Juniper Networks NSM Plug-In
Version 7.1.0 (MR2)

User Guide

IBM

Note: Before using this information and the product that it supports, read the information in "Notices and Trademarks" on page 13.

CONTENTS

ABOUT THIS GUIDE

The *Juniper Networks NSM Plug-In Users Guide* provides you with information on installing and configuring the Juniper Networks NSM Plug-In.

Intended Audience

The guide is intended for system administrators responsible for installing, configuring, or using plug-in components on your IBM Security QRadar SIEM Console.

Conventions

The following conventions are used throughout this guide:

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.

WARNING: Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.

Technical Documentation

For information on how to access more technical documentation, technical notes, and release notes, see the *Accessing IBM Security QRadar Documentation Technical Note*.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacting Customer Support

For information on contacting customer support, see the *Support and Download Technical Note*.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of

your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

1 INSTALLING THE NSM PLUG-IN

You can use the Juniper Networks NSM Plug-In to view policy details from the Juniper Networks NSM server for an event.

NSM Plug-In overview

Juniper Networks Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. Juniper Networks NSM delivers integrated, policy-based security and network management for all devices.

Ensure you have the latest QRadar SIEM patch installed on your IBM Security QRadar SIEM Console (Patch 7.0.0.182810 or later).

Installing the Juniper Networks NSM Plug-In results in the httpd and Tomcat processes automatically restarting. This causes a service disruption while the processes restart.

Installing the NSM Plug-In

Use SSH to install the Juniper Networks NSM Plug-In on your QRadar SIEM Console.

About this task

The target directory (/opt/qradar/conf/webplugins/117/) must exist on your QRadar SIEM system. After you install the plug-in, the target directory is automatically created when you log in to the QRadar SIEM user interface and click the **NSM Settings Plugin** icon on the **Admin** tab.

If multiple users or remote users are viewing the **Admin** tab, you may need to refresh your browser for the NSM Plug-in Settings icon to be displayed.

Procedure

Step 1   Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**

Step 2   To verify that you have the `nsm_plugin-7.0.0-<build>.i386.rpm` file, type the following command:

```
ls /opt/qradar/rpms
```

Where `<build>` is the related build number.

If the file is not listed, go to **Step 3**. If the file is listed, go to **Step 4**.

Step 3   Mount the QRadar SIEM installation ISO file and install the NSM Plug-in rpm:

   a   To mount the IBM Security QRadar SIEM installation ISO file, type the following command:

```
mount -o loop <path to the QRadar ISO> /media/cdrom
```

Where `<path to the QRadar SIEM ISO>` is the directory path to where the installation ISO is stored.

   b   Type the following command to unpack and install the NSM Plug-in rpm:

```
rpm -Uvh
/media/cdrom/post/qradar/nsm_plugin-7.0.0-<build>.i386.rpm
```

Where `<build>` is the related QRadar SIEM build number.

The package manager automatically unpacks and installs the NSM Plug-in rpm.

The NSM Plug-in installation is complete when the following text is displayed:

```
Starting Tomcat: [ok]
Starting httpd: [ok]
```

   c   Go to **Step 5**.

Step 4   Type the following command:

```
rpm -Uvh /opt/qradar/rpms/nsm_plugin-7.0.0-<build>.i386.rpm
```

Where `<build>` is the related QRadar SIEM build number.

The package manager automatically unpacks and installs the NSM Plug-in rpm.

The NSM Plug-in installation is complete when the following text is displayed:

```
Starting Tomcat: [ok]
Starting httpd: [ok]
```

Step 5   To create the target directory:

   a   Log in to the QRadar SIEM user interface:

```
https://<IP Address>
```

Where `<IP Address>` is the IP address of the QRadar SIEM system.

Username: **admin**

Password: **<password>**

   b   Click the **Admin** tab.

   c   Click the **NSM Plug-in Settings** icon.

Step 6   Choose one of the following options:

   •   To connect to a Juniper NSM 2010 device, go to **Step 7**.

   •   To connect to another Juniper NSM version, go to **Step 10**.

Step 7 Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**

Step 8 Type the following command to copy the server certificate from your Juniper NSM appliance to QRadar SIEM:

```
scp root@<NSM IP
address>:/usr/netscreen/GuiSvr/lib/webproxy/conf/server.crt
/opt/qradar/conf/webplugins/117/nsmPlugin.cert
```

Where **<NSM IP address> is the** IP address of the Juniper Networks NSM server.

The server.crt file is copied from the Juniper Networks NSM appliance and renamed to nsmPlugin.cert on your QRadar SIEM Console.

Step 9 Type the following command to set the file permission for the directory and the nsmPlugin.cert file:

```
chown nobody:nobody
/opt/qradar/conf/webplugins/117/nsmPlugin.cert
```

Step 10 Type the following command to restart Tomcat:

```
service tomcat restart
```

What to do next

Setting up the plug-in

2 SETTING UP THE PLUG-IN

The Juniper Networks NSM Plug-in allows IBM Security QRadar SIEM to integrate with your Juniper Networks NSM appliance to view policy-based security and network management information from NSM appliances. Before you can view policy information, you must configure QRadar SIEM permissions and user roles.

Configuring the server settings

After you have successfully installed the Juniper Networks NSM Plug-in, you must configure your QRadar SIEM Console with the IP address and port number of your Juniper Networks NSM appliance.

Procedure

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Plug-ins**.

Step 3 In the Plug-In Configuration pane, click the **NSM Plug-in Settings** icon.

Step 4 In the **NSM Server URL** field, type the IP address or hostname of the Juniper Networks NSM server to which you want to connect. For example, https://192.168.2.1:8443.

Step 5 Click **Save Changes**.

Setting user permissions

You must ensure that each QRadar SIEM user who requires access to the Juniper NSM Plug-in has been assigned the appropriate user permissions. You must have administrative privileges to configure user roles in QRadar SIEM.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 In the User Management pane, click the **User Roles** icon.

Step 4 Choose one of the following options:

a If you want to create a new role, click **Create Role**.

b If you want to edit an existing role to include NSM Plug-in Settings, click the **Edit** icon for the role which requires the assigned permissions.

Step 5   Select the user permissions for the NSM Plug-in Settings:

   • **Launch NSM Client** - Select this check box if you want to allow users to launch the NSM Client from the main user interface. By default, this check box is clear.

   • **View NSM Policy Details from Events interface** - Select this check box if you want to allow users to view policy details for the Juniper Networks NSM server from the Log Activity page. By default, this check box is clear.

Step 6   Select the remaining permissions. For more information on role permissions, see the *IBM Security QRadar SIEM Administration Guide*.

Step 7   Complete the steps of the wizard.

Step 8   On the **Admin** tab, click **Deploy Changes**.

Setting user preferences

All users with the **View NSM Policy Details from Events interface** role permission must enter their user settings to authenticate their user account with the Juniper Networks NSM server. This ensures that appropriate users are able to view policy details for an event.

Before you begin

Make sure you have Events permissions to access the policy details.

About this task

If your administrator has not completed the configuration of the plug-in, an information message is displayed. Contact your system administrator to complete the configuration before continuing. For more information, see **Configuring the server settings**.

If your credentials are rejected by the Juniper Networks NSM server, but you have verified your access information, your IP address may be blocked by the Juniper Networks NSM server as a result of too many failed login attempts. Contact your Juniper Networks NSM server administrator to unblock the following IP address: 127.0.0.1 using the **Tools > Manage Blocked Hosts** option in the Juniper Networks NSM client.

Procedure

Step 1   In the upper-right corner of the IBM Security QRadar SIEM user interface, click **NSM Preferences**.

Step 2   Enter values for the following parameters:

   • **NSM Login** - Type your user name, as defined on the Juniper Networks NSM server.

   • **NSM Password** - Type your password, as defined on the Juniper Networks NSM server.

   • **NSM Domain** - Type your domain, as defined on the Juniper Networks NSM server. The default is global.

Step 3   Click **Save Changes**.

3 USING THE PLUG-IN

After you have configured and set up the plug-in, you can view policy event information.

Launching NSM

You can launch NSM from the QRadar SIEM user interface.

Procedure

Step 1   In the upper-right corner of the IBM Security QRadar SIEM user interface, click **Launch NSM**.

Step 2   Choose one of the following options:

- If you are using FireFox and this is the first time you are launching NSM, go to **Step 3**.

- If you are using Microsoft® Internet Explorer 8.0 or 9.0, with Compatibility View enabled, and this is the first time you are launching NSM, go to **Step 4**.

- If you have previously launched NSM, go to **Step 5**.

Step 3   To launch NSM for the first time using FireFox:

    a   In the Opening window, select the **Open with** option.

    b   Click **Browse**.

    c   Select the NSM executable from the appropriate directory:

        -   For NSM 2010, the file path is c:\Program Files\Network and Security Manager\NSM.exe.

        -   For previous NSM versions, the file path is c:\Program Files\NSM\NSM.exe.

    d   Click **OK**.

    e   Select the **Do this automatically for files like this from now on** check box.

    f   Click **OK**.

    g   Go to **Step 5**.

Step 4   To launch NSM for the first time using Internet Explorer 8.0 or 9.0, with Compatibility View enabled, you must:

    a   Create a new association for the .nsm extension and change the extension to access the NSM.exe file. Select the NSM executable from the appropriate directory:

- For NSM 2010, the file path is c:\Program Files\Network and Security Manager\NSM.exe.

- For previous NSM versions, the file path is c:\Program Files\NSM\NSM.exe.

For more information on creating a file association, see your vendor documentation.

b Go to **Step 5**.

Step 5 Type the necessary login credentials for the Juniper Networks Client.

Step 6 Click **OK**.

Viewing policy details

After the Juniper Networks NSM Plug-In is installed and configured, you can view policy details using the Log Activity tab. However, before you can view policy details, you must add the **NSM Policy (custom)** column to the Log Activity page display.

Adding the policy column

Use the event search page to add the **NSM Policy (custom)** column to the Log Activity page:

About this task

This task includes only the search criteria for displaying **NSM Policy (custom)** column. For information about additional search parameters, see the *IBM Security QRadar SIEM Users Guide*.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, select **New Search**.

Step 3 From the **Available Columns** list, select **NSM Policy (custom)**.

Step 4 Select the arrow to move the item to the **Column** list.

Step 5 Click **Filter**.

Result

The Log Activity page displays the **NSM Policy (custom)** column.

Viewing policy details

You can view policy details from the Log Activity tab.

About this task

Each Juniper Networks NSM policy includes groups of rule bases and rules. This window provides details of the selected NSM policy and details of the associated rules for this policy. This window may require several minutes to populate depending on the amount of data.

For more information on the Juniper Networks NSM policy, see your Juniper Networks NSM documentation.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 If events are displayed in Real Time (streaming) mode, click the Pause button.

Step 3 Right-click the NSM Policy (custom) parameter for the event you want to investigate, and then select **More options > View NSM Policy Details**.

A   NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

INDEX

A

adding
    policy column 10

C

configure
    server settings 7
conventions 1

I

installing
    plug-in 3

N

NSM plug-in
    installing 3
    launching 9

P

plug-in
    installing 3
    using 9
policy column
    adding 10
policy details
    viewing 10

S

server settings
    configure 7
setup
    server settings 7
    user permissions 7
    user preferences 8

U

user permissions
    setting 7
user preferences
    setting 8