Release Notes

Published
2022-05-02

JSA 7.5.0 Update Package 1 SFS

Juniper Networks | Engineering Simplicity

Table of Contents

Installing the JSA 7.5.0 Update Package 1 Software Update | 1

Installation Wrap-up | 3

Clearing the Cache | 4

Known Issues and Limitations | 4

Resolved Issues | 5

Installing the JSA 7.5.0 Update Package 1 Software Update

JSA 7.5.0 Update Package 1 resolves reported issues from users and administrators from previous JSA versions. This cumulative software update fixes known software issues in your JSA deployment. JSA software updates are installed by using an SFS file. The software update can update all appliances attached to the JSA Console.

The 7.5.0.20220215133427 SFS file can upgrade the following JSA versions to JSA 7.5.0 Update Package 1:

- JSA 7.3.2 (Fix Pack 3 - Fix Pack 7)
- JSA 7.3.3 (GA - Fix Pack 10)
- JSA 7.4.0 (GA - Fix Pack 4)
- JSA 7.4.1 (GA - Fix Pack 2)
- JSA 7.4.2 (GA - Fix Pack 3)
- JSA 7.4.3 (GA - Fix Pack 4)
- JSA 7.5.0 (GA)

This document does not cover all the installation messages and requirements, such as changes to appliance memory requirements or browser requirements for JSA. For more information, see the Juniper Secure Analytics Upgrading JSA to 7.5.0.

Ensure that you take the following precautions:

- Back up your data before you begin any software upgrade. For more information about backup and recovery, see the Juniper Secure Analytics Administration Guide.
- To avoid access errors in your log file, close all open JSA webUI sessions.
- The software update for JSA cannot be installed on a managed host that is at a different software version from the Console. All appliances in the deployment must be at the same software revision to update the entire deployment.
- Verify that all changes are deployed on your appliances. The update cannot install on appliances that have changes that are not deployed.
- If this is a new installation, administrators must review the instructions in the Juniper Secure Analytics Installation Guide.

To install the JSA 7.5.0 Update Package 1 software update:

1. Download the 7.5.0.20220215133427 SFS from the Juniper Customer Support website.
   https://support.juniper.net/support/downloads/
2. Using SSH, log into your system as the root user.
3. To verify you have enough space (5 GB) in **/store/tmp** for the JSA Console, type the following command:

   df -h /tmp /storetmp /store/transient | tee diskchecks.txt

   - Best directory option: **/storetmp**

     It is available on all appliance types at all versions. In JSA 7.5.0 versions /store/tmp is a symlink to the /storetmp partition.

   If the disk check command fails, retype the quotation marks from your terminal, then re-run the command. This command returns the details to both the command window and to a file on the Console named diskchecks.txt. Review this file to ensure that all appliances have **at minimum 5 GB of space available in a directory to copy the SFS** before attempting to move the file to a managed host. If required, free up disk space on any host that fails to have less than 5 GB available.

   NOTE: In JSA 7.3.0 and later, an update to directory structure for STIG compliant directories reduces the size of several partitions. This can impact moving large files to JSA.

4. To create the **/media/updates** directory, type the following command:

   mkdir -p /media/updates
5. Using SCP, copy the files to the JSA Console to the **/storetmp** directory or a location with 5 GB of disk space.
6. Change to the directory where you copied the patch file.

   For example, **cd /storetmp**
7. Unzip the file in the **/storetmp** directory using the bunzip utility:

   bunzip2 7.5.0.20220215133427.sfs.bz2
8. To mount the patch file to the /media/updates directory, type the following command:

   mount -o loop -t squashfs /storetmp/7.5.0.20220215133427.sfs /media/updates
9. To run the patch installer, type the following command:

   /media/updates/installer

   NOTE: The first time that you run the software update, there might be a delay before the software update installation menu is displayed.

10. Using the patch installer, select **all**.

- The **all** option updates the software on all appliances in the following order:
  - Console
  - No order required for remaining appliances. All remaining appliances can be updated in any order the administrator requires.
- If you do not select the **all** option, you must select your console appliance.

  As of the JSA 2014.6.r4 patch and later, administrators are only provided the option to update **all** or update the Console appliance. Managed hosts are not displayed in the installation menu to ensure that the console is patched first. After the console is patched, a list of managed hosts that can be updated is displayed in the installation menu. This change was made starting with the JSA 2014.6.r4 patch to ensure that the console appliance is always updated before managed hosts to prevent upgrade issues.

  If administrators want to patch systems in series, they can update the console first, then copy the patch to all other appliances and run the software update installer individually on each managed host. The console must be patched before you can run the installer on managed hosts. When updating in parallel, there is no order required in how you update appliances after the console is updated.

  If your Secure Shell (SSH) session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the patch installation resumes.

Installation Wrap-up

1. After the patch completes and you have exited the installer, type the following command:

   umount /media/updates

2. Clear your browser cache before logging in to the Console.
3. Delete the SFS file from all appliances.

Result

A summary of the software update installation advises you of any managed host that were not updated. If the software update fails to update a managed host, you can copy the software update to the host and run the installation locally.

After all hosts are updated, administrators can send an email to their team to inform them that they will need to clear their browser cache before logging in to the JSA.

Clearing the Cache

After you install the patch, you must clear your Java cache and your web browser cache before you log into the JSA appliance.

Before you begin

Ensure that you have only one instance of your browser open. If you have multiple versions of your browser open, the cache might fail to clear.

Ensure that the Java Runtime Environment is installed on the desktop system that you use to view the user interface. You can download Java version 1.7 from the Java website: http://java.com/.

About this task

If you use the Microsoft Windows 7 operating system, the Java icon is typically located under the Programs pane.

To clear the cache:

1. Clear your Java cache:
   a. On your desktop, select **Start** > **Control Panel**.
   b. Double-click the Java icon.
   c. In the Temporary Internet Files pane, click **View**.
   d. On the Java Cache Viewer window, select all **Deployment Editor entries**.
   e. Click the Delete icon.
   f. Click **Close**.
   g. Click **OK**.
2. Open your web browser.
3. Clear the cache of your web browser. If you use the Mozilla Firefox web browser, you must clear the cache in the Microsoft Internet Explorer and Mozilla Firefox web browsers.
4. Log in to JSA.

Known Issues and Limitations

The known issues addressed in the JSA 7.5.0 Update Package 1 are listed below:

- When you upgrade to JSA 7.5.0 Update Package 1, the hostcontext service might not start properly, because of signing issues in the JCE Policy files.
- If your network connection is behind a firewall, the App Host is unable to communicate with your Console.

  There is no workaround currently.
- After you install JSA 7.5.0, your applications might go down temporarily while they are being upgraded to the latest base image.
- '9804.install' fails when managed host is removed from deployment before upgrading to JSA 7.5.0.
- If you have WinCollect 7.3.xx installed when you upgrade to JSA 7.5.0, the JSA patch pre-test can fail when the check_yum.sh pre-test does not clean out the old yum cache.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 1 are listed below:

- CVE-2021-3712-OpenSSL as used by JSA is vulnerable to information disclosure.
- CVE-2021-4034-Polkit as used by JSA is vulnerable to privilege escalation.
- CVE-2021-44790, CVE-2021-34798, and CVE-2021-39275-Apache HTTP server as used by JSA is vulnerable to buffer overflow and denial of service.
- Uninstalling a content pack can cause rules to not function as expected.
- Installing a new version of an app can leave the old version still installed and running.
- JSA error when attempting to execute a long AQL query.
- Asset Profiler Configuration ‘Use Advanced’ option changes new input values to a value of zero (0).
- Asset Profiler treats hostnames with different cases (upper and lower) as separate assets.
- Blank Operating System (OS) field displayed for imported assets where the OS is unknown to JSA.
- Attempting to perform a clean vulnerabilities can fail due to a timeout in the backend.
- The clean vulnerabilites function does not work as expected for assets that do not have an IP address configured.
- Updating an asset using the JSA API when the asset has no IP address defined fails with an 'Illegal Argument Exception'.

- Restore fails when deployment configuration is not auto selected when asset data is being restored.
- The Health Metrics log source name from a configuration backup overwrites the new Console's hostname in the log source.
- Hostcontext out of memory can occur when a large certificate revocation list exists.
- Httpd service can fail to start if an issue occurs while installing a new certificate using **install-ssl-cert.sh**.
- Content Management Tool import can change some properties causing saved searches to fail.
- “Optimized” custom event property with different expression types do not properly parse.
- CEP parsing breaks when obfuscation is activated and the CEP has force parsed enabled.
- Regex based data obsfuscation only obfuscates the first data match, not all data matches.
- Event payloads fail to parse correctly when the payload ends in a quotation mark preceded by a space.
- Glusterfs migration manager can fail during rsync of data back to the /store partition.
- Glusterfs migration tool fails when the /store partition encountered is in ext4 format.
- Flows can stop being received by JSA when the ‘FlowGovernor’ experiences a block while trying to connect to ecs-ec process.
- Flow processor process fails to start when the RPM database contains corruption.
- Unable to retrieve maxmind geolite2-city.mmdb updates using a configured proxy in JSA.
- Benign message written to JSA logging on HA secondary: **“[WARN] HA is active but this is not the active box. exiting...”**.
- High Availability Secondary in ‘offline’ state when it is rebooted a few minutes after the Primary during patch process.
- Shutting down the system on a new ISO install before the license agreement causes setup to fail when the system is powered up.
- QNI attempt to connect to license.xforce-security.com after a decapper ran Out Of Memory.
- An API error is generated while using the Log Source Management app when configured to use the ‘norsk (Norge)’ locale in JSA.
- 'An unexpected API error has occurred. please refer to the JSA error logs' when using Log Source Management app.

- Log Source Identifier column displays "N/A" when selected in a log activity page search.
- Intermittent JSA System Notifications 'Time Syncronization has failed - socat failed to initialize' when encryption enabled.
- The offense API updates the offense in the database but the offense manager is not aware of it.
- The JSA Offense model can experience reduced responsiveness after an update is made to a large network hierarchy.
- Flow Processor can sometimes stop processing IPFIX packets sent from QRadar Network Insights.
- Source and destination payloads for ICMP traffic fail to be captured by QRadar Network Insights.
- JSA deploy function can fail to QRadar Network Interface (QNI) appliances after patching.
- Incident Results window can take longer than expected to load.
- Two QNI Tika instances can start on the same port due to a race condition causing repeated messages written to JSA logs.
- Performing a Forensics Recovery can appear to succeed when the task failed silently and never started.
- Higher than expected CPU usage on QRadar Network Insights.
- JSA Risk Manager can display a confirmation message during device import when the devices are not imported.
- JSA Vulnerability Manager report in xls format can fail due to ‘NumberFormatException’.
- System Notification stating QVM processor failure to start can be caused by checkQRMLIcenseTrigger in db table.
- Scheduled reports can run on raw data causing them to fail or take longer than expected to complete.
- Routing rule filters drop down list does not reload appropriate options when toggling between online and offline.
- Routing rules with a filter containing a trailing backslash are not editable once saved.
- AQL custom event properties in email templates display as ‘N/A’ after patching to JSA 7.4.3 or newer.
- Dependent rules are not displayed when reference sets are used in an AQL or ariel filter test in a custom rule.
- Rule owner can fail to be reassigned after a user is deleted.

- Corrupt reference data table can cause the rule wizard to fail to work as expected.
- Rule Response email fails to be sent due to “&” (ampersand) symbol in email address being changed to “&”.
- Rules can fail to work as expected due to the accumulator process failing to connect to ecs-ep process.
- When modifying geographic rule conditions under the Spanish locale Belarus is shown as Brasil instead of Bielorrusia.
- Rules can be incorrectly generated in deployments where dual stack is configured and a JSA patch has been applied.
- JSA User Interface rules page can take longer than expected to load.
- JSA Vulnerability Manager (QVM) scan status remains at 'Outside Operational Window' after scan completes.
- When the QVM processor is not running on the console, scan start and stop emails contain incorrect data in subject and body.
- Error message generated in the UI when a security admin attempts to view another user’s saved search results.
- Offenses without naming cannot be searched by description.
- Unable to delete an empty Log Source Group due to dependency check fail.
- "Software Install" JSA Event Collector or DataNode can fail to start required services after added to JSA deployment.
- A JSA notification is generated when the autogenerated QRadar_SAML certificate cannot be renewed.
- Notification of dropped flows is not occurring in JSA notifications.
- JSA patching can fail if duplicate IP addresses are present in database table.
- JSA “patch successful with errors” failing on “...9804.install” file.
- JSA patching process can fail on destination site when the Data Sync app is installed.
- JSA patch pre-test can fail due to check_yum.sh issues when WinCollect 7.3.1-16 installed.
- '[Warning] all applicable hosts have migrated from glusterfs to drbd. exiting' when running glusterfs to DRBD migration tool.