Release Notes: Juniper Identity Management Service 1.1.3

Release 1.1.3
7 January 2019
Revision 4

Contents

Introduction

This release note accompanies Juniper® Identity Management Service Release 1.1.3. It describes the product and its known behavior, problems, and limitations.

Juniper Identity Management Service (for Windows) is a standalone Windows service application that collects and maintains a large database of user, device, and group information from Active Directory domains, enabling SRX Series firewalls to rapidly identify thousands of users in a large, distributed enterprise. SRX Series Service Gateways can create, manage, and refine firewall rules that are based on user identity rather than IP address, query Juniper Identity Management Service, obtain the proper user identity information, and then enforce the appropriate security policy decisions to permit or deny access to protected corporate resources and the Internet.

Features

The following features are new in Juniper Identity Management Service (JIMS) v1.1:

- **Contrail Service Orchestrator (CSO) Integration**—If your network environment uses Contrail Service Orchestration (CSO), Juniper Identity Management Service supports operation with each CSO to facilitate the handling of firewall security policy decisions between the CSO platform and SRX Series devices by providing domain, group, user, and device identity information from Active Directory domains to each CSO. Juniper Identity Management Service is available as a standalone product or as an integrated identity management service from within Contrail Service Orchestration (CSO)

  CSO is deployed in the cloud, and the tenant infrastructure includes the tenant premises behind a firewall and cannot directly access Microsoft Active Directory in the customer's domain. Juniper Identity Management Service acts as the communication layer between identity servers such as Microsoft Active Directory and the CSO platform. Juniper Identity Management Service assists CSO in making policy user firewall decisions to filter traffic on SRX Series devices in a distributed deployment by providing user, device, and group identity information from the Active Directory domains to each CSO.

  All communication between Juniper Identity Management Service and CSO is initiated by the JIMS server. Upon startup, or configuring or updating CSO, the JIMS server initiates HTTPS connection to each fully configured CSO. The information exchange between Juniper Identity Management Service and each fully configured CSO is secure, live, and allows for a full resynchronization at any point in the data collection process.

  [See Introduction and Configuring the Connection to a CSO Client.]

- **Templates**—You can develop one or more templates in Juniper Identity Management Service:

  - SRX Series Device Templates—Support the grouping of client configurations to facilitate the configuration of multiple SRX Series devices.
  - Data Source Templates—Support the grouping of event or information source configurations to facilitate the configuration of a specific data source.

A template is a way to share common configuration attributes across items within a homogeneous collection without having to re-enter those attributes for each configuration instance. Templates allow configurations to share common data. A template provides default settings that can be referenced to create an instance.

For example, when using an SRX series device template, you can specify a username and password in a template, and assign that template across all SRX Series devices that require the same login credentials. Utilizing a template allows you to copy the configuration and only re-enter the password for the specific template.

[See Configuring SRX Series Device Templates and Configuring Data Source Templates.]

- **User/Device Event Filters**—Event filters on the JIMS server enable you to apply a filter in your network to define users or devices to *exclude* from reports the JIMS server sends to SRX Series devices. The User/Device Event filter performs regular expression matching to filter specific users or devices by name. The filter ignores events associated with a particular user or device.

  [See Configuring Event and Group Filters.]

- **Support IPv6 Reports**—The JIMS server allows IPv6-related report information to pass from the JIMS server to SRX Series devices.

  NOTE: SRX Series devices must be running the Junos OS 18.1R1 release, or a later release, to receive IPv6 reports.

  [See Configuring the Connection to an SRX Series Device.]

- **Processing Events**—On startup, the JIMS server now attempts to learn all groups and then all users from the user directories before processing events. If the learn procedure takes more than 90 seconds, the JIMS server will begin to process events for users which have already been learned. For a domain that is still learning, an event may continue to wait up to 4 minutes for a particular user to be read before the JIMS server begins executing parallel queries in an attempt to process the event.

Specifications

Table 1: SRX and JIMS Server Requirements and Specifications

Component	Operating System and Kernel Versions
Supported Junos OS software releases	• 15.1X49-D160.2, 17.4R3, or a later release • 12.3X48-D45 or a later release
Supported SRX Series device platforms	• vSRX Virtual Firewall, SRX300 line, SRX1500, SRX4100, SRX4200, SRX5000 line (Junos OS Release 15.1X49-D160.2, 17.4R3, or a later release) • SRX650, SRX240H2, SRX3000 line, and SRX5000 line (Junos OS Release 12.3X48-D45 or a later release)

Table 1: SRX and JIMS Server Requirements and Specifications (continued)

Component	Operating System and Kernel Versions
Supported Contrail Service Orchestration (CSO) release	Release 4.0.1 or later NOTE: If your network deployment includes Contrail Service Orchestration (CSO), JIMS 1.1.3 is currently certified for use only with the upcoming CSO 4.0.1 release or later. Please see Contrail Service Orchestration Documentation to determine which SRX releases are used with specific releases of CSO.
Maximum SRX Series devices	100
Maximum CSO platforms	10
Maximum event log sources	150
Maximum Active Directories	100
Maximum domains	25
Maximum user entries	500,000

System Requirements

Juniper Identity Management Service can be installed on the following Microsoft Windows platforms:

- Windows Server 2016
- Windows Server 2012 R2 with Windows Server 2012 R2 Updates (KB2919355 and KB2999226)
- Windows Server 2008 R2 with Service Pack 1 (SP1) and Update for Windows Server 2008 R2 x64 Edition (KB3140245)

NOTE: Windows Server 2008 R2 with SP1 also requires installation of an update that provides support for Transport Layer Security (TLS) 1.1 and TLS 1.2. See Update to enable TLS 1.1 and TLS 1.2 as a default secure protocols in WinHTTP in Windows for details. After you apply the update, select **Run as administrator** to restart the JIMS Administrative Interface.

BEST PRACTICE: Note the following best practices when installing Juniper Identity Management Service on a Microsoft Windows platform:

- Because Juniper Identity Management Service participates in the security infrastructure protecting your network, we recommend using Windows

Update regularly and judiciously to obtain the latest Security Updates and other Critical Updates from Microsoft.

- Juniper Identity Management Service requires a server with a 4-core, 64-bit compatible 1.4 GHz or higher CPU, a minimum of 16 GB of system memory, and 100 GB of disk space.
- If using Windows Server 2008 R2, avoid installation on a primary domain controller (PDC). Juniper Identity Management Service should be installed in a separate, non-domain controller instance.

Supported Identity Sources

Juniper Identity Management Service supports the following identity sources:

- Microsoft Active Directory on Windows Server 2008 R2 and later
- Microsoft Exchange Server 2010 with Service Pack 3 (SP3)

Changes in Behavior and Syntax

This section lists the changes in behavior of JIMS features and changes from Juniper Identity Management Service (JIMS) v1.1.3.

- JIMS will not deconflict certain change notifications and might lead to minor degraded performance or behavior associated with the last update to the Active Directory when uSNChanged value receives zero. Starting in JIMS Release 1.1.3, when JIMS detects the user or group uSNChanged value as zero, the following error message **Error: received uSNChanged of zero - do you have sufficient permissions (User Rights "Synchronize directory service data") for this AD? <AD Name> -- <dn> -- <server ip>** is logged. Specifying the synchronize directory service data privilege for the configured user account addresses the issue.
- One of JIMS various protections against some kinds of denial-of-service (DoS) flood attacks are triggered by SRX Series device due to the bursts of queries for unknown IP addresses. Starting in JIMS Release 1.1.3, to avoid triggering this situation, JIMS default connection constraints are modified to allow 100 connections to be enqueued before being processed.

Known Behavior

This section lists the known behaviors and limitations in Juniper Identity Management Service Release 1.1.3.

- The JIMS server can crash if there are too many certificates loaded under the following path **Console Root / Certificates (Local Computer) / Personal / Certificates**. The following warning message **(Configuration:Warning) There are an excessive number of certificates in the 'my' store, total xxx** is added to the JIMS log. If you see this warning, you should remove any excess / expired certificates from the store.
- Juniper Identity Management Service uses the event log timestamp to decide the order of events, and, therefore, you might experience unexpected side effects if your domain controllers and Active Directories are not synchronized. This is more likely to happen across domains than within domains, which typically time-synchronize with their domain controller. Juniper Identity Management Service uses UTC (GMT) internally, and the time zone should not matter, only the time synchronization. See the Windows Time Service Tools and Settings documentation for Windows Server 2016, 2012 R2, or 2008 R2.
- If you install applications such as Juniper Identity Management Service that add a shortcut inside a folder on the Start menu, the shortcut does not work until you log out and log back in again. See the release notes for Windows Server 2016, 2012 R2, or 2008 R2 for more information regarding this issue.
- After more than 210 groups per user for an Active Directory group filter are configured on and reported by Juniper Identity Management Service, the SRX Series device generates an error and any additional groups are dropped.

  NOTE: **You can specify a group filter to ensure that only the relevant groups are included.**

- If you delete an Active Directory as a user information source from the JIMS server, the corresponding users and groups will continue to appear in the CSO UI for an additional period of time (approximately two hours). The associated users and groups will eventually be removed from the CSO UI.

  The users and groups associated with the deleted Active Directory will not be removed until you restart the JIMS server.
- While installing Juniper Identity Management Service (JIMS), the InstallShield installer window title has the version as 1.14.86 instead of 1.1.4.86.

Known Issues

This section lists the known issues in Juniper Identity Management Service Release. 1.1.3

- When the client-id/client-secret is modified on JIMS server, it may cause the JIMS connection status show as invalid credential even SRX Series device client-ID/client-secret is changed to the same. Restarting the JIMS service can get the connection status recovered. PR1400224
- For instances of Juniper Identity Management Service installed on Windows Server 2012 R2 or 2008 R2, the JIMS administrative interface does not get removed after you uninstall the application. PR1283035

- When changing the description on either the Event Source or Info Source page, this action might cause the JIMS server to reload all events, as if you had changed something more substantial such as the IP address. PR1289775
- In JIMS release 1.0.0, the SRX Debug (http) Port was enabled by default, and you were restricted from modifying the setting from the JIMS server Administrative Interface UI. Starting with JIMS release 1.1.0, you can enable or disable the SRX Debug (http) Port from the General tab of the Administrative Interface UI (**Settings > General**). To increase security, the inbound SRX Debug (http) Port is disabled by default, and we recommend that you use the TLS (https) Port for inbound connections from SRX Service devices. However, if your configuration requires an inbound HTTP connection, you can enable the Debug (http) Port from the General tab of the Administrative Interface UI. PR1349065
- The User/Device Event filter uses a regular expression to perform a match, unlike the SRX Group filter which uses a simple string match. For example, entering a name ("user1") would match a prefix (also matching "user11", "user112", and so on). To enter a full string, add a dollar sign suffix ("user1$") to the filter. PR1370306
- The JIMS server is not able to handle a query that contains a username with a blank space (for example, “test 100”). This behavior occurs because the JIMS server does not support a query with Percent-Encoding (RFC 3986). RFC 3986 defines the percent encoding that can be used with URIs. In this case, it is possible that JIMS Release 1.1.3 will not be able to handle a query from an SRX Series device with a username/ID that contains an embedded space. PR1374810

  

  NOTE: **Microsoft recommends against including spaces in a username.**
- An SRX Series device will receive a dynamic update from the JIMS server when JIMS detects that a user has been disabled in the Active Directory (AD), and another dynamic update from JIMS if that user is subsequently reenabled. This update retains the domain and username in the table, but does not include any groups associated with that user. PR1380771

Resolved Issues

This section lists the resolved issues in Juniper Identity Management Service Release. 1.1.3

- When upgrading earlier JIMS release with JIMS 1.1.3, the file, C:\Program Files (x86)\Juniper Networks\Juniper Identity Management Service\bin\JimsEventLogReader.dll does not update to the latest release. This issue is fixed in JIMS Release 1.1.3R4 (version 1.1.3 build 80) and later. PR1405081
- When JIMS server attempts to find users by domains, User Principal Name (UPN) domain suffixes in the Active Directory (AD) domain were not considered by JIMS server. Starting in JIMS Release 1.1.3, JIMS will read the list of UPN domain suffixes and mark them as aliases to the DNS domain. PR1391170

- Updates to a user's group membership in Active Directory are not forwarded to the SRX Series device if a user was previously moved from one organizational unit to another organizational unit, and in addition, sAMAccountName changes are not forwarded. These issues are fixed in JIMS Release 1.1.3 and later. PR1397748
- In JIMS Release 1.1.2 and earlier, if the JIMS Administrative Interface failed to connect, you will get a blank dialog box with no error message. This issue is resolved in JIMS Release 1.1.3R1 with a warning message **Please enter the valid credentials** prompted if you log on GUI with an incorrect password. PR1373567.

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

7 January 2019—Revision 4—Juniper Identity Management Service Release 1.1.3

7 December 2018—Revision 2—Juniper Identity Management Service Release 1.1.3

12 November 2018—Revision 1—Juniper Identity Management Service Release 1.1.3