Sentinel Plug-Ins 2011.1r2

Sentinel Link Overview Guide

November 2016

Legal Notice

Contents

About this Book and the Library

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.

Intended Audience

This guide is intended for Sentinel administrators and consultants.

Other Information in the Library

For complete documentation on the Sentinel products, see the NetIQ Sentinel Documentation web page.

For information about Sentinel plug-ins, see the NetIQ Sentinel Plug-ins web page.

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

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

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

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click the comment icon on any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

1 Introduction

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

- Section 1.1, “Benefits,” on page 9
- Section 1.2, “Supported Platforms,” on page 9
- Section 1.3, “Prerequisite,” on page 9
- Section 1.4, “Configuring Sentinel Link,” on page 9

1.1 Benefits

Multiple Sentinel servers can be hierarchically linked to monitor the consolidated event information.

1.2 Supported Platforms

Sentinel 7.3 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 13
- 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 NetIQ Sentinel Plug-ins Web site.

2.1 Accessing Event Source Management

This section describes how to access Event Source Management in Sentinel.

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**.

2.2 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 NetIQ 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 NetIQ 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 NetIQ 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 NetIQ 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 NetIQ Sentinel Plug-ins Web site.

3 Configuring Sentinel Systems for Sending Events

You can configure Sentinel to forward events to another Sentinel server.

- Section 3.1, “Configuring Sentinel as a Sender,” on page 13

3.1 Configuring Sentinel as a Sender

If Sentinel 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 NetIQ Sentinel Plug-ins Web site.

Perform the following instructions to configure Sentinel server to send the events:

- Section 3.1.1, “Configuring the Sentinel Link Integrator Plug-In,” on page 13
- Section 3.1.2, “Importing and Configuring the Sentinel Link Action Plug-In,” on page 13
- Section 3.1.3, “Automatically Forwarding Events to the Receiver,” on page 14
- Section 3.1.4, “Manually Forwarding Events to the Receiver,” on page 16

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 NetIQ 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 NetIQ 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 NetIQ 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 NetIQ 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 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.

This section describes how to use Correlation rules to forward events to the receiver in a Sentinel system.

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.

This section describes how to use Global Filters to forward events to the receiver in a Sentinel system.

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 documentation.

4 Verifying a Sentinel Link

This chapter described how to verify that Sentinel Link is successfully configured.

To verify a Sentinel Link:

1. Configure a Sentinel computer to send events.

   For more information, see Section 3.1, “Configuring Sentinel as a Sender,” on page 13.

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 computer, generate an event with severity greater than 3, such as a failed login.
4. To view that event, go to the Sentinel Main 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, available in the NetIQ Sentinel Plug-ins Web site.

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.
582547	In Sentinel Link Collector, the `DeviceEventTimeString` field is now set to the correct value.

Bug Number	Resolution
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.