Release Notes

Published
2024-02-21

JSA 7.5.0 Update Package 5 ISO

Table of Contents

Administrator Notes

About this Installation

These instructions are intended to assist administrators when installing JSA 7.5.0 Update Package 5 by using an ISO file. This ISO can install JSA, JSA Risk Manager, JSA Vulnerability Manager products to version JSA 7.5.0 Update Package 5.

What's New in JSA 7.5.0 Update Package 5

The new feature addressed in JSA 7.5.0 Update Package 5 is listed below:

- The software installation menu will not be visible in the installation wizard by default.

For more information about what's new in JSA 7.5.0 Update Package 5, see What's New Guide.

Installing the JSA 7.5.0 Update Package 5

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 5 — To upgrade to JSA 7.5.0 Update Package 5, 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 5 ISO:

1. Download the 7.5.0.UP5.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.

> **NOTE**: In JSA 7.3.1 Patch 6, a kernel update was introduced to address issues with appliances failing to log in or list unit files. These issues could prevent the appliance from rebooting. This new kernel does not take effect until the appliance is rebooted. You might need to reboot your system manually for the kernel update to take effect.

To work around this issue, you must perform a restart of the appliance. To do this, type the **reboot** command.

Result

A summary of the ISO installation advises you of any issues. If there are no issues, use SSH to log in to the managed hosts and start the installer on each host to run the setup in parallel.

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 5 are listed below:

- Upgrades to 7.5.0 Update Package 5 will overwrite custom cache tuning in **/opt/qradar/conf/spillovercache.properties**. Before performing the upgrade, run the following command to backup the file:

  /opt/qradar/support/all_servers.sh -C cp -p /opt/qradar/conf/spillovercache.properties /root/spillovercahce.properties.bak

  It is possible the threshold values will need to be corrected after the upgrade is completed. Contact Juniper Customer Support for further assistance.

- Upgrades to JSA 7.5.0 Update Package 5 might take an extended amount of time to complete due to glusterfs file cleanup. You must allow the upgrade to continue uninterrupted.

- After upgrading to JSA 7.5.0 Update Package 5, WinCollect 7.X agents can experience management or configuration change errors.

- It is possible for autoupdates 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.

- 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.

- 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 5 are listed below:

- CVE-2022-43863 - JSA is vulnerable to privilege escalation.
- JSA is vulnerable to using components with known vulnerabilities.
- JSA apps can stop running on an app host after it is set up with High Availability (HA).
- Geographic tests performed within JSA can cause performance issues due to XML parsing process.
- JSA dependency checker sometimes does not find dependent rules or building blocks.
- Restored config backups can cause an rpm mismatch between the rpm version of dsm, protocols, vis, and the jars installed.
- When overriding an eventID with two different CEF or LEEF keys using the dsm editor/LSX, only the first is properly parsed.
- The High Availability (HA) restore process allows a primary to be rebuilt as a secondary 500 appliance.
- The value of 'most recent results' in an offense report displays as a negative when using a different user account.
- Logging for tenant filtering only logs one tenant and reports incorrect values.
- 80xx log manager appliance type displays as 'event processor' in system and license management.
- A managed host can fail to inherit the correct license pool allocation when it has been re-added to a deployment.
- Patching from a mounted sfs file in /store is allowed by JSA but can cause high availability patching to fail.
- A non-admin user role user cannot re-assign or move a log source to a different group using the log source management app.
- The JSA pipeline can stop receiving all events due to a stringoutofboundsexception occurring.

- Error written to JSA logging: "There was an error reading authentication.properties. Settings will not be reloaded".
- Repetitive /var/log/audit.log messages being written after a failed protocol test using the log source management app.
- Glusterfs migration or pretest can fail after removing a 15xx appliance from the deployment.
- Replication process can take longer than expected on encrypted hosts after a high availability failover.
- TaskManagementRetentionAgent can overload Tomcat with threads causing it to fail.
- Making a change on a high availability pair can cause an unexpected active node reboot and failover.
- JSA is unable to verify SAML signatures in some instances.
- Null Pointer Exception occurs during log source configuration where certificate key usage validation fails.
- Event to identify indexed value is 'NULL' is not generated by rules indexed by custom event properties.
- Unable to delete JSA user during reassignment of custom flow properties.
- 'Application error' can occur when disabling a user that has dependencies.
- Missing file /var/log/si-postgres-pam.log causes some services to fail to properly startup.
- Access to the user interface may be lost due to missing authorized service tokens.
- Event pipeline can stop due to secstoreforwarddestinationjava.lang.interalerror:sigbus.
- Scheduled reports can run on raw data causing them to fail or take longer than expected to complete.
- AQL equality operators do not work with AQL xforce functions array output.
- Users cannot access log source management despite having manage log source and JSA log source management permissions.
- DSM parameter changes not being saved for environment with single event collector.
- AQL search with conditions imatches or ilike return fewer results if the super index is used.
- Upgrading a detached host or HA standby with an expired license displays 'patch successful (with errors)'.
- Get_logs.sh does not run correctly on systems that no longer support MegaCLI.

- Geodata_update.sh returning false positive notifications on HA standby consoles.
- When running an AQL search with group by using a cep value that exceeds 1000 characters, the cep value is truncated.
- Modifying the rule 'multiple login failures for single username' might cause an NPE error when JSA is reading the rule.
- Hostdefinition building block VA scanner source IP is overwritten on every deploy if additional IP addresses are added.
- JSA.jsp call to licensekeymanager.areLicensesValid() causes a delay on login for customers having multiple managed hosts.
- Users patching from JSA 7.3.2 to JSA 7.5.0 might experience longer patch times than expected.
- New searches started in the offenses tab display incorrect time range options in the user interface.
- An application error occurs when a domain user attempts to assign an inactive offense.
- Authenticated HTTP request failure response incorrectly redirect win collect configuration requests to the login page.
- Users who log in to JSA can receive an error 'invalid license key' when the license is valid.
- Reference data API source response does not reflect the requested API source value.
- Application upgrades can fail when a health check executes on all applications.
- System rule names that were modified have old name in offense summary.
- Use Case Manager exports fail while session was in an open transaction state.
- Offense takes the offense start time from an older unrelated partial match event.
- Applications might fail to install because the application start time exceeds 500 seconds.
- QRM device backup failures caused by spillover cache.
- Domain mapped events might be incorrectly tagged to the default domain.
- In JSA, when IP addresses overlap during deployment, known hosts values can be removed.
- Authentication module settings page might be blank in JSA 7.5.0 Update Package 4.
- Offense summary page event/flow count field does not match the event count in log activity.
- Saving an LDAP repository can result in a nullpointerexception error causing login.conf file to go blank.

- Rules action for severity, credibility, and relevance are not properly displayed in the UI after an update.
- After you install the kernel and the reboot is complete, the installer hangs on a hardware check involving Myver and MegaCli.
- The software menu displays unsupported functionalities.
- The console displays as an event collector in the System and Licensing, License Appliance Type column.
- Log Analytics is missing from the installation wizard menu.
- The Network Insights installation fails without error.