Security Agent for UNIX 7.5 Release Notes

November 2016

Security Agent for UNIX includes new features, improves usability, and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Security Agent for UNIX NetIQ Documentation (https://ww.netiq.com/documentation/change-guardian/) page. To download this product, see the Security Agent for UNIX Product Upgrade (http://www.netiq.com/products) website.

1 What’s New?

The following outline the key features and functions provided by this version, as well as issues resolved in this release:

1.1 New Platform Support

Security Agent for UNIX includes support for the following platforms:

- Red Hat Enterprise Linux 7.2

- Red Hat Enterprise Linux 7.1

- Red Hat Enterprise Linux 7.0

- Red Hat Enterprise Linux 6.7

- SUSE Linux Enterprise Server 12 SP1

- SUSE Linux Enterprise Server 12

For more information see, Technical Information page.

1.2 Enhancements and Software Fixes

Security Agent for UNIX includes enhancements and software fixes that resolve several previous issues.

1.2.1 New Agent Manager Connector for Sentinel users

The new Agent Manager Connector addresses communication issues between the Security Agent for UNIX and the Sentinel server due to a mismatch of the hostname in the certificate.

1.2.2 Dynamic Rules Update on Linux Auditing

When you assign the policies to the agent, the audit rules are dynamically created based on the required criteria. When you unassign the policies, the audit rules are dynamically destroyed.

1.2.3 Federal Information Processing Standards (FIPS) support for Security Agent for UNIX

You can install Security Agent for UNIX 7.5 in FIPS mode. For more information see, Understanding FIPS Implementation in *Security Agent for UNIX Installation and Configuration Guide*.

1.2.4 Removal of 32-bit Dependencies on Linux Platforms

You can install Security Agent for UNIX 7.5 on all 64-bit platforms without any 32-bit library dependencies.

1.2.5 Addition of Open Enterprise Server Rule Set for Sentinel

Open Enterprise Server (OES) rule group monitors Linux Auditing events generated by Network Security Services (NSS) auditing engine on Open Enterprise Server computers using the Agent. The Agent reads the Open Enterprise Server events and forwards the events to Sentinel.

1.2.6 Security Agent for UNIX Does Not Handle Event Load Beyond 250 EPS

Issue: When the event load on Security Agent for UNIX exceeds approximately 250 EPS, it accumulates a large number of spool files. As a result, the disk fills up and the event flow stops to Sentinel.(`Bug 1027965`)

Fix: Security Agent for UNIX performance is improved and certified to handle approximately 3000 EPS on testing hardware.

2 System Requirements

For detailed information on hardware requirements and supported operating systems and browsers, see Technical Information page.

3 Installing Security Agent for UNIX

The following steps provide an overview of how to install the Security Agent for UNIX:

1. Install the UNIX Agent Manager Server.
2. On the computers where you want to monitor agents, install the UNIX Agent Manager Console.
3. On the UNIX and Linux computers you want to manage, install Security Agent for UNIX.

For more information about installing these components, or if you are upgrading from a previous release, see the Security Agent for UNIX Installation and Configuration Guide, on the Change Guardian Documentation Web site.

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

4.1 Touch Command Does Not Generate Events for File Modification

The HP-UX 11iv3 auditing subsystem does not provide information for the `utimes`, `utime`, `dup`, or `dup2` system calls. This limitation means that Change Guardian is not able to report events for the `utimes` access type in the CGU `FileMod` object and cannot report events when the contents of a file changes.

When you monitor changes to the attributes of a file on a HP-UX computer, Change Guardian does not generate events when the time attribute changes. `(Bug 969023)`

4.2 Cannot Generate Events for File Handling on RHEL7.2

The Security Agent for UNIX on RHEL 7.2 does not generate file handling events while using the Vi command, because the auditing system cannot generate utime events. `(Bug 968824)`

4.3 Exception in Agent When You Forward Events from the Agent for Change Guardian to the Standalone Sentinel Server

Issue: When you forward File Integrity Changed events from the agent for Change Guardian to the Standalone Sentinel server, file integrity attachments might display the following exception: `Error parsing JSON: ReferenceError: changed is not defined.(Bug 971624)`

Note: This issue is not found in Sentinel 7.4 or later versions.

Workaround: Ignore the exception. There is no impact to the performance because of this exception.

4.4 Events Generated for File Deletion Using rm –rf Command Display Incorrect Information

Issue: When you enable the **Including Subdirectories** or **Excluding Subdirectories** filter for monitoring file deletion, the events generated for file deletion do not display correct path information for the deleted files. The events are generated as file deletion events when you delete directories and sub-directories, even though the policy applied is for monitoring **file** deletion only.

When you enable **Excluding Subdirectories** filter, events are generated when you delete files under subdirectories also.`(Bug 975953)`

4.5 Directory Delete and Rename Events Might Not Appear For Linux

When you delete or rename directories on Linux platforms, the audit logs show null value for the directory name. Change Guardian might not capture the correct directory name in the audit logs. `(Bug 974273)`

4.6 Unable to Deploy Agents Remotely via UAM in FIPS mode

Issue: When the UNIX Agent Manager is running in FIPS mode, it does not support the remote deployment of the agents. `(Bug 989710)`

Workaround: You should manually install the agents, and then add them to UAM using **Add Host**.

4.7 Manual Configuration Required to Use UNIX File System Browser

To enable the UNIX file system browser in Change Guardian, you must set the `repositoryEnabled` flag (under `HKLM\Software\NetIQ\ChangeGuardianAgent\repositoryEnabled`) to `1`, and then restart the agent.

If you do not manually set the flag to `1`, when you use the Registry Browser, you will receive a `Could not connect to UNIX Data Source error.(Bug 981826)`

NOTE: To enable browsing for UNIX data sources while creating a policy, the computer where you install the Policy Editor must have a Windows agent. If you do not install an agent on the Policy Editor computer, you must manually enter the data source paths while creating a policy.

4.8 Upgrading Agents to 7.5 via UAM Linux Fails

Issue: Due to important security updates to OpenSSL, the normal upgrade process for agents prior to UNIX Agent Manager 7.5 fails with the following error: `ERROR: An error was encountered while performing the upgrade.....(Bug 995912)`

Workaround: To upgrade the agent, perform the steps in Upgrading Agent to 7.5 Using UNIX Agent Manager.

4.9 Agent Fails to Connect to Secure Configuration Manager 6.0 in FIPS Mode

Issue: When you install and register Security Agent for Unix 7.5 to Secure Configuration Manager 6.0 in FIPS mode, the agent will display an error.`(Bug 996866)`

Workaround: Upgrade Secure Configuration Manager to 6.1 or higher versions. For more information, see Upgrading Secure Configuration Manager.

4.10 UNIX Agent Manager 7.5 Cannot Deploy Agent on FIPS Enabled Linux or UNIX Computers

When the operating system is running in FIPS mode, UNIX Agent Manager 7.5 (Linux and Windows) cannot deploy the Security Agent for UNIX. It displays the following error:

```
SSH Install Failed - Session.connect: java.io.IOException: End of IO Stream Read
```

```
Installation Failed - Session.connect: java.io.IOException: End of IO Stream Read.(Bug 999496)
```

4.11 UNIX Agent Manager 7.5 Cannot Monitor Security Agent for UNIX 7.4

Issue: The communication between UNIX Agent Manager 7.5 and Security Agent for UNIX 7.4 fails due to protocol mismatch.

Workaround: Upgrade Security Agent for UNIX 7.4 to 7.5. For more information about upgrading to Security Agent for UNIX 7.5, see Upgrading Agent Using UNIX Agent Manager `(Bug 989481)`.

4.12 Event Diagnostics Not Supported for Security Agent for UNIX

The **Assets Monitoring Failures** report contains Windows assets only. It does not contain data related to the UNIX assets (Bug 906282).

4.13 Events Not Generated When Soft Link for File is Deleted

Issue: `File was deleted` events are not generated when soft link for file is deleted (Bug 975575).

4.14 Sentinel Agent Manager Connector Not Working in FIPS Mode

Issue: Sentinel Agent Manager Connector does not work in FIPS mode.

Workaround: For the Sentinel Agent Manager Connector to work in FIPS mode, perform the steps mentioned in NetIQ Knowledge Base Article 7018187. (Bug 997589)

4.15 UNIX Agent Manager 7.5 Cannot Manage AppManager Agent for UNIX

Issue: UAM 7.4 is packaged and is compatible with AppManager Agent for UNIX 8.1. When the Security Agent for UNIX 7.5 is installed on the same host as the AppManager Agent for UNIX, it becomes incompatible with UAM 7.4 due to secure communication incompatibilities. Therefore, UAM 7.5 must be used to manage the Security Agent for UNIX 7.5 on the host.

NOTE: UAM 7.5 is not compatible with AppManager Agent for UNIX.

Workaround: For instructions on managing the AppManager Agent for UNIX installations on the hosts where Security Agent for UNIX 7.5 is also installed, use the procedure, Installing Locally on a UNIX or Linux Computer in *NetIQ AppManager for UNIX and Linux Servers Management Guide*. (Bug 1001277)

4.16 Issues with UNIX Agent Version 7.4

The following are known issues with version 7.4 of the UNIX agent:

- If the Change Guardian Server is running in FIPS mode, version 7.4 of the UNIX agent cannot register with the Change Guardian Policy Repository. (Bug 948202)
- When you are creating a policy, if you browse to a UNIX agent that is version 7.4 or older, you will receive a `Could not connect to UNIX Data Source` error. You can avoid this error by manually entering the file paths in the policy. To find the file paths, log on to the UNIX or Linux computer you want to monitor, and then use the `cd` and `ls` commands. (Bug 953718)
- If you are using a version of the UNIX agent released prior to December 2015, the Policy Name and Policy ID fields on UNIX events are blank. Functionality that uses the information in these fields, such as alerts, does not work. (Bug 906274)

5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

6 Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.