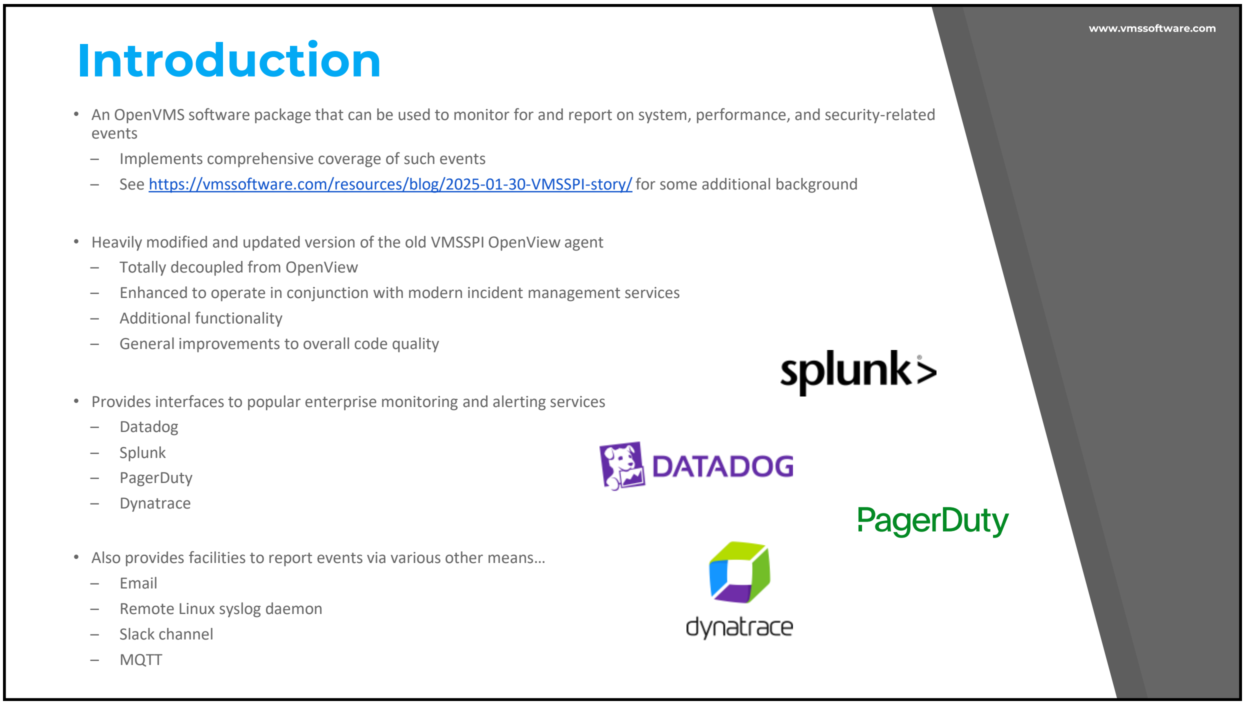
VMSSPI Overview

Webinar
February 2025

brett.cameron@vmssoftware.com

VMS Software

1



www.vmssoftware.com

Introduction

- An OpenVMS software package that can be used to monitor for and report on system, performance, and security-related events
  - Implements comprehensive coverage of such events
  - See https://vmssoftware.com/resources/blog/2025-01-30-VMSSPI-story/ for some additional background
- Heavily modified and updated version of the old VMSSPI OpenView agent
  - Totally decoupled from OpenView
  - Enhanced to operate in conjunction with modern incident management services
  - Additional functionality
  - General improvements to overall code quality
- Provides interfaces to popular enterprise monitoring and alerting services
  - Datadog
  - Splunk
  - PagerDuty
  - Dynatrace
- Also provides facilities to report events via various other means…
  - Email
  - Remote Linux syslog daemon
  - Slack channel
  - MQTT

2

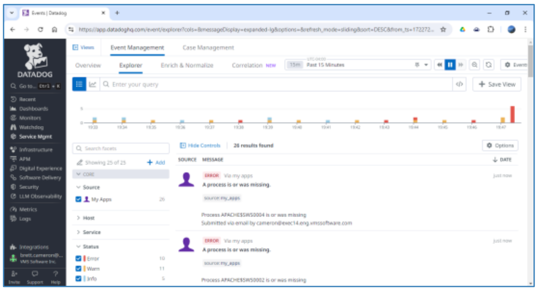
Core functionality

- Three main modules…
  - System:
    Reports on system-related items such as processes, disks, shadow sets, queues, …
  - Performance:
    Reports on system and process resource utilization
  - Security:
    Reports in real-time on security events detected by the audit server

- Plus, an experimental performance metrics module
  - Makes various metrics used by VMSSPI available to Prometheus
  - https://prometheus.io/

System module

- Activated at regular time intervals and can report on the following items
  - Changes in error count
  - OpenVMS cluster changes
  - Process availability
  - Disk status and free space
  - Queue manager status
  - Batch queue status
  - Print queue status
  - Batch job status
  - Shadow sets
  - Intrusions



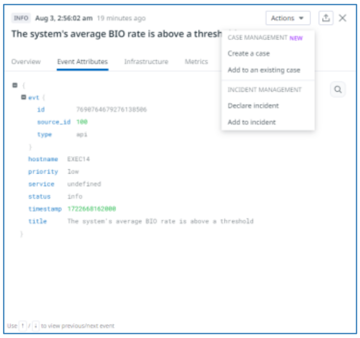
26 results found

ERROR Via my apps — just now
A process is or was missing.
source:my_apps
Process APACHE$SWS0004 is or was missing
Submitted via email by cameron@eexec14.eng.vmssoftware.com

ERROR Via my apps — just now
A process is or was missing.
source:my_apps
Process APACHE$SWS0002 is or was missing

Performance module

- Monitors various resources whose usage affects system and process performance
  - CPU utilization
  - Memory utilization
  - Page file utilization
  - Swap file utilization
  - Buffered I/O count
  - Direct I/O count
  - Processes in COM or COMO state
  - Total number of processes
  - Non-paged pool expansions
  - System page faults
  - Resource hash table utilization
  - LAN device utilization
  - Looping processes
  - Active CPUs
  - Processes in special states
  - Disk I/O (DIO rate, queue lengths, hot files)
  - Process quota utilization

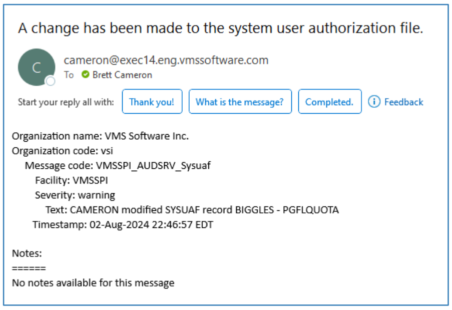


```
{
  evt {
    id         7690764679276138506
    source_id  100
    type       api
  }
  hostname   EXEC14
  priority   low
  service    undefined
  status     info
  timestamp  1722668162000
  title      The system's average BIO rate is above a threshold
}
```

Security module

- Continuously monitors and reports on security events recorded by the audit server, as defined by the module configuration
  - Logins, logouts, and login failures
  - Changes to the user authorization, rights list, and network proxy files
  - Access to protected objects such as files, devices, global sections, queues, …
  - Changes to the security attributes of protected objects
  - …

  - *Be careful what you enable* ☺



A change has been made to the system user authorization file.

cameron@exec14.eng.vmssoftware.com
To Brett Cameron

```
Organization name: VMS Software Inc.
Organization code: vsi
   Message code: VMSSPI_AUDSRV_Sysuaf
      Facility: VMSSPI
      Severity: warning
         Text: CAMERON modified SYSUAF record BIGGLES - PGFLQUOTA
     Timestamp: 02-Aug-2024 22:46:57 EDT

Notes:
======
No notes available for this message
```

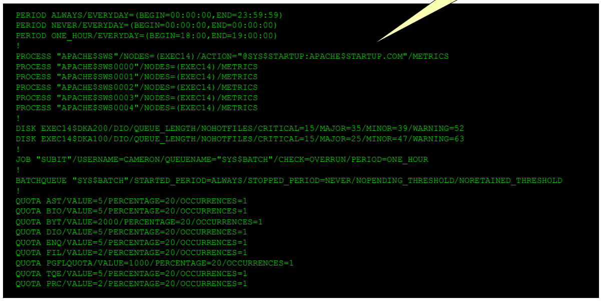
www.vmssoftware.com

Configuration

- Two configuration files…

- The main configuration file contains details of the items to monitor and when to monitor them
  - Cluster name information
  - Time interval(s) for performing checks
  - Restricted periods for monitoring
  - Enabling intrusion detection
  - Defining specific processes to be monitored
  - Disks to be monitored
  - Batch queues to be monitored
  - Print queues to be monitored
  - Batch jobs to be monitored
  - Shadow sets to be monitored
  - LAN devices to monitor
  - Process quota thresholds
  - Security filter settings
  - …

Note use of the "`/action`" and "`/metrics`" options



```
PERIOD ALWAYS/EVERYDAY=(BEGIN=00:00:00,END=23:59:59)
PERIOD NEVER/EVERYDAY=(BEGIN=00:00:00,END=00:00:00)
PERIOD ONE_HOUR/EVERYDAY=(BEGIN=18:00,END=19:00:00)
!
PROCESS "APACHE$SWS"/NODES=(EXEC14)/ACTION="@SYS$STARTUP:APACHE$STARTUP.COM"/METRICS
PROCESS "APACHE$SWS0000"/NODES=(EXEC14)/METRICS
PROCESS "APACHE$SWS0001"/NODES=(EXEC14)/METRICS
PROCESS "APACHE$SWS0002"/NODES=(EXEC14)/METRICS
PROCESS "APACHE$SWS0003"/NODES=(EXEC14)/METRICS
PROCESS "APACHE$SWS0004"/NODES=(EXEC14)/METRICS
!
DISK EXEC14$DKA200/DIO/QUEUE_LENGTH/NOHOTFILES/CRITICAL=15/MAJOR=35/MINOR=39/WARNING=52
DISK EXEC14$DKA100/DIO/QUEUE_LENGTH/NOHOTFILES/CRITICAL=15/MAJOR=25/MINOR=47/WARNING=63
!
JOB "SUBIT"/USERNAME=CAMERON/QUEUENAME="SYS$BATCH"/CHECK=OVERRUN/PERIOD=ONE_HOUR
!
BATCHQUEUE "SYS$BATCH"/STARTED_PERIOD=ALWAYS/STOPPED_PERIOD=NEVER/NOPENDING_THRESHOLD/NORETAINED_THRESHOLD
!
QUOTA AST/VALUE=5/PERCENTAGE=20/OCCURRENCES=1
QUOTA BIO/VALUE=5/PERCENTAGE=20/OCCURRENCES=1
QUOTA BYT/VALUE=2000/PERCENTAGE=20/OCCURRENCES=1
QUOTA DIO/VALUE=5/PERCENTAGE=20/OCCURRENCES=1
QUOTA ENQ/VALUE=5/PERCENTAGE=20/OCCURRENCES=1
QUOTA FIL/VALUE=2/PERCENTAGE=20/OCCURRENCES=1
QUOTA PGFLQUOTA/VALUE=1000/PERCENTAGE=20/OCCURRENCES=1
QUOTA TQE/VALUE=5/PERCENTAGE=20/OCCURRENCES=1
QUOTA PRC/VALUE=2/PERCENTAGE=20/OCCURRENCES=1
```

www.vmssoftware.com

The messages file

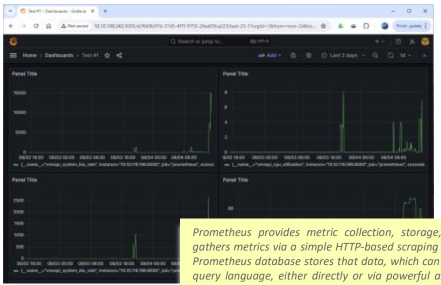
- Defines the characteristics and properties of all alerts that can be raised by any of the VMSSPI modules
- Describes details about how alerts will be reported
  - Email
  - Via a service such as DataDog, Splunk, Dynatrace, PagerDuty, MQTT, …
  - …

- Essentially comprises two sections:
  1. Definitions for various general/global items (mailing lists, SMTP gateway, organizational information, alerting module configuration)
  2. Customisable definitions for all possible messages/alerts that can be reported

- Every message/alert has a name (cannot be changed) and a set of configurable attributes
  - John will show examples
  - Blame me for the syntax

Performance metrics

- Somewhat experimental module (will be supported in the next release)
- Makes a (small but useful) subset of metrics used by VMSSPI available to Prometheus (https://prometheus.io/)
  - Average CPU utilization
  - Percentage network bandwidth utilization
  - Disk queue length
  - Overall memory utilization
  - Page file free space
  - Resource hash table usage
  - Swap file free space
  - System BIO and DIO rates
  - System page fault rate
  - Percent disk full (per monitored disk)
  - Per-process metrics for selected processes



Prometheus provides metric collection, storage, and query capabilities. It generally gathers metrics via a simple HTTP-based scraping system that pulls data from hosts. The Prometheus database stores that data, which can then be queried using the Prometheus query language, either directly or via powerful analytic and visualization tools such as Grafana (https://grafana.com/) to display and analyze the collected data in a near-real-time manner.

… Laim will talk about some things he's been doing with the Prometheus interface!

- Can readily include more metrics, but...
  - Will typically need to selectively include process metrics
  - Heisenberg wins…
    - Measurements will start to influence results

In summary…

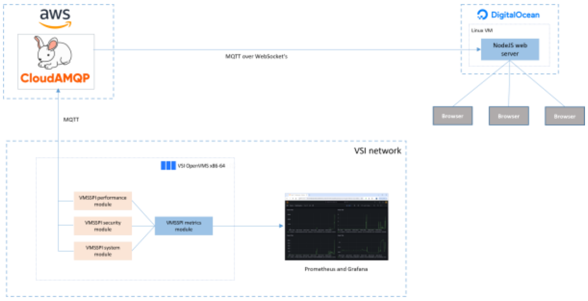
The aim of VSI VMSSPI is to provide a mechanism for OpenVMS systems to seamlessly and efficiently share incident and performance data with modern centralized (and possibly cloud-based) services such as Splunk, Dynatrace, PagerDuty, and Datadog, making it possible for organizations to monitor their OpenVMS systems in the same way as they monitor their other operating systems.

- Powerful, flexible, extensive monitoring and alerting solution for VSI OpenVMS
- Integrates with popular incident management systems
  - And can easily be extended to support new integrations (considering one or two)
- Important tool for VSI Managed Services
- Straightforward to install and run
  - But recommend engaging VSI Professional Services to help get the most out of it
- Some interesting future plans
  - Additional integrations (driven by customer requirements)
  - Expose (some) additional metrics
  - …

One more thing…

- Browse to http://192.241.141.109/
  - Uses MQTT over WebSockets to communicate with a RabbitMQ broker hosted with CloudAMQP on AWS
  - John has configured his demo to publish alerts via MQTT to this broker
  - Alerts will also be published to an internal Slack channel

- Anyone with the above web page open will (should) see alerts displayed as John triggers them



11

Over to John Seder…

VMS Software

12

VMSSPI Experiences

Liam Bainsfair – IT Systems Engineer

Environment Context

Newcastle Greater Mutual Group offers retail banking services to more than half a million Australians.

We have a workforce of more than 1600 and total assets of more than $20 billion.

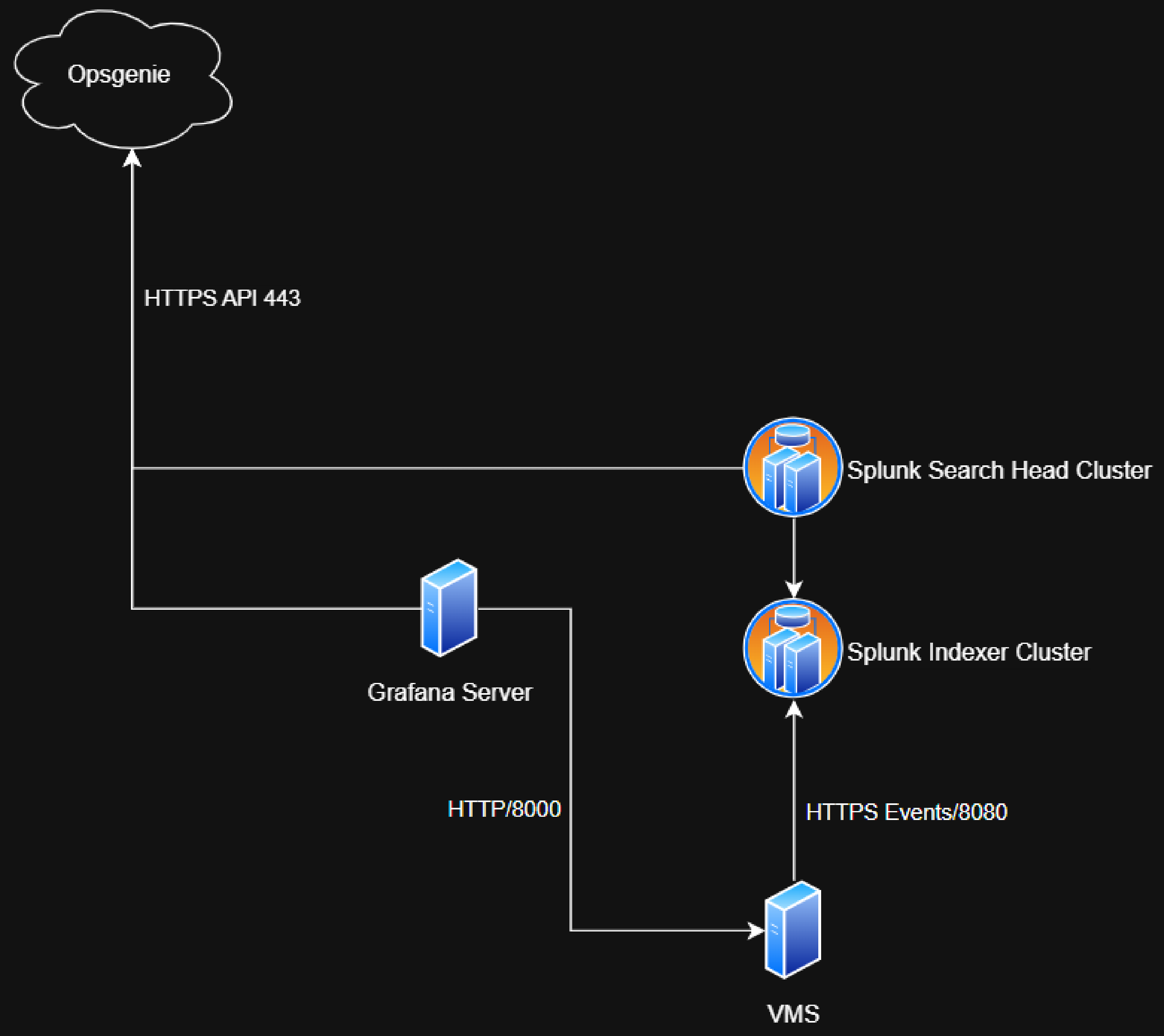
Running multiple OpenVMS clusters since the 1980’s

VAX > Alpha > IA64

Already running Splunk Enterprise (on-premise) cluster for application layer logging

Using an on-call solution, Opsgenie (Atlassian) for a few years

Existing real-time monitoring of VMS nodes was done through COMs, queues and SMTP



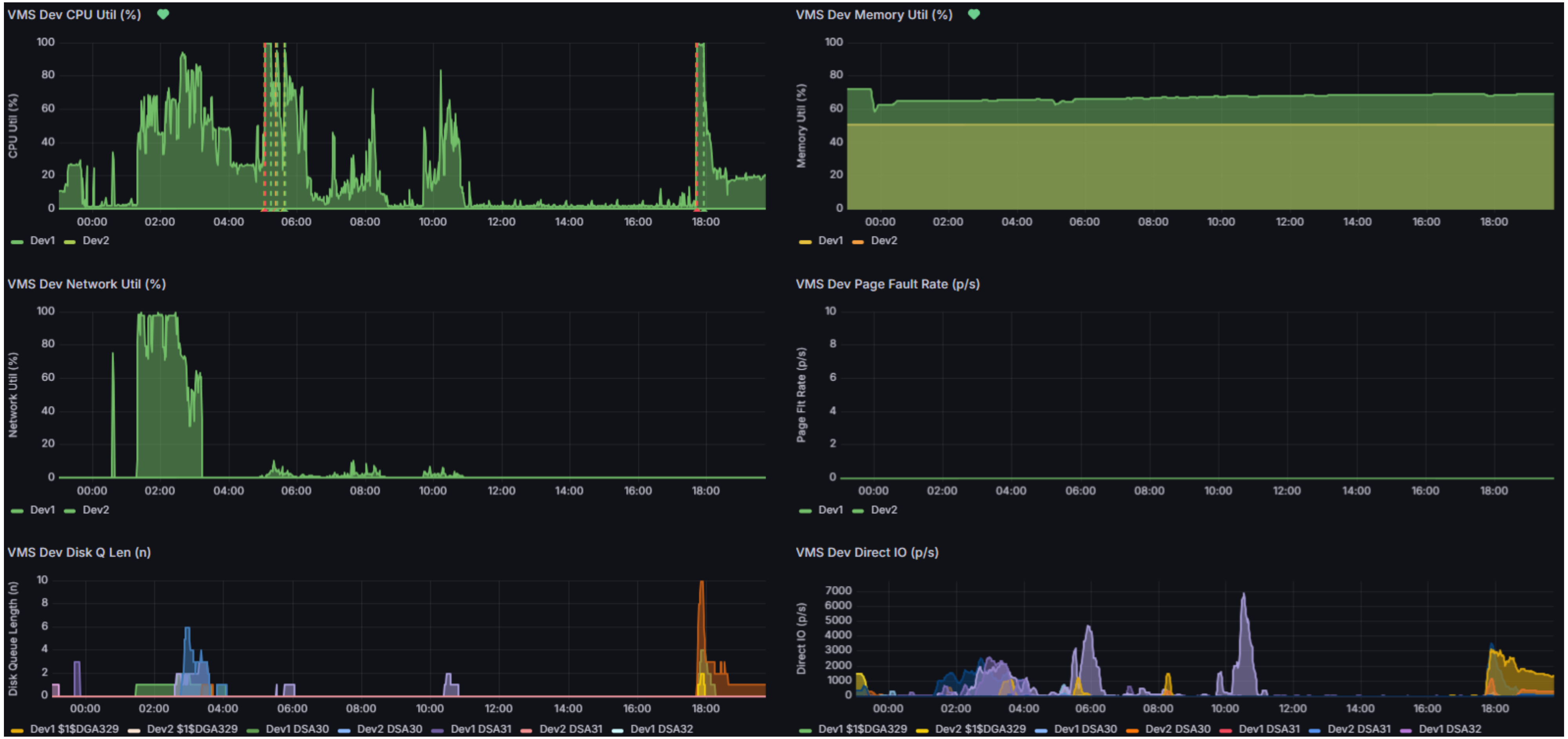
Basic Architecture Overview

- Real-time monitoring (Grafana)
- Log ingestion (Splunk)

Real-time Monitoring - Config

- Prometheus installed as a service, configured to look at VMS Servers on port 8000
- Grafana installed and configured to use Prometheus as an endpoint
- Dashboards are set up to show critical information
- Alerts are tied to data reaching certain thresholds (i.e. 90% CPU Utilisation)
- Alerts are configured to push to Opsgenie instance

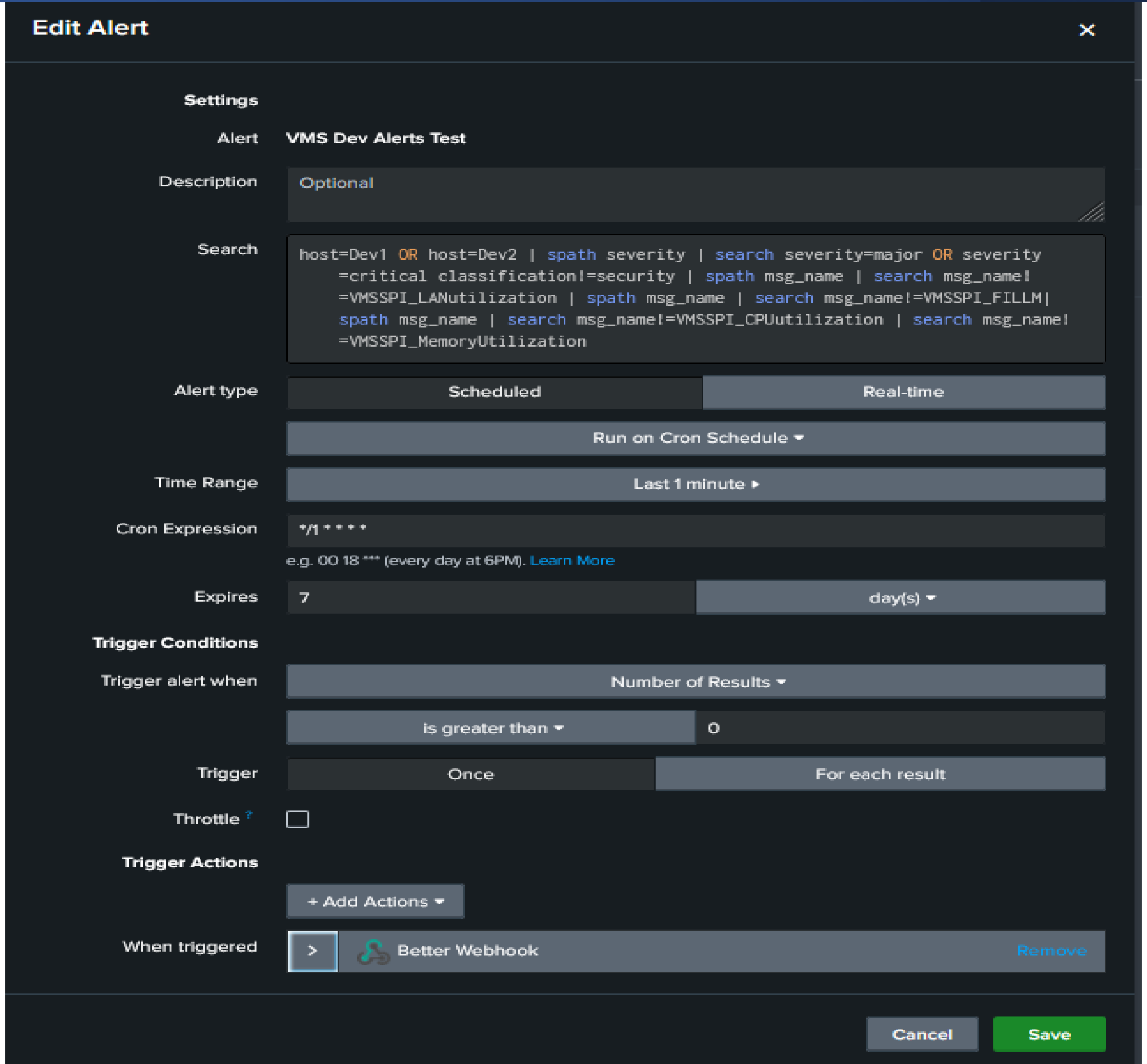
Real-time Monitoring - Example



Log Ingestion - Config

- Using preexisting Splunk Enterprise Environment, configured HTTP Event Collector (HEC) Endpoints
- Configured VMSSPI to use the Splunk endpoint
- Configure Alerts within Splunk to forward certain events to Opsgenie

Log Ingestion - Example



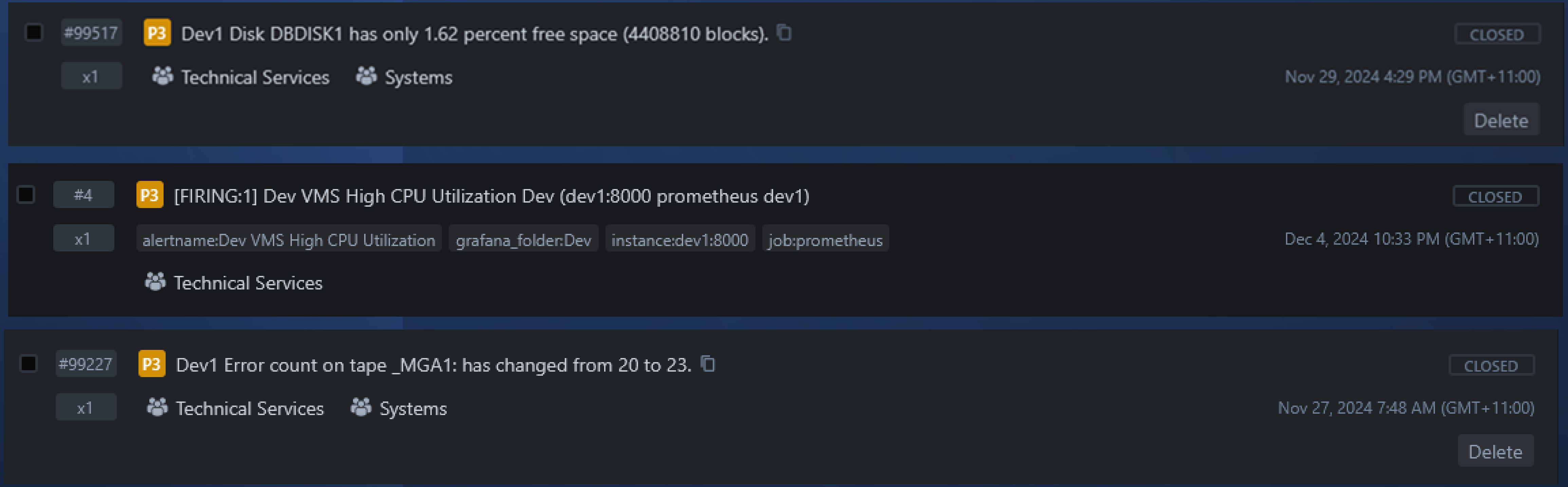
Edit Alert

Settings	
Alert	**VMS Dev Alerts Test**
Description	Optional
Search	see below

```
host=Dev1 OR host=Dev2 | spath severity | search severity=major OR severity
    =critical classification!=security | spath msg_name | search msg_name!
    =VMSSPI_LANutilization | spath msg_name | search msg_name!=VMSSPI_FILLM|
    spath msg_name | search msg_name!=VMSSPI_CPUutilization | search msg_name!
    =VMSSPI_MemoryUtilization
```

Alert type	Scheduled	Real-time
	Run on Cron Schedule ▾	
Time Range	Last 1 minute ▸	
Cron Expression	*/1 * * * *	
	e.g. 00 18 *** (every day at 6PM). Learn More	
Expires	7	day(s) ▾
Trigger Conditions		
Trigger alert when	Number of Results ▾	
	is greater than ▾	0
Trigger	Once	For each result
Throttle ?	☐	
Trigger Actions		
	+ Add Actions ▾	
When triggered	> Better Webhook	Remove

Opsgenie Examples



□ #99517 P3 Dev1 Disk DBDISK1 has only 1.62 percent free space (4408810 blocks).

x1 Technical Services Systems

CLOSED

Nov 29, 2024 4:29 PM (GMT+11:00)

Delete

□ #4 P3 [FIRING:1] Dev VMS High CPU Utilization Dev (dev1:8000 prometheus dev1)

x1 alertname:Dev VMS High CPU Utilization grafana_folder:Dev instance:dev1:8000 job:prometheus

Technical Services

CLOSED

Dec 4, 2024 10:33 PM (GMT+11:00)

□ #99227 P3 Dev1 Error count on tape _MGA1: has changed from 20 to 23.

x1 Technical Services Systems

CLOSED

Nov 27, 2024 7:48 AM (GMT+11:00)

Delete