Release Notes

Published
2024-05-14

JSA 7.5.0 Update Package 8 ISO

Table of Contents

Administrator Notes

About this Installation

These instructions are intended to assist administrators when installing JSA 7.5.0 Update Package 8 by using an ISO file. This ISO can install JSA and JSA Risk Manager products to version JSA 7.5.0 Update Package 8.

Installing the JSA 7.5.0 Update Package 8

To install JSA software:

- System Requirements — For information about hardware and software compatibility, see the detailed system requirements in the Juniper Secure Analytics Installation Guide.
- Upgrading to JSA 7.5.0 Update Package 8 — To upgrade to JSA 7.5.0 Update Package 8, see the Upgrading Juniper Secure Analytics to 7.5.0 Guide.
- Installing JSA — For installation instructions, see the Juniper Secure Analytics Installation Guide.

To install the JSA 7.5.0 Update Package 8 ISO:

1. Download the 7.5.0.UP8.iso from the Juniper Customer Support website.
   https://support.juniper.net/support/downloads/
2. Using SSH, log in to the Console as the root user.
3. To run the ISO installer on the Console, type the following command:
   /media/cdrom/setup

   NOTE: Installing JSA 7.5.0 should take approximately 2 hours on a Console appliance.
4. Wait for the Console primary update to complete.

Installation Wrap-up

1. After all hosts are updated, you must clear you browser cache before logging in to the JSA Console.

2. To unmount the `/media/cdrom` directory on all hosts, type:

   /opt/qradar/support/all_servers.sh -C -k “umount /media/cdrom"

3. Delete the ISO file from all appliances.

4. If you use WinCollect agents version 7.2.6 or latest, you must reinstall the SFS file on the JSA Console. This is due to issues where the ISO replaces the SFS on the Console with WinCollect 7.2.5.

5. Review any static routes or customized routing. As mentioned in the administrator notes, all routes were removed and will need to be reconfigured after the upgrade completes.

6. Review any iptable rules that are configured to see if the interface names that have changed in JSA 7.5.0 due to the Red Hat Enterprise 7 operating system updates affect them. Update any iptables rules that use Red Hat 6 interface naming conventions.

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:

- 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.
- 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.
- 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 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.