Release Notes

Published
2025-11-24

JSA 7.5.0 Update Package 14

Table of Contents

What's New in JSA 7.5.0 Update Package 14

The new feature addressed in JSA 7.5.0 Update Package 14 are listed below:

Support for Tiered Storage

A new approach to managing JSA (Ariel) data that improves search performance and cost of ownership and includes.

- Hot and Warm Tiers: Newly ingested data is stored in the Hot tier for fast access and is automatically migrated to the Warm tier as it ages, based on a defined data migration policy.
- Improved Performance and Efficiency: By keeping recent data readily accessible and moving older data to more cost-effective storage, Tiered Storage helps balance search speed, cost, and deployment footprint.

Improved Performance in the Pipelines (Parsing, CRE) to Reduce Routing to Storage

JSA is now smarter when making the routing to storage decisions in the data processing pipeline, accounting for the processing utilization of the Parsing and CRE data processing thread pools, significantly reducing false-positive routing to storage and increasing the security posture by reducing the number of unparsed and uncorrelated events.

Improved event/flow burst handling capability on services startup

The JSA data processing pipeline services now allocate process memory on startup, improving performance and stability of those real-time processes. This improves handling of event spikes after services startup.

LVM Phase 2

This release introduces enhancements focused on improving the management of Logical Volume Management (LVM) on appliance-installed systems. The key areas of improvements are enabling LVM expansion for appliance installations.

Enhanced Visibility and user experience for Custom AQL Queries in Managed Search Results

In previous JSA versions, custom AQL searches on the Managed Search Results screen were labeled generically as "Custom AQL Query", with no visibility into the actual query logic until the user clicked into the search. This enhancement improves usability by:

- Replacing the generic name, "Custom AQL Query", with the actual AQL query string for custom AQL searches
- Displaying the full AQL query in a tooltip on hover
- Adding a Copy to Clipboard button for quick and easy reuse.

These improvements streamline the user experience and make working with custom AQL searches more efficient.

Managed Search Results Enhancements

The Managed Search Results screen now includes visual indicators for searches that may be slow, expensive and degrade system efficiency including:

- Non-Indexed Fields: Searches that do not utilize indexed fields are flagged to highlight potential performance bottlenecks.
- Pattern matching usage without additional filters: Searches using strictly the "payload contains" or "payload matches" operations are flagged due to their inefficiency and potential high resource consumption

These indicators help users identify and revise inefficient queries, promoting best practices for building performant searches.

Version History for Rules

This enhancement gives you the flexibility to revert changes to any previous version of a rule not just the original, making it easier to manage updates and recover from mistakes. You can now see who made changes, what was changed, and when, giving your team full visibility into rule modifications. Authors also have the option to add a brief note explaining the reason for each change, helping everyone stay aligned and informed. These updates are automatically tracked and displayed, so you don't need to modify your existing notes. This release brings greater transparency, accountability, and control to how your rules change over time.

Offence Enhancements: Rule Test Filter by Magnitude Value

You can now set magnitude thresholds when creating rule tests. This helps you prioritize offenses based on their criticality making it easier to focus on the most important threats and respond faster.

Enhanced Offences Tracking

This update tracks only the most recent time an offense was assigned to a user along with the assignment timestamp.

JSA (Flow Processor) - Autonomous System Number (ASN) information

Flow Processor now automatically enriches network flows with Autonomous System Number (ASN) information. The ASN field is now populated, increasing an analyst’s ability to determine the origin of IP traffic. Now, JSA automatically performs ASN lookups, providing valuable context such as the network or ISP associated with each IP address. Benefits are to:

- Gain immediate visibility into the ownership and origin of IP traffic
- Quickly identify traffic from suspicious or high-risk networks

- Eliminate the need for manual ASN enrichment
- Enhance correlation rules and threat detection with enriched flow metadata

This improvement helps security teams respond faster, improve triage accuracy, and align with modern SIEM expectations for enriched, actionable data.

JSA Risk Manager Supports Check Point HTTPS integration

JSA Risk Manager now receives firewall rule event logs directly from Check Point Security Management Servers (SMS). This enhancement enables real-time monitoring of firewall rule event counts, helping customers manage and optimize the effectiveness of their firewall rule policies across all managed devices. Benefits are:

- Identify most and least used Checkpoint HTTPS firewall rules
- Detect rules that may unnecessarily block network access
- Highlight frequently triggered rules that may impact performance
- View detailed rule event data for analysis
- Schedule reports to improve policy management and visibility

This helps users to monitor and optimize Check Point firewall rules in real time for improved security and network efficiency.

Installing the JSA 7.5.0 Update Package 14 Software Update

JSA 7.5.0 Update Package 14 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 7.5.0.20251017194912.sfs file can upgrade the following JSA versions to JSA 7.5.0 Update Package 14:

- 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
- JSA 7.5.0 Update Package 13 SFS
- JSA 7.5.0 Update Package 13 Interim Fix 01
- JSA 7.5.0 Update Package 13 Interim Fix 02

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 14 software update:

1. Download the 7.5.0.20251017194912.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 7.5.0.20251017194912.sfs.bz2

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

   mount -o loop -t squashfs /storetmp/7.5.0.20251017194912.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: 2021.6.8.20250718011446
New Available Version: 2021.6.13.20251017194912

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 14 are listed below:

- LVM warning menu should not show up on MH that is not configured with LVM.
- Field extraction based on custom property only extracts the last part of the value when space exists in value.

Resolved Issues

The known issues resolved in the JSA 7.5.0 Update Package 14 are listed below:

- Offense rule email will not work in Update Package 13 because of duplicate common-lang3 jar in ecs-ep pipeline.
- Forwarding events over TLS may cause an error after upgrading to Update Package 12: Selective Forwarding can trigger 'too many open files' errors and events are not forwarded.
- Data Sync App - Software Install setup : Apps Restore functionality showing validation and Failover is not getting initiated in the new DSApp v3.2.2.
- Known_hosts file on managed hosts is being cleared.
- Ariel out of memory due to map failed.

- Risk Manager rule counting for Check Point not working.
- JSA Update Package 12 Java 11 warning messages on accumulator_rollup.
- Connection lost from EC to EP: Channel key IO Error.
- AppFW health check time attributes in nva.conf are not honored.
- JSON property extraction does not work with stringify nested objects .
- Applications that uses CentOs and Python2.x base image will not work on JSA.
- Deployment Configuration option can be inadvertently disabled in config restore page.
- Config restore page checkboxes are not being checked automatically.
- Flow processor always consumes a full CPU, even when not doing any work.
- Missing entry in /etc/hosts since change to podman causes unnecessary DNS requests.
- JSA GUI is displaying wrong time on console using Africa/Cairo timezone.
- DSM Editor not parsing if JSON Keys have '\' (backslash) for escape characters.
- Administrators cannot change the day auto updates runs when the schedule is monthly.
- Assets details UI can display multiple instances of the same IPv6 address.
- Administrators can unexpectedly restore a data synchronization application-initiated backup from the admin tab.
- Restoring a nightly config backup fails as deselecting license incorrectly unchecks deployment configuration.
- Auto updates can generate 'could not apply qidmap update with serial xxxxxxxxx' errors.
- System monitoring dashboard `eps/fpm` graphs might not display as expected due to a multikey creator expression predicate exception.