Sentinel Link Overview Guide

Sentinel Plug-Ins 2011.1r2

December 2012

Legal Notice

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

This product may also claim FIPS compliance by use of one or more of the Open SSL cryptographic components listed below. These components were certified by the Open Source Software Institute and obtained the FIPS certificates as indicated.

918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1

1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1

1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

Note: Windows FIPS algorithms used in this product may have only been tested when the FIPS mode bit was set. While the modules have valid certificates at the time of this product release, it is the user's responsibility to validate the current module status.

This product may also claim FIPS compliance by use of the following Network Security Services (NSS) component listed below. This component was certified by Wind River Systems, Inc. and obtained the FIPS certification via the CMVP.

1475 - Network Security Services (NSS) v 3.12.4 - 140-2

Contents

About This Guide

The *Sentinel Link Overview Guide* helps you understand how to use Sentinel Link to send event data from a Sentinel system to other Sentinel installations.

Audience

This guide is intended for the Sentinel administrator.

Additional Documentation

For complete documentation on the Sentinel products, see the NetIQ Documentation Web site.

For information on building your own plug-ins, see the Sentinel SDK Web page.

Contacting Novell and NetIQ

Sentinel is now a NetIQ product, but Novell still handles many support functions.

- Novell Web site
- NetIQ Web site
- Technical Support
- Self Support
- Patch download site
- Sentinel Community Support Forums
- Sentinel TIDs
- Sentinel Plug-in Web site
- **Notification Email List:** Sign up through the Sentinel Plug-in Web site

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide: NetIQ Office Locations

United States and Canada: 888-323-6768

Email: info@netiq.com

Web site: www.netiq.com

1 Introduction

Sentinel Link is a mechanism that provides the ability to hierarchically link multiple Sentinel servers, including Sentinel Log Manager, Sentinel, and Sentinel Rapid Deployment. You can hierarchically link two or more Sentinel servers to forward filtered events from one Sentinel server to another for further evaluation.

1.1 Benefits

- Multiple Sentinel Log Manager servers, local or distributed, can be linked in a hierarchical manner. Using this setup, Sentinel Log Manager servers can manage a large volume of data, retaining raw data and event data locally, while forwarding important events to a central Sentinel Log Manager for consolidation.
- One or more Sentinel Log Manager servers can forward important data to either a Sentinel server or a Sentinel Rapid Deployment server. These systems provide real-time visualization of data, advanced correlation and actions, workflow management, and integration with identity management systems.
- Multiple Sentinel or Sentinel Rapid Deployment servers can be hierarchically linked to monitor the consolidated event information.
- One or more Sentinel or Sentinel Rapid Deployment servers can forward important events to a Sentinel Log Manager server for event consolidation.

1.2 Supported Platforms

- Sentinel 6.1 Service Pack 1 Hotfix 2 or later
- Sentinel 7 or later.
- Sentinel 6.1 Rapid Deployment Hotfix 2 or later
- Sentinel Log Manager 1.0 Hotfix 1 or later

1.3 Prerequisite

- Before you forward events from the sender computer, ensure that the Sentinel Link server is running on the receiver computer.

1.4 Configuring Sentinel Link

In a Sentinel Link setup, the Sentinel server that forwards the events is called the sender and the Sentinel server that receives the events is called the receiver. You can simultaneously link multiple Sentinel servers to a single receiver system.

To configure a Sentinel link, you must configure at least two systems: the sender computer and the receiver computer. For further details on configuring Sentinel Link, read the following:

- Chapter 3, “Configuring Sentinel Systems for Sending Events,” on page 15
- Chapter 2, “Configuring Sentinel Systems for Receiving Events,” on page 11

2 Configuring Sentinel Systems for Receiving Events

On the receiver computer, you must import and configure the Sentinel Link Collector, which generates events from the data received by the Sentinel Link Connector. You must also import the Sentinel Link Connector and configure a Sentinel Link Event Source Server to receive the event data from the sender computer.

NOTE: For more information on Sentinel Link Connector and Collector, see the corresponding plug-in documentation in the Sentinel Plug-ins Web site.

2.1 Accessing Event Source Management

This section describes how to access Event Source Management in different Sentinel products such as Sentinel 6.1, Sentinel 7.x, Sentinel 6.1 Rapid Deployment:, and Sentinel Log Manager.

2.1.1 Sentinel 6.x

To access Event Source Management in Sentinel 6.x:

1. As the Sentinel Administrator User (esecadm), change directory to:

   ```
   $ESEC_HOME/bin
   ```

2. Run the following command:

   ```
   control_center.sh
   ```

3. Specify the administrator user name and password, then click **OK**.
4. In the Sentinel Control Center, select **Event Source Management > Live View**.

2.1.2 Sentinel 7.x

To access Event Source Management in Sentinel 7.x:

1. Open a Web browser to the following URL:

   ```
   https://svrname.example.com:port/sentinel
   ```

Replace `svrname.example.com` with the actual DNS name or IP address (such as 192.168.1.1) of the server where Sentinel is running.

2. If you are prompted to verify the certificates, review the certificate information, then click **Yes** if it is valid.
3. Specify the user name and password for the Sentinel account you want to access.
4. Click **Log in**.
5. In the Sentinel Web interface, click **Collection**.
6. In the Collection page, click **Advanced**.
7. In the Advanced page, click **Launch Control Center** to open the Sentinel Control Center.
8. Select **Event Source Management > Live View**.

2.1.3 Sentinel Rapid Deployment

To access Event Source Management in Sentinel Rapid Deployment:

1. Open a Web browser to the following URL:

   `https://svrname.example.com:port/sentinel`

   Replace svrname.example.com with the actual DNS name or IP address (such as 192.168.1.1) of the server where Sentinel Rapid Deployment is running.
2. If you are prompted to verify the certificates, review the certificate information, and click **Yes** if it is valid.
3. Specify the user name and password for the Sentinel Rapid Deployment account you want to access.
4. Use the **Languages** list to specify which language you want to use.
5. Click **Sign in**.
6. In the Web interface, select **Applications** from the left panel.
7. In the Application page, click **Launch** to open the Sentinel Control Center.
8. Log in to the Sentinel Control Center as administrator.
9. Select **Event Source Management > Live View**.

2.1.4 Sentinel Log Manager

To access Event Source Management in Sentinel Log Manager:

1. Open a Web browser to the following URL:

   `https://svrname.example.com:port/novelllogmanager`

   Replace svrname.example.com with the actual DNS name or IP address (such as 192.168.1.1) of the server where Sentinel Log Manager is running.
2. If you are prompted to verify the certificates, review the certificate information, then click **Yes** if it is valid.
3. Specify the user name and password for the Log Manager account you want to access.
4. Use the **Languages** drop-down list to specify which language you want to use.
5. Click **Sign in**.
6. In the Log Manager Web interface, click **Collection**.

7 In the Collection page, click **Advanced**.

8 In the Advanced page, click **Launch** to open the Event Source Management.

2.2 Importing the Sentinel Link Collector

The Sentinel Link Collector comes pre-installed with the Sentinel platform. To get the latest performance enhancements and other enhanced features, visit the Sentinel Plug-ins Web site and download the latest set of Plug-ins.

NOTE: When updating any single Sentinel Link Plug-in, you should also update all related Plug-ins across all platforms to ensure compatibility.

For more information, see the Sentinel Link Collector documentation in the Sentinel Plug-ins Web site.

2.3 Importing the Sentinel Link Connector

The Sentinel Link Connector comes pre-installed with the Sentinel platform. To get the latest performance enhancements and other enhanced features, visit the Sentinel Plug-ins Web site and download the latest set of Plug-ins.

NOTE: When updating any single Sentinel Link Plug-in, you should also update all related Plug-ins across all platforms to ensure compatibility.

For more information, see the Sentinel Link Connector documentation in the Sentinel Plug-ins Web site.

2.4 Setting Up a Sentinel Link Connection

This section describes how to set up the Sentinel Link connection to receive messages from another Sentinel or Sentinel Log Management system, and enable the Collector to process the messages. To set up the Sentinel Link connection, you must, at a minimum, create and configure a Sentinel Link Event Source server. The Sentinel Link Event Source server automatically creates and configures the Connector, the Collector, and the Event Source nodes as needed. You can also manually create the Collector, the Connector, and the Event Source nodes.

For more information about manually configuring the Sentinel Link connection, see the documentation for the Sentinel Link Collector and Connector Plug-ins, available on the Sentinel Plug-ins Web site.

3 Configuring Sentinel Systems for Sending Events

You can configure Sentinel Log Manager, Sentinel, or Sentinel Rapid Deployment to forward events to another Sentinel server.

3.1 Configuring Sentinel or Sentinel Rapid Deployment Server as a Sender

If Sentinel or Sentinel Rapid Deployment is the sender, you must import and configure the Sentinel Link Integrator plug-in and the Sentinel Link Action plug-in to create a Sentinel Link configuration. You also need to create an action that forwards the selected events to the receiver. To filter the events, use the Correlation Manager to set a correlation rule. Associate the action to the rule and deploy it. You can also use Global Filters to filter the events and forward them to the receiver.

NOTE: For more information on Sentinel Link Integrator and Action, see the corresponding plug-in documentation in the Sentinel Plug-ins Web site.

Follow the instructions below to configure Sentinel or a Sentinel Rapid Deployment server to send the events:

3.1.1 Configuring the Sentinel Link Integrator Plug-In

The Sentinel Link Integrator comes pre-installed with the Sentinel platform. To get the latest performance enhancements and other enhanced features, visit the Sentinel Plug-ins Web site and download the latest set of Plug-ins.

NOTE: When updating any Sentinel Link Plug-in, you should also update all related Plug-ins across all platforms to ensure compatibility.

For instructions on configuring the Sentinel Link Integrator, see the Sentinel Link Integrator documentation in the Sentinel Plug-ins Web site.

3.1.2 Importing and Configuring the Sentinel Link Action Plug-In

The Sentinel Link Action plug-in comes pre-installed with the Sentinel platform. To get the latest performance enhancements and other enhanced features, visit the Sentinel Plug-ins Web site and download the latest set of Plug-ins.

NOTE: When updating any Sentinel Link Plug-in, you should also update all related Plug-ins across all platforms to ensure compatibility.

For instructions on configuring the Sentinel Link Action, see the Sentinel Link Action documentation in the Sentinel Plug-ins Web site.

3.1.3 Automatically Forwarding Events to the Receiver

To select events that you want to automatically forward to a receiver, you need a filtering mechanism. Use Correlation rules or Global Filters to filter the desired events, and associate the Sentinel Link Action to forward to the receiver.

NOTE: To forward events to another Sentinel or Sentinel Log Manager server based on simple filtering conditions, use Sentinel Link with Global Filters.

You can also use Sentinel Link anywhere in Sentinel to execute a javascript action, such as Correlation, Incidents, and Event right-click. Be aware that these mechanisms can forward the same event more than once. Use them only when simple filtering conditions are not enough.

For example, using Correlation, you can configure filter(1=1) and filter(e.sev>=3), and launch Sentinel Link action to forward the events to the same receiver. When you trigger the action, the receiver gets duplicated events.

Note that some field values of the events change during event forwarding. For example, the event id changes, but, the event name remains the same when you forward an event.

Another advantage of Global Filters over Correlation rule is that the events are sent in batches of 500 events to the receiver system. With Correlation rule, each event is forwarded to the receiver as soon as an event is generated.

Using Correlation Rules to Forward Events to the Receiver

You can create Correlation rules that filter the desired events for forwarding to the receiver system. After creating a rule, associate the Sentinel Link Action while deploying the rule.

The topics in this section describe how to use Correlation rules to forward events to the receiver in a Sentinel or Sentinel Rapid Deployment system.

Sentinel 6.x and Sentinel Rapid Deployment

The following example illustrates creating a simple rule that forward events with severity greater than 3.

1. In the Sentinel Control Center, select **Correlation Rule Manager**.
2. Click **Add**.

   The Correlation Rule wizard is displayed.
3. Click **Simple**.

4 Set the criteria to `Severity>3`, then click **Next**.

5 Select **Do not perform actions every time this rule fires** and use the drop-down menu to set the time period to 1 minute. Click **Next**. The General Description window displays.

6 Name the rule as **Sev4Rule**, provide a description, and click **Next**.

7 Select **No, do not create another rule** and click **Next**.

8 Click **Save**.

9 Select the Correlation Rule Manager window.

10 Select **Sev4Rule**, and click **Deploy Rules**.

11 In the Deploy Rule window, select the Engine to deploy the rule.

12 Select **Sentinel Link**, then click **OK**.

Sentinel 7.x

The following example illustrates creating a simple rule that forward events with severity greater than 3.

1 Log in to the Sentinel Web interface as a user with the Manage Correlation Engine and Rules permission.

2 In the navigation panel, click **Correlation**.

3 Click **Create**.

4 In the Subrule window, click **Create a new expression**.

5 Select the criteria to set it to `Severity>3`, then click **OK**.

The specified criteria are displayed in the Subrule window.

6 To associate one or more actions to the rule, in the Actions panel, click  .

7 Select **Send Events via Sentinel Link** action.

8 Click **OK**.

9 Click **Save As**.

10 Specify an intuitive name, for example, **Sev4Rule** for the rule and an optional description, then click **OK**.

11 Double-click the rule that you want to deploy.

12 In the Deploy/Undeploy section, select the engine to which you want to deploy the rule, then click **Deploy**.

NOTE: You can also deploy a rule from the Correlation dashboard. In the Correlation panel, click the engine to which you want to deploy rules. In the Available rules section, select the rule or rules that you want to deploy, then click **Deploy**.

Using Global Filters to Forward Events to the Receiver

You can use Global Filters to filter the desired events for forwarding to the receiver system.

The topics in this section describe using Global Filters to forward events to the receiver in a Sentinel or Sentinel Rapid Deployment system.

Sentinel 6.x and Sentinel Rapid Deployment

In the Global Filter Configuration window, you can add the Sentinel Link Action, then deploy the rule.

NOTE: This feature is supported only on Sentinel 6.1 SP1 Hotfix 2 or later, and Sentinel 6.1 Rapid Deployment 6.1 Hotfix 2 or later.

---

1. In the Sentinel Control Center, select the **Admin** Tab.
2. In the left navigation bar, select **Global Filter Configuration** to display the Global Filter Configuration window.
3. Click the **Add** button on the right-side of the window.
4. Click the button below the **Filter Name** field, then click the drop-down to set a filter.
5. Select the **Active** check box.
6. Select one of the following from the Route list:
   - drop
   - database only
   - database and gui
   - gui only
7. Click the button below the **Action** field to display the Select Action window.
8. Select the Sentinel Link Action you created, then click **OK**.

   If you have not created a Sentinel Link Action, click **Action Manager**, then follow the instructions. For more information, see Section 3.1.1, "Configuring the Sentinel Link Integrator Plug-In," on page 15.
9. Alternatively, you can also add Sentinel Link Action as the default Action.
   - 9a Click the button below the Default Action.
   - 9b Select the Sentinel Link Action, then click **OK**.
10. Click **Save**.

Sentinel 7.x

You must configure and activate the rule to forward events to another Sentinel system.

Configuring the Rule to Forward Events to the Receiver

Sentinel is installed with a rule, **Forward Events to Another Sentinel System** that forwards events to another Sentinel server. By default, the **Forward Events To Another Sentinel System** rule is configured to filter out internal system events and events with severity greater than three. This rule filters the following three types of system events:

- Audit (A)
- Performance (P)
- Internal (I)

You can also change the conditions of the rule to filter more events or remove conditions to filter fewer events.

NetIQ recommends that you configure the rule to forward only those events that you want to store on the Sentinel server for more in-depth reporting and analysis.

Activating the Rule to Forward Events to the Receiver

The **Forward Events To Another Sentinel System** rule is installed with Sentinel, but it is in the inactive (off) state. You must activate the rule to forward the events to another Sentinel system.

To activate the rule to forward events to the receiver:

1. Log in to the Sentinel Web UI as an administrator.
2. Click **Routing** in the toolbar.
3. Click **Edit** link next to the **Forward Events To Another Sentinel System** rule.
4. Select **Send Events via Sentinel Link** from the **Perform the following actions:** list.
5. Click **Save**.
6. Select the check box adjacent to the **Forward Events To Another Sentinel System** rule.

3.1.4 Manually Forwarding Events to the Receiver

You can forward events to the receiver by manually executing the Sentinel Link Action:

- Executing the Sentinel Link Action on an Incident.
- Executing the Sentinel Link Action on events in Active Views.
- Executing the Sentinel Link Action on events in Search results.

For more information, see the Sentinel product documentation:

- **Sentinel 6.x:** "Sentinel User Guide".
- **Sentinel 6.1 Rapid Deployment:** "Sentinel 6.1 Rapid Deployment User Guide".
- **Sentinel 7.x:** "Sentinel 7.x User Guide".

3.2 Configuring Sentinel Log Manager as a Sender

Installing Sentinel Log Manager installs the plug-ins and the event forwarding rule by default. You only need to configure the system for Sentinel link and activate the rule for sending the event data.

Follow the instructions below to configure a Sentinel Log Manager to send the event data:

- Section 3.2.1, "Configuring the Sentinel Link Action," on page 19
- Section 3.2.2, "Automatically Forwarding Events to the Receiver," on page 20
- Section 3.2.3, "Manually Forwarding Events to the Receiver," on page 20

3.2.1 Configuring the Sentinel Link Action

You can configure the Sentinel Link Action using the Sentinel Log Manager Web Interface. For instructions on configuring the action, see Sending the Events to a Sentinel Link in the Sentinel Log Manager Administration Guide.

3.2.2 Automatically Forwarding Events to the Receiver

This section describes how to configure and activate a rule to forward events to the receiver.

Configuring the Rule to Forward Events to the Receiver

Installing Sentinel Log Manager also installs the plug-ins and the event forwarding rule. The rule is called Forward Events to Another Sentinel System. By default, the Forward Events To Another Sentinel System rule filters out internal system events and events with severity greater than three. This rule filters the following three types of system events:

- Audit (A)
- Performance (P)
- Internal (I)

You can also change the conditions of the rule to filter more events or remove conditions to filter fewer events.

NetIQ recommends that you configure the rule to forward only those events that you want to store on the Sentinel system for more in-depth reporting and analysis.

Activating the Rule to Forward Events to the Receiver

The Forward Events To Another Sentinel System rule is installed with Log Manager, but it is in the inactive (off) state. You must activate the rule to forward the events to another Sentinel system.

1. Log in to the Log Manager Web interface as an administrator.
2. Click **rules** in the upper left corner of the page.
3. The **Rules** tab displays on the right panel of the page.
4. Click the check box next to the rule to activate the *Forward Events To Another Sentinel System* rule.

3.2.3 Manually Forwarding Events to the Receiver

You can forward events to the receiver by manually executing the Sentinel Link Action on events in Search results.

For more information see the Sentinel Log Manager Administration Guide.

4 Verifying a Sentinel Link

In this example, a Sentinel Log Manager computer is used as the sender and a Sentinel computer is used as the receiver.

To verify a Sentinel Link:

1. Configure a Sentinel Log Manager computer to send events.

   For more information, see Section 3.2, “Configuring Sentinel Log Manager as a Sender,” on page 19.
2. Configure a Sentinel computer to receive the events.

   For more information, see Chapter 2, “Configuring Sentinel Systems for Receiving Events,” on page 11.
3. On the sender machine, generate an event with severity greater than 3, such as a failed login.
4. To view that event, go to the Sentinel Web interface, and search for events with sev:[3 TO 5].

A Known Issues

Refer to the known issues section of the respective documents of Sentinel Link Collector, Connector, Integrator, and Action.

B Revision History

B.1 Rev: 2011.1r2

Sentinel Link has been rebranded to NetIQ.

Refer to the revision history of the respective Sentinel Link plug-in documents for specific bug fixes.

B.2 Rev: 2011.1r1

The updates include bug fixes to Sentinel Link Collector, Connector, Integrator, and Action. Refer to the revision history of the respective documents for specific bug fixes.

B.3 Rev: 6.1r5

Sentinel Link now supports IBM JRE 1.6 or later.

B.4 Rev: 6.1r4

Sentinel Link is now supported on Sentinel Log Manager 1.1.

In Sentinel Link Integrator, a new Alert Settings window is added that allows you to configure the conditions for the Integrator to generate alerts (internal events), while configuring the Sentinel Link Integrator. For more information about setting Alerts, refer to the *Sentinel Link Integrator* document.

Table B-1 *Bugs Fixed*

Bug Number	Resolution
596479	The `.JSON` file is now created with the correct name when the Sentinel Link Collector runs in the debug execution mode.

Bug Number	Resolution
582547	In Sentinel Link Collector, the `DeviceEventTimeString` field is now set to the correct value.
536119	In Sentinel Link Collector, the values of the incoming event fields are now preserved by the Collector except for RV 21 - RV 25, which are overwritten to track the ESM nodes that parsed the event.
529913	The Sentinel Link Connector now does not allow you to run two Sentinel Link Event Source servers on the same port, and displays an error message indicating that 'Port is already in use'.
531859 and 535964	Log message errors are fixed.
541101, 536115, and 541272	A number of event message handling errors are fixed.
539925	Sentinel Link Integrator is now supported on Sentinel 6.1.1.2 and later.
603050	In Sentinel Link Integrator, the logging level of some chatty messages is now changed from `INFO` to `FINE` so that they do not show up in the log unless specifically requested.

B.5 Rev: 6.1r3

Table B-2 *Bugs Fixed*

Bug Number	Resolution
561424	Issue: The Sentinel Link showed the `PermGen Space OutofMemory` error when run on the Sentinel RD Hotfix 2 platform. However, sending of events continued without any problem. Fixed: The incorrect occurrence of PermGen memory exception is resolved in the Sentinel RD SP1 platform.

B.6 Rev: 6.1r2

Table B-3 *Bugs Fixed*

Bug Number	Description
558091	Issue: DeviceEventTime is not displayed same as the DeviceEventTime that is displayed on running the original Collector on Sentinel. For example, on running the original collector on Sentinel, for a particular log line, device event time is displayed as 2/22/03 1:23:08 p.m. but when the same event is forwarded from Sentinel Log manager to Sentinel Link Collector has the device event time as 2/22/03 11:53:08 p.m. Fixed: Now the same DeviceEventTime is getting displayed when event is forwarded from one sentinel system to another sentinel system(s).
548654	Issue: The `Plugin.pdf` file is not available with the Sentinel Link Action 6.1r1. Fixed: The `Plugin.pdf` file is now packaged with Sentinel Link Action 6.1r2.

Bug Number	Description
540856	Issue: Sentinel Link count log messages are very chatty as the logging level for the log message was set to `INFO`, which is the default logging level. Fixed: Now the logging level for the Sentinel Link count log message is set to `FINE`, so that messages will be logged when the user sets the logging level to `FINE`.

B.7 Rev: 6.1r1

New Sentinel Link Overview Guide.