

Integration With Third Party SIEM Solutions

NetIQ® Secure Configuration Manager™

October 2016

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see <http://www.netiq.com/company/legal/>.

Copyright © 2016 NetIQ Corporation. All Rights reserved.

For information about NetIQ trademarks, see <http://www.netiq.com/company/legal/>. All third-party trademarks are the property of their respective owners.

Contents

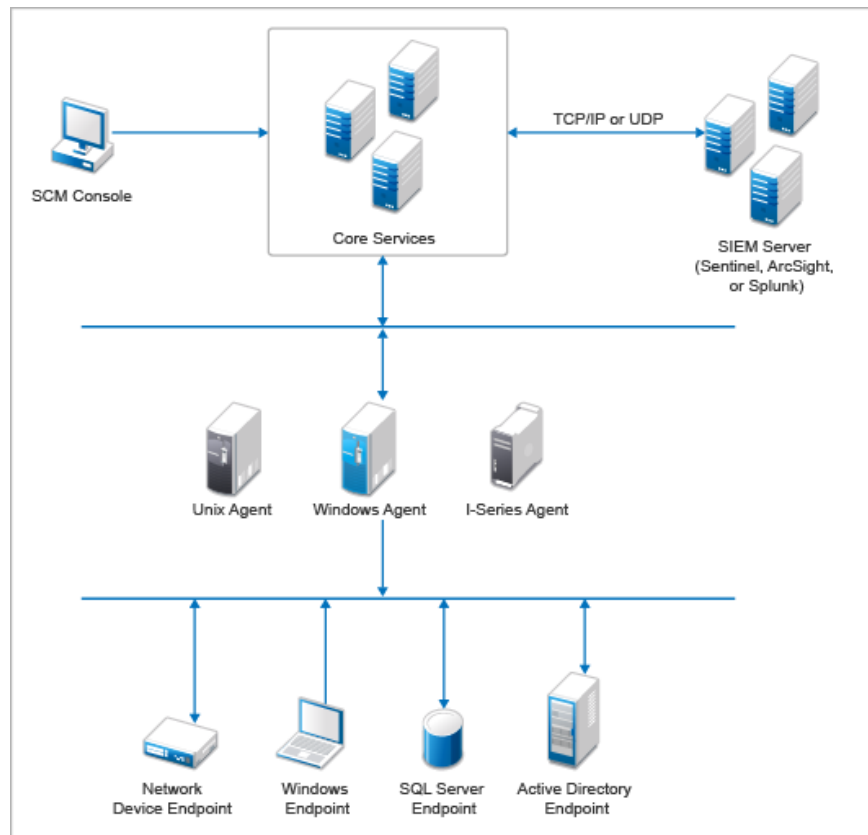
1. Introduction.....	4
2. Configuring Secure Configuration Manager for the Integration	5
3. Sending Events to SIEM Solutions	9
4. Integrating Secure Configuration Manager and Splunk Server	11
Configuring Splunk	11
Viewing Raw Secure Configuration Manager Events in Splunk Server	12
Viewing the Splunk Dashboard	13
Generating Alerts on Secure Configuration Manager Events	14
5. Integrating Secure Configuration Manager and ArcSight Server.....	15
Viewing Raw Secure Configuration Manager Events in ArcSight Server	16
Viewing the ArcSight Dashboard	17
Generating Alerts on Secure Configuration Manager Events	17

1. Introduction

NetIQ Secure Configuration Manager helps you to proactively enforce security configuration policy across critical systems in evolving IT environments. It helps in reducing the risk of security breaches, failed audits, or costly downtime. Security Information and Event Management (SIEM) is an approach that provides a holistic view of an organization's Information Technology (IT) security. However, you cannot determine compliance to configuration policy through a SIEM system at present. Determining compliance to configuration policy through SIEM solution will help in recording configuration compliance in line with system activity. It will inform the enterprise administrator about the compliance to configuration in times of anomalous activity.

This white paper describes how Secure Configuration Manager sends configuration compliance information as an event to SIEM solutions, such as Splunk and ArcSight. In this process, Secure Configuration Manager compliance information will be available in Splunk and ArcSight Dashboard for Enterprise administrator reference. Enterprise administrator can generate various reports on configuration compliance, and can also trigger alerts and actions such as sending emails for anomalous activity.

Secure Configuration Manager sends compliance data to the SIEM solution in common event format (CEF), through TCP or UDP connection. You can configure to send compliance data in TCP or UDP connection, based on the configuration of the SIEM solution. The following graphic depicts the overview.



As shown in the above graphic, Secure Configuration Manager Core Services component connects to the data receiver component of the SIEM solution, and sends the compliance data in CEF.

2. Configuring Secure Configuration Manager for the Integration

Perform the following configuration in Secure Configuration Manager to enable it to send compliance data to SIEM solutions:

1. Open Core Services Configuration Utility in your Secure Configuration Manager system and go to the Forward Assessment Report tab.
2. Set the required values in the fields in the Forward Assessment Report tab, or leave them as default values.

Note: Set the **Forward Assessment Events** field to `By Asset (Default)` to enable Secure Configuration Manager to send reports to the SIEM solutions for policy template runs.

3. Go to the **Advanced** tab.

Note: To access the **Advanced** tab in the Core Services Configuration Utility, perform the following steps:

- Close the Core Services Configuration Utility if it is open.
- Run the `config.bat` program in the `<Installation Directory>\Core Services\bin` folder.
- Reopen the Core Services Configuration Utility, and you will see the **Advanced** tab.

4. In the **Advanced** tab:

- **assessment/Thirdparty/SIEM/AppIntegration/Enabled:** Set this field to `true`.
- **assessment/Check/Include:**
 - Set this field to `true` to send a report to the SIEM solution for each check that is run as part of a template.
 - Set this field to `false` to send a consolidated report to the SIEM solution for each template you run.

Core Services Configuration Utility

File Help

Logging Database Network Discovery Heartbeat Login Alerts Task Alerts Out of Compliance Alerts Web Services
License Keys Exception Approvals SCAP Forward Assessment Report Advanced Hosts Allowed Hosts Denied

Hosts.Directory: etc

alert/refresh/interval/max: 10000

alert/refresh/interval/min: 2000

assessment/Check/Include: true

assessment/Event/Dispatcher: EventWithReport

assessment/Protocol: TLS

assessment/Severity/InCompliance: 1

assessment/Severity/Incomplete: 2

assessment/Severity/OutOfCompliance/HighRisk: 5

assessment/Severity/OutOfCompliance/LowRisk: 3

assessment/Severity/OutOfCompliance/MediumRisk: 4

assessment/Thirdparty/SIEM/AppIntegration/Enabled: true

assessment/ThreadPoolSize: 5

autosync/autodownload/patchdb/oncheckforupdates: true

autosync/check/dlpack: T

autosync/check/dltoc: T

autosync/check/download/patchdb: true

autosync/check/login: false

autosync/client/address: 127.0.0.1

autosync/client/port: 1626

autosync/client/provider: vssla

autosync/load/windows/update/enabled: false

autosync/load/windows/update/filename: Windows_Agent_6.2.nap

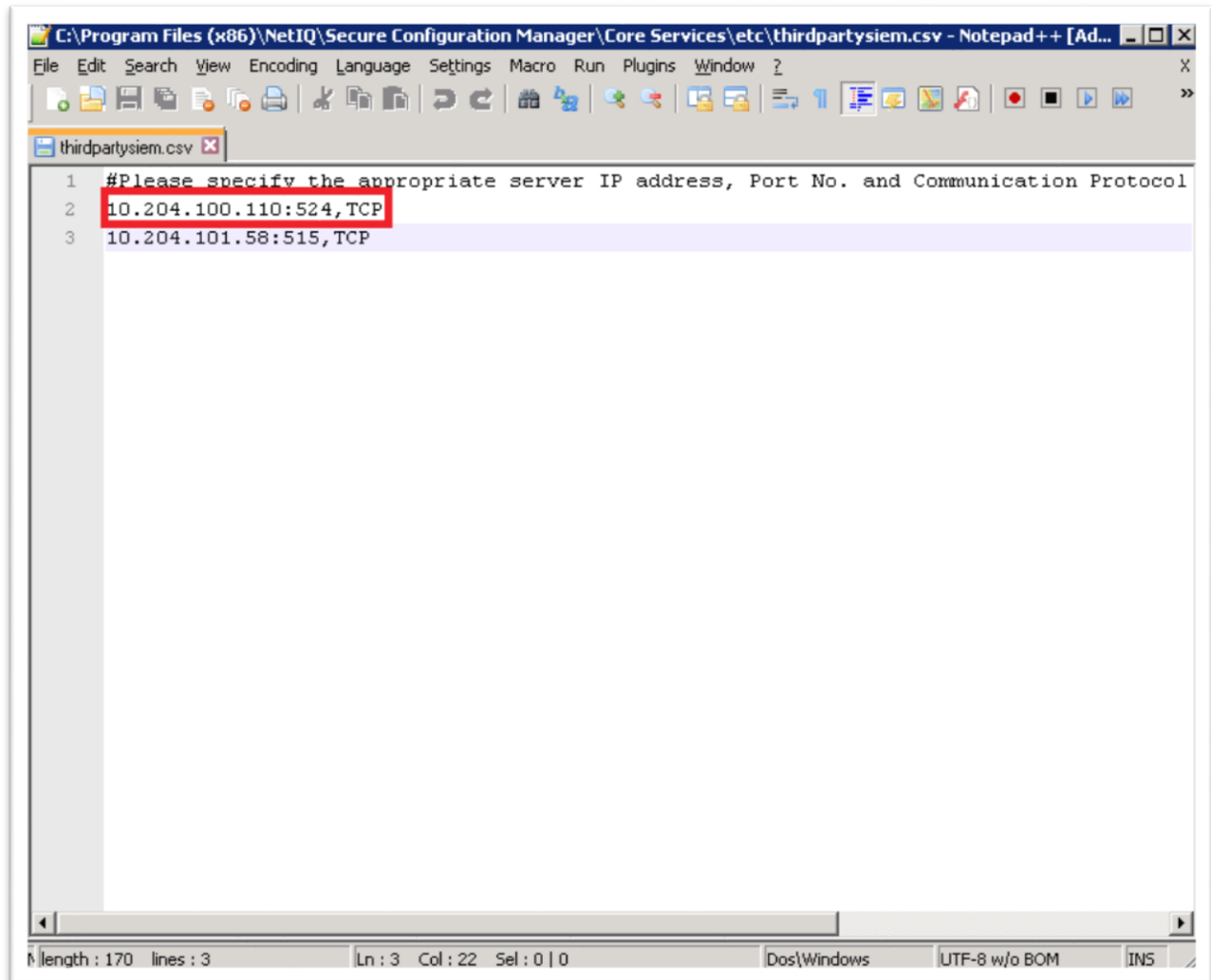
(NOTE: You must restart Core Services if you change an item in bold text.)

OK Apply Close Undo Default

5. Configure the SIEM solution server IP address, port, and protocol for sending data:
 - a. Open the \NetIQ\Secure Configuration Manager\Core Services\etc\thirdpartysiem.csv file.
 - b. Update this file with new entries, specifying the server configuration for each SIEM solution that you want to send compliance data. For example:

10.204.100.110:524, TCP

Where 10.204.100.110 is the IP address of the SIEM solution, 524 is the port number, and TCP is the protocol to be used to send compliance data.



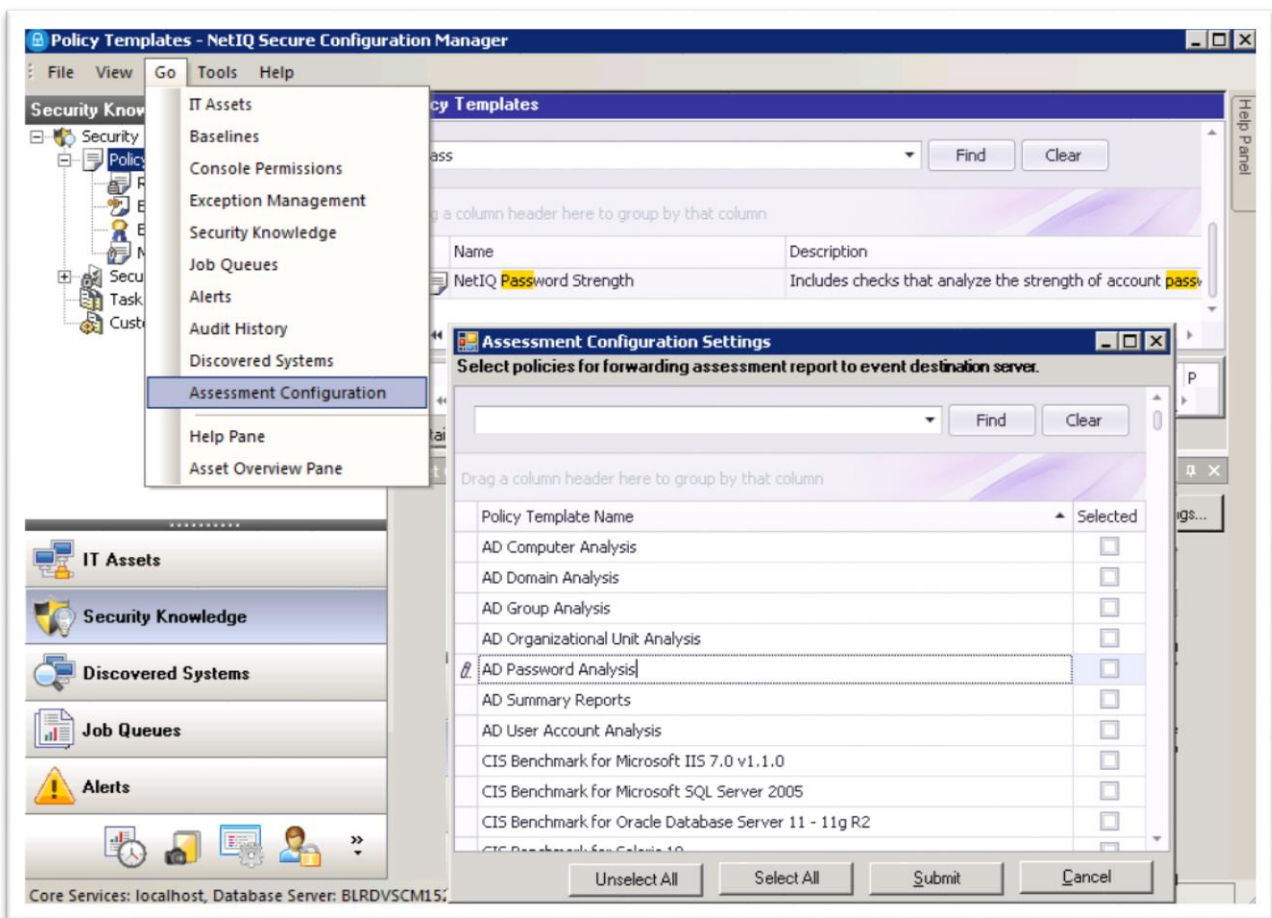
For more information about configuring advanced options, see the [Secure Configuration Manager User Guide](#).

3. Sending Events to SIEM Solutions

After you have configured Secure Configuration Manager to send compliance events to SIEM solutions as specified in **Configuring Secure Configuration Manager for the Integration**, you can send the compliance data to SIEM servers as events. You can choose to send events to SIEM servers while running policy templates in the following two ways.

Selecting Policy Templates to Send Events:

In the Secure Configuration Manager Console, click **Go > Assessment Configuration**. In the **Assessment Configuration Settings** window, select the policy templates for which events need to be sent to the SIEM server.




Selecting to Send Events While Executing the Policy Template:

When you run a policy template, select the **Forward Assessment Report to Destination Server** option in the **Run Policy Template Wizard** window.

Run Policy Template Wizard

Run Options

Specify whether to run the report from the database or the agent, and whether to use email alerts.



Targets

Run Options

Report Options

Schedule

Delta Reporting

Distribution

Summary

☐ Run report from database

Date Range

Start Date

12/ 9/2014 12:31


End Date

12/ 9/2014 12:31

No End Date

☐ Enable e-mail compliance alerts

☒ Forward Assessment Report to Destination Server



Cancel

< Back

Next >

Finish

10 | Page

4. Integrating Secure Configuration Manager and Splunk Server

Integration of Secure Configuration Manager and Splunk server enables Secure Configuration Manager Server to send configuration compliance information as events to Splunk SIEM solution.

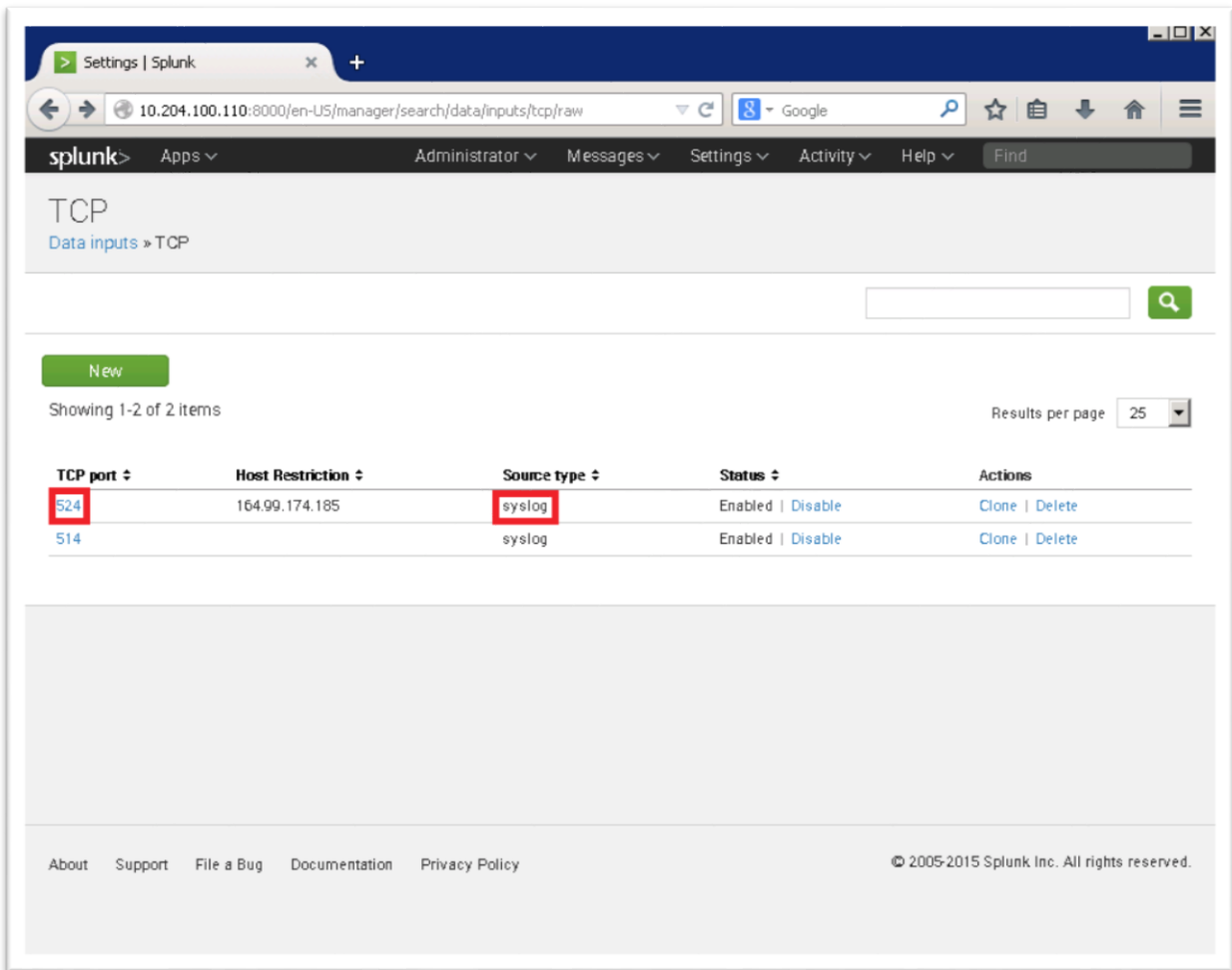
Configuring Splunk

Configure the Splunk Enterprise Server to listen on a network port for incoming data:

1. Configure a TCP/UDP data input listener with syslog source type, as shown in the following figure.

The screenshot shows the 'Add Data' configuration page in the Splunk web interface. The 'Select Source' step is active, showing a list of data sources on the left. The 'TCP / UDP' source is selected. The main configuration area on the right is titled 'Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog)'. It includes a 'Port' field set to 524, a 'Source name override' field set to 'optional', and an 'Only accept connection from' field set to '164.99.174.185'. A 'Next >' button is visible at the top right. Below the configuration fields is an 'FAQ' section with links to help topics.

When the data input is configured, it will be added in the **TCP Data inputs** table, as shown in the following figure.



Viewing Raw Secure Configuration Manager Events in Splunk Server

After you configure Splunk to receive events from Secure Configuration Manager, whenever policy templates are executed in Secure Configuration Manager against selected endpoints, you can view the

events in Splunk server search panel.

i	Time	Event
1	12/4/14 3:39:04 PM	Dec 4 15:39:04 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Incomplete 2 cat=Configuration Management suid= suser=admin rt=1417687743909 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=Oracle nsg=SCM Endpoint Assessment of 127.0.0.1 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=127.0.0.1 cs1Label=TotalRisk cs1=1 cs2Label=ExceptedRisk cs2=-1 cs3Label=ManagedRisk cs3=-1
2	12/4/14 3:39:02 PM	Dec 4 15:39:02 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Out Of Compliance 5 cat=Configuration Management suid= suser=admin rt=1417687741647 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=IIS nsg=SCM Endpoint Assessment of 164.99.174.157 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=164.99.174.157 cs1Label=TotalRisk cs1=1780 cs2Label=ExceptedRisk cs2=0 cs3Label=ManagedRisk cs3=1780
3	12/4/14 3:39:00 PM	Dec 4 15:39:00 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Out Of Compliance 3 cat=Configuration Management suid= suser=admin rt=1417687739595 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=Windows Machine nsg=SCM Endpoint Assessment of 164.99.174.157 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=164.99.174.157 cs1Label=TotalRisk cs1=10 cs2Label=ExceptedRisk cs2=0 cs3Label=ManagedRisk cs3=10
4	12/4/14 2:34:49 PM	Dec 4 14:34:49 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Incomplete 2 cat=Configuration Management suid= suser=admin rt=1417683888897 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=Oracle nsg=SCM Endpoint Assessment of 127.0.0.1 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=127.0.0.1 cs1Label=TotalRisk cs1=-1 cs2Label=ExceptedRisk cs2=-1 cs3Label=ManagedRisk cs3=-1
5	12/4/14 2:34:47 PM	Dec 4 14:34:47 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Out Of Compliance 5 cat=Configuration Management suid= suser=admin rt=1417683888837 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=IIS nsg=SCM Endpoint Assessment of 164.99.174.157 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=164.99.174.157 cs1Label=TotalRisk cs1=1780 cs2Label=ExceptedRisk cs2=0 cs3Label=ManagedRisk cs3=1780
6	12/4/14 2:34:45 PM	Dec 4 14:34:45 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Out Of Compliance 3 cat=Configuration Management suid= suser=admin rt=1417683884769 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=Windows Machine nsg=SCM Endpoint Assessment of 164.99.174.157 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=164.99.174.157 cs1Label=TotalRisk cs1=10 cs2Label=ExceptedRisk cs2=0 cs3Label=ManagedRisk cs3=10
7	12/4/14 1:00:35 PM	Dec 4 13:00:35 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Incomplete 2 cat=Configuration Management suid= suser=admin rt=1417678234095 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=Oracle nsg=SCM Endpoint Assessment of 127.0.0.1 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=127.0.0.1 cs1Label=TotalRisk cs1=-1 cs2Label=ExceptedRisk cs2=-1 cs3Label=ManagedRisk cs3=-1
8	12/4/14 1:00:33 PM	Dec 4 13:00:33 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Out Of Compliance 5 cat=Configuration Management suid= suser=admin rt=1417678232038 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=IIS nsg=SCM Endpoint Assessment of 164.99.174.157 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=164.99.174.157 cs1Label=TotalRisk cs1=1780 cs2Label=ExceptedRisk cs2=0 cs3Label=ManagedRisk cs3=1780
9	12/4/14 1:00:30 PM	Dec 4 13:00:30 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Out Of Compliance 3 cat=Configuration Management suid= suser=admin rt=1417678229968 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=Windows Machine nsg=SCM Endpoint Assessment of 164.99.174.157 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=164.99.174.157 cs1Label=TotalRisk cs1=10 cs2Label=ExceptedRisk cs2=0 cs3Label=ManagedRisk cs3=10
10	12/4/14 12:43:42 PM	Dec 4 12:43:42 BLRVSQM408 CEF:0 NetIQ Secure Configuration Manager 6.0 NetIQ Best Practices SCM Endpoint Assessment - Incomplete 2 cat=Configuration Management suid= suser=admin rt=1417677341671 sourceDnsDomain= shost=BLRVSQM408 src=164.99.174.157 sourceServiceName=Oracle nsg=SCM Endpoint Assessment of 127.0.0.1 based on NetIQ Best Practices cnt=null filePath= destinationDnsDomain= dhost=BLRVSQM408 dst=127.0.0.1 cs1Label=TotalRisk cs1=-1 cs2Label=ExceptedRisk cs2=-1 cs3Label=ManagedRisk cs3=-1

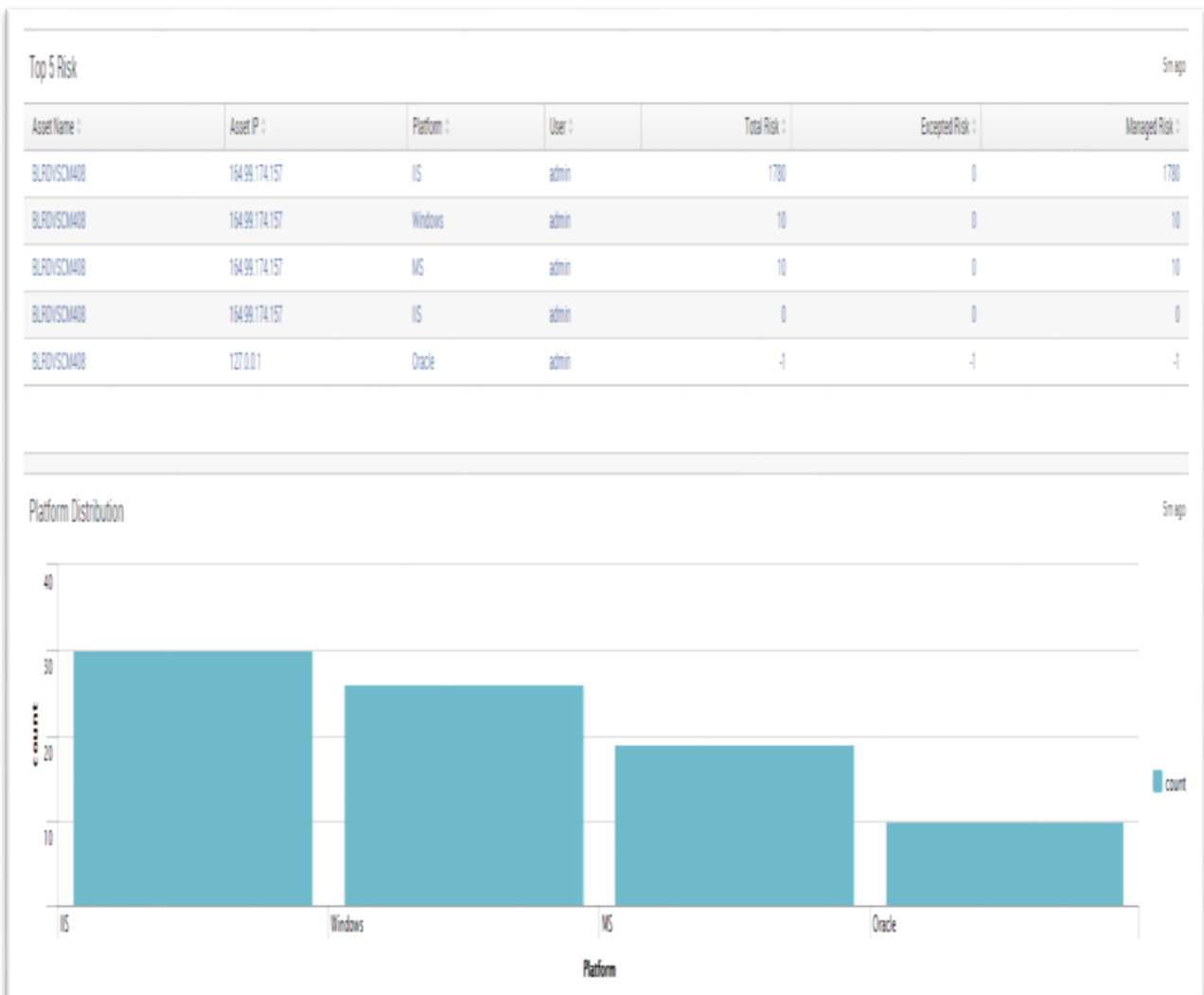
Viewing the Splunk Dashboard

You can generate reports in Splunk Dashboard using the Secure Configuration Manager events data.

For example, you can use the following search string to create a report of top assets by Risk:

```
<searchString>source="164.99.174.185" | top 5  
cs3,cs1,cs2,dst,dhost,sourceServiceName,suser showcount=false  
showperc=false | table dhost,dst,sourceServiceName,suser,cs1,cs2,cs3 |  
sort -cs3 | rename cs3 as "Managed Risk" | rename cs2 as "Excepted  
Risk" | rename suser as "User" | rename dhost as "Asset Name" | rename  
dst as "Asset IP" | rename sourceServiceName as "Platform" | rename  
cs1 as "Total Risk"</searchString>
```

Similarly, you can create a number of reports in various panels of Splunk Dashboard, using the attributes of event sent by Secure Configuration Manager.

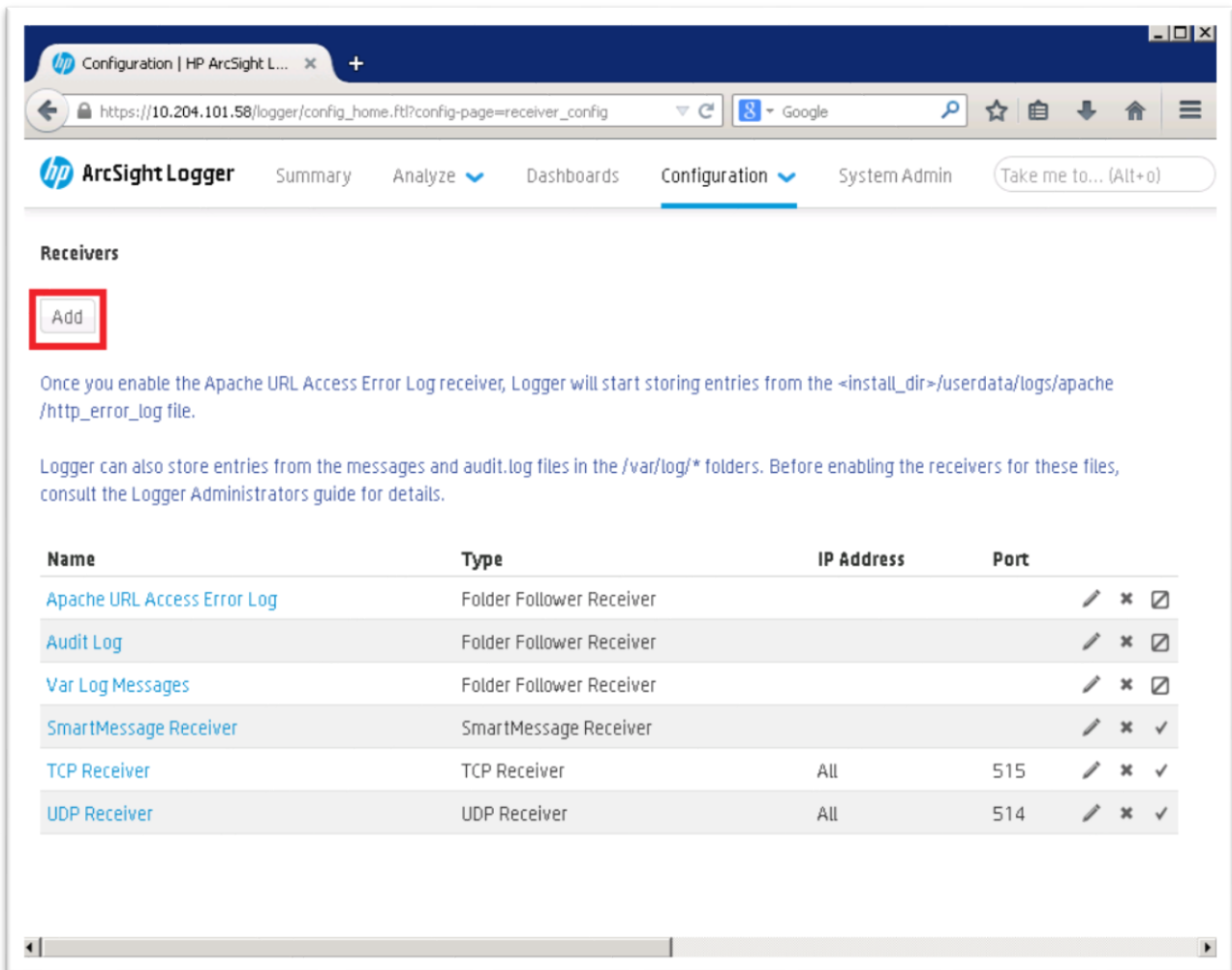


Generating Alerts on Secure Configuration Manager Events

You can generate alerts for Secure Configuration Manager events on Splunk Server. Splunk Server has a provision to trigger alerts on a specific saved search condition. There are options for performing actions such as sending emails and running scripts. See the Splunk Server documentation to configure saved searches, alert action, and other configurations.

5. Integrating Secure Configuration Manager and ArcSight Server

Configure a receiver in ArcSight to accept events from Secure Configuration Manager server, as shown in the following figures.



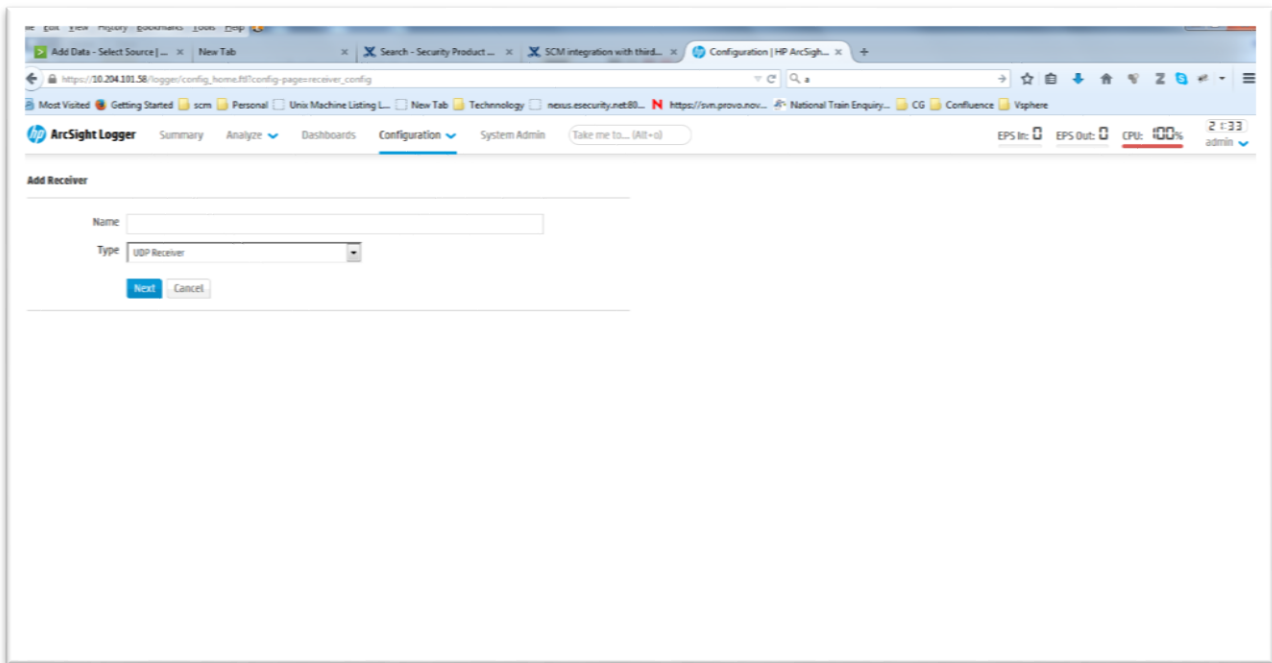
Receivers

Add

Once you enable the Apache URL Access Error Log receiver, Logger will start storing entries from the <install_dir>/userdata/logs/apache/http_error_log file.

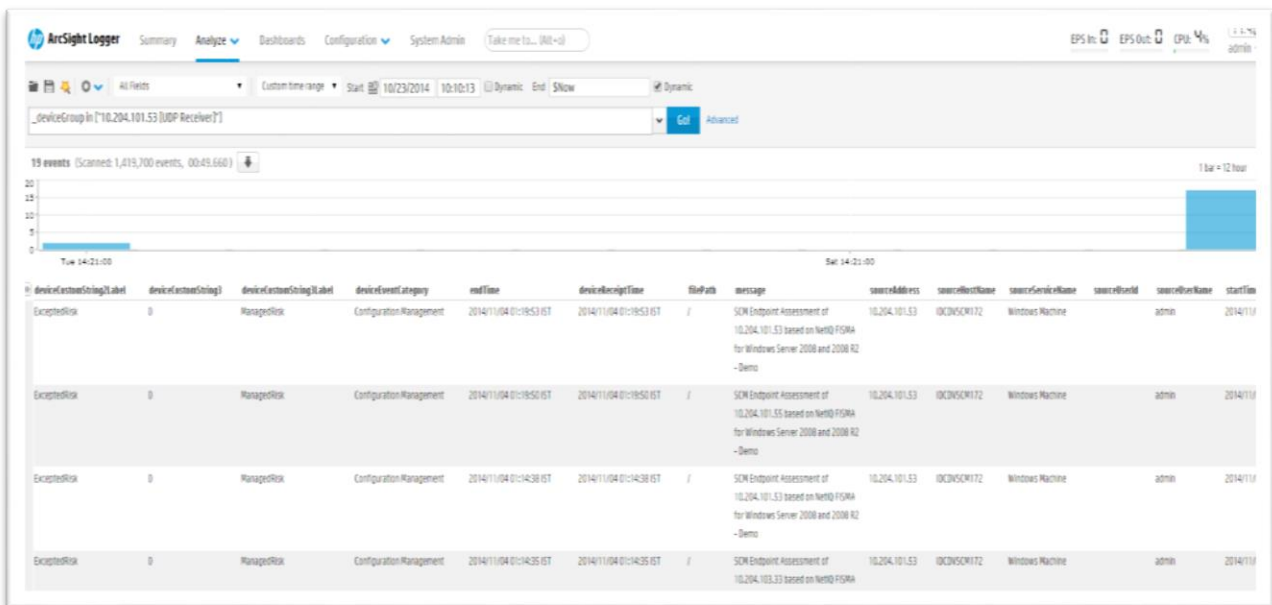
Logger can also store entries from the messages and audit.log files in the /var/log/* folders. Before enabling the receivers for these files, consult the Logger Administrators guide for details.

Name	Type	IP Address	Port	
Apache URL Access Error Log	Folder Follower Receiver			
Audit Log	Folder Follower Receiver			
Var Log Messages	Folder Follower Receiver			
SmartMessage Receiver	SmartMessage Receiver			
TCP Receiver	TCP Receiver	All	515	
UDP Receiver	UDP Receiver	All	514	



Viewing Raw Secure Configuration Manager Events in ArcSight Server

After configuring ArcSight to receive events from Secure Configuration Manager, you can view Secure Configuration Manager events in the ArcSight search panel. Whenever policy templates are executed in Secure Configuration Manager, events will be forwarded to ArcSight sever.



Viewing the ArcSight Dashboard

You can generate a number of reports in the ArcSight Dashboard using various saved searches such as top policies and compliance distribution. The following figure shows examples of reports.



Generating Alerts on Secure Configuration Manager Events

You can generate alerts on Secure Configuration Manager events based on saved searches, with various actions such as email and syslog event source. See the ArcSight documentation to configure alert generation for saved searches.