 20% free disk space. For example, you need at least 20 GB of free space if your system drive is 100 GB in size.

IMPORTANT: Do not install the Legacy Windows Collector on a domain controller.



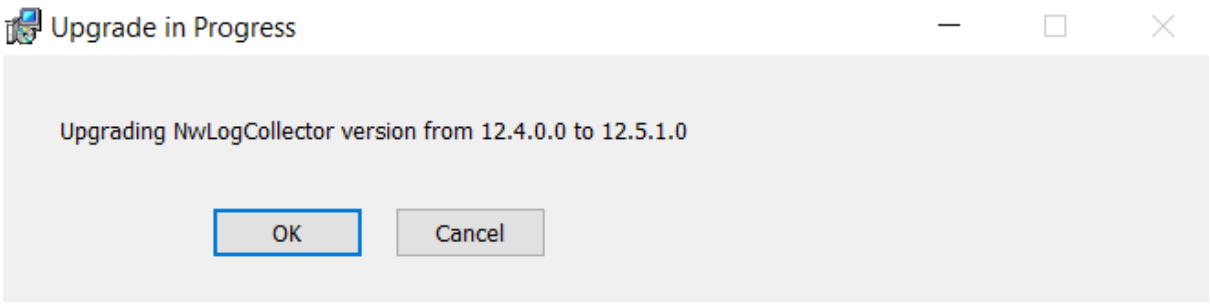
Update the NetWitness Legacy Windows Collector to 12.5.x

To update the NetWitness Legacy Windows Collector to 12.5.x on a Windows 64-Bit server:

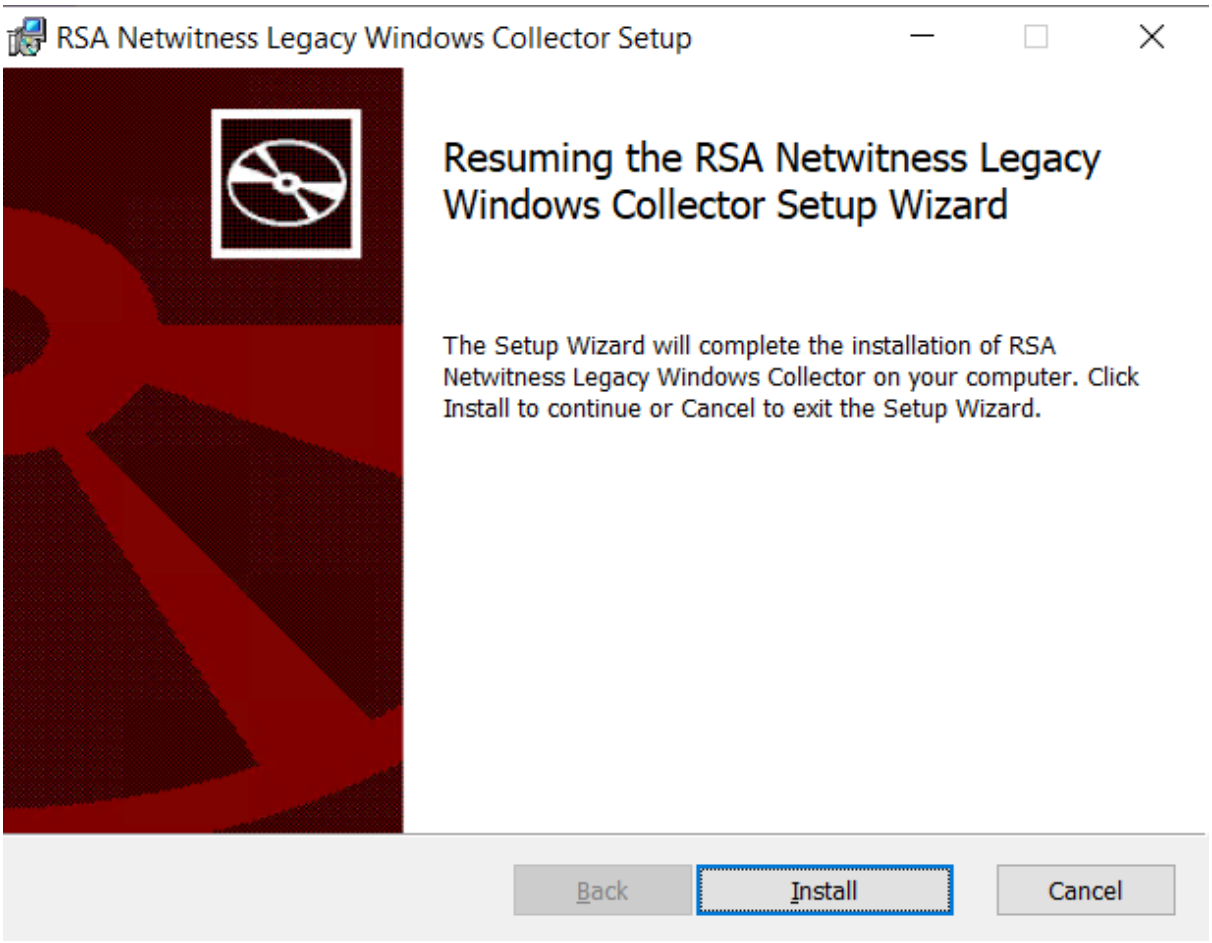
Note: These instructions are applicable only for upgrades to versions 12.5.1 and above.

1. Navigate to NetWitness Platform 12.5.1 Upgrade Guide and click **NetWitness Platform 12.5.1 Legacy Windows Collector** to download the ZIP archive.
2. Unzip the downloaded file.
3. Log on to a Windows 2012, 2016, 2019 or 2022 Server.
4. Copy **NWLegacyWindowsCollector-*version-number*.exe** to the Windows Server.
5. Right click on **NWLegacyWindowsCollector-*version-number*.exe** and select **Run As Administrator**.

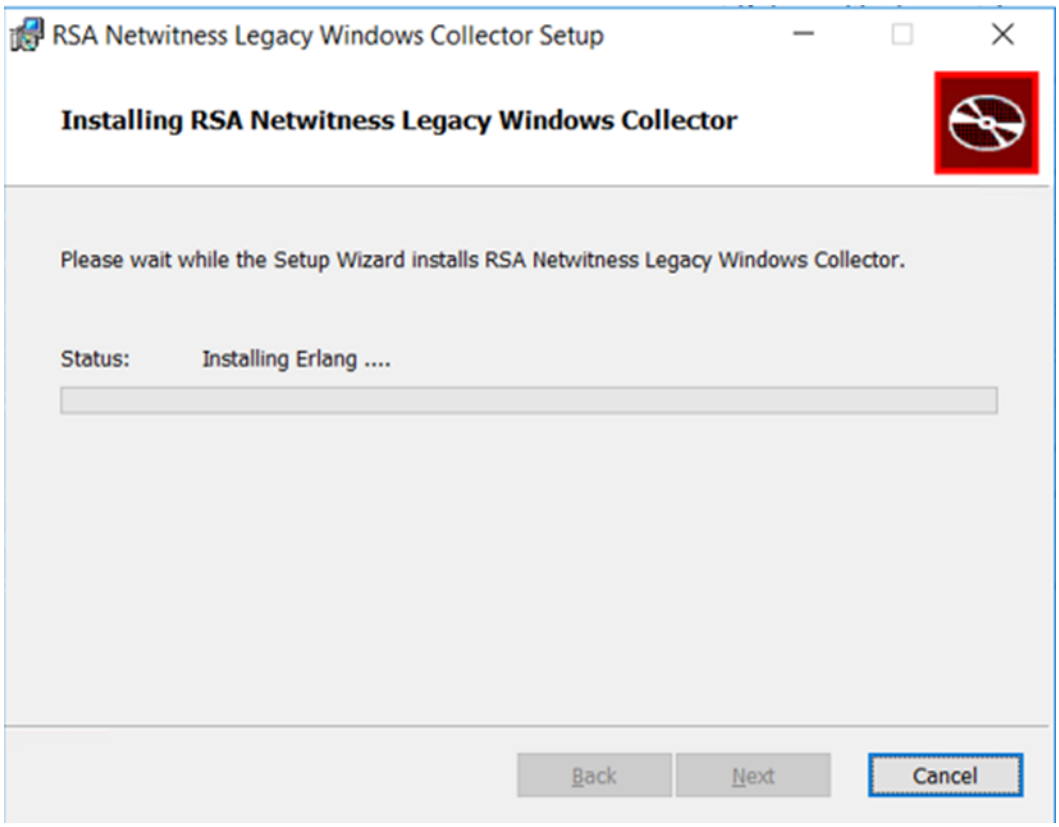
   Before it starts the update, the wizard asks if you want to continue or cancel the installation of the update.

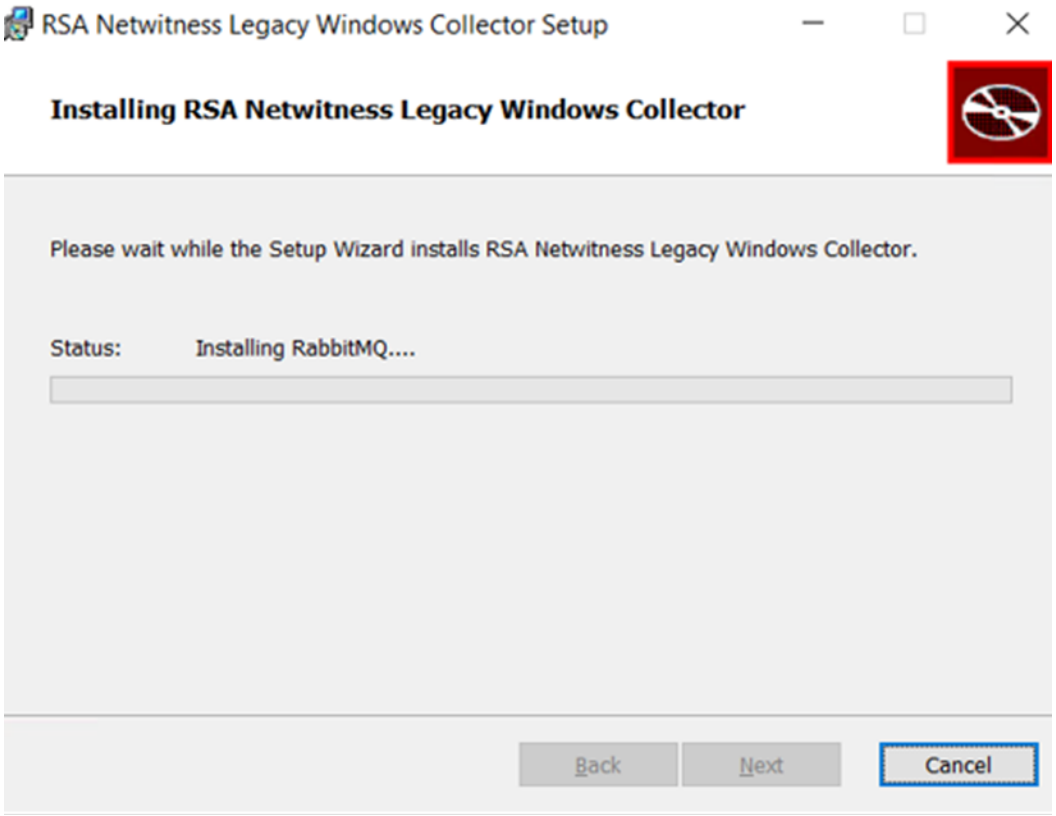


6. Click **OK** to continue installing the update.
7. Click **Install**.



The Installation screens for the Legacy Windows Collector page is displayed.

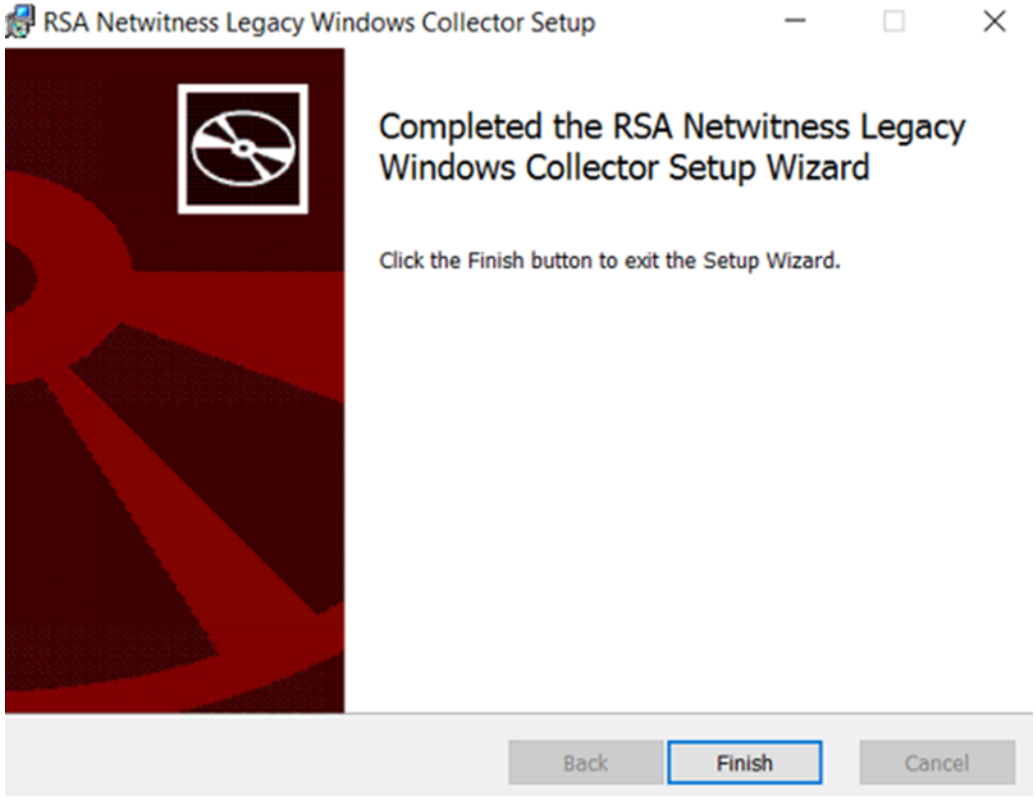

RSA Netwitness Legacy Windows Collector Setup
Installing RSA Netwitness Legacy Windows Collector
Please wait while the Setup Wizard installs RSA Netwitness Legacy Windows Collector.
Status: Installing Erlang ....
Back
Next
Cancel


RSA Netwitness Legacy Windows Collector Setup
Installing RSA Netwitness Legacy Windows Collector
Please wait while the Setup Wizard installs RSA Netwitness Legacy Windows Collector.
Status: Installing RabbitMQ....
Back
Next
Cancel

After the update installation completes, the **Next** button becomes active.

8. Click **Next**.

   The Installation Completed page is displayed.



9. Click **Finish**.
10. Add or reconfigure the Windows Legacy Collector Host and Service in NetWitness Platform. *For details on adding or reconfiguring Windows Legacy Collector Host and Service in Netwitness Platform, refer* *Add or Reconfigure a Windows Legacy Collector Host and Service in NetWitness Platform*.
11. Reboot the machine.

This completes the update of the NetWitness Legacy Windows Collector to 12.5.x.

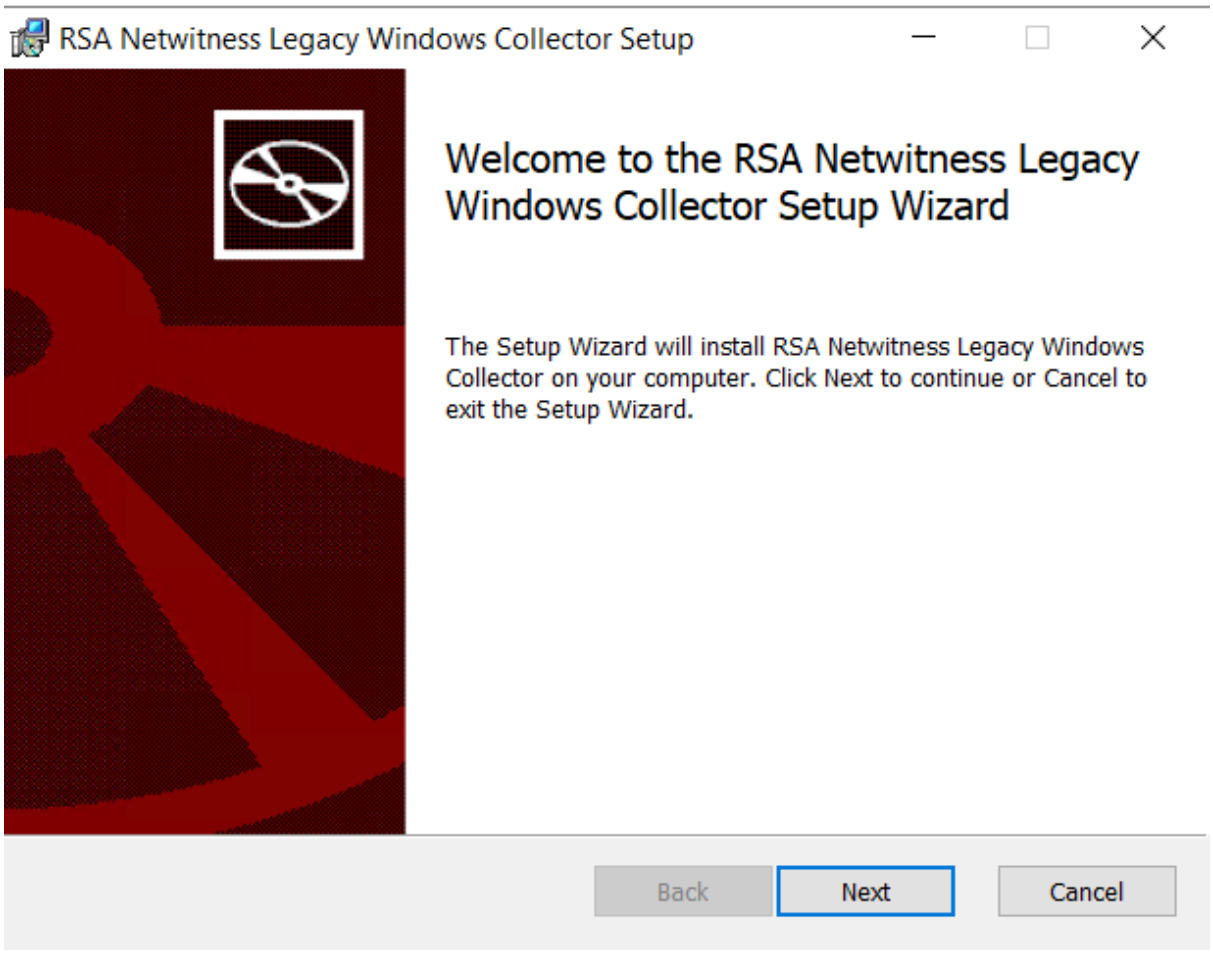
Fresh Install 12.5.x Legacy Windows Collector

This section describes how to install the 12.5.x Legacy Windows Collector on a Windows 2012, 2016, 2019 or 2022 64-Bit server

Note: These instructions apply only for NetWitness Platform versions 12.5.1 and above.

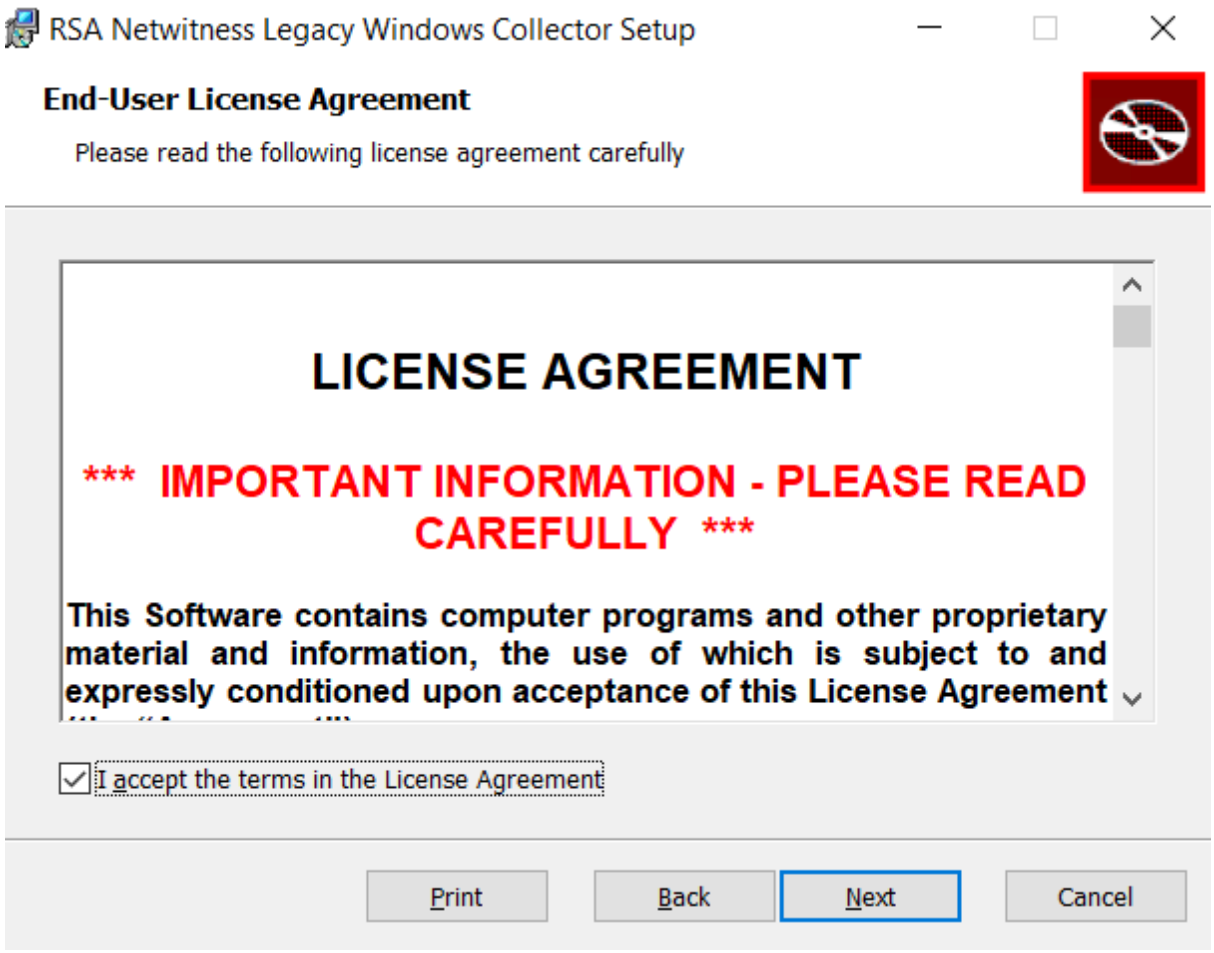
1. Navigate to NetWitness Platform 12.5.1 Upgrade Guide and click **NetWitness Platform 12.5.1 Legacy Windows Collector** to download the ZIP archive.
2. Unzip the downloaded file.
3. Copy the **NWLegacyWindowsCollector-*version-number*.exe** to the Windows Server.
4. Right click on the **NWLegacyWindowsCollector-*version-number*.exe** and select **Run As Administrator**.

   The **Welcome** page of installation wizard is displayed.



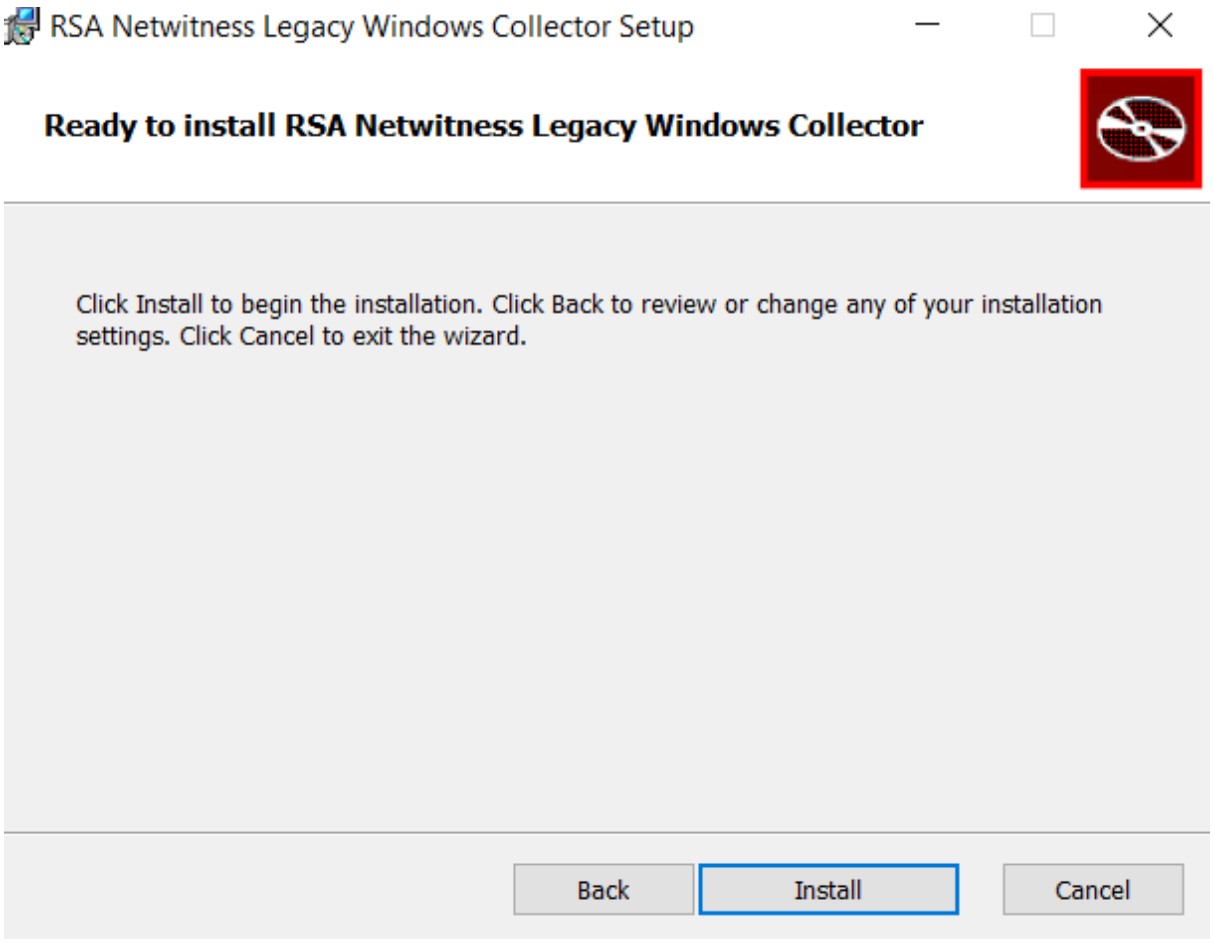
5. Click **Next**.

   The License Agreement page is displayed.



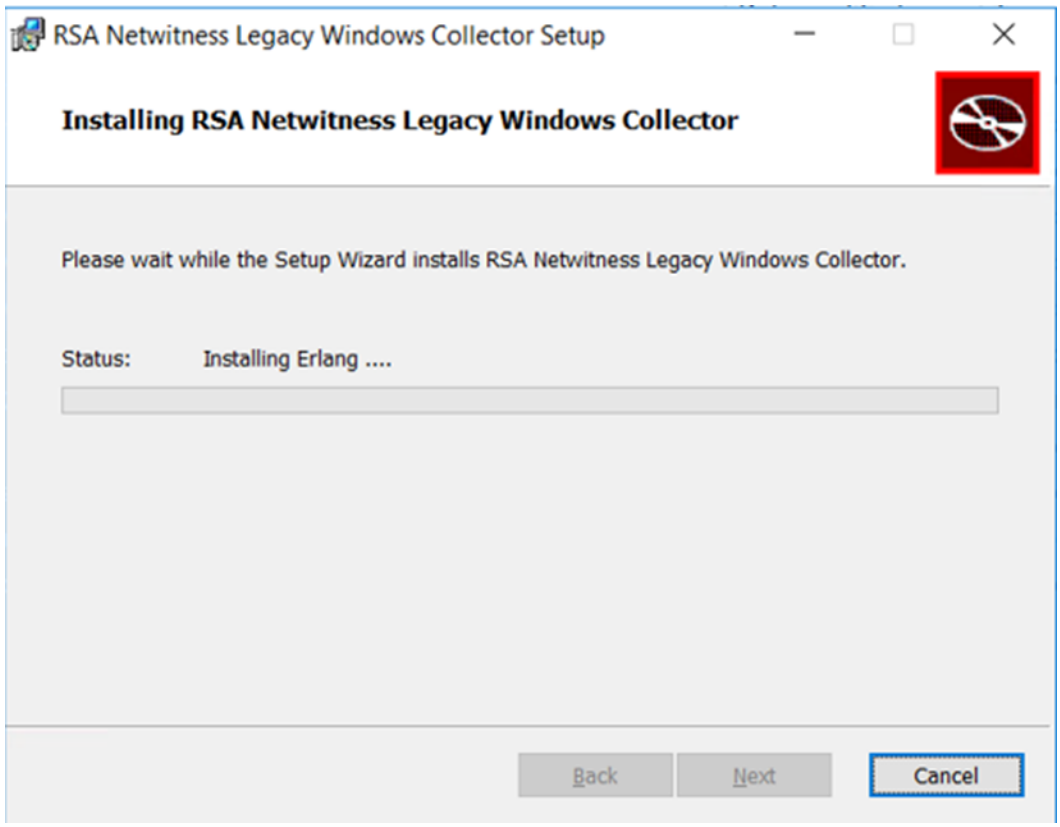
6. Read the License agreement carefully, select the **I accept the terms in the License Agreement** radio button, and click **Next**.

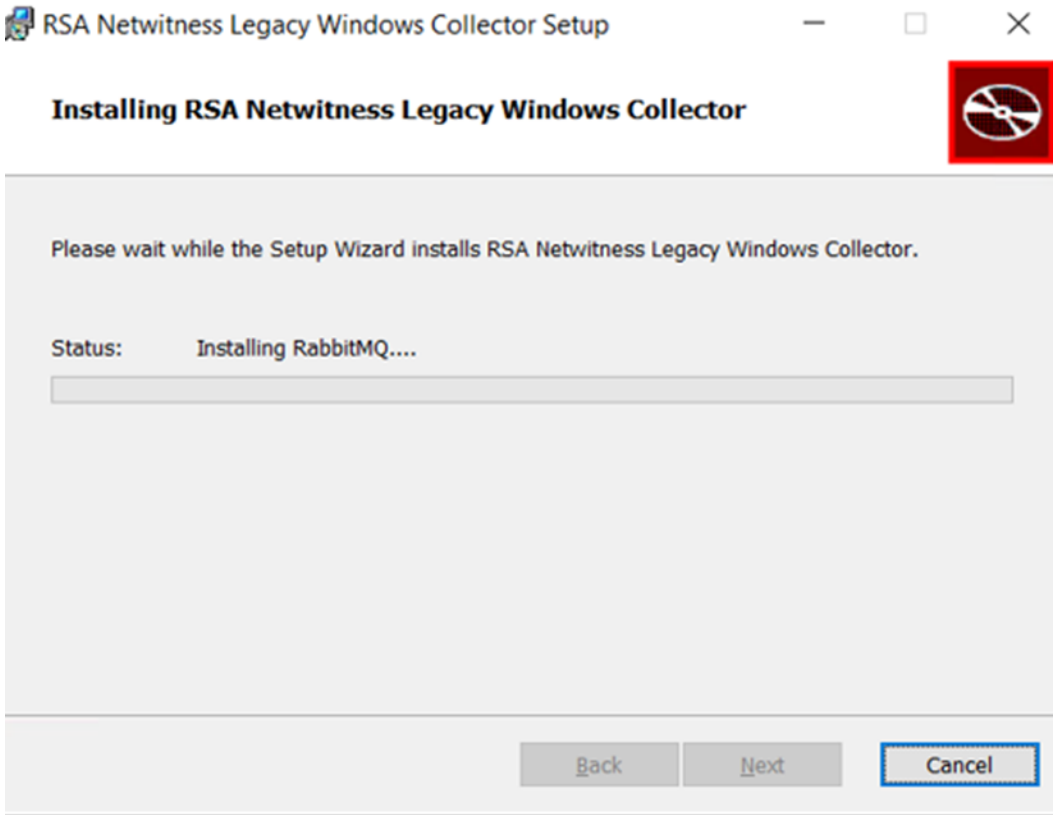
   The Ready to Install the Program page is displayed.



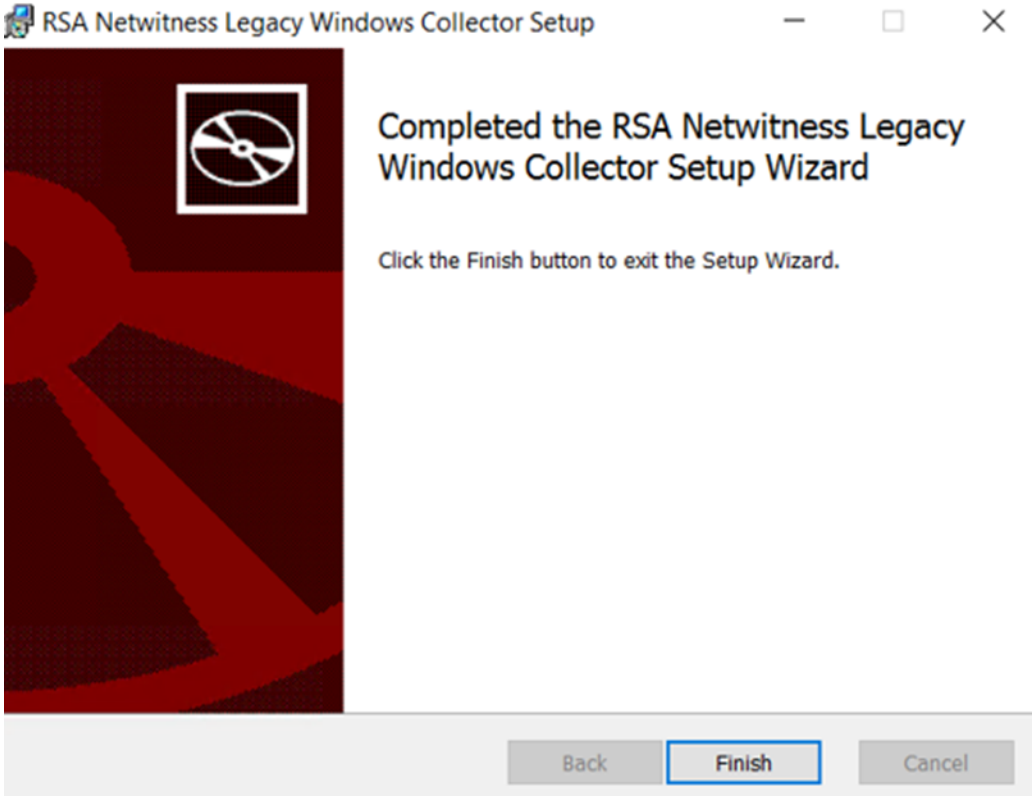
7. Click **Install**.

   The Installation screens for the Legacy Windows Collector page are displayed.


RSA Netwitness Legacy Windows Collector Setup
Installing RSA Netwitness Legacy Windows Collector
Please wait while the Setup Wizard installs RSA Netwitness Legacy Windows Collector.
Status: Installing Erlang ....
Back
Next
Cancel


RSA Netwitness Legacy Windows Collector Setup
Installing RSA Netwitness Legacy Windows Collector
Please wait while the Setup Wizard installs RSA Netwitness Legacy Windows Collector.
Status: Installing RabbitMQ....
Back
Next
Cancel

The Installation Completed page is displayed.



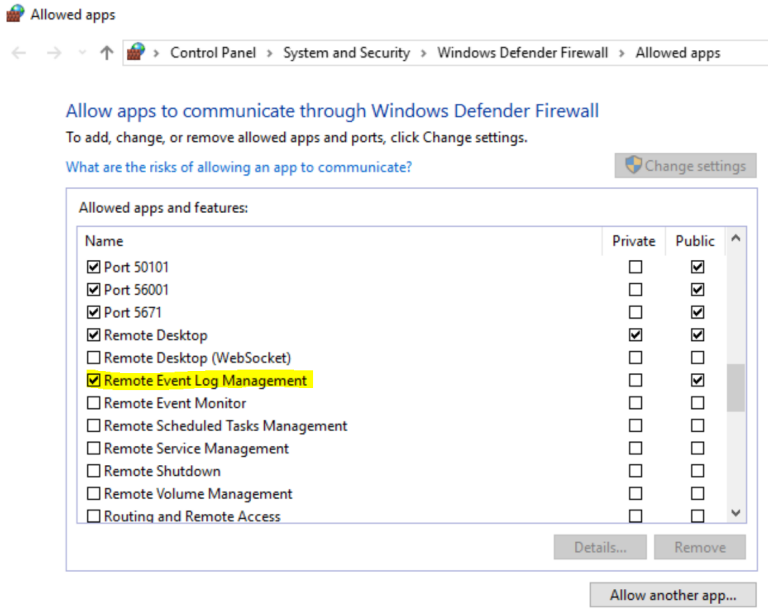
8. Click **Finish**.
9. Reboot the machine.

This completes the installation of the 12.5.x Legacy Windows Collector. Please refer to the Windows Legacy and NetApp Collection Configuration Guide on NetWitness Community for instructions on how to configure Legacy Windows collection in NetWitness.

Configure the Windows Server

For the NetWitness to communicate with the Windows Server, you need to allow Remote Event Log Management on the Windows Server.

1. On the Windows Server, in Services, start the Remote Registry Service.
2. In Firewall, enable Remote Event Log Management for your network, as shown below.



Add or Reconfigure a Windows Legacy Collector Host and Service in NetWitness Platform

For this version of the Windows Legacy Collector, NetWitness has provided a script that replaces the manual steps of adding a Windows Legacy Collector host and service in the NetWitness UI.

To create a Windows Legacy Collector Host and Service in NetWitness:

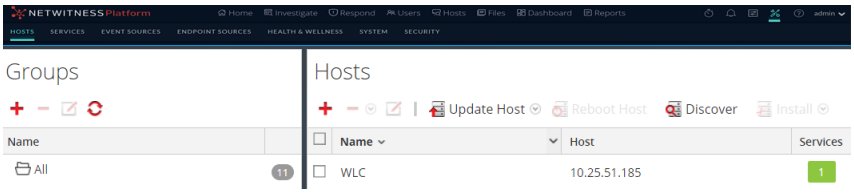
1. SSH to your NetWitness server.
2. Run the following command:

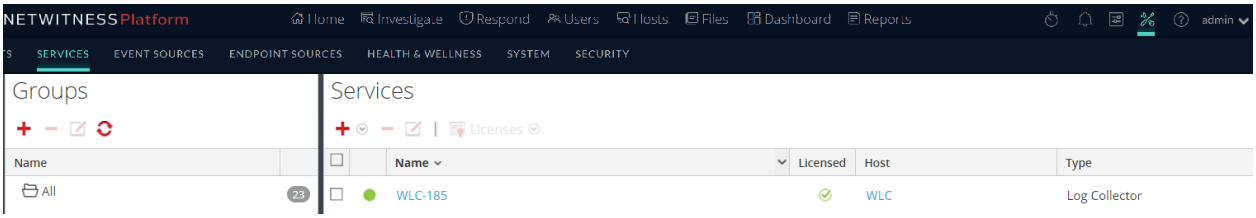
   ```
   wlc-cli-client --host-display-name hostDisplayName --service-display-name
   serviceDisplayName --host WLChostIPAddress --port 50101 --use-ssl false
   ```

   The parameters are explained below:

   - **--host-display-name**: the name for the host as it is displayed in the NetWitness Hosts page
   - ***--service-display-name***: the name for the host as it is displayed in the NetWitness Services page
   - **--host**: the IP address for the Windows Legacy Collector
   - **--port**: the port NetWitness uses to communicate with the Windows Legacy Collector. The recommended value is 50101.
3. You will be prompted to supply the following information:
   - **Windows Log Collector REST Username** and **Windows Log Collector REST Password**: you must supply admin credentials for the Windows Legacy Collector.
   - **Security Server Username** and **Security Server Password**: you must supply admin credentials for NetWitness.

After you complete this procedure, you should see the Windows Legacy Collector Host and Service as shown in the following screenshots.





Troubleshoot a Fresh or Upgrade Install

Logs to Examine for Information

Refer to the following log files if you need to troubleshoot problems:

- `%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log`
- `%systemDrive%\Program Files\NwLogCollector\installlog.txt`

Run `C:\Program Files\NwLogCollector\ziplogfiles.vbs` to generate the ***hostname***`_WLCversion_timestamp.zip` that contains all the log files and other information needed for troubleshooting.

Issues with the Lockbox

When you create a lockbox password on a new Windows Legacy Collector, you might see the following error:

```
failed to set secure storage password: failed to create lockbox: The Lockbox or cryptography library could not be found.
```

This can occur if you are running Windows Legacy Collector older version.

If you encounter this issue, download and install both of the following redistributable packages:

- Visual C++ 2010: https://www.microsoft.com/en-us/download/details.aspx?id=14632
- Visual C++ 2012: https://www.microsoft.com/en-us/download/details.aspx?id=30679

SA Fails to Connect to WLC Showing RED in SA -> Hosts Page

This can occur during mixed mode upgrade. If you encounter this issue, follow these steps.

1. Copy the `/etc/pki/nw/carlos/rsa-nw-sa-server-cert.pem` from SA node to WLC node using the REST of WLC *http://<wlc-ip>:50101/sys/trustpeer*.
2. Restart the WLC node and then restart Jetty service from the SA node.

New WLCs Offline on the User Interface

Follow these steps to troubleshoot and resolve the issue of new WLCs appearing offline on the UI.

1. Add the certificates to Trustpeer through the REST interface of the WLC by following these steps:
   a. Open your web browser and navigate to **https://<WLC IP>:50101** to log into the WLC's REST page.
   b. Click **Sys** to access the **Sys** page.
   c. Go to */Sys/trustpeer* to navigate to Trustpeer.
   d. Add Admin Server Certificate by following these steps:
      i. Click **Add**.
      ii. Open the Admin Server's */etc/pki/nw/peer/sa-server/<UUID>.pem* file.
      iii. Copy the contents of this file.
      iv. Paste the copied content into the text box on the *sys/trustpeer* WLC's REST page.
      v. Click **Upload**.
   e. Add the Admin Certificate by following these steps:
      i. Repeat the steps given under 'Add Admin Server Certificate' for the */etc/pki/nw/peer/admin-cert.pem* file.
      ii. Copy the contents of this file.
      iii. Paste the copied content into the text box on the *sys/caupload* WLC's REST page.
      iv. Click **Upload**.
2. Restart the following services to apply the changes:
   - NwLogcollector
   - NwStatCollector
   - RabbitMQ
3. Check the UI to ensure the new WLCs are now online.
4. Verify that the certificates have been added correctly and the services are operational.

(Optional) Change the Windows Legacy Collector IP Address

Note: The procedures in this section apply to NetWitness 12.3 and later only.

On occasion, you may need to change the IP address of your Windows Legacy Collector. You may also need to edit any Destination Groups that you have configured.

Change WLC IP Address

The following procedure describes how to change the IP address for your system.

1. Log onto the Windows Legacy Collector system and manually change the IP address on the system.
2. In the UI, confirm that the Log Collector service corresponding to the WLC system shows up in error (Red). It might take some time for it to reflect the changed status.
3. On the NetWitness Server, use the **nw-manage** utility to view the host information for the WLC using the following command:

   ```
   nw-manage --list-hosts
   ```

   Sample output from running the command is shown here:

   ```
   {
   "id" : "fdb8150c-e040-459e-8cc5-3c60ec2c65ae",
   "displayName" : "WLC-HOST-104",
   "hostname" : "10.101.216.102",
   "ipv4" : "10.101.216.102",
   "ipv4Public" : null
   } ]
   ```

   You use the value of **"id"** from your output in the following step.
4. Use the **nw-manage** utility to change the IP address of the WLC. For the **host-id** argument, use the value for the **"id"** that you noted from step 3. For the **ipv4** value, use the new IP Address to which you are changing.

   ```
   nw-manage --update-host --host-id "fdb8150c-e040-459e-8cc5-3c60ec2c65ae" --ipv4 10.101.216.105
   ```
5. After you see the message that the previous command ran successfully, go to the NetWitness Server UI and verify that the WLC service is running without any errors.

Edit Destination Groups For Log Collectors and VLCs

The Windows Legacy Collector is often configured with Destination Groups to forward events to Log Collectors or Virtual Log Collectors. If the IP address of any such Destination LC or VLC is changed, the Windows Legacy Collector can no longer forward events. To remediate this, you must edit the Destination groups for the WLC, making sure to select the new LC or VLC IP Address.

(Optional) Enhance Security by Disabling Weak Cipher Suites

Using weak cipher suites can expose your system to security risks like man-in-the-middle attacks and data breaches. Disabling these weak ciphers ensures secure communication and prevents vulnerabilities on port 5986, used by the Windows Log Collector.

Note: If weak ciphers are enabled, vulnerability scanners might flag the port used by the Windows Log Collector (WLC). To maintain system security, it's crucial to keep all cryptographic configurations up to date.

Disable Weak Cipher Suites

To disable weak cipher suites:

1. Open **PowerShell** as an Administrator.
2. Run the following commands to disable weak ciphers.

   To disable SSL 2.0

   - ```
     New-Item -Path
     "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
     \Protocols\SSL 2.0" -Force

     New-Item -Path
     "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
     \Protocols\SSL 2.0\Server" -Force

     Set-ItemProperty -Path
     "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
     \Protocols\SSL 2.0\Server" -Name "Enabled" -Value 0
     ```

   To disable SSL 3.0

   - ```
     New-Item -Path
     "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
     \Protocols\SSL 3.0" -Force

     New-Item -Path
     "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
     \Protocols\SSL 3.0\Server" -Force

     Set-ItemProperty -Path
     "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
     \Protocols\SSL 3.0\Server" -Name "Enabled" -Value 0
     ```

   To disable RC4 128/128

- ```
  New-Item -Path
  "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
  \Ciphers\RC4 128/128" -Force

  Set-ItemProperty -Path
  "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
  \Ciphers\RC4 128/128" -Name "Enabled" -Value 0
  ```

To disable RC4 40/128

- ```
  New-Item -Path
  "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
  \Ciphers\RC4 40/128" -Force

  Set-ItemProperty -Path
  "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
  \Ciphers\RC4 40/128" -Name "Enabled" -Value 0
  ```

To disable RC4 56/128

- ```
  New-Item -Path
  "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
  \Ciphers\RC4 56/128" -Force

  Set-ItemProperty -Path
  "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
  \Ciphers\RC4 56/128" -Name "Enabled" -Value 0
  ```

Configure Strong Cipher Suites

Caution: These changes will affect the system's cryptographic settings and could affect other services. We recommend enabling only strong cipher configurations, but please verify the compatibility of these changes with other services before implementation.

To configure strong cipher suites:

1. Navigate to the registry path.

   ```
   HKEY_LOCAL_
   MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\
   Local\SSL\00010002
   ```

2. Edit the Functions key to include only strong cipher suites.
3. Remove support for the following:
   - CBC (Cipher Block Chaining) Ciphers
   - SHA-1 Hash Algorithm
   - RC4 Ciphers
4. Enable support for cipher suites under TLS 1.2 or higher, such as:
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   ```

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

5. Restart the system to apply the changes.

(Optional) Backup and Restore Legacy Windows Collector

This section tells you how to backup and restore the NetWitness Legacy Windows Collector.

Note: You only need to do this if you are changing the Windows VM where you run the Windows Legacy Collector.

During upgrade, the backup script for the Windows Legacy Collector is invoked automatically, and creates the previous version configuration and run-time backups. After the latest version installation is completed, run the Restore script to restore the configuration and run-time files for the updated Windows Legacy Collection.

Restore the Windows Legacy Collection Backup after Upgrade

To restore the Windows Legacy Collection setup on a newly upgraded NetWitness platform:

1. On the Windows Legacy Collector, open a command prompt window.
2. Navigate to **C:\Program Files\NwLogCollector**, where the scripts are stored.
3. Run the following commands for restoring a backup:
   - Backup configuration files: `WLC-Restore.bat "Config-bkup_`***`timestamp`***`.zip"`
   - Backup run-time files: `WLC-Restore.bat "Runtime-bkup_`***`timestamp`***`.zip"`
4. Once the restore is completed, set the lockbox SSV to use the password that you created during previous version setup.
   a. In the **Security Analytics** menu, select **Services**, then select your Windows Legacy Collector and choose **Explore**.
   b. From the left navigation pane, expand **logcollection > properties > crypto**.
   c. Run the following command: `op=setssv pw=`***`password_for_<version no.>_lockbox`***, and hit **Send**. (Replace version no. with previous version number.)

Revert Windows Legacy Collection from 12.5.x Back to Previous Version

To revert the Windows Legacy Collection setup from 12.5.x back to previous version:

1. Uninstall the 12.5.x Setup. Note the location of the backup folder created by the system during the uninstall procedure.
2. Install the previous version of the Windows Legacy Collector.
3. Navigate to **C:\Program Files\NwLogCollector**, where the scripts are stored.
4. Run the Restore script from backup folder present in **C:\Program Files\NwLogCollector** to restore the configuration and run-time setup on the Windows Legacy Collector.
   - Backup configuration files: `WLC-Restore.bat "Config-bkup_`***`timestamp`***`.zip"`
   - Backup run-time files: `WLC-Restore.bat "Runtime-bkup_`***`timestamp`***`.zip"`
5. Once the restore is completed, set the lockbox SSV to use the password that you created during previous version setup.
   a. In the **Security Analytics** menu, select **Services**, then select your Windows Legacy Collector and choose **Explore**.
   b. From the left navigation pane, expand **logcollection > properties > crypto**.
   c. Run the following command: `op=setssv pw=`***`password_for_<version no.>_lockbox`***, and hit **Send**. (Replace version no. with previous version number.)