Release Notes: Juniper Identity Management Service 1.0.3

Release 1.0.3
9 May 2018
Revision 1

Contents

Introduction

These release notes accompany Juniper® Identity Management Service Release 1.0.3. They describe 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.

Juniper Identity Management Service Release 1.0.3 is supported by SRX Series devices running Junos® OS Releases 15.1X49-D100, 17.4R1, 12.3X48-D45 or a later release.

Features

Juniper Identity Management Service (JIMS) has the following features:

- **Support for identity-based security policies on SRX Series devices**—Juniper Identity Management Service enables you to filter traffic on SRX Series devices based on user identity information such as usernames and user groups in addition to IP addresses. The service provides IP address-to-username-to-group mapping information to the SRX Series devices, which use the mapping information to generate entries for their authentication tables that you can use to enforce user-based and group-based security policy control.

  NOTE: On SRX Series devices, user groups are known as user roles.

  [See Introduction]

- **Centralized user identity data collection**—Juniper Identity Management Service provides a scalable service that can take over user identity data collection from Microsoft Active Directories, domain controllers, and Exchange servers, serving as a single, centralized data collection source for all SRX Series devices in your network.

  For example, Juniper Identity Management Service can replace the connections from individual SRX Series devices to multiple Microsoft Active Directory domain controllers with a single connection from the service to each domain controller, eliminating scaling limitations.

  [See Introduction]

- **Data collection from event log sources**—Juniper Identity Management Service connects to event log sources to collect user and device status events and provide IP address-to-username mappings to the SRX Series devices. For user login events, it collects the domain name and username. For device login events, it collects the domain name and machine name.

An event log source can be a Microsoft Active Directory domain controller or a Microsoft Exchange server.

[See Introduction]

- **Data collection from user information sources**—Juniper Identity Management Service connects to user information sources to collect group information for users and their devices and provide username-to-group mappings to the SRX Series devices. The service queries each user information source for its supported domains and selects a source by domain when it needs to initiate user or device information queries. It queries the appropriate user information source each time it receives a login event for a user. Microsoft Active Directories are used as user information sources for Juniper Identity Management Service.

  [See Introduction]

- **Domain PC probing**—Domain PC probing acts as a supplement to event log reading. When a user logs into a domain, the event log contains that information. When there is no IP address-to-username mapping from the event log, Juniper Identity Management Service initiates a domain PC probe to the device to get the username and domain of the currently active user. Domain PC probes are also used to determine a device's status after its logged-in state has expired.

  NOTE: Domain PC probing works on Microsoft Windows endpoints only.

  [See Introduction]

- **User identity information reporting**—Juniper Identity Management Service generates reports that contain records of the IP address, username, and group relationship information collected from the user identity data sources.

  The service also generates reports for device-only sessions without sending the username in the report when the username is not available. SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release can enforce security policies based on device authentication as well as on user authentication.

  [See Introduction]

- **SRX Series device query support**—Juniper Identity Management Service responds to queries from SRX Series devices with the corresponding IP addresses, usernames, and device names. The service also responds to individual IP address queries with the corresponding usernames and device names.

  For SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, batch queries from individual SRX Series devices can filter information based on a combination of timestamp, domain, and IP address. When SRX Series devices miss data for an existing flow, they can engage a captive portal to get the username. Once the user is authenticated by the captive portal, the SRX Series devices can issue an additional query to Juniper Identity Management Service, specifying the username and IP address to obtain the corresponding group information.

  [See Introduction]

- **Server certificates for authentication with SRX Series devices**—Juniper Identity Management Service enables you to select automatically generated server certificates or import previously configured certificates for server authentication with the SRX Series devices in your network. Specifying a server certificate enables the JIMS server to authenticate with SRX Series devices before communicating with them.

  [See Introduction]

- **System-level IP address and user group filtering**—Juniper Identity Management Service enables you to specify IP address ranges to include in or exclude from the reports sent to the SRX Series devices. You can also specify Active Directory user groups to include in the reports. These filters are applied to all the SRX Series devices in your network.

  [See Introduction]

- **Connected network device monitoring**—You can monitor the status of the network devices connected to the JIMS server, including:

  - SRX Series devices
  - Event log sources, which can be Microsoft Active Directory domain controllers or Exchange servers
  - User information sources, which can be Microsoft Active Directories
  - Domain PC probes to user devices

  [See Introduction]

- **System logging**—For troubleshooting purposes, Juniper Identity Management Service is installed with a default log called **jims_*yyyymmdd_nnnnn*.log**, which is stored in **\Program Files (x86)\Juniper Networks\Juniper Identity Management Service\logs**. For example, a default log can be called: jims_20170707_00000. The log includes the following event types:

  - **System**—Configuration, administration, and system-level events
  - **Client**—HTTPS/HTTP GET requests from and HTTPS/HTTP POST submissions to the SRX Series devices
  - **Event source**—User and device login events per Active Directory domain controller and Exchange server
  - **Info source**—Active Directory events
  - **PC probe**—PC probe requests per set of administrative credentials
  - **Sessions**—Internal session finite state machine (FSM) transitions and internal cache events for domains, sessions, users, devices, and groups

  Logging levels for each component can be set to:

  - **None**—No logging
  - **Error**—Critical events affecting the entire system
  - **Warning**—Unexpected per-transaction events

  - **Standard**—Minimal logging for a concise view of transaction flows
  - **Detail**—Detailed logging for a broader view of transaction flows
  - **Debug**—Most detailed logging level for troubleshooting

  Each logging level includes events from the previous levels.

  [See Introduction]

- **High availability**—JIMS servers can be configured in a primary and secondary server configuration on SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release. The SRX Series devices send HTTPS queries to the primary JIMS server and fall back to the secondary server when queries to the primary server fail. The SRX Series devices probe the primary server and revert back to it when it becomes available again.

  [See Introduction]

- **OpenSSL release 1.0.2n**—With JIMS Release 1.0.2, the JIMS server now utilizes release 1.0.2n of the OpenSSL toolkit.

Specifications

Supported Junos OS software releases	15.1X49-D100, 17.4R1, or a later release 12.3X48-D45 or a later release
Supported platforms	vSRX, 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 event log sources	100
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)

Known Behavior

This section lists the known behaviors and limitations in Juniper Identity Management Service Release 1.0.3.

- To mitigate brute force attacks, Juniper Identity Management Service only accepts requests from known devices and will limit failed login attempts. To further protect against attacks, customers should implement strong security business continuity plans, limit the exploitable attack surface, and only allow trusted administrators, networks, and hosts to access Juniper Identity Management Service deployments.
- Juniper Identity Management Service uses the event log timestamp to decide the order of events, and, therefore, you might experience unexpected side issues 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.
- Health mailboxes on Microsoft Exchange servers (users with a prefix of HealthMailBox) are filtered out by default by Juniper Identity Management Service.
- Juniper Identity Management Service creates and maintains sessions for Active Directory domain controllers as well as domain PCs. This might result in the service attempting to send PC probes to the domain controllers. To avoid this behavior, add the IP addresses of the domain controllers to an IP filter on Juniper Identity Management Service.

Known Issues

This section lists the known issues in Juniper Identity Management Service Release. 1.0.3

- 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 the SRX Series device push rate is lower than the event generation rate, Juniper Identity Management Service's memory usage might increase. To avoid running out of memory, Juniper Identity Management Service delays reading events when there is a significant backlog. PR1286413
- Saving changes made to user group filters causes the sequence of the listed IPv4 address range filters to change. There is no effect on address filters or performance. PR1288376
- The TCP connection between an SRX Series device and Juniper Identity Management Service times out. The solution is to enforce keep-alives on the TCP connection. To address this behavior, the JIMS 1.0.1 release includes a workaround to avoid the issue—the Juniper Identity Management Service server enforces keep-alives on the TCP connection. PR1311446

  Workaround: The TCP connection limit has been raised from 10 to 1000.

Resolved Issues

This section lists the resolved issues in Juniper Identity Management Service Release 1.0.3

- Adding a group filter to include a grandparent (or higher) group would fail to update SRX Series devices for those sessions. With JIMS Release 1.0.3, after the group filter is updated, the JIMS server works in the background to refresh a multitude of sessions across all configured SRX Series clients. Note that these changes may take several minutes to propagate to the SRX Series devices. PR1349937

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

9 May 2018—Revision 1—Juniper Identity Management Service Release 1.0.3

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.