Release Notes: Juniper Identity Management Service 1.2.0

Release 1.2.0
4 December 2019
Revision 1

Contents

Introduction

This release note accompanies Juniper® Identity Management Service Release 1.2.0. 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 in-memory cache 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 Release 1.2.0:

- **Support remote system syslog messages**—Starting in JIMS Release 1.2.0, we support the ability to receive remote system log (also called syslog) event and user information data from an event source such as a DHCP server. You define the IP address and port of the remote syslog server that the JIMS server permits a connect from the remote server and configure the JIMS server on how to process the syslog messages received. The JIMS server receives and processes data from syslog messages and transmits this information to each SRX Series device to use in making policy decisions in the user firewall. UDP 514 and TCP 514 are the default ports to support the syslog server.

  [See Configuring JIMS to Receive Remote Syslog Messages.]

- **IPv6 support**—Starting in JIMS 1.2.0 Release, we support IPv6 connectivity between the JIMS server and the SRX Series devices running with Junos OS Release 18.3R1 and later. By default, the JIMS server listens for IPv4 incoming IP addresses from the SRX Series devices on the specified port. You can click the **Advanced** button to configure IPv6 or IPv6 and IPv4 (dual-stack) connections between the JIMS server and the SRX Series device.

  With JIMS server running JIMS 1.2.0 Release and SRX Series devices running Junos OS Release 18.3R1 and later, you can apply IPv6 address filters in addition to IPv4 address filters for the SRX Series devices in your network.

  [See Configuring IP Address Filters.]

- **Support import and export JIMS server configuration**—Starting in JIMS Release 1.2.0, we support backing up or exporting an existing JIMS server configuration. Exporting allows you to import (clone) the configuration onto another JIMS server (passwords will need to be re-entered), while backing it up allows

you to import (restore) it to the same JIMS server from which it is created to recover the configuration (passwords are preserved in encrypted form).

[See Exporting or Backing Up a JIMS Server Configuration and Importing a JIMS Server Configuration.]

- **Support domain alias**—Starting in JIMS Release 1.2.0, you can create an alias for the JIMS Active Directory domain names. Domain aliases enable you to assign different domain names to your primary domain name. JIMS creates a domain object for each Active Directory forest that it connects. The domain object maintains a list of outstanding devices and users. JIMS maps the domain names to the domain object by mapping the long name (juniper.net) and the short name (juniper) to reference the same domain object to support Active Directory configuration. This permits events received domains that are not explicitly connected to user directory accounts such as a DNS alias to match a real user in a particular directory source.

  [See Domain Alias.]

Specifications

Table 1: SRX and JIMS Server Requirements and Specifications

Component	Operating System and Kernel Versions
Supported Junos OS software releases	• 15.1X49-D100, 17.4R1, 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-D100, 17.4R1, or a later release) • SRX650, SRX240H2, SRX3000 line, and SRX5000 line (Junos OS Release 12.3X48-D45 or a later release)
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

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

Component	Operating System and Kernel Versions
Maximum syslog sources	200

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)

> **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)
- Syslog

Changes in Behavior and Syntax

There are no changes in behavior and syntax for Juniper Identity Management Service in JIMS Release 1.2.0.

Known Behavior

This section lists the known behaviors and limitations in Juniper Identity Management Service Release 1.2.0.

- Memory utilization stabilizes at a plateau as times goes on. The memory is related to the amount of users, devices, groups, and the number of groups per user, plus sessions, and the number of updates per session.

  In the case of messages burst, new user creation or updates, JIMS retains in memory an expanded backlog of reports or sessions. This retention is until they are drained by the SRX Series devices, which may persist to the point it could exhaust memory.

  Monitor your JIMS server for excessive memory usage. If issues are detected regularly, schedule the JIMS server restarts during appropriate maintenance windows and contact JTAC support at https://myjuniper.juniper.net. PR1466320

Known Issues

This section lists the known issues in Juniper Identity Management Service in JIMS Release 1.2.0.

- Avoid importing the configuration while JIMS has user info sources in the learning state. The Microsoft library generates a core when interrupted, which will emerge as an error in the administrator GUI and to restart JIMS. You must import the configuration after JIMS is restarted and not in the learning state. PR1469305
- After you delete a user info source, the info source status shows the deleted user info source as reconnecting. You must wait until the user info source gets deleted in the status or restart the JIMS server. PR1411436
- Active session counter do not change when the sessions are logged off or expired. JIMS takes some time to reflect the active session counter go down after the logoff or expired. PR1459742

- You must restart the JIMS server after you change the IP address associated with a client entry to subsequently ignore those entries. PR1468857
- Due to the nature of efficient writing to files on windows, results returned via the GUI syslog regular expression **test** button may not contain the latest results. PR1472064
- When syslog message triggers **Per Session Group Mask**, a group is masked and forced back with two of the same group sent to the SRX Series device. PR1454890

Resolved Issues

This section lists the resolved issues in Juniper Identity Management Service Release in JIMS Release 1.2.0.

- You may not be able to log in the Active Directory domain controllers and the servers on which JIMS sever is installed and running, when you set the LAN manager authentication network security level to **MTLMv2 Only. Reject NTLM and LM**. You must set the LAN manager authentication network security level to lower than the maximum level to log in the domain controllers and servers. PR1461882
- Modifying the client ID or client secret on JIMS causes the JIMS connection status showing as invalid credentials. JIMS connection status shows as invalid credentials even the client ID or client secret on SRX Series device is changed to the same. Restart the JIMS service to recover the connection with the SRX Series device. PR1400224
- When a new group is added to the Active Directory, the filtering calculation is done after the sessions for the initial users in the group are updated. This change causes SRX Series device to see the newly added group transiently depending on how long the batch query rate is set. Starting in JIMS Release 1.2.0, the filter is checked when the group is created before the sessions are updated the first time. PR1416529
- Starting in JIMS Release 1.2.0, JIMS supports OpenSSL version 1.0.2-r, which is licensed under the OpenSSL license as well as the original SSLeay license. PR1432282
- By default, JIMS disables the tcp **keep-alive** for the syslog sources which result in new connections being refused. You can enable the tcp **keep-alive** to accept the new tcp connections from the syslog source. PR1463528
- The syslog_all file takes lot of hard disk space causing JIMS to refuse the connections from the source. Starting with JIMS Release 1.2.0, the log levels are reset to the default. PR1470340

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

4 December 2019—Revision 1—Juniper Identity Management Service Release 1.2.0