



splunk®

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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

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

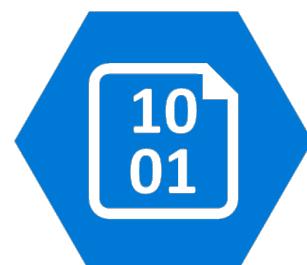
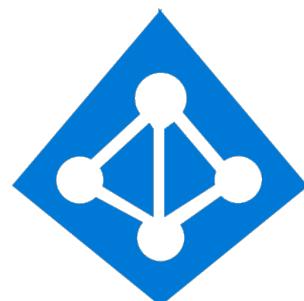
Different Planes for Data

Control & Data



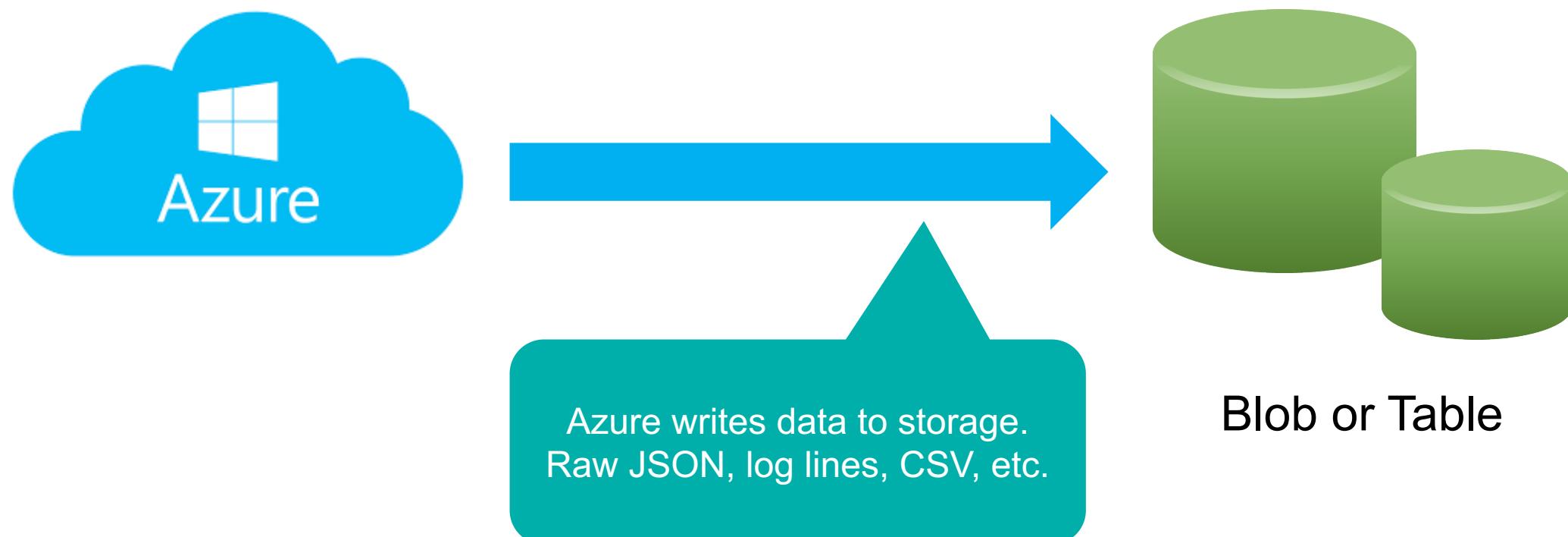
Control Plane: System Configuration and Management

Data Plane: Provisioned Service and Diagnostic Data



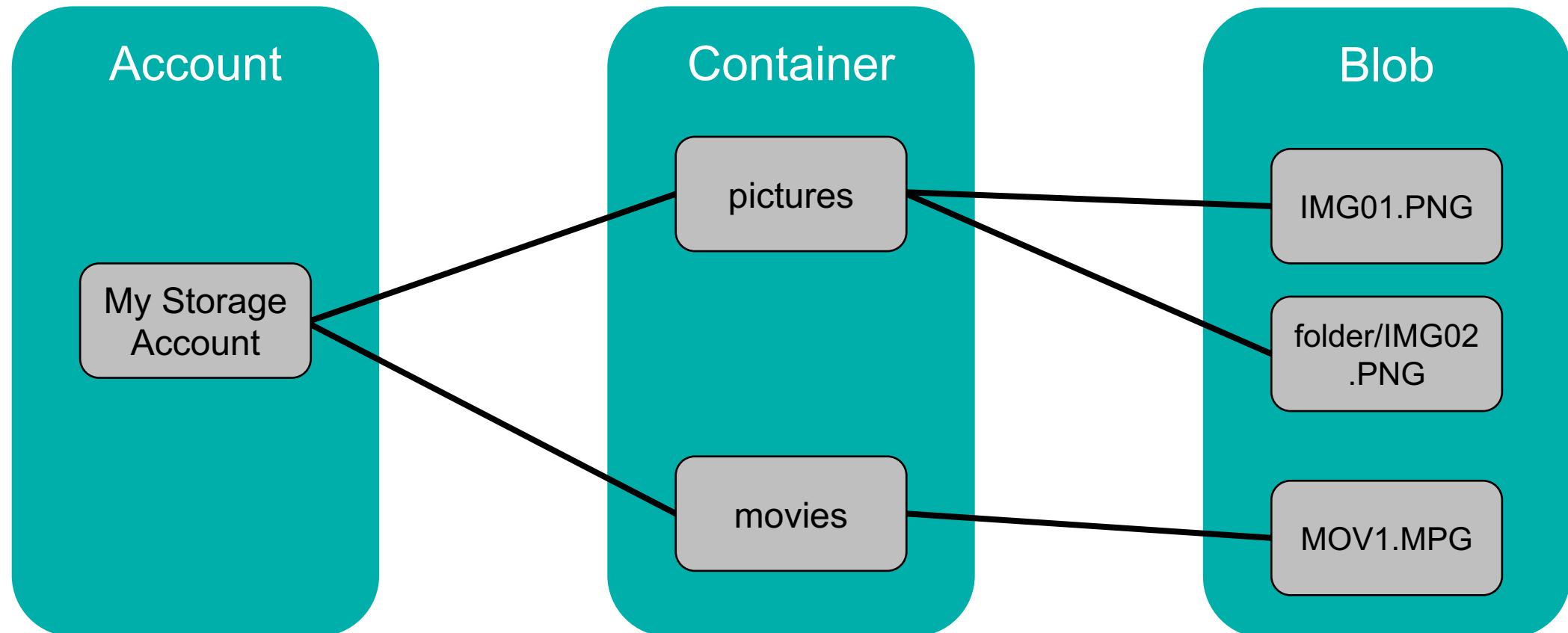
Storage Account

Storage Accounts are the Least Common Denominator for Azure Services



Storage Account Blobs

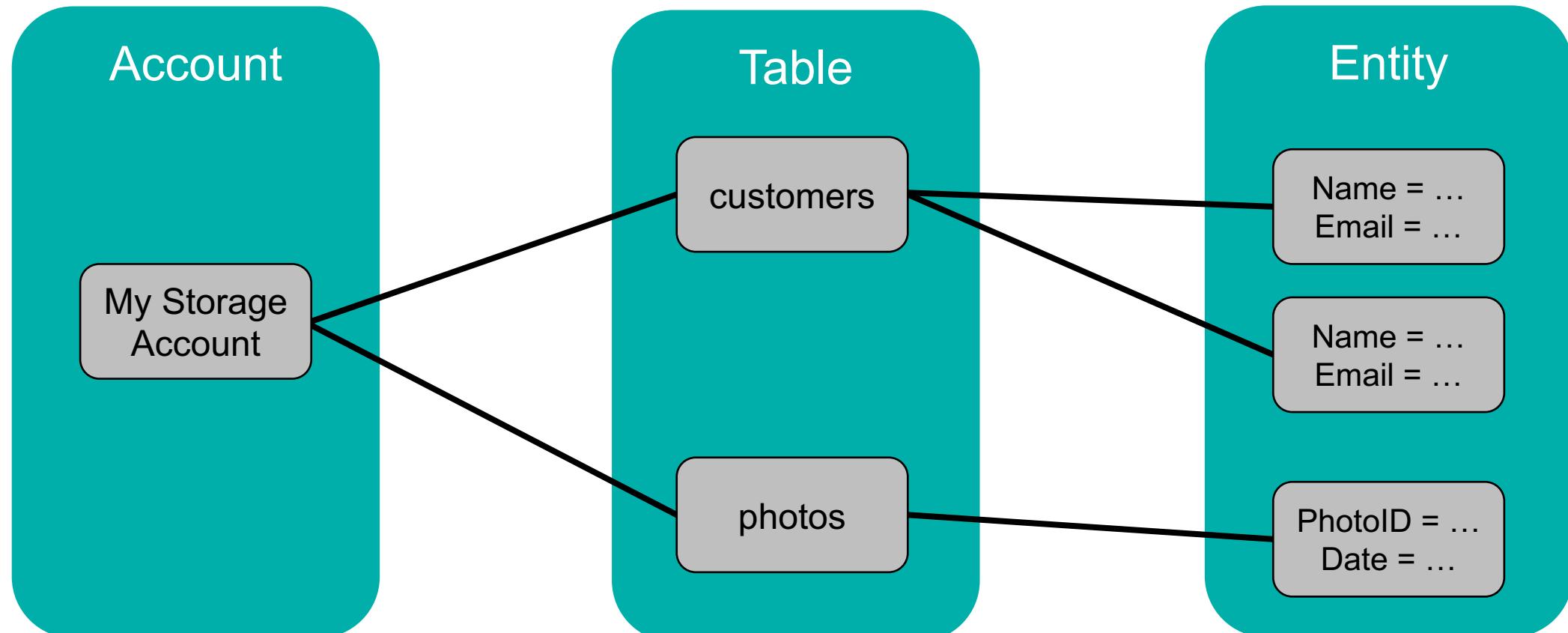
Similar to a File system



Example: NSG Flow Logs

Storage Account Table

Similar to CSV or Database Table



Example: VM Performance Logs

REST APIs

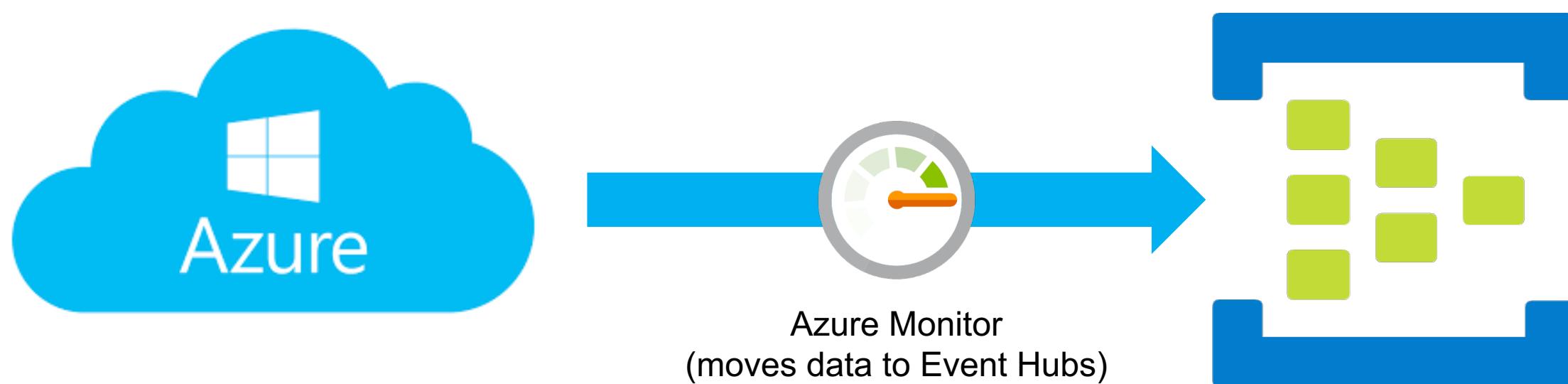
Metadata, Topology, Consumption



{ REST }

Event Hubs

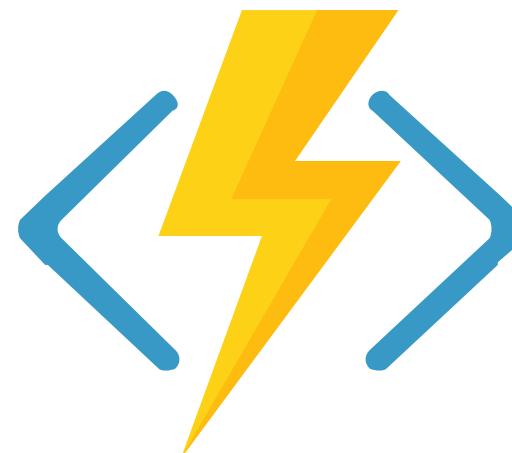
High Velocity and Scale



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

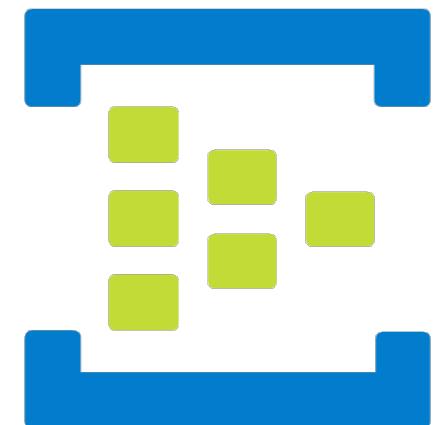
Storage Accounts, REST, Event Hub



Storage



API



Event Hub

Azure Add-on Landscape

Tools for your Splunk + Azure Toolbox

Azure Add-on Landscape

Is there an add-on for that?

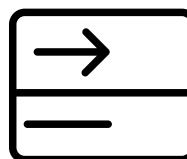
	Splunk Add-on for Microsoft Cloud Services				Azure Monitor Add-on for Splunk			Azure Billing Add-on for Splunk		Azure Inventory Add-on for Splunk			Splunk DB Connect
	Audit Input	Blob Input	VM Metrics Input	Resource Input	Audit Input	Diagnostics input	Metric Input	Consumption and Billing input	VM Input	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)

Where do Add-ons run?

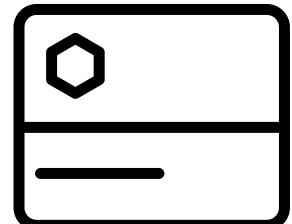
Indexing, forwarding, egress, compression



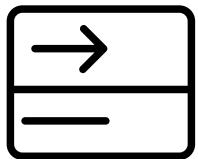
Forwarder Inside Azure?



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



Indexing



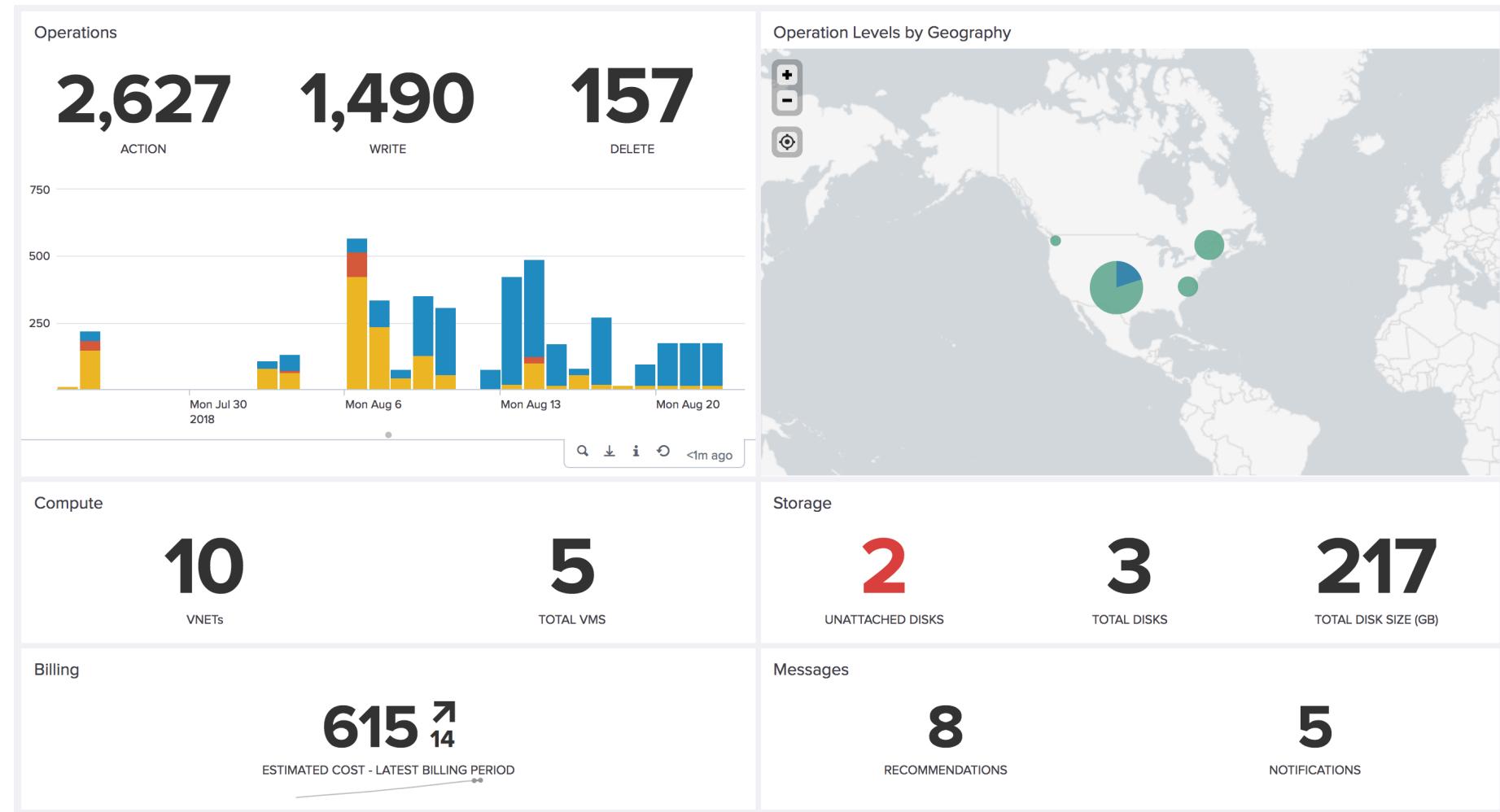
Forwarder Outside Azure?

Azure Data Use Cases

I've got the data, now what?

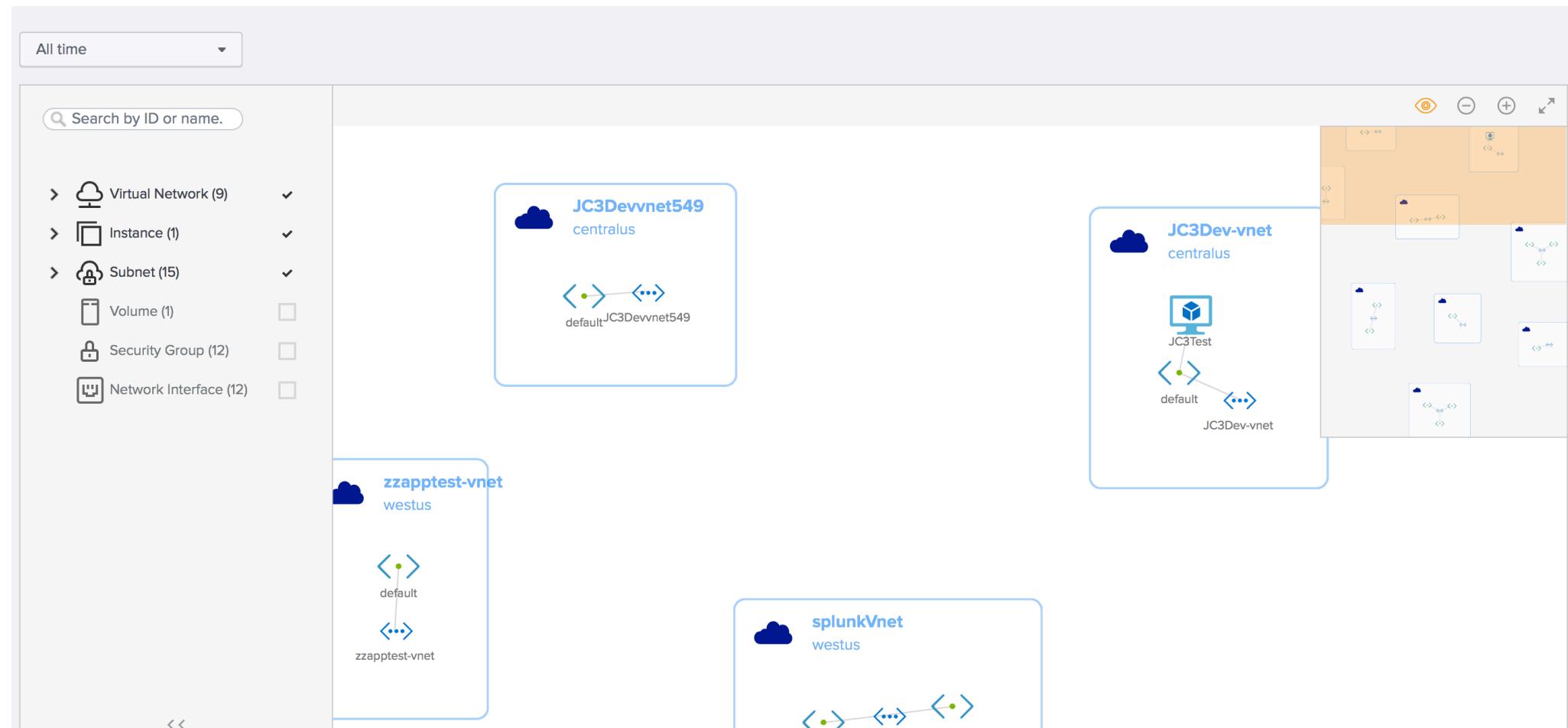
Environment Overview

Multiple Subscriptions and Tenants in one place



Topology

Multiple Account and Subscription Topology Visualization



Billing and Consumption

Analyze Spend and Predict Costs

Estimated Cost - Current Billing Period

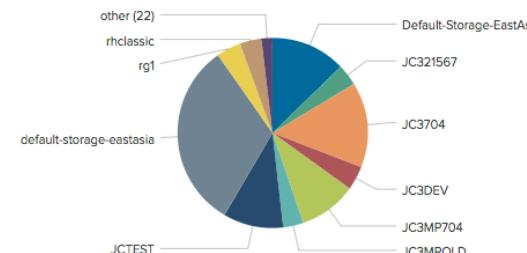
615 ↑
14

ESTIMATED COST - LATEST BILLING PERIOD

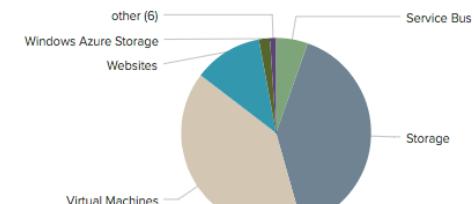
Total Projected Cost - by Month End

861

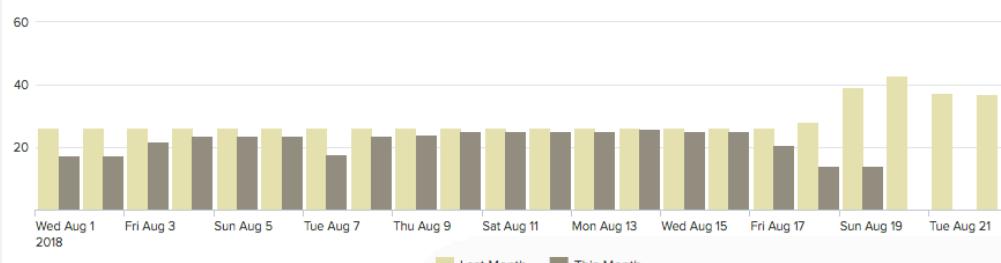
Estimated Cost by Resource Group



Estimated Cost by Meter Category



Month over Month Comparison - Daily Cost



Subscription Id

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%

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 + Azure + BYOL

Running Splunk in Azure

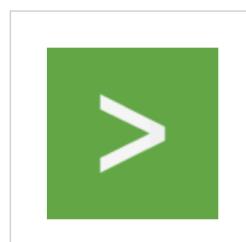


Microsoft Azure

Why Azure ▾ Solutions Products ▾ Documentation Pricing Training Marketplace ▾

Azure Marketplace Apps Consulting services Sell Learn

Products > Splunk Enterprise



Splunk Enterprise

Splunk

Overview [Plans](#)

Gain operational intelligence by turning machine data into insights

Get Started with Splunk Enterprise on Azure

Pricing information

Cost of deployed template components

Categories



DEPLOYING SPLUNK® ENTERPRISE ON MICROSOFT® AZURE™

Splunk provides the leading platform for Operational Intelligence. Splunk software searches, monitors, analyzes and visualizes machine-generated big data from websites, applications, servers, networks, sensors and mobile devices. More than 11,000 organizations use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, improve service performance and reduce costs. Splunk Enterprise indexes machine data in real time, enabling multiple roles across the organization—from system administrators to business analysts—to rapidly gain insight from the massive amounts of machine data generated by your environment.

Adopting a cloud strategy enables organizations to increase agility, reduce costs, decrease time to market and empower innovation. Splunk Enterprise is perfect for deploying in a cloud environment, offering enterprise-grade availability and scalability to support mission-critical applications in the cloud.

packaged forms for most operating systems. While all major Splunk components can be run from a single installation on a single cloud instance, they can also run independently from within different cloud instances. Depending on the deployment infrastructure, considerations must also be taken to allocate the proper amount of resources per component type.

Forwarders perform data collection, data forwarding and data load balancing. Low amounts of resources are required to run a forwarder as they typically read and send data with minimal overhead. A Universal Forwarder is a lightweight package of the Splunk software that can perform most, if not all, of the forwarder functionality.

Indexers write the data to a storage device and perform searching on the data. These can be resource intensive and slow (e.g., HDFS, HBase).

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**



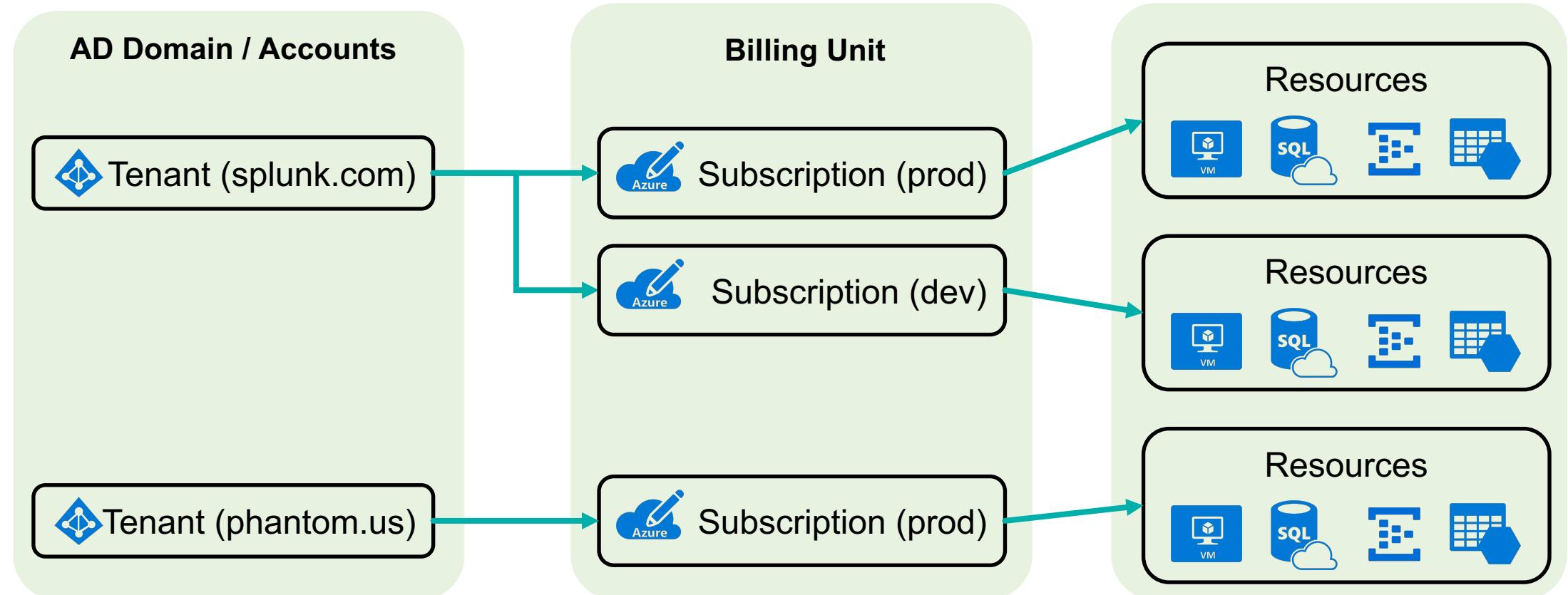
Concepts

Tenants and Subscriptions
AAD Applications
Service Principals
Log Profiles



Azure Organization, Tenants, Subscriptions

Organization (Enterprise Account)



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

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

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.