Monitoring OpenVMS Servers using Slunk

Introduction

Options to manage and administer the OpenVMS server estate in the past were quite limited, with T4 being the usual choice. Today there are more technology options to chose from by using the VSI layered product VMSSPI. SPI can send alerts to several monitoring solutions including Dynatrace, Slunk, Slack, Datadog, Pagerduty and via a MQTT broker to any monitoring solution that supports MQTT.

This article shows how to monitor OpenVMS using Splunk.

OpenVMS Configuration

One provisor is that OpenVMS must be using the native TCPIP services otherwise VMSSPI is not an option. VMSSPI can be downloaded and tested free for 30 days, once that period as expired it requires a license.

Download **<arch>VMS-VMSSPI-V0900-27-1** from the VSI service site. There are three variants of the package, replace <arch> with X86 for intel, I64 for Itanium and AXP for AXP systems. There is also a detailed user manual that guides you through the installation which is a standard procedure for layered products.

VMSSPI for VSI OpenVMS User Guide

Once installed SPI can be controlled with a couple of commands.

1. SET DEF VMSSPI$DATA - Sets the default directory to the SPI data directory.
2. @ SYS$STARTUP:VMSSPI$STARTUP.COM – Starts the three processes the make up SPI.
3. @ SYS$STARTUP:VMSSPI$SHUTDOWN.COM – Stops the three processes.

I noticed that occasionally when stopping the processes, they didn't all stop after issuing the shutdown command. So check that the processes are all stopped when shutting down and all started when starting up.

```
PIPE SHOW SYSTEM | SEARCH SYS$INPUT VMSSPI
```

If any process is still running after shutdown it can be stopped using the stop command and the process id which is listed from the piped show system command above.

```
STOP/ID=<PRO_ID>
```

SPI can be configured using two files, VMSSPI$CONFIGURATION.DAT and MESSAGES.TXT. The installed default configuration will allow all alerts to be monitored. This could overload the system with too many messages, so initially certain classes of event could be disabled in the configuration file by editing the security filter settings. This is fully explained in the VMSSPI User Guide.

To configure monitoring all that is required is to edit the relevant monitoring module entry in the Messages file. To enable monitoring for Splunk and some of the other monitoring technologies a token is required which can be created using the monitoring programs administration functions (see below for Splunk).

Find the following line in the Message file and edit it, don't forget to remove the leading '#'.

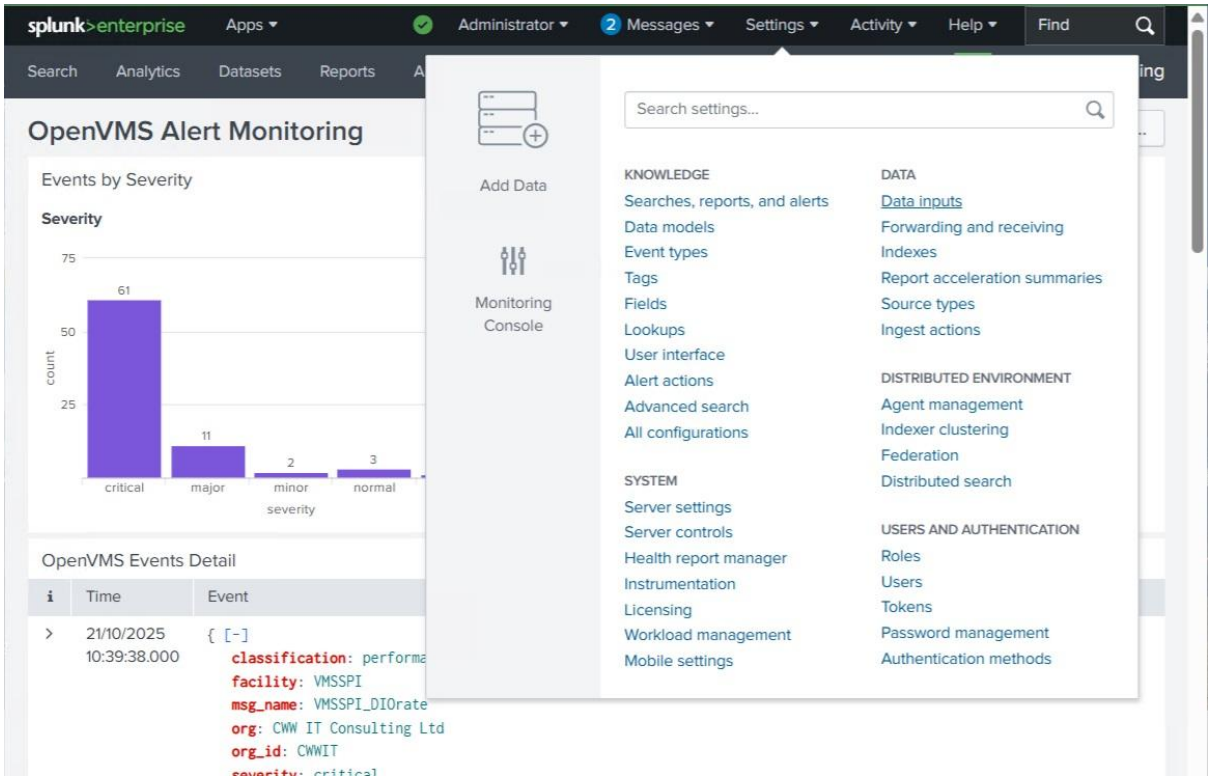
```
use interface module "vmsspi$root:[lib]vmsspi$splunk_shr.exe"
                     "https://<IP_Addr>:8088/services/collector/event <Token created in Splunk>";
```

Only two alerting modules can be enabled at any one time, so check the previous 'use interface' lines to make sure they are commented with a leading '#'.

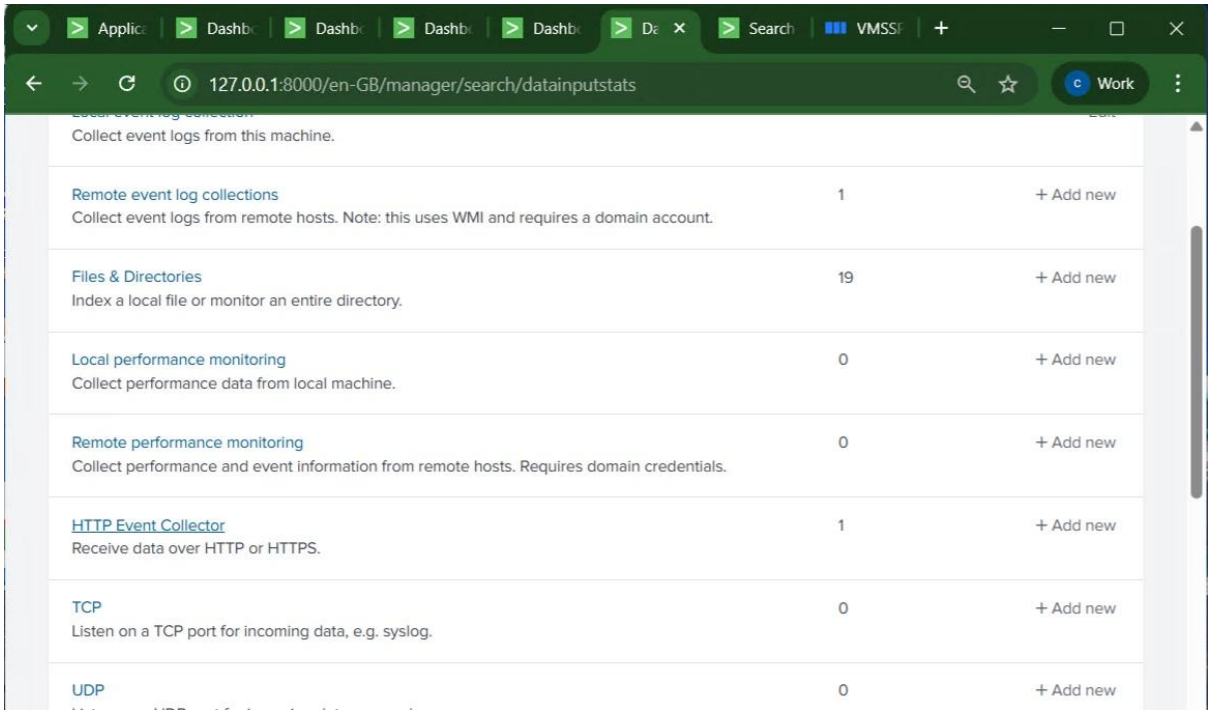
Once the edit is complete shutdown and startup the SPI processes and OpenVMS configuration is complete.

Splunk Configuration

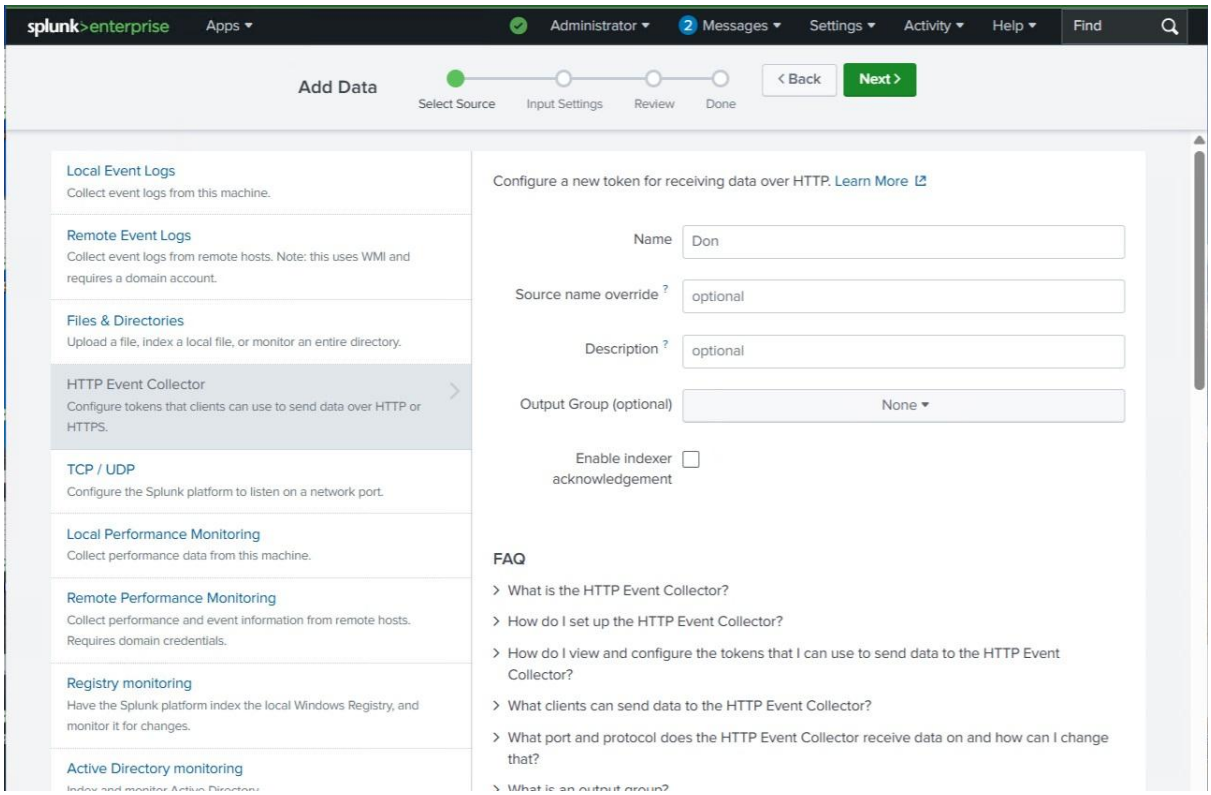
In Splunk a new token for OpenVMS monitoring needs to be created. Click the 'settings' menu and select 'Data inputs'.



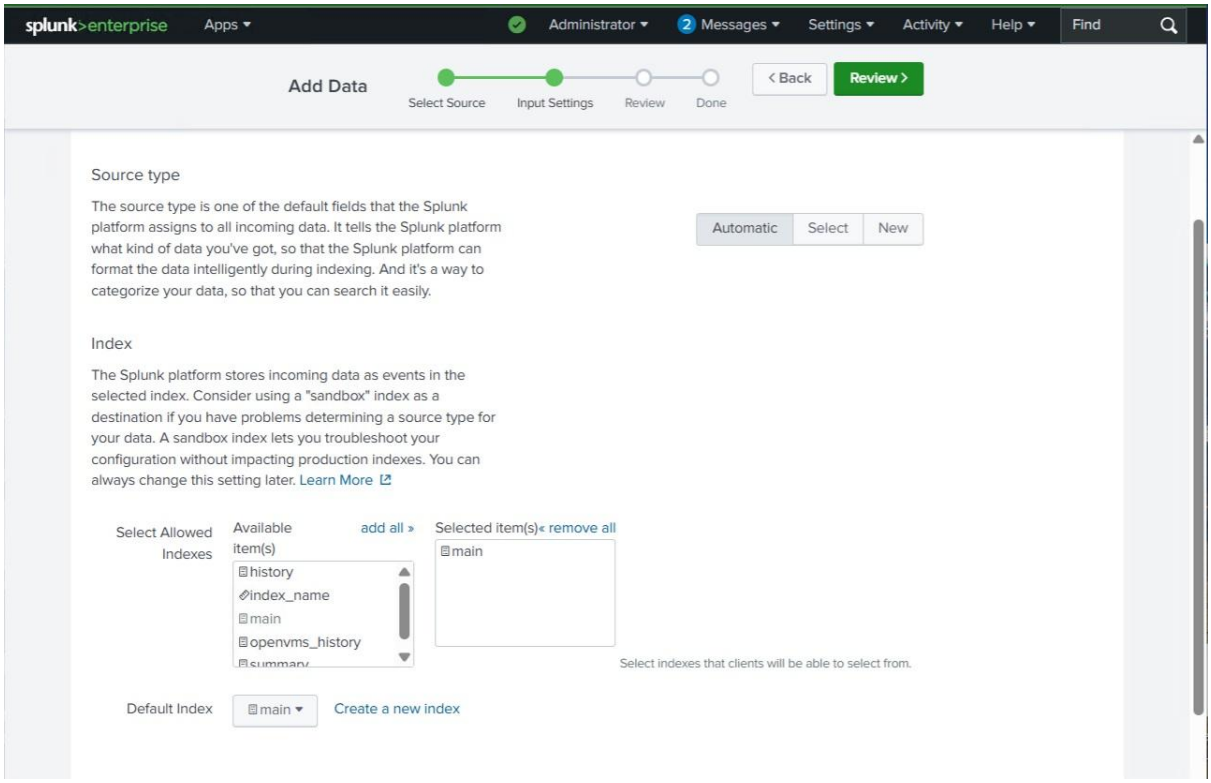
Select 'HTTP Event Collector' from the displayed list of data source types and click 'Add new'.



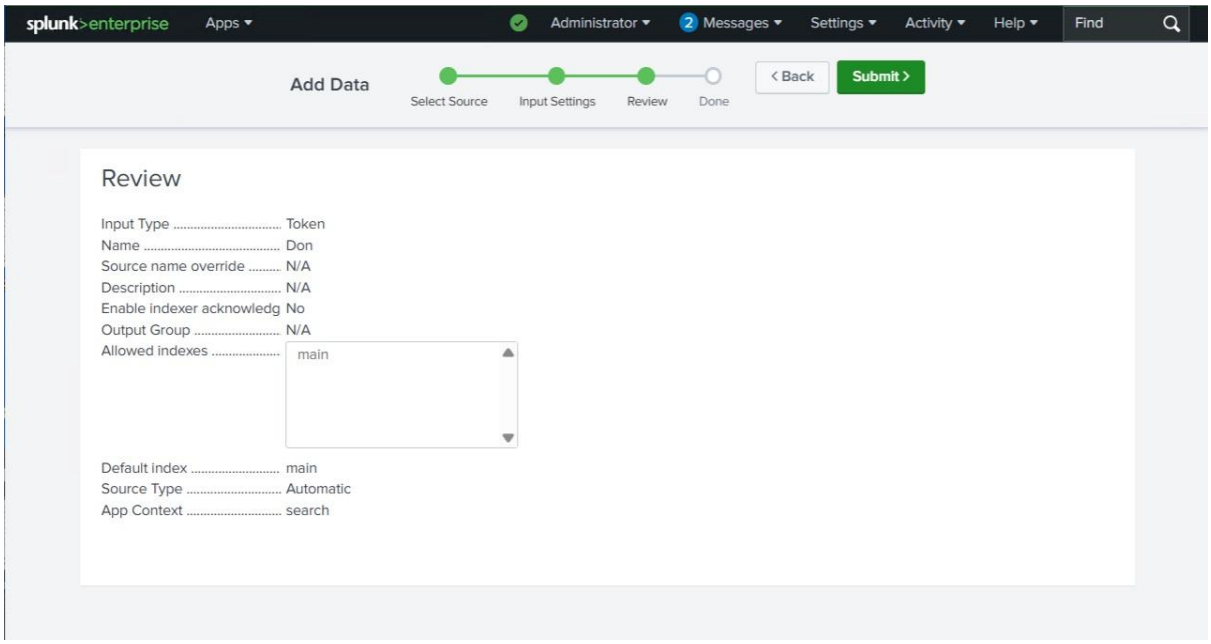
On the Add Data screen displayed, at least give the token a name and click the Next button.



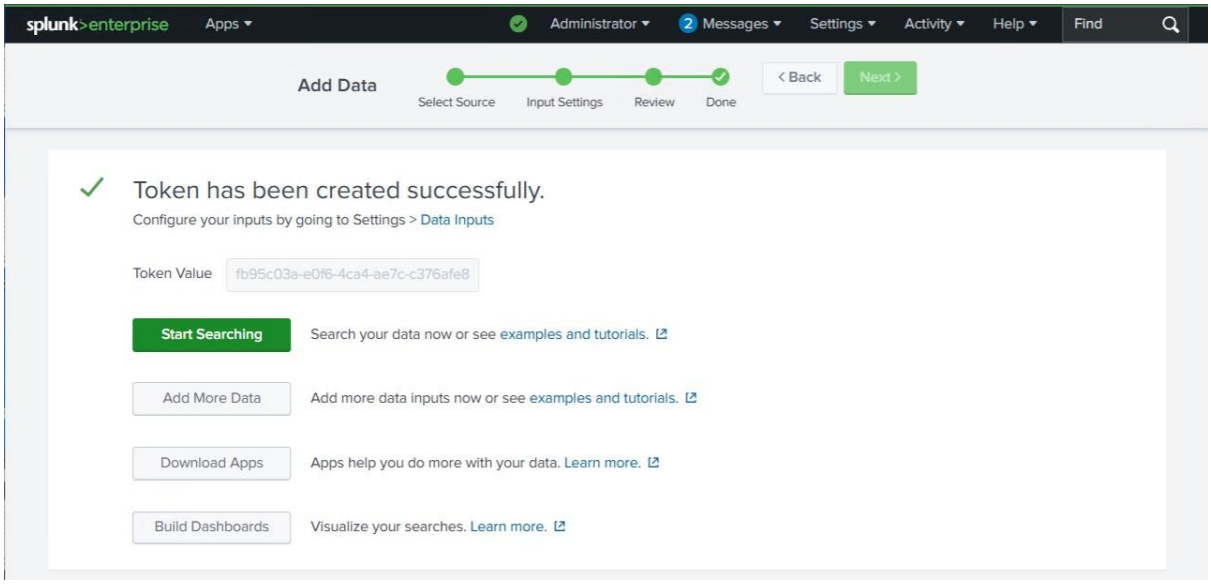
The data source will require an index, select one from the dropdown list. ‘main’ is a good option in most situations and click the Review button.



A review screen is displayed showing your selections, click the Submit button.



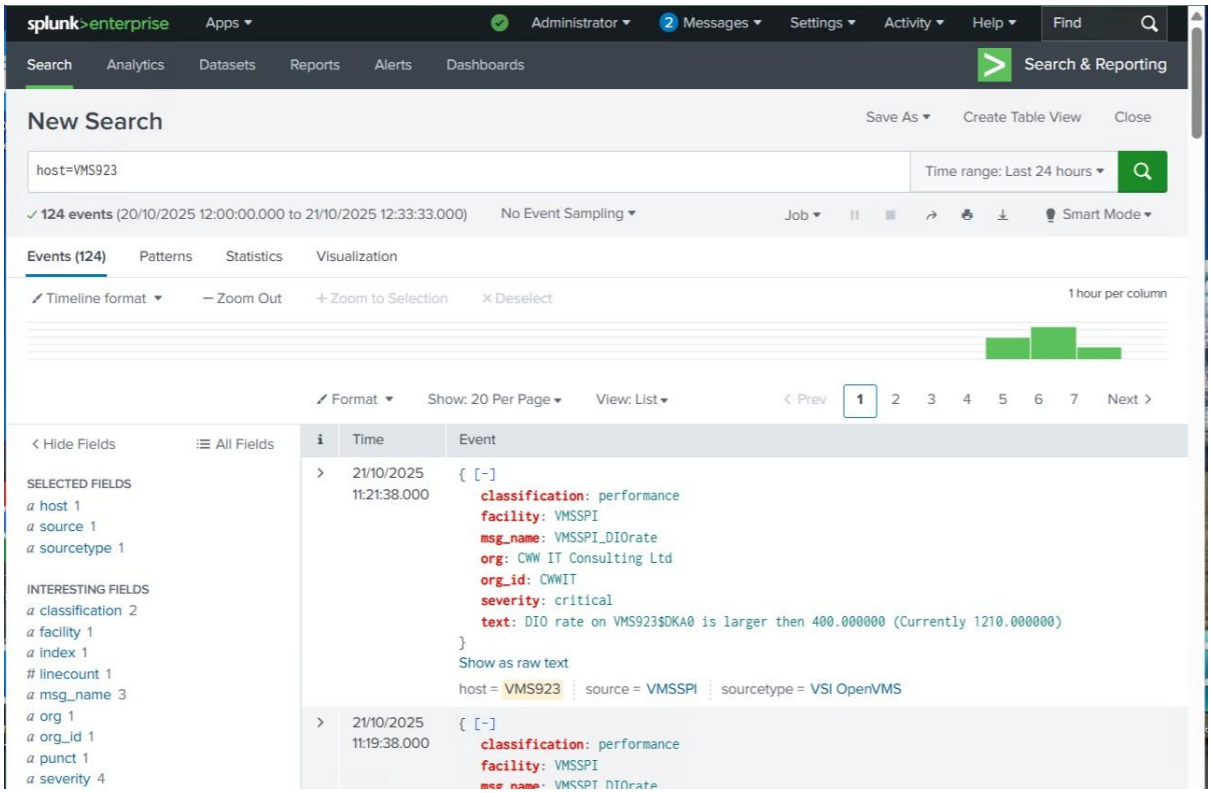
A ‘Token has been created successfully’ screen should be displayed. Take a note of the Token Value, this is the value that needs editing into the VMSSPI Message file ‘use interface’ line discussed previously.



Searching and Displaying data in Splunk

To generate some OpenVMS events, mount a volume, stop/start a process or if possible run UETP to generate more events.

In Splunk from the Home page select 'Search & Report', in the Search screen that's displayed click the 'Data Summary' button. A list of Hosts, Sources and Sourcetypes are displayed and your OpenVMS host should be in the list if events are being received by Splunk. Select the host from the dropdown and events should be displayed in the events window.



A dashboard can easily be created in Splunk to monitor the OpenVMS estate or a single host. The following simple dashboard contains four controls which can be added with the Dashboard Editor, it took approximately 30 minutes to create. :-

1. Dropdown list containing static names of the servers to be monitored.
   Default & Initial Value = All,
   First Entry All = *
   Rest of Entries Servername = Servername
2. Histogram to show event severity

   Search string host=$field1$ | chart count by severity

3. Pie Chart to show event categories
   Search string host=$field1$| stats by classification
4. Event Table to show event detail
   Search string host=$field1$