Release Notes

Published
2024-08-27

JSA 7.5.0 Update Package 8 SFS

Table of Contents

Installing the JSA 7.5.0 Update Package 8 Software Update

JSA 7.5.0 Update Package 8 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 7.5.0.20240302192142.sfs file can upgrade the following JSA versions to JSA 7.5.0 Update Package 8:

- JSA 7.5.0 Update Package 7 SFS
- JSA 7.5.0 Update Package 7 Interim Fix 1
- JSA 7.5.0 Update Package 7 Interim Fix 2
- JSA 7.5.0 Update Package 7 Interim Fix 3
- JSA 7.5.0 Update Package 7 Interim Fix 4
- JSA 7.5.0 Update Package 7 Interim Fix 5
- JSA 7.5.0 Update Package 7 Interim Fix 6

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 8 software update:

1. Download the 7.5.0.20240302192142.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 (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 7.5.0.20240302192142.sfs.bz2
8. To mount the patch file to the /media/updates directory, type the following command:

   mount -o loop -t squashfs /storetmp/7.5.0.20240302192142.sfs /media/updates
9. To run a Leapp preset, type the following command:

   /media/updates/installer --leapp-only
10. To run the patch installer, type the following command:

    /media/updates/installer
11. 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 8 are listed below:

- VMWare upgrades do not complete successfully due to an mtpbase driver issue.
- WinCollect 7.3.1-43 upgrade fails.
- Upgrading to JSA 7.5.0 Update Package 8 or later in high availability systems may initiate a full DRBD re-sync.
- Upgrading to JSA 7.5.0 Update Package 8 from JSA version 7.2.x can fail due to insufficient disk space.
- The e1000 network driver is not supported in Red Hat Enterprise Linux 8.
- Upgrades to JSA 7.5.0 Update Package 8 can hang in environments using network address translation (NAT).
- NAT deployments fail as leapp-only pretests do not verify public IPs.
- After you upgrade to JSA 7.5.0 Update Package 5, WinCollect 7.X agents can experience management or configuration change errors.
- Upgrades to JSA 7.5.0 Update Package 8 can hang in environments using network address translation (NAT).
- NAT deployments fail as leapp-only pretests do not verify public IPs.

- After you upgrade to JSA 7.5.0 Update Package 5, WinCollect 7.X agents can experience management or configuration change errors.
- After you upgrade to JSA 7.5.0 Update Package 8 with SSH, CLI session is down temporarily.
- Upgrading to RHEL-8 on systems with LUKS encrypted partitions is not supported.
- HA host status does not update during the sync process.

  NOTE: In JSA 7.5.0 Update Package 8, administrators with High Availability (HA) appliances in their deployment must complete a post-installation step. For more information, see KB80989.

- Leapp pretests do not verify sufficient disk space.
- Leapp pretests are not supported on HA secondaries.
- Leapp pretests are not supported on JSA 7.5.0 Update Package 7 ISO installations.
- Leapp pretests are not supported on detached console HA.
- Leapp pretests fail due to multiple physical network interface configurations.
- Upgrade patch pretest fails on dual stack.
- Cannot send udp syslog to QRADAR_CONSOLE_IP from app container on an AppHost.
- Duplicate app entries on Traefik when JSA console is powered off and on again.
- Factory reinstall on JSA 7.5.0 Update Package 8 in the recovery partition fails.
- Managed WinCollect 7 agents cannot receive updates from encrypted JSA Managed Hosts with 7.5.0 Update Package 7 Interim Fix 05 and later.
- Error messages appear during decapper startup in JSA Network Insights.
- Cert file /etc/httpd-qif/tls/httpd-qif.cert fails the key modulus check in JSA 7.5.0 Update Package 8.
- RHEL 8.8 - scaserver does not start after system reboot.
- HA pairing on JSA console fails when Network File System (NFS) is configured on the JSA 7.5.0 Update Package 8 install.
- The patch installation is not complete due to memory dumps in **/store/jheap**.

  Workaround:

  Run the following command to remove the dump files, and then run the upgrade again.

 # rm -rf /store/jheap/ccpp*

- JSA 7.5.0 Update Package 8 users with WinCollect 7 must update to the latest version. If you upgrade to JSA 7.5.0 Update Package 8 and have WinCollect 7.x agents deployed in managed mode, you must install the WinCollect 7.3.1-43 SFS file.
- Apps might go down during the base image update.
- Issue adding Data Nodes to a cluster.
- Upgrade from 7.5.0 Update Package 7 to 7.5.0 Update Package 8 version failed for console and managed hosts.

  For more information, see KB82902.
- When patching to 7.5.0 UP8, the RHEL8 Leapp migration script fails to remove the mptbase kernel module on VMware hosts.

  For workaround, see Juniper Customer Support.
- Upgrading to JSA 7.5.0 Update Package 8 will fail on virtual hosts using an e1000 NIC adapter.

  For workaround, see Juniper Customer Support.
- DNS Analyzer app version 2.0.1 failed to install on JSA 7.5.0 Update Package 8.

  For workaround, see Juniper Customer Support.
- Database replication and deploys can fail due to a column sizing issue in the database.

  For workaround, see Juniper Customer Support.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 8 are listed below:

- Unbound-anchor.service is reaching out publicly to DNS root servers.
- False-positive offenses are produced after the restart of ecs-ep process.
- Null Pointer Exception in Regex Monitor causes perfromance issues in event parsing.
- Re-adding a managed host can appear to be hung at the final step in the 'Host is Being Added to Deployment' window.
- False Positive offenses produced where rules use reference set not conditions.

- Unknown offense created on destination JSA when forwarding normalized data from Source JSA.
- Dropped events in log source protocol queue after upgrade to JSA 7.5.0 Update Package 7.
- CRE Rule seems to be affecting the parsing of ADE AQL Properties.
- The managed search results page can be slow to load in JSA environments with a large amount of Ariel query handles.
- JSA - High availability crossover enable fails with ssh StrictHostKeyChecking.
- JSA 7.5.0 Update Package 7 Interim Fix 03 Java change causes Amazon Web Service Log Source Type to stop working.
- Retain option available on freshly installed High Availability (HA) systems from factory reinstall.
- Time server set during initial installation reset after running qchange.
- HA Setup fails with "failed to change group ownership error".
- JSA tunnel-monitor service incorrectly attempts to create connections from HA standby appliances.
- Common rule test 'Event or flow processed by custom rules engine' can display a Number Format Exception.
- When AQL properties created before JSA 7.4.3 exist in the forwarding profile, offline forwarding is slow.
- Invalid byte sequence for encoding "UTF8" while accessing reference data API or UBA import user.
- Historical correlation offense summary page can display a 'file access error' when viewing grouped events.
- STIG hardening on JSA 7.5.0 Update Package 7 might not set a boot password, forcing a reinstall.
- HA Secondary disk space issues can occur when files for older versions of ECS are not removed.
- Hostcontext can exceed the default 256MB allocation, leading to out of memory issues on hosts.
- Custom rules: Match count rules do not trigger as expectedly when used with coalescing log sources.
- Log File protocol configured to connect with SFTP can stop collecting events unexpectedly in JSA 7.5.0 Update Package 7.
- Rule Wizard displays a blank pop up for the 'Name of the flow source is one of these sources' test.
- Asset details window does not display the latest email address when changed.
- Reference Table value incorrectly displayed in the rule responses of the Rule Wizard when edited.

- JSA Applications failing to install/update after upgrading to JSA 7.5.0 Update Package 6.
- Rule Wizard displays 'The response count must be 0 or greater' when enabling response limiters with non-english UI locales.
- Nightly backups fail if applications are in error status.
- Rule "Source/Destination asset weight is low" can trigger when weight is higher than the defined parameter.