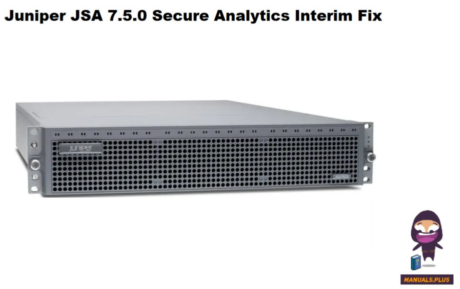

Juniper JSA 7.5.0 Secure Analytics Interim Fix Instruction Manual

Contents

Juniper JSA 7.5.0 Secure Analytics Interim Fix

Product Information

The JSA 7.5.0 Update Package 8 Interim Fix 02 is a software update that resolves reported issues from users and administrators of previous JSA versions. It is a cumulative software update that fixes known software issues in your JSA deployment. This update can be used to upgrade the JSA version to 7.5.0 Update Package 8 Interim Fix 02.

Precautions:
Before installing the update, ensure that you have enough space available and follow the precautions mentioned in the user manual.

Specifications:

- **Product Name:** JSA 7.5.0 Update Package 8 Interim Fix 02
- **Release Date:** May 27, 2024

Installation Instructions:

1. Download the 7.5.0.20240429142841.sfs file from the Juniper Customer Support website.
2. Using SSH, log into your system as the root user.
3. Verify you have enough space (10 GB) in /store/tmp for the JSA Console using the command: df -h /tmp /storetmp /store/transient | tee diskchecks.txt

Installation Wrap-up:

1. After the patch completes and you have exited the installer, type the command: umount /media/updates

Clearing the Cache:

1. Select Start > Control Panel on your desktop.
2. Double-click the Java icon.
3. In the Temporary Internet Files pane, click View.
4. Select all Deployment Editor entries on the Java Cache Viewer window and click the Delete icon.
5. Open your web browser and clear the cache.
6. Log in to JSA.

FAQ:

- **Known Issues and Limitations:**
  If there are any known issues or limitations with the Update Package 8 installation, refer to the product documentation for more information.
- **Resolved Issues:**
  If you encounter any issues during or after the update installation, please refer to the resolved issues section in the product documentation for troubleshooting steps and information.

Installing the JSA 7.5.0

JSA 7.5.0 Update Package 8 Interim Fix 02 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 7.5.0.20240429142841.sfs file can upgrade the following JSA version to JSA 7.5.0 Update Package 8 Interim Fix 02:

- JSA 7.5.0 Update Package 8
- JSA 7.5.0 Update Package 8 Interim Fix 01

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 Interim Fix 02 software update:

1. Download the 7.5.0.20240429142841.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 7.5.0.20240429142841.sfs.bz2
8. To mount the patch file to the /media/updates directory, type the following command: mount -o loop -t squashfs /storetmp/7.5.0.20240429142841.sfs /media/updates
9. To run the Leapp pretest, type the following command: /media/updates/installer –leapp-only
10. 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.

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 issue addressed in the JSA 7.5.0 Update Package 8 Interim Fix 02 are listed below:

- 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 8.
- 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.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 8 Interim Fix 02 are listed below:

- LDAP authentication does not allow the mapping of tenants.
- Data obfuscation can experience performance issues due to empty or null string checking.
- HA synchronization status in 7.5.0 Update Package 8 is not displayed in System and License Management.
- Log sources status column might not update as expected leading to stale or outdated status information.

Documents / Resources

Release Notes Published 2024-05-27 JSA 7.5.0 Update Package 8 Interim Fix 02 SFS	**Juniper JSA 7.5.0 Secure Analytics Interim Fix** [pdf] Instruction Manual JSA 7.5.0, JSA 7.5.0 Secure Analytics Interim Fix, JSA 7.5.0, Secure Analytics Interim Fix, Analytics Interim Fix, Interim Fix, Fix

References

- Downloads
- Juniper Secure Analytics Administration Guide | JSA 7.5.0 | Juniper Networks
- Juniper Secure Analytics Installation Guide | JSA 7.5.0 | Juniper Networks
- Upgrading Juniper Secure Analytics to 7.5.0 | JSA 7.5.0 | Juniper Networks
- User Manual