White Paper

JUNIPER NETWORKS SERVICE AUTOMATION

An Ecosystem of Tools, Applications and Systems to Simplify and Streamline Operations, Bring Operational Efficiency, Reduce Downtime and Increase ROI

Table of Contents

Introduction . . . 3
Executive Summary . . . 3
Security for Service Automation Solution . . . 3
Juniper Networks Service Automation Architecture and Key Components . . . 4
Advanced Insight Scripts (AI-Scripts) . . . 5
Junos Space Service Now . . . 5
Junos Space Service Insight . . . 5
Juniper Networks Support Systems . . . 5
Security Considerations for Automation Solution Architectural Components . . . 6
Advance Insight Scripts . . . 6
Confidentiality . . . 6
Integrity . . . 6
Availability . . . 7
Junos Space Service Now . . . 7
Confidentiality . . . 7
Availability . . . 7
Confidentiality . . . 7
Integrity . . . 8
Availability . . . 8
Support System . . . 9
Confidentially . . . 9
Integrity . . . 9
Availability . . . 9
Solution Guidelines for Deployment and Operation . . . 9
Design and Planning . . . 9
Deployment . . . 9
Operational . . . 9
Conclusion . . . 10
About Juniper Networks . . . 10

List of Figures

Figure 1: Three tenets of the Security Triad . . . 4
Figure 2: Incident management with Junos Space Service Now . . . 4
Figure 3: Guide to communication protocols between Service Now and network nodes and Service Now and JSS . . . 8

Introduction

Juniper Networks Service Automation consists of an ecosystem of tools, applications and systems designed to simplify and streamline operations, bring operational efficiency, reduce downtime and increase ROI from your network running Juniper Networks® Junos® operating system.

Automation brings operational efficiency by automating several time-consuming tasks such as incident management and inventory management. Service Automation capabilities delivered with Juniper Networks Juniper Care Technical Services automate these and deliver tailored, proactive network intelligence and support services for Juniper's high-performance platforms. With the unmatched capability of Juniper Networks Service Automation solution, network operations can become simpler, more reliable and more cost-effective.

Executive Summary

The two issues most important to today's network operators are the reduction of downtime and the reduction of operational expenses (OpEx). Juniper Networks Service Automation solution is designed specifically to address both of these issues. The automation solution provides a comprehensive set of tools and technologies to automate the delivery of tailored, proactive network intelligence and support services for Juniper Networks high-performance platforms. By distributing proactive network intelligence from Juniper engineers and systems, automating support steps for customers, and providing proactive insight into Junos OS software device operations, Service Automation enables network operations to become simpler, more reliable and more cost-effective.

Juniper Networks Service Automation solution is:

- An enabling technology available exclusively with Juniper Networks Juniper Care Technical Services portfolio.
- An expert analysis system that brings the experience and insight of Juniper's development teams directly into Juniper Networks platforms.
- A data mining system that stores and tracks potential risks and problem conditions in the platform.
- An early warning system that keeps a constant vigil for potential problems in the platform and proactively notifies customers of potential risks, performing expert analyses to prevent problems before they arise.
- A troubleshooting assistant that automates and speeds the resolution of problems by providing expert-based logic to automate the process of opening a case with the Juniper Networks Technical Assistance Center (JTAC), and by sending the necessary information for JTAC to identify and resolve the problem with minimal effort on the part of operations personnel.
- A highly secure, customizable system that performs according to customers' specifications and within their operational and security policy guidelines.

Passion for innovation has driven the continuous development of Junos OS from the inception of Juniper Networks. Continuing the tradition of introducing innovative solutions, Juniper Networks Service Automation solution is the key enabling technology of the Juniper Care Technical Services portfolio.

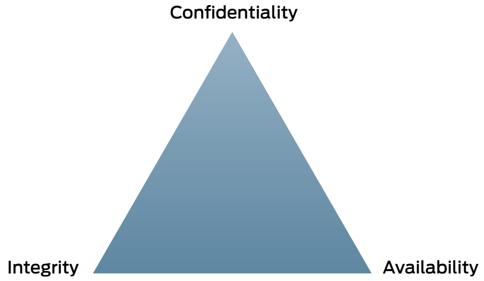
Security for Service Automation Solution

The Service Automation solution offers significant benefits to customers by automating both reactive and proactive technical support processes. Automation enables faster problem identification and resolution, and more effective problem avoidance within the customer's own support organization, the Juniper Networks partner's support organization and JTAC.

To provide these benefits, the automation solution collects data from Juniper Networks devices that are selected by the customer. To ensure maximum benefit, the data needs to arrive at Juniper Networks verifiably intact and complete. When the data is inside the Service Automation "back-office" infrastructure or Juniper Support Systems (JSS), it must be protected in accordance with customer confidentiality requirements, as some of the data collected might be considered sensitive or of particular value to the customer.

To achieve these requirements, Juniper has designed the automation solution with numerous inherent security features, from the AI-Scripts or agents deployed on individual devices to capture data, to the gateway applications that store and filter this data on the customer site, and finally to the transport, storage and access of this data within JSS.

To better illustrate the key objectives of the security architecture applied to Service Automation, it is important to understand generically how security is provided at a high level. The "Security Triad" is an excellent benchmark to apply to most security models at the highest level.



CONFIDENTIALITY: Assurance that information is shared only among authorized persons or organizations with a legitimate access requirement.

INTEGRITY: Assurance that information is authentic and complete. This ensures that information canbe relied upon as sufficiently accurate for its slated purpose.

AVAILABILITY: Assurance that both the information and the systems responsible for delivering, storing, and processing that information are accessible when needed, by those who need them.

Figure 1: Three tenets of the Security Triad

This white paper describes the architectural components of the Service Automation solution and where appropriate[1], the security controls, mechanisms and techniques applied to the Service Automation solution components and infrastructure that provide protection to the data throughout its life cycle. In keeping with the Security Triad benchmark, the features outlined here are broken into the three tenets—confidentiality, integrity and availability—to better illustrate the solution's function and benefits.

Juniper Networks Service Automation Architecture and Key Components

The Service Automation solution includes components that seamlessly work within a customer's environment and are securely integrated with Juniper Networks case management, contract management, and other systems and databases to deliver a connected experience to the customer. These components include the following elements:

- **Advanced Insight Scripts (AI-Scripts)** run on each Junos OS-based device and are written based on the experience and knowledge of JTAC engineers.
- **Junos Space Service Now** is the key technology that enables the Service Automation infrastructure.

Juniper Networks Junos Spaceis a comprehensive Network Management Solution that simplifies and automates management of Juniper's switching, routing, and security devices. Junos Space consists of a network management platform for deep element management, plug-n-play management applications for reducing costs and provisioning new services quickly, and a programmable SDK for network customization. With each of these components working cohesively, Junos Space offers a unified network management and orchestration solution to help you more efficiently manage the New Network.

Junos Space Service Now, one of the Junos Space Management Applications that runs on the Junos Space Network Management Platform, provides a centralized control of the Service Automation infrastructure including automated incident detection (detection of error events), reporting and log collection as well as automated inventory management.

- **Junos Space Service Insight** is the key Junos Space Management Applications that provides actionable network intelligence- enabling proactive maintenance.
- **Juniper Support Systems (JSS)** consists of expert systems located within Juniper Networks premises and securely integrated with the solution, providing an interface to existing CSC Case Management, contract management systems and knowledge repositories.

Figure 2 shows how the components of Juniper Networks Service Automation seamlessly fit together.

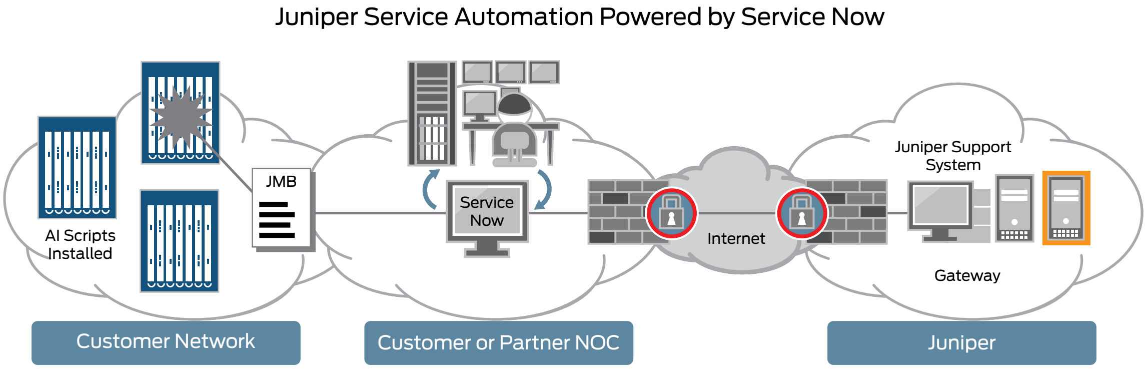


Figure 2: Incident management with Service Now

[1] To protect Juniper Networks against disclosure of the Service Automation "back-end" security infrastructure, this document deliberately does not detail the internal security measures protecting the Service Automation infrastructure. If necessary, this topic can be discussed under appropriate NDA by proper negotiation.

Advanced Insight Scripts (AI-Scripts)

Advanced Insight Scripts are Junos scripts that are installed on Juniper devices to monitor for problem signatures and collect associated diagnostic information. You receive access to these AI-Scripts as part of your service contract entitlement.

These expert scripts are written by JTAC experts based on their collective experience of various troubleshooting scenarios. For specific events that are identified by these scripts, the relevant information from the device is sent out as information packages called Juniper Message Bundles (JMB). JMBs are sent to predefined designated targets including the Junos Space Service Now instance in your environment.

JMBs can be "event-driven," created for events related to service impacting issues (both hardware and software), or they can be "intelligence-driven," generated periodically to collect information including inventory, resource utilization and configurations. Service Now collects all the JMBs and provides an interface and control for the administrator to take action on the event.

Users can select the events that they want to monitor on the device by defining "Event Profiles" on Service Now, thus giving users the flexibility to pick and choose events that they want to detect on a particular device.

Junos Space Service Now

Junos Space Service Now is the control point for Service Automation information flow. The Junos Space Network Management Platform runs as a virtual appliance on a VMware partition or a hardware appliance that can be ordered from Juniper.

Service Now is the management point for all events detected by the AI-Scripts. The JMB generated as a result of the events detected is made available on the Service Now console for management of the event and the opening of a related case with Juniper should you need to do so.

When Service Now receives a JMB from a device running AI-Scripts, it stores information from the bundle in its database and presents this information through the incident management reporting interface. This information is used by network administrators to review and diagnose issues (event-based) or to track device characteristics including hardware inventory, device configurations and systems resources (intelligence-based). Service Now ensures that valuable insight into the network supported by Service Automation is always at your administrator's fingertips.

Junos Space Service Insight

Junos Space Service Insight is the application within the Service Automation solution responsible for delivering targeted network intelligence such as end-of-life notifications and proactive bug notifications for the devices in the network.

Service Insight depends upon the data collected in the intelligence JMB via Service Now and the analysis done on the collected data within Juniper Support Systems (JSS) to deliver these proactive notifications.

Juniper Networks Support Systems

Junos Space Service Now and Junos Space Service Insight run in your environment and communicate with JSS to transfer JMBs and receive updates on cases and proactive notifications. This transfer is configurable and controlled by the network administrator. This intelligence-driven information, transferred to Juniper Networks by Service Now, is stored and used by Juniper to generate a wide variety of proactive analysis and reports.

Event-driven information transferred to JSS is used to open trouble tickets (cases) automatically with JTAC by a secure integration with Juniper Networks case management systems.

Note that Service Now always initiates the secure communication transfer of JMBs between JSS and Service Now. JSS never initiates sessions with Service Now to request JMBs or to send any proactive information. All JMBs are pushed from Service Now to JSS and proactive information is pulled from JSS on a periodic basis. Also, the administrators always have complete control of the level of information that is sent to JSS.

When proactive analysis or trouble case updates are completed by JTAC engineers and documented in the CSC Case Manager system, the information is automatically transferred to Service Now and accessible via the incident management reporting interface.

Security Considerations for Automation Solution Architectural Components

Juniper Networks Service Automation uses Junos Space to provide secure communications that meet industry expectations around security and information protection. The following techniques allow you to provide complete clarity and control when dealing with the security aspects of the solution:

- Standard, secure protocols including HTTPS, SSH and NETCONF are used anytime data is transferred between Service Automation components. Also, connections between some combination of Service Now and Service Insightand JSS are always authenticated.
- All communication between some combination of Service Now and Service Insight and JSS is always initiated from Junos Space.
- You have the ability to adjust the level of information share that Service Now sends to JSS through four levels of filtering—from no sharing to full share with user login information is always automatically deleted from configurations.

Any changes to Junos Space, managed devices or both are recorded in the the Audit Log database and the records identify the user who initiated the modification, the time of the request, the appliance that was used and the list of the modifications. The audit trail is supported for the following procedures:

- User logins/logouts
- User creation/deletion
- User timeouts
- Authentication failures
- Each operation attempted by a logged in GUI user
- Transactions initiated by OSS via northbound interfaces

Finally, Juniper Networks uses strict access control policies and systems to prevent, limit and track access to your encrypted data in JSS. Only Juniper Networks personnel involved in delivering technical services to you are allowed access to the secure systems within Juniper's network that store your data.

Using information that you share, Juniper Networks is uniquely positioned to determine potential risks to your network, perform migration analysis, prepare detailed bug impact analysis and suggest other technical recommendations.

The subsequent sections outline the specific features that ensure the confidentiality and integrity of data access and collection within the Service Automation solution components.

Advance Insight Scripts

AI-Scripts and the data contained in JMBs are afforded protection as follows:

JMB is an XML file, which contains information collected from the device when an event is detected. Once all the output has been collected, a JMB is created and stored on the device. The JMB is validated on Service Now when received so only data that meets strict structure and schema requirements is accepted and processed.

Confidentiality

JMBs from Network Elements (NEs) to Service Now target locations are always transferred over a secure connection using Juniper's Device Management Interface (DMI). DMI uses SSH and NETCONF to ensure secure transfer between the device and the Service Now application.

Integrity

- AI-Scripts are tested and published by Juniper Networks and include a digital signature that is validated by the Junos OS device. If the signature is not valid, the AI-Scripts do not work with Service Now. This ensures that only a signed AI-Scripts package from Juniper is installed on the device.
- The AI-Scripts leverage embedded management capabilities within Junos OS to generate and transmit JMBs when a failure or other issue occurs. Once formed, the device running Junos OS automatically pushes the JMB to the Service Now target location. This means that it is not necessary for Junos Space Service Now to poll or otherwise connect to the devices.
- The JMBs sent to Service Now have a specific Extensible Markup Language (XML) schema that must be adhered to. Failure to meet this schema results in the JMB not being processed at Service Now.

Availability

The AI-Scripts attempt to send JMBs to possible Service Now target locations configured at installation.

AI-Scripts are written in XSLT language and can be viewed as clear text. This affords transparency and visibility into the script logic at the device.

Junos Space Service Now

Junos Space Service Now is installed on the customer or partner network and is fully managed and maintained by customer or partner personnel. Juniper Networks personnel do not require access to Service Now to provide services. The Service Now security model focuses on customer protection. In line with this objective, all transactions from Service Now to a cascaded Service Now (such as Service Now running partner proxy) or to JSS use a "push" model. Service Now always works as a client when communicating with external systems. This helps customers and partners maintain network security, as only outbound communications are allowed.

Confidentiality

- Once a device has been discovered, the Junos Space Network Management Platform synchronizes the configuration on the device and marks it managed. Junos Space uses ICMP or SNMP for the initial discovery process for devices. For devices running worldwide Junos OS, device discovery is done via a telnet session. The device discovery can be initiated via the device or initiated by Junos Space. Once the device has been discovered, all information exchange happens over DMI.
- AI-Scripts are installed and configured on devices via SSH and some combination of NETCONF and DMI.

Integrity

- The Junos Space Network Management Platform resynchronizes the configuration with individual devices when any trigger that impacts device connectivity or configuration is detected.
- All instances of Service Now must be authorized by the JSS service (or associated partner proxy) before any data is transmitted. During the Service Now setup, credentials previously established with Juniper Networks are entered on the administration console. When Service Now connects to the JSS gateway application, the software and service credentials are validated before information is shared. JSS also conducts a services entitlement check before any data is transmitted.
- All connections to Service Now, Service Insight or both are always authenticated before they are served. Every connection from Service Now and Service Insight to JSS is stateless. Stateful connections are not supported.

Availability

- The Junos Space Network Management Platform is built to be an enterprise-class platform with inherent high availability (HA) and resiliency features that include clustering for load balancing and HA mode for redundant operation.

Data held, processed and transmitted from Service Now is afforded the following protections:

Confidentiality

- Service Now to JSS communication utilizes industry standard Secure Sockets Layer (SSL) communication to either an upstream Service Now or JSS.
- Information JMBs (iJMBs) can only be sent once Service Now is configured, licensed and activated by the customer or partner.
- The device configuration information forwarded to JSS by Service Now is configurable by the end customer or partner to provide protection for any sensitive information. There are four levels of configuration filtering that a customer or partner can use to define the amount of information shared with Juniper Networks:
  - full share (all configuration)
  - configuration with IP addresses removed
  - configuration indexes only (only a list of configuration options used without any specific information included)
  - no share (only for intelligence JMB)
- Role-based access control (RBAC) policies are available to apply to Junos Space user accounts. Junos Space administrators can restrict the operations and permissions of individual users to maintain necessary control over user authority. Actions that can be assigned to individual users include opening cases with Juniper (JSS) or Service Now partner proxy, assigning detected events to other Service Now users, deleting events reports, and creating a notification policy that defines notifications sent by Service Now to external systems.
- Junos Space is expected to allow users to be configured to have access and control to "logical" environments. Each "organization" in Service Now represents an individual environment with its own NEs and device groups, and users can be associated to these. RBAC policies are applied at the organization level. This allows for customers and partners to effectively separate networks and apply different policies for user authority for each network or customer configured on Service Now.

Integrity

- Checks including using encrypted site ID credentials for authentication and authorization and validating JMB file composition ensure that data passed from Service Now to an upstream Service Now or JSS is authentic and complete. Each JMB must adhere to a specific structure and schema. When processing JMBs, Service Now first checks these elements and rejects JMBs that do not match standards.

Availability

- Service Now is architected so that if the transfer of JMBs to the JSS fails, it retries sending the same.

The only regular traffic types that are sent between devices and Service Now are JMBs and system log messages. JMBs are uncompressed XML text-only files. Informational (iJMBs) and Event (eJMBs) JMBs are collected from the devices by the appliance on receipt of an appropriate system log message. Any JMBs created by the network device are marked so they are sent by best-effort queues if default class-of-service configurations are used.

iJMBs are delivered from Service Now to Juniper Networks (JSS) the first time they are received from a device and thereafter once every week. eJMBs are delivered when a user submits a case.

Service Now requests the following information from Juniper Support Systems via a secure Internet connection:

- Case updates—These are updates to case status for all cases opened against the customer contract.
- Intelligence updates—These include notifications and message alerts.

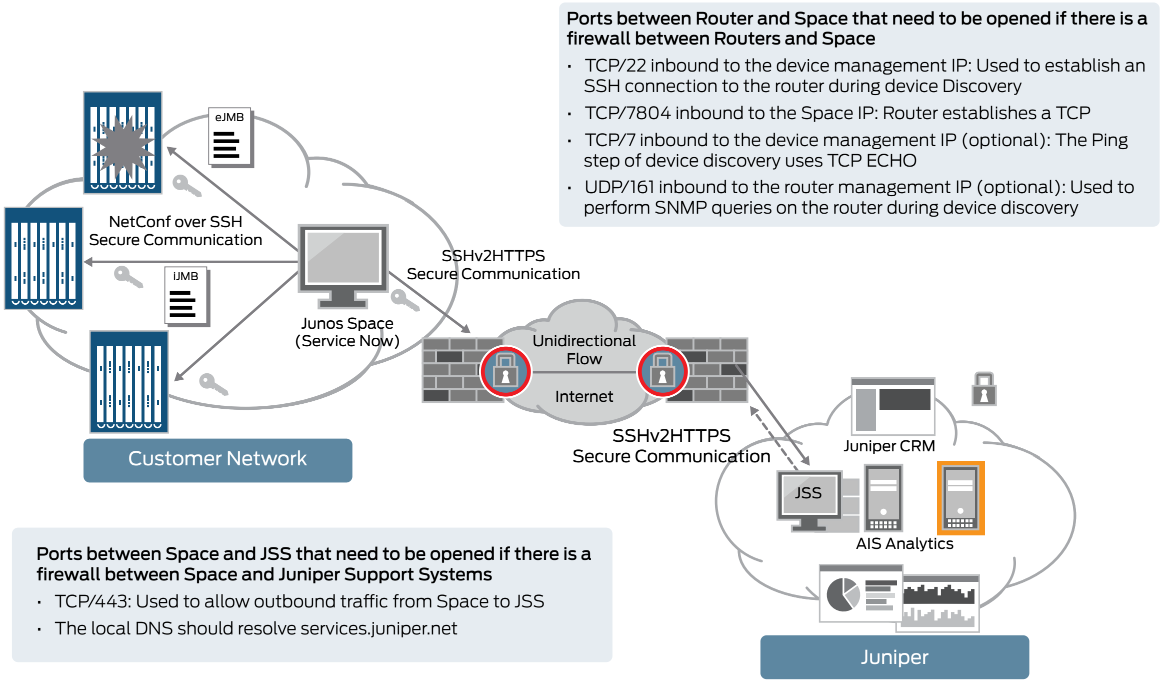
Service Now can send the following:

- Notification emails
- SNMP traps

Service Insight requests the following information from Juniper Support Systems via a secure Internet connection:

- Proactive bug notification report (PBN) and EOL/EOS reports

All standard ports used for communications between the device, Junos Space and JSS are listed in Figure 3.



Ports between Router and Space that need to be opened if there is a firewall between Routers and Space

- TCP/22 inbound to the device management IP: Used to establish an SSH connection to the router during device Discovery
- TCP/7804 inbound to the Space IP: Router establishes a TCP
- TCP/7 inbound to the device management IP (optional): The Ping step of device discovery uses TCP ECHO
- UDP/161 inbound to the router management IP (optional): Used to perform SNMP queries on the router during device discovery

Ports between Space and JSS that need to be opened if there is a firewall between Space and Juniper Support Systems

- TCP/443: Used to allow outbound traffic from Space to JSS
- The local DNS should resolve services.juniper.net

Figure 3: Guide to communication protocols between Service Now and network nodes and Service Now and JSS

Support System

As data enters Juniper Support Systems, it traverses Juniper Networks' own security infrastructure. Particular care is taken to protect the infrastructure here, not just at the edge of Juniper's network, but also internally—to ensure that only those with a "need to know" can access the information from within.

Confidentially

- Juniper's internal authentication, authorization, and accounting (AAA) mechanisms are applied to ensure that access to customer or partner information occurs only for appropriately authorized and authenticated staff, and is auditable by approved staff.

Integrity

- Checks including encrypted site IDs, JMB validation, and authentication and authorization checks ensure that data passed from Service Now and Service Insight to JSS is authentic and complete.

Availability

- JSS and its supporting infrastructure are designed with fault tolerance and are highly resilient, ensuring that service is available on a 24x7x365 basis for customers, partners and Juniper Networks staff.

Solution Guidelines for Deployment and Operation

Juniper Networks Service Automation solution provides you with the flexibility of deployment and operation based on how you receive support on your Juniper products.

Customers receiving support directly from Juniper can configure Service Now with their support contract to connect directly with JSS for getting support from JTAC.

Customers receiving support from an Operate Specialist partner should contact their support provider for more details on how to take advantage of automation functionality.

The Service Now and Service Insight applications are the user interface to the Service Automation solution. The Junos Space Network Management Platform itself is available as a virtual platform or an appliance-based platform. We recommend that the following security procedures be followed when deploying Junos Space and some combination of Service Now and Service Insight in their environment.

Design and Planning

- Carry out a risk assessment encompassing all aspects of the Service Automation deployment.
- Document the devices and data to be included in the coverage for Service Now, Service Insight or both.
- Assess the level of filtering necessary on the data that Service Now forwards to JSS.
- Create a full security profile for the project, including appropriate design, deployment and operational information.

Deployment

- Carry out hardening according to recommendations.
- Ensure that communication between Network Elements and Junos Space uses out-of-band (OOB) management infrastructure where possible, or other segregation mechanisms such as VLANS or MPLS VPNs.
- Configure Junos Space in HA mode to ensure availability.

Operational

- Restrict access to the Junos Space Network Management Platform to staff with a direct operational requirement.
- Utilize RBAC procedures to limit the administration commands to authorized users only.
- Ensure that all logs from this server are exported off the host and regularly checked.
- Place Junos Space Network Management Platform in a secure, monitored segment of the OOB management network.
- Carry out regular maintenance of the underlying operating system according to the manufacturer's recommendation—applies to Junos Space Network Management Platforms running on a virtualized environment.

Conclusion

Juniper Networks Service Automation solution can provide significant benefits to the organization deploying it. With a carefully planned and implemented security plan as part of the deployment strategy, security can be maintained at an appropriate level, in line with the organization's own security profile, objectives and policy.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

2000466-002-EN Jan 2013

Printed on recycled paper