**Overview:**

This document is intended for use primarily by the IT Operations as a production support guideline for this weekend’s network RDC ACI and NetScaler cutover.

The document is broken out into 2 main parts, an inventory of critical applications to consider during this activity and examples from key dashboards. The listings call out certain things which will be key indicators of issues. It will also list remedial activities along with preventive activities.

This listing is by no means inclusive, it focuses on certain key critical which are more prone to err out in the event of a network interruption. And I’m sure this list will be second guessed by those who have never done prod support here.

The second part of the document focuses on what to look for in the monitoring dashboard for those applications. The dashboard for this weekend will cover only 1 or 2 KPIs be application and will focus primarily on some basic predictive algorithms to look for deviations from expected norms.

As a member of the Operations team you should have sufficient familiarity with operational norms to bring value to this activity and recognize possible issues beyond the key systems listed here.

Note: If there are serious issues we will be without access to core tools like Splunk, Extrahop or SCOM. At this point just assume things are really bad.

Critical Apps/Systems to Evaluate:

* **Splunk**

1. Remediation:
2. Put cluster into maintenance mode
3. Restart Forwarder
4. Considerations:
5. Search Peers will not be able to communicate
6. Forwarders may stop reporting

* **Commvault**:

1. Remediations:
2. Suspend Jobs
3. Considerations:

* **SCOM:**

1. Remediations:
2. Restart Server/Services
3. Considerations:
4. Email alerts will not be delivered

* **BizTalk/Foresight/MQ Series**

1. Remediation:
2. Shutdown Host Instances
3. Weekly Reset of MP-BTS-SS01/SS02
4. Restart GlassFish Instances
5. Restart Foresight Workflows
6. Files not being consumed by BizTalk/Foresight
7. MQ Channels are largely self-healing

B) Considerations:

1) SQL Connectivity

2) Suspended Service Instances

3) CIFS

* **Web Tier**

1. Remediation:
2. Reset IIS on “WAS”, “WSS”, “SCR” servers
3. Considerations:
4. ASP.NET errors
5. API errors
6. HTTP 404/5XX errors
7. Response Times

* **Active Batch**

1. Remediation:
2. If necessary, restart cluster and verify state of scheduler
3. If necessary, Restart individual work queues
4. Considerations:
5. Error Rates (typical ABAT error rate is less than 0.05 percent
6. Alerts on cluster/scheduler status

* **Image Retriever**

1. Remediation:
2. Application stack reset via Vcenter
3. Considerations:
4. Error Rate from IR application logs
5. Response Times
6. IIS Error Rates
7. HTTP 503 errors will not be captured in IIS or in the application logs

* **IVR**

1. Remediation:
2. Tomcat Resets on the LP-IVR-W01 and W02 Servers
3. Possible full stack reset of IVR and MPP servers
4. Considerations:
5. DB Call failures (these a errors invoking external resouces)
6. Call Durations

* **Sterling Integrator (SI)**

1. Remediation:
2. Restart node(s) in a manner consistent with normal operating procedures
3. Considerations:
4. Stalled files
5. Error Rate in file transfer activity
6. Evaluate inbound file ingestion rates based on expected values

* **Vital/HMS**

1. Remediation:
2. Restart Tomcat web servers
3. Restart Cincom
4. Repair Active MQ
5. Considerations:
6. Overnight conventional refresh will fail
7. Web services has heavy DB dependency on MP-HMS-MD01N01
8. Vital Timer
9. Vital Image Retriever Integration

* **Elastic Search**

1. Remediation:
2. Reset failed nodes (contact John Craig or myself for this)
3. Considerations:
4. Cluster/Node Failure

* **CSS**

1. Remediation:
2. Not Applicable
3. Considerations:
4. CSS is not an enterprise application in the conventional sense, it is a desktop application which collects “responses” from multiple enterprise applications
5. We will be tracking errors by count and type to assess broader health status

* **Pinnacle/Dire**

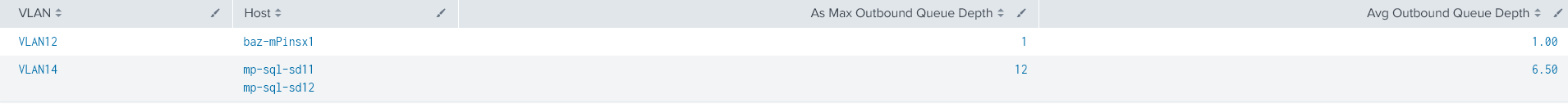
1. Remediation
2. Server and services restart consistent with existing Ops documentation
3. Considerations:
4. Pinnacle and Dire have significant DB dependencies and will be susceptible to failures after a network interruption
5. Pinnacle and Dire activities are often “internally scheduled”, meaning that errors may not show up immediately and may be expressed as some failed activity at a later time
6. Both applications have specific alerts

Dashboards:

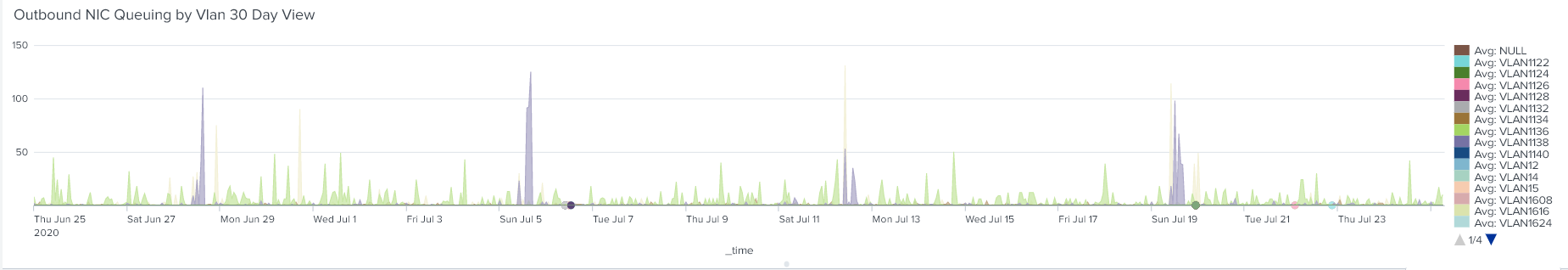
**Primary Overview Dashboard**

* This is a high level “all inclusive” dashboard tracking representative applications at highlevel based on those more obvious indicators of system issues
* The dashboard is also pulling network stats from all servers and looking general indicators of network health – e.g. NIC queuing and discard rate. These metrics are evaluated at the VLAN level to serve as a general indicator of network issues.
* Link: <http://splunkops.azblue.com/en-US/app/bcbsaz_ta_app_ops/overview__v1>
* Network Stat Panels

1. NIC queueing by VLAN ( It’s not uncommon for SQL servers to experience NIC queueing



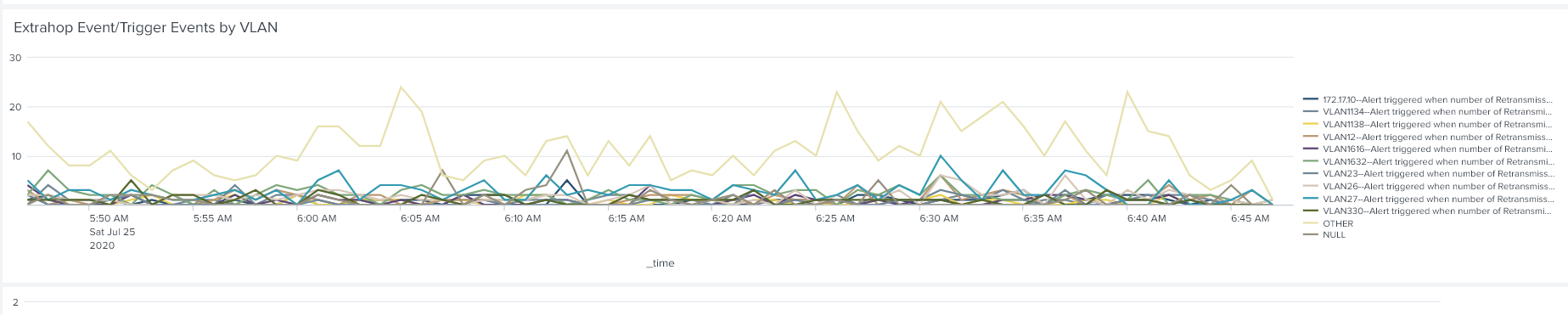
1. Historical Norms for NIC Queuing by day/hour



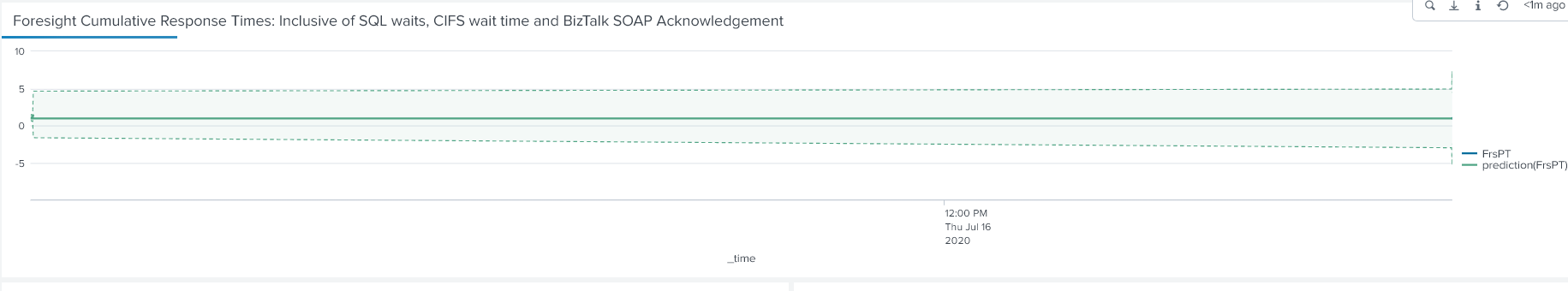
1. Trellised View of NIC discard rate aggregated by VLAN



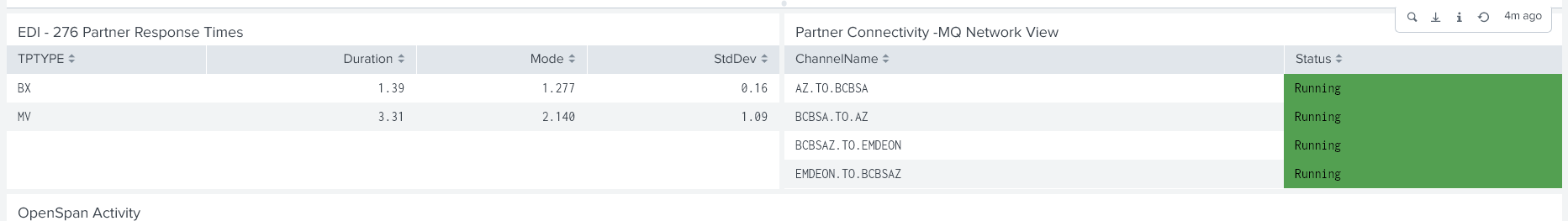
1. Summary Data from Extrahop Tracking Error Triggers by VLAN



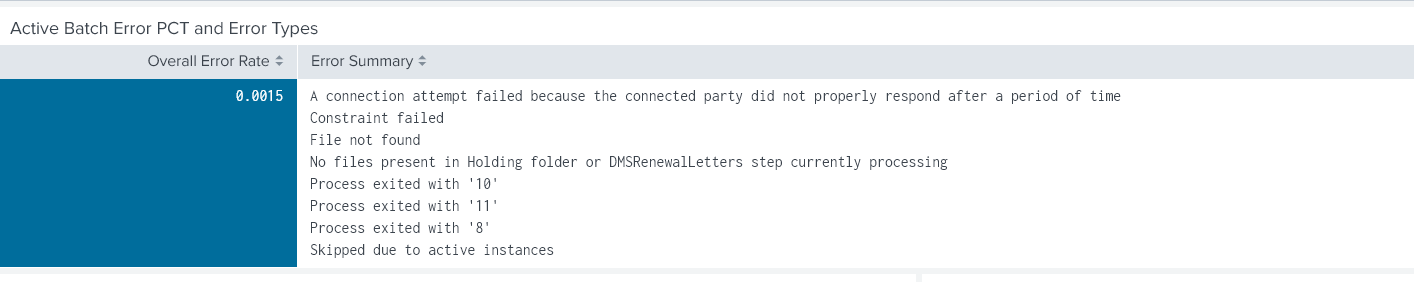
1. Foresight Web Workflow timings. This a “predictive view” and assess current timing against historical norms based on day and time – This metric will capture overall processing time as a function of:
2. SQL activity
3. CIFS activity
4. SOAP/WEB response times
5. This metric will cover a number of broad metrics to assess the state of the network
6. For deeper BizTalk and Workflow activity use ( <http://splunkops.azblue.com/en-US/app/bcbsaz_ta_app_5010/5010_biztalk_general_wellbeing> and <http://splunkops.azblue.com/en-US/app/bcbsaz_ta_app_5010/5010_BTS_FRS_Dir>)



1. Internal/External Partner Response Timings
2. This evaluates our ability to connect to BX and DXC, and tracks response times
3. Due to the nature of the 276 timings and multiple internal dependencies to generate response it serves a broader indicator of system and network functions.



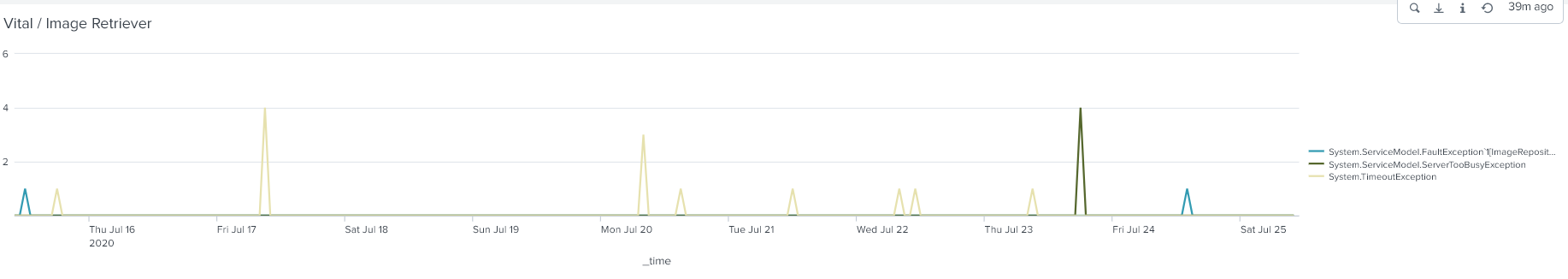
1. Active Batch – The focus is on captured errors at the platform level. Note that most jobs in ABAT have weak exception handling. The other focus is “cluster” state. In a network outage the ABAT environment may not be able to successful designate a master scheduler
2. This panel will color code error percentage. Any error percentage over 1 represents a significant deviation from the norm.
3. For connection failed errors in the “Error Summary Section”

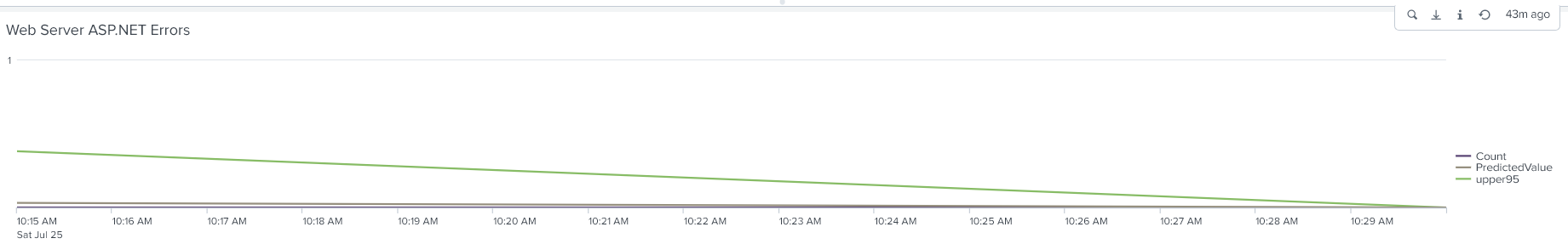


1. Sterling - The key focus for Sterling is “Bytes Transferred” per hour. This is another predictive view, using historical values to anticipate current values based on a seasonal algorithm. Error rates are also tracked an color coded.
2. If the current traffic is significantly below the expected lower boundary value this may suggest connectivity issues at the front door
3. The error rate for Sterling is, under normal conditions, between 0.05 and 0.78. If this values goes above 1% it’s cause for concern.
4. Elastic Search - A component of the largely undocumented Velocity connect solution. This is a cluster environment and the main thing to look at it failures in internal communication.
5. The cluster will function with failed nodes, but this should be seen another barometer of network and infrastructure health



1. Vital – Vital in the overview dashboard is represented by the state/ability to integrate with Image retriever. This is a specific metric which can be seen a broader indicator of system health.
2. This will track timeouts and general failures (HTTP 503 errors) with the IR stack.
3. This can serve to reflect the state of Vital and the Image Retriever environment.
4. For a more detailed view of the Vital environment use (<http://splunkops.azblue.com/en-US/app/bcbsaz_ta_app_hms/hms_vital_system_summary> and <http://splunkops.azblue.com/en-US/app/bcbsaz_ta_app_hms/vital_letters>)



1. Portal/Web Servers – The primary metric in the overview dashboard will be ASP.NET errors, again as broader metric of web portal/health
2. Typically, this value is very low. However sharp spikes in these numbers are suggestive of SQL and network connectivity issues. This is also a predictive view.
3. For a more detailed view of the web tier use this secondary dashboard ( [http://splunkops.azblue.com/en-US/app/bcbsaz\_ta\_app\_5010/web\_tracking)](http://splunkops.azblue.com/en-US/app/bcbsaz_ta_app_5010/web_tracking))
4. IVR – The primary concern with IVR can measured by simple call initiation events. If calls are not reaching IVR there is an upstream (Telco/Avaya issue).
5. Secondary dashboard (<http://splunkops.azblue.com/en-US/app/bcbsaz_ta_app_ivr/ivr_service_response_times_as_volume_increases>)

