

plexer

Integrating Scrutinizer with EndaceProbe Network History

Scrutinizer can be integrated with EndaceProbes to provide a seamless connection to the recorded Network History residing on the EndaceProbes in your network.

This integration enables analysts to pivot directly from an alert in the Scrutinizer console to view the packet history related to that event in the EndaceVision investigation application. Connecting Scrutinizer to the network history on EndaceProbes is done by adding a parameterized URL string to the Scrutinizer configuration file.

This parameterized URL uses the Pivot to Vision API function to define a pre-configured investigation in EndaceVision which retrieves the packet history related to a specific Scrutinizer event and displays the results in EndaceVision.

EndaceVision provides a number of traffic visualization tools that analysts can use to filter the packet history, zoom the timeframe in or out and identify specific packets of interest to analyze in EndacePackets or download in a packet capture file for analysis in Wireshark.

The URL parameters specify:

- Which EndaceProbe or EndaceCMS Central Management Server to access to run the investigation.
- Which RotationFile(s) to search (RotationFiles are where recorded Network History is stored on EndaceProbes).
- The start and end times for the investigation period (these are provided automatically by Scrutinizer in order to select just the packet history relating to the alerted event).
- Which default EndaceVision visualization tools to use in the investigation.

Editing the Scrutinizer config file

Configuring Scrutinizer to connect to your EndaceProbes is done by editing the Scrutinizer config file.

To edit the config file:

1. SSH into the Scrutinizer Server
2. Edit `/home/plexer/scrutinizer/files/applications.cfg`

Configuring server and data source options

The configuration settings for integrating Scrutinizer with the Network History on EndaceProbes are specified by adding a URL string to the config file using the following URL encoded format:

```
[INTEGRATION NAME], https://[HOSTNAME or IP]/vision2/pivotintovision/?datasources=[DATASOURCES]&title=Scrutinizer-Investigation&start=%zs&end=%ze&tools=conversations_by_ipaddress%2Cbandwidth%2CtopTalkers_by_ipaddress%2CtrfficOverTime_by_prot&ip=%i, Endace Vision 2 - Investigations
```

Where:

[INTEGRATION NAME] is the name that is used in Scrutinizer's popup menu to identify the integration. It shows up under "Other" in the Reports menu in Scrutinizer relating to an alert. NOTE: it is possible to define more than one URL entry in the configuration file if you wish to. In this case, it's advisable to choose Integration Names that uniquely identify each configuration setting.

[HOSTNAME or IP] specifies the server that you want to connect Scrutinizer to. This will either be the IP address or hostname of an EndaceProbe, or alternatively the IP address or hostname of an EndaceCMS Central Management Server if you want to connect to multiple EndaceProbes simultaneously using Central Vision.

[DATASOURCES] specifies the names of the data sources (RotationFiles) that you wish to be included in searches for packet history related to the Scrutinizer alert. You can specify multiple datasources, separated by the URL encoded comma character (%2C). These datasources must be fully qualified in the format `hostname:rotfile_name`. Note that the colon must be URL encoded (%3A) too.

Below is a sample URL that is configured to connect to an EndaceCMS Central Management Server and access the data residing in RotationFiles on three different EndaceProbes:

Example URL configuration

```
Pivot to Vision, https://end_cms/vision2/pivotintovision  
/?datasources=ep1%3Aweekly%2Cep2%3Aweekly%2Cep3%3Aweekly  
&title=Scrutinizer-Investigation&start=%zs&end=%ze&tools  
=conversations_by_ipaddress%2Cbandwidth%2CtopTalkers_by_  
ipaddress%2Ctrafficovertime_by_prot&ip=%i, Endace Vision 2 -  
Investigations
```

EndaceVision has a number of different visualization tools that may be specified in the URL configuration. For more information on what visualization tools are available, refer to the EndaceVision v2 User Guide.

This document is provided on an "AS IS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND" basis, including (without limitation) any warranties or conditions as to accuracy, non-infringement, merchantability or fitness for a particular purpose. This documentation is subject to change without notice.

In no event shall Endace Technology Limited and/or any of its affiliates be liable for damages, losses (direct or indirect) or costs incurred as a result of the use of this documentation or any inaccuracies or errors contained in this documentation, and the use of this documentation is at your own risk.

Endace™, the Endace logo and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

For more information on the Endace portfolio of products,
visit: endace.com/products

For further information, email: info@endace.com