



```
KQL /> AzureAnnouncements  
      | where conference == 'Ignite'  
      | project Description, Demo
```

Maarten Goet (MVP, RD)



MVP

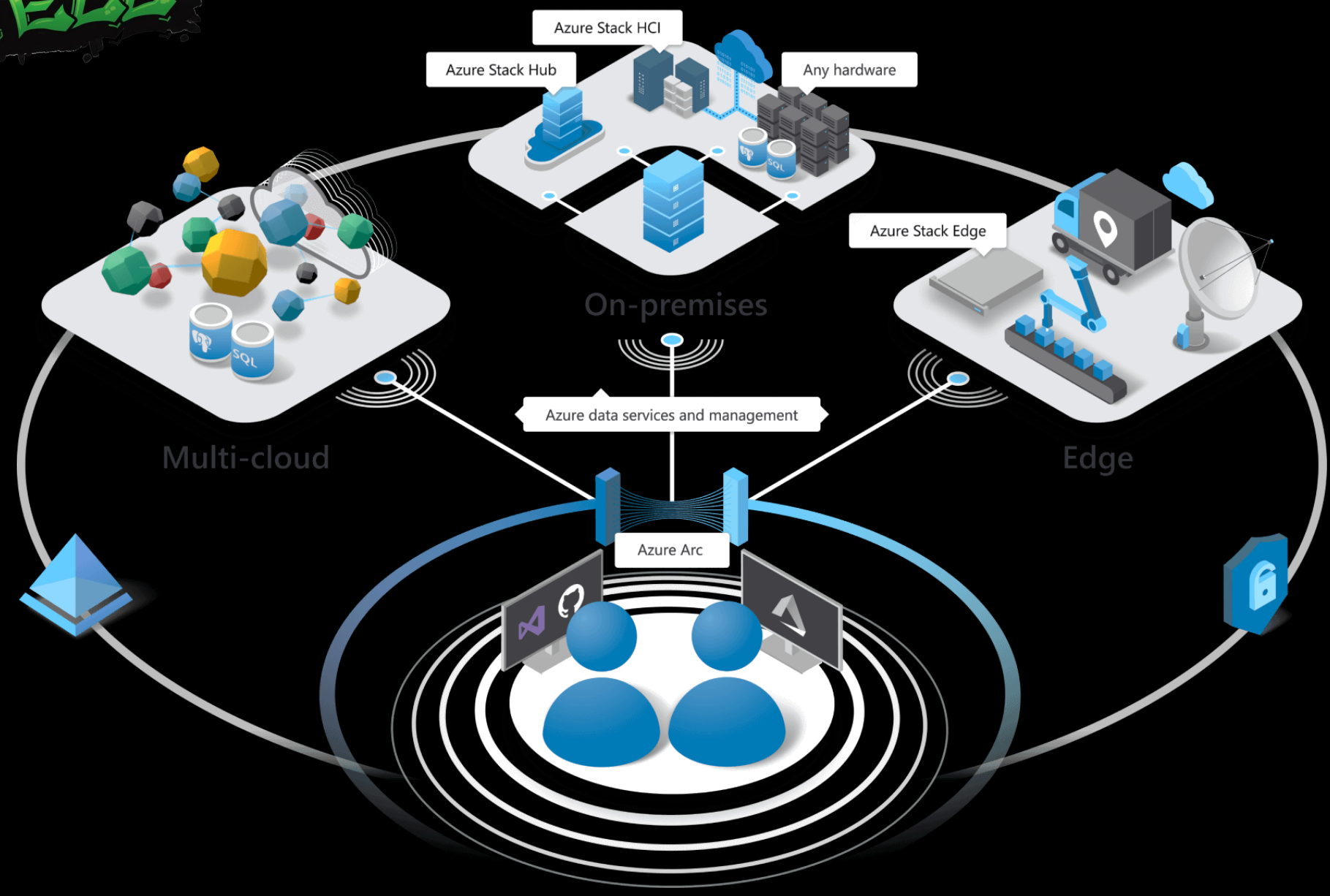
RD



Agenda

- Azure Arc
- Azure Bastion
- Azure Stack
- Azure Firewall
- Azure Cloud Shell
- Azure Governance
- Azure Monitor
- Azure Security Center
- Azure Kubernetes Service
- Azure Sentinel





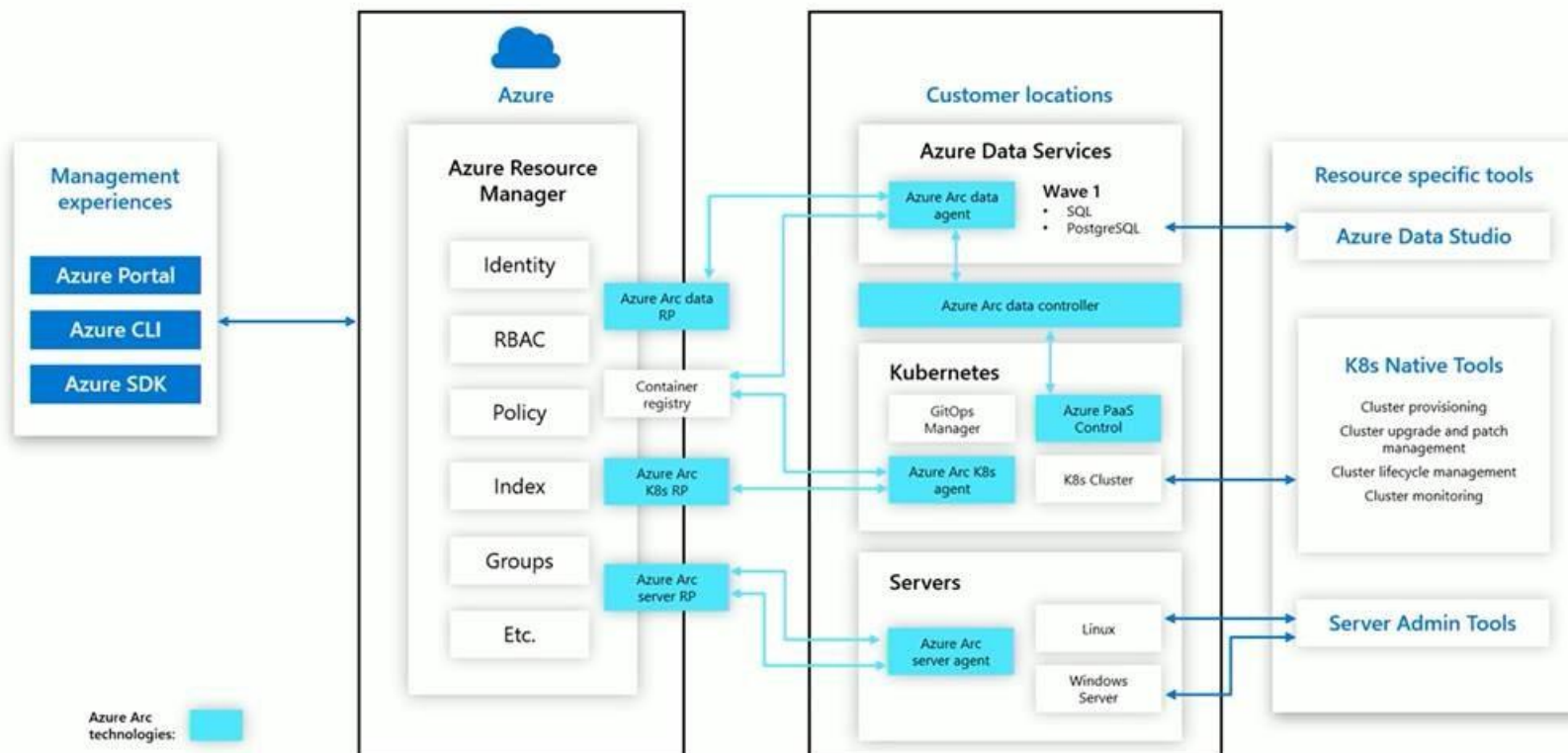
Azure Arc



- Deployment of Azure services anywhere
- Extend Azure management to any infrastructure
- Register a Linux or Windows VM, or Kubernetes cluster
- Two services in preview
 - SQL Managed Instance
 - PostgreSQL Hyperscale
- Applications deployed as microservices to Kubernetes
- Use Azure Security Center to ensure compliance
- Enable preview via Azure cloud shell
 - `az account set --subscription "{Your Subscription Name}"`
 - `az provider register --namespace 'Microsoft.HybridCompute'`
 - `az provider register --namespace 'Microsoft.GuestConfiguration'`

Tools and

Azure Arc



ore...

d inventory
roups | Tags

compliance
Blueprints

local tools

Azure Data Studio
K8s Native Tools
Windows Admin Center
System center suite
Server management tools



Generate script

Script

Run the following script on any machine you're onboarding to Azure Arc. The script can also onboard multiple machines. Note that those machines will all be assigned to the same subscription, resource group, and Azure region. [Learn more](#)

```
# Download the package
Invoke-WebRequest -Uri https://aka.ms/AzureConnectedMachineAgent -OutFile AzureConnectedMachineAgent.msi

# Install the package
msiexec /i AzureConnectedMachineAgent.msi /l*v installationlog.txt /qn | Out-String

# Run connect command
& "$env:ProgramFiles\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "demo-hybridrg" --tenant-id
"72f988bf-86f1-41af-91ab-2d7cd011db47" --location "westeurope" --subscription-id "c8123574-273e-4755-93b2-1cc287f99223"
```

Download









< Previous



server01

Tools



-  Scheduled tasks
 -  Services
 -  Storage
 -  Storage Migration Service
 -  Storage Replica
 -  System Insights
 -  Updates
- Extensions
-  Azure Security Center

Settings

Settings

- General
- Environment variables
 - Azure Arc for Servers**
 - Power configuration
 - Remote Desktop
 - Role-based Access Control



Azure Arc for Servers PREVIEW ⓘ

Inventory your on-premises servers in Azure, organize and manage servers using tags, govern servers using Azure policy, control access using Azure RBAC, and enable additional services from Azure. Azure Arc for Servers comes at no additional cost.

[Get an overview of Azure Arc for Servers](#) 

[Sign in to Azure](#)



Microsoft Azure

Search resources, services, and docs (G+)



Dashboard > Machines - Azure Arc

Machines - Azure Arc

MSA - PREVIEW



+ Add Edit columns Refresh Assign tags

Subscriptions: All 5 selected – Don't see a subscription? [Open Directory + Subscription settings](#)

Filter by name... All subscriptions All resource groups All locations All tags No grouping

1 items

<input type="checkbox"/> Name ↑↓	Status	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Type ↑↓	
<input type="checkbox"/> Server01	Connected	azurearc-rg	West Europe	tm01 Azure MSDN Pre...	Machine - Azure Arc	...

Azure Arc



“Why Azure Arc Is A Game Changer”

<https://www.forbes.com/sites/janakirammsv/2019/11/05/why-azure-arc-is-a-game-changer-for-microsoft>

- vs AWS Outposts
- vs Google Anthos

Azure Bastion



- Private and fully managed RDP and SSH access
- Bastion Host in your subscription
- Provisioned directly in your VNET
- HTML5 web client
- Using SSL through public IP address
- **General Available**

A screenshot of the "Connect to virtual machine" dialog box in the Azure portal. The dialog has a title bar with a close button. Below the title bar is an orange banner with a warning icon and the text "To improve security, enable just-in-time access on this VM. →". Underneath the banner are three tabs: "RDP", "SSH", and "BASTION". The "BASTION" tab is selected and highlighted with a red rectangular box. Below the tabs, there is instructional text: "To connect to your virtual machine over the web, enter login credentials and click connect (opens a new browser window)." followed by a small "o" icon. There are two input fields: "Username" with the value "testuser" and a green checkmark, and "Password" with masked characters "*****" and a green checkmark. Below these fields is a checkbox labeled "Open in new window" which is checked. At the bottom is a blue "Connect" button.



Azure Stack



- Extending Azure to everywhere you run your business
- Azure Stack is now Azure Stack Hub
- Windows Server Hyper-V is now Azure Stack HCI
- Introducing Azure Stack Edge
- Azure Arc extends to Azure Stack Hub and HCI
- Azure Kubernetes Services (AKS) is now GA on Azure Stack Hub
- Windows Virtual Desktop (WVD) preview on Azure Stack Hub

Azure Stack rugged series



Azure Firewall

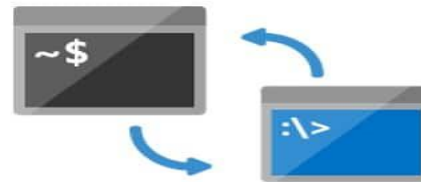
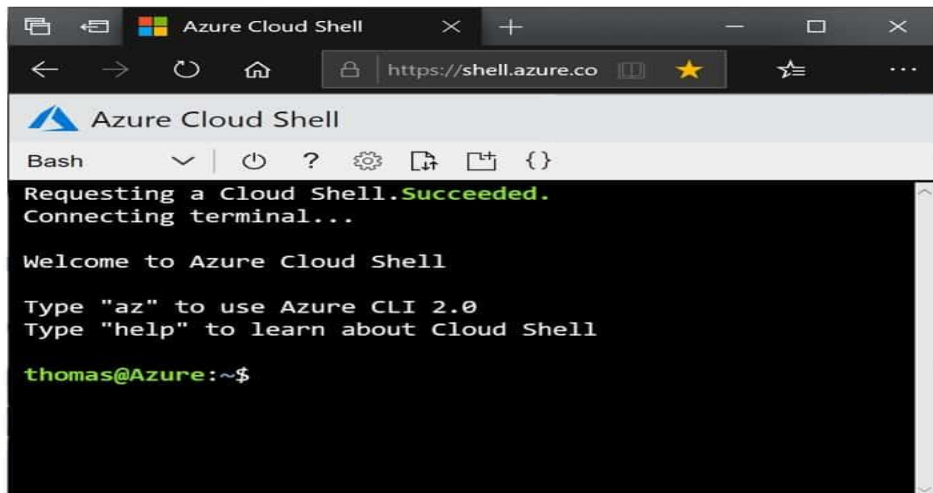


- Azure Firewall Manager is now in preview
- Central network security policy and route management
- Secured Virtual Hubs
- Register the network provider:
 - `Register-AzProviderFeature -FeatureName AllowCortexSecurity -ProviderNamespace Microsoft.Network`
- Migrate your Azure Firewall to :
 - `https://github.com/wortell/azure/blob/master/MigrateAzureFirewallConfigToAzureFirewallPolicy.ps1`

Azure Cloud Shell



- Browser-accessible, pre-configured shell experience
- Manage Azure resources
- **New:** choose region where to store your data
- **New:** integration in Microsoft 365 admin center



- Settings
- Domains
- Microsoft Search
- Services & add-ins
- Security & privacy
- Organization profile
- Partner relationships
- Setup
- Reports

Office 365

☒ The new admin center

Domains

[+ Add domain](#) [Buy domain](#) [Refresh](#)

Domain name	Status	Choose columns
[REDACTED]	Healthy	
[REDACTED]	Incomplete setup	
[REDACTED]	Possible service issues	

PowerShell

Azure: /

PS Azure:\> Get-AzureADTenantDetail

ObjectId	DisplayName	VerifiedDomain
923712ba-[REDACTED]-09d0684d0cfb	Office 365	[REDACTED]

Azure: /

PS Azure:\> Get-AzureADDomain

Name	AvailabilityStatus	AuthenticationType
[REDACTED]		Managed
microsoft.com		Managed
[REDACTED]		Managed
[REDACTED]		Managed
[REDACTED]		Managed
[REDACTED]		Managed
[REDACTED]		Managed
[REDACTED]		Managed
[REDACTED]		Managed

Azure: /

PS Azure:\>

[Need help?](#)

Azure Governance



- Test your ARM template
 - `test-aztemplate`
- ARM template for VS code extension updated
 - Intellisense improvements
 - `//` and `/* */` comments
 - Open-source snippets ([aka.ms/ARMTemplateSnippets_](https://aka.ms/ARMTemplateSnippets)
 - [\[more\]](#)
- **What-If** is coming to ARM templates
 - Pre-deployment analysis

How What-If works

ON THAT RESOURCE, WHETHER IT'S AN
UPDATE, A CREATION, A


ARM Template

+

Target scope
Parameters
Mode (Incremental,
Complete)



Predicted **desired**
state

+

GETs on all resource
for **current** state

GET on resource1

...

GET on resourceN



Noise
Suppression
service



Calculated diff

Resource1 → UPDATE

Resource2 → DELETE

ResourceN → IGNORE





whatIfDemo.json ×

{ } extensionDemo.json

Press **Esc** to exit full screen

1: pwsh



whatIfDemo.json

```
11 "location": "[resourceGroup()
12 "tags": {
13   "displayName": "virtualNe
14 },
15 "properties": {
16   "addressSpace": {
17     "addressPrefixes": [
18       "10.0.0.0/15"
19   ]
20 },
21 "subnets": [
22   /*
23   {
24     "name": "Subnet-1
25     "properties": {
26       "addressPrefi
27   }
28   },
29   */
30   {
31     "name": "Subnet-2
32     "properties": {
33       "addressPrefi
```

- Delete
- + Create
- ~ Modify

The deployment will update the following scope:

Scope:

/subscriptions/e93d3ee6-fac1-412f-92d6-bfb379e81af2/resourceGroups/test-005

~ Microsoft.Network/virtualNetworks/virtualNetwork1

- properties.enableDdosProtection: false
- properties.enableVmProtection: false

~ properties.addressSpace.addressPrefixes: [

- 0: "10.0.0.0/16"
- + 0: "10.0.0.0/15"

]

~ properties.subnets: [

- 0:

name: "Subnet-1"
properties.addressPrefix: "10.0.0.0/24"

]

Resource changes: 1 to modify.

PS C:\Users\alfran\OneDrive - Microsoft\Desktop\ignite2019>

Azure Monitor



- Monitor containers anywhere
- Prometheus integration
- Network Insights is now in preview
 - Troubleshoot networking issues faster
 - Process NSG logs at 10-minute interval now
- Workbooks
- Azure Monitor for Cosmos DB
- Capacity-based pricing for Log Analytics

Search (Ctrl+ /)

- Overview
- Activity log
- Alerts
- Metrics
- Logs
- Service Health
- Workbooks (preview)
- Insights
 - Applications
 - Virtual Machines (preview)
 - Storage Accounts (preview)
 - Containers
 - Networks (preview)
 - More
- Settings
 - Diagnostics settings
 - Autoscale
- Support + Troubleshooting
 - Usage and estimated costs
 - Advisor recommendations

Refresh | Feedback

Environment: Azure Stack (Preview)

- Azure
- Azure Stack (Preview)
- Non-Azure (Preview)
- All

Cluster Status

2

Total

Critical

Warning

Unknown

Healthy

0

Non-monitored

Monitored clusters (2)

Non-monitored clusters (0)

Search by name...

CLUSTER NAME	CLUSTER TYPE	VERSION	STATUS	↑ ↓ NODES	USER PODS	SYSTEM PODS
azure-stack-k8smi00	AKS-Engine, AzureStack	1.12.8	Critical	2 / 2	6 / 8	12 / 12
jadarsie-ci3	AKS-Engine, AzureStack	1.12.8	Warning	3 / 3	23 / 25	15 / 15





Subscription == 5 Selected

Resource Group == All

Type == All

Fetched both alerts and health

Resource Types

Show health ☒ Available Degraded ☒ Unavailable ☒ Unknown ☒ Health not supported



Network security groups(407)



Public IPs(393)



Network interfaces(368)



Virtual networks(253)



Load balancers(28)



Route tables(9)



Connections(29)



Application gateways(4)



ExpressRoute circuits(5)



Virtual network gateways(26)

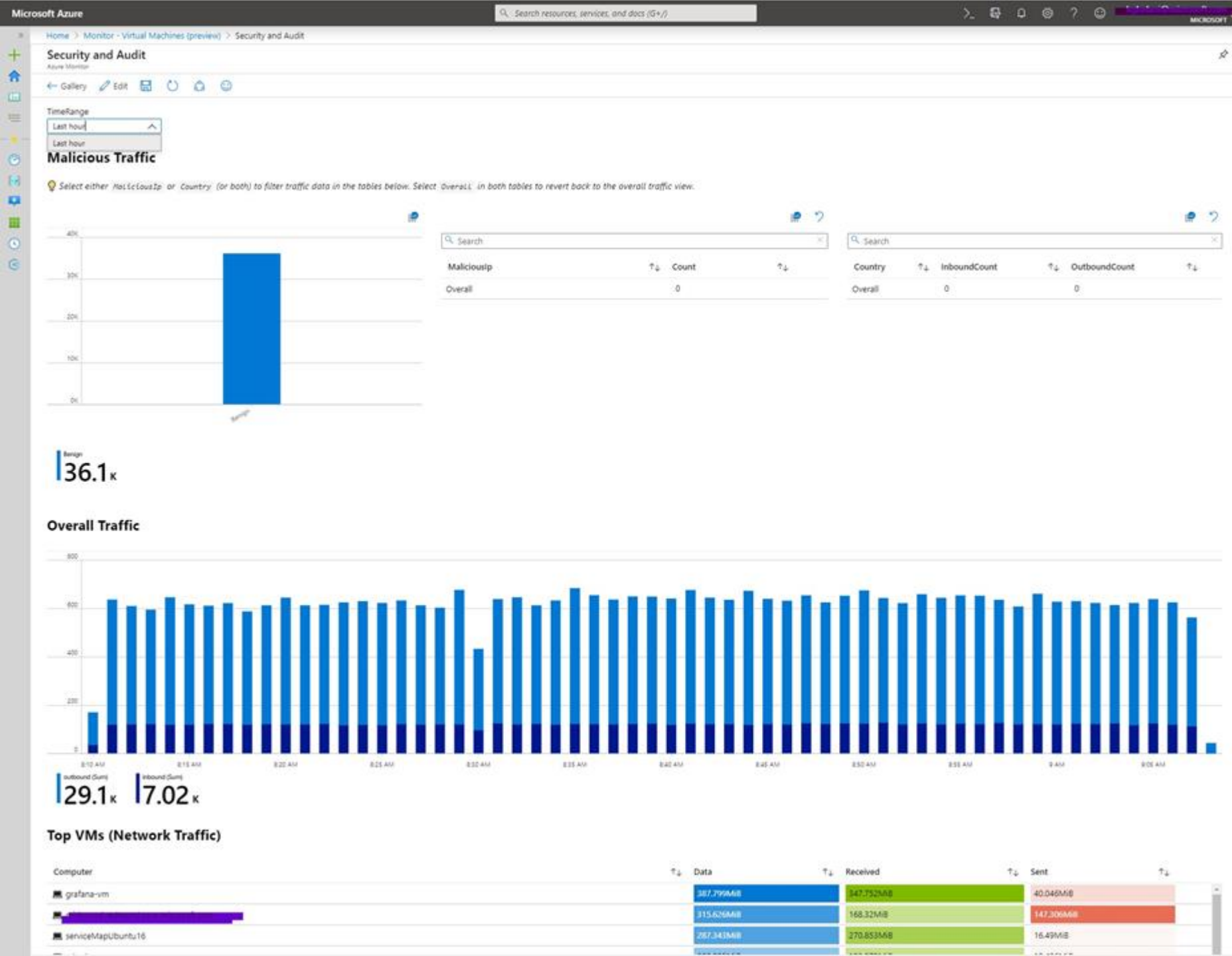


Local network gateways(5)



Virtual hubs(1)





Azure Security Center



- Secure Score enhancements
- Continuous exporting & reporting
- Custom policies in preview
- Additional regulatory compliance standards
 - NIST SP 800-53 R4, SWIFT CSP CSCF v2020, Canada Federal PBMM, UK Official, UK NHS, Azure CIS 1.1.0
- Vulnerability Management on Servers
 - Qualys-based
- Automatic onboarding of EC2 VM's on AWS in preview
- Onboard VMs to ASC using Windows Admin Center
- Logic Apps connector



Azure Security Center community

What is it?

Open source community facilitating collaboration among customers and partners through GitHub. Visit our [GitHub repository](#) to explore sample content for playbooks and automation scripts, remediation templates for recommendations, custom recommendations and more.

How does it work?

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center. To get started, visit the community [GitHub](#) (you may need to create a GitHub account)

These are the types of content you can find in the community:



Remediation templates

Access the template deployment scripts Security Center uses as part of its recommendation remediation platform, and try out new remediation templates before they are integrated into the product.



Programmatic tools

Automate and configure Security Center with programmatic scripts shared by the community, in PowerShell, CLI, and other languages. Use custom policy definitions to manage Security Center at scale.



Additional security recommendations

Create your own security recommendations with custom logic, by creating custom Policy and onboard it into Azure Security Center. Contribute and use custom recommendations by the community.



Logic App playbooks (coming soon)

Explore the ecosystem of Azure Logic Apps connectors to customize automation in. Import playbooks from the community to use them as customized automation.

[Go to community GitHub](#)

Azure Kubernetes Service



- **BREAKING NEWS:** ATP for Azure Kubernetes
 - Discover managed AKS instances
 - Recommend best practices in AKS
 - Threat detection: "a privileged container detected"
 - Container scanning in Azure Container Registry (vulnerability management)
- Find it in Azure Security Center
- Use ASC to get these AKS ATP signals into Azure Sentinel



Azure Sentinel



- More connectors
 - ZScaler
- LiveStream now in preview
- Connect threat intelligence sources using STIX/TAXII
- Automatically detonate URLs to speed investigation
- Defender ATP connector in preview
 - Alerts only
- Coming soon
 - New Jupyter notebooks experience

Azure Sentinel - Data connectors

Selected workspace: 'CyberSecurityDemo'

Search (Ctrl+/)

Refresh

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks

Configuration

Data connectors

Analytics

Playbooks

Community

Workspace settings











32
Connectors21
Connected1
Coming soon

Search by name or provider

PROVIDERS : All

DATATYPES : All

Status ↑↓ Connector name

	Microsoft
	Microsoft Defender Advanced Threat Protection (Preview) Microsoft
	Microsoft web application firewall (WAF) Microsoft
	Office 365 Microsoft
	Palo Alto Networks Palo Alto Networks
	Palo Alto Networks New Palo Alto Networks
	Security Events Microsoft
	Threat Intelligence Platforms (Preview) Microsoft
	Windows Firewall Microsoft
	Zscaler Zscaler



Zscaler

CONNECTED
STATUSZSCALER
PROVIDER21 SECONDS A...
LAST LOG RECEIVED

Description

The Zscaler data connector allows you to easily connect your Zscaler Internet Access (ZIA) logs with Azure Sentinel, to view dashboards, create custom alerts, and improve investigation. Using Zscaler on Azure Sentinel will provide you more insights into your organization's Internet usage, and will enhance its security operation capabilities.

10/18/19, 09:46 AM

Related content

2

Workbooks

2

Queries

Data received

[Go to log analytics](#)[Open connector page](#)

Home > Azure Sentinel - Hunting

Azure Sentinel - Hunting

Selected workspace: 'RedmondSentinelDemoEnvironment'

Search (Ctrl+/)

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks

Notebooks (Preview)

Configuration

Data connectors

Analytics

Playbooks

Community

Workspace settings



Refresh

Last 24 hours

Live stream

88
Total Queries4
My Bookmarks14
Live Stream Results

MITRE ATT&CK™

(16) (20) (14) (10) (1) (13) (7) (7) (5) (10) (14) (11)

LEARN MORE
About hunting

Queries Live Stream Bookmarks

Search queries

STATUS: Paused, Running

St...	Query	Results	Last Result	Last Result Time	
RU...	Threat Intel map IP entity to ZS...	12	6	01:58 PM	
RU...	Suspicious Powershell Comman...	2	0	02:11 PM	

New Live Stream - failed login attempts

Last Hit Results Data Source

Query

```
SecurityEvent  
| where AccountType == 'User' and EventID == 4625  
| project TimeGenerated, Computer, Account, EventID
```

View query results >

Pause

Open live stream



Azure Sentinel - Notebooks (Preview)

Selected workspace: 'CyberSecurityDemo'

Search (Ctrl+J)

[Clone Notebooks](#) [Go to your Notebooks](#) [Refresh](#) **4**
Total notebooks **0**
Coming soon[LEARN MORE](#)
[Learn more about Azure Notebooks](#)

Search by name or provider

PROVIDERS: Microsoft

Notebook name ↑ ↓

Status

 Guided Hunting - Office 365 Explorer Microsoft	Last version update: 04/23/19, 05:00 PM Hunting
 Guided Hunting - Windows Host Explorer Microsoft	Last version update: 04/22/19, 05:00 PM Hunting
 Guided Investigation - Anomaly Lookup Microsoft	Last version update: 07/30/19, 05:00 PM Investigation
 Guided Investigation - Process Alerts Microsoft	Last version update: 04/22/19, 05:00 PM Investigation




Guided Hunting - Office 365 Explorer

 **MICROSOFT**
CREATED BY **6 MONTHS AGO**
LAST VERSION UPDATE

Description

Brings together a series of queries and visualizations to help you investigate the security status of Office 365 subscription and individual user activities.

Required data types

 OfficeActivity 10/18/19, 08:36 AM

Data sources

Office 365





Threat Intelligence - TAXII (Preview)

Connected

STATUS

Microsoft

PROVIDER

--

LAST LOG RECEIVED

Description

Azure Sentinel integrates with TAXII 2.0 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators from TAXII 2.0 servers to Azure Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Last data received

--

Related content



0



2

Workbooks

Queries

Data received

[Go to log analytics](#)

100

80

60

40

20

0

September 8

September 15

September 22

September 29

Total data received

0

Data types

ThreatIntelligenceIndicator --

[Instructions](#)[Next steps](#)

Prerequisites

To integrate with Threat Intelligence - TAXII (Preview) make sure you have:



Workspace: read and write permissions are required.



TAXII 2.0 Server: TAXII 2.0 Server URI and Collection ID are required



Configuration

Configure TAXII servers for ingesting STIX 2.0 threat indicators to Azure Sentinel

You can connect your TAXII servers to Azure Sentinel using the built-in TAXII client.

Enter the server, collection and authentication (if available) information and click 'Add' to configure a TAXII server.

* Friendly Name (for server)

* Server URI

* Collection ID

Username

Password

[Add](#)

List of configured TAXII 2.0 servers


FRIENDLY NAME

TAXII SERVER

COLLECTION ID

LAST INDICATOR RE...



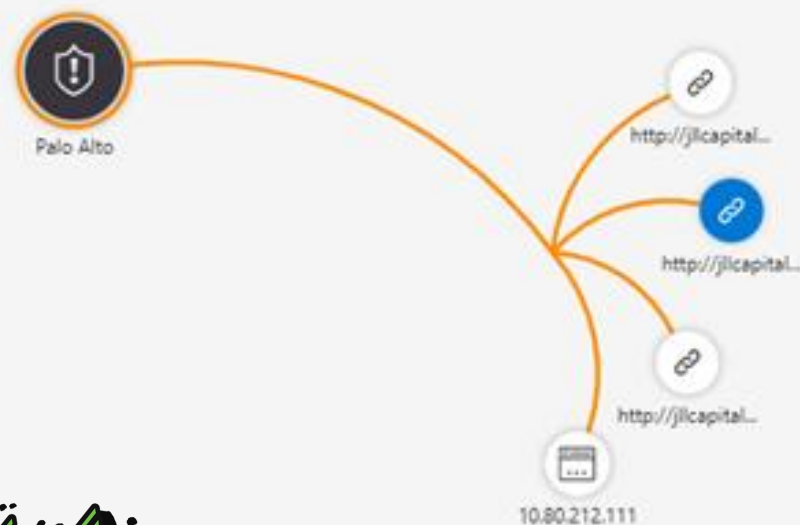
 Palo Alto Alert Rule
Incident

 Medium
Severity

 New
Status

 Unassigned
Owner

 9/16/2019, 10:15:29 AM
Last incident update time



ENTERPRISE SECURITY
WORTTELL

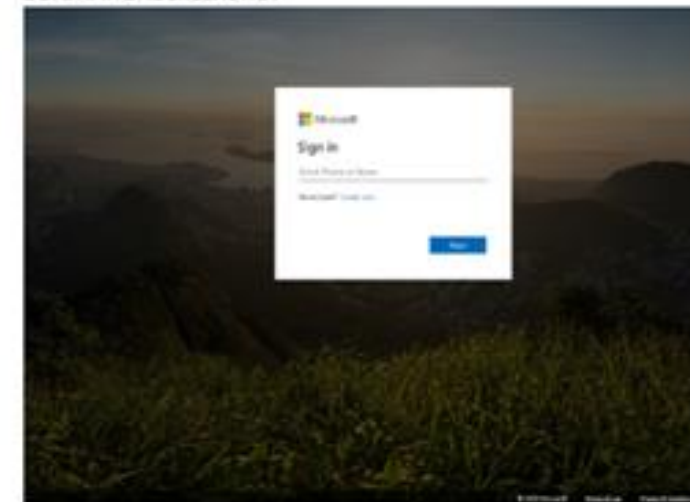


<http://jllcapitalsinc.com/ofh>

DETONATIONVERDICT
BAD

DETONATIONFINALURL
http://jllcapitalsinc.com/ofh/login.php?i=_JeHFUq_VJOXX0QWHt...

DETONATIONSCREENSHOT



URL
<http://jllcapitalsinc.com/ofh>

FRIENDLYNAME
<http://jllcapitalsinc.com/ofh>

Microsoft Defender ATP



- EDR capabilities for Mac now in preview
 - Live response
 - Remediate options
 - Rich investigation experience
- Linux agent announced



Search results > -MacBook-Pro



-MacBook-Pro

- Domain
- Workgroup
- OS
 - macOS x64
 - Build 1634819
- Risk level ⓘ
 - Low
- Exposure level ⓘ
 - No data available
- Health state
 - Active
- Active alerts ⓘ
 - 12
- Active incidents
 - 2
- Azure ATP alerts

Manage Tags Initiate Automated Investigation Initiate Live Response

Active alerts 180 days Logged on users 30 days

Risk level: **Low**
12 active alerts
in **2 incidents**



1 logged on user
Most frequent: dan
Least frequent: dan

[See all users](#)

Alerts Timeline

Customize columns 30 items

✓	Title
	Microsoft Defender ATP detected 'Generic.Application.Powersploit.Mon
	Microsoft Defender ATP detected 'Generic.Application.Powersploit.Mon
	Microsoft Defender ATP detected 'W97M.Downloader.CZI' malware
	Microsoft Defender ATP detected 'W97M.Downloader.CZI' malware
	Microsoft Defender ATP detected 'VB.Chronos.7.Gen' malware

Other



- Customer Lockbox for Microsoft Azure beyond virtual machines
- Release of Microsoft Secure Code Analysis toolkit
- Azure Disk Encryption in more places, and more services offering customer-managed keys
 - Azure Event Hubs, Azure Managed Disks, Power BI
- New Azure policies to manage certificates across your organization
 - fi: Expiry Policy: Flag certificates that are (or are not) renewed within "X" number of days of their expiry date.
- Azure Key Vault Virtual Machine extension now generally available
- Free Azure managed certificates for your domains on Azure



Win een
Ninjacat t-shirt





<https://security.wortell.nl>