Gain End-to-End Visibility Into Your Azure Cloud Environment using Splunk

A data journey through Azure

Jason Conger | Splunk

October 2018 | Version 1.0

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

whoami

jason.conger@splunk.com
@JasonConger
http://www.linkedin.com/in/JasonConger
https://www.splunk.com/blog/author/jconger.html

Staff Solutions Architect
Global Strategic Alliances

6+ years at Splunk

Created or consulted on 25+ Splunkbase applications

2

There are 10 types of people in the world;
those that understand binary and those that do not.

How Azure Makes Data Available

splunk> .conf18

Different Planes for Data

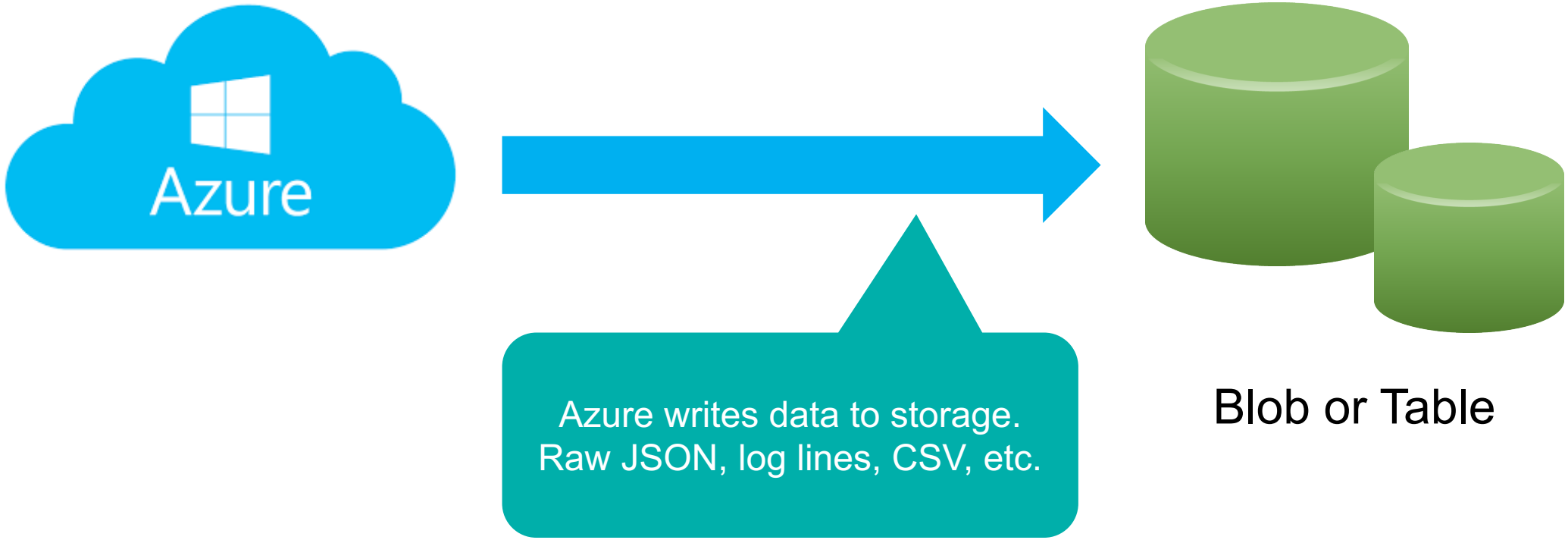
Control & Data

Control Plane: System Configuration and Management

Data Plane: Provisioned Service and Diagnostic Data

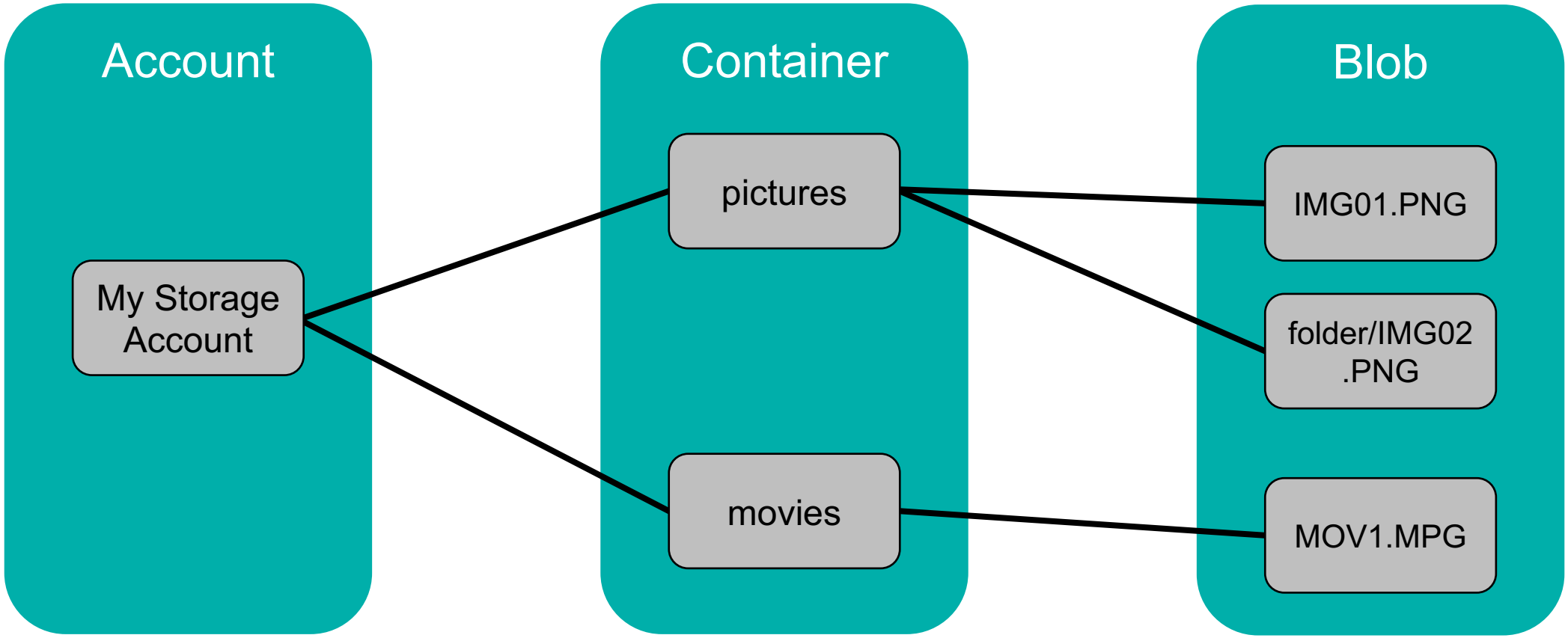
Storage Account

Storage Accounts are the Least Common Denominator for Azure Services



Storage Account Blobs

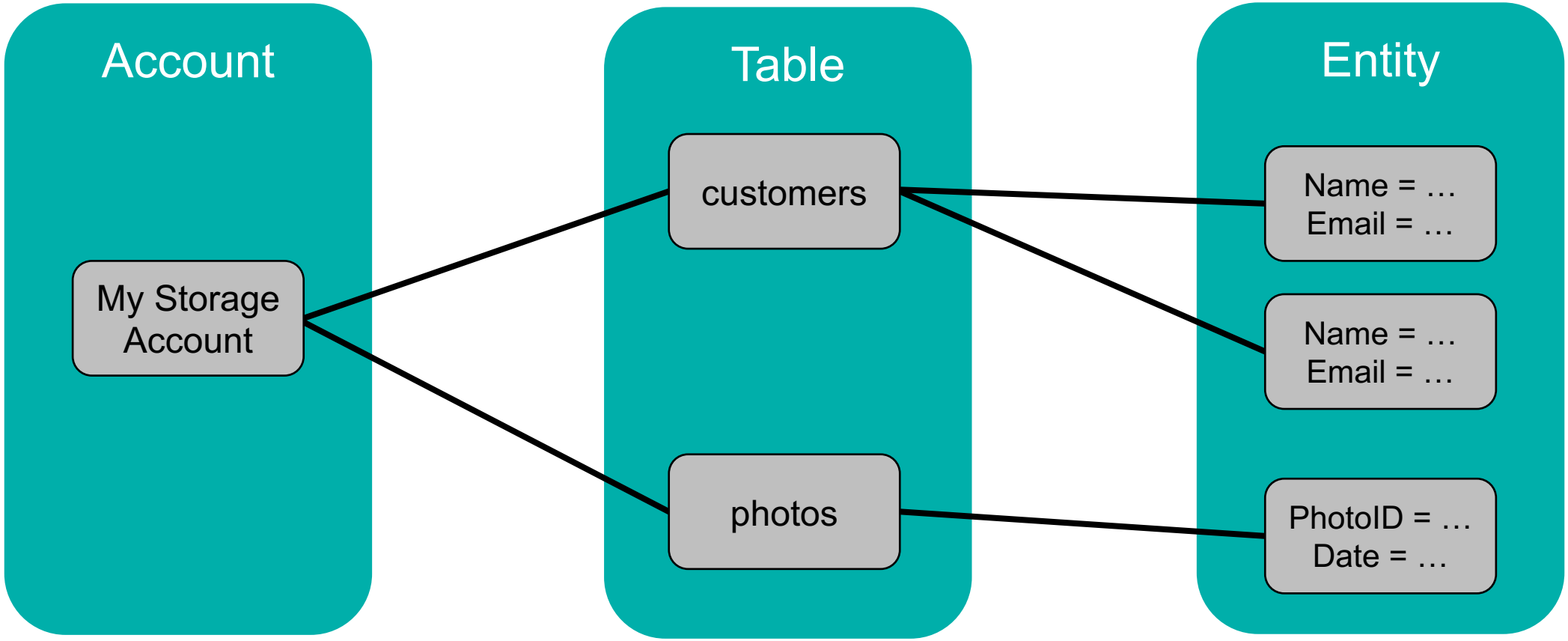
Similar to a File system



Example: NSG Flow Logs

Storage Account Table

Similar to CSV or Database Table



Example: VM Performance Logs

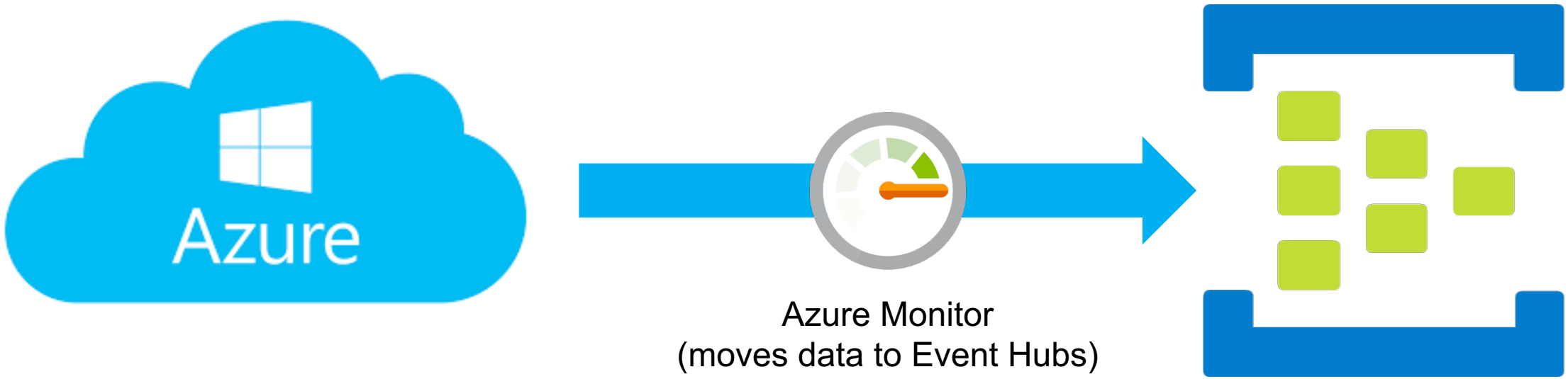
REST APIs

Metadata, Topology, Consumption

{ REST }

Event Hubs

High Velocity and Scale

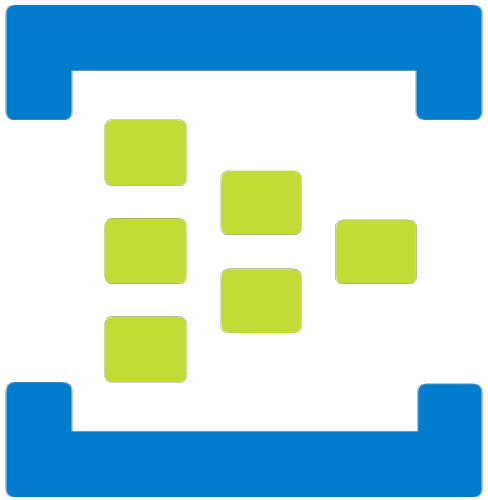


Azure Monitor
(moves data to Event Hubs)

The Azure Monitor Add-on for Splunk pulls data from Event Hubs

Azure Functions

Serverless Code



Serverless code can take action on events in the hub.

Azure Function blueprints to push data to Splunk via HEC:
https://github.com/Microsoft/AzureFunctionforSplunkVS

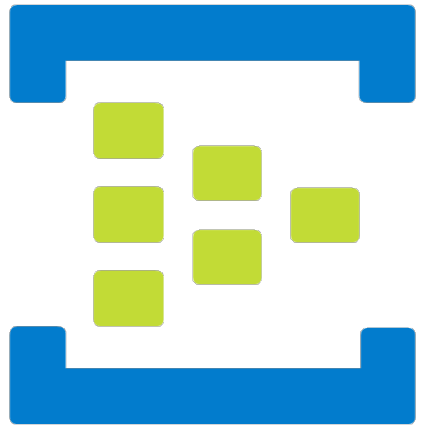
Recap

Storage Accounts, REST, Event Hub

Storage

{ REST }

API



Event Hub

Azure Add-on Landscape

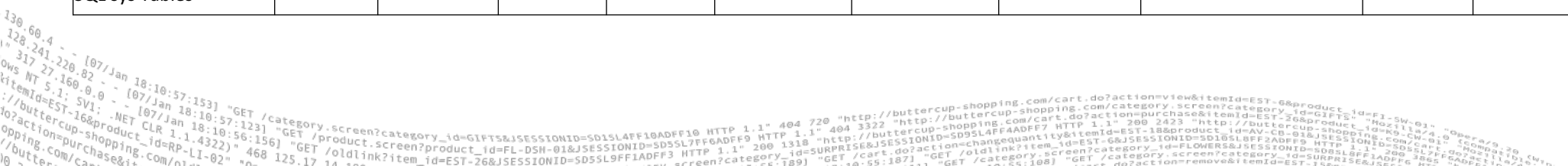
Tools for your Splunk + Azure Toolbox

splunk> .conf18

Azure Add-on Landscape

Is there an add-on for that?

	Splunk Add-on for Microsoft Cloud Services				Azure Monitor Add-on for Splunk			Azure Billing Add-on for Splunk	Azure Inventory Add-on for Splunk			Splunk DB Connect
	Audit Input	**Blob Input**	**VM Metrics Input**	**Resource Input**	**Audit Input**	**Diagnostics input**	**Metric Input**	**Consumption and Billing input**	**VM Input**	**Storage Input**	**Topology Input**	
Audit Logs	(via API)				(via Event Hub)							
Diagnostic Logs		(via Storage)				(via Event Hub)						
Azure AD Sign-ins						(via Event Hub)						
Azure AD Audit						(via Event Hub)						
VM Metrics			(via Table)				(via API)					
Metrics*							(via API)					
VM Metadata				(via API)					(via API)			
Storage Metadata										(via API)		
Topology											(via API)	
NSG Flow Logs		(via Storage)										
Security Center						(via Event Hub)						
Consumption and Cost								(via API)				
SQL sys Tables												(via SQL)

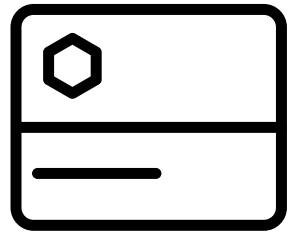


splunk> .conf18

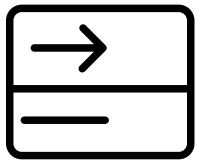
Where do Add-ons run?

Indexing, forwarding, egress, compression

Possible Data Egress (tiered costs)

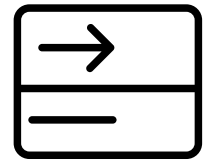


Indexing

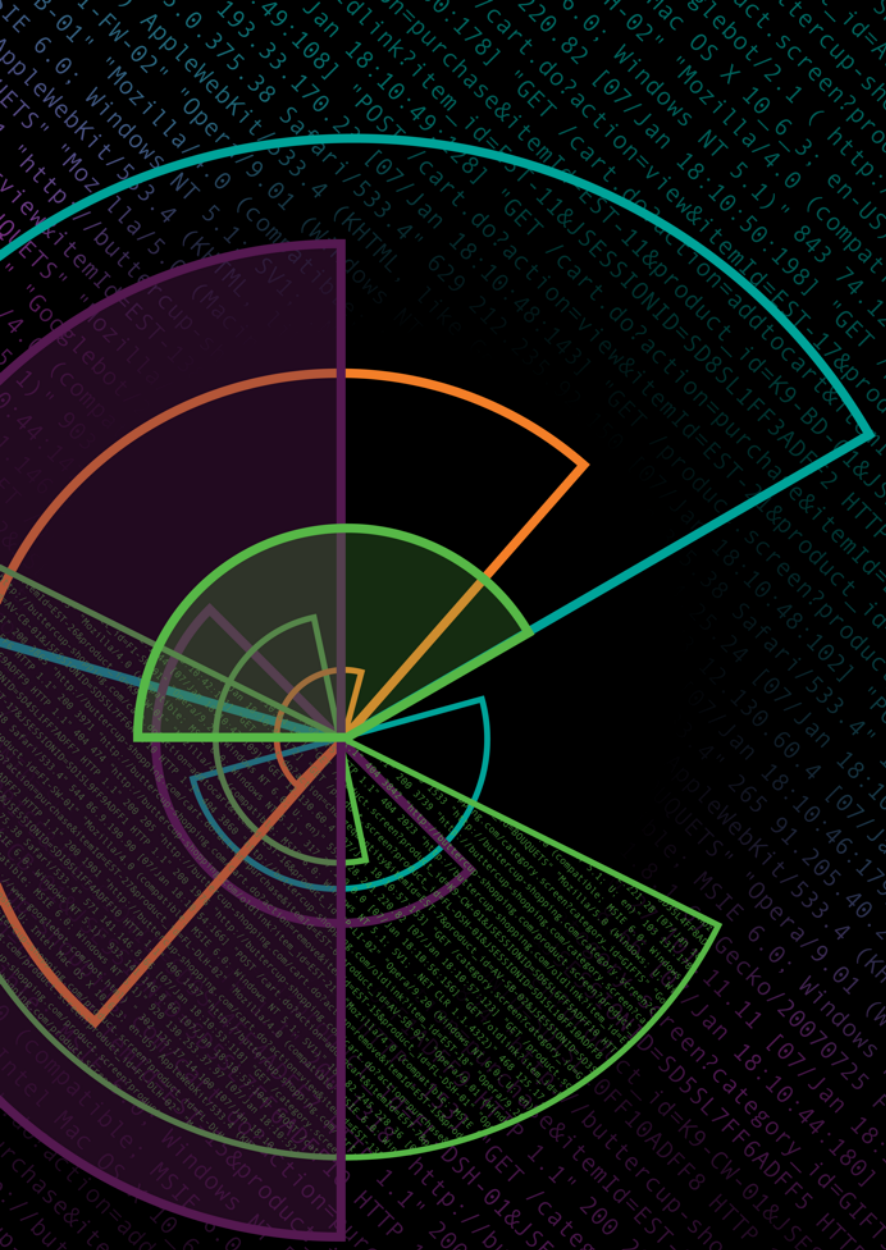


Forwarder
Inside Azure?

Inside Azure	Outside Azure
VM Cost - OpEx	CapEx
S2S compression = lower egress usage	Uncompressed data = more egress usage
Filtering via Splunk options prior to egress	Filtering on API level requires coding



Forwarder
Outside Azure?

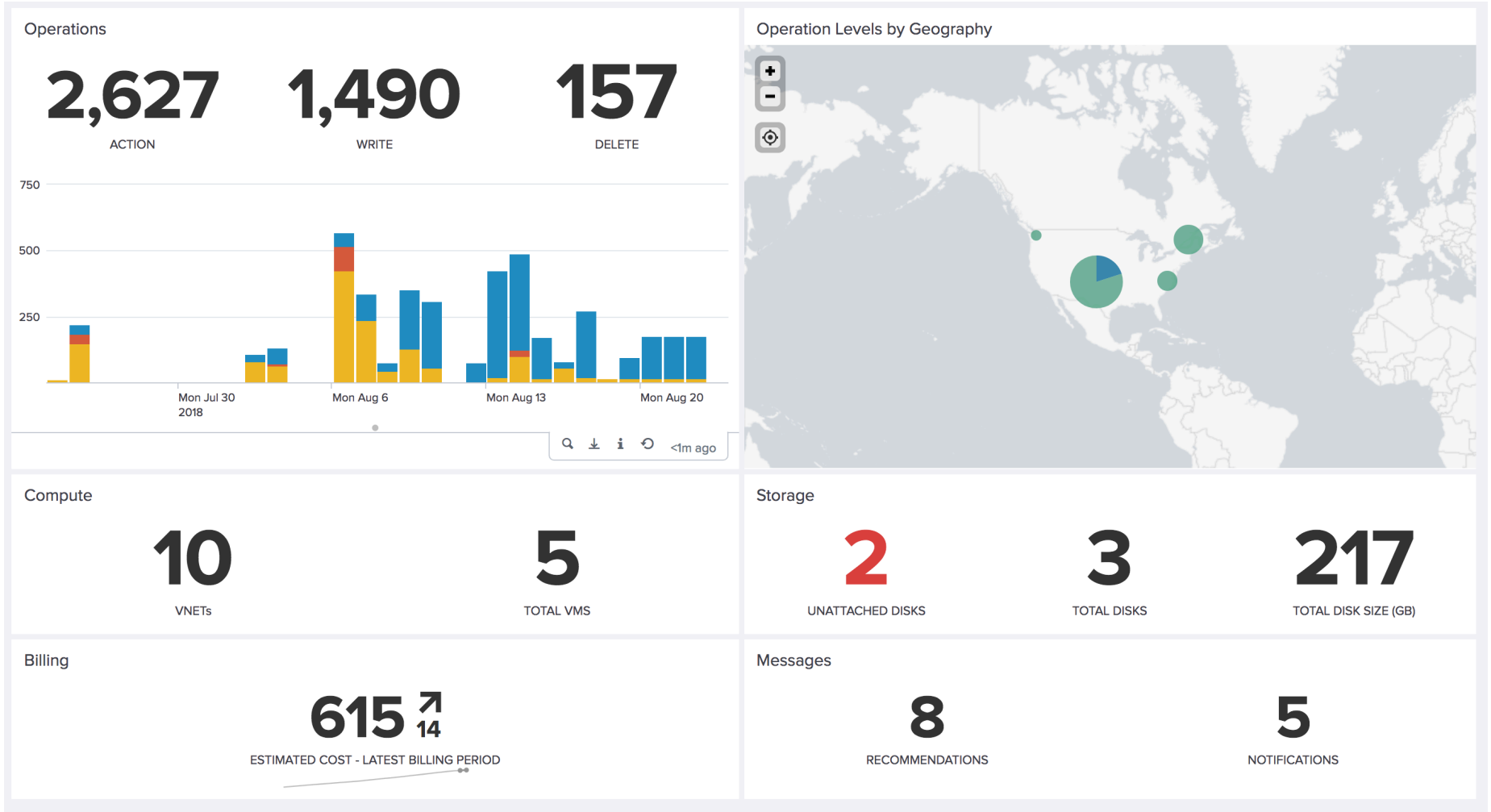


Azure Data Use Cases

I've got the data, now what?

Environment Overview

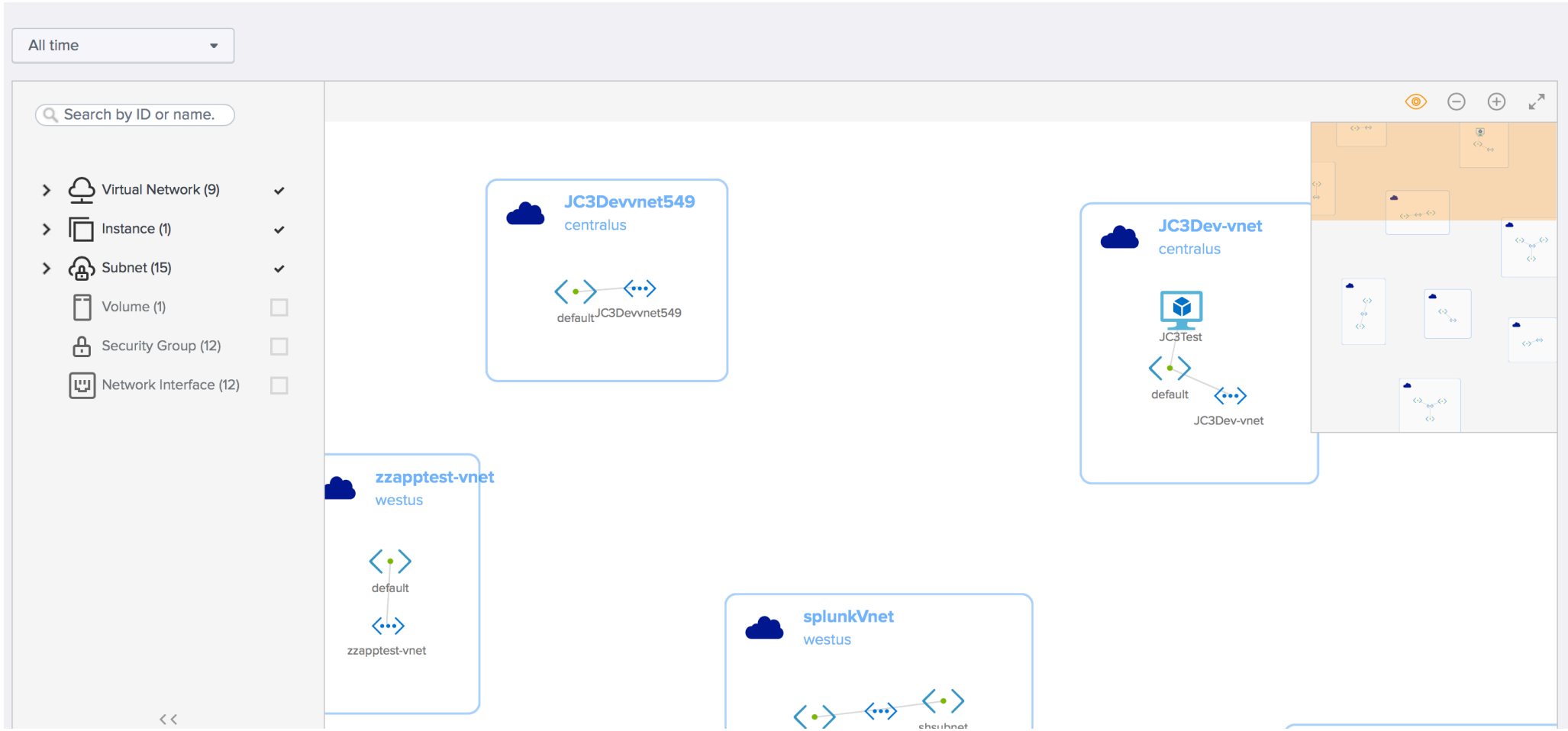
Multiple Subscriptions and Tenants in one place



splunk> .conf18

Topology

Multiple Account and Subscription Topology Visualization



Billing and Consumption

Analyze Spend and Predict Costs

Estimated Cost - Current Billing Period

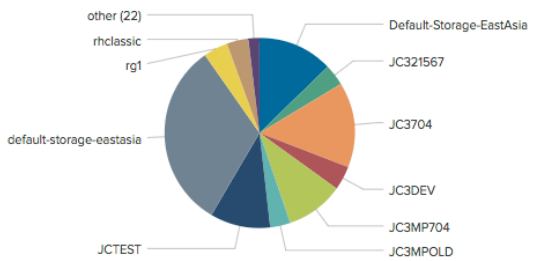
615 ↗ 14

ESTIMATED COST - LATEST BILLING PERIOD

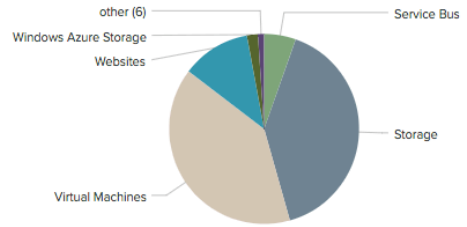
Total Projected Cost - by Month End

861

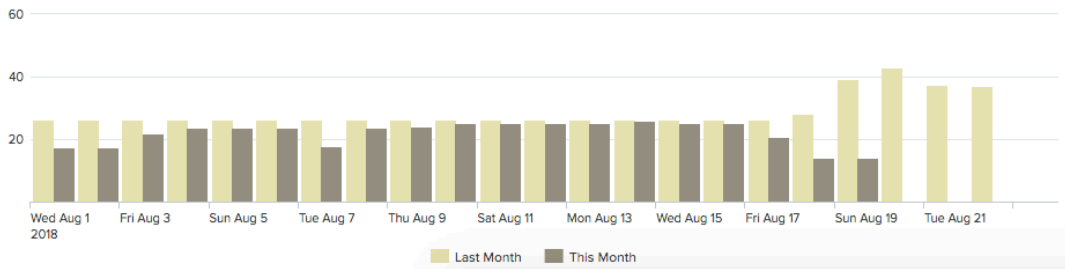
Estimated Cost by Resource Group



Estimated Cost by Meter Category



Month over Month Comparison - Daily Cost



Subscription Id	Category	Cost	Percentage
ae4ab7c9-dcdf-4427-9729-48e8c7551be9	Storage	$247	40.22%
ae4ab7c9-dcdf-4427-9729-48e8c7551be9	Virtual Machines	$244	39.76%
ae4ab7c9-dcdf-4427-9729-48e8c7551be9	Websites	$72	11.71%
ae4ab7c9-dcdf-4427-9729-48e8c7551be9	Service Bus	$33	5.41%
ae4ab7c9-dcdf-4427-9729-48e8c7551be9	Windows Azure Storage	$12	1.88%
ae4ab7c9-dcdf-4427-9729-48e8c7551be9	Networking	$5	0.79%
ae4ab7c9-dcdf-4427-9729-48e8c7551be9	Data Management	$1	0.13%

splunk> .conf18

Demo

Exploring Azure data with Splunk

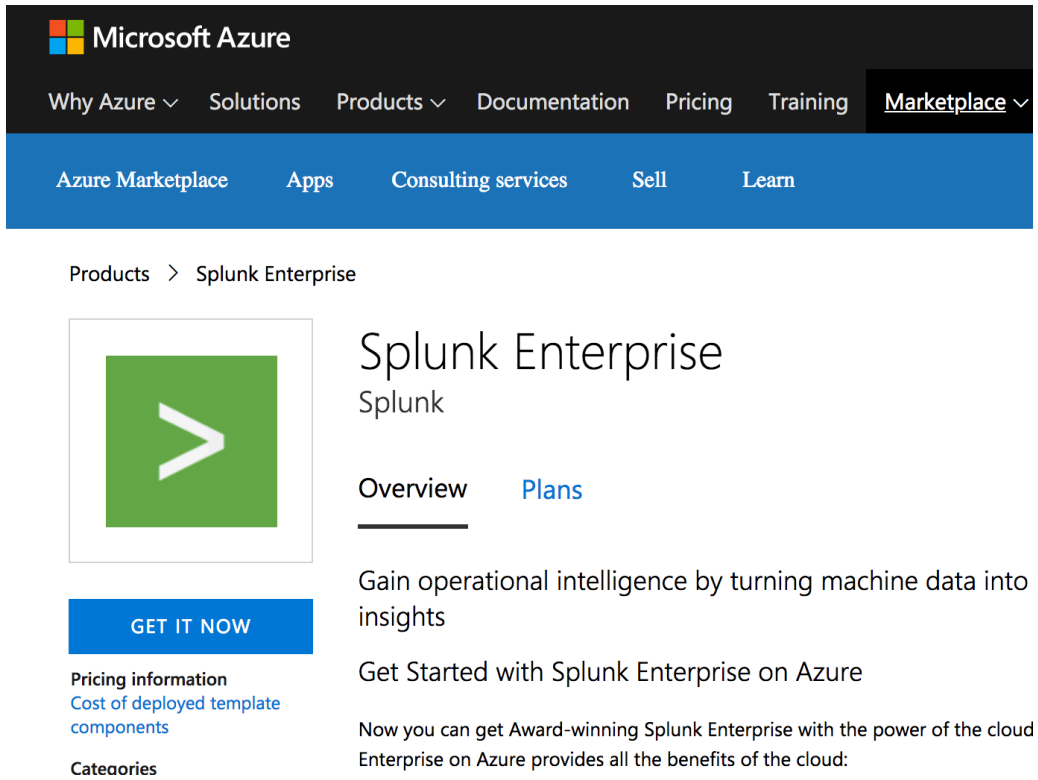
Additional Microsoft Cloud Sessions at .conf18

- **SEC1297 - Down in the Weeds, Up in the Cloud: Splunking Your Azure and Office 365**
  - Tuesday, Oct 02, 2:15 p.m. - 3:00 p.m.
- **SEC1355 - Hunting the Known Unknown: Microsoft Cloud**
  - Tuesday, Oct 02, 4:45 p.m. - 5:30 p.m.
- **IT1452 - Reaching Cloud Nirvana in a Multi-Cloud World**
  - Wednesday, Oct 03, 11:30 a.m. - 12:15 p.m.
- **SEC1097 - Office 365 in Nearly That Many Days: Splunking Microsoft Cloud Data, Then and Now**
  - Wednesday, Oct 03, 4:30 p.m. - 5:15 p.m.

splunk> .conf18

Splunk + Azure + BYOL

Running Splunk in Azure



splunk> .conf18

Additional Resources

- Splunk Blogs
  - https://www.splunk.com/blog/search.html?query=azure
- Splunk Security Essentials
  - https://splunkbase.splunk.com/app/3435/
- Azure Storage Explorer
  - https://azure.microsoft.com/en-us/features/storage-explorer/
- Azure Metrics List
  - https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-supported-metrics
- Diagnostic Log List
  - https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-diagnostic-logs-schema

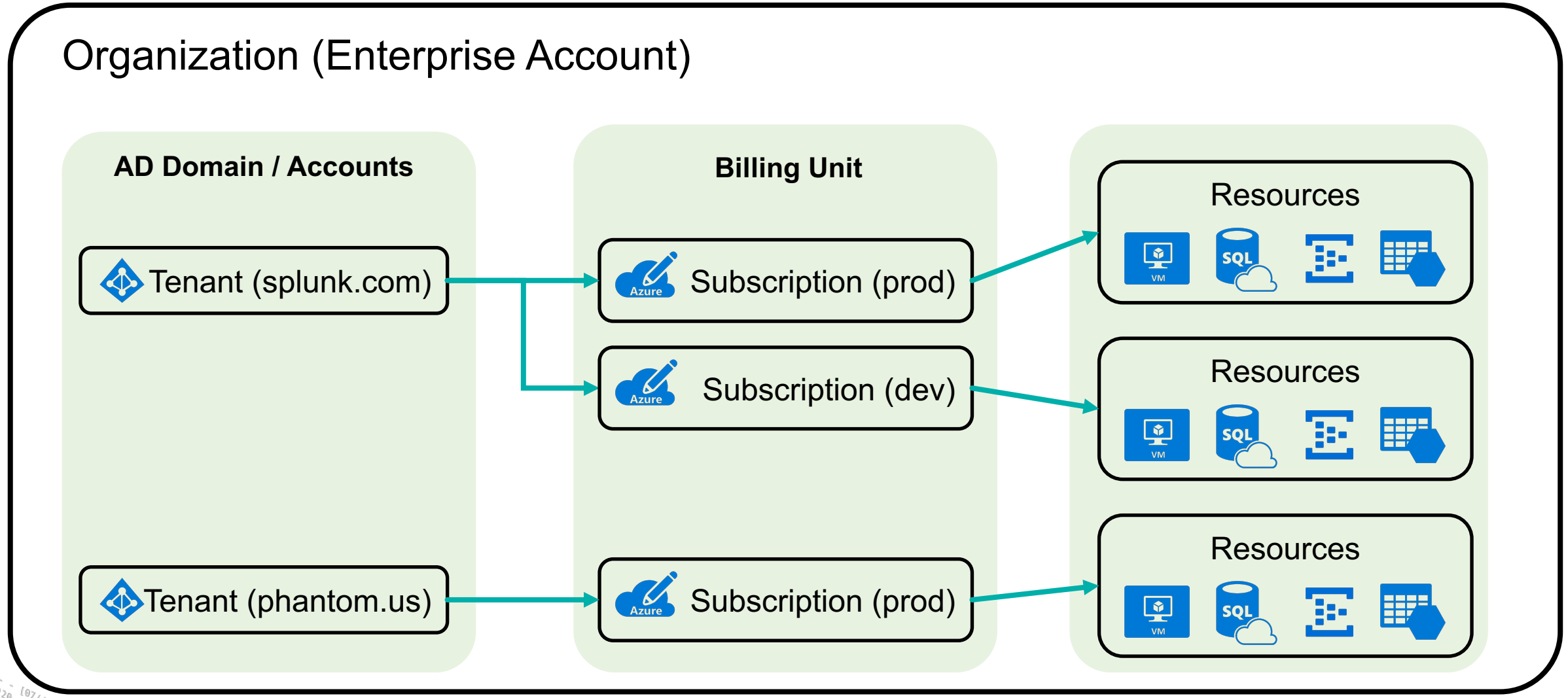
Thank You

Don't forget to rate this session in the .conf18 mobile app

Concepts

Tenants and Subscriptions
AAD Applications
Service Principals
Log Profiles

Azure Organization, Tenants, Subscriptions



Metrics Available from Azure Monitor

https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-supported-metrics

- Microsoft.AnalysisServices/servers
- Microsoft.ApiManagement/service
- Microsoft.Automation/automationAccounts
- Microsoft.Batch/batchAccounts
- Microsoft.Cache/redis
- Microsoft.ClassicCompute/virtualMachines
- Microsoft.ClassicCompute/domainNames/slots/roles
- Microsoft.CognitiveServices/accounts
- Microsoft.Compute/virtualMachines
- Microsoft.Compute/virtualMachineScaleSets
- Microsoft.Compute/virtualMachineScaleSets/virtualMachines
- Microsoft.ContainerInstance/containerGroups
- Microsoft.ContainerService/managedClusters
- Microsoft.CustomerInsights/hubs
- Microsoft.DataFactory/datafactories
- Microsoft.DataFactory/factories
- Microsoft.DataLakeAnalytics/accounts
- Microsoft.DataLakeStore/accounts
- Microsoft.DBforMySQL/servers
- Microsoft.DBforPostgreSQL/servers
- Microsoft.Devices/IotHubs
- Microsoft.Devices/provisioningServices
- Microsoft.DocumentDB/databaseAccounts
- Microsoft.EventHub/namespaces
- Microsoft.HDInsight/clusters

splunk> .conf18

Metrics Available from Azure Monitor

https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-supported-metrics

- Microsoft.Insights/AutoscaleSettings
- Microsoft.KeyVault/vaults
- Microsoft.LocationBasedServices/accounts
- Microsoft.Logic/workflows
- Microsoft.Network/loadBalancers
- Microsoft.Network/dnszones
- Microsoft.Network/publicIPAddresses
- Microsoft.Network/applicationGateways
- Microsoft.Network/virtualNetworkGateways
- Microsoft.Network/expressRouteCircuits
- Microsoft.Network/trafficManagerProfiles
- Microsoft.Network/networkWatchers/connectionMonitors
- Microsoft.Relay/namespaces
- Microsoft.Search/searchServices
- Microsoft.ServiceBus/namespaces
- Microsoft.SignalRService/SignalR
- Microsoft.Sql/servers/databases
- Microsoft.Sql/servers/elasticPools
- Microsoft.Sql/servers
- Microsoft.Storage/storageAccounts
- Microsoft.Storage/storageAccounts/blobServices
- Microsoft.Storage/storageAccounts/tableServices
- Microsoft.Storage/storageAccounts/queueServices
- Microsoft.Storage/storageAccounts/fileServices

splunk> .conf18

Metrics Available from Azure Monitor

https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-supported-metrics

- Microsoft.StreamAnalytics/streamingjobs
- Microsoft.TimeSeriesInsights/environments
- Microsoft.TimeSeriesInsights/environments/eventsources
- Microsoft.Web/serverfarms
- Microsoft.Web/sites (excluding functions)
- Microsoft.Web/sites (functions)
- Microsoft.Web/sites/slots
- Microsoft.Web/hostingEnvironments/multiRolePools
- Microsoft.Web/hostingEnvironments/workerPools

Terms and Aliases

- Tenant ID = Directory ID
- Application ID = Client ID
- Key = Client Secret
- Service Principal
  - When creating an Azure AD application, the Service Principal is the representation of that application in the tenant(s).
- Log Profile
  - Defines where logs go. Note: logs can go to more than one place at the same time.