RSA NetWitness Platform

Integration Configuration Guide

Anomali Link

Last Modified: Thursday, July 29, 2021

Integration Product Information:

Vendor: Anomali
Versions: API v1.0

Partner Product Information:

Supported On: Netwitness Platform 11.2 and later

Anomali Link for RSA NetWitness

Anomali Link is a software that fetches events at a configured interval from RSA NetWitness server and uploads them to **Anomali Match** to perform correlation and advanced security analysis. This enhancement does not require any additional configuration on RSA NetWitness. Anomali Link 1.0 is compatible with Anomali Match 4.3.

About Installing

Anomali Link must be installed on a standalone system that adheres to the requirements specified in System Requirements.

Guidelines for Installing

1. Install Anomali Link for each server to collect data from multiple RSA NetWitness servers.
2. Configure Anomali Link to connect to the Internet over a proxy server.
3. Review the Prerequisites.

System Requirements

Anomali Link is currently supported on Linux with the following specifications:

Platform	Specifications
Linux (64-bit)	• Any RedHat, CentOS, Ubuntu release, running kernel version 2.6 or later • CPUs: 8 Cores • Memory: 8 GB • Minimum disk space: 20 GB **Note:** Anomali recommends installing Anomali Link on a solid state drive for best performance.
RSA NetWitness version	RSA NetWitness 11.2 or higher

Performance Numbers

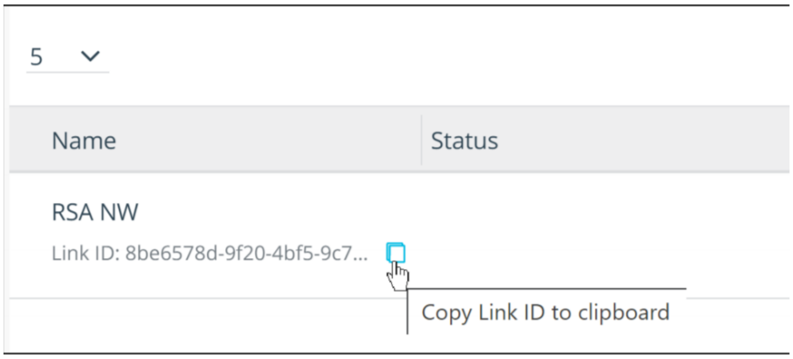
The following table summarizes the performance numbers for Anomali Link. Anomali Link is installed to the memory (8 GB) and disk (20 GB) specifications, as described in System Requirements.

CPUs	Maximum EPS (for CEF events)
8 Cores	5K Events Per Second

Prerequisites

Before installing Anomali Link, ensure the following prerequisites are met:

- You must have Anomali Match version 4.3 or higher already deployed before installing Anomali Link.
- Go to the **Settings** > **Links** page in the Anomali Match User Interface and create Anomali Link. Refer to the *Anomali Match Administration & User Guide* for information on creating Anomali Link. When you create Anomali Link in Anomali Match, a Link ID is automatically generated for it. This ID is required to complete the configuration of Anomali Link during installation. Copy this ID, as shown in the following example.



Enter this ID during Anomali Link installation.

- You must have a user account on Anomali Match that will be used by Anomali Link to communicate with the Anomali Match server. The Anomali Match user must belong to the admin group.
- You must install Anomali Link as a non-root user.
- Check for the availability of port 9776 during installation. The Link uses port 9776 on the system where it is installed for event drilldown to RSA NetWitness. If the port is not available, the next available port is **automatically** selected during the installation process.
- Ensure that the system on which you will install Anomali Link has the `lsof` utility available. To check if the utility is available, run this command:

  ```
  rpm -qa | grep lsof
  ```

  If `lsof` is available, the command returns a value similar to the following: **lsof-4.87-4.el7.x86_64**.

Installing Anomali Link for RSA NetWitness

Perform the following steps to install Anomali Link for RSA NetWitness

- Log in as a non-root user on the system where you want to install Anomali Link.
- Copy the Anomali Link installation file on this system to the home directory of the non-root user you are logged in as.
- Enter this command to change the mode of the installation file:

  ```
  chmod +x anomali_link_rsa_1.0.0_linux64.nn.bin
  ```

  where `nn` is the build number as specified in the installation file.
- Run the following command to start installation:

  ```
  ./anomali_link_rsa_1.0.0_linux64.nn.bin
  ```
- Enter the installation directory where you want to install Anomali Link. The installation process runs in the background and installs the software.
- Specify the following settings:

Destination Settings	
Setting	**Description**
Anomali Match root URL	URL for the Anomali Match server Format: **https://localhost:8080/api/v1** Replace localhost with the host name of the system on which Anomali Match is installed. By default, the Anomali Match service is installed to use port 8080. However, if a port conflict is found during the Anomali Match installation, you are prompted to enter an alternate port.
Username	Anomali Link Username to authenticate into the Anomali Match server. Go to **Settings** > **Users** and select any user that belongs to the **admin** group on the Anomali Match system.
Password	Password for the user you specified above.

RSA NetWitness Settings

Setting	Description
RSA NetWitness URL	Host name or IP address where the RSA NetWitness server is installed, and the port number to the RSA SDK. Format is http://<rsa_concentrator_host_or_IP>:50105 **Note:** The SDK port default is 50105 and it is the *Concentrator* component of RSA NetWitness which runs the SDK.
RSA NetWitness username	Username for RSA NetWitness. **Caution:** Make sure that the RSA NetWitness user account has permission to use the RSA NetWitness API. For more information, see RSA NetWitness Support.
RSA NetWitness password	Password for the RSA NetWitness user.
Link ID	The ID that is generated on Anomali Match when Anomali Link is added on the **Settings** > **Links** UI page. For example, 85812ac9-935b-48a2-b9fb-91ee3a28a229 See Prerequisites.

Backfill Settings

Setting	Description
Enable Backfill	By default, it is set to **no**. Anomali Link fetches the first set of events from RSA NetWitness from the time it is up and running. However, this setting can be configured to fetch past events by entering **yes**. When you enable this setting, a separate workflow runs on Anomali Link to fetch events from the past.

Backfill Settings

Setting	Description
Backfill Start Time	Specify how far back in time from which Anomali Link will backfill events. Default: **-7d@d** This means to start from 7 days ago. Specify a different time setting; for example, **-2M@M** (2 months), **-24h@h** (24 hours). This format **@d**/**@h** is a rounding value. For example, **-24h@h** will subtract 24 hours from the current time and then round to the exact hour. Rounding the value is optional. These values are also valid: **-2M**, **-7d**, **-12h**, and so on. Absolute time is also accepted in this format: **2020-08-04 00:00:00**
Backfill End Time	Specify the end time when backfill should stop filling events. Default: **now** As with Backfill Start Time, you can specify a different time setting; for example, -1d@d (1 day), -12h@h (12 hours) Absolute time is also accepted in this format: **2020-08-11 14:43:07** **Note:** If you accept both the Backfill Start Time and Backfill End Time default values, the last 7 days of events will be backfilled.

Proxy Settings

Setting	Description
Enable proxy support	By default, it is set to **no** If you choose **yes**, enter the following additional information • Type of proxy: HTTP ; Default: **HTTP** • Proxy server host name or IP address

Proxy Settings

Setting	Description
	• Port (on which the proxy server listens for connections) • Does the proxy require authentication? **Yes** or **No**; Default: **no** If the value is set to **yes**, enter the user name and password needed to connect to the proxy server. The credentials are obfuscated before they are stored in the configuration file.

Upgrade

Setting	Description
Update Anomali Link when upgrade becomes available	**yes** or **no**; Default: **yes** Whether to automatically upgrade Anomali Link when updates are available from Anomali. Anomali strongly recommends that you set this option to **yes** to ensure that your Anomali Link is running the latest software.

Query Processing

Setting	Description
Timespan for each query iteration	Default: **10m**
Number of threads for live event processing	Default: **2** The number of simultaneous queries to run on the RSA NetWitness server.
Number of threads for backfill processing	Default: **2** The number of simultaneous queries to execute for backfill.

Important: Before increasing any thread count, note that RSA NetWitness can handle a limited number of simultaneous queries. Performance may decline if you exceed the limit as configured in the RSA NetWitness server. Drilldown performance may be impacted if the maximum concurrent queries are consumed by live event and backfill processing.

Important: For more information on how to configure the query limits on RSA NetWitness, see RSA NetWitness documentation for the **max.concurrent.queries** setting. The documentation includes recommended settings based on the number of cores on your system.

- If port 9776 was unavailable on the system on which you are installing Anomali Link, the next available port was automatically selected and configured. This information and the selected port number is displayed on your installation screen. Edit the existing entry for the RSA NetWitness URL with this port number in Anomali Match for event drilldown to work properly.

  For more information on editing Anomali link, see *Anomali Match Administration and User Guide*.

- Once you see the **Anomali Link installed...** message, run this command to start Anomali Link in standalone mode:

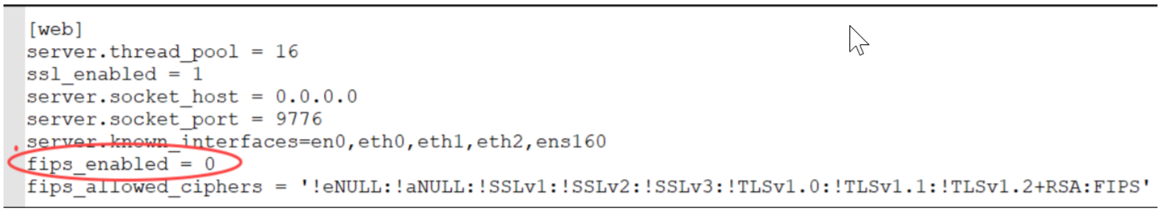
  ```
  <install_dir>/bin/anomali_link start
  ```

Alternatively, you can run Anomali Link as a service, as described in Running Anomali Link as a Service.

Anomali Link is ready for use. It works automatically without requiring any further action from you.

Enable FIPS-140

Anomali Link has the capability for being FIPS-140 compliant. However, this feature is not enabled by default, as shown in the `[web]` section of *etc/anomali_link_default.conf*



```
[web]
server.thread_pool = 16
ssl_enabled = 1
server.socket_host = 0.0.0.0
server.socket_port = 9776
server.known_interfaces=en0,eth0,eth1,eth2,ens160
fips_enabled = 0
fips_allowed_ciphers = '!eNULL:!aNULL:!SSLv1:!SSLv2:!SSLv3:!TLSv1.0:!TLSv1.1:!TLSv1.2+RSA:FIPS'
```

Caution: Do not edit any *XXX.default.conf* file directly. These contain default configurations as shipped from Anomali. They are overwritten during fresh installs and upgrades. You therefore run the risk of losing your customizations.

Important: As a best practice, enter the customizations in the corresponding *XXX.conf* file to ensure that they are preserved. If possible, take a back up of this file. This file is preserved through upgrades. Restore from backup if necessary.

Steps to Enable FIPS-140 Compliance

1. Add the `[web]` section if it does not yet exist in the anomali_link.conf file:

   ```
   [web]
   ```

2. Add the following line to the `[web]` section, setting the value to **1**, as shown:

   ```
   fips_enabled = 1
   ```

3. Save the *anomali_link.conf* file.

4. Stop, then start Anomali Link. See Anomali Link Commands.

Anomali Link Commands

Start Link : `<install_dir>/bin/anomali_link start`

Stop Link : `<install_dir>/bin/anomali_link stop`

Check status of Link : `<install_dir>/bin/anomali_link status`

Running Anomali Link as a Service

Follow the procedure below and configure Anomali Link to run as a service

1. Log in as a `root` user.

2. Run this command:

   ```
   <install_dir>/bin/alink_install_service
   ```

3. Start the service:

   ```
   /etc/init.d/alink start
   ```

Removing Anomali Link Service

Steps to remove Anomali link service

1. Log in as a `root` user.

2. Run this command:

   ```
   <install_dir>/bin/alink_install_service uninstall
   ```

Rerunning Configuration Wizard

Steps to rerun the configuration wizard

1. Stop Anomali Link using the below command:

   ```
   <install_dir>/bin/anomali_link stop
   ```

2. Run this command on the system where Anomali Link is installed:

   ```
   <install_dir>/bin/anomali_link config
   ```

3. Restart the Anomali Link server using the below command:

```
<install_dir>/bin/anomali_link start
```

Uninstalling Anomali Link

Steps to uninstall Anomali Link

1. Log in as the same non-root user that installed the Anomali Link software.
2. Run this command:

```
<install_dir>/bin/uninstall
```

Appendix A: Field Mapping

This appendix lists field mappings used by Anomali Link to map RSA NetWitness event fields to Anomali Match.

Note: The field mappings in this table are fixed and cannot be customized.

The following table provides information on the RSA NetWitness fields and the corresponding Anomali Match fields.

RSA NetWitness Field	Anomali Match Field
action	action
checksum	file_hash
device.ip	host
device.type	sourcetype
email.dst	receiver
email.src	sender
filename	file_name
host.dst	dest
host.src	src
ip.dst	dest_ip
ip.dstport	dest_port
ip.src	src_ip
ip.srcport	src_port
protocol	protocol
referrer	http_referrer
result.code	return_code
time	event_time

RSA NetWitness Field	Anomali Match Field
url	url
user.agent	http_user_agent
user.dst	user

November 2020

Trademarks