Release Notes

Published
2025-09-07

JSA 7.5.0 Update Package 13

Table of Contents

Installing the JSA 7.5.0 Update Package 13 Software Update | 1

Installation Wrap-up | 4

Clearing the Cache | 4

Known Issues and Limitations | 5

Resolved Issues | 6

Installing the JSA 7.5.0 Update Package 13 Software Update

JSA 7.5.0 Update Package 13 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 7.5.0.20250718011446.sfs file can upgrade the following JSA versions to JSA 7.5.0 Update Package 13:

- JSA 7.5.0 Update Package 10 SFS
- JSA 7.5.0 Update Package 10 Interim Fix 01
- JSA 7.5.0 Update Package 10 Interim Fix 02
- JSA 7.5.0 Update Package 11 SFS
- JSA 7.5.0 Update Package 11 Interim Fix 01
- JSA 7.5.0 Update Package 11 Interim Fix 02
- JSA 7.5.0 Update Package 11 Interim Fix 03
- JSA 7.5.0 Update Package 11 Interim Fix 04
- JSA 7.5.0 Update Package 12 SFS
- JSA 7.5.0 Update Package 12 Interim Fix 03

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 13 software update:

1. Download the 7.5.0.20250718011446.sfs from the Juniper Customer Support website.
2. Using SSH, log into your system as the root user.
3. To verify you have enough space (10 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.
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 10 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 7.5.0.20250718011446.sfs.bz2
8. To mount the patch file to the /media/updates directory, type the following command:

   mount -o loop -t squashfs /storetmp/7.5.0.20250718011446.sfs /media/updates
9. To run the patch installer, type the following command:

   /media/updates/installer
10. From the patch installer menu, you can upgrade your JSA products by using Legacy Patching (Sequential) or Parallel Patching. For more information, see Upgrading JSA by using Parallel Patching.
11. During installation, the users will be prompted with the following questions. You can confirm the action and continue patching.

```
This patch introduces a kernel RPM update.

Please note that if you continue with the patch and the kernel is upgraded:
* This system is restarted automatically after patch installation is complete.
* On all managed hosts patched from the Console, a restart occurs automatically after patch
```

```
installation is complete.



Do you wish to continue? (Y/N):
```

```
Ensure that all apps on your system are updated before you update QRadar. Out-of-date apps
might not work after you install this update.

Do you want to continue, or abort the patch?
Choices:
1) Yes, my apps are up-to-date and I want to continue.
2) No, abort the patch so I can update my apps.
```

```
An update for the event collection service is available.

Currently Running Version: 2021.6.8.20240302192142
New Available Version: 2021.6.13.20250718011446

Applying the update requires the event collection service to restart, which could result in
a gap in data collection.
You can continue to use the version that you are currently running, and update to the new
version later.
For more information about manually updating the event collection service, see the IBM
Security QRadar Administration Guide.

Note: The option that you choose is applied to all managed hosts that are patched from this
QRadar console.

Choices:
1) Update and restart the event collection service now.
2) Continue using the current version of the event collection service for now. Update the
event collection service during the next restart.
3) Abort patch
```

12. After the patch installation is complete, reboot the system.
13. 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.

  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.

Results

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 13 are listed below:

- Hostcontext error visible in the logs when creating backup on the ui on backup and recovery.
- SAML IdP server metadata generator page is not getting Open from Browser URL for JSA IPV6 environment.
- Data Sync App - Software Install setup : Apps Restore functionality showing validation and Failover is not getting initiated in the new DSApp v3.2.2.

Resolved Issues

The known issues resolved in the JSA 7.5.0 Update Package 13 are listed below:

- If the "JSA" postgresql database is in use during a configuration restore, it can cause the restore to fail, invalidating the database.
- podman_apps_registry_restore.sh stuck when registry keystore is broken.
- Reference set "does not exist in any/all of" filters return incorrect search results.
- Ariel queries with a criteria involving indexed properties open data files in cases where it should not, reducing search speed.
- 'Accumulator falling behind' notifications after default global views for event rate and flow rate have been recreated.
- Warning message " /opt/qradar/bin/setComponentThreadSchedulerPolicy.sh: failed to set scheduler.
- Ariel out of memory due to map failed.
- F5 networks big-ip apm events can display 'parsed but not mapped' in DSM Editor.
- Linux OS and McAfee ePolicy Orchestrator, TLS Syslog, some events parsing correctly in log activity but display as unknown in the DSM Editor.
- VMWare VCenter events show parsed but not mapped in DSM editor.
- The Event Id and Event Category values are not automatically populated in the 'Create a New Event Mapping' dialog box for some DSMs.
- Suggest Regex feature in DSM Editor does not work unless the user role is set to Admin.
- High Availability setup may fail on systems with very large drives.
- High availability setup can fail or take an excessive amount of time to complete on hosts with large /store filesystems.
- JSA Trend Micro Deep Discovery Director and Inspector event mapping issue.
- JSA hosts installed using a RHEL8-based ISO and legacy BIOS cannot reinstall using the recovery ISO.
- Parallel Patch -l option (limit bandwidth) not applied.
- qradarca-monitor restarts services every hour when expiring cert is skipped for regeneration.

- Upgrading JSA environment on appliance installs in High Availability to 7.5.0 Update Package 11 can cause the secondary to fail.
- Update Package 11 : Export as Building Block is not visible in rule wizard in light mode.
- Search Parameter section in Edit or New Search has buttons covering items in some cases in Dark Mode.
- CEP (Custom property) cache issues when a system has over 1000 properties.
- Header text is not visible in Offenses -> Rules table for Dark theme.
- Some appliance are now getting a timebomb license with a month expiration.
- License is over allocated after patching to Update Package 11 with software ECs with QVM Scanners.
- Backup failing after upgrade to Update Package 12 or Update Package 12 Interim Fix 01.
- Time_sync.sh can fail to complete successfully if socat takes longer than 0.5 seconds to connect.
- French language symantec endpoint protection events do not display as expected in the dsm editor.
- Report wizard can be unexpected. Select the csv format when users click the back button.
- Connection lost from EC to EP: Channel key IO Error.