RSA NETWITNESS® SUITE

NetWitness® Endpoint 4.4.0.2 Release Notes

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

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 RSA Link. 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

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

January 2018

Contents

Introduction

This document describes the enhancements and fixes included in RSA NetWitness® Endpoint 4.4.0.2. RSA recommends reading this document before installing and using RSA NetWitness Endpoint 4.4.0.2. This document contains the following sections:

Update Notes

RSA NetWitness Endpoint 4.4.0.2 supports upgrade paths from previous versions, as follows:

- The following RSA NetWitness Endpoint releases may update directly to RSA NetWitness Endpoint 4.4.0.2:
  - RSA NetWitness Endpoint 4.4.0.0 or 4.4.0.1
  - RSA NetWitness Endpoint 4.3.0.5 or 4.3.0.6
  - RSA NetWitness Endpoint 4.2.0.4
- Users on all other versions must first upgrade to a supported version before updating to 4.4.0.2.

Note: If you have configured your previous version of NetWitness Endpoint to work with OPSWAT Metascan (now called Metadefender Core) v3, once you update to NetWitness Endpoint 4.4.0.2, you must download and install OPSWAT Metadefender Core v4.8.0. OPSWAT Metadefender v3 will not work with NetWitness Endpoint 4.4.0.1 or later. For directions on downloading and installing OPSWAT Metadefender Core, see the topic "Step 9: (Optional) Install Metascan" in the latest version of the *NetWitness Endpoint 4.4 Installation Guide*.

Note: For all agents communicating through the Roaming Agents Relay (RAR), you should wait until agents are communicating directly to the ConsoleServer before updating to ensure a successful update.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Endpoint 4.4 User Guide	https://community.rsa.com/docs/DOC-81665
RSA NetWitness Endpoint 4.4 Installation Guide	https://community.rsa.com/docs/DOC-81664

Fixed Issues

This section lists issues that were found in RSA NetWitness Endpoint 4.2.0.x, 4.3.0.x, or 4.4.0.x and fixed in RSA NetWitness Endpoint 4.4.0.2.

Note: The fixed issues only refer to issues fixed in this release. To check issues fixed in releases previous to 4.4.0.2, refer the respective release notes, available on RSA Link.

Tracking Number	Description
ECATCE-884	Different network process results are returned when pivoting from UI to Investigator.
ECATCE-877	Failed KernelData.csv download attempt corrupts previously good version of the file.
ECATCE-838	Max Pool Errors are filling NetWitness Endpoint log files.
ECATCE-835	Queued MachineCommands that are outdated, such as retrievecount > 5, need to be rolled off to improve performance of processing agent commands on the SQL servers.
ECATCE-816	NetWitness Endpoint agent causing BSOD and boot loops.
ECATCE-798	mocNetAddresses table is actually larger after weekend maintenance job runs.
ECATCE-706	NetWitness Endpoint agent (full monitoring) with Eclipse or Visual Studio with Ncrunch degrades performance.
ECAT-8840	Enabling OPSWAT results in the following error: "String was not recognized as a valid DateTime."
ECAT-8819	Blacklisted IIOC alerts are sent repeatedly for NetWitness Endpoint agent on secondary server.
ECAT-8814	IIOC bias status is not updated when machine status is changed to Gold Image.
ECAT-8813	GlobalAggregations value is not in sync and throws an error message on secondary server "TableLastSyncTime" DBtable after running a query.
ECAT-8812	In the NetWitness Endpoint UI, the Global IP list does not show modules or machines data in the bottom panel for some selected events.
ECAT-8804	If user selects more than that 99 Linux or Mac downloaded modules, the Scan with YARA option is not available

Tracking Number	Description
ECAT-8803	Unintended RSA Live feeds refresh interval is used.
ECAT-8798	RSA Live feeds are not downloading.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Tracking Number: ECAT-8807
Problem: RSA feeds are not downloading, but the last updated time in the UI is up-to-date.
Workaround: In Microsoft SQL Server Management Studio, enter the following command: `update SubscribedFeeds set LastUpdatedInLiveUTC=NULL`, then click **Download Now**, and **Refresh** (give it some time to download).

Tracking Number: ECATCE-763
Problem: In the Modules view, when a user right-clicks a column header and selects Column Chooser, if the user expands the Reputation category in the Customization dialog, the user is unable to scroll to the last item, which is Yara Scan result.
Workaround: In the UI, use the search area to find "Yara scan result."

Tracking Number: ECATCE-822
Problem: When doing a fresh install of NetWitness Endpoint 4.3.0.5 or later, if the "sa" sysadmin account was previously removed from the MSSQL database, a database error occurs.
Workaround: Enable or recreate the "sa" sysadmin account for the MSSQL database and repeat the NetWitness Endpoint installation process.

Tracking Number: ECAT-8741
Problem: If a user applies a filter to the Machine View, changes the column order, then closes and restarts the NetWitness Endpoint UI, the Machine View display is blank and the following error message is displayed: "Error occurred during processing server request (The binary operator Equal is not defined for the...)." This occurs because the grid view layout for the Machine view, including the column order and filter, is saved to disk when column order is changed by the user. When the UI is restarted, the previous filter and the previous column order are both reapplied.
Workaround: To prevent this issue, user should avoid applying filters to the Machine View when also making any column modifications, such as reordering or adding or removing. To recover from this issue, the user should remove the applied filter and do some reordering of columns, which will overwrite the previously saved filter on disk. The user can then continue to work as usual.

Tracking Number: ECAT-8611
Problem: For some downloaded modules, OPSWAT automatic and manual scans are not working properly.
Workaround:

Tracking Number: ECAT-8349
Problem: In the Machine and Module views, the row count shows as "0" for a group even though the group has rows.
Workaround: The user can expand each group to update the group count data.

Tracking Number: ECAT-8301
Problem: If a NetWitness Endpoint 4.3.0.x user has subscribed to all RSA Live feeds, when that user upgrades to version 4.3.0.4, all the subscribed feeds get cleared.
Workaround: After upgrading the NetWitness Endpoint ConsoleServer to version 4.3.0.4, in the NetWitness Endpoint UI, navigate to **Configure > External Components Configuration**. On the External Components Configuration dialog, select to edit the RSA Live configuration. On the RSA Live dialog, click **Select All** and then click **Save**.

Tracking Number: ECATCE-624
Problem: RSA NetWitness® Endpoint 4.1.2.0 may fail to download the KernelData.csv file from the liveecat.rsa.com site, even though the ECAT Server is able to access the internet. The reason for this is that RSA NetWitness® Endpoint 4.1.2.0 uses .NET 4.5, which by default does not support TLS 1.1+. (Beginning with release 4.2.0.0, RSA NetWitness® Endpoint uses .NET 4.6, which does support TLS 1.1.+.) More information may be found here: https://blogs.msdn.microsoft.com/dotnet/2016/08/02/announcing-net-framework-4-6-2/.
Workaround: You can enable TLS 1.1+ in .NET 4.5 via registry key by setting the SchUseStrongCrypto value as described here: https://technet.microsoft.com/en-us/library/mt791311(v=office.16).aspx.

Tracking Number: ECAT-7884
Problem: If you decommission a server with an agent under containment, the agent will be moved to the Primary server. However, after this point, the agent will be self-contained, because it does not have the Primary server IP in the exclusion list.
Workaround: You must manually reinstall a new agent on the machine.

Tracking Number: ECAT-7545
Problem: Mac IIOC alertable values set to False after upgrading ConsoleServer from pre-4.3 to 4.3.0.0.
Workaround: Manually change Mac IIOC alertable values to True after updating to 4.3.0.0.

Tracking Number: ECAT-7263
Problem: Updating of agents while in Roaming Agents Relay (RAR) mode is not supported.
Workaround: Update agent only when agent is communicating directly to the ConsoleServer.

Tracking Number: ECAT-7213/ECAT-7214
Problem: The Delete from Quarantine function was not working correctly and was removed from the RSA NetWitness Endpoint UI.
Workaround: Do not use any quarantine features.

Installation

RSA NetWitness® Endpoint 4.4.0.2 supports upgrade paths from previous versions, as follows:

- The following RSA NetWitness Endpoint releases may update directly to RSA NetWitness Endpoint 4.4.0.2:
  - RSA NetWitness Endpoint 4.4.0.0 or 4.4.0.1
  - RSA NetWitness Endpoint 4.3.0.5 or 4.3.0.6
  - RSA NetWitness Endpoint 4.2.0.4
- Users on all other versions must first upgrade to a supported version before updating to 4.4.0.2.

Note: It is considered a best practice for RSA NetWitness Endpoint agents to be updated to the installed version. If merge issues are encountered, agents need to be updated to RSA NetWitness Endpoint 4.4.0.2.

Note: If you have configured your previous version of NetWitness Endpoint to work with OPSWAT Metascan (now called Metadefender Core) v3, once you update to NetWitness Endpoint 4.4.0.2, you must download and install OPSWAT Metadefender Core v4.8.0. OPSWAT Metadefender v3 will not work with NetWitness Endpoint 4.4.0.1 or later. For directions on downloading and installing OPSWAT Metadefender Core, see the topic "Step 9: (Optional) Install Metascan" in the latest version of the *NetWitness Endpoint 4.4 Installation Guide*.

Note: For all agents communicating through RAR, you should wait until agents are communicating directly to the ConsoleServer before updating to ensure a successful update.

Note: The installation directory for Linux agents changed with release 4.3.0.4. The new installation directory for Linux agents is: `/opt/rsa/nwe-agent`. Additionally, the agent binary is located in `/opt/rsa/nwe-agent/bin` and the certificate and configuration are located in `/opt/rsa/nwe-agent/config`. The service name has also changed from `ecat-agent` to `nwe-agent`. To stop or start the agent, you need to execute `service nwe-agent` stop command. To uninstall the agent, execute `rpm -e nwe-agent` command.

Installation Prerequisites

RAID Configuration

RSA strongly recommends the following configuration when using a single RAID 10 volume for the RSA NetWitness Endpoint Microsoft SQL database: You must use a 64K block size in Windows with a 1024 offset and NTFS file system when formatting the partition. If this is not the configuration used, there could be serious impacts to system performance.

Database Backup

It is also strongly recommended to backup all RSA NetWitness Endpoint Microsoft SQL databases, primary and secondary, and create a backup copy of the server and client certificates. For complete details, see the "Update Installation" section of the *RSA NetWitness Endpoint 4.3 Installation Guide*.

Note: Supported versions of Microsoft SQL Server are: MSSQL 2012 and MSSQL 2014, Standard and Enterprise Editions.

Microsoft Windows Update Service

To avoid a potential error message during the RSA NetWitness Endpoint update procedure, caused by the Microsoft Windows Update service affecting the connection to the MSSQL Server, it is strongly recommended that you stop the Windows Update service before initiating the RSA NetWitness Endpoint update installation. Furthermore, to avoid interference with the RSA NetWitness Endpoint system, RSA recommends that you keep the Windows Update service turned off and use the following process for applying Windows Updates:

1. Stop the RSA ECAT Server and RSA ECAT API Server services.
2. Stop the SQLServerAgent service.
3. Turn on the Windows Update service and proceed with the Windows Update and all necessary steps such as download, installation, and reboot.
4. When the Windows Update is complete, turn off the Windows Update service.
5. Restart the SQLServerAgent service.
6. Restart the ECAT Server and ECAT API Server services.

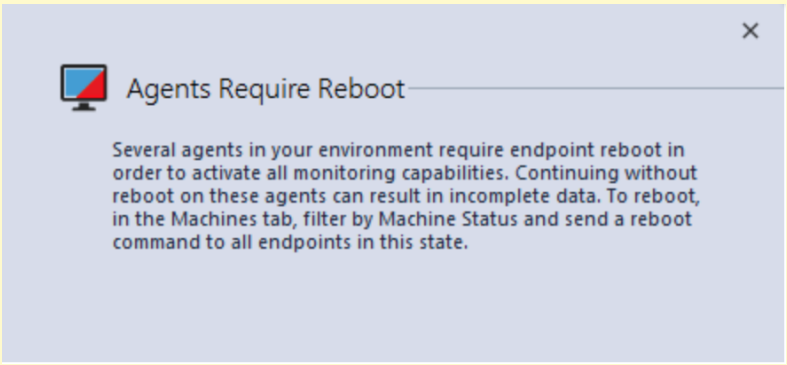
Installation Procedure

To update from a supported update version of RSA NetWitness Endpoint, see the complete update instructions in the "Update Installation" section of the *RSA NetWitness Endpoint 4.4 Installation Guide*, using the 4.4.0.2 archive file (**rsa_nwe_4.4.0.2_sw.zip**).

If you are currently using the Roaming Agents Relay (RAR), you will also need to update RAR to version 4.4.0.2, as described in the "Update Installation" section of the *RSA NetWitness Endpoint 4.4 Installation Guide*, using the 4.4.0.2 archive file (**rsa_nwe_4.4.0.2_roaming_agents_relay.zip**).

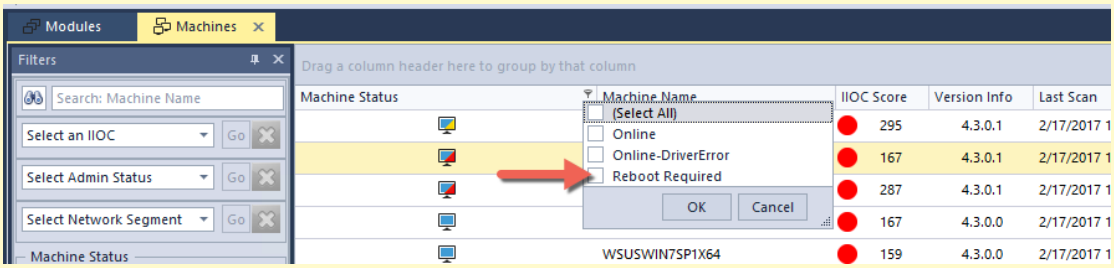
Note: NetWitness Endpoint 4.4.0.2 release does not support full install of the product.

Caution: After updating agents to 4.4, when the Machines table is loaded in the RSA NetWitness Endpoint UI, if any RSA NetWitness Endpoint agents are currently in the driver error 0x20010007 state, the following message will be displayed:



You must reboot the affected machines to ensure agents are collecting complete data, as follows:

1. In the Machines table, select to filter the Machine Status column by **Reboot Required**, as shown below:



2. Select all machines that match that status (these machines will all have this machine status icon: .)

3. Right-click and select **Advanced > Reboot...**.

For more information on rebooting machines, see the "Reboot a Machine" topic in the *RSA NetWitness® Endpoint 4.4 User Guide*.

Note: Beginning with RSA NetWitness Endpoint 4.3.0.1, encryption for generated certificates has changed from SHA1 to SHA256 and the length has also changed from 2048 to 4096. This change will not be apparent to users. However, if users elect to generate new certificates, the certificate names will change as follows: EcatCA is now NweCA, EcatClientExported is now NweAgentCertificate, and EcatServerExported is now NweServerCertificate. You can also still select to continue using existing certificates, in which case the certificate names will not change, but will continue to be valid.

Contacting Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness Endpoint product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com/welcome
Contact RSA Support	https://community.rsa.com/docs/DOC-1294
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email	nwsupport@rsa.com
Community	https://community.rsa.com/community/products/netwitness
Support Plans and Options	https://community.rsa.com/docs/DOC-40401

Revision History

Revision	Date	Description
1.0	January 2018	Initial version