JUNIPER NETWORKS 7.5.0 Secure Analytics Instructions

Contents

JUNIPER NETWORKS 7.5.0 Secure Analytics

Product Information

The JSA 7.5.0 Update Package 4 SFS is a software update package for the JSA (Juniper Secure Analytics) product. It was published on May 3, 2023. The update package is compatible with all appliance types and versions of JSA 7.5.0. The update package includes bug fixes, improvements, and new features.

Installing the JSA 7.5.0 Update Package 4 Software Update

JSA 7.5.0 Update Package 4 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 7.5.0.20221129155237.sfs file can upgrade the following JSA versions to JSA 7.5.0 Update Package 4:

- JSA 7.3.2 (GA – Fix Pack 3 and later)
- JSA 7.3.3 (All versions)
- JSA 7.4.0 (All versions)
- JSA 7.4.1 (All versions)
- JSA 7.4.2 (All versions)
- JSA 7.5.0 (All versions)

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 4 software update:

1. Download the 7.5.0.20221129155237 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.
     If the disk check command fails, retype the quotation marks from your terminal, then re-run the command. This command returns the details to both the command window and to a file on the Console named diskchecks.txt. Review this file to ensure that all appliances have at minimum 5 GB of space available in a directory to copy the SFS before attempting to move the file to a managed host. If required, free up disk space on any host that fails to have less than 5 GB available.
     NOTE: In JSA 7.3.0 and later, an update to directory structure for STIG compliant directories reduces the size of several partitions. This can impact moving large files to JSA.

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 7.5.0.20221129155237.sfs.bz2
8. To mount the patch file to the /media/updates directory, type the following command: mount -o loop -t squashfs /storetmp/7.5.0.20221129155237.sfs /media/updates
9. 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.
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. As of the JSA 2014.6.r4 patch and later, administrators are only provided the option to update all or update the Console appliance. Managed hosts are not displayed in the installation menu to ensure that the console is patched first. After the console is patched, a list of managed hosts that can be updated is displayed in the installation menu. This change was made starting with the JSA 2014.6.r4 patch to ensure that the console appliance is always updated before managed hosts to prevent upgrade issues.

      If administrators want to patch systems in series, they can update the console first, then copy the patch to all other appliances and run the software update installer individually on each managed host. The console must be patched before you can run the installer on managed hosts. When updating in parallel, there is no order required in how you update appliances after the console is updated.

      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 4 are listed below:

- It is possible for auto-updates to revert to a previous version of autoupdates after upgrading. This will cause autoupdate to not work as intended. After you upgrade to JSA 7.5.0 or later, type the following command to check your autoupdate version: /opt/qradar/bin/UpdateConfs.pl -v
- Docker services fail to start on JSA appliances that were originally installed at JSA release 2014.8 or earlier, then upgraded to 7.5.0 Update Package 2 Interim Fix 02 or 7.5.0 Update Package 3. Before you upgrade to JSA 7.5.0 Update Package 2 Interim Fix 02 run the following command from the JSA Console: xfs_info /store | grep ftype Review the output to confirm the ftype setting. If the output setting displays “ftype=0”, do not proceed with the upgrade to 7.5.0 Update Package 2 Interim Fix 02 or 7.5.0 Update Package 3. See KB69793 for additional details.
- If your network connection is behind a firewall, the App Host is unable to communicate with your Console. To workaround this issue, remove encryption from the App Host and open the following ports on any firewall between your App Host and Console: 514, 443, 5000, 9000.
- After you install JSA 7.5.0, your applications might go down temporarily while they are being upgraded to the latest base image.
- When adding a Data Node to a cluster, they must either all be encrypted, or all be unencrypted. You cannot add both encrypted and unencrypted Data Nodes to the same cluster.
- Installing High Availability (HA) using JSA 7.5.0 GA can cause the partition layout to be built incorrectly. If you need to rebuild, reinstall, or install an HA appliance, do not use the JSA 7.5.0 GA ISO file. You can download and use the JSA 7.5.0 Update Package 3 ISO, or contact **https://support.juniper.net/support/**.
- After you install the kernel and the reboot is complete, the installer hangs on a hardware check involving Myver and MegaCli.

Resolved Issues

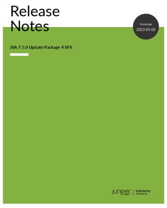
The resolved issues addressed in the JSA 7.5.0 Update Package 4 are listed below:

- ‘Globalview’ AQL (advanced search) function can sometimes fail to return results.
- AQL reference set contains function does not use indexes when reference set is alphanumeric.
- The Analyst Workflow App version 2.31.4 displays an internal server error when default locale is changed.
- App host does not communicate with console correctly when connection is encrypted and has to pass a firewall.
- Buttons added to the user interface by QRadar apps do not respond.
- Duplicate server types in server discovery assets menu.
- Vulnerability records can become orphaned for scanned assets that do not have clean vuln ports configured.
- Asset saved search criteria that is configured as default changes on subsequent result pages.
- Updated rule response is marked blank if modifying all responses.
- Bind credential for LDAP repos clears if saved without successful connection test.
- Modified system building blocks stop matching any events until ecs-ep service is restarted.
- XML custom event properties fail to work as expected for payloads that contain a byte order mark.
- Event processor cre thread unexpectedly shutdown due to AQL custom property with the same name as existing regex custom property.
- Host key verification failed and known_host not updating in encrypted deployment after moving gateway to new event processor.
- Rebalance can lead to a destination host reaching service shutdown due to disk space usage threshold exceeded.
- Deploy changes can error out if the server table has a non fully qualified domain name.
- Deployments with a large number of HA hosts, hostcontext processes might not complete due to the number of managed host.
- Host context timeout due to “file /storetmp/addhost_{host ip}1/status.Txt does not exist” error.
- Unable to add an additional log source to domain after 100 log sources are present.
- JSA patch fails after running the glusterfs_migration_manager on required event collectors.
- Custom property and AQL properties on forwarding profiles are not checked for if they are in use before deletion.
- Stored events that are forwarded using online forwarding go to ‘sim generic’ log source on the receiving JSA system.
- A value of ‘null’ can sometimes be incorrectly displayed in network activity for geographic country/region column.
- High availability (HA) pairing fails when the ip address of the secondary is the same as a deleted managed host.
- Incorrect status for network interfaces can be displayed for high availability host.
- Serial console installations create duplicate entries in grub.
- A JSA “software install” can unexpectedly attempt to run an older ISO installation after reboot.
- Mysql log sources using the jdbc protcol and tls can stop working after 2:00 am.
- QRadar Log Source Management 7.0.7 displays blank page when accessed from the filter panel on the admin page.
- The Log Source Management App might display protocol update alert when the protocol is already the latest version.
- Performance issues can occur when JSA attemps a reload of sensor devices when log sources exceed 2

million.

- Time synchronization can fail on managed hosts.
- Encrypted tunnels between managed hosts can fail to start after patching to JSA 7.5.0 Update Package 1 or later.
- Sorting by column in the offenses tab removes search filters.
- Application error on destination ip validation for incorrect format of IP address.
- The “top 5 source ips” offense emails do not contain the country name.
- ‘Application error’ occurs after an extended period of time when attempting to load the offense page.
- Performance degradation caused by AQL properties parsing on every query.
- “Scheduled adapter backup for device” error message when device added to risk manager with backup option.
- /qrm/srm_update_1138.Sql can cause 7.5.0 Update Package 1 upgrade to fail on hosts where required index doesn’t exist.
- JSA Risk Manager can display a confirmation message during device import when the devices are not imported.
- Error exporting data when filtering from the manage vulnerabilites list.
- JSA Vulnernabiity Manager scan results screen displays ‘could not receive message’ error.
- Chrome and Edge browsers cut off the bottom edge of the report wizard.
- Reports fail to generate with no error in UI.
- Daily or weekly reports generated during daylights savings end 1 hour early.
- Refreshing the page after the changes are made for sharing reporting groups, the changes do not appear to have been saved.
- Rules containing tests against geographic location can sometimes cause issues with cre pipeline performance.
- Rule_id was not found for uuid = system-1151.
- A custom property called ‘hostname’ changes to ‘host name’ when used as a response limiter in the rule wizard.
- Offense rule using ‘and when the destination list includes any of the following A.B.C.D/e’ test with public ip does not trigger.
- Flow ID super index consumes a large amount of storage space.
- Searches using a custom property can be slower to complete than expected.
- Clicking the help icon results in “page not found” for system notification: “the accumulator has fallen behind…”.
- Timezone cannot be changed from UI and system time settings UI tab might fail to load.
- Collation errors in JSA logging occur when JSA is set to some locales.
- The delegated admin role is being created without giving permission for the Log Source Management App.

Documents / Resources

 Release Notes Published 2023-05-03 JSA 7.5.0 Update Package 4 SFS Juniper | Engineering Simplicity	**JUNIPER NETWORKS 7.5.0 Secure Analytics** [pdf] Instructions 7.5.0 Secure Analytics, Secure Analytics, Analytics

References

- java.com/
- Support
- Support
- Downloads
- CEC Juniper Community
- 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