

Gain Insights into your Microsoft Azure Data using Splunk

Cory Fowler

Microsoft

Jason Conger

Splunk

.conf2016

splunk >

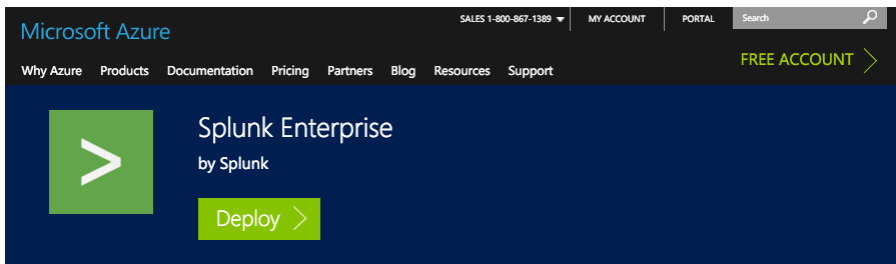
Disclaimer

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 the 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.

Agenda

- Deploying Splunk on Azure
- Collecting Machine Data from Azure
- Splunk Add-ons
- Use cases for Azure Data in Splunk

Splunk available in Azure Marketplace



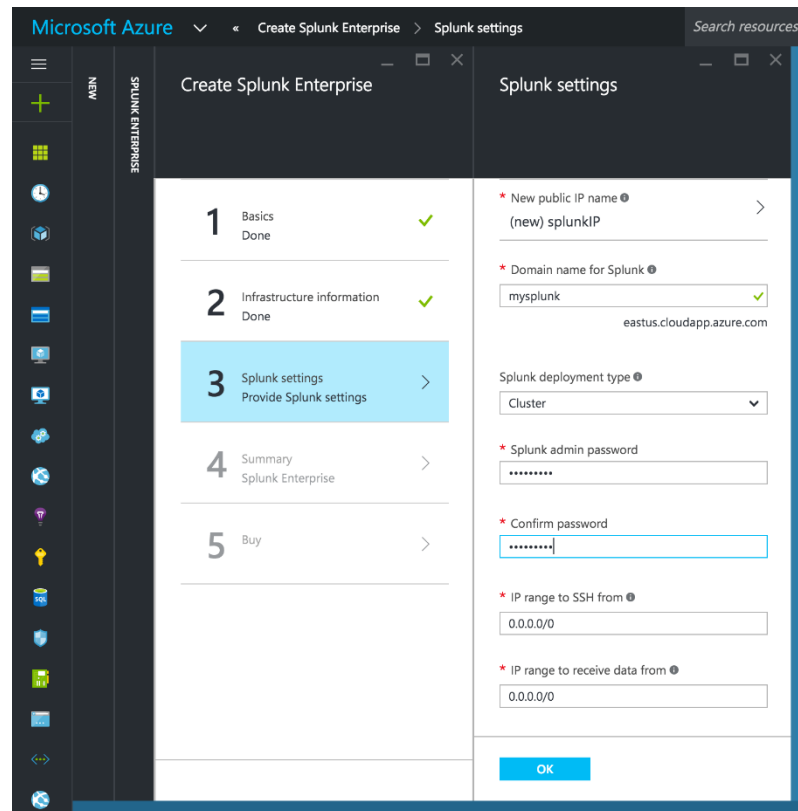
Get Started with Splunk Enterprise on Azure

Now you can get Award-winning Splunk Enterprise with the power of the cloud! Splunk Enterprise on Azure provides all the benefits of the cloud:

- Low total cost of owning & operating an enterprise-grade Operational Intelligence solution
- Faster time-to-value since it is easy & quick to get started on Azure without worrying about lengthy installation and configuration processes
- Easily scale your solution without dealing with months of hardware and capacity planning
- Increased collaboration with access to your data anywhere, anytime and by any authorized user

This Bring Your Own License (BYOL) solution template uses Splunk's 60-day Enterprise Trial license which includes 500MB of indexing per day. [Contact the Splunk sales team online](#) if you need to extend your license or need more volume per day.

Deployment typically takes 10-30 minutes, depending on the deployment size requested. Once complete, Splunk Enterprise can be accessed at <https://{domainName}.{location}.cloudapp.azure.com>. For example, if the deployment is created in the West US region with parameter domainName set to "example", Splunk Enterprise can be accessed at <https://example.westus.cloudapp.azure.com> using Splunk username admin and configured Splunk password.



Splunk in Azure Marketplace

What can Splunk solution template do for you?

- **Accelerates** deployment time down to minutes
- **Abstracts away** details of configuring distributed Splunk
- Incorporates Splunk **best practices** for operations and administration
- **Extensible** and **customizable** templates to fit custom needs

<https://azure.microsoft.com/en-us/marketplace/partners/splunk/splunk-enterprisebyol/>

<https://www.splunk.com/pdfs/technical-briefs/deploying-splunk-enterprise-on-microsoft-azure.pdf>

Azure Marketplace Demo

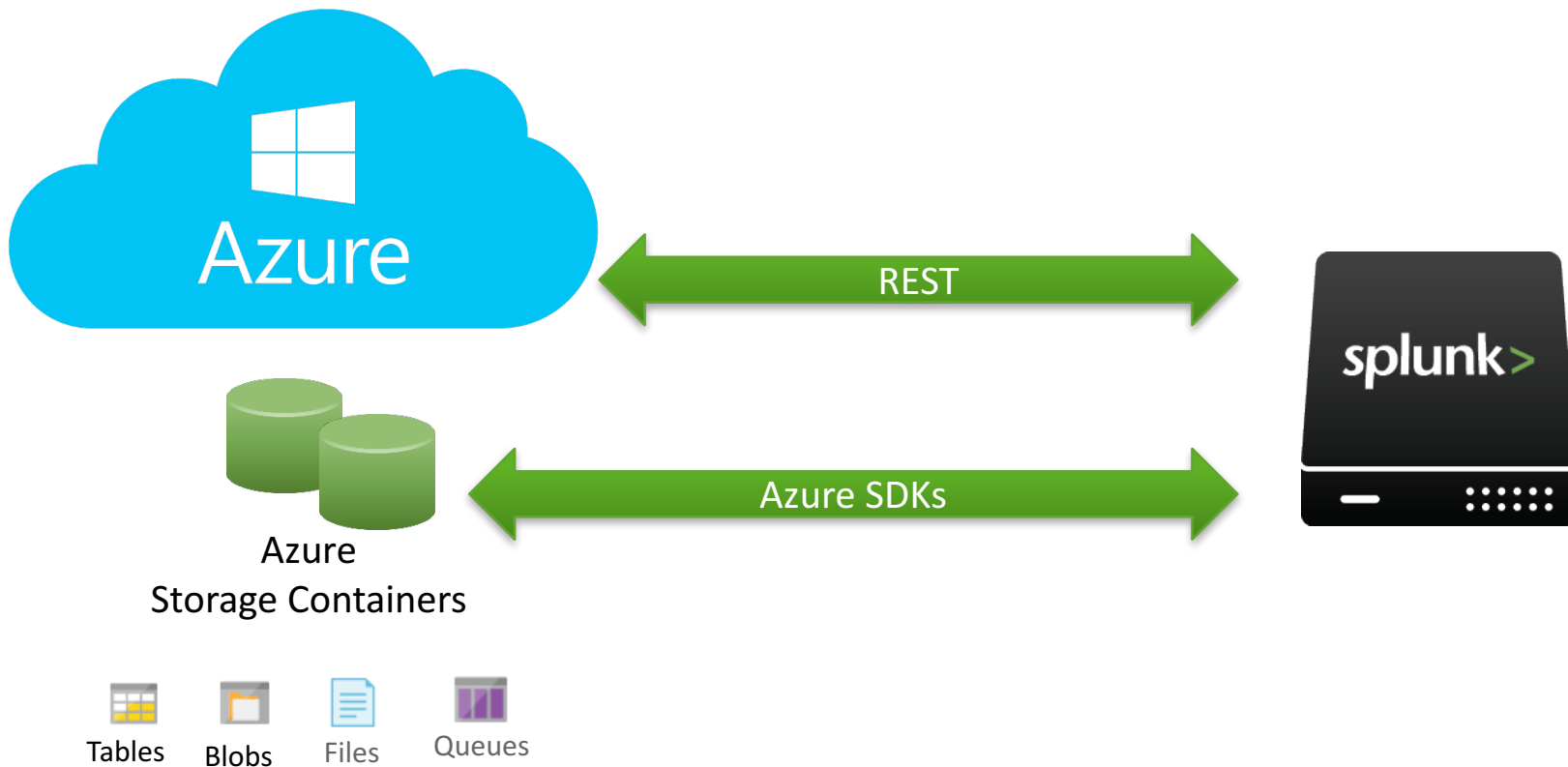
.conf2016

Collecting Machine Data from Azure



.conf2016

How we collect Azure Data



Azure Storage Table Data

PartitionKey	RowKey	Timestamp	MDSHash	N	PhysicalTableName	Reserved1	Reserved2	Reserved3	Schema
0000000000000000...	WADMetricPT...	4/15/2016 6:01:...	23b10029922d0...	0000000000000000...	WADMetricPT1HP10DV2S				<MdsConf
0000000000000000...	WADMetricPT...	4/15/2016 7:22:...	23b10029922d0...	0000000000000000...	WADMetricPT1MP10DV2S				<MdsConf
0000000000000000...	LinuxCpuVer2v0...	1/28/2016 10:16:...	b1ab5b6501e53...	0000000000000000...	LinuxCpuVer2v0				<MdsConf
0000000000000000...	WADWindowsE...	4/15/2016 4:25:...	4906b5683cf854...	0000000000000000...	WADWindowsEventLogsTable				<MdsConf
0000000000000000...	WADWindowsE...	4/14/2016 3:43:...	5faf8d86c81da5...	0000000000000000...	WADWindowsEventLogsTable				<MdsConf
0000000000000000...	LinuxDiskVer2v0...	1/28/2016 10:16:...	b32f36218d3e15...	0000000000000000...	LinuxDiskVer2v0				<MdsConf

PartitionKey	RowKey	Timestamp	PreciseTimeStam	DeploymentId	Role	RoleInstance	Level	ProviderGuid	EventId	Pid
06358599150000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599150000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358599156000...	2350e8fc-c9dc-...	12/17/2015 11:2...	12/17/2015 11:2...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	3		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716
06358610358000...	2350e8fc-c9dc-...	12/19/2015 6:34...	12/19/2015 6:33...	2350e8fc-c9dc-...	aaS	_SplunkJCVMO1	2		64000	1716

Azure Storage Blob Data

The image displays three sequential screenshots of the Azure Storage Explorer interface, illustrating the navigation through a storage container hierarchy. Each screenshot shows a search bar at the top with the placeholder text "Search blobs by prefix (case-sensitive)" and a table of blobs below.

gsawp Container

NAME	MODIFIED	BLOB TYPE	SIZE
splunkgsa			-
SPLUNKGSA			-

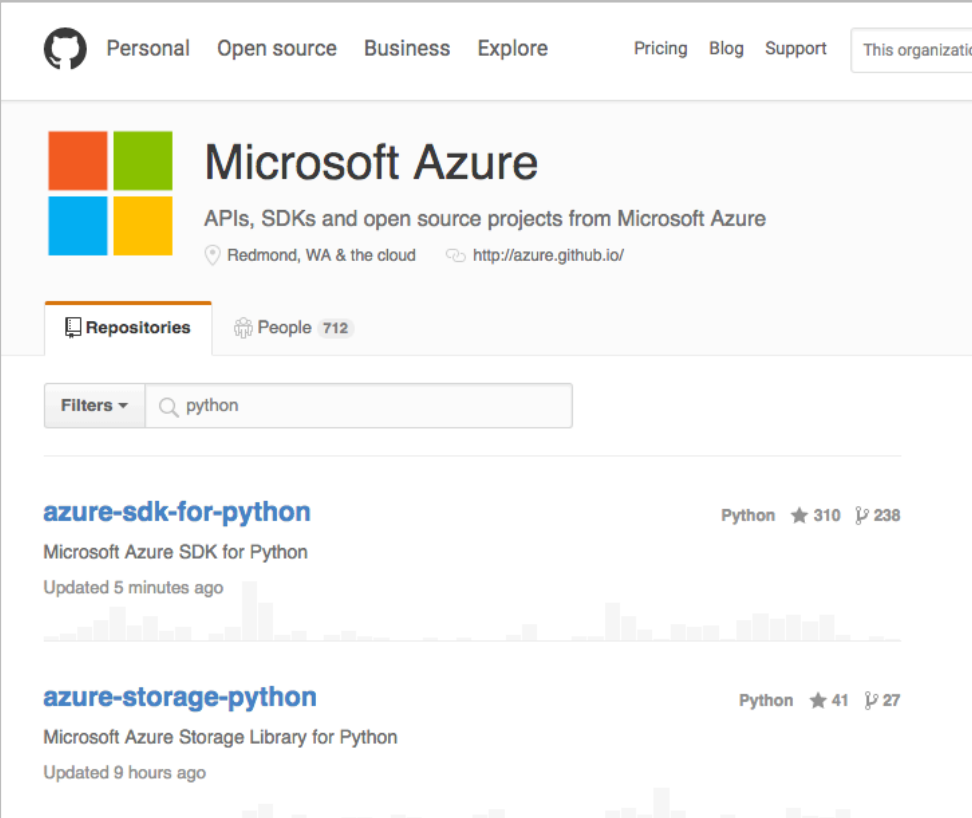
SPLUNKGSA Folder

NAME	MODIFIED	BLOB TYPE	SIZE
2016			-

2016 Folder

NAME	MODIFIED	BLOB TYPE	SIZE
05			-

Microsoft Azure Python SDKs



The screenshot shows the GitHub profile for the Microsoft Azure organization. At the top, there are navigation links: Personal, Open source, Business, Explore, Pricing, Blog, Support, and This organization. The organization's name is Microsoft Azure, with a description: APIs, SDKs and open source projects from Microsoft Azure. The location is Redmond, WA & the cloud, and the website is http://azure.github.io/. Below this, there are tabs for Repositories and People (712). A search bar contains the text 'python'. Two repositories are listed:

- azure-sdk-for-python**: Python, 310 stars, 238 forks. Description: Microsoft Azure SDK for Python. Updated 5 minutes ago.
- azure-storage-python**: Python, 41 stars, 27 forks. Description: Microsoft Azure Storage Library for Python. Updated 9 hours ago.

Demo



.conf2016

Splunk Add-ons for Microsoft Azure Data

.conf2016

Demo



.conf2016

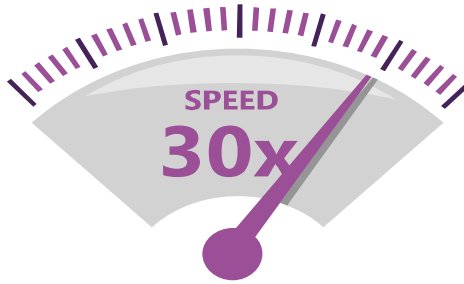
Azure Functions

.conf2016

What is Serverless?



Server Abstraction



Event-driven scale

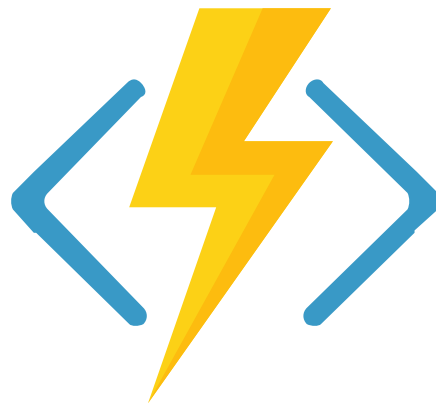


Sub-second billing

Azure Functions

Process events with Serverless code.

- Make composing Cloud Apps insanely easy
- Develop Functions in C#, Node.js, F#, Python, PHP, Batch and more
- Easily schedule event-driven tasks across services
- Expose Functions as HTTP API endpoints
- Scale Functions based on customer demand
- Easily integrate with Workflows

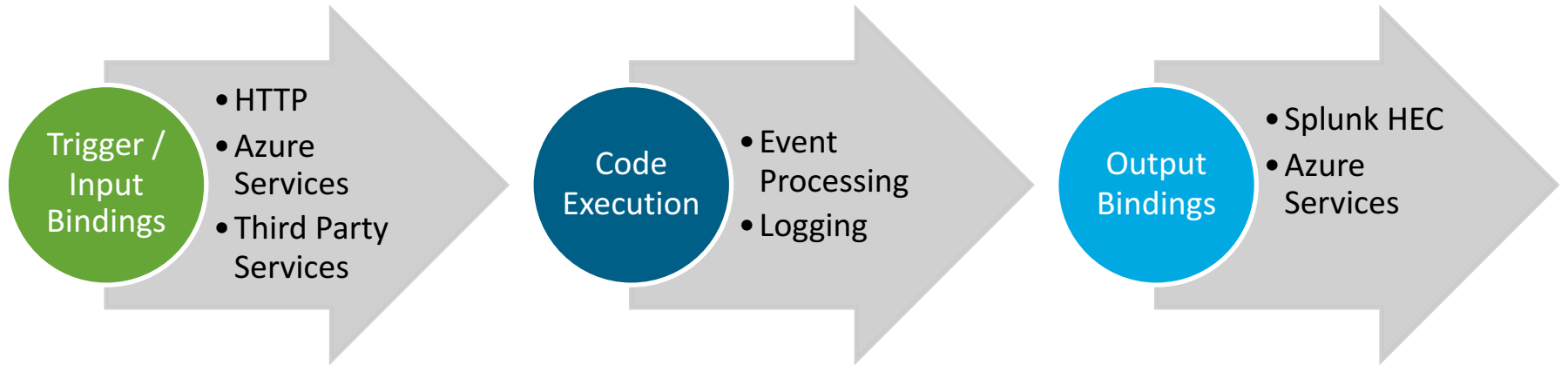


Demo



.conf2016

Azure Functions + Splunk



Demo



.conf2016

Use Cases (IT Ops)

- Server and application diagnostics
- Container logs
- CDN logs
- IoT data
- Application logs
- Windows Event logs
- IIS logs
- Storage metrics
- Management data (access logs, billing, AD logs)
- Network security group and load balancer logs

Use Cases (Security)

- Audit
- Compliance
- Unauthorized access attempts
- Resource change tracking
- Network configuration changes
- Vulnerabilities in hosts or firewalls

References

- [Splunk on the Azure Marketplace](#)
- [Splunk Add-on for Microsoft Cloud Services](#)
- <http://blogs.splunk.com/2016/04/18/announcing-splunk-add-on-for-microsoft-cloud-services/>
- <http://blogs.splunk.com/2016/02/18/announcing-splunk-enterprise-in-microsoft-azure-marketplace/>
- <http://blogs.splunk.com/2016/03/15/splunking-microsoft-azure-data/>
- <http://blogs.splunk.com/2016/03/28/splunking-microsoft-azure-audit-data/>

THANK YOU

.conf2016