



RSA Security Analytics Ready Implementation Guide

Last Modified: December 2, 2013

Partner Information

Product Information	
Partner Name	Nominum, Inc.
Web Site	www.nominum.com
Product Name	Vantio
Version & Platform	5.2, Redhat Enterprise Linux 5/6, Suse Linux Enterprise Server 10/11
Product Description	Caching DNS System



Solution Summary

Nominum’s Vantio caching nameserver outputs events that are easily consumed by RSA Security Analytics for the purpose of monitoring and alerting on network activity. In doing so, security threats directed at an organization or directed at specific clients can be exposed prior to an actual security event. For example, Vantio can send an alert to Security Analytics when query loads increase beyond normal levels, indicating a potential denial of service attack. Using this same output and reporting structure, another example of the power of this combined offering is how Vantio and Security Analytics provide visibility into resource utilization. When utilization reaches abnormal levels due to non-responding name servers, an alert is generated to show the potential of a misconfigured “popular” zone. To make use of this combined solution, Vantio simply needs to be configured to send syslog messages to RSA Security Analytics. Vantio has a number of options that can be set to best match the organization’s requirements on security or operations monitoring, making the overall solution both flexible and powerful.

RSA Security Analytics Features	
Nominum Vantio 5.2	
Integration package name	nominumvantiope
Device display name within Security Analytics	nominumvantiope
Event source class	Application Server
Collection method	Syslog



Release Notes

Release Date	What’s New In This Release
12/02/2013	Initial support for Nominum Vantio.

Security Analytics Integration Package

The RSA Security Analytics (SA) Community is an online forum for customers and partners to exchange technical information and best practices with each other. The forum also contains the location to download the SA Integration Package for this guide. All Security Analytics customers and partners are invited to register and participate in the [RSA Security Analytics Community](#).

Once you have downloaded the package from the Security Analytics Community, the next steps are to deploy this on all log decoders. Follow the rest of this Implementation Guide to proceed.

 **Note:** For steps to disable or remove the Security Analytics Integration Package, please refer to the Appendix of this Guide.

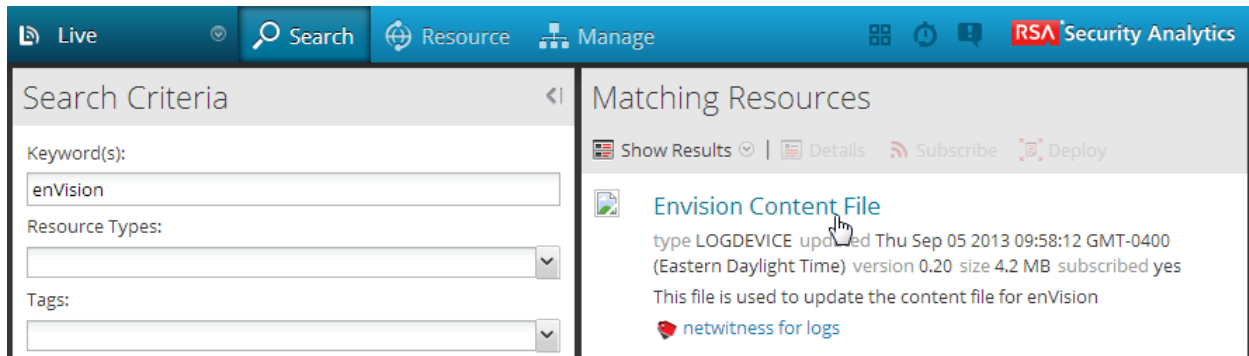
An overview of the RSA Security Analytics package consists of the following files:

Filename	File Function
nominumvantiope.envision	This file is deployed during the Deploy Security Analytics Integration Package section in this guide.
index-concentrator-custom.xml	This file can be referenced for the Create the index-concentrator-custom.xml section.
table-map.xml	This file can be referenced for the Modify the table-map.xml section.
variables.txt	This file can be used to determine which variables are used within the parser/XML. The format of the file consists of: <i>enVision variable name --> SA variable name --> SA variable type</i>

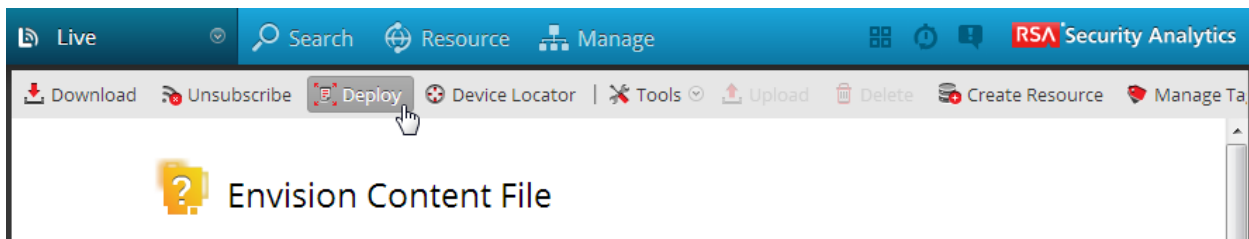
Deploy enVision Content File

In order to use RSA Partner created content, you must first deploy the *enVision Content File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

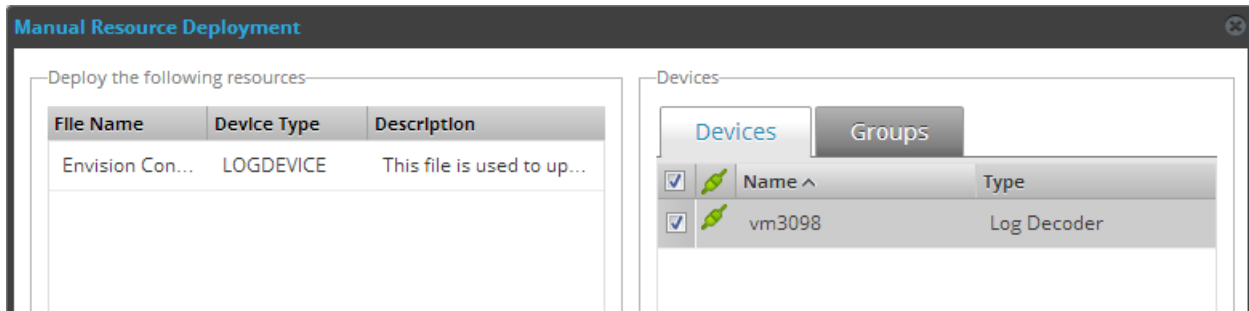
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Content File** in Matching Resources.
4. Click on **Envision Content File**.



5. Next click **Deploy** in the menu bar.



6. Check your **Log Decoder(s)** in Devices tab and then click **Push**.



7. Once deployed, you will receive a **COMPLETE** message in the Deployment Job Progress window.

Deploy Security Analytics Integration Package

After completing the previous section, *Deploy enVision Content File*, you can now deploy the Security Analytics Integration Package. Download the appropriate RSA Partner Integration Package, then log into Security Analytics to perform the following actions:

1. From the Security Analytics menu, select **Administration > Devices**.
2. Select your Log Decoder from the list, select **View > Config**.

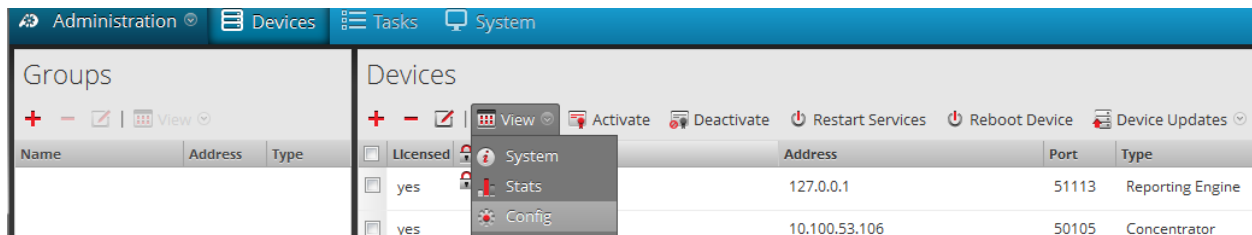
 **Note:** In an environment with multiple Log Decoders, deploy the Integration Package on each Log Decoder that will use the new device.

3. Next, select the **Parsers** tab and click the **Upload** button.
4. From the *Upload Parsers* window, click the **Add** button and select the *.envision* file.
5. Under the file name column, select the integration package name and click **Upload**.
6. Navigate to **Administration > Devices** and check the **Log Decoder** then click **Restart Services**.



Licensed	Name	Address	Port	Type
yes	vm3105	127.0.0.1	51113	Reporting Engine
yes	vm3106	10.100.53.106	50105	Concentrator
yes	vm3107	10.100.53.107	50101	Log Collector
yes	vm3107	10.100.53.107	50102	Log Decoder

7. From the **Administration > Device** screen check **Log Decoder** and select **View > Config**.



Licensed	Name	Address	Port	Type
yes	vm3106	10.100.53.106	50105	Concentrator

8. The new device will automatically be listed under **General > Device Parsers Configuration**.

The screenshot shows the configuration interface for device vm3107. It is divided into three main sections:

- System Configuration:** A table with columns 'Name' and 'Config Value'.

Compression	0
Port	50002
SSL	off
Stat Update Interval	1000
- Log Decoder Configuration:** A table with columns 'Name' and 'Config Value'.

Adapter	
Berkley Packet Filter	
Capture Interface Selected	
Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB
- Device Parsers Configuration:** A table with columns 'Name' and 'Config Value'.

ALERTS	<input checked="" type="checkbox"/>
BITTORRENT	<input checked="" type="checkbox"/>
FeedParser	<input checked="" type="checkbox"/>
FIX	<input checked="" type="checkbox"/>
GeoIP	<input type="checkbox"/>
GNUTELLA	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>

Create the *index-concentrator-custom.xml*

Modify the *index-concentrator-custom.xml* file to retrieve meta details from log collections.

1. Log into the log decoder via console or SSH.
2. On the log decoder, go to the `/etc/netwitness/ng/envision` directory.
3. If the `index-concentrator-custom.xml` file does not exist, copy the `index-concentrator-custom.xml` from the Integration zip file to this directory.
If the `index-concentrator-custom.xml` file already exists then append the content to the existing file.
4. Navigate to **Administration > Devices** and check the **Log Decoder** then click **Restart Services**.

The screenshot shows the 'Devices' page in the configuration interface. It displays a table of devices with columns for 'Licensed', 'Name', 'Address', 'Port', and 'Type'. The 'Log Decoder' device (vm3107) is selected.

Licensed	Name	Address	Port	Type
<input type="checkbox"/>	vm3105	127.0.0.1	51113	Reporting Engine
<input type="checkbox"/>	vm3106	10.100.53.106	50105	Concentrator
<input type="checkbox"/>	vm3107	10.100.53.107	50101	Log Collector
<input checked="" type="checkbox"/>	vm3107	10.100.53.107	50102	Log Decoder

Below is an example of the *index-concentrator-custom.xml* for the enVision attributes `macaddr` and `node`.

```
<key description="macaddr" level="Indexvalues" name="eth.host" format="Text" valueMax="100000" />
<key description="node" level="Indexvalues" name="node" format="Text" valueMax="100000" />
```

Modify the *table-map.xml*

The *table-map.xml* file contains the enVision to NetWitness meta map.

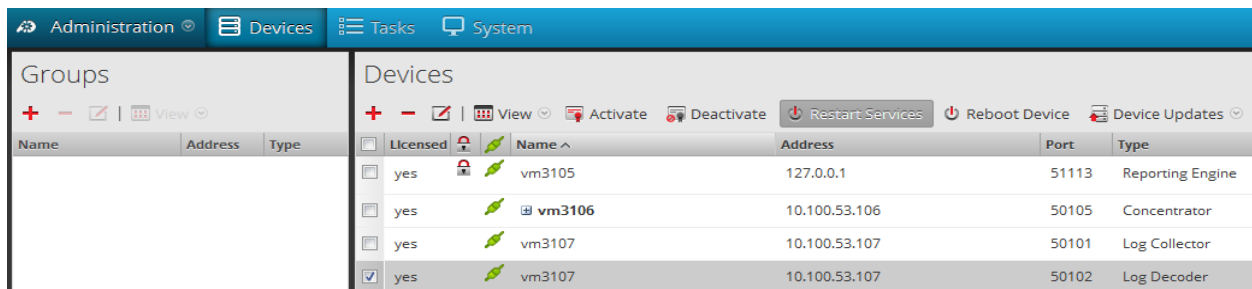
1. Log into the Log Decoder via console or SSH.
2. On the Log Decoder, go to `/etc/netwitness/ng/envision/etc`.
3. Use the name fields in the *index-concentrator-custom.xml* file to determine the list of attributes which need to be modified in the *table-map.xml* file.

- Copy the **table.map.xml** from **/etc/netwitness/ng/envision/etc** to **/etc/netwitness/ng/envision**.
- Open **/etc/netwitness/ng/envision/table.map.xml** file and modify the field **flags=Transient** to **flags=None** for only the attributes that exist in the name field of the index-concentrator-custom.xml file.

The below table-map.xml maps is an example of the enVision attribute **macaddr** and **node** mapped to the correlated NetWitness attribute, with the flag field modified to **None**.

```
<?xml version="1.0" encoding="utf-8"?>
<!--
# attributes:
#   envisionName:   The name of the column in the universal table
#   nwName:        The name of the Netwitness meta field
#   format:        Optional. The language key data type. See LanguageManager. Defaults to "Text".
#   flags:         Optional. One of None|File|Duration|Transient. Defaults to "None".
#   failureKey:    Optional. The name of the NW key to write data if conversion fails. Defaults to system
#   parse.error" meta.
#   nullTokens:   optional. The list of "null" tokens. Pipe separated. Default is no null tokens.
-->
<mappings>
  <!-- These entries are defined and created by Panorama and can be turned on/off here -->
  <mapping envisionName="device_class" nwName="device.class" flags="None" />
  <mapping envisionName="device_ip" nwName="device.ip" format="Text" flags="None" />
  <mapping envisionName="device_type" nwName="device.type" flags="None" />
  <mapping envisionName="device_type_id" nwName="device.type.id" format="Int" flags="Transient" />
  <mapping envisionName="lwrite" nwName="lwrite" format="Int32" nullTokens="(null)" flags="Transient" />
  <mapping envisionName="macaddr" nwName="eth.host" format="MAC" flags="None" />
  <mapping envisionName="mail_id" nwName="mail.id" flags="Transient" />
  <mapping envisionName="mask" nwName="mask" flags="Transient" />
  <mapping envisionName="message_body" nwName="message.body" flags="Transient" />
  <mapping envisionName="network_port" nwName="network.port" format="Int32" flags="Transient" />
  <mapping envisionName="msg" nwName="msg" format="Text" flags="Transient" />
  <mapping envisionName="network_service" nwName="network.service" flags="Transient" />
  <mapping envisionName="node" nwName="node" flags="None" />
  <mapping envisionName="node_name" nwName="node.name" flags="Transient" />
  <mapping envisionName="workspace_desc" nwName="workspace" flags="Transient" />
  <mapping envisionName="workstation" nwName="alias.host" flags="None" />
  <mapping envisionName="zone" nwName="zone" flags="Transient" />
</mappings>
```

- Navigate to **Administration > Devices** and check the **Log Decoder** than click **Restart Services**.



- The Log Decoder is now ready to parse events for this device.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Nominum Vantio with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Nominum Vantio components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Vantio Configuration

The first step is to configure Vantio to send all log messages to RSA Security Analytics.

1. Edit `/etc/syslog.conf` to include the following lines
Log Nominum remotely to RSA Security Analytics
local1.* @<IP address of Security Analytics>
2. Restart the syslogd daemon:
> kill -HUP `cat /var/run/syslogd.pid`
3. Edit the file `/usr/local/nom/etc/sysconfig/vantio` and add the following line:
VANTIO_SYSLOG_FACILITY=local1
4. Restart Vantio:
>/etc/init.d/vantio restart

As the next step you want to consider the security related events of interest and configure Vantio to emit log messages accordingly. Please refer to the Vantio user guide for more details.

Certification Checklist for RSA Security Analytics

Date Tested: December 2, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.2SP2	Virtual Appliance
Nominum Vantio	5.2	5.2, Redhat Enterprise Linux 5/6

Security Analytics Test Case	Result
Device Administration	
Partners device name appears in Device Parsers Configuration	✓
Device can be enabled from Device Parsers Configuration	✓
Device can be disabled from Device Parsers Configuration	✓
Device can be removed from Device Parsers Configuration	✓
Investigation	
Device name displays properly from Device Type	✓
Displays Meta Data properly within Investigator	✓

GLS / PAR

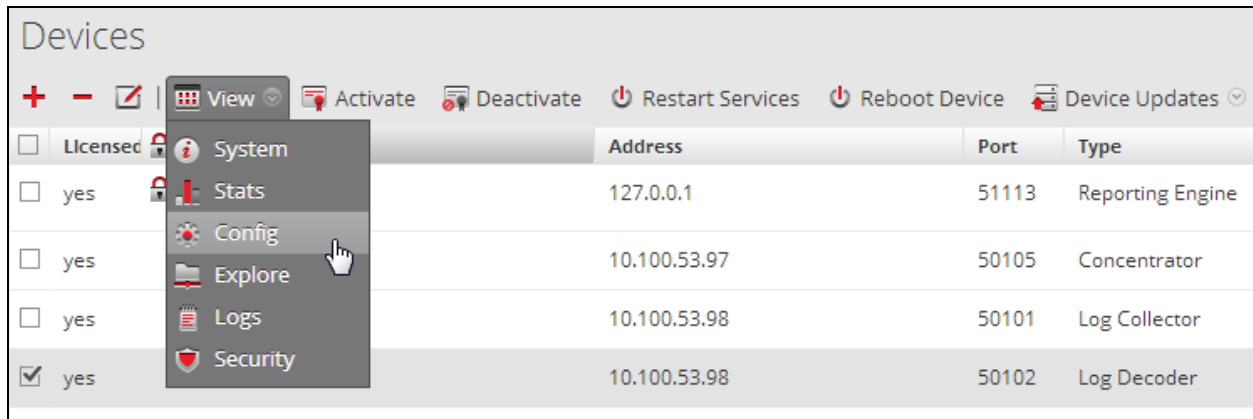
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

Security Analytics Disable Device Parser

To disable the Security Analytics Integration Package but not delete the XML from the system, perform the following:

1. From the Security Analytics menu, select **Administration > Devices**.
2. Check your Log Decoder from the **Devices** list and then select **View > Config**.



3. From the **Device Parses Configuration** window, scroll down to the device you wish to disable and uncheck the box.
4. Click **Apply** to save settings.

Security Analytics Remove Device Parser

To remove the Security Analytics Integration Package files from the environment, perform the following:

1. Connect to the Security Analytics Log Decoder/Collector Server using SSH and open the **/etc/netwitness/ng/envision/etc/devices** folder.
2. Search for the device you are targeting for removal and delete the folder containing the device xml.
3. Returning the system to its original state will require additional changes to the **table-map.xml** and **index-concentrator-custom.xml** files. To identify which variables were added locate the zip file downloaded from the RSA Website and open the **index-concentrator-custom.xml** contained within.
4. Edit **index-concentrator-custom.xml** on the SA server, removing only the lines present in the **index-concentrator-custom.xml** extracted from the zip.