

Release Notes

Published
2023-12-06

Junos Space Security Director Insights Release Notes 23.1R1

Table of Contents

Introduction	1
New Features	1
Product Compatibility	1
Installation and Upgrade Instructions	3
Known Issues	3
Resolved Issues	4
Hot Patch Release	4
Finding More Information	5

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.

New Features

There are no new features in Juniper Security Director Insights Release 23.1R1.

Product Compatibility

IN THIS SECTION

- [Supported Security Director Software Versions | 2](#)
- [Virtual Machine Specification | 2](#)
- [Supported Browser Versions | 2](#)

This section describes the supported hardware and software versions for Juniper Security Director Insights. For Security Director requirements, see the Security Director 23.1R1 Release Notes.

Supported Security Director Software Versions

Security Director Insights is supported only on specific Security Director software versions as shown in ["Supported Security Director Software Versions" on page 2](#).

Table 1: Supported Security Director Software Versions

Security Director Insights Software Version	Compatible with Security Director Software Version
23.1R1	23.1R1

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 23.1R1, see [Deploy and Configure Security Director Insights with OVA files](#).

For more information about installing Security Director Insights 23.1R1 with KVM, see [Install Security Director Insights With KVM virt-manager](#).

For Security Director Insights upgrade instructions, see [Upgrade Security Director Insights](#)

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

The following are the resolved issues in Security Director Insights Release 23.1R1:

- 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](#)

Hot Patch Release

IN THIS SECTION

- [Resolved Issues](#) | 4

This section describes the resolved issues in Security Director Insights Release 23.1R1 Hot Patch v1.

Resolved Issues

[Table 2 on page 5](#) lists the resolved issues in the Security Director Insights Release 23.1R1 hot patch.

Table 2: Resolved Issues in the Hot Patch

PR	Description	Hot Patch Version
PR1750693	User is unable to expand the disk space for Security Director Insights.	v1
PR1744576	When you install Security Director Insights using a KVM image, it fails to deploy eth0, instead deploys eth1000.	v1

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/>.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2023 Juniper Networks, Inc. All rights reserved.