Enterprise Monitoring (EM) for the Defense Meteorological Satellite Program (DMSP) Ground System (GS)

Mike Drumheller, Systems Engineer

Don Anderson, Integration Engineer

January 25, 2019

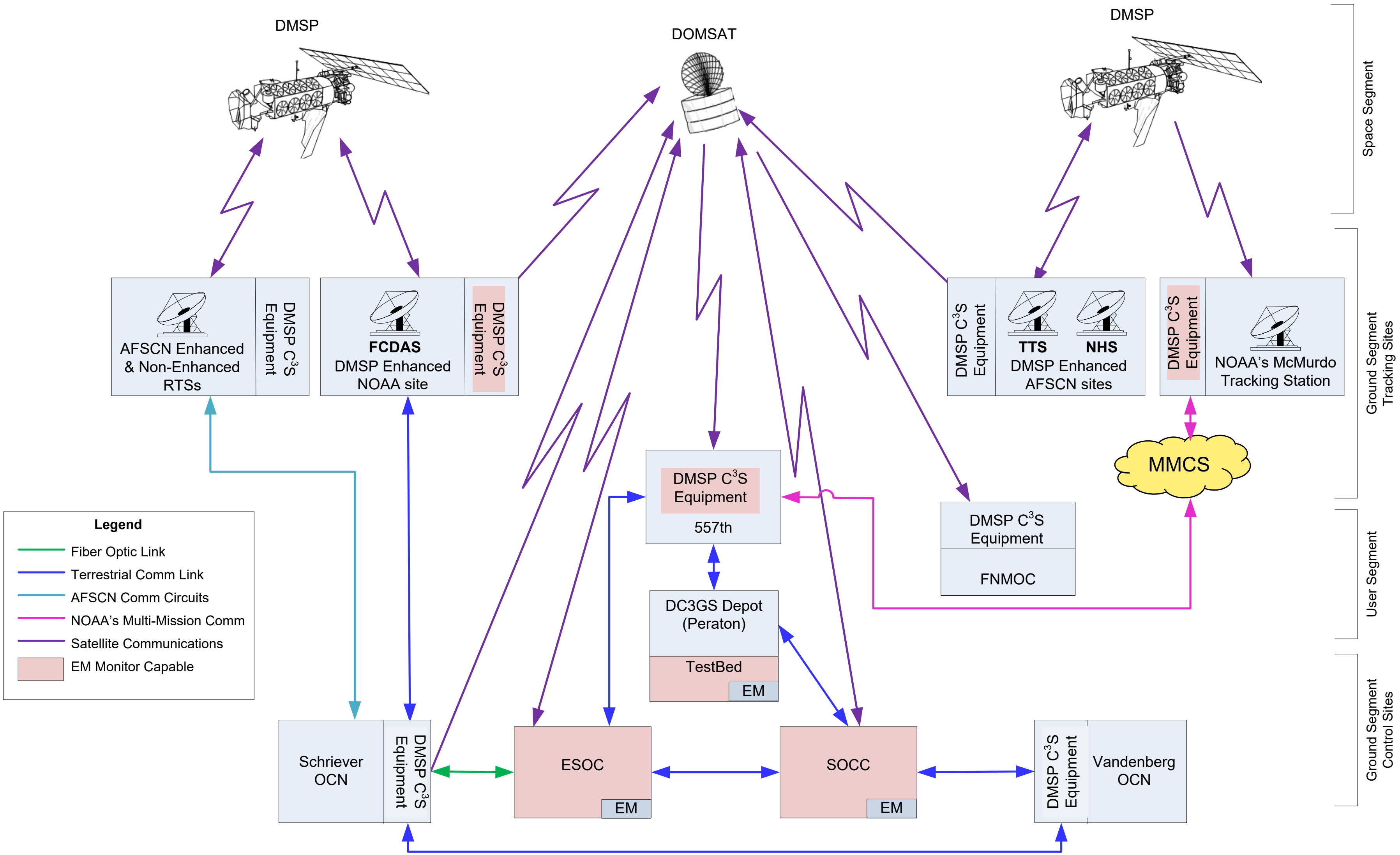
Agenda

- DMSP Overview
- Genesis of EM
- EM Capabilities
- Pre-EM Situational Awareness and Monitoring
- Move to IT-Centric and Modernization
- Operational Views
- Real World Benefits of EM
  - Prevent Operational Outage
  - Proactively Plan for Circuit Outage
  - Correlate Multiple System Metrics to Isolate a Problem
- Future Enhancements Leveraging EM Capabilities
  - Alerts from an Air-gapped System
  - Further Consolidation and Visualization of Log Data
  - Expand Traffic Flow Analysis

DMSP Overview

- **DMSP Mission**
  - Collect and disseminate – through all levels of conflict, consistent with the survivability of the supported elements – global visible and infrared cloud cover imagery in support of worldwide Department of Defense (DoD) operations and high-priority programs
  - Data is gathered continuously by the sensor payload onboard the satellite, transmitted in real-time to provide the direct readout of local area environmental data to components of the United States
  - 557th Air Force Weather Wing (AFWA) is assigned Tactical Control (TACON) of the DMSP per DoD directive. They establish data requirements and approve distribution of the meteorological information to the various authorized users
- **DMSP Command, Control and Communications (C3) Segment**
  - Operations centers at the National Oceanographic and Atmospheric Administration (NOAA) Satellite Operations Control Center (SOCC) at the Suitland, Maryland and the Environmental Satellite Operations Center (ESOC) at Schriever AFB, Colorado
  - Data acquisition at NOAA's Fairbanks Command and Data Acquisition Station (FCDAS) in Fairbanks Alaska, the National Aeronautical and Space Administration's (NASA) McMurdo Ground Station in Antarctica, and the Air Force Satellite Control Network (AFSCN) Remote Tracking Stations (RTSs)

DMSP Architecture



Genesis of EM

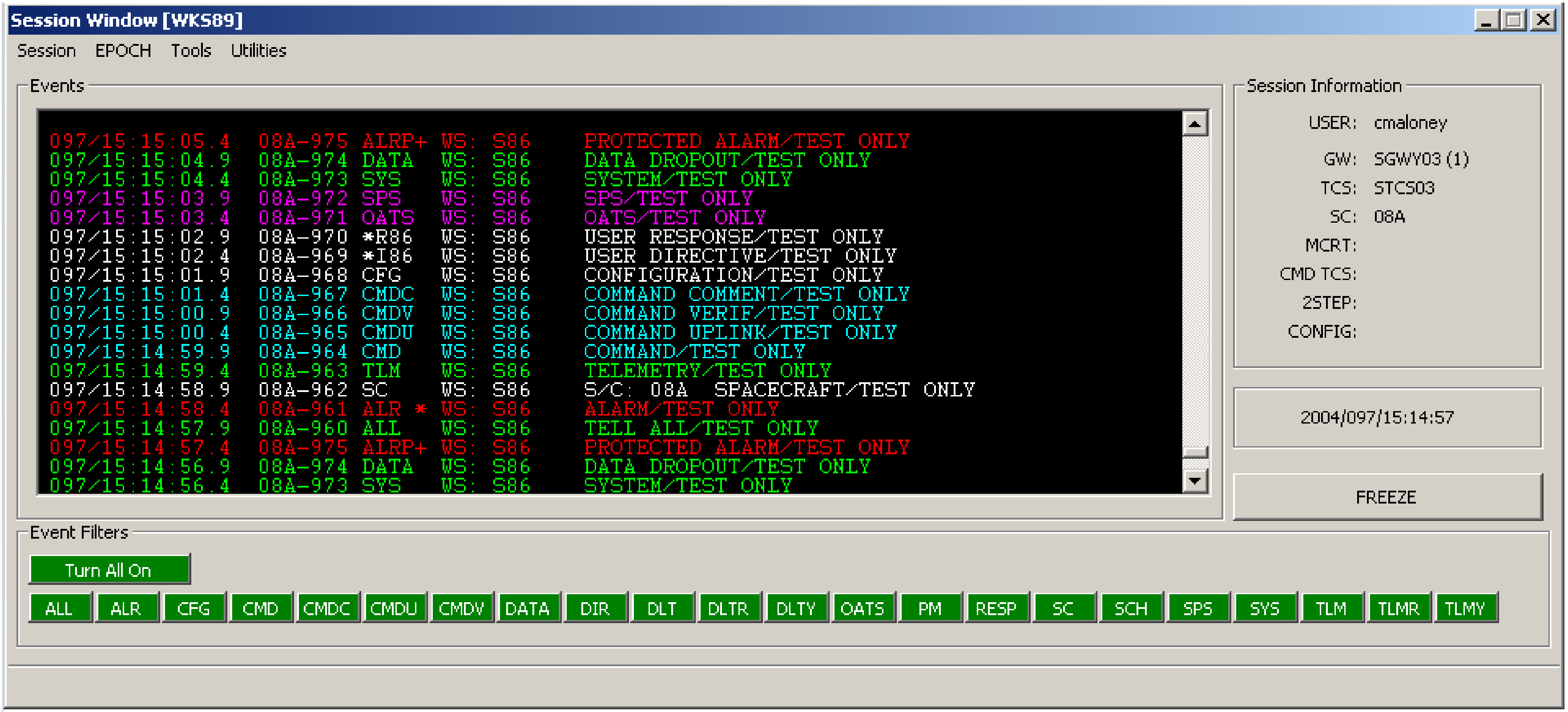
- **The legacy DMSP ground system was developed in the 1980s**
  - The design and technology at that time did not provide much of a monitoring and remote maintenance capability
    - Many ground system problems were discovered in real time or after the fact, which led to a reactive sustainment posture and failed contacts
    - Post forensics on ground system failures required many man hours to analyze numerous pieces of information and logs to determine the cause of failure
    - Problem isolation often involved multiple engineers and disciplines
- **Component and subsystems upgrades authorized by Air Force Space Command (AFSPC) Space and Missile Systems Center (SMC) Remote Sensing Systems (RSS) over the past five years provided the IT-centric infrastructure for EM**
  - EM provided the tools and capabilities to help the ground system remain viable and sustainable until mission end of life

EM Capabilities

- **Provide enterprise monitoring capability to monitor DMSP components and applications at critical locations improving situational awareness**
  - Empower engineers to tailor requests for information based on needs
  - Allow for proactive maintenance activities that increase availability
  - EM implemented at two locations following the current ground system operational concept where two Satellite Operation Centers, SOCC and ESOC, are utilized to support the mission
  - Focus placed on monitoring two critical and recently modernized subsystems
    - Mission Planning and Scheduling Subsystem (MPSS)
    - Telemetry and Commanding Subsystem (TCS)
- **Core monitoring capabilities added for DMSP component and applications**
  - System health/performance monitoring (storage, memory, processes)
  - Fault management (identification and alerts)
  - Event log monitoring and centralized security logging
  - Resource usage and trend analysis
  - Actively monitor server/network device and application availability
  - Analyze Local Area Network (LAN)/Wide Area Network (WAN) traffic flow and automate network change and configuration management

Pre-EM Situational Awareness and Monitoring

- Situational awareness before EM was only available to the operators from different views on their console
- The console display is limited and doesn’t provide enterprise view



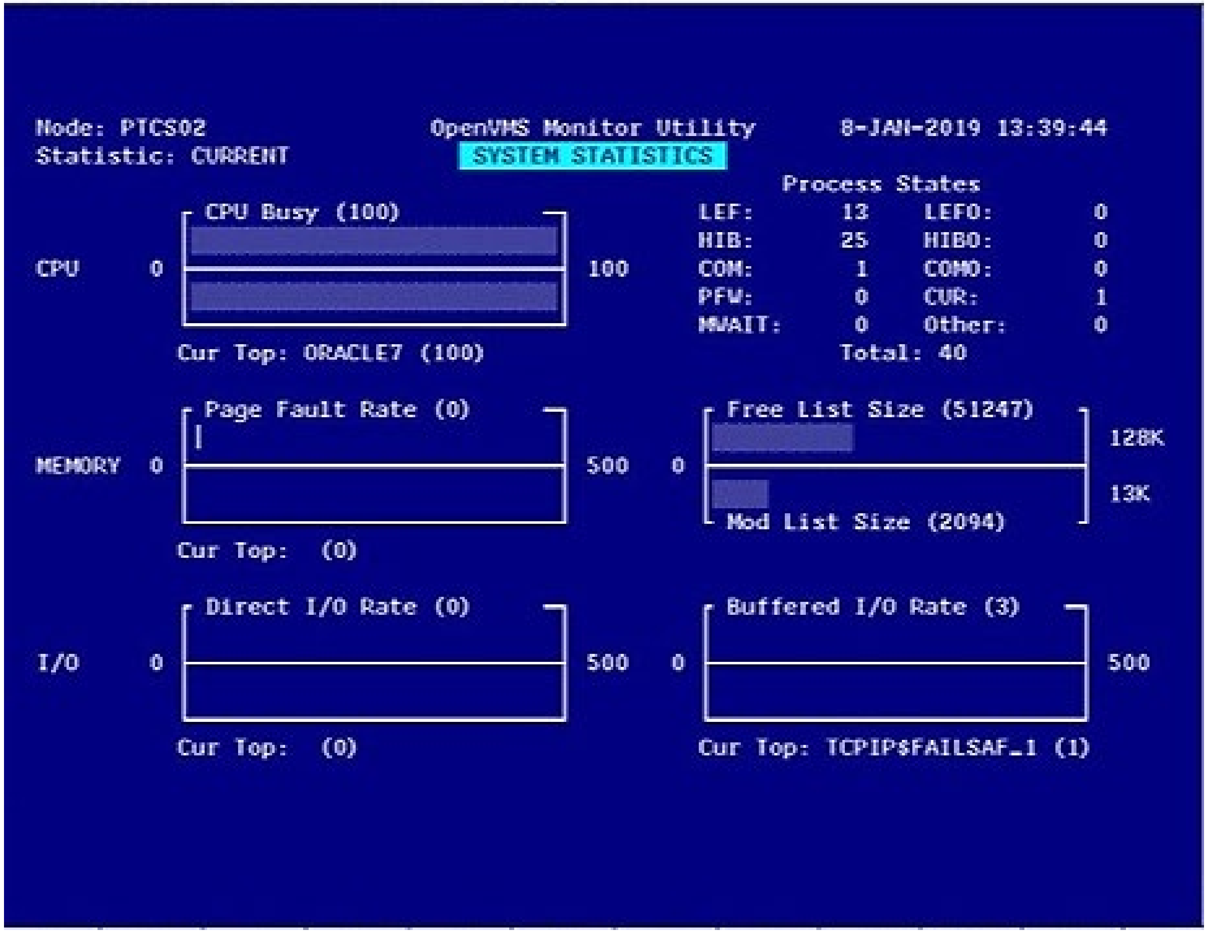
```
097/15:15:05.4   08A-975 ALRP+ WS: S86    PROTECTED ALARM/TEST ONLY
097/15:15:04.9   08A-974 DATA  WS: S86    DATA DROPOUT/TEST ONLY
097/15:15:04.4   08A-973 SYS   WS: S86    SYSTEM/TEST ONLY
097/15:15:03.9   08A-972 SPS   WS: S86    SPS/TEST ONLY
097/15:15:03.4   08A-971 OATS  WS: S86    OATS/TEST ONLY
097/15:15:02.9   08A-970 *R86  WS: S86    USER RESPONSE/TEST ONLY
097/15:15:02.4   08A-969 *I86  WS: S86    USER DIRECTIVE/TEST ONLY
097/15:15:01.9   08A-968 CFG   WS: S86    CONFIGURATION/TEST ONLY
097/15:15:01.4   08A-967 CMDC  WS: S86    COMMAND COMMENT/TEST ONLY
097/15:15:00.9   08A-966 CMDV  WS: S86    COMMAND VERIF/TEST ONLY
097/15:15:00.4   08A-965 CMDU  WS: S86    COMMAND UPLINK/TEST ONLY
097/15:14:59.9   08A-964 CMD   WS: S86    COMMAND/TEST ONLY
097/15:14:59.4   08A-963 TLM   WS: S86    TELEMETRY/TEST ONLY
097/15:14:58.9   08A-962 SC    WS: S86    S/C: 08A  SPACECRAFT/TEST ONLY
097/15:14:58.4   08A-961 ALR * WS: S86    ALARM/TEST ONLY
097/15:14:57.9   08A-960 ALL   WS: S86    TELL ALL/TEST ONLY
097/15:14:57.4   08A-975 ALRP+ WS: S86    PROTECTED ALARM/TEST ONLY
097/15:14:56.9   08A-974 DATA  WS: S86    DATA DROPOUT/TEST ONLY
097/15:14:56.4   08A-973 SYS   WS: S86    SYSTEM/TEST ONLY
```

USER: cmaloney
GW: SGWY03 (1)
TCS: STCS03
SC: 08A
MCRT:
CMD TCS:
2STEP:
CONFIG:

2004/097/15:14:57

Pre-EM Situational Awareness and Monitoring

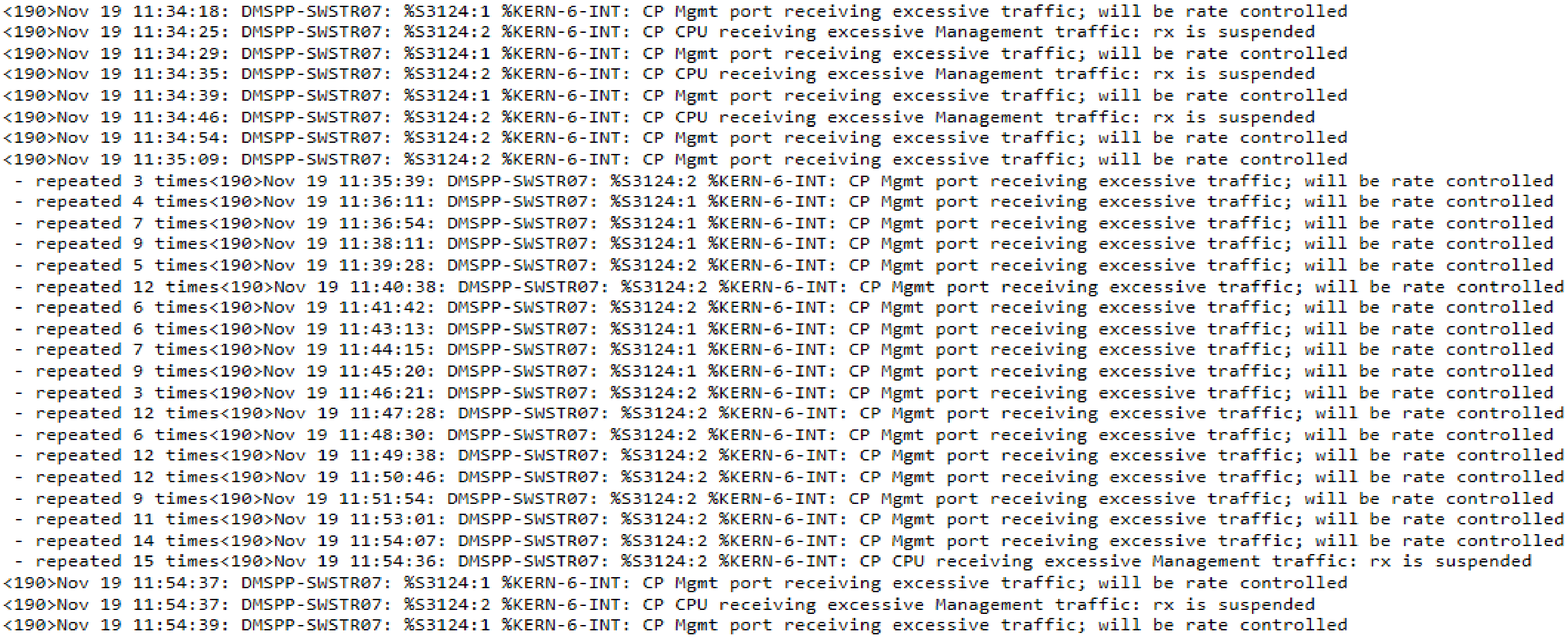
- **Antiquated monitoring utilities used on an individual machine basis**



```
Node: PTCS02                   OpenVMS Monitor Utility       8-JAN-2019 13:39:44
Statistic: CURRENT               SYSTEM STATISTICS
                                                          Process States
                 CPU Busy (100)                     LEF:       13    LEFO:        0
                                                    HIB:       25    HIBO:        0
CPU       0                                   100   COM:        1    COMO:        0
                                                    PFW:        0    CUR:         1
                                                    MWAIT:      0    Other:       0
                 Cur Top: ORACLE7 (100)                  Total: 40

                 Page Fault Rate (0)                  Free List Size (51247)
                                                                                  128K
MEMORY    0                                   500   0
                                                                                  13K
                                                      Mod List Size (2094)
                 Cur Top:  (0)

                 Direct I/O Rate (0)                  Buffered I/O Rate (3)

I/O       0                                   500   0                             500

                 Cur Top:  (0)                      Cur Top: TCPIP$FAILSAF_1 (1)
```

Pre-EM Situational Awareness and Monitoring

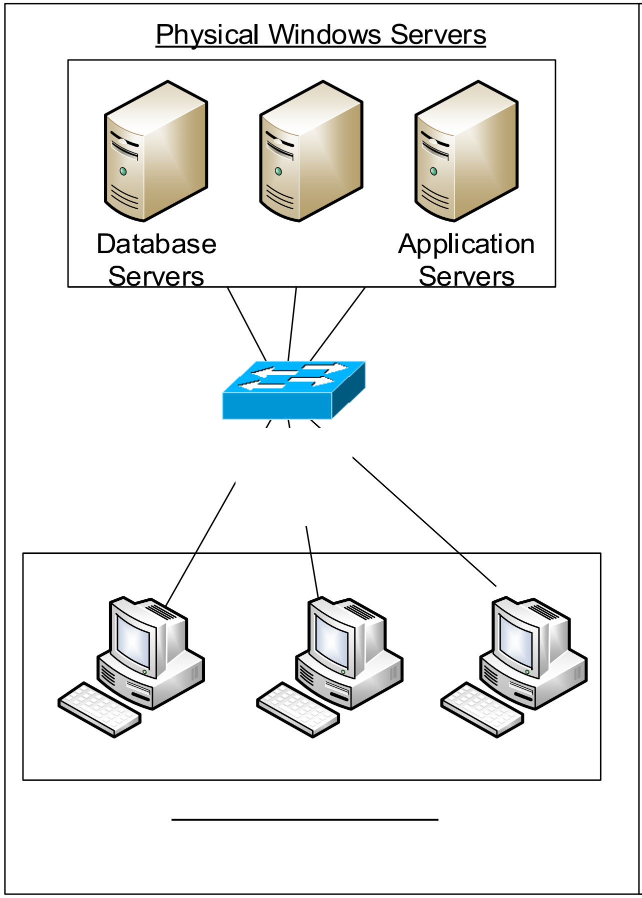
- **Manually viewing multiple log files on a per device basis**
- **Switch syslog:**



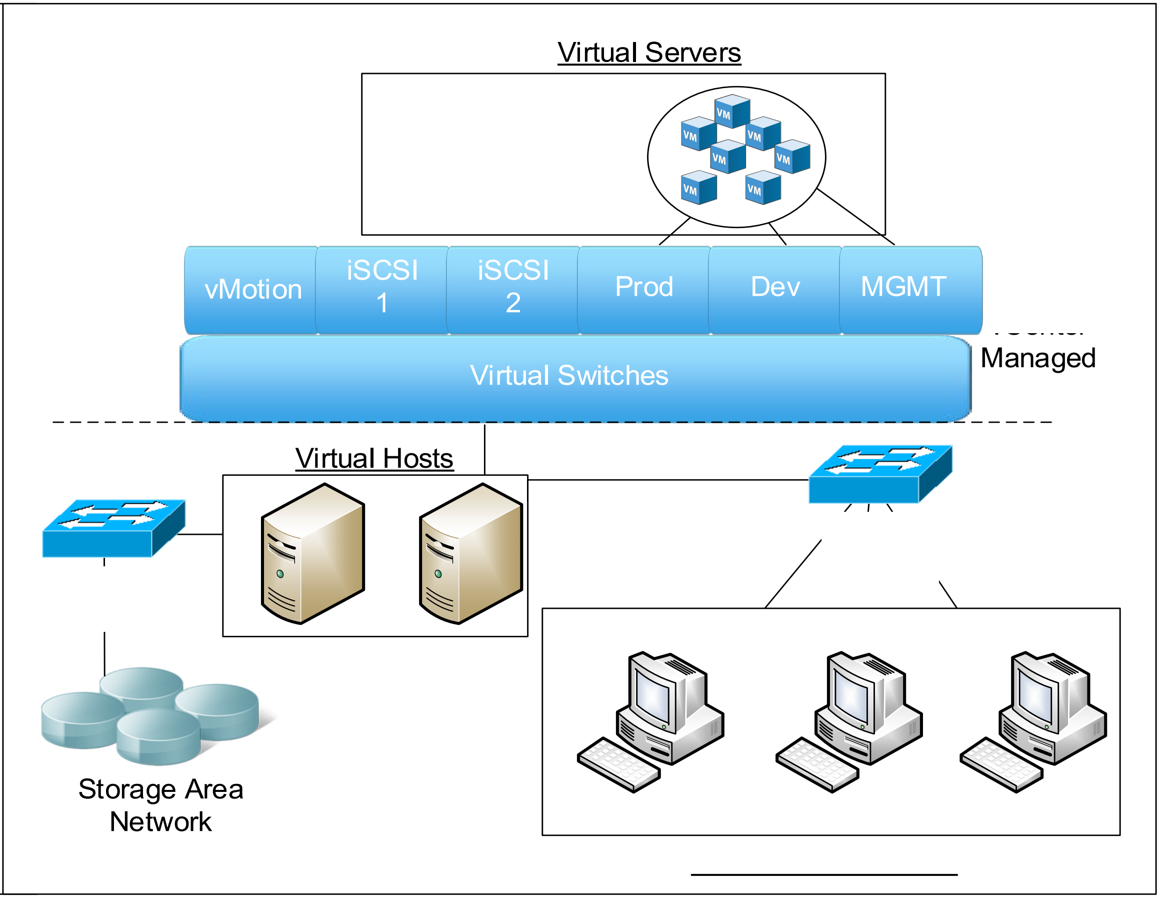
```
<190>Nov 19 11:34:18: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
<190>Nov 19 11:34:25: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP CPU receiving excessive Management traffic: rx is suspended
<190>Nov 19 11:34:29: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
<190>Nov 19 11:34:35: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP CPU receiving excessive Management traffic: rx is suspended
<190>Nov 19 11:34:39: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
<190>Nov 19 11:34:46: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP CPU receiving excessive Management traffic: rx is suspended
<190>Nov 19 11:34:54: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
<190>Nov 19 11:35:09: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 3 times<190>Nov 19 11:35:39: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 4 times<190>Nov 19 11:36:11: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 7 times<190>Nov 19 11:36:54: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 9 times<190>Nov 19 11:38:11: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 5 times<190>Nov 19 11:39:28: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 12 times<190>Nov 19 11:40:38: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 6 times<190>Nov 19 11:41:42: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 6 times<190>Nov 19 11:43:13: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 7 times<190>Nov 19 11:44:15: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 9 times<190>Nov 19 11:45:20: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 3 times<190>Nov 19 11:46:21: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 12 times<190>Nov 19 11:47:28: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 6 times<190>Nov 19 11:48:30: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 12 times<190>Nov 19 11:49:38: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 12 times<190>Nov 19 11:50:46: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 9 times<190>Nov 19 11:51:54: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 11 times<190>Nov 19 11:53:01: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 14 times<190>Nov 19 11:54:07: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
 - repeated 15 times<190>Nov 19 11:54:36: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP CPU receiving excessive Management traffic: rx is suspended
<190>Nov 19 11:54:37: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
<190>Nov 19 11:54:37: DMSPP-SWSTR07: %S3124:2 %KERN-6-INT: CP CPU receiving excessive Management traffic: rx is suspended
<190>Nov 19 11:54:39: DMSPP-SWSTR07: %S3124:1 %KERN-6-INT: CP Mgmt port receiving excessive traffic; will be rate controlled
```

MPSS Move to Modern Virtual Infrastructure

Old MPSS

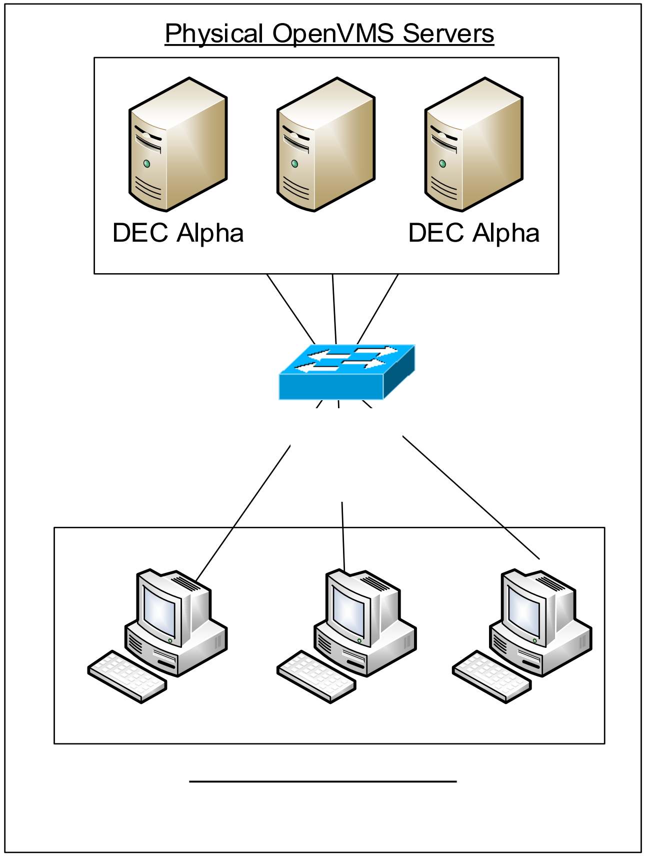


New MPSS

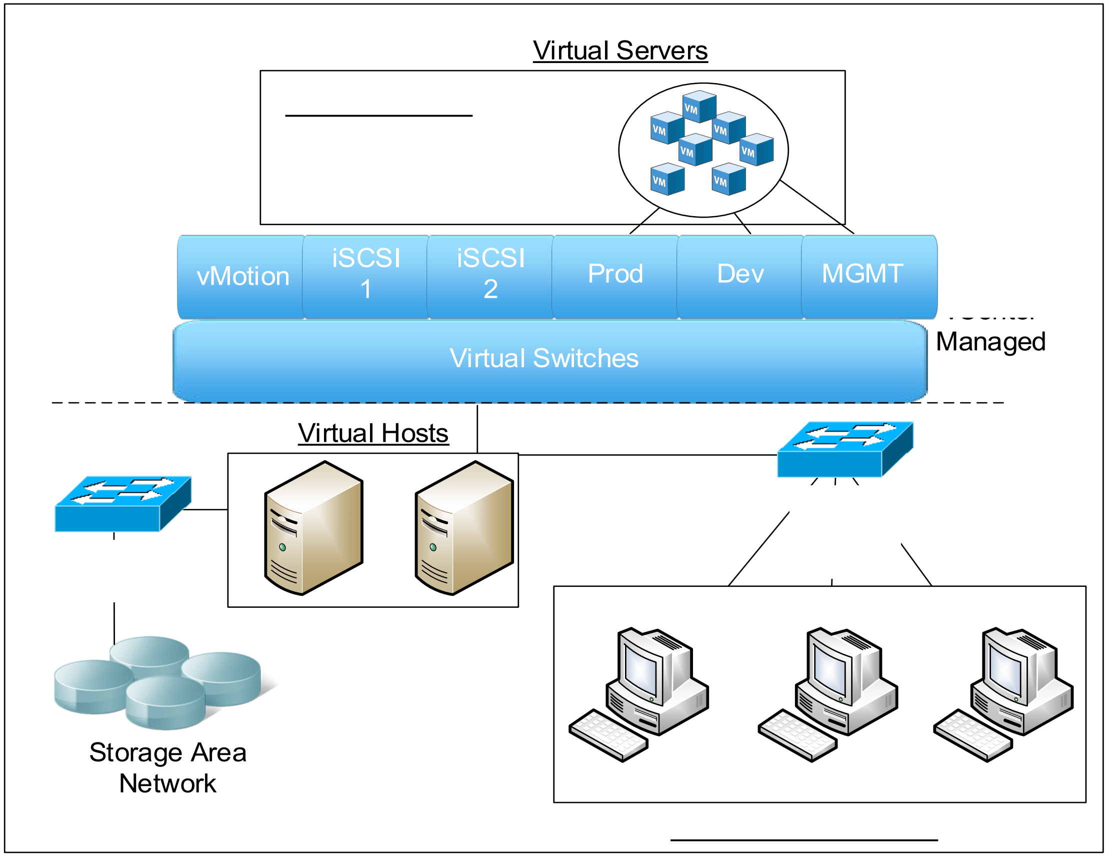


TCS Move to Modern Virtual Infrastructure

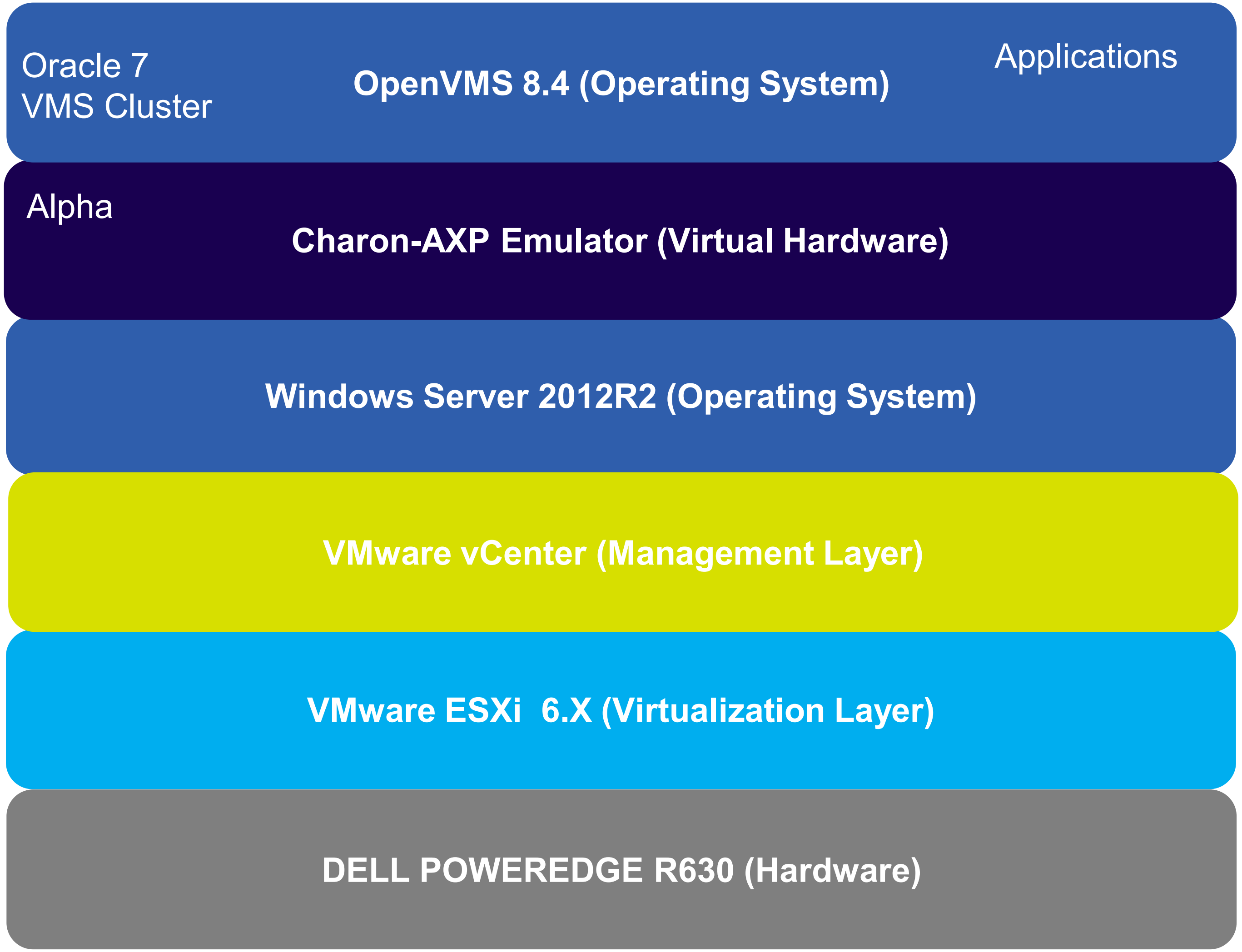
Old TCS



New TCS



TCS Layered Technology Stack



Oracle 7
VMS Cluster

OpenVMS 8.4 (Operating System)

Applications

Alpha

Charon-AXP Emulator (Virtual Hardware)

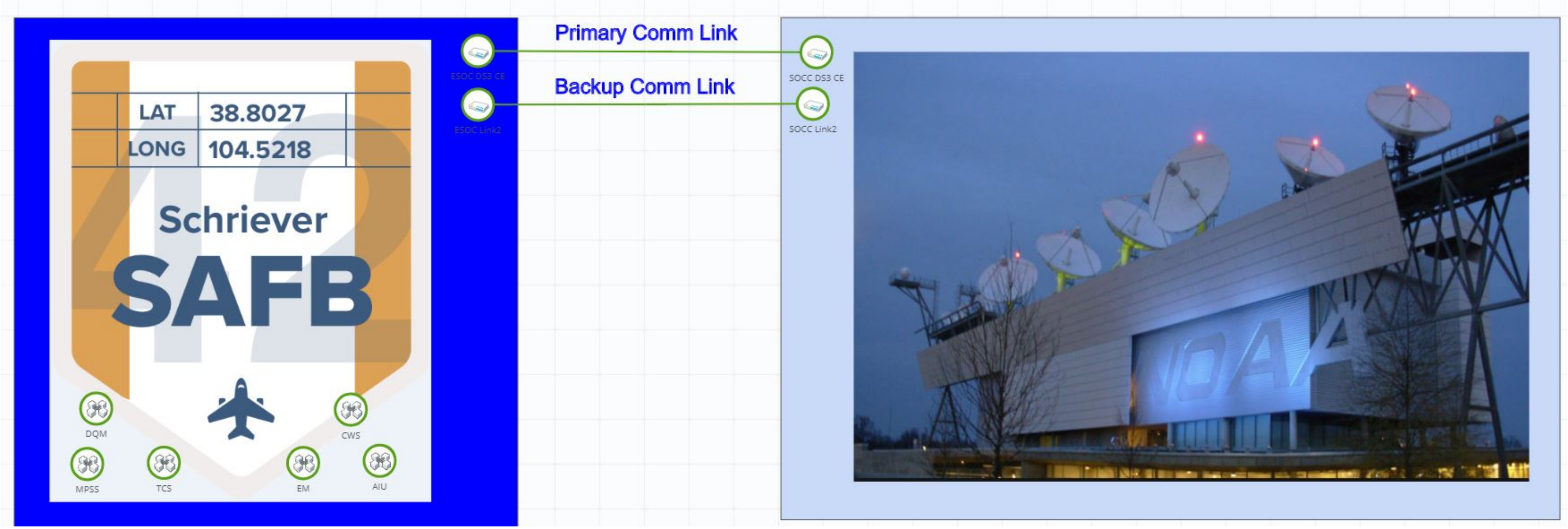
Windows Server 2012R2 (Operating System)

VMware vCenter (Management Layer)

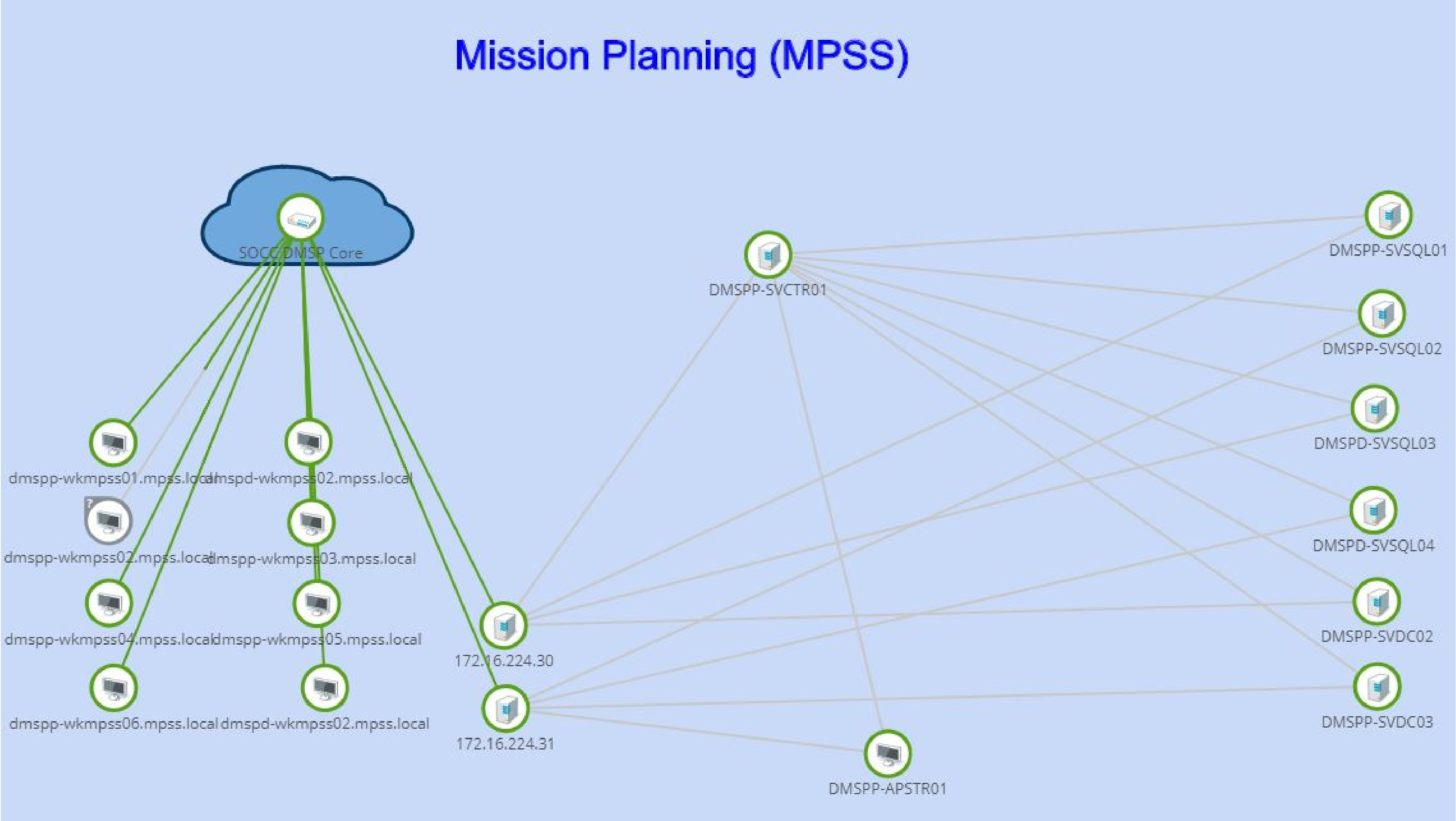
VMware ESXi 6.X (Virtualization Layer)

DELL POWEREDGE R630 (Hardware)

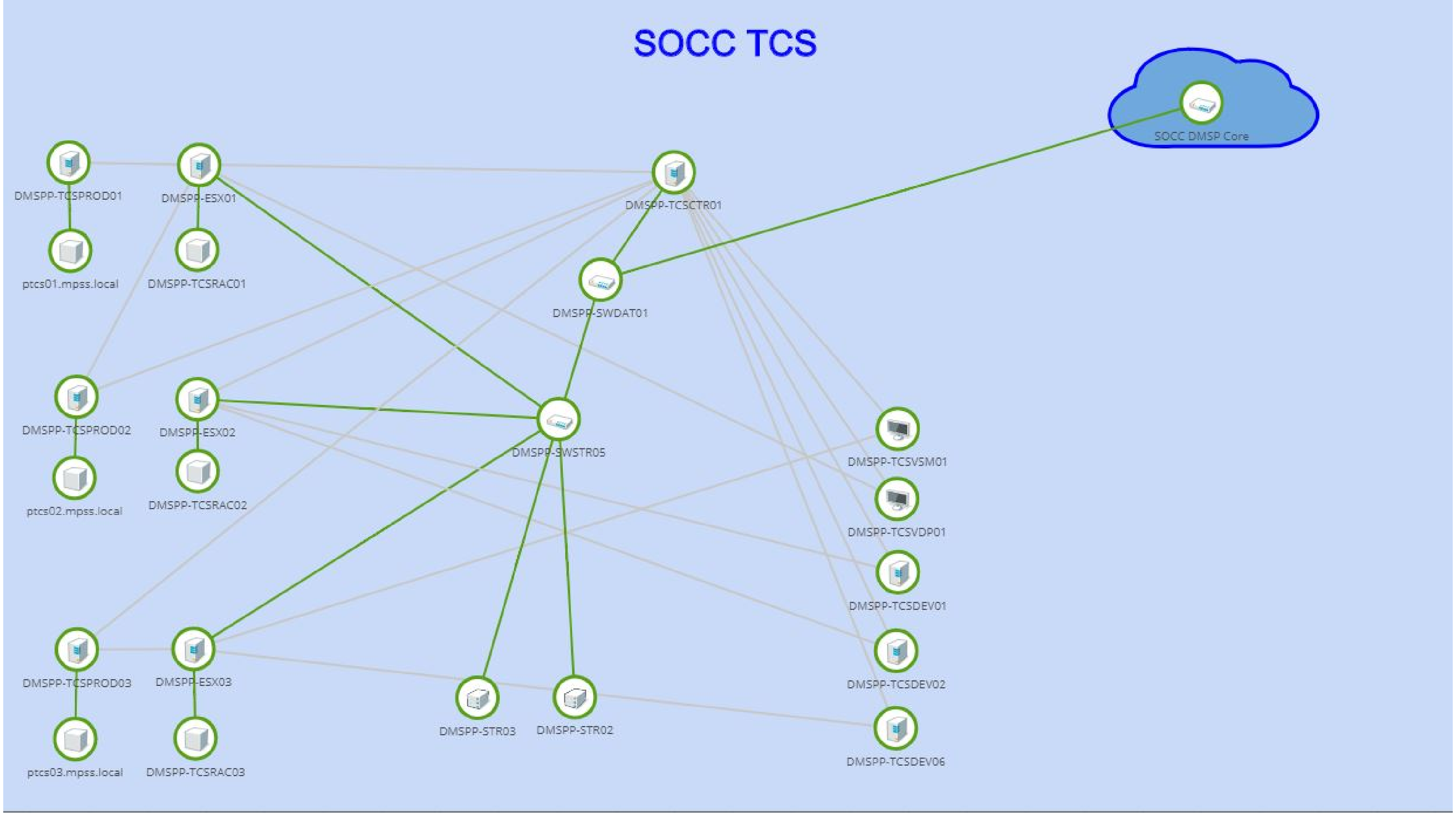
DMSP Operation Centers with Subsystems Top Level View



MPSS Subsystem Top Level View


Mission Planning (MPSS)
SOCC DMSP Core
DMSPP-SVCTR01
DMSPP-SVSQL01
DMSPP-SVSQL02
DMSPD-SVSQL03
DMSPD-SVSQL04
DMSPP-SVDC02
DMSPP-SVDC03
dmspp-wkmpss01.mpss.local
dmspd-wkmpss02.mpss.local
dmspp-wkmpss02.mpss.local
dmspp-wkmpss03.mpss.local
dmspp-wkmpss04.mpss.local
dmspp-wkmpss05.mpss.local
dmspp-wkmpss06.mpss.local
dmspd-wkmpss02.mpss.local
172.16.224.30
172.16.224.31
DMSPP-APSTR01

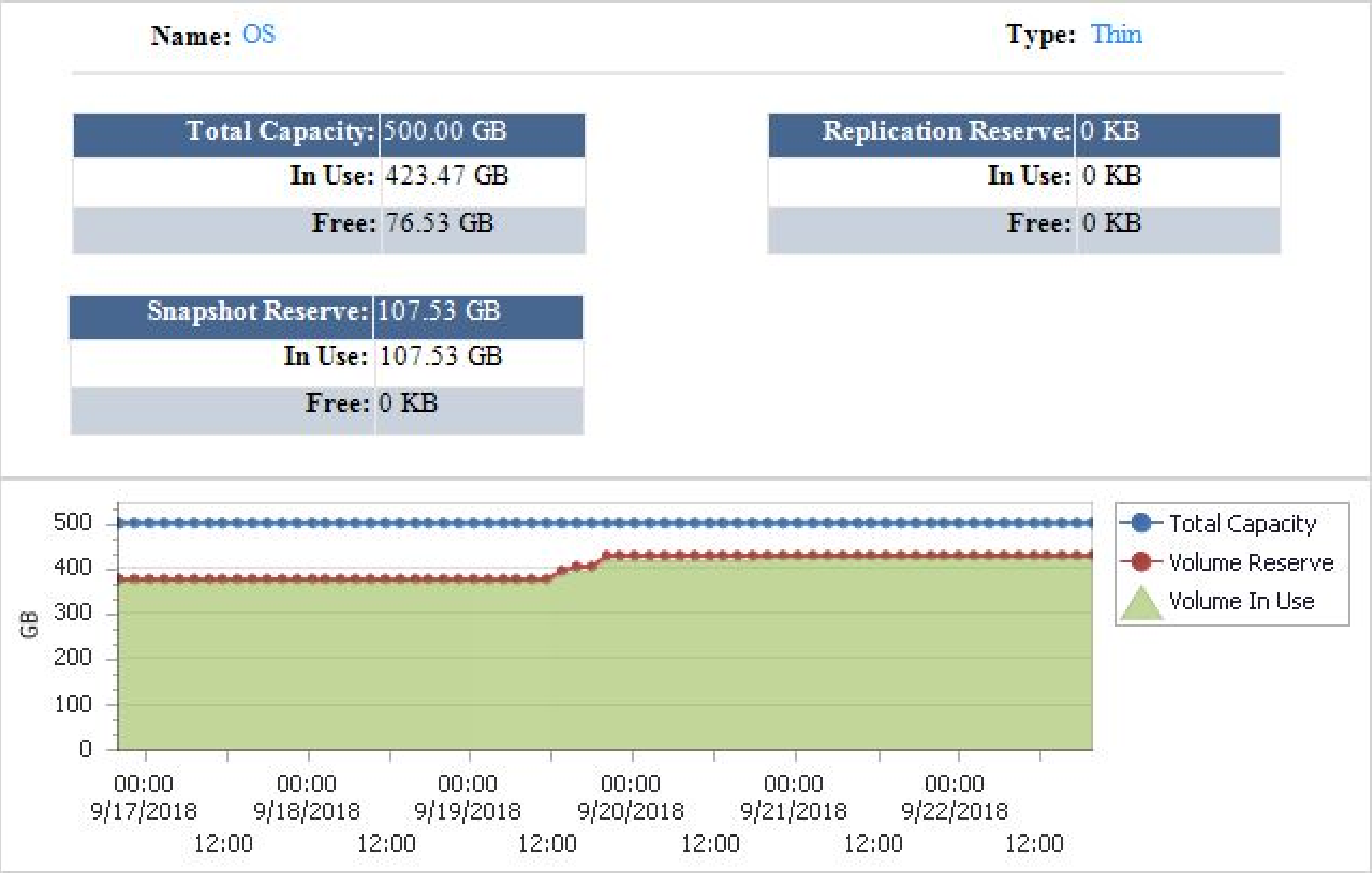
TCS Subsystem Top Level View



MPSS Storage Monitoring – Prevented Operational Outage

- **Summary**
  - EM showed MPSS Datastore/Storage Area Network (SAN) volume was approaching capacity
  - Engineers began planning for a configuration change to increase capacity
  - Before the change could be made, EM showed one MPSS management server went down
  - Engineers performed emergency change to increase capacity and restore the management server
  - No operational servers were affected

MPSS SAN Volume Approaching Capacity Limit



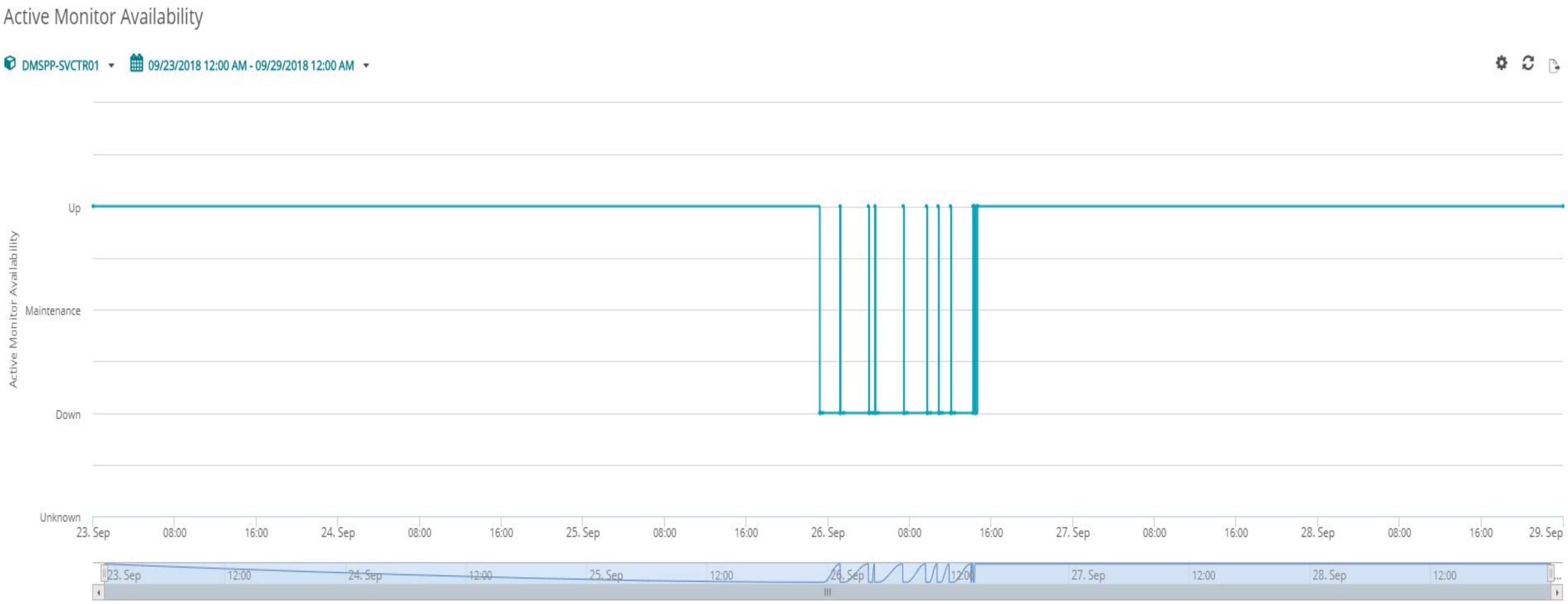
Name: OS **Type:** Thin

Total Capacity:	500.00 GB
In Use:	423.47 GB
Free:	76.53 GB

Replication Reserve:	0 KB
In Use:	0 KB
Free:	0 KB

Snapshot Reserve:	107.53 GB
In Use:	107.53 GB
Free:	0 KB

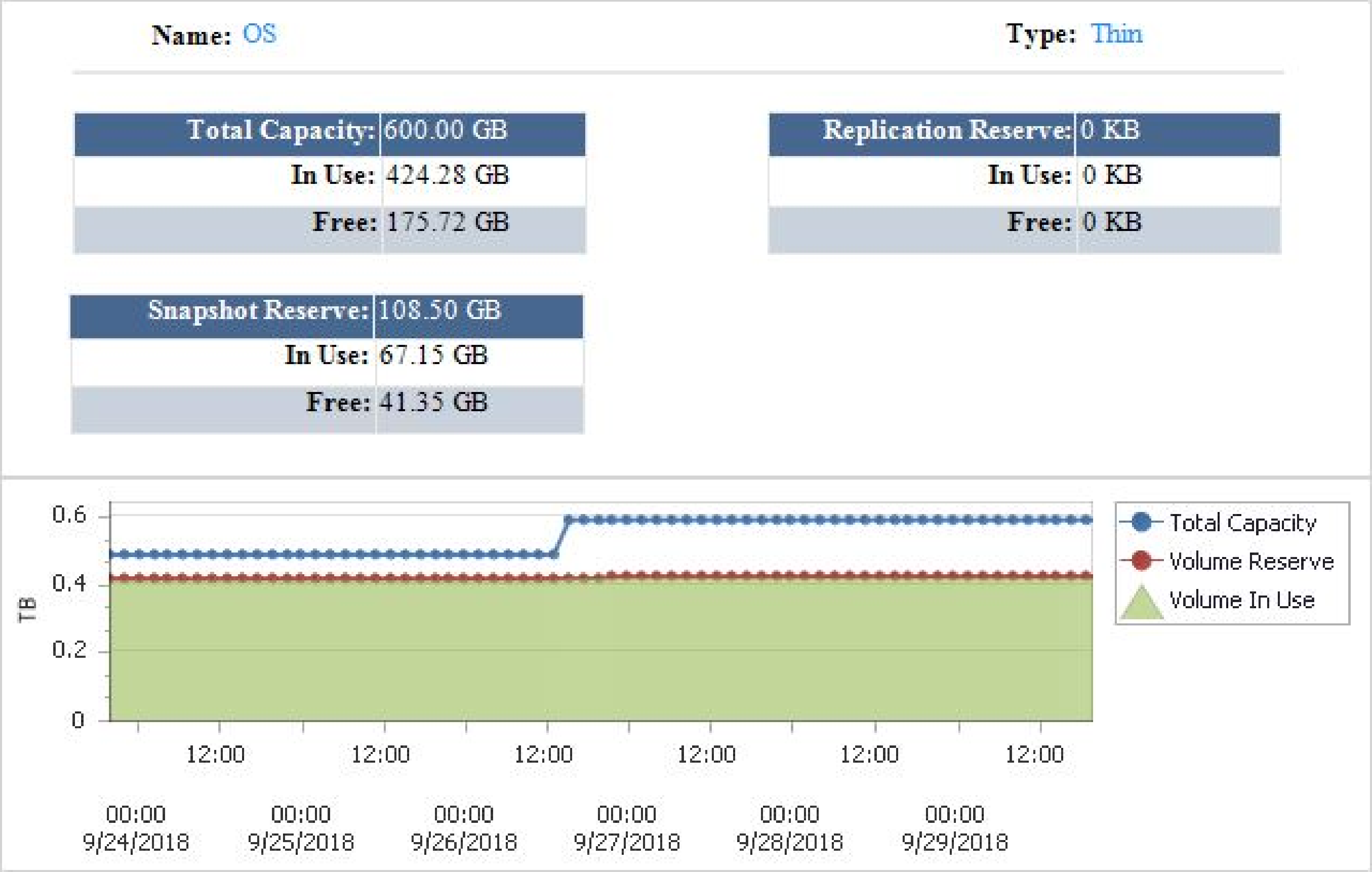
MPSS Management Server Down



Active Monitor Availability

DMSPP-SVCTR01 ▾ 09/23/2018 12:00 AM - 09/29/2018 12:00 AM ▾

MPSS SAN Volume Capacity Increased



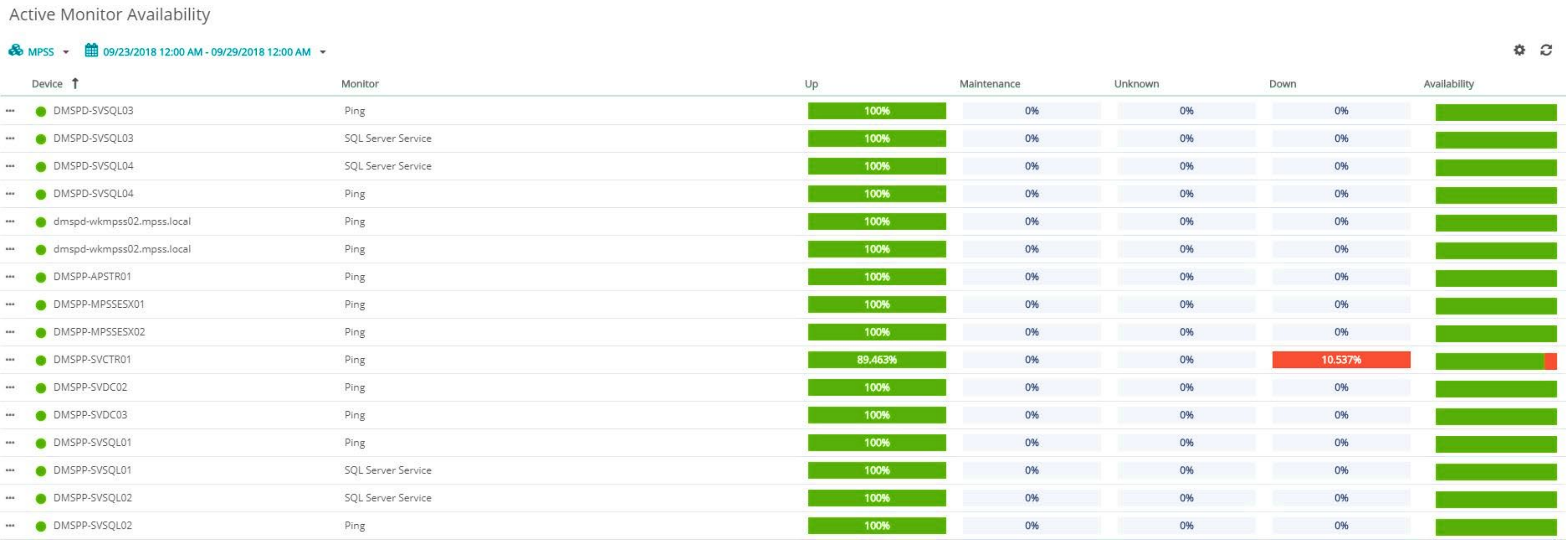
Name: OS **Type:** Thin

Total Capacity:	600.00 GB
In Use:	424.28 GB
Free:	175.72 GB

Replication Reserve:	0 KB
In Use:	0 KB
Free:	0 KB

Snapshot Reserve:	108.50 GB
In Use:	67.15 GB
Free:	41.35 GB

No Operational Servers Affected



Active Monitor Availability

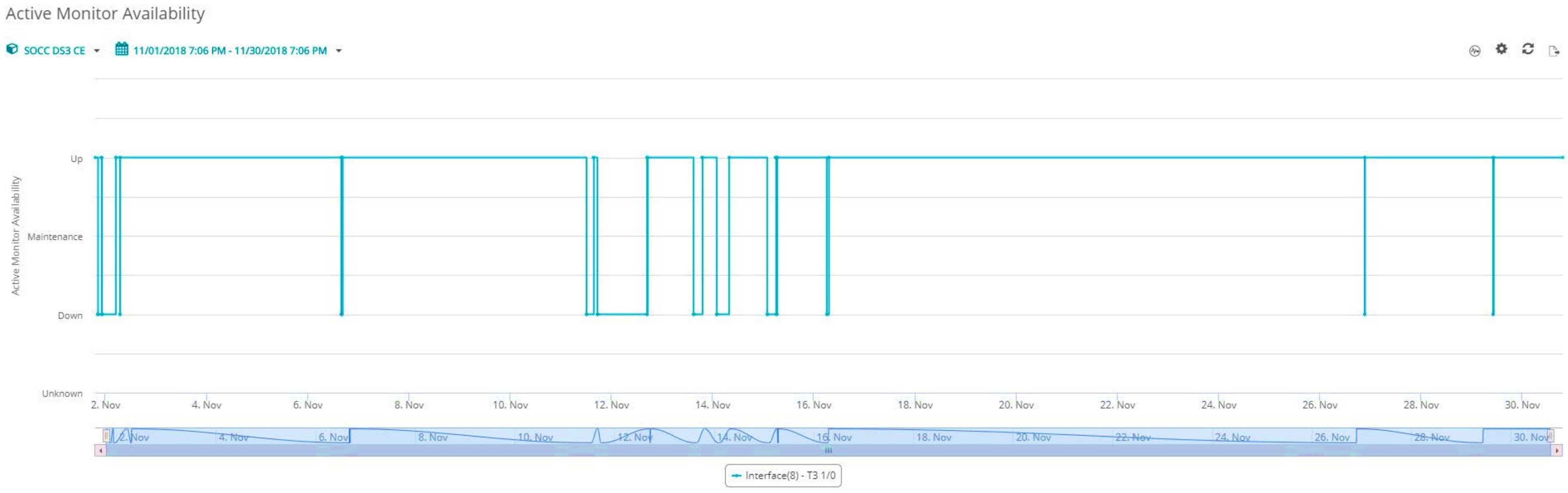
MPSS ▾ 09/23/2018 12:00 AM - 09/29/2018 12:00 AM ▾

Device ↑	Monitor	Up	Maintenance	Unknown	Down	Availability
● DMSPD-SVSQL03	Ping	100%	0%	0%	0%	🟩
● DMSPD-SVSQL03	SQL Server Service	100%	0%	0%	0%	🟩
● DMSPD-SVSQL04	SQL Server Service	100%	0%	0%	0%	🟩
● DMSPD-SVSQL04	Ping	100%	0%	0%	0%	🟩
● dmspd-wkmpss02.mpss.local	Ping	100%	0%	0%	0%	🟩
● dmspd-wkmpss02.mpss.local	Ping	100%	0%	0%	0%	🟩
● DMSPP-APSTR01	Ping	100%	0%	0%	0%	🟩
● DMSPP-MPSSESX01	Ping	100%	0%	0%	0%	🟩
● DMSPP-MPSSESX02	Ping	100%	0%	0%	0%	🟩
● DMSPP-SVCTR01	Ping	89.463%	0%	0%	10.537%	🟩🟥
● DMSPP-SVDC02	Ping	100%	0%	0%	0%	🟩
● DMSPP-SVDC03	Ping	100%	0%	0%	0%	🟩
● DMSPP-SVSQL01	Ping	100%	0%	0%	0%	🟩
● DMSPP-SVSQL01	SQL Server Service	100%	0%	0%	0%	🟩
● DMSPP-SVSQL02	SQL Server Service	100%	0%	0%	0%	🟩
● DMSPP-SVSQL02	Ping	100%	0%	0%	0%	🟩

Proactive Communications Network Monitoring

- **Summary**
  - EM showed multiple short duration down events on primary communications circuit between SOCs
  - Engineers informed Government comm representative
  - Ticket opened with Defense Information System Agency (DISA)
  - EM performance monitoring started showing a steady increase in errors on the line which triggered engineers to start planning for a failover to backup comm lines
  - Quick failover to backup comm once error rates were causing instability
  - EM allowed for proactive planning to occur and rapid failover to backup comm path

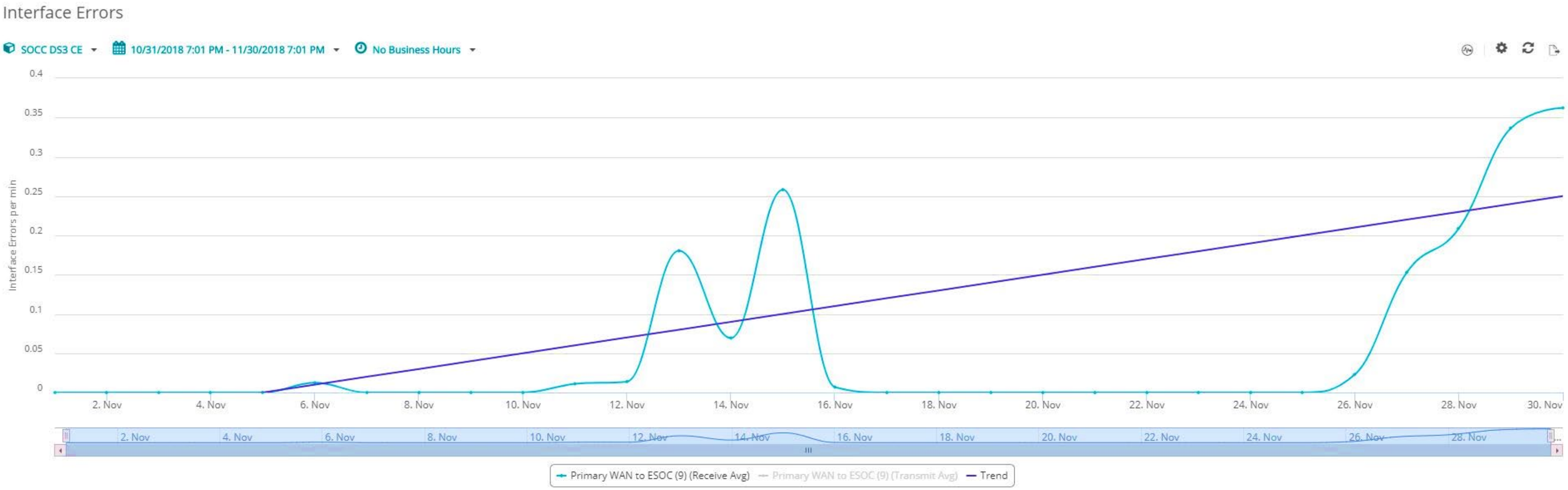
Primary Comm Circuit Outages



Active Monitor Availability

SOCC DS3 CE 11/01/2018 7:06 PM - 11/30/2018 7:06 PM

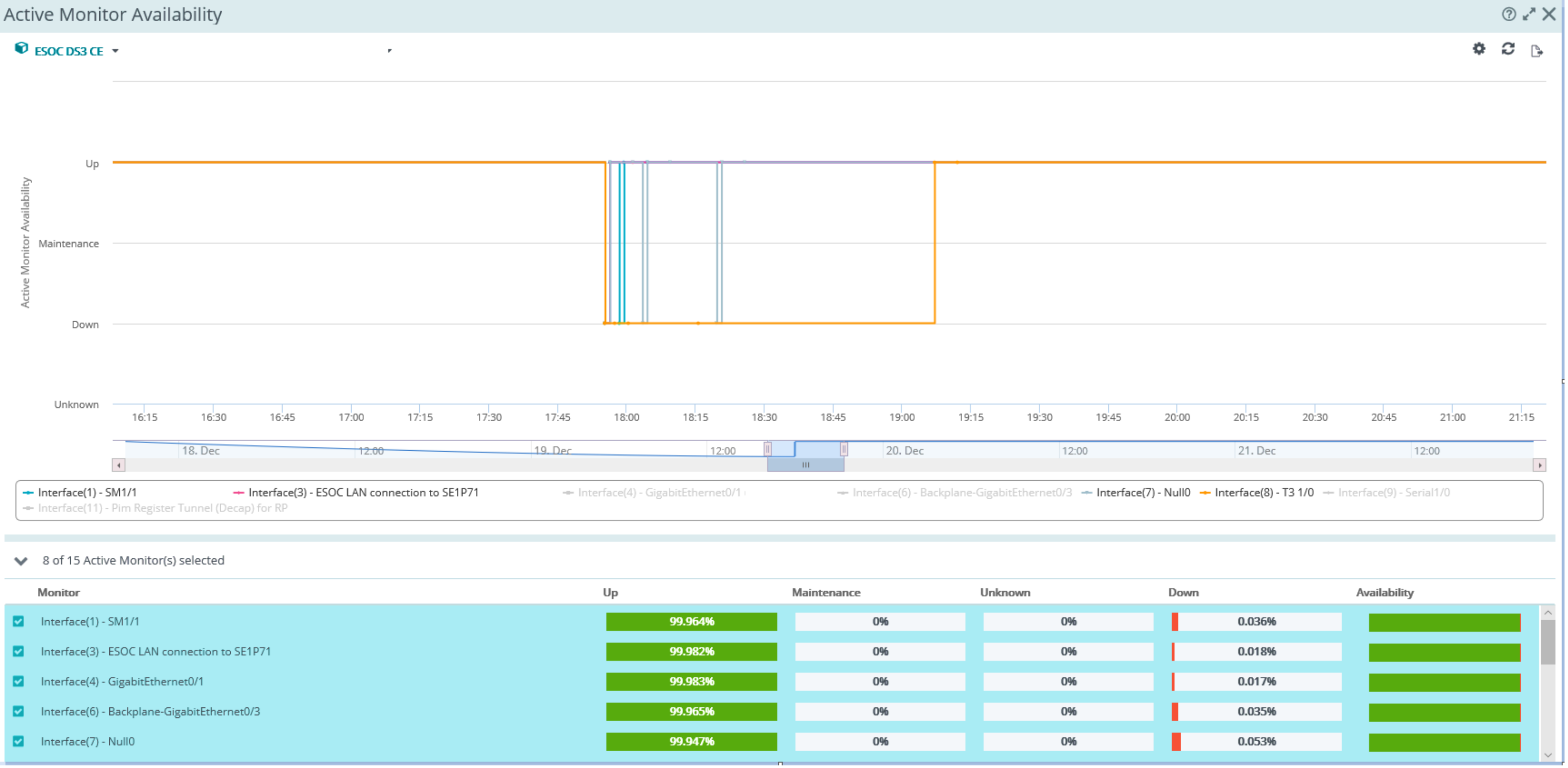
Primary Comm Errors – Trending Up



TCS Outage Analysis – Multiple System Metrics

- **Summary**
  - Engineering notified of TCS instability at primary SOC
  - Operations failed over to backup SOC due to slow or no response to their local TCS
  - EM reported multiple items of interest for this event
    - Primary comm between SOCs had been flapping up/down
    - Primary SOC OpenVMS TCS server (PTCS02) reported 100% CPU utilization
    - Virtual Host where PTCS02 was running reported CPU spikes to100%
  - Software engineers verified PTCS02 processes were trying to use all of their CPU resources causing the CPU spikes
  - Operations failed over to backup comm, restarted PTCS02 software and the system stabilized

Primary Comm Flapping Up/Down



Active Monitor Availability

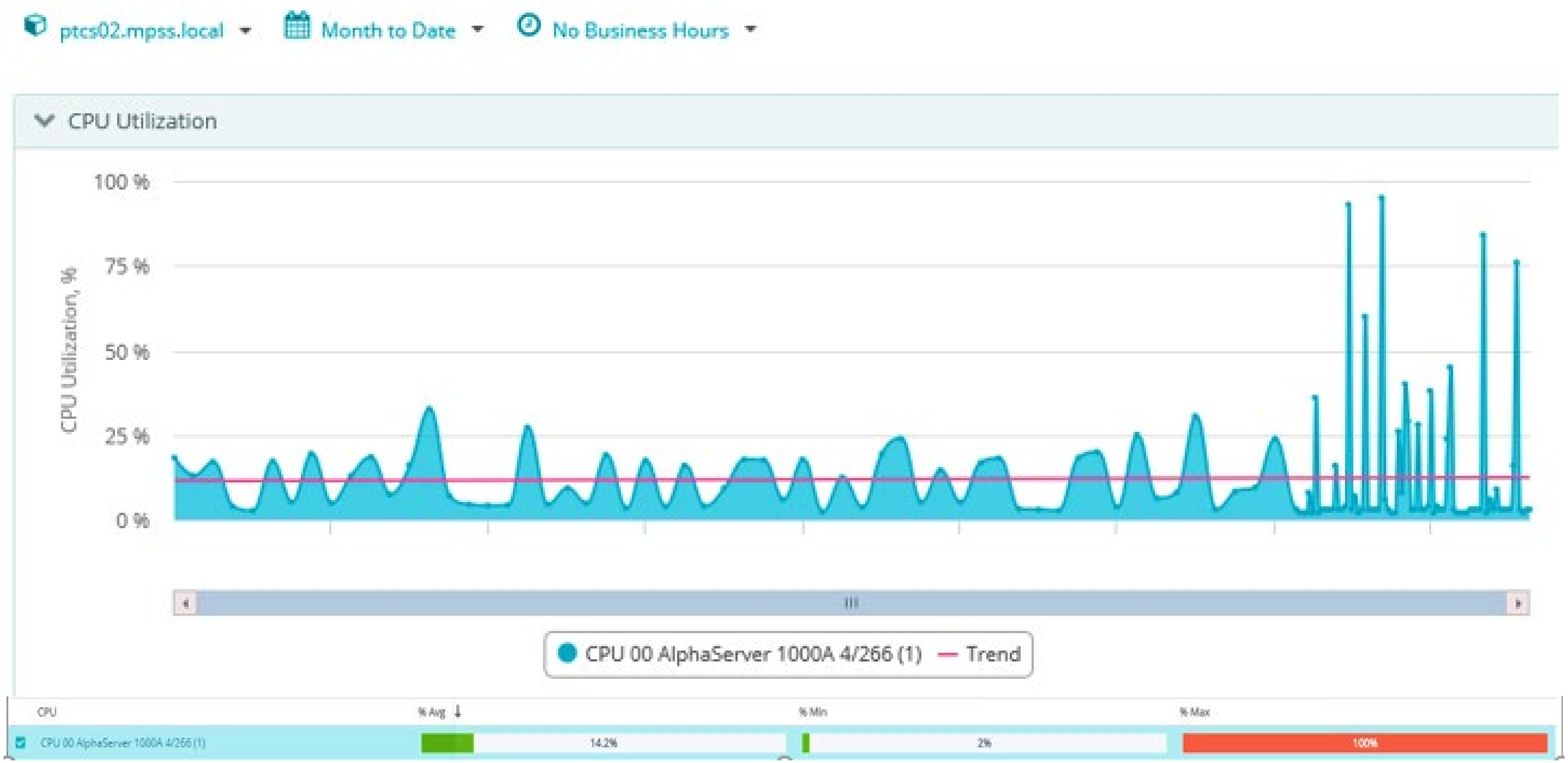
ESOC DS3 CE

- Interface(1) - SM1/1
- Interface(3) - ESOC LAN connection to SE1P71
- Interface(4) - GigabitEthernet0/1
- Interface(6) - Backplane-GigabitEthernet0/3
- Interface(7) - Null0
- Interface(8) - T3 1/0
- Interface(9) - Serial1/0
- Interface(11) - Pim Register Tunnel (Decap) for RP

8 of 15 Active Monitor(s) selected

	Monitor	Up	Maintenance	Unknown	Down	Availability
☑	Interface(1) - SM1/1	99.964%	0%	0%	0.036%	🟩
☑	Interface(3) - ESOC LAN connection to SE1P71	99.982%	0%	0%	0.018%	🟩
☑	Interface(4) - GigabitEthernet0/1	99.983%	0%	0%	0.017%	🟩
☑	Interface(6) - Backplane-GigabitEthernet0/3	99.965%	0%	0%	0.035%	🟩
☑	Interface(7) - Null0	99.947%	0%	0%	0.053%	🟩

TCS PTCS02 CPU Utilization

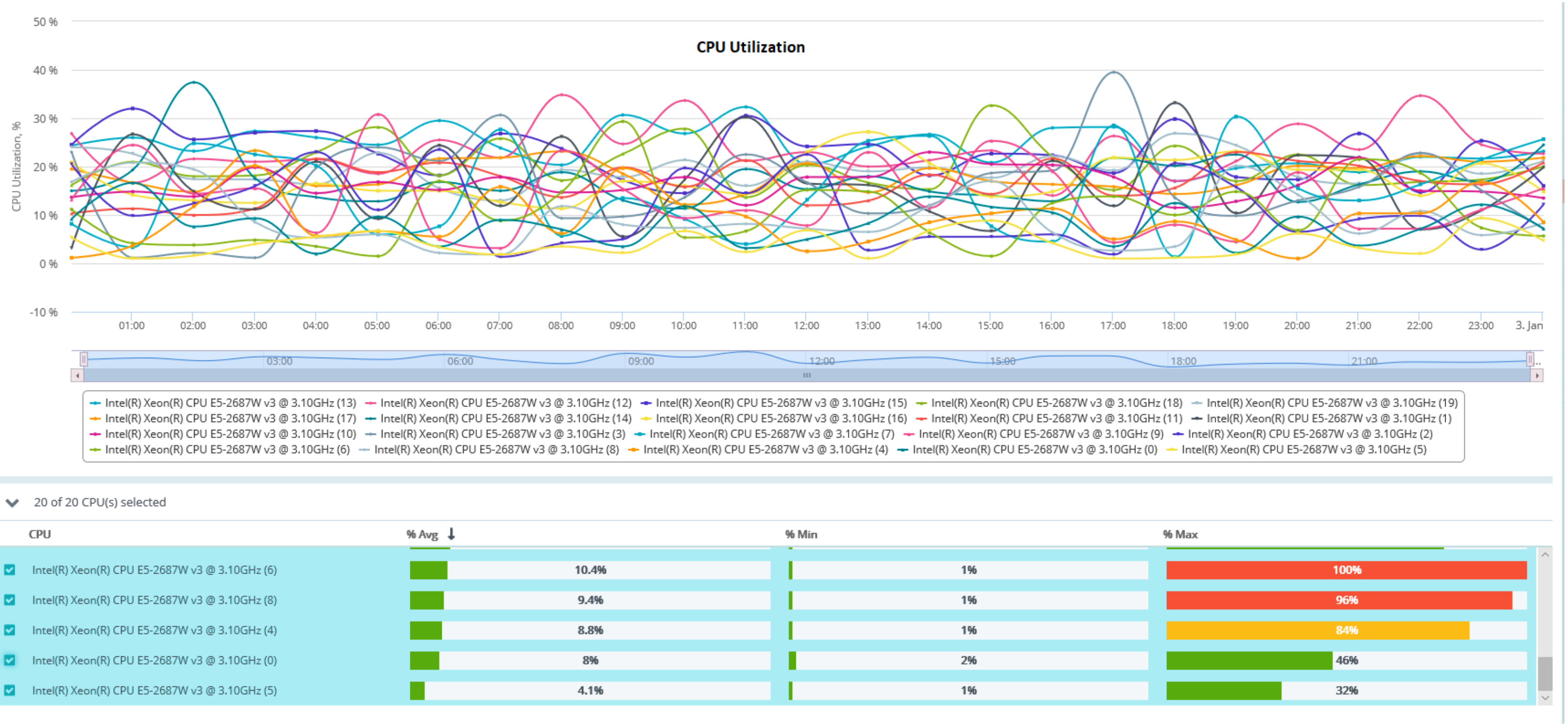


ptcs02.mpss.local ▾ Month to Date ▾ No Business Hours ▾

CPU Utilization

CPU	% Avg ↓	% Min	% Max
☑ CPU 00 AlphaServer 1000A 4/266 (1)	14.2%	2%	100%

TCS Virtual Host CPU Utilization


CPU Utilization
CPU Utilization, %
50 %
40 %
30 %
20 %
10 %
0 %
-10 %
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
3. Jan
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (13)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (12)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (15)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (18)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (19)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (17)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (14)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (16)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (11)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (1)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (10)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (3)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (7)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (9)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (2)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (6)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (8)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (4)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (0)
Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (5)

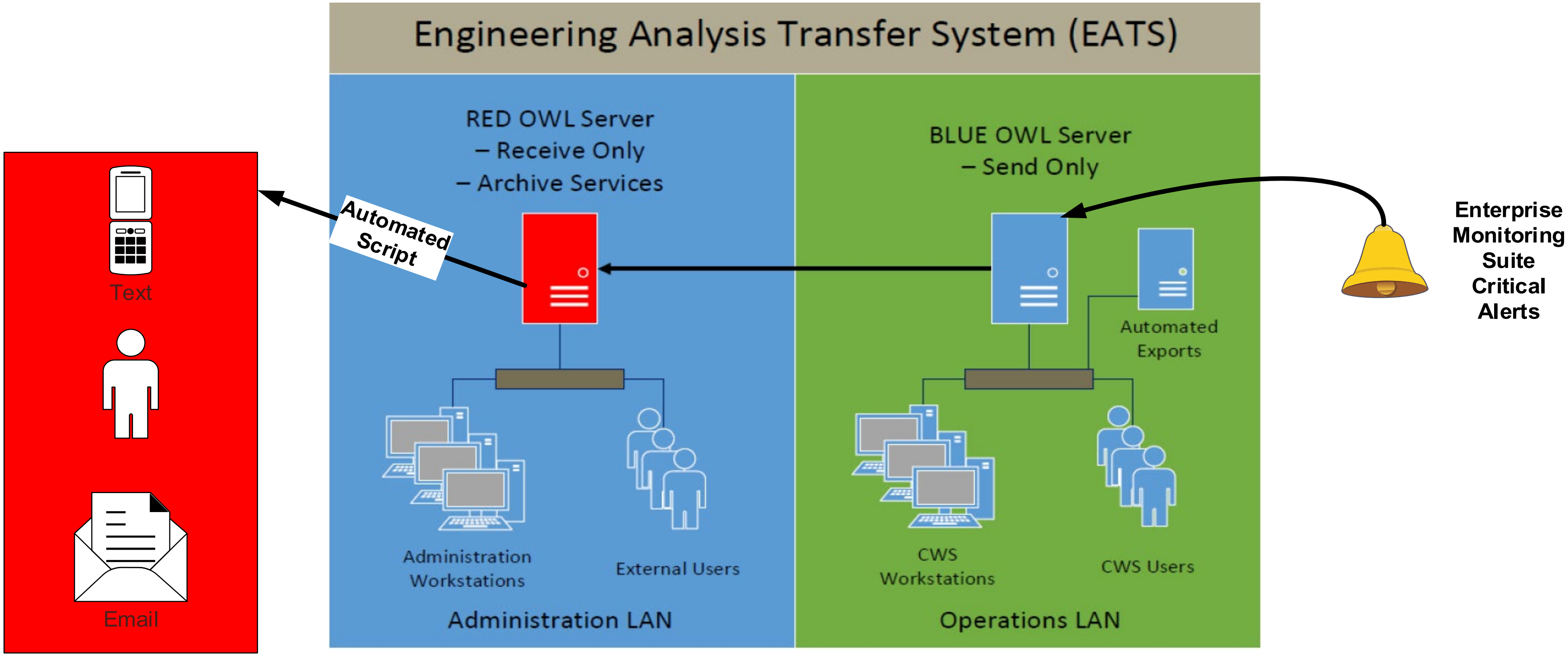
20 of 20 CPU(s) selected

	CPU	% Avg ↓	% Min	% Max
☑	Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (6)	10.4%	1%	100%
☑	Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (8)	9.4%	1%	96%
☑	Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (4)	8.8%	1%	84%
☑	Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (0)	8%	2%	46%
☑	Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (5)	4.1%	1%	32%

Future Enhancements Leveraging EM Capabilities

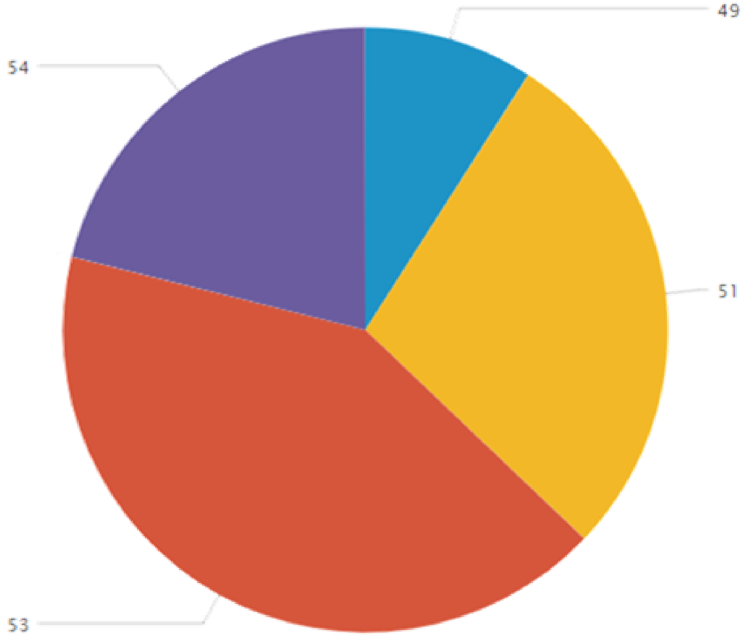
- **Alerts from an air-gapped system**
  - Utilize existing secure one-way gateways
  - Allow critical logs and alerts to be sent to engineers via text and/or email
- **Further consolidation and visualization of log data**
  - Streamline log analysis process
  - Consolidate any and all logs from DMSP systems
- **Expand traffic flow analysis**

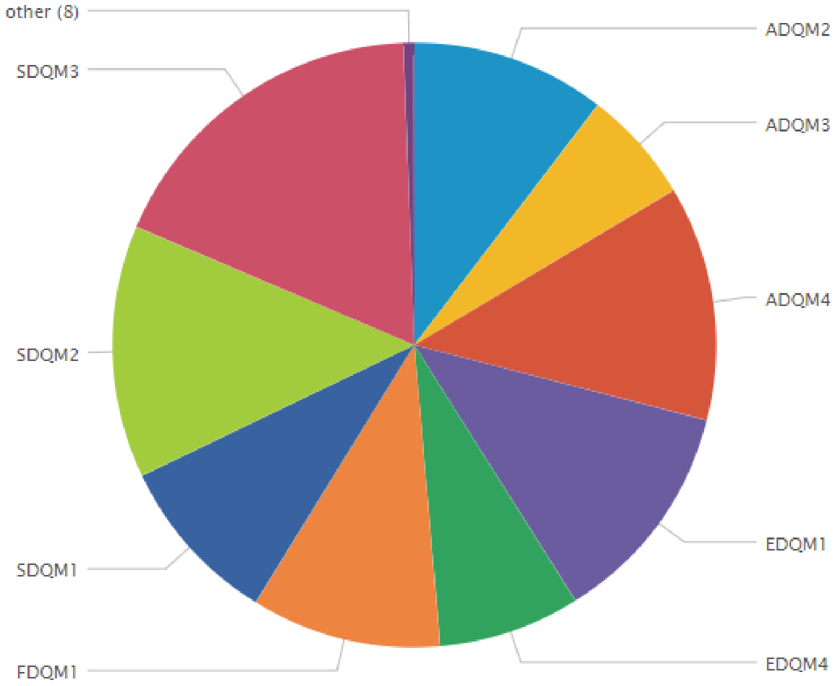
External Notifications from Air-gapped GS



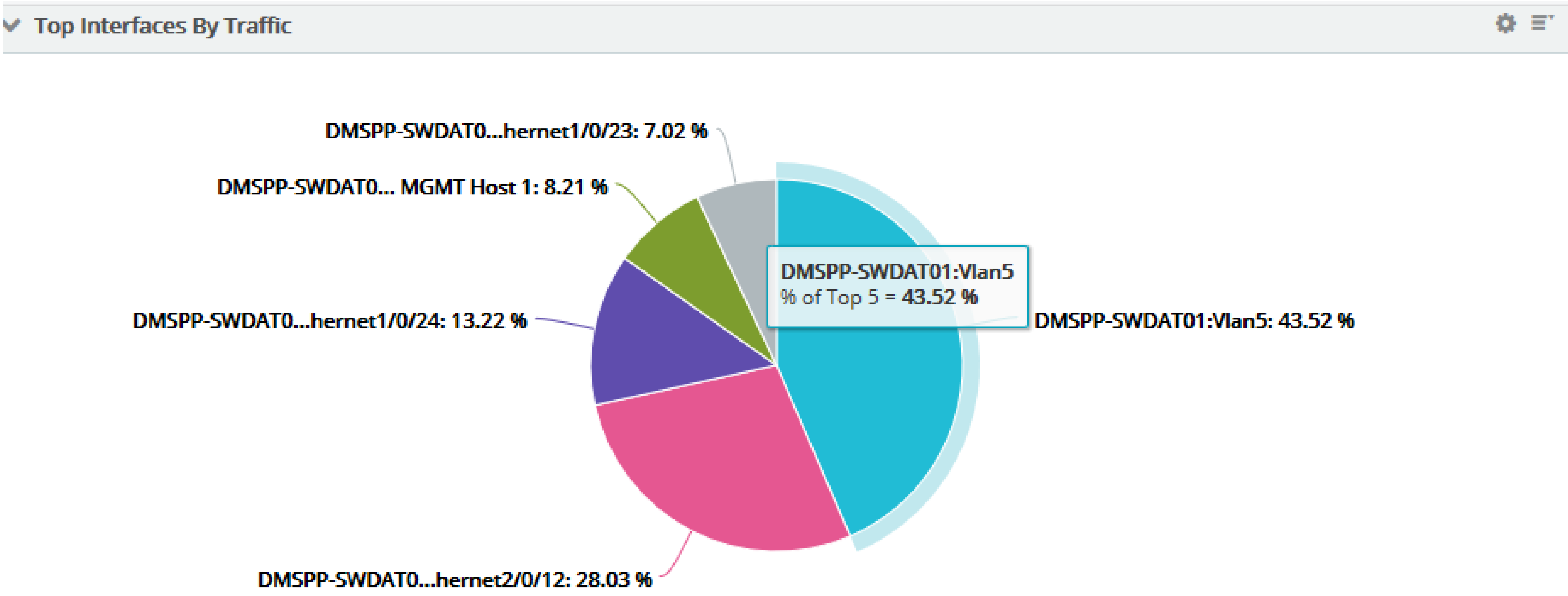
Further Consolidation and Visualization of Critical Logs

- **Data Quality Monitor (DQM) Logs – Error Counts by Spacecraft ID and DQM (weekly)**





Expand Traffic Flow Analysis


Top Interfaces By Traffic
DMSPP-SWDAT0...hernet1/0/23: 7.02 %
DMSPP-SWDAT0... MGMT Host 1: 8.21 %
DMSPP-SWDAT0...hernet1/0/24: 13.22 %
DMSPP-SWDAT0...hernet2/0/12: 28.03 %
DMSPP-SWDAT01:Vlan5: 43.52 %
DMSPP-SWDAT01:Vlan5
% of Top 5 = 43.52 %

Results

- **Adding EM Capabilities to the DMSP GS allows for proactive monitoring and maintenance and improved mission situational awareness**
  - Problem **isolation and resolution** has become much more efficient
  - Performance and utilization of **commercial off-the-shelf (COTS) solutions** can now be monitored to proactively fix issues before they become critical
  - EM capabilities are now in place to **expand further into the ground system** and provide a level of monitoring that has never been present
  - Both engineers and operators, contractor and Government, now have a **comprehensive dashboard to provide situational awareness** of the DMSP ground system