
ONUG
ONUG FALL 2018
OCTOBER 22 & 23| HOSTED BY FedEx
Metropolitan Pavilion, New York City

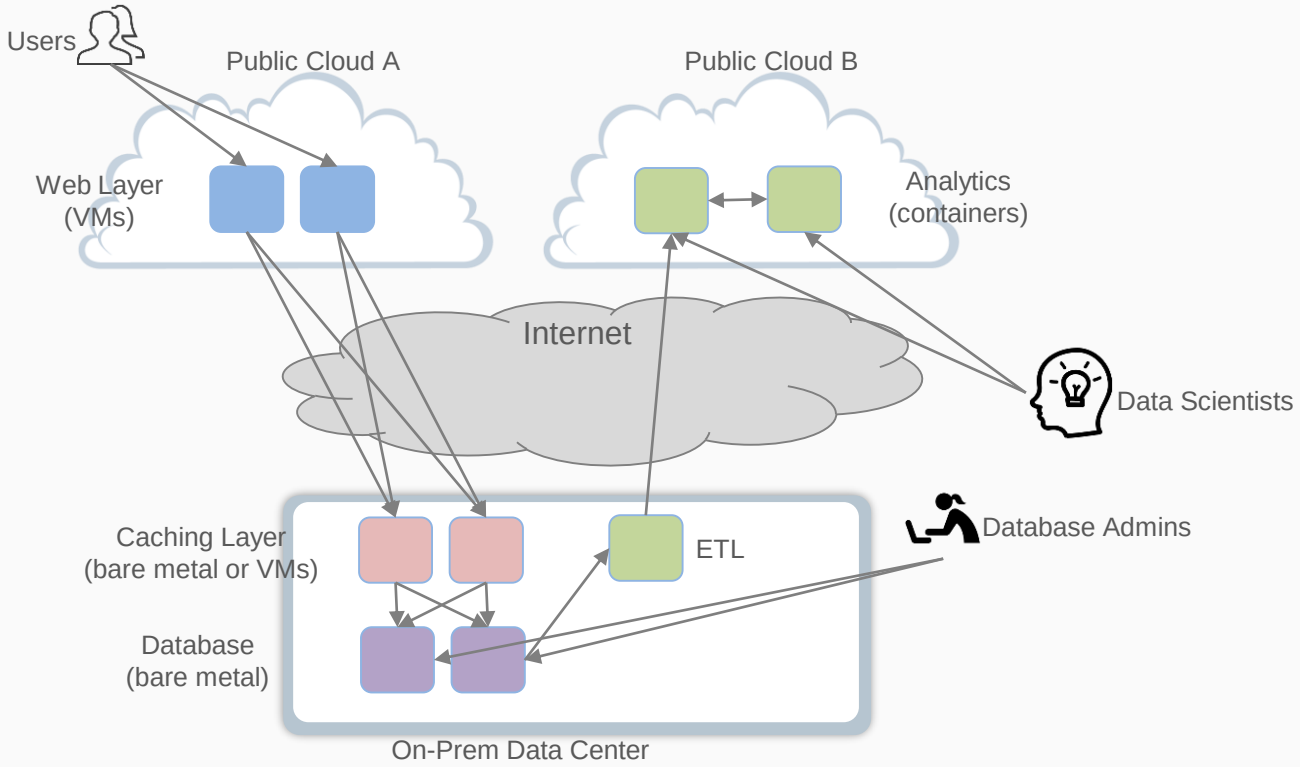
ONUG Fall 2018 PoC Guidelines

- In this deck are PoCs use case guidelines that sponsors may choose to demonstrate at ONUG Fall
- Sponsors are highly encouraged to do a PoC associated with the ONUG Working Group (SDSS, M&A & OSE) use cases
- Some sponsors will be participating in the ONUG Reference Designs taking place now & are encouraged to use PoCs to show how their company plugs into the ONUG Reference Designs being developed in the SDSS, M&A & SD-WAN Working Groups
- **These PoC Guidelines are suggestions**
- **DEADLINES: Abstract by Fri, 9/21, & Slide Deck by Fri, 10/5**

Structure

- All PoCs are based upon the hybrid/multi-cloud use case, detailed in the next slide
- The 3 remaining PoCs are focused upon how one may
  - Connect via SD-WAN
  - Secure via Software-Defined Security Services
  - Monitor & perform Analytics
- Each sponsor has the opportunity to demonstrate in the PoC Theater

ONUG Hybrid/Multi-Cloud PoC Configuration

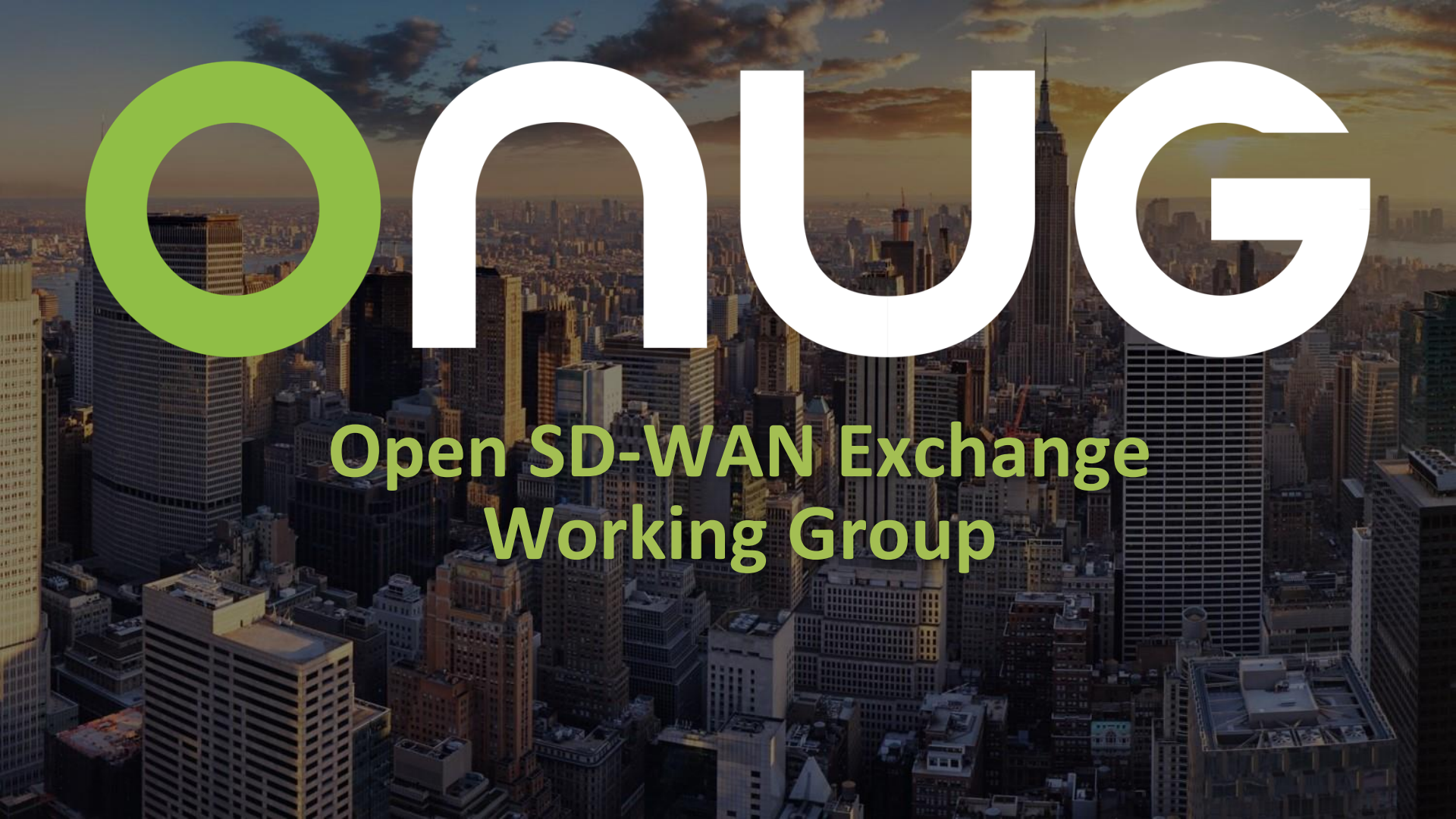


PoC Environment Set-Up Description

- Hybrid/multi-cloud infrastructure deployment
  - Web layer in “public cloud A” running on VMs
  - Caching layer in on-prem data center running on VMs
  - Database running in on-prem data center on bare metal servers
  - Analytics cluster in “public cloud B” running as containers
  - ETL (Extract, Transform, Load) from DBs to Analytics
- Communication needed to make things work
  - Web layer uses caching layer to serve the content
  - Caching layer uses database for persistent storage
  - Users on the internet access the web layer
  - Database Admins (DBAs – internal users) need administrative access to databases
  - ETL process loads data from databases and uploads it to analytics cluster

PoC Options

- Based upon the hybrid/multi-cloud PoC configuration, vendors may choose to demonstrate the following ONUG Working Group Use Cases
  - Connectivity via SD-WAN or the ONUG Open SD-WAN Exchange
  - Secure via Software-Defined Security Services
  - Monitor & perform Analytics
- The next 3 sections detail the above 3 PoC options


ONUG
Open SD-WAN Exchange
Working Group

OSE Outline

- SD-WAN PoC Options
- SD-WAN PoC Requirements

SD-WAN PoC Options

- Based upon the hybrid/multi-cloud PoC configuration, slide 4/5:
  - Cloud A/B may be public cloud providers, SaaS providers, IaaS vendors, etc.
  - Demonstrating configuration & workload movement between
    - Public-Private Cloud, Public Clouds, Remote Access, etc.
    - The next slide offers use case requirements to consider highlighting in your PoC

SD-WAN PoC Requirements

1. Remote site to leverage public WAN only - via broadband (if available) or via bring your own 4G LTE, remotely connect to demo, or record demo from lab to show at ONUG
2. CPE in a virtual form factor on commodity h/w
3. A secure hybrid WAN architecture allowing dynamic traffic eng specified by app policy, availability, etc. (see slide 4 & 5); vendor to either arrange for multiple WAN access at ONUG, use 4G LTE, remotely connect to demo, or record demo from its lab to show at ONUG
4. Visibility, prioritization & steering of biz critical & RT apps as per security & corp. governance & compliance policies
5. A highly available & resilient hybrid WAN, see 3 above for wide access options
6. Site, Application & VPN performance level dashboard reporting, assume no encryption for this requirement
7. Open northbound API for controller access & mgmt.: log events to net event co-relation mgr, SIEM
8. Zero touch for remote vm provisioning & deployment

Software-Defined Security Services Working Group

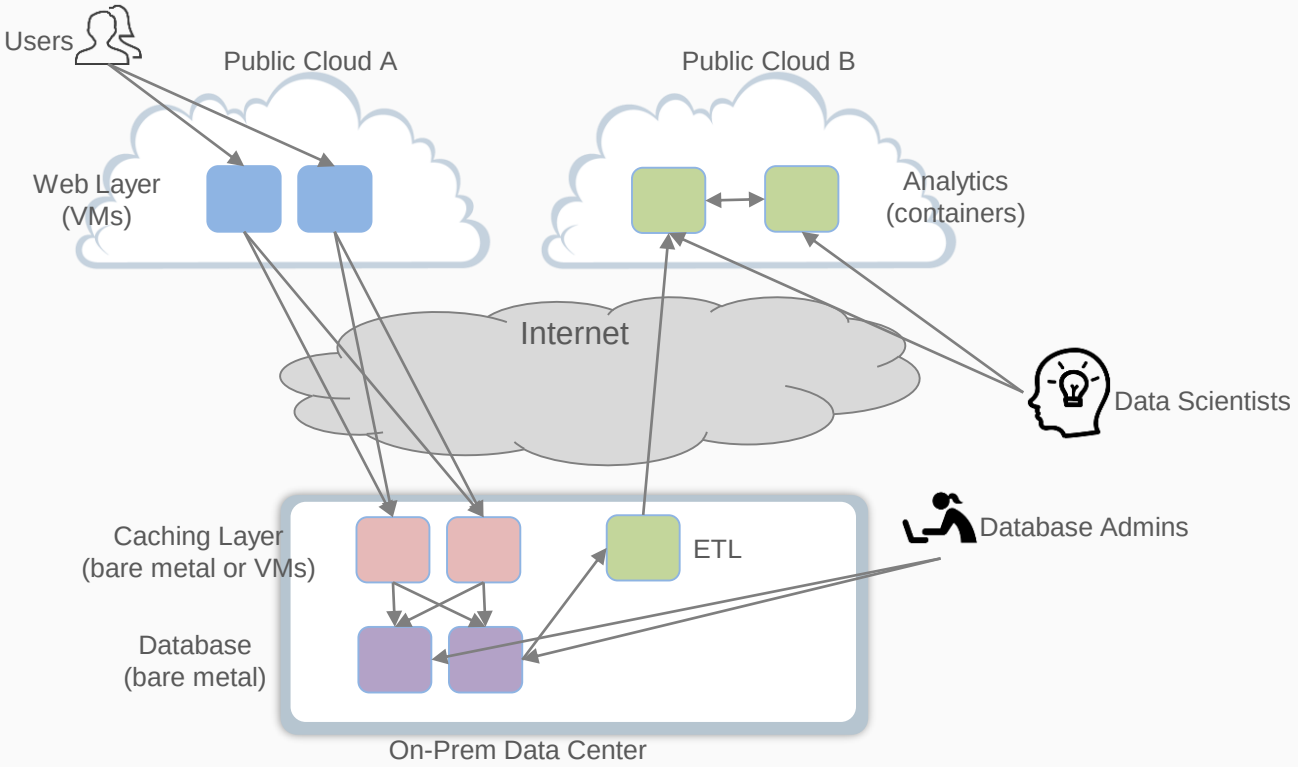
SDSS Outline

- S-DSS Position Statement
- PoC Environment Setup
- PoC Environment Security Services
- PoC Environment: Visibility & Analytics

S-DSS Position Statement

"The S-DSS working group's framework consists of an intent-based security architecture that ties policies to workloads, independent upon of host model that is bare metal, hypervisor, container and serverless. Policy enforcement is local to the workload and independent upon its physical location be it on or off premises"

S-DSS PoC Environment Setup



PoC Environment Setup - Description

- Hybrid infrastructure deployment
  - Web layer in “public cloud A” running on VMs
  - Caching layer in on-prem data center running on VMs
  - Database running in on-prem data center on bare metal servers
  - Analytics cluster in “public cloud B” running as containers
  - ETL (Extract, Transform, Load) from DBs to Analytics
- Communication needed to make things work
  - Web layer uses caching layer to serve the content
  - Caching layer uses database for persistent storage
  - Users on the Internet access the Web layer
  - Database Admins (DBAs – internal users) need administrative access to databases
  - ETL process loads data from databases & uploads it to analytics cluster
  - Data Scientist (internal users) need access to analytics cluster

PoC Environment Security Services

- Access Control / Firewall / Microsegmentation Policies
  - Web workloads provides “http/https” service to the any user on the Internet
  - Caching workloads provide “caching” service to the Web workloads
  - Database workloads provide “database” service to the Caching workloads
  - Database workloads provide “database” service to Database Admins (internal users)
  - Database workloads provide “database” service to ETL workloads
  - Analytics workloads provide “analytics” service to Analytics workloads
  - Analytics workloads provide “https” service to Data Scientists (internal users)
  - Other policies for allowing core services & monitoring the applications
  - All other communication except the above needs to be blocked!
- Visibility & Analytics
  - Demonstrate the ability to support visibility, analytics & reporting for security (e.g., telemetry to a SIEM, report of all the connections going into a PCI application for compliance)

PoC Environment Security Services

- Encryption policies for data-in-transit
  - Traffic between Web layer & Caching layer needs to be encrypted
  - Traffic between ETL & Analytics cluster needs to be encrypted

There are a broad range of other security services including, but not limited to, IDS/IPS, Deception, Data Loss Detection/Prevention, & User Behavioral Analytics

Vendors are encouraged to showcase any of these services during the PoC

PoC Environment: Visibility & Analytics

- Demonstrate the ability to support visibility, analytics & reporting for security (e.g., telemetry to a SIEM, report of all the connections going into a PCI application for compliance)
- Demonstrate the ability to detect user-defined security threats
  - Reporting workloads being attacked by user-defined threats
  - Ability to quarantine threats and mitigate the threats
- Demonstrate the ability to detect & report the “Command-and-control servers” events
  - Provide statistics of DCs being infected, statistics on the source of attacks, etc.
- Demonstrate the ability to categorize various attacks by domains, sources, etc.
  - Such as phishing files downloaded to workloads
  - Malicious C&C flows, DGA domain name requests
- Demonstrate an ability to monitor compliance to policy enforcements for application workload state changes


ONUG
Monitoring & Analytics
Working Group

M&A Outline

- M&A Position Statement
- Scope of M&A PoC
- PoC Area of Focus – Application Assurance
- PoC Area of Focus – Infrastructure Assurance
- PoC Area of Focus – Network Assurance

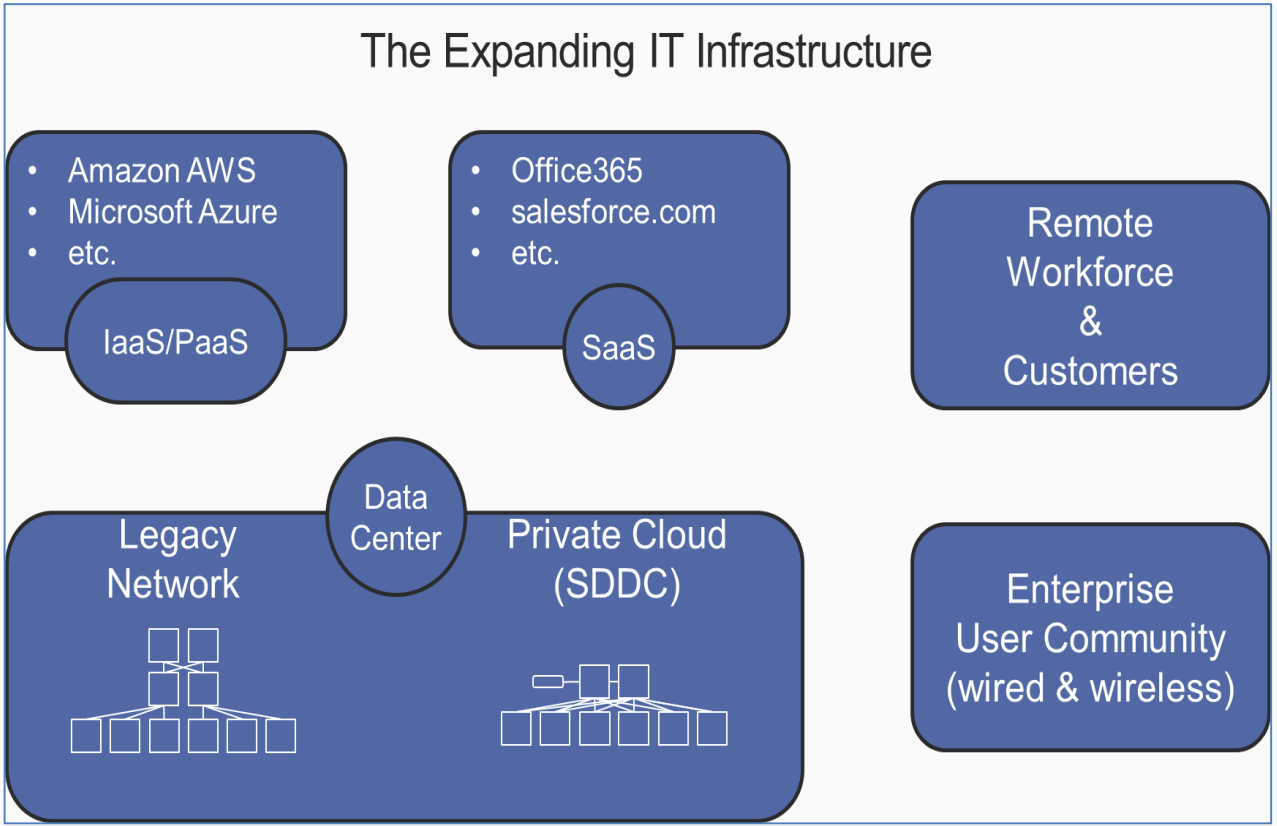
M&A Position Statement

"The M&A Working Group's framework consists of a Monitoring and Analytics architecture that collects and derives information from physical and virtual infrastructure (e.g., compute, storage, network, management systems) and applications, independent upon physical location be it on or off premises (e.g., public cloud). Data is ingested into a data warehouse or data lake so that data and event visualization and correlation, monitoring and other operational use cases are possible in the operationalizing of the infrastructure."

Scope of M&A PoC

- PoCs are encouraged to address one, or ideally, more of the following M&A Working Group areas of focus:
  - Application Assurance
  - Infrastructure Assurance
  - Network Assurance
- Each of these is defined further in the following slides
- PoCs should demonstrate how their solution is relevant to hybrid environments
- Optionally, PoCs may include legacy physical, virtualized, private & public cloud platforms.
- Participants are encouraged to read: “An Introduction to Monitoring & Analytics Requirements,” *ONUG 2017 M&A Working Group* https://www.onug.net/wp-content/uploads/2018/02/2017-Spring_Monitoring-and-Analytics.pdf

The Modern Enterprise



PoC Area of Focus – Application Assurance

- Application Assurance
  - For the purposes of this PoC, application assurance is the task of ensuring that an application is available, responsive & functioning as expected
  - Application optimization & debugging features may be included, but are of secondary focus
- Example approaches include: synthetic transactions, wire data analytics, application & database agents, applications logs
- Example KPIs include:
  - Application response time (excluding network delay)
  - Number & type of any errors returned by the application
  - Dependencies between components of the service, shared enabling services, e.g., DNS & NTP, & upon third-party services
  - Is the application reachable?

PoC Area of Focus – Infrastructure Assurance

- Infrastructure Assurance
  - For the purposes of this PoC, infrastructure assurance is the task of ensuring that network and application infrastructure is available, responsive & functioning as expected
- Infrastructure includes compute, storage, network devices, management systems (physical & virtual)
- Example approaches include: device APIs, controller APIs, agents, logs
- Example KPIs & metadata include:
  - Hypervisor, container & cloud information
  - CPU, memory, storage usage
  - Errors
  - Environmental factors
  - State tables

PoC Area of Focus – Network Assurance

- Network Assurance
  - For the purposes of this PoC, network assurance is the task of ensuring that an network is available, delivering expected performance & correctly configured
- Network Assurance can be considered as a subset of Infrastructure Assurance
- Example approaches include: passive wire data analytics, flow information
- Example KPIs include:
  - Profile of traffic on a link
  - Network delay contribution to application response time
  - Metrics related to quality of service markings
  - Virtual network identifiers, e.g., VLAN, VRF ID, VNI, VSID
  - Microbursts, packet loss and jitter
  - Is the site reachable?