

Azure Security Overview

Maxime Coquerel - MVP Azure



Disclaimer

“Tous les posts de ce blog ne reflètent que mon opinion et non celle de mes employeurs et clients.”

Speaker

Maxime Coquerel

Cloud Security Specialist

Email : max.coquerel@live.fr

Blog : zigmax.net (Since 2012)

Github : <https://github.com/zigmax>

Twitter : @zig_max

Open Source Contributor (OpenStack).



Session Agenda / Goal

- Introduction
- Compliance
- Azure Network Security
- Azure Key Vault
- Azure WAF
- Azure Security Center
- Azure SIEM
- Conclusion

“Global overview of Azure Security capabilities with a focus on Azure Security Center.”



How A 'Publicly Accessible Cloud Server' Exposed 198 Million US Voters' Data Used By President Donald Trump Team

By João Marques Lima | PUBLISHED: 06:45, 26 June, 2017 | UPDATED: 00:24, 26 June, 2017



Data repository on an AWS S3 bucket containing names, ages, addresses and phone numbers was accessible to anyone with an internet connection for 12 days.

The Azure Periodic Table

Explore the power and possibilities of Azure

Explore the power and possibilities of Azure

 SECURITY CENTER													 AZURE IOT HUB
 LINUX HUB	 VIRTUAL MACHINES							 AZURE AD B2C	 AZURE AD	 AZURE AD DC	 MULTI-FACTOR	 EVENT HUBS	
 SCHEDULER	 SERVICE FABRIC							 MEDIA PLAYER	 CONTENT PROTECTION	 MEDIA ENCODING	 MEDIA STREAMING	 POWERBI	
 AUTOMATION	 BATCH	 VPN GATEWAY	 EXPRESSROUTE	 AZURE DNS	 APPLICATION GATEWAY	 AZURE BACKUP	 BIZTALK SERVICES	 CDN	 DATA CATALOG	 DATA FACTORY	 DATA LAKE ANALYTICS	 MACHINE LEARNING	
 OPINSIGHTS	 REMOTEAPP	 RESERVED IP	 VIRTUAL NETWORK	 TRAFFIC MANAGER	 LOAD BALANCER	 SITE RECOVERY	 SERVICE BUS	 MEDIA SERVICES	 HDINSIGHT	 TABLE/BLOB STORAGE	 DATA LAKE STORAGE	 STREAM ANALYTICS	
 KEY VAULT	 CLOUD SERVICES	 PUBLIC IP	 LOGIC APPS	 API APPS	 APP SERVICES	 API MANAGEMENT	 MOBILE APPS	 MOBILE ENGAGEMENT	 WEB APPS	 CUSTOM DOMAIN	 SSL CERTIFICATES	 NOTIFICATION HUBS	
 DEVTEST LABS	 VS APP INSIGHTS	 VS ONLINE	 SQL DATABASE	 SQL DATA WAREHOUSE	 DOCUMENTDB	 CACHE	 SEARCH	 STORAGE	 STORSIMPLE	 IMPORT / EXPORT	 PREMIUM STORAGE	 SQL ELASTIC DB	

The Trusted Cloud

Azure has the deepest and most comprehensive compliance coverage in the industry

GLOBAL



ISO 27001



ISO 27018



ISO 27017



ISO 22301



ISO 9001



SOC 1
Type 2



SOC 2
Type 2



SOC 3



CSA STAR
Self-Assessment



CSA STAR
Certification



CSA STAR
Attestation

US GOV



Moderate
JAB P-ATO



High
JAB P-ATO



DoD DISA
SRG Level 2



DoD DISA
SRG Level 4



DoD DISA
SRG Level 5



SP 800-171



FIPS 140-2



Section 508
VPAT



ITAR



CJIS



IRS 1075

INDUSTRY



PCI DSS
Level 1



CDSA



MPAA



FACT UK



Shared
Assessments



FISC Japan



HIPAA /
HITECH Act



HITRUST



GxP
21 CFR Part 11



MARS-E



IG Toolkit UK



FERPA



GLBA



FFIEC

REGIONAL



Argentina
PDPA



EU
Model Clauses



UK
G-Cloud



China
DJCP



China
GB 18030



China
TRUCS



Singapore
MTCS



Australia
IRAP/CCSL



New Zealand
GCIO



Japan My
Number Act



ENISA
IAF



Japan CS
Mark Gold



Spain
ENS



Spain
DPA



India
MeitY



Canada
Privacy Laws

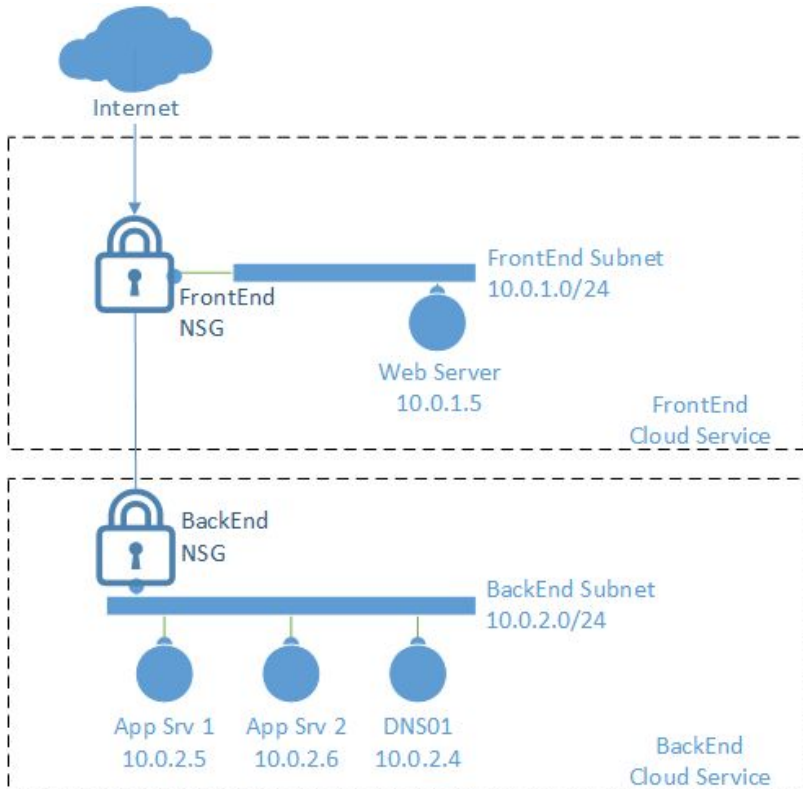


Privacy
Shield



Germany IT
Grundschutz
workbook

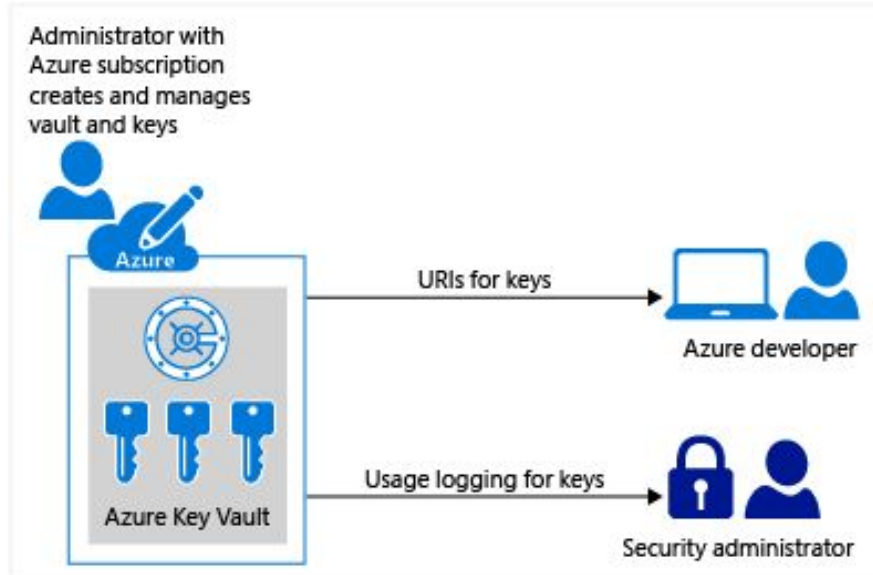
Azure Network Security Group



```
New-AzureNetworkSecurityGroup -Name $NSGName `
-Location $DeploymentLocation `
-Label "Security group for $VNetName subnets in
$DeploymentLocation"
```

```
Get-AzureNetworkSecurityGroup -Name $NSGName | `
Set-AzureNetworkSecurityRule -Name "Enable RDP
to $VNetName VNet" `
-Type Inbound -Priority 110 -Action Allow `
-SourceAddressPrefix INTERNET -SourcePortRange
'*' `
-DestinationAddressPrefix VIRTUAL_NETWORK `
-DestinationPortRange '3389' `
-Protocol *
```


Azure Key Vault



- 1.....Creates a key vault.
- 2.....Authorizes applications and users for specific operations.
- 3.....Add keys and secrets to key vault.
- 4.....Configure application with URI of key or secret or entire vault
- 5.....Use secrets and keys in the key vault.
Or, less commonly, add / update keys and secrets in the key vault.
- 6..... Monitors key vault logs.
- 7.....Update keys and secrets as needed.
- 8.....Updates permissions as needed.
- 9.....Delete key or secret when no longer needed.
- 10.....Deletes key vault when no longer needed.

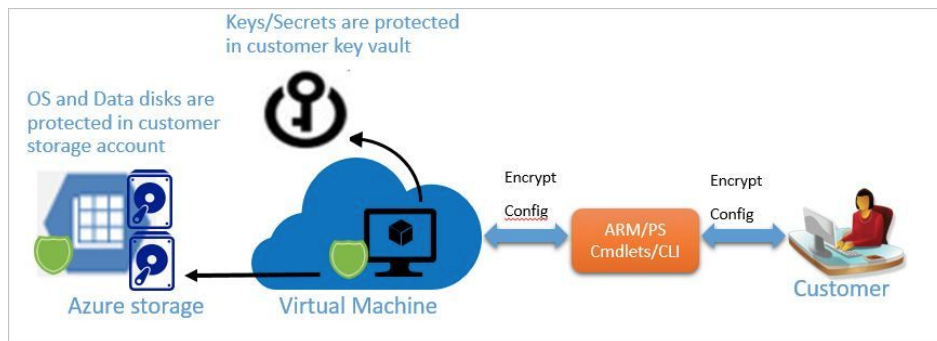
Azure Key Vault - Demo



Demo Files: <https://github.com/zigmax/azureqc17-keyvault>

Azure Disk Encryption

- Need Azure Key Vault / Azure AAD /
- Based on Windows : BitLocker / Linux : DM-CRYPT



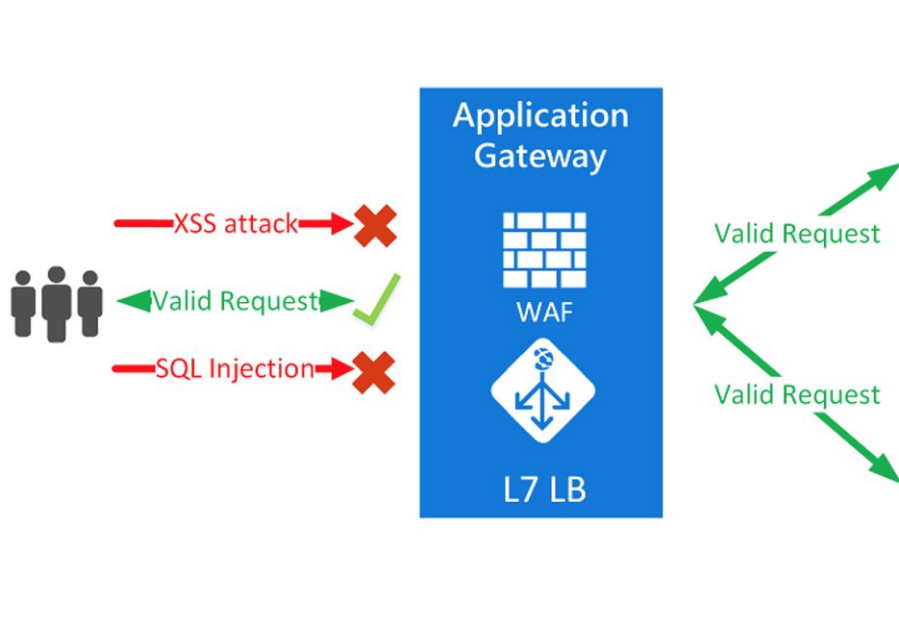
Howto : Azure Disk Encryption

<http://zigmax.net/azure-chiffre-une-machine-virtuelle-azure-disk-encryption/>

Official Documentation :

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption>

Azure Web Application Firewall (WAF)

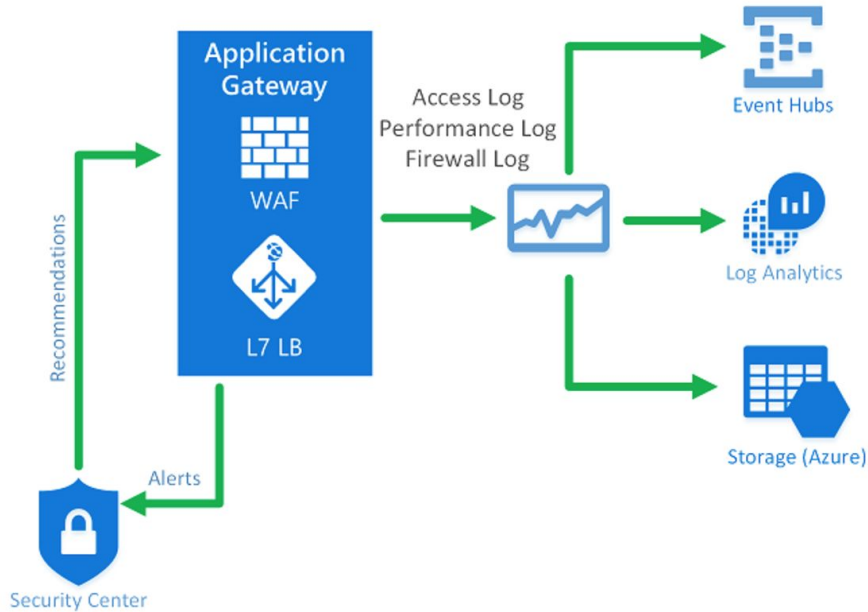


OWASP_3.0

The 3.0 core rule set provided has 13 rule groups as shown in the following table. Each of these rule groups contains multiple rules, which can be disabled.

RuleGroup	Description
REQUEST-910-IP-REPUTATION	Contains rules to protect against known spammers or malicious activity.
REQUEST-911-METHOD-ENFORCEMENT	Contains rules to lock down methods (PUT, PATCH< ..)
REQUEST-912-DOS-PROTECTION	Contains rules to protect against Denial of Service (DoS) attacks.
REQUEST-913-SCANNER-DETECTION	Contains rules to protect against port and environment scanners.
REQUEST-920-PROTOCOL-ENFORCEMENT	Contains rules to protect against protocol and encoding issues.
REQUEST-921-PROTOCOL-ATTACK	Contains rules to protect against header injection, request smuggling, and response splitting
REQUEST-930-APPLICATION-ATTACK-LFI	Contains rules to protect against file and path attacks.
REQUEST-931-APPLICATION-ATTACK-RFI	Contains rules to protect against Remote File Inclusion (RFI)

Azure WAF



Create application gateway

1 Basics
Configure basic settings

2 Settings
Configure application gateway ...

3 Summary
Review and create

Settings

* Public IP address

Choose a public IP address

Listener configuration

* Protocol

HTTP HTTPS

* Port

80

Web application firewall

* Firewall status

Enabled Disabled

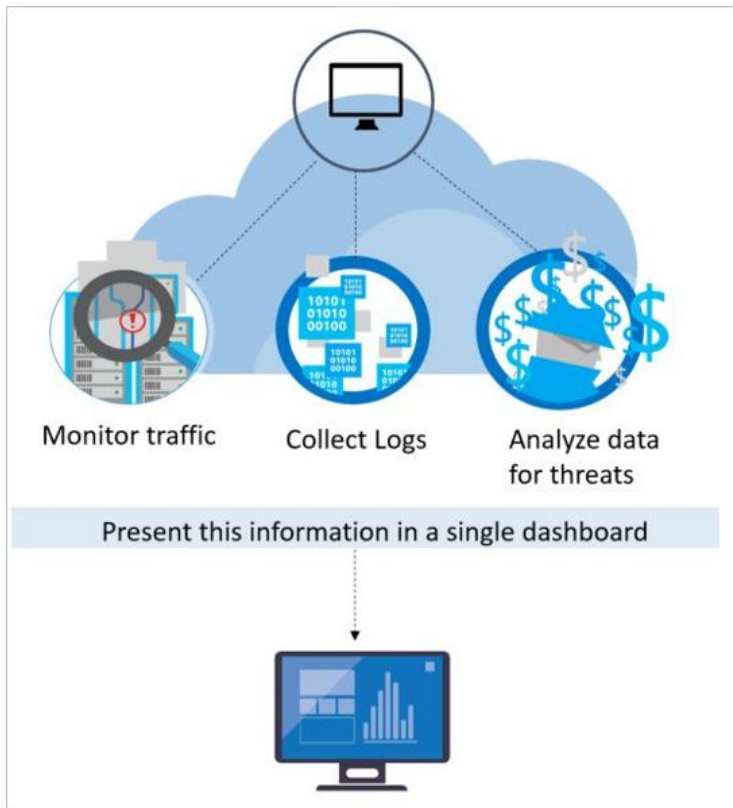
* Firewall mode

Detection Prevention

To view your detection logs, enable diagnostic logs after creating your application gateway.

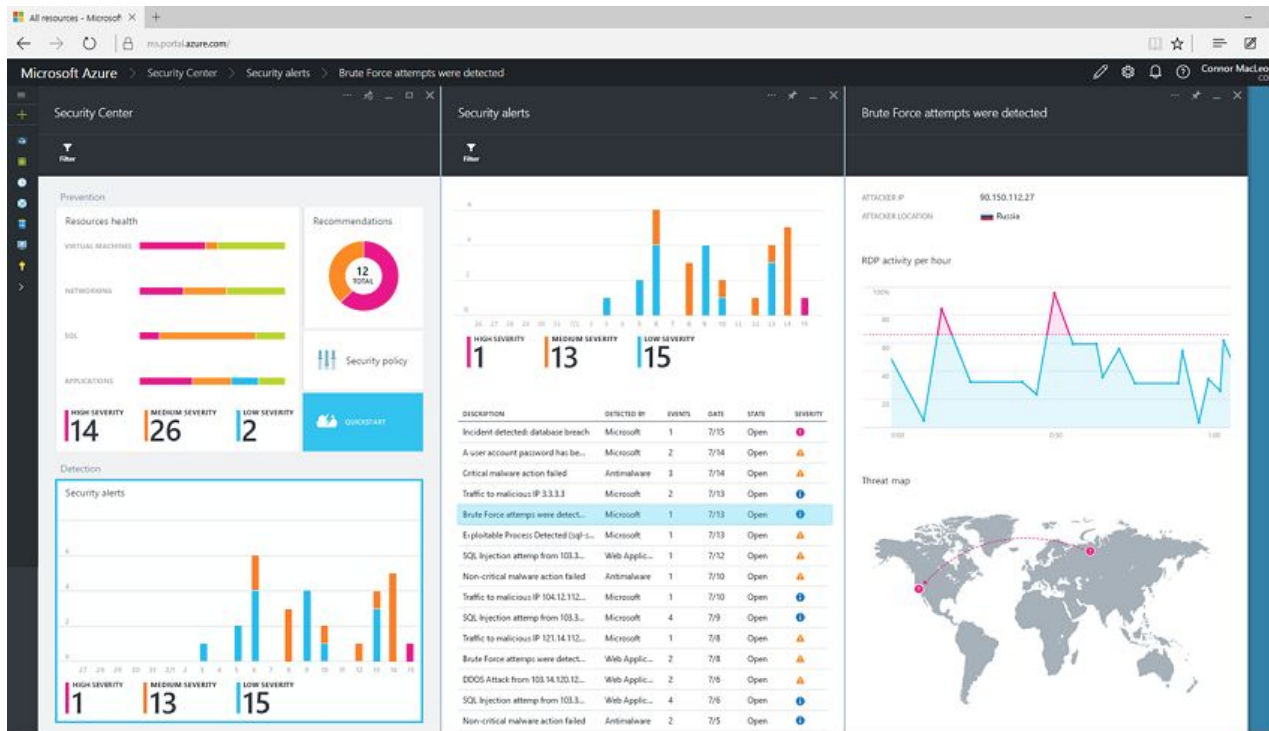
OK

Azure Security Center



- Integrated threat intelligence
- Behavioral analytics
- Anomaly detection

Azure Security Center



Prevention policy

Microsoft Azure Sponsorship

Show recommendations for

- System updates ☒ On ☐ Off
- OS vulnerabilities ☒ On ☐ Off
- Endpoint protection ☒ On ☐ Off
- Disk encryption ☒ On ☐ Off
- Network security groups ☒ On ☐ Off
- Web application firewall ☒ On ☐ Off
- Next generation firewall ☒ On ☐ Off
- Vulnerability Assessment ☒ On ☐ Off
- Storage Encryption ☒ On ☐ Off
- SQL auditing & Threat detection ☒ On ☐ Off
- SQL Encryption ☒ On ☐ Off













OK

Azure Security Center

Choose your pricing tier

Browse the available plans

The standard tier adds powerful features, including advanced threat detections and more. Try it for free for 60 days. For additional details, visit our pricing page. [Learn more](#)

Free	Standard – Free Trial	Standard
Basic detection	Advanced detection	Advanced detection
 Security policy	 Security policy	 Security policy
 Security assessment	 Security assessment	 Security assessment
 Recommendations	 Recommendations	 Recommendations
 Connected solutions	 Connected solutions	 Connected solutions
0.00 FREE	0.00 FREE FOR 60-DAYS	15.00 USD / NODE / MONTH

Recommendations

Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY	
Enable advanced security for subscription...	1 subscriptions	Resolved	High	...
Add a Next Generation Firewall	win16labmax...	Open	High	...
Finalize Internet facing endpoint protect...	lab01-ub-ma...	Open	High	...
Enable Network Security Groups on sub...	2 subnets	Open	High	...
Route traffic through NGFW only	lab01-ub-max	Open	High	...
Apply disk encryption	2 virtual mac...	Open	High	...
Enable encryption for Azure Storage Acc...	4 storage acc...	Open	High	...
Restrict access through Internet facing e...	win16labmax...	Open	Medium	...
Add a vulnerability assessment solution	win16labmax...	Open	Medium	...
Provide security contact details	1 subscriptions	Resolved	Medium	...

Select

Azure Security Center

lab01-ub-max-nsg



Edit inbound rules

Network security group info

NETWORK SECURITY GROUP lab01-ub-max-nsg

LOCATION eastus

DESCRIPTION Your NSG has inbound rules that open access to 'Any' or 'Internet' which might enable attackers to access your resources. We recommend that you edit the below inbound rules to restrict access to a specified set of sources.

Related inbound rules

PRIORITY	NAME	SOURCE	SERVICE	ACTIONS
1000	default-allow-ssh	*	TCP	Allow

Associated with

NAME	VIRTUAL MACHINE
lab01-ub-max642	lab01-ub-max

Microsoft Azure << Create a new Next Generation Firewall solution > Cisco ASAv - BYOL 4 NIC

Cisco ASAv - BYOL 4 NIC



The physical Cisco ASA and Cisco ASAv support the same rich policy constructs. Virtual and physical domains are coalesced into a single policy domain so the same policies can be applied to all Cisco ASAs, whether they are physical or virtual.

Cisco ASAv offers the same features as a physical Cisco ASA, including VPN services that can be deployed in the virtual domain. Site-to-site, remote-access, and clientless VPN services can be deployed quickly in a private cloud or over a virtual infrastructure in response to demand.

Cisco ASAv offers the REST API, an HTTP-based interface that facilitates management of the appliance, including changing the security policy and monitoring the status. Using REST APIs, multiple cloud management solutions can be used to manage both physical and virtual instances of Cisco ASA.

- **FREE TRIAL**- ASAv has a demo mode that runs with reduced performance. No license required.
- Supported Azure Instances: Standard_D3 and Standard_D3_V2
- ASAv is integrated with Azure Security Center
- ASAv is available in the Azure Government Cloud.

This deployment creates an ASAv with four NICs, plus public and private subnets.

PUBLISHER Cisco Systems, Inc.

USEFUL LINKS [ASAv Home Page](#) [Quick Start Guide](#) [Datasheet](#) [ASAv COMMUNITY SUPPORT PORTAL](#) [Instructional Youtubes](#)

Create

Azure Security Center - Alert

TCP packet, no conn, denied

10.1.0.4



DESCRIPTION

%ASA-6-106015: Deny TCP (no connection) from 124.243.216.102/11207 to 10.1.0.4/22 flags RST on interface management

DETECTION TIME

Monday, June 26, 2017, 9:20:00 PM

SEVERITY

Low

STATE

Active

ATTACKED RESOURCE

10.1.0.4

SUBSCRIPTION

[Microsoft Azure Sponsorship](#)
(7db5e03c-f3c2-48b1-b326-aa53faaaafc3)

DETECTED BY

Cisco ASAv

ACTION TAKEN

Blocked

ENVIRONMENT

Azure

RESOURCE TYPE

Azure Resource

HIT COUNT

1

SOURCE IPS

124.243.216.102

Secure <https://www.abuseipdb.com/check/124.243.216.102>

IP Abuse Reports for 124.243.216.102:

This IP address has been reported a total of **26** times. 124.243.216.102 was first reported on 18 Jun 2017. The most recent report was **2 hours ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

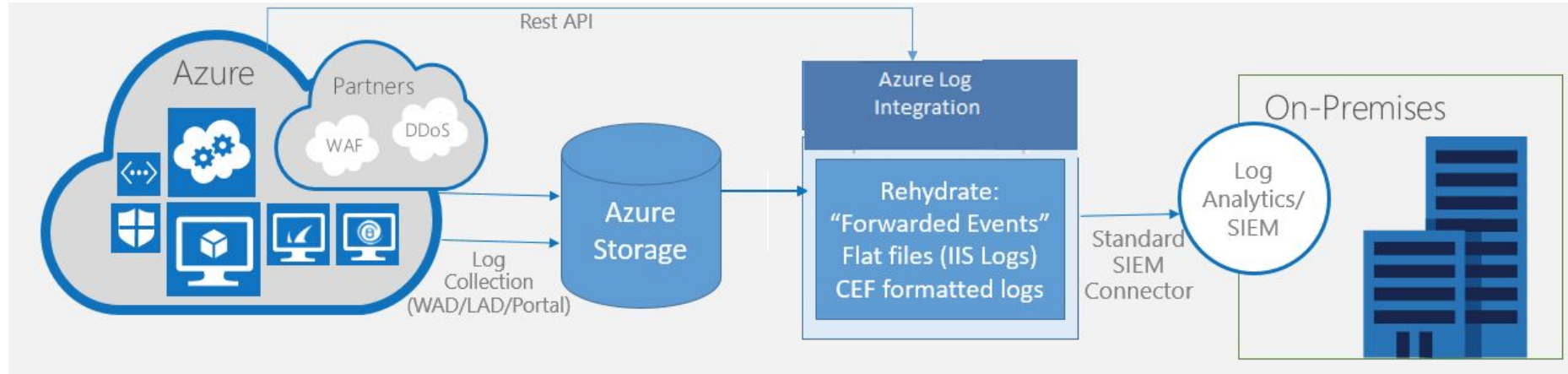
Search:

Reporter	Date	Comment	Categories
✓ infosky.net	2 hours ago	SSH/22 MH Probe, BF -	Brute-Force SSH
🇺🇸 Anonymous	6 hours ago	Jun 26 14:30:16 ns sshd\[20408\]: pam_unix(sshd:auth \\\): authentication failure\; logname= uid=0 eui ... show more	DDoS Attack
✓ doyoucheck.com	14 hours ago	ssh intrusion attempt	SSH
🇷🇺 Anonymous	25 Jun 2017	Brute force SSH login	Brute-Force SSH
✓ cutkit.eu	25 Jun 2017	SSH brute force	Brute-Force SSH
blueSh4rk	25 Jun 2017	unauthorized ssh connection attempt	Brute-Force SSH
✓ blog.demees.net	25 Jun 2017	ssh-bruteforce	SSH
✓ infosky.net	25 Jun 2017	SSH/22 MH Probe, BF -	Brute-Force SSH
✓ infosky.net	25 Jun 2017	SSH/22 MH Probe, BF -	Brute-Force SSH

Azure Security Center - Demo



Azure SIEM (IBM QRadar + Splunk)



Howto Azure with IBM QRadar: <http://zigmax.net/azure-siem-ibm-qradar/>

Forensic investigation (Logs)

Microsoft Azure Monitor - Activity log

max.coquerel@live.fr
RÉPERTOIRE PAR DÉFAUT

Monitor - Activity log
Microsoft

Search (Ctrl+/)

EXPLORE

- Activity log
- Metrics
- Diagnostics logs
- Log search

MANAGE

- Alerts
- Action groups
- Autoscale

HEALTH

- Service notifications
- Resource health

Columns Export Log search

Select query ...

Insights (Last 24 hours): 0 failed deployments | 0 role assignments | 2 errors | 0 alerts fired | 0 outage notifications

* Subscription ⓘ Resource group ⓘ Resource ⓘ Resource type ⓘ * Operation ⓘ

Microsoft Azure Sponsors... All resource groups All resources All resource types All operations

Timespan ⓘ Event category ⓘ * Event severity ⓘ Event initiated by ⓘ Search ⓘ

Last 6 hours All categories 4 selected Email or name or servi...

Apply Reset

Query returned 45 items. [Click here to download all the items as csv.](#)

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
ListKeys	Started	3 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr
Update website	Succeeded	9 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr
Update website	Succeeded	19 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr
Validate	Started	19 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr

Summary JSON

Operation name
ListKeys

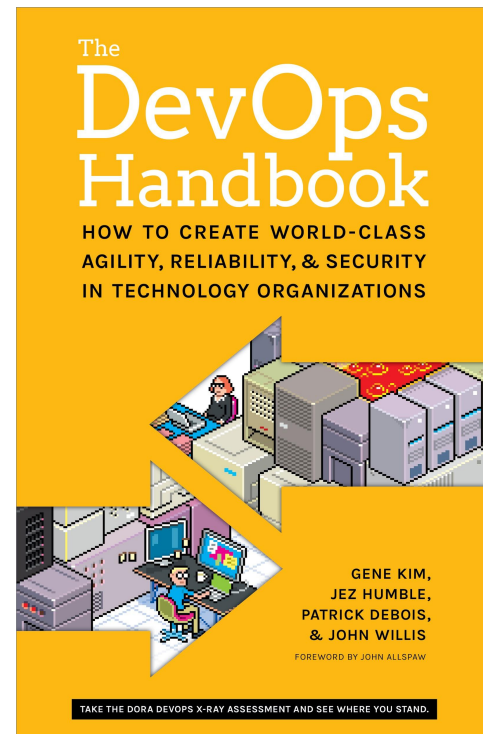
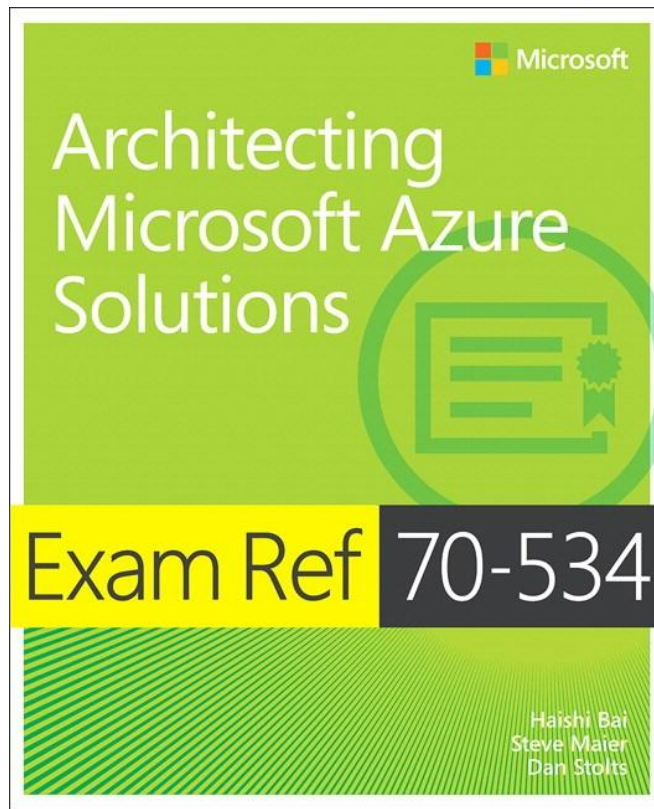
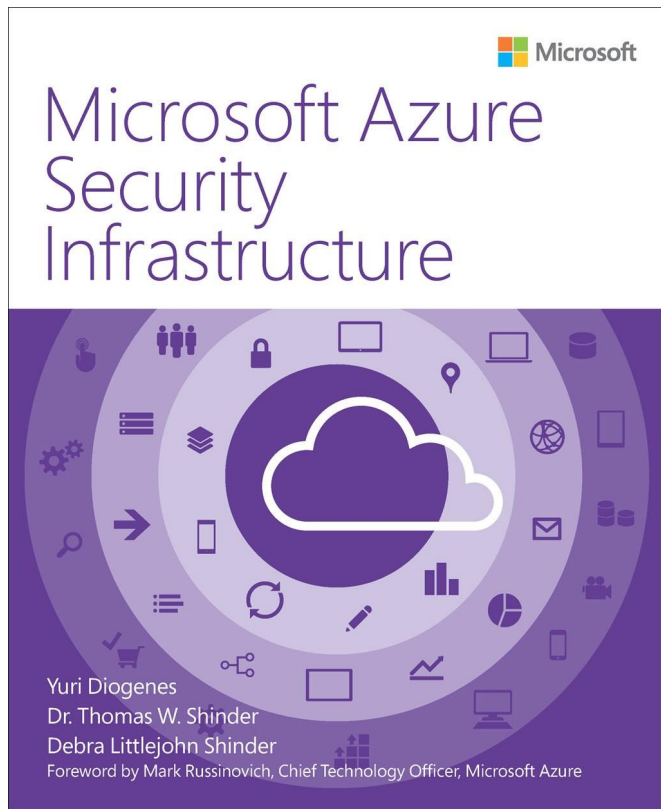
Time stamp

Conclusion

- > Your business requires compliance ?
- > Identity Management ... **Azure Active Directory**
- > No flat networks ... **Network Security Group**
- > Manage your secret ... **Azure Key Vault**
- > Deploy Advance Firewall (Layer 7 with **WAF**)
- > Threat Analytics - **Azure Security Center**
- > Have fun :) !



Books



Technical Ressources

Microsoft Virtual Academy (FR) - <https://stanislas.io/2016/04/26/41/>

Microsoft Technical Community Content

<https://github.com/Microsoft/TechnicalCommunityContent>

Azure Security Blog - <https://azure.microsoft.com/en-us/blog/topics/security/>

Mathieu Benoit - <https://alwaysupalwayson.blogspot.ca/>

Maxime Blog - <http://zigmax.net>

Questions / Talks