Juniper 7.5.0 Secure Analytics User Guide

JUNIPer NETWORKS | Engineering Simplicity

Release Notes
JSA 7.5.0 Update Package 7 Interim Fix 05 SFS
Published 2024-02-26

Contents

Installing the JSA 7.5.0 Update Package 7 Interim Fix 05 Software Update

JSA 7.5.0 Update Package 7 Interim Fix 05 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 7.5.0.20240129133209.sfs file can upgrade the following JSA version to JSA 7.5.0 Update

Package 7 Interim Fix 05: · JSA 7.5.0 Update Package 7

- JSA 7.5.0 Update Package 7 Interim Fix 01
- JSA 7.5.0 Update Package 7 Interim Fix 02
- JSA 7.5.0 Update Package 7 Interim Fix 03
- JSA 7.5.0 Update Package 7 Interim Fix 04

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.

To install the JSA 7.5.0 Update Package 7 Interim Fix 05 software update:

1. Download the 7.5.0.20240129133209.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.
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 7.5.0.20240129133209.sfs.bz2
8. To mount the patch file to the /media/updates directory, type the following command: mount -o loop -t squashfs /storetmp/7.5.0.20240129133209.sfs /media/updates
9. To run the patch installer, type the following command: /media/updates/installer
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. 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 7 Interim Fix 05 is listed below:
When a JSA system is being built and a reboot occurs during the install configuration, the User Interface admin password can sometimes fail to be set correctly.
Workaround:
Change the admin account password in the command-line interface.
NOTE: This procedure requires that you restart the Tomcat service and deploy changes, resulting in a temporary loss of access to the JSA user interface while services restart. Administrators can complete this procedure during a scheduled maintenance window as users are logged out, exports in the process are interrupted, and scheduled reports might need to be restarted manually.

If you do not have access to the admin account from the user interface, it can be necessary to change the admin password from the command-line interface.

1. Using SSH, log in to the JSA Console as the root user.
2. To change the admin user password, type:

   ```
   /opt/qradar/support/changePasswd.sh -a
   ```
3. Enter the new password as prompted.
4. Confirm the new password.

   ```
   [root@qr750-3199-29271 ~]# /opt/qradar/support/changePasswd.sh -a Please enter the new admin password.
   Password:
   Confirm password: The admin password has been changed.
   ```
5. To restart the user interface, type: systemctl restart tomcat

   NOTE: This command works on JSA versions at JSA 7.3.x and later.
6. Log in to the user interface as an administrator.
7. Click Admin tab > Advanced > Deploy Full Configuration.

Important: Performing a Deploy Full Configuration results in services being restarted. While services are restarting, event processing stops until services restart. Scheduled reports that are in progress need to be manually restarted by users. Administrators with strict outage policies are advised to complete the Deploy Full Configuration step during a scheduled maintenance window for their organization.
Results: After the service restarts, the admin account password is changed.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 7 Interim Fix 05 are listed below:

- False-positive offenses are produced after the restart of ecs-ep process.
- Re-adding host does not close dialog and does not allow remapping components.
- CRE Rule seems to be affecting the parsing of ADE AQL Properties.

Documents / Resources

 Release Notes Published 2024-02-26 JSA 7.5.0 Update Package 7 Interim Fix 05 SFS Juniper Networks | Engineering Simplicity	Juniper 7.5.0 Secure Analytics [pdf] User Guide 7.5.0 Secure Analytics, 7.5.0, Secure Analytics, Analytics

References

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