ExtremeSwitching™

Configuring the SLA Mon Agent for VOSS

Release 8.1.5 (VOSS)
9035886-01 Rev AA
April 2020

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Extreme Networks VSP 4000 Series (includes VSP 4450 Series)
- Extreme Networks VSP 4900 Series
- Extreme Networks VSP 7200 Series
- Extreme Networks VSP 7400 Series
- Extreme Networks VSP 8000 Series (includes VSP 8200 Series and VSP 8400 Series)
- Extreme Networks VSP 8600 Series
- Extreme Networks XA1400 Series

> **Note:**
>
> VOSS is licensed on the XA1400 Series as a Fabric Connect VPN (FCVPN) application, which includes a subset of VOSS features. FCVPN transparently extends Fabric Connect services over third-party provider networks.

This document provides conceptual and procedural information to configure the Service Level Agreement Monitor (SLA Mon) agent as part of the SLA Mon solution.

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
❗ **Important:**	A situation that can cause serious inconvenience.
✳ **Note:**	Important features or instructions.
➕ **Tip:**	Helpful tips and notices for using the product.
⚠ **Danger:**	Situations that will result in severe bodily injury; up to and including death.
⚠ **Warning:**	Risk of severe personal injury or critical loss of data.
⚠ **Caution:**	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.

Table continues…

Convention	Description
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware/software compatibility matrices for Campus and Edge products
Supported transceivers and cables for Data Center products
Other resources, like white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Document

There are no feature changes in this document.

Notice about Feature Support

This document includes content for multiple hardware platforms across different software releases. As a result, the content can include features not supported by your hardware in the current software release.

If a documented command, parameter, tab, or field does not appear on your hardware, it is not supported.

For information about physical hardware restrictions, see your hardware documentation.

Chapter 3: Service Level Agreement Monitor

Table 3: SLA Mon product support

Feature	Product	Release introduced
For configuration details, see Configuring the SLA Mon Agent for VOSS.		
SLA Mon	VSP 4450 Series	VOSS 4.1
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	Not Supported

The switch supports the Service Level Agreement Monitor (SLA Mon) agent as part of the SLA Mon solution.

SLA Mon uses a server and agent relationship to perform end-to-end network Quality of Service (QoS) validation and to distribute monitoring devices. You can use the test results to target under-performing areas of the network for deeper analysis.

SLA Mon Server and Agent

The switch supports the SLA Mon agent. You must have an Avaya Diagnostic Server with SLA Mon technology in your network to use the SLA Mon feature. Most of the SLA Mon configuration occurs on the server; configuration on the SLA Mon agent is minimal.

The SLA Mon server initiates the SLA Mon functions on one or more agents, and the agents run specific QoS tests at the request of the server. Agents can exchange packets between one another to conduct the QoS tests.

SLA Mon can monitor a number of key items, including the following:

- network paths

- Differentiated Services Code Point (DSCP) markings
- loss
- jitter
- delay

The following figure shows an SLA Mon implementation.

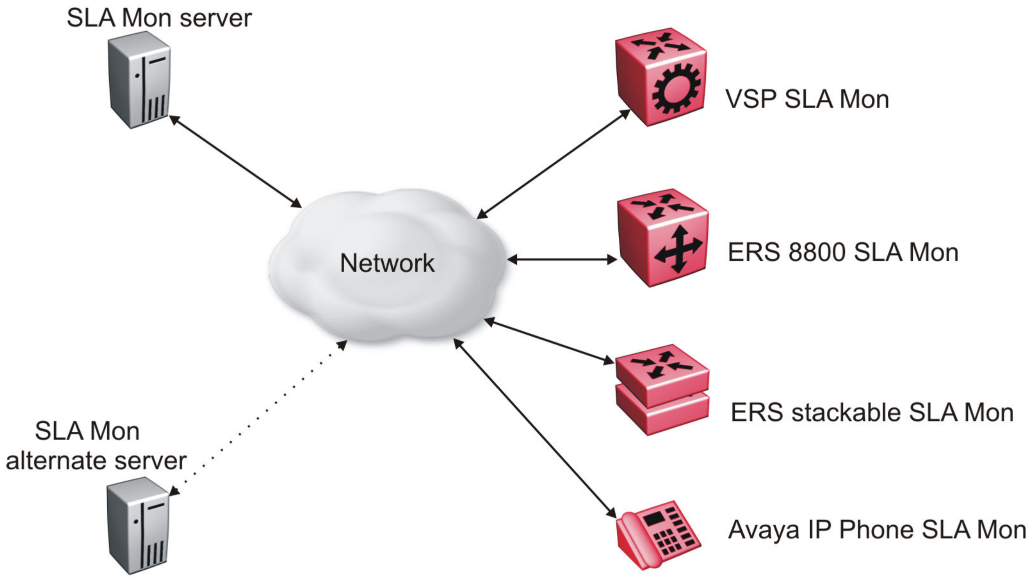

Figure 1: SLA Monitor network

An SLA Mon agent remains dormant until it receives a User Datagram Protocol (UDP) discovery packet from a server. The agent accepts the discovery packet to register with an SLA Mon server. If the registration process fails, the agent remains dormant until it receives another discovery packet.

An agent can attempt to register with an SLA Mon server once every 60 seconds. After a successful registration, the agent reregisters with the server every 6 hours to exchange a new encryption key.

An agent only accepts commands from the SLA Mon server to which it is registered. An agent can use alternate SLA Mon servers to provide backup for time-out and communication issues with the primary SLA Mon server.

Note:

If you configure the SLA Mon agent address under an IP address for a VLAN or brouter, you must remove the SLA Mon address before you can remove the IP address for the VLAN or brouter.

HA Support

SLA Monitor agent provides partial HA support. In HA mode, the agent startup and initialization occurs only on the master CP module. When reset occurs, the standby CP takes over the operations. Based on the SLAMon agent operation-mode, the agent on the standby CP restarts the initialization and registration and gets registered only when the server sends a discovery. The user configuration updates on the Master CP is saved on the Standby CP and used when the reset occurs.

QoS tests

SLA Mon uses two types of tests to determine QoS benchmarks:

- Real Time Protocol (RTP)

  This test measures network performance — for example, jitter, delay, and loss — by injecting a short stream of UDP packets from source to destination (an SLA Mon agent).
- New Trace Route (NTR)

  This test is similar to traceroute but also includes DSCP values at each hop in the path from the source to the destination. The destination does not need to be an SLA Mon agent.

Limitations

SLA Mon agent communications are IPv4–based. Agent communications do not currently support IPv6.

SLA Mon configuration using CLI

Configuring the SLA Mon Agent

Configure the SLA Mon agent to communicate with an SLA Mon with SLA Mon technology to perform Quality of Service (QoS) tests of the network.

Before you begin

- To use the SLA Mon agent, you must have an Avaya Diagnostic Server with SLA Mon technology in your network.

About this task

To configure the SLA Mon agent, you must assign an IP address and enable it. Remaining agent parameters are optional and you can operate the agent using the default values.

Note:

- If you want to change SLA Mon parameters, you must first disable SLA Mon.

If you are configuring SLA Mon at the switch side for the first time, make sure you configure the SLA Mon agent address under an IP address for a VLAN or brouter, and you must remove the SLA Mon address before you can remove the IP address for the VLAN or brouter. To remove the SLA Mon address, first use the command **`no slamon oper-mode enable`**, followed by **`slamon agent ip address 0.0.0.0`**.

Procedure

1. Enter Application Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   application
   ```

2. Configure the SLA Mon agent IP address:

   Note:

   The SLA Mon Agent uses its own reserved Host IP address, reachable via the Switch VLAN IP interface of the same IP subnet.

   ```
   slamon agent ip address {A.B.C.D} [vrf WORD<1-16>]
   ```

3. **(Optional)** Configure the UDP port for agent-server communication:

   ```
   slamon agent port <0-65535>
   ```

4. **(Optional)** Restrict which servers an agent can use:

   ```
   slamon server ip address {A.B.C.D} [{A.B.C.D}]
   ```

   ```
   slamon server port <0-65535>
   ```

5. **(Optional)** Control the port used for Real Time Protocol (RTP) and New Trace Route (NTR) testing:

   ```
   slamon agent-comm-port <0-65535>
   ```

6. **(Optional)** Install a Secure Socket Layer (SSL) certificate for the agent:

   ```
   slamon install-cert-file WORD<0-128>
   ```

7. Enable the agent:

   ```
   slamon oper-mode enable
   ```

8. Verify the agent configuration:

   ```
   show application slamon agent
   ```

Example

- Configure the SLA Mon agent IP address. Configure the agent so that it only accepts registration packets from a specific server communicating on a specific port. Finally, enable the SLA Mon agent, and then verify the configuration.

  ```
  Switch:1>enable
  Switch:1#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  ```

```
Switch:1(config)#application
Switch:1(config-app)#slamon agent ip address 192.0.2.1
Switch:1(config-app)#slamon server ip address 192.0.2.24
Switch:1(config-app)#slamon server port 50011
Switch:1(config-app)#slamon oper-mode enable
Switch:1(config-app)#show application slamon agent
==================================================================
                            SLA Monitor Agent Info
==================================================================
SLAMon Operational Mode: Enabled
SLAMon Agent Address: 192.0.2.1
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Registered
SLAMon Registered Server Address: 192.0.2.24
SLAMon Registered Server Port: 50011
SLAMon Server Registration Time: 130
SLAMon Encryption Mode: Supported
SLAMon Configured Agent Address: 192.0.2.1
SLAMon Configured Agent Port: 0
SLAMon Configured Server Address: 192.0.2.24 0.0.0.0
SLAMon Configured Server Port: 50011 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0
SLAMon Configured Agent Address Vrf Name:
```

Note:

The SLA Mon agent IP address given in this example is on the same subnet as `VLAN120`, as shown below.

- Show result of the SLA Mon agent IP address.

```
Switch:1#show ip interface
=====================================================================================
IP Interface - GlobalRouter
=====================================================================================
INTERFACE IP           NET             BCASTADDR REASM   VLAN BROUTER
          ADDRESS      MASK            FORMAT    MAXSIZE ID   PORT
-------------------------------------------------------------------------------------
Clip1     198.51.100.0 255.255.255.255 ones      1500     -   false
Vlan120   192.0.2.24   255.255.255.0   ones      1500   120  false
Vlan126   198.51.100.2 255.255.255.0   ones      1500   126  false
Vlan129   198.51.100.5 255.255.255.0   ones      1500   129  false
Vlan130   198.51.100.7 255.255.255.0   ones      1500   130  false
All 5 out of 5 Total Num of IP interfaces displayed
```

Next steps

If you have configured SLA Mon, but the agent does not function as expected, use the **`show khi performance pthread [{slot[-slot][,...]}]`** command to verify that the slamon task is running.

If the SLA Mon agent is not running, use the commands **`no slamon oper-mode enable`** and **`slamon oper-mode enable`** to start the agent.

If the agent task is running, perform typical troubleshooting steps to verify agent accessibility:

- Verify IP address assignment and port use.
- Ping the server IP address.
- Verify the server configuration.
- Use the **`trace level 192 <0-4>`** command to observe the status of the SLA Mon software module.

Variable definitions

Use the data in the following table to use the **slamon** command.

Variable	Value
agent-comm-port *<0–65535>*	Configures the port used for RTP and NTR testing in agent-to-agent communication. The default port is 50012. If you configure this value to zero (0), the default port is used.
agent ip address {A.B.C.D}	Configures the SLA Mon agent IP address. You must configure the IP address before the agent can process received discovery packets from the server. The agent ip address is a mandatory parameter. The default value is 0.0.0.0.
agent port *<0–65535>*	Configures the UDP port for agent-server communication. The SLA Mon agent receives discovery packets on this port. The default is port 50011. The server must use the same port.
install-cert-file	Installs an SSL certificate. *WORD<0-128>* specifies the file name and path of the certificate to install. If you install a certificate on the SLA Mon agent, you must ensure a matching configuration on the server.
oper-mode enable	Enables the SLA Mon agent. The default is disabled. If you disable the agent, it does not respond to discovery packets from a server. If you disable the agent because of resource concerns, consider changing the server configuration instead, to alter the test frequency or duration, or the number of targets.
server ip address {A.B.C.D} [{A.B.C.D}]	Restricts the SLA Mon agent to use the server at this IP address only. The default is 0.0.0.0, which means the agent can register with any server. You can specify a secondary server as well.
server port *<0–65535>*	Restricts the SLA Mon agent to use this registration port only. The default is 0, which means the agent disregards the source port information in server traffic. The server must use the same port.
vrf *WORD<1-16>*	Specifies the name of a VRF.

SLA Mon Configuration using EDM

Configuring the SLA Mon Agent

Configure the SLA Mon agent to communicate with an Avaya Diagnostic Server with SLA Mon technology to perform Quality of Service (QoS) tests of the network.

Before you begin

- To use the SLA Mon agent, you must have an Avaya Diagnostic Server with SLA Mon technology in your network.

About this task

To configure the SLA Mon agent, you must assign an IP address and enable it. Remaining agent parameters are optional and you can operate the agent using the default values.

✱ **Note:**

If you want to change SLA Mon parameters, you must first disable SLA Mon.

If you configure the SLA Mon agent address under an IP address for a VLAN or brouter, you must remove the SLA Mon address, before you can remove the IP address for the VLAN or brouter. To remove the SLA Mon address, first select disabled from the **Status** field, then configure the IP address in the **ConfiguredAgentAddr** field to 0.0.0.0.

Procedure

1. In the navigation pane, expand the **Configuration** > **Serviceability** folders.
2. Click **SLA Monitor**.
3. Click the **SLA Monitor** tab.
4. For the status, select **enabled**.
5. In the **ConfiguredAgentAddr** field, enter the SLA Mon agent IP address
6. Configure optional parameters as required.
7. Click **Apply**.

SLA Monitor field descriptions

Use the data in the following table to use the **SLA Monitor** tab.

Name	Description
Status	Enables or disables the SLA Mon agent. The default is disabled. If you disable the agent, it does not respond to discovery packets from a server. If you disable the agent because of resource concerns, consider changing the server configuration instead, to alter the test frequency or duration, or the number of targets.

Table continues…

Name	Description
CertFileInstallAction	Installs or uninstalls a Secure Sockets Layer (SSL) certificate file. The default is noAction.
CertFile	Specifies the file name and path of the SSL certificate. If you install a certificate on the SLA Mon agent, you must ensure a matching configuration on the server.
ConfiguredAgentAddrType	Specifies the address type of the agent: IPv4.
ConfiguredAgentAddr	Configures the agent IP address. You must configure the IP address before the agent can process received discovery packets from the server. The agent IP address is a mandatory parameter. The default value is 0.0.0.0.
ConfiguredAgentPort	Configures the UDP port for agent-server communication. The SLA Mon agent receives discovery packets on this port. The default is port 50011. The server must use the same port.
ConfiguredAgentVrfName	Specifies the name of a VRF.
ConfiguredServerAddrType	Specifies the address type of the server: IPv4.
ConfiguredServerAddr	Restricts the SLA Mon agent to use the server at this IP address only. If the default of 0.0.0.0 is used, then the SLA Mon agent can register with any server.
ConfiguredServerPort	Restricts the SLA Mon agent to use this registration port only. The default is 0, which means the agent disregards the source port information in server traffic. The server must use the same port.
ConfiguredAltServerAddrType	Specifies the address type of the secondary server: IPv4.
ConfiguredAltServerAddr	Configures a secondary server in the event that the primary server is unreachable.
ConfiguredAltServerPort	Restricts the SLA Mon agent to use this registration port on the secondary server only. The default is 0, which means the agent disregards the source port information in server traffic. The server must use the same port.
SupportedApps	Shows the type of testing supported: Real Time Protocol (RTP) and New Trace Route (NTR).
AgentAddressType	Shows the SLA Mon agent address type.
AgentAddress	Shows the configured SLA Mon agent IP address.
AgentPort	Shows the configured SLA Mon agent port.
RegisteredWithServer	Indicates if the SLA Mon agent has registered with a server.

Table continues…

Name	Description
RegisteredServerAddrType	Shows the address type for the registered server.
RegisteredServerAddr	Shows the IP address for the registered server.
RegisteredServerPort	Shows the port number for the registered server.
RegistrationTime	Shows the amount of time, in seconds, since the SLA Mon agent registered with the server.
AgentToAgentPort	Shows the port for SLA Mon agent-to-agent communication.
ConfiguredAgentToAgentPort	Configures the port used for RTP and NTR testing in SLA Mon agent-to-agent communication. The default port is 50012. If you configure this value as zero (0), the default port is used.