| IT SQUARED LLC

IT Squared / AppInternals SNMP traps ingestion into Splunk

Contents

General Information

Receiving SNMP data from AppInternals is possible and that data can contain useful context and information that can be used to enrich data in Splunk. When used to its full potential, this data can drive key insights into your environment.

Setting up ingestion and parsing of SNMP traps into Splunk is split into several steps. Once data starts flowing in, a user can use the **Splunk App for AppInternals** dashboards to enrich the gathered data.

SNMP traps ingestion from AppInternals configuration steps

1. Install and configure application

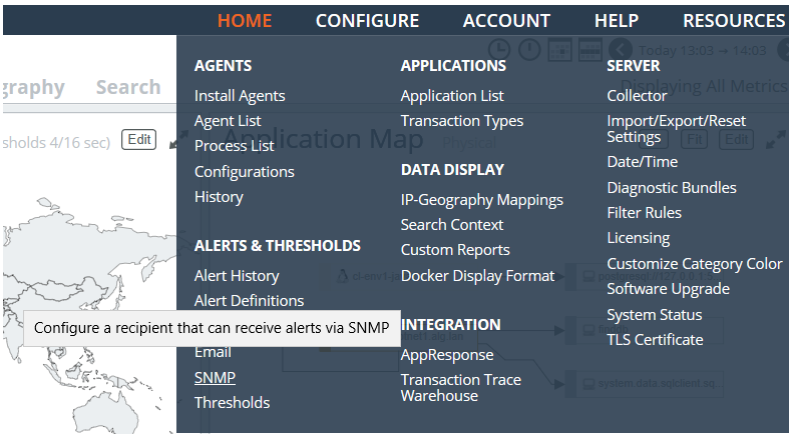
Install and configure application to receive and log SNMP messages, which will write those logs to disk where **Splunk Universal Forwarder** will pick them up. The choice of application is up to the user and depends on the environment and OS. For linux, it is recommended to install snmptrapd.

Configuration settings for AppInternals SNMP traps are simple, use community string that AppInternals would normally be using (see Step 2). For example, configuration file **snmptrapd.conf** for snmptrapd will look like this:

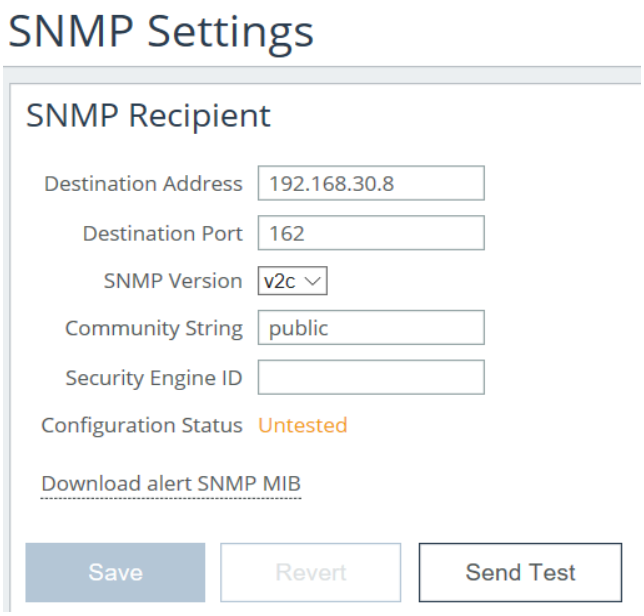
```
authCommunity   log    public

[snmp]

logOption f
/var/log/snmptraps.log
```

2. Configure SNMP recipient in AppInternals

Open the WEB UI for AppInternals as an administrator, and go into Configure -> SNMP.

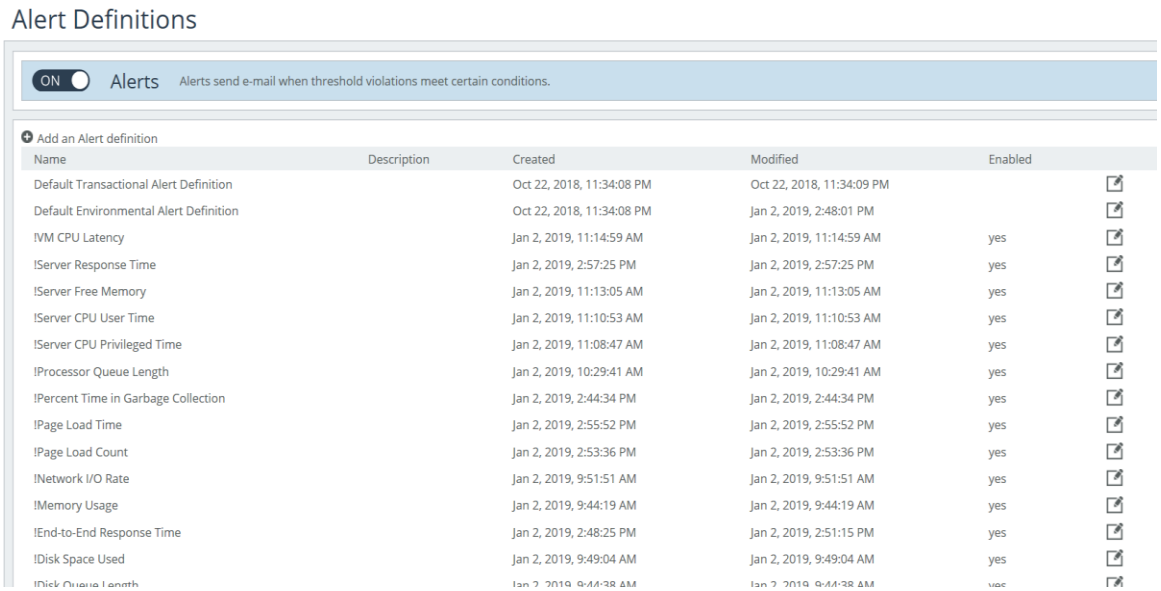


In the SNMP Settings window, set up the destination address for SNMP traps, port (if the user uses a non-standard port), community string (make sure to use the same string as for Step 1 as well).

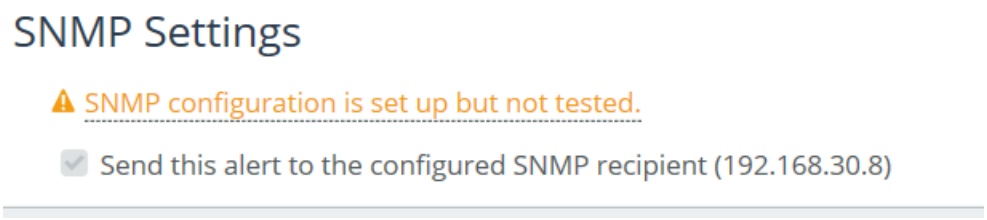


3. Configure Alert Definitions in AppInternal

Open the WEB UI for AppInternals as an administrator, go into Configure -> Alert Definitions.



Create or edit an existing Alert Definition(s) and in the SNMP settings section, enable sending alerts to what was configured on Step 2 SNMP recipient. Repeat this process for all desired alerts sent via SNMP traps into Splunk.



Note: Setting up Alert Definitions is not covered by this instructions, please refer to AppInternals documentation if you are not familiar with this feature.

4. Install the technical Splunk Add-On for the host name extraction from SNMP traps

Install the technical Splunk Add-On (appinternals_snmp.tar.gz) which can be found in **snmp** folder of **Splunk App for AppInternals**. The Add-On is responsible for host name extraction from SNMP traps during index time.

- For single instance Splunk - unpack appinternals_snmp.tar.gz into **apps** folder and restart the server to pick up settings.
- For distributed environment with single indexer - unpack appinternals_snmp.tar.gz into **apps** folder and restart the server to pick up settings.
- For distributed environment with index cluster - use the cluster bundle to distribute the add-on to all indexers and restart them.

If using a Deployment Server, unpack appinternals_snmp.tar.gz into the **deployment-apps** folder, add it to server class(es) of all Indexer(s) with restartSplunkd = true, reload server class(es).

5. Set up ingestion of generated log files

Previous steps created SNMP receiver, and instructed AppInternals what alerts to send and where to send them. On the Splunk side it was also set up to understand which sourcetype to expect and how to deal with that sourcetype. Finally, set up the ingestion of log files created by SNMP receiver.

This step is the same regardless whether those logs would be picked up by Splunk Universal Forwarder or by full server. Set up ingestion via simple local app configuration.

- Go to the instance where the logs file will be ingested from and navigate to **$SPLUNK_HOME/etc/apps** folder
- Create **local_inputs_appinternals_snmp** folder, then **local_inputs_appinternals_snmp/local** subfolder

- Create and edit **inputs.conf** file in **local_inputs_appinternals_snmp/local** folder with the following stanza, changing **path where to look for logs** and **index** according to the user's setup.

[monitor:///var/log/snmptraps.log]
disabled = false
index = main
sourcetype = aix_snmp_traps

- Restart Splunk to pick up the new monitoring stanza

Extracted fields

Once the steps above are completed, the alerts set up in AppInternals should be available in Splunk.

The following extracted fields are available:

- **alert_value**
- **alert_threshold**
- **alert_start_time**
- **alert_obj_name**
- **alert_metric**
- **alert_severity**
- **alert_aggregation**
- **alert_url**

The following calculated fields are available:

- **alert_category**
- **alert_transaction**
- **alert_instance**
- **alert_server**

Troubleshooting

If data is not present:

1. Check to see whether SNMP receiver is actually writing log files, and check its own errors.

2. If the log files do have data, and there is no data in Splunk, then likely there is something wrong with the stanza in inputs.conf; check Splunk logs for errors.

3. If SNMP events appear in Splunk but the user does not see extracted fields, check whether the Add-On from Step 3 is installed where it is supposed to be, and whether or not the **Splunk App for AppInternals** is installed on a Search Head(s) where the user is looking for data.

4. If all else appears correct - check raw events. The raw events should have this structure:

```
2019-02-18 16:48:53 cl-env1-aix1 [UDP: [192.168.30.10]:50763->[192.168.30.8]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (0) 0:00:00.00    SNMPv2-
MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.17163     SNMPv2-
```

```
SMI::enterprises.17163.1.1 = STRING: "1100.0"  SNMPv2-SMI::enterprises.17163.1.2 =
STRING: "2.0" SNMPv2-SMI::enterprises.17163.1.3 = STRING: "2019-02-18 14:30:00"
       SNMPv2-SMI::enterprises.17163.1.4 = STRING: "transaction type Web Resources"
       SNMPv2-SMI::enterprises.17163.1.5 = STRING: "Transactions"  SNMPv2-
SMI::enterprises.17163.1.6 = STRING: "major"   SNMPv2-SMI::enterprises.17163.1.7 =
STRING: "count"     SNMPv2-SMI::enterprises.17163.1.8 = STRING: "! Transactions"
       SNMPv2-SMI::enterprises.17163.1.9 = ""  SNMPv2-SMI::enterprises.17163.1.10 =
STRING: "https://cl-env1-aix1/#transactions:time=25841667+5&ttTableKey=1"
```

If notation is different, check the settings of your SNMP receiver.