Release Notes: Security Director Insights Release 22.3R1

30 June 2023
Revision 2

Contents

Introduction

Security Director Insights facilitates automated security operations. It enables you to take effective automated actions on security events from Juniper Networks security products. The events that affect a host or events that are impacted by a particular threat source are presented by Security Director Insights from different security modules. These events provide instantaneous information about the extent and stage of an attack. Security Director Insights also detects the hosts and servers under attack by analyzing events that are not severe enough to block. The application contains an option to verify the incidents using your trusted threat intelligence providers. After you have verified the incidents, you can take preventive and remedial actions using the rich capabilities of our security products.

Release Notes for Juniper Security Director Insights

IN THIS SECTION

New Features

There are no new features in Juniper Security Director Insights Release 22.3R1.

Product Compatibility

This section describes the supported hardware and software versions for Juniper Security Director Insights. For Security Director requirements, see the Security Director 22.3R1 Release Notes.

Supported Security Director Software Versions

Security Director Insights is supported only on specific Security Director software versions as shown in Table 1 on page 3.

Table 1: Supported Security Director Software Versions

Security Director Insights Software Version	Compatible with Security Director Software Version
22.3R1	22.3R1

> **NOTE:** The time zones set for Security Director and Security Director Insights must be the same and synchronize the time.

Virtual Machine Specification

Security Director Insights requires VMware ESXi server version 6.5 or later to support a virtual machine (VM) with the following configuration:

- 8 CPUs

- 24-GB RAM

- 1.2-TB disk space

Supported Browser Versions

Security Director and Juniper Security Director Insights are best viewed on the following browsers.

- Mozilla Firefox
- Google Chrome

Installation and Upgrade Instructions

For more information about installing Security Director Insights 22.3R1, see Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files.

For more information about installing Security Director Insights 22.3R1 with KVM, see Install Security Director Insights With KVM virt-manager.

For Security Director Insights upgrade instructions, see Upgrade Security Director Insights

Known Issues

There are no known issues in Security Director Insights Release 22.3R1.

Resolved Issues

There are no resolved issues in Security Director Insights Release 22.3R1.

Hot Patch Releases

This section describes the known issues and resolved issues in Security Director Insights Release 22.3R1 Hot Patch v1.

known Issues

- HA upgrade fails when SDI hostname has uppercase letters. PR1743770

  Workaround:

  You must disable HA, change hostname with only lowercase letters, and then enable HA again to successfully upgrade HA.

  SDI as Log Collector only (Only CLI is available)

  1. Disable HA via CLI on only primary node.

     CLI> (server) ha disable

  2. Change both primary and secondary SDI hostnames with only lowercase letters.

     CLI> (server) set hostname <...>

  3. Re-enable HA via CLI from primary node only. See Configure High Availability for Security Director Insights as Log Collector.

  4. After you have enabled HA, check **CLI> (server) ha status**, it should display that both the nodes are up.

  5. Perform HA upgrade from primary node. See Upgrade HA.

  SDI as analytics and Log Collector (Enable HA via GUI)

  1. Disable HA via GUI. See Disable HA.

  2. Change both primary and secondary SDI hostnames via CLI with only lowercase letters.

     CLI> (server) set hostname <...>

  3. Re-enable HA from GUI. See Enable HA.

  4. Wait till SDI HA setup is back online. GUI displays that both the nodes are up.

  5. Perform HA upgrade from primary node. See Upgrade HA.

Resolved Issues

- There is a circuit_breaking_exception while running Security Director reports. PR 1727690

- Group By "Category" shows No Data even though there are logs with category defined and seen in the events. PR1728499

Finding More Information

For the latest, most complete information about known and resolved issues with Junos Space Network Management Platform and Junos Space Management Applications, see the Juniper Networks Problem Report Search application at: http://prsearch.juniper.net.
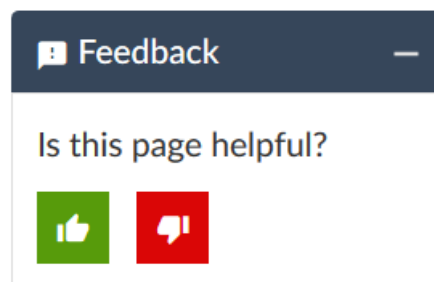
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: http://www.juniper.net/techpubs/content-applications/content-explorer/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:

  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.

- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/

- Search for known bugs: https://prsearch.juniper.net/

- Find product documentation: https://www.juniper.net/documentation/

- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/

- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/

- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/

- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

Revision History

22 December, 2022—Revision 1—Security Director Insights Release 22.3R1.

30 June, 2023—Revision 1—Security Director Insights Release 22.3R1 Hot Patch v1.