

PUBLIC



++

A Penetration Tester's Guide to the Azure Cloud

Apostolos Mastoris

22nd July 2016

MWR
LABS



Key direction

- + Understand main Azure components and concepts.
- + Familiarise with Azure's key security features.
- + Explore penetration testing capability in Azure.
- + Demonstrate Azurite.



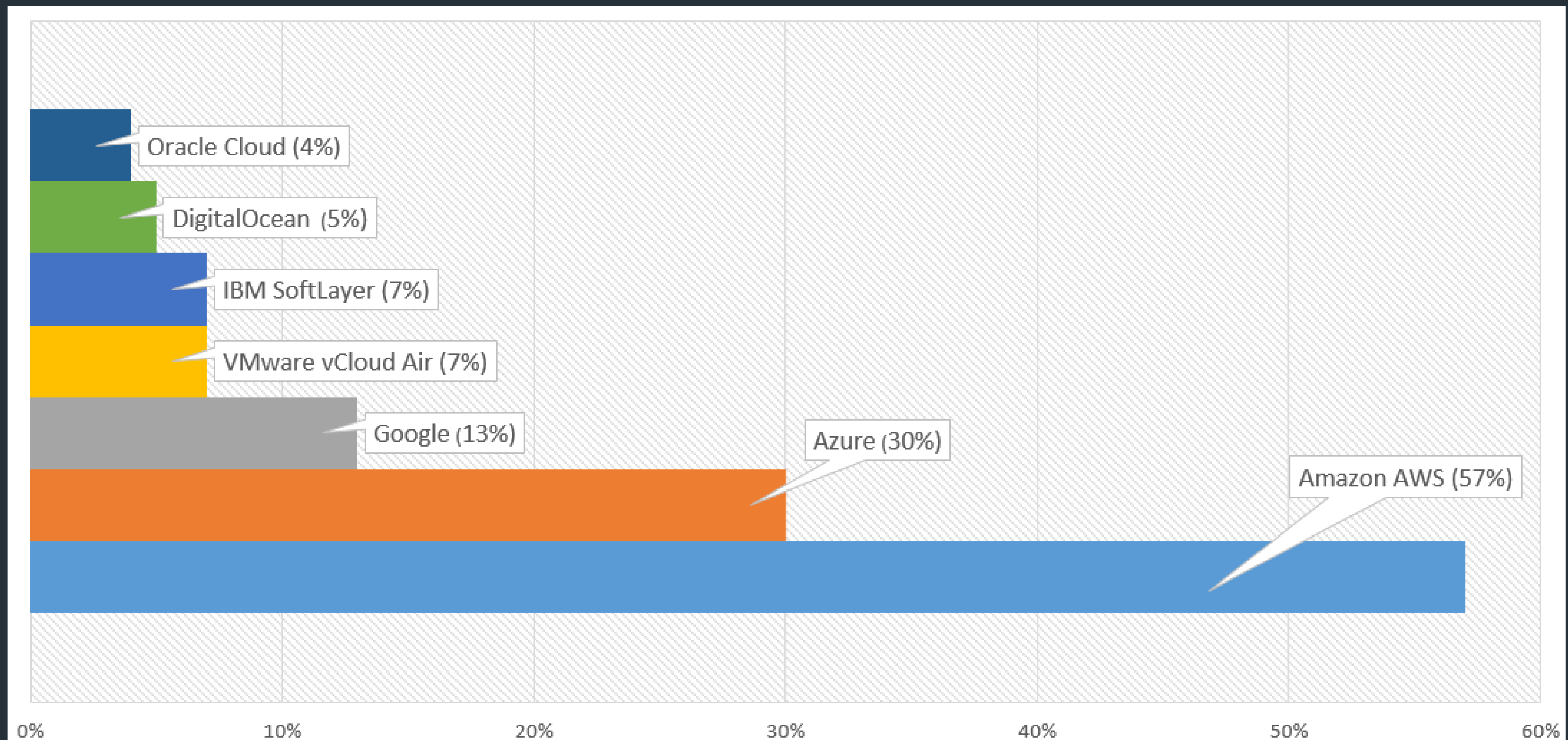
Contents

1. Cloud Services Trends, Challenges & Azure
2. Azure Security Controls & Pentesting
3. Azurite - Explore & Visualize
4. Conclusions

Cloud Services Trends, Challenges & Azure

++

How is the use of public cloud services distributed this year?



Cloud Services Trends, Challenges & Azure

++

Cloud Computing Challenges

- + Security – Are there appropriate security controls to secure the deployments?
- + Compliance – Can companies store sensitive data (e.g. PII, payment data) in the Cloud?
- + Trust/Privacy – Can companies trust the Cloud provider with their assets?
- + Governance – Do Cloud services provide appropriate controls to monitor and control the security of the systems?

Cloud Services Trends, Challenges & Azure

++ Azure Service Models & Responsibilities



Cloud Services Trends, Challenges & Azure

++

Azure Deployment

- + Subscription
- + Deployment models:
 - Classic – Based on cloud services
 - Azure Resource Manager (ARM)– Based on resource groups
- + Regions (e.g. East US)
- + Templates
- + Extensions (e.g. Microsoft Antimalware)

Cloud Services Trends, Challenges & Azure

++

Azure Management

- + Web Access – Azure Management Portal (Classic Mode) & Azure Portal (Classic and Resource Manager Modes)
- + API Access – Azure Service Management (ASM) & Resource Manager (ARM) REST APIs
- + Command-line Access – Azure PowerShell & Azure Client Tools
- + Traditional Clients – RDP, WinRM & SSH

PUBLIC



Cloud services Trends, Challenges & Azure – Azure Management

++

Azure Portal

Microsoft Azure All resources

Default Directory

+ Add Columns Refresh

Subscriptions: Free Trial

Filter items...

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
testresourcegroup14850	Storage account	test-resource-group-1	East US	Free Trial
testresourcegroup24543	Storage account	test-resource-group-2	North Europe	Free Trial
testresourcegroup39861	Storage account	test-resource-group-3	West US	Free Trial
TestVNet1	Virtual network	test-resource-group-1	East US	Free Trial
TestVNet2	Virtual network	test-resource-group-2	North Europe	Free Trial
TestVNet3	Virtual network	test-resource-group-3	West US	Free Trial
ubuntu1Front1	Virtual machine	test-resource-group-1	East US	Free Trial
ubuntu1Front1	Network security group	test-resource-group-1	East US	Free Trial
ubuntu1Front1	Public IP address	test-resource-group-1	East US	Free Trial
ubuntu1front1487	Network interface	test-resource-group-1	East US	Free Trial
ubuntu221	Virtual machine	test-resource-group-2	North Europe	Free Trial



Contents

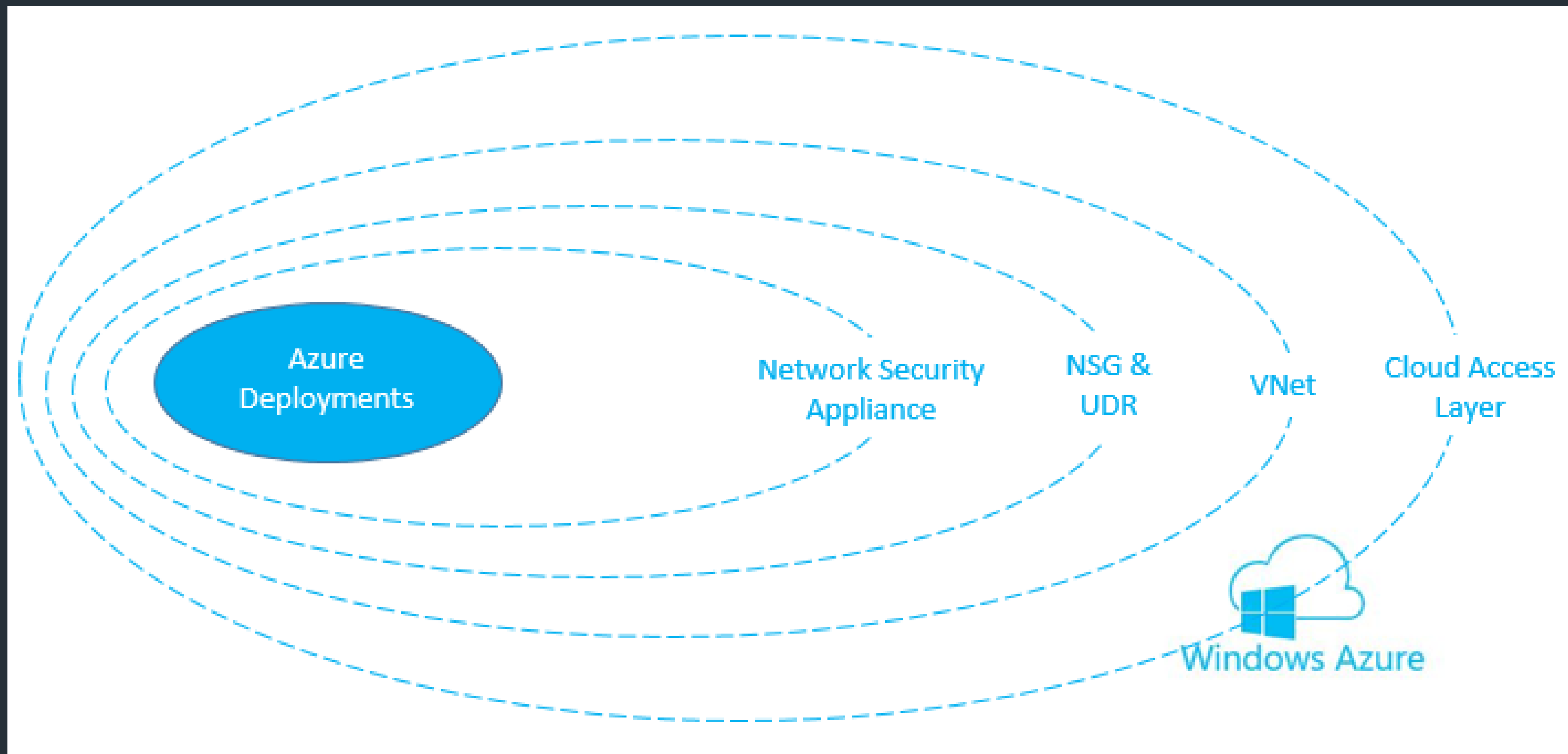
1. Cloud Services Trends, Challenges & Azure
2. Azure Security Controls & Pentesting
3. Azurite - Explore & Visualize
4. Conclusions

Azure Security Controls & Pentesting - Network Security

++

Network Security

+ Azure provides controls to secure each network layer:



Azure Security Controls & Pentesting - Network Security

++

Cloud Access Layer

+ DDoS Protection

- Offers DDoS protection against large-scale attacks. In case of attack customer resources are served from different location (DC or region).
- Transparent protection – Not accessible/configurable from customers.
- Tenant responsible for the DDoS protection of their individual applications/infrastructure (e.g. in case they experience a targeted attack).
- 3rd party solutions available as VMs to protect against targeted DDoS attacks (e.g. aiProtect)

Azure Security Controls & Pentesting - Network Security

++

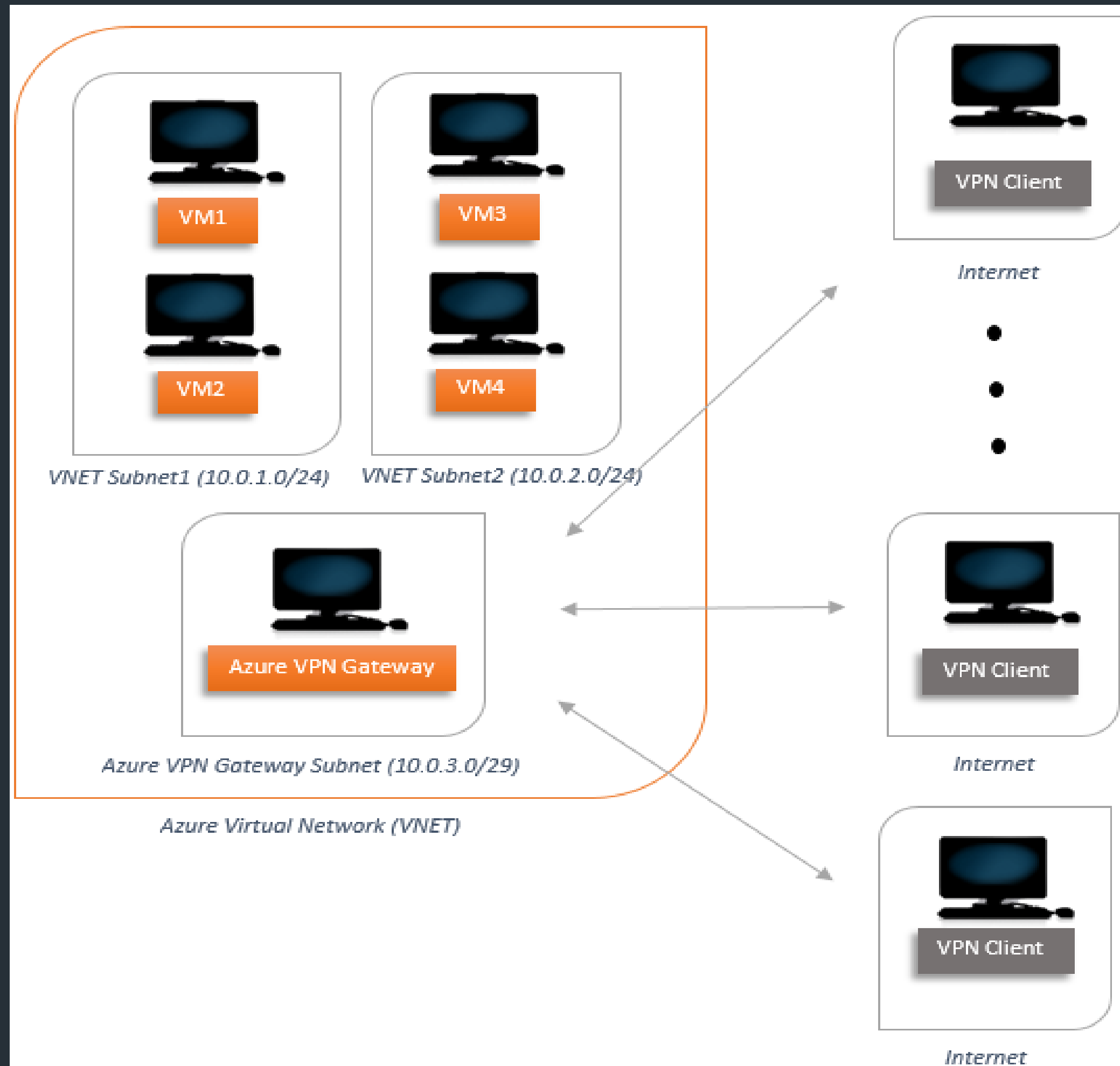
virtual Network (VNet)

- + Network isolation/segregation
- + Contains Subnets and Gateway Subnets
- + Connectivity Scenarios
 - RDP/SSH/WinRM services exposed on the Internet
 - Point-to-Site VPN
 - Site-to-Site VPN
 - ExpressRoute

Azure Security Controls & Pentesting - Network Security

++

VNet - Point-to-Site VPN



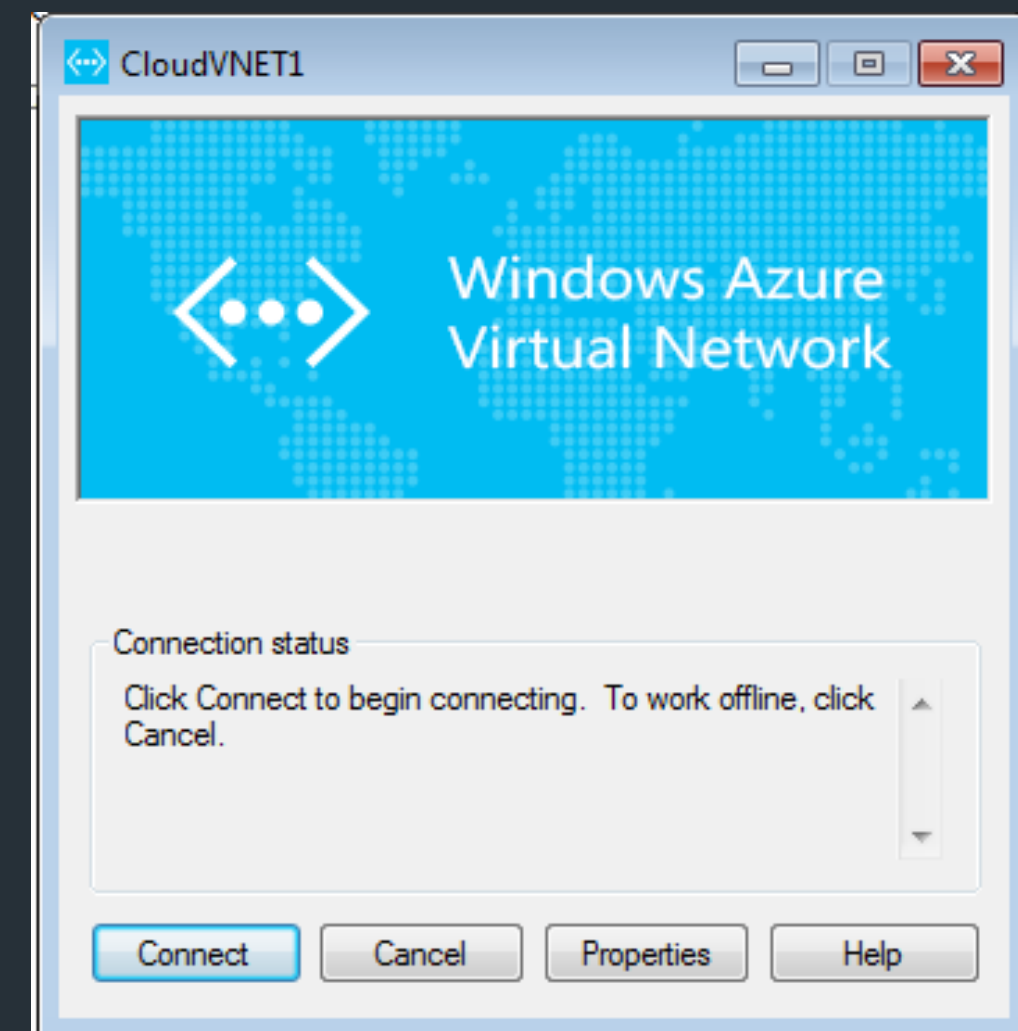
Azure Security Controls & Pentesting - Network Security

++

P2S VPN - Connect to VNet Gateway in Classic & Resource Manager Models

- + Tenant to generate client certificate for authentication to VPN service.
- + In Classic model - Download VPN client package from Azure Management Portal (Windows 32-bit & 64-bit supported).
- + In Resource Manager model - PowerShell cmdlet

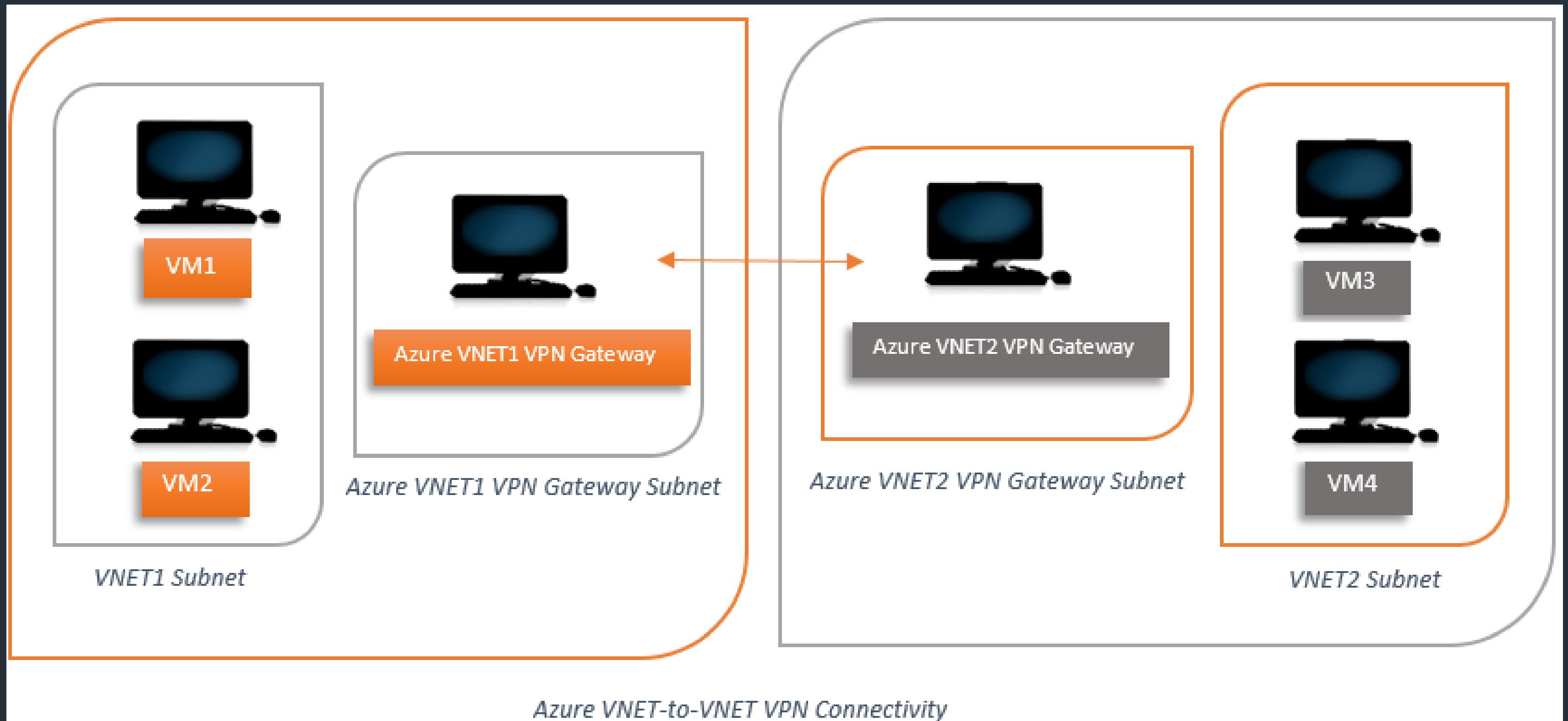
```
PS> Get-AzureRmVpnClientPackage  
-ResourceGroupName [Resource_Group]  
-VirtualNetworkGatewayName [VNet_Gateway]  
-ProcessorArchitecture  
Amd64
```
- + Pentester to authenticate with the client certificate.



Azure Security Controls & Pentesting - Network Security

++

VNet - Site-to-Site (S2S) VPN

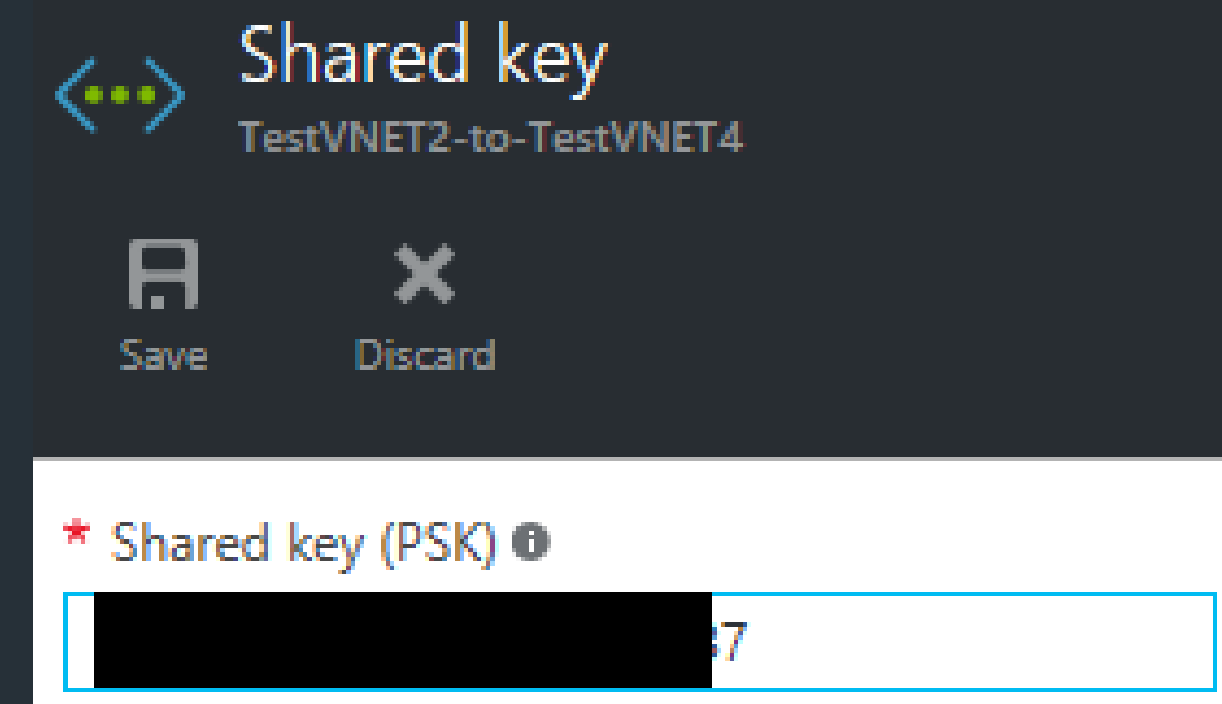
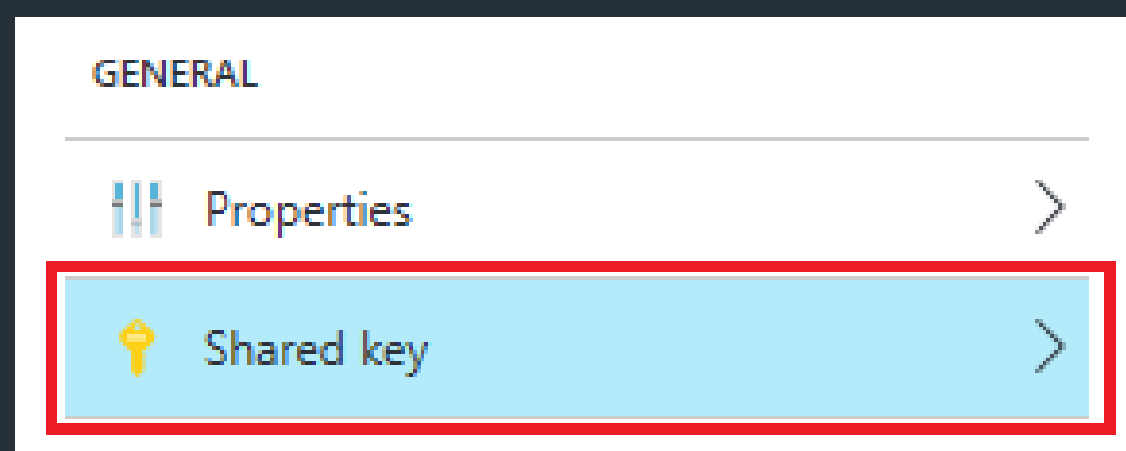


Azure Security Controls & Pentesting - Network Security

++

VNet - Site-to-Site (S2S) VPN

- + VNet-to-VNet connection requires a Pre-Shared Key (PSK) for encryption. Can be found in cleartext in the connection 'Settings' pane:



Azure Security Controls & Pentesting - Transport Security

++

Transport Security - Web Apps

+ SSL/TLS Certificate

HOST NAME	CERTIFICATE	SSL TYPE
msazuresite.xyz	msazuresite.xyz,www....	IP Based SSL SNI SSL



NAME	EXPIRATION	THUMBPRINT
msazuresite.xyz,www....	6/27/2017	566DC91096C4E54FC35AB1565248B8A531006D44

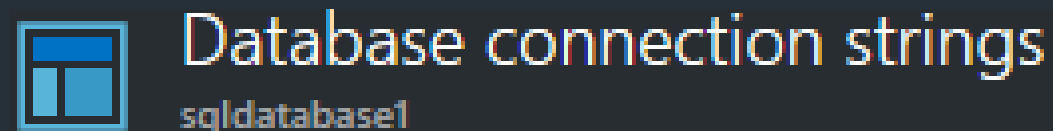
- IP-based or SNI-based
- + Extensions for 'Let's encrypt' CA support
- + Extension to enforce HTTPS access.
- + Configuration to redirect from HTTP to HTTPS:
<https://azure.microsoft.com/en-us/documentation/articles/web-sites-configure-ssl-certificate/>

Azure Security Controls & Pentesting - Transport Security

++

Transport Security - Azure SQL Database

+ Azure SQL Database connection strings



ADO.NET(SQL authentication)

```
Server=tcp:sqlserver13.database.windows.net,1433;Data Source=sqlserver13.database.windo
```

ODBC (Includes Node.js)

```
Driver={SQL Server Native Client 11.0};Server=tcp:sqlserver13.database.windows.net,1433;Da
```

PHP

```
Server: sqlserver13.database.windows.net,1433 \r\nSQL Database: sqldatabase1\r\nUser Nam
```

JDBC (SQL authentication)

```
jdbc:sqlserver://sqlserver13.database.windows.net:1433;database=sqldatabase1;user=vmuser
```

Azure Security Controls & Pentesting - Transport Security

++

Transport Security – Azure SQL Database

+ Azure SQL Database connection strings:

```
{Server=tcp:sqlserver13.database.windows.net,1433;Data
Source=sqlserver13.database.windows.net;Initial
Catalog=sqldatabase1;Persist Security Info=False;User
ID={your_username};Password={your_password};MultipleActi
veResultSets=False;Connection Timeout=30;
Encrypt=True;TrustServerCertificate=False;}
```

- `TrustServerCertificate=False;` #Always validate server's certificate – Mitigate against MitM attacks
- `Encrypt = True;` # Encrypt all communications

Azure Security Controls & Pentesting -
Network Access Control

++

Network Security Virtual Appliances

- + IDS, IPS, WAF → 3rd party Virtual Machines
(e.g. Barracuda Firewall, F5)
- + VPN appliances – available in Azure's Marketplace

Azure Security Controls & Pentesting – Network Access Control

- ++ Network Access Control – Network Security Groups (NSGs)
- + Access control lists for Subnets and VMs (Classic) / NICs (Resource Manager)
- + Can be created once and be used multiple times.
- + Structure – Source IP, Source Port, Destination IP, Destination Port, Protocol, Direction
- + When created, they contain default rules with very low priority.

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
65000	AllowVnetInBound	VirtualNetwork	VirtualNetwork	Any/Any	Allow
65001	AllowAzureLoadBalancerInBound	AzureLoadBalancer	Any	Any/Any	Allow
65500	DenyAllInBound	Any	Any	Any/Any	Deny

Azure Security Controls & Pentesting – Network Access Control

++

Endpoint Access Control List (ACL)

- + Applied at the endpoint (e.g. VM)
- + Cannot co-exist with NSGs on a VM.
- + When created all access to VM is blocked.

Azure Security Controls & Pentesting – Network Access Control

++

User Defined Routing (UDR)

- + Routing in Azure is performed automatically based on systems routes.
- + UDR allows to specify routes when used in combination with 3rd party security appliances.
- + VM acting as network appliance requires IP forwarding enabled.
- + Considered security best practice for defence-in-depth.

PUBLIC



Azure Security Controls & Pentesting – Network Access Control

++

Azure SQL Server & Database Firewall

- + Exposed on the Internet on port 1433/tcp – Hostname convention: <azuresqlservername>.database.windows.net
- + Connectivity to Azure SQL Server through SQL Server Management Studio (SSMS).
- + Firewall configuration allows only trusted IP addresses to connect to the server.

Firewall settings Allow access for specific IPs



Save



Discard



Add client
IP

Allow access to Azure services ON OFF

Client IP address [REDACTED].132

RULE NAME	START IP	END IP
ClientIPAddress_2016-2-6_2...	[REDACTED].132	[REDACTED].132

Azure Security Controls & Pentesting – Network Access Control

++

Azure SQL Server & Database Firewall

+ Firewall configuration can also be applied at the database level.

+ T-SQL command in the SSMS:

```
SQL> EXECUTE sp_set_database_firewall_rule N'MWR  
Test IP 1', '1.2.3.4', '1.2.3.4';
```

+ List configured database firewall rules in SSMS (T-SQL):

```
SQL> SELECT * FROM sys.database_firewall_rules;
```

	id	name	start_ip_address	end_ip_address	create_date	modify_date
1	1	MWR Test IP 1	[REDACTED].131	[REDACTED].131	2016-06-29 14:16:40.217	2016-06-29 14:16:40.217

Azure Security Controls & Pentesting – Network Access Control

++

Traffic in Azure

- + By default, Azure resources require to connect to Azure services to provide details about their status or request information e.g. DHCP request.
- + Example: DHCP, DNS and Health monitoring:
168.63.129.16

118	19.149168607	10.0.1.4	168.63.129.16	TCP	74 36120 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=7087228 TSecr=0 WS=128
119	19.149595720	168.63.129.16	10.0.1.4	TCP	74 80 → 36120 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=847398678 TSecr=7087228
120	19.149617621	10.0.1.4	168.63.129.16	TCP	66 36120 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=7087228 TSecr=847398678
121	19.149652822	10.0.1.4	168.63.129.16	HTTP	212 GET /machine/?comp=goalstate HTTP/1.1
122	19.151113165	168.63.129.16	10.0.1.4	TCP	1494 [TCP segment of a reassembled PDU]
123	19.151129366	10.0.1.4	168.63.129.16	TCP	66 36120 → 80 [ACK] Seq=147 Ack=1429 Win=32128 Len=0 TSval=7087228 TSecr=847398678

- + Azure Datacentre IP address ranges:
<https://www.microsoft.com/en-gb/download/details.aspx?id=41653>

Azure Security Controls & Pentesting - Encryption

++

Encryption

- + OS & disk encryption
 - Bitlocker for Windows
 - DM-Crypt for Linux
- + Transparent Data Encryption (TDE) for SQL Databases
- + Azure storage – Blob encryption
- + Key management service → Azure Key Vault

Azure Security Controls & Pentesting - Encryption

++

Azure Key Vault

- + Cryptographic key management service
- + Acts as secure container for keys and secrets:
 - Keys – Cryptographic keys, stored encrypted in HSM (powered by Thales) or Software.
 - Secrets – SSL/TLS certificates, passwords, connection strings.
 - Azure services do not have access to the keys unless specifically instructed (e.g. access keys to boot encrypted OS)
 - Keys do not leave the region of the Key Vault.
 - Keys are not exportable.
 - Key Encryption Key (KEK) adds additional layer of security.

Azure Security Controls & Pentesting - Encryption

++

Azure Key Vault – Properties

- + Retrieve Key Vault ‘test-key-vault-1’ configuration:

```
PS> Get-AzureRmKeyVault -VaultName 'test-key-vault-1'
```

- + Can Azure services access it?

```
[...] Enabled For Disk Encryption? : True [...]  
# Key vault was created with '-enabledForDiskEncryption'
```

- + Review “Access Policies” property for assigned permissions:

```
e.g. Access Policies :  
[...]  
Permissions to Keys : all # Access  
permission for keys  
Permissions to Secrets : all # Access  
permissions for secrets
```

Azure Security Controls & Pentesting - Encryption

++

Azure Key Vault – Key Properties

- + Retrieve Key Vault's key 'test-key-vault-1-kek-1' configuration:

```
PS> Get-AzureKeyVaultKey -Name test-key-vault-1-kek-1 -VaultName  
test-key-vault-1
```

- + Key type:

```
[...] "kty":"RSA" [...]
```

- RSA: Keys (2048-bit RSA key) processed by Key Vault software encrypted at-rest with encryption key located at Azure's HSM.
- RSA-HSM: Key (2048-bit RSA key) stored in Thales HSM.

- + Key operations:

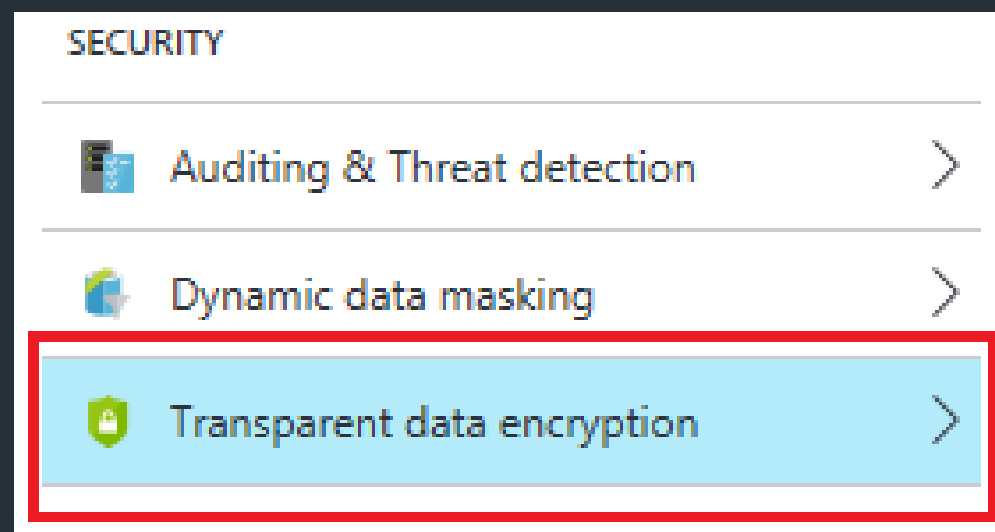
```
[...] "key_ops":["encrypt","decrypt","sign","verify","wrapKey","unwrapKey"] [...]
```

Azure Security Controls & Pentesting - Encryption

++

Azure SQL Database

+ Transparent Data Encryption (TDE) for SQL databases – Configuration through Azure Portal “Settings” pane:



Transparent data encryption

Save Discard Feedback

Transparent Data Encryption protects your data and helps meet compliance requirements by encrypting your database, associated backups, and transaction log files at rest without requiring changes to your application.

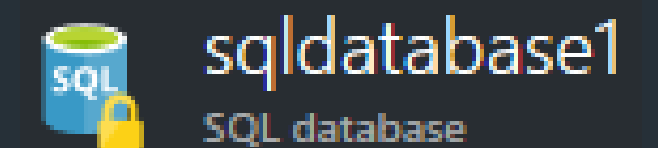
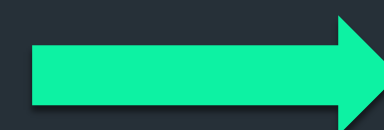
[Learn more about transparent data encryption.](#)

Data encryption

ON OFF

Encryption status

Encrypted



Azure Security Controls & Pentesting - Encryption

++

Azure SQL Database

- + Transparent Data Encryption (TDE) for SQL databases – Encrypt through SSMS:

```
SQL> ALTER DATABASE [database_name] SET ENCRYPTION ON;
# Azure SQL Database level
```

- + Authoritative way to review encryption status in the DB:

```
SQL> SELECT * FROM sys.dm_database_encryption_keys;
```

Output:

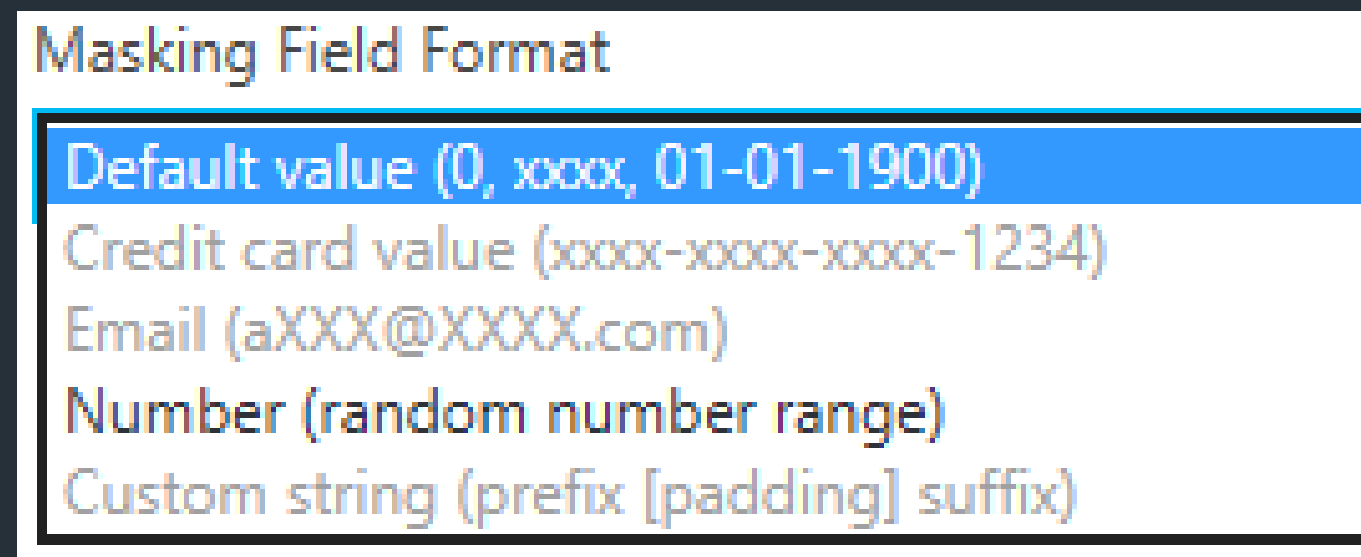
	database_id	encryption_state	create_date	regenerate_date	modify_date	set_date	opened_date	key_algorithm	key_length	encryptor_thumbprint	encryptor_type
1	2	3	2016-07-10 20:09:28.457	2016-07-10 20:09:28.457	2016-07-10 20:09:28.457	1900-01-01 00:00:00.000	2016-07-10 20:09:28.457	AES	256	0x	ASYMMETRIC KEY
2	5	3	2016-06-29 09:39:08.503	2016-06-29 09:39:08.503	2016-06-29 09:39:08.503	2016-06-29 09:39:13.707	2016-07-10 20:09:28.457	AES	256	[REDACTED]	CERTIFICATE

Azure Security Controls & Pentesting

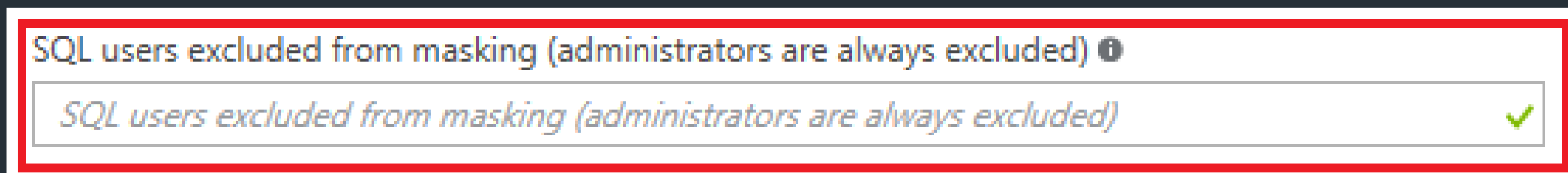
++

Database Data Masking

- + Azure SQL database supports data masking at column level.
- + Various masking formats based on the data:



- + Admins and specified users can view the data unmasked – defined in each masking rule:



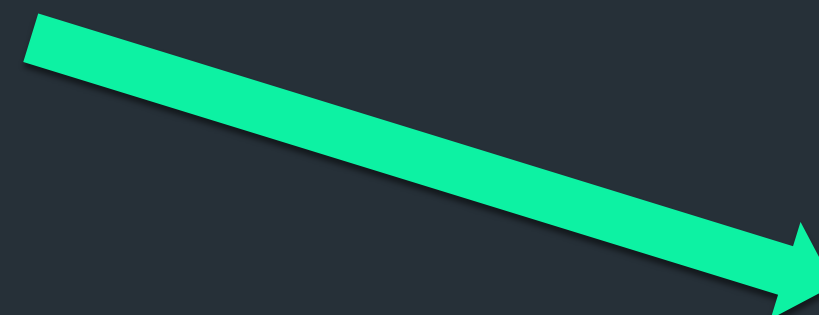
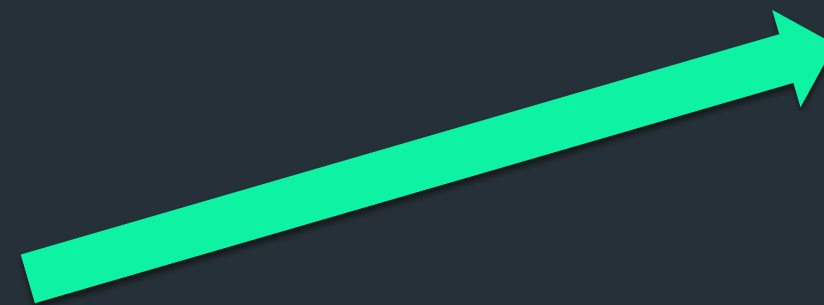
Azure Security Controls & Pentesting

++

Endpoint Protection

+ Anti-virus & Anti-Malware Extensions

- ESET File Protection
- Deep Security Trend Micro
- Microsoft Antimalware



License key ⓘ

Components to install
Install Real-time file system protection ⓘ
 Yes No
Install Web and email component ⓘ
 Yes No
Install Device control ⓘ
 Yes No
Initial product settings
Enable ESET LiveGrid® reputation system (recommended) ⓘ
 Yes No
Enable detection of potentially unwanted applications ⓘ
 Yes No

EXCLUDED FILES AND LOCATIONS ⓘ

EXCLUDED FILE EXTENSIONS ⓘ
EXCLUDED PROCESSES ⓘ
REAL-TIME PROTECTION ⓘ
 Enable Disable
RUN A SCHEDULED SCAN ⓘ
 Enable Disable
SCAN TYPE ⓘ
 Quick Full
SCAN DAY ⓘ
Saturday ▼
SCAN TIME ⓘ
120

Azure Security Controls & Pentesting – Backup Security

++

Backup Security

- + MSSQL – Configuration during VM creation:
- + Azure SQL Database



SQL Automated Backup

Configure backups for databases in your virtual machine.

Automated backup

Disable Enable

Retention period (days)

30

Storage account

(new) testresourcegroup5047

Encryption

Disable Enable

Azure Security Controls & Pentesting –
Access Controls

++

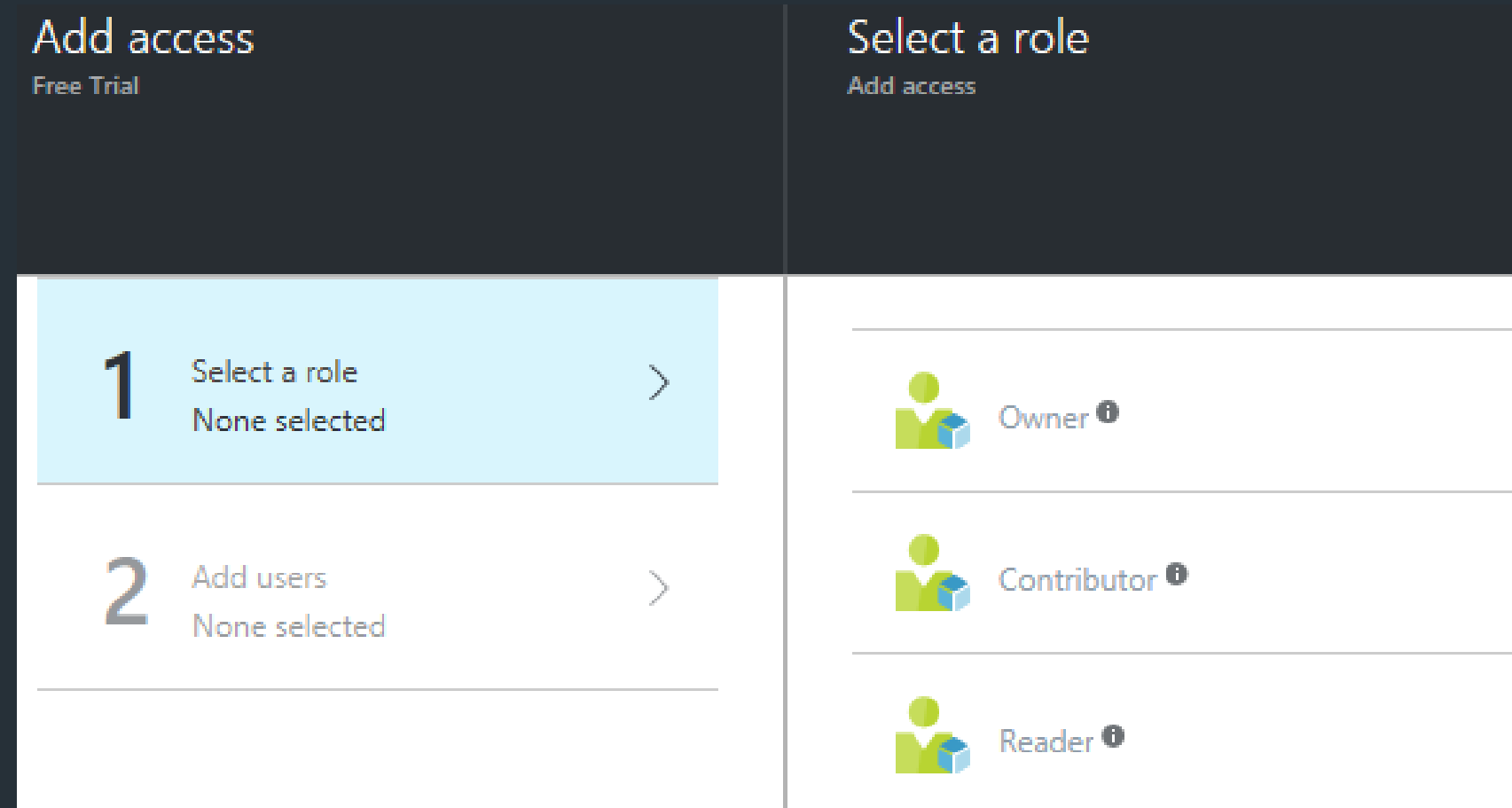
Access Controls

- + Classic model
- + Role Based Access Control (RBAC) – Resource Manager model
- + Azure Active Directory Identities
- + 3rd Party Authentication/Authorisation SSO
- + Multi-factor Authentication (MFA)

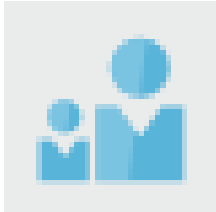
Azure Security Controls & Pentesting – User Access Controls

++ Role-Based Access Control (RBAC)

+ Fine-grained access configuration



+ Service administrators (Classic model) inherit 'Owner' user role:

USER	ROLE	ACCESS
 Subscription admins ⓘ	Owner	Inherited

Azure Security Controls & Pentesting – Access Controls

++

Authentication/Authorisation – Azure SQL Database

- + Administrator – dbo (member of the db_owner group)
- + Other Groups:
 - db_datareader – Grants read access to every table in the database.
 - dbmanager – Permissions to create new databases.
 - db_owner – Full control of a database.

Azure Security Controls & Pentesting – Access Controls

++ Authentication/Authorisation – Web Apps

Authentication / Authorization

Save Discard

Authentication / Authorization

Authentication / Authorization is a turn key solution that lets you control access to your a

App Service Authentication

Off On

- Allow request (no action)
- Log in with Azure Active Directory
- Log in with Facebook
- Log in with Google
- Log in with Microsoft Account
- Log in with Twitter

Azure Active Directory	Not Configured
Facebook	Not Configured
Google	Not Configured
Twitter	Not Configured
Microsoft Account	Not Configured

Azure Security Controls & Pentesting

++

Scanning Azure Services Externally

+ Vnet Gateway (65535 ports TCP, 1000 ports UDP)

- 443/tcp, 8443/tcp, 8444/tcp, 10001/tcp, 10002/tcp, 20000/tcp
- 500/udp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

+ Azure SQL Server (65535 ports TCP)

- 443/tcp, 1433/tcp, 1434/tcp, 1439/tcp, 5002/tcp, 5022/tcp, 5024/tcp, 8000/tcp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

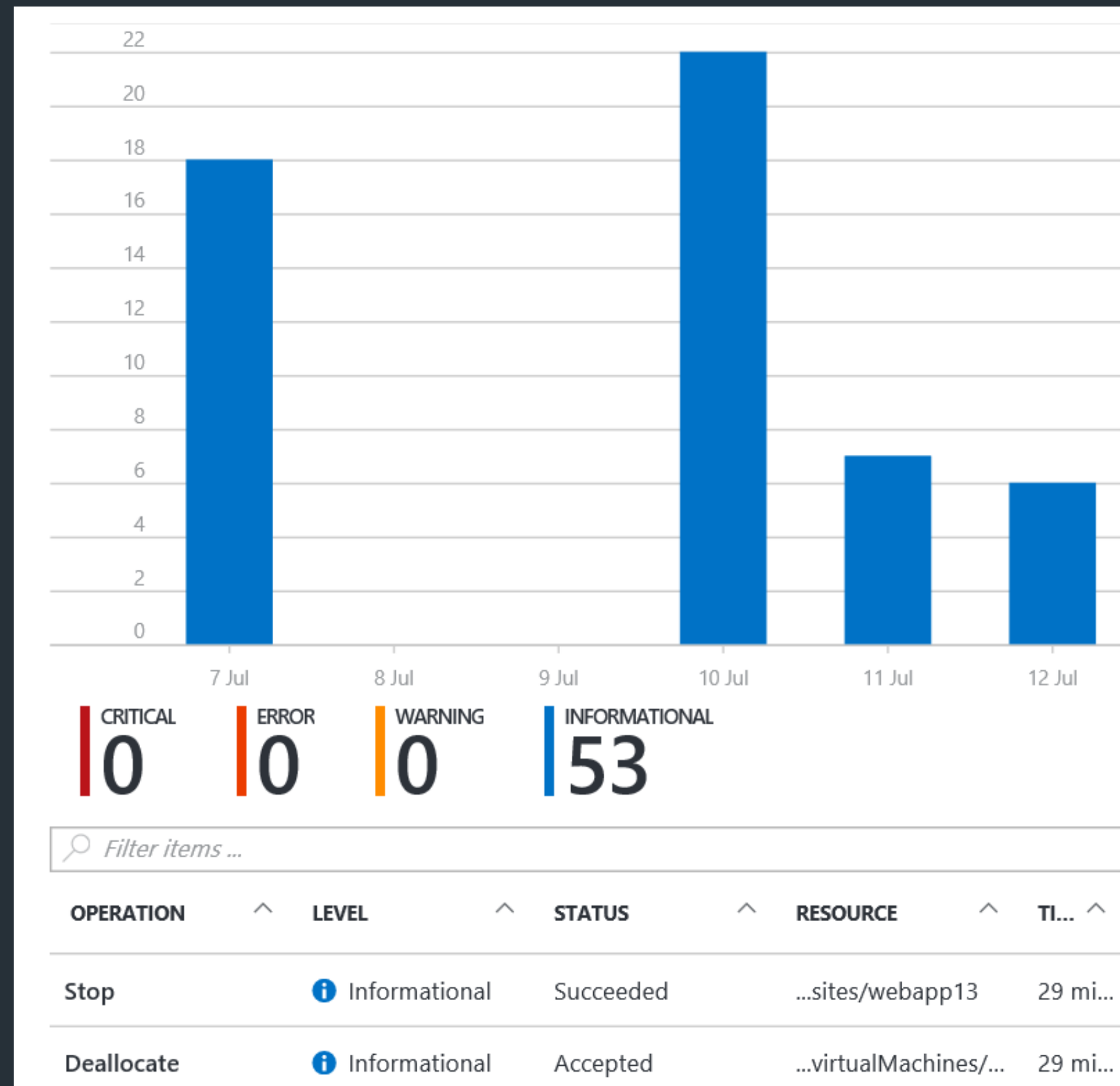
+ Azure Web App (65535 ports TCP)

- 80/tcp, 443/tcp, 454/tcp, 455/tcp, 1221/tcp, 4016/tcp, 4018/tcp, 4020/tcp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Azure Security Controls & Pentesting – Auditing & Monitoring

++

Auditing & Monitoring

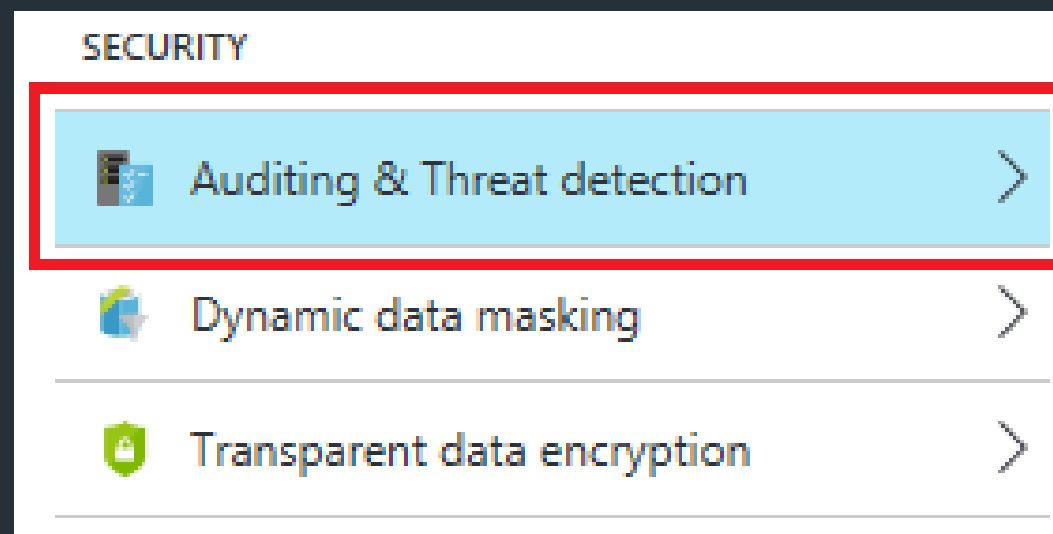


Azure Security Controls & Pentesting – Auditing & Monitoring

++

Auditing – Azure SQL Server

+ Auditing configuration



Auditing Settings

Default settings for all databases on server

Save as default Discard Feedback

Auditing

ON OFF

Downlevel clients require the use of Security Enabled Connection Strings.

* Storage Details >
teststorageaccount13

Audited Events >
All

Audited Events

Event Category	<input checked="" type="checkbox"/> Success	<input checked="" type="checkbox"/> Failure
Plain SQL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Parameterized SQL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Stored Procedure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Login	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transaction Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

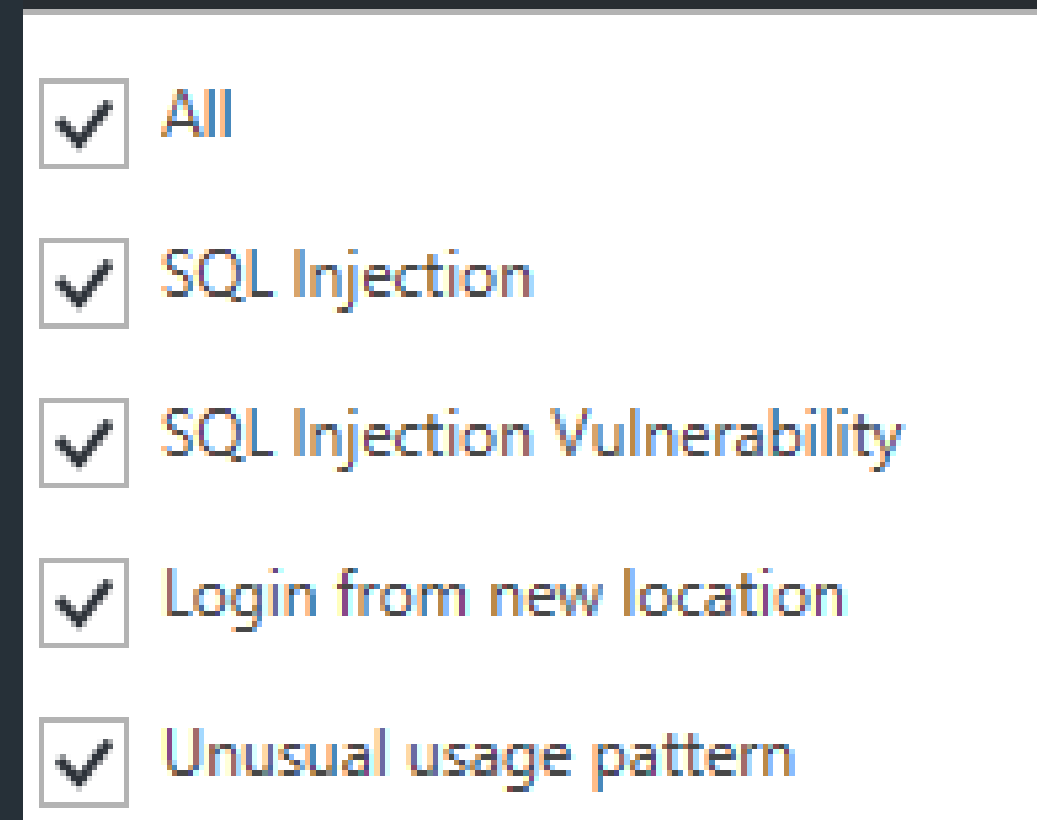
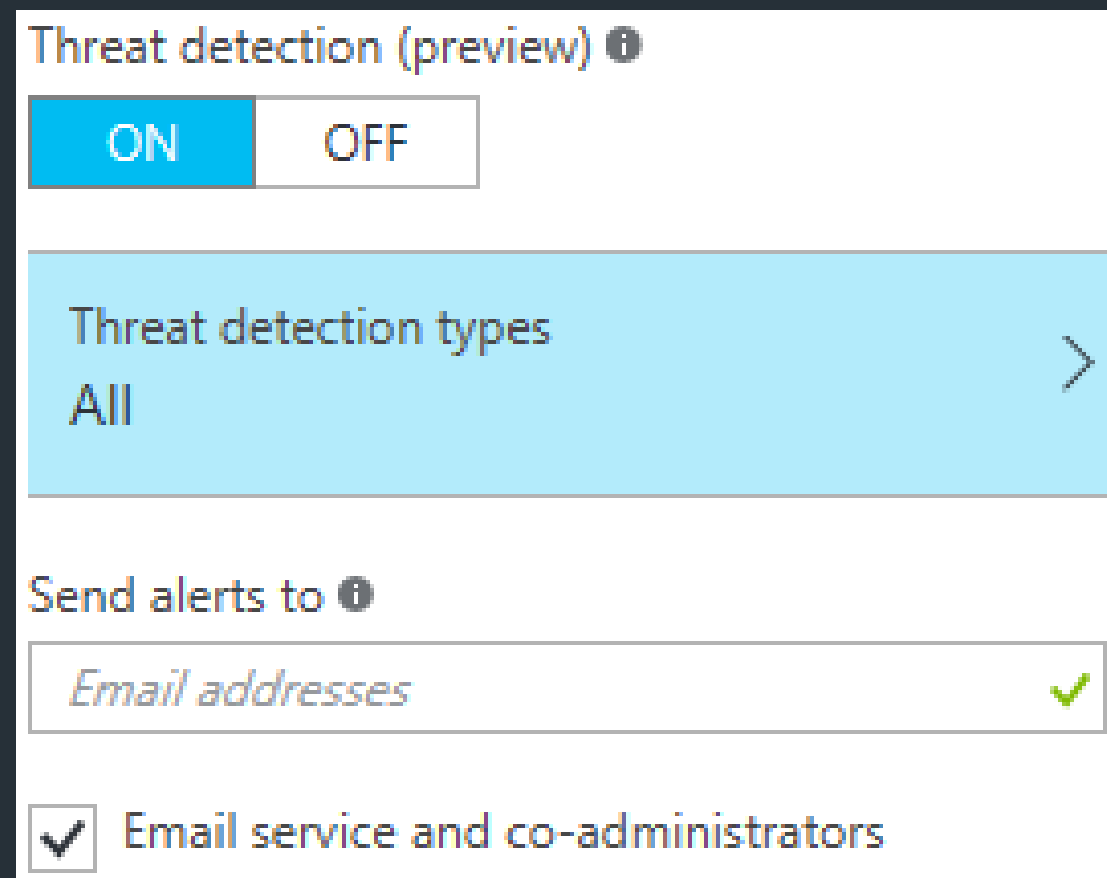
Azure Security Controls & Pentesting – Auditing & Monitoring

++

Threat Detection – Azure SQL Server

+ Threat detection

Threat detection types

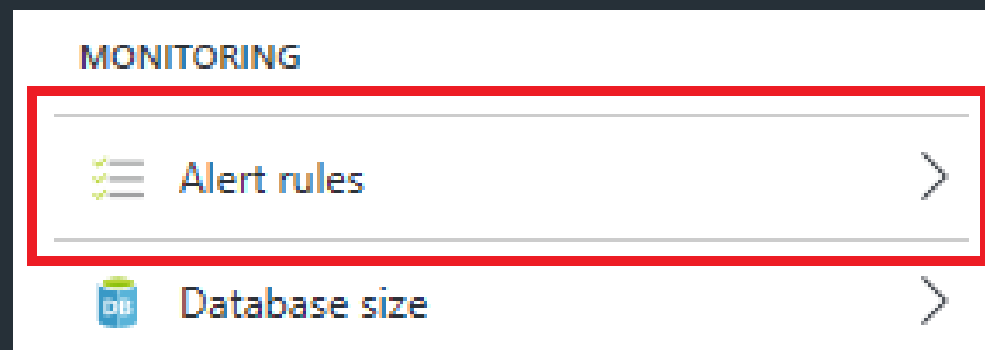


Azure Security Controls & Pentesting – Auditing & Monitoring

++

Monitoring – Azure SQL Server

+ Monitoring of various events based on configured rules.



Add an alert rule

A screenshot of the 'Add an alert rule' configuration page in Azure. The page is divided into several sections:

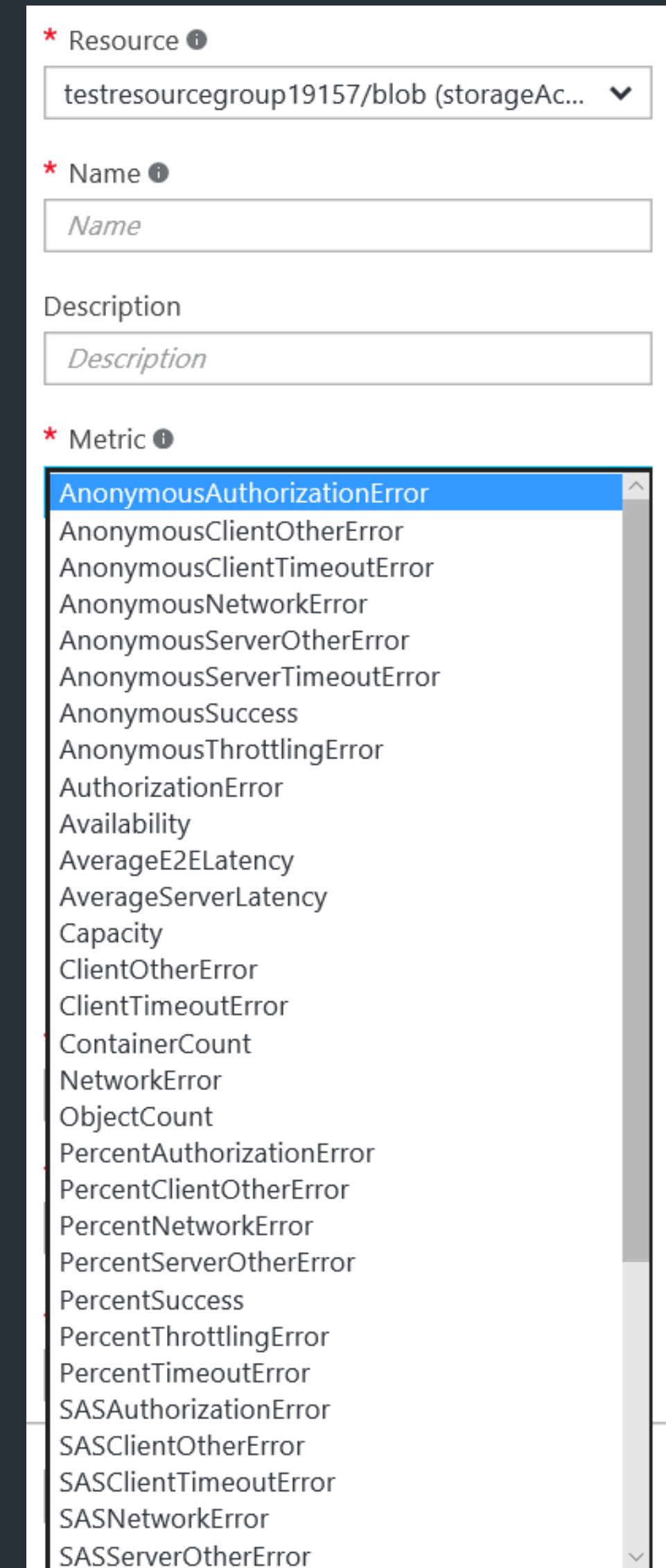
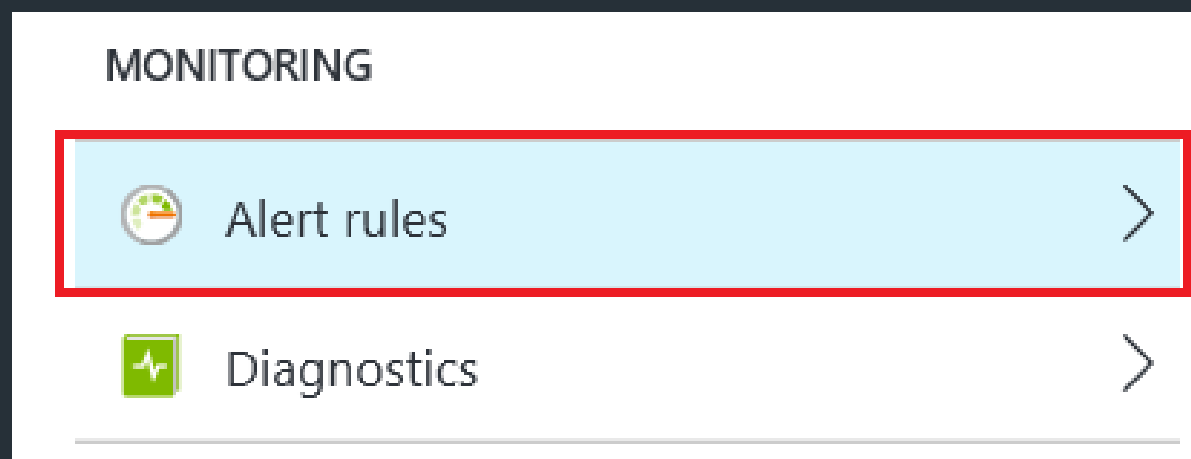
- * Resource:** A dropdown menu showing a resource ID: `/r1/azuresqldb (servers/d...`.
- * Name:** A text input field with the placeholder text `Name`.
- Description:** A text input field with the placeholder text `Description`.
- * Metric:** A list of metrics with 'Blocked by Firewall' selected and highlighted in blue. Other metrics include: Failed Connections, Successful Connections, CPU percentage, Deadlocks, DTU percentage, Log IO percentage, Data IO percentage, Total database size, Database size percentage, and In-Memory OLTP storage percent(Preview). Below the list is a small line graph showing a flat line at zero.
- * Condition:** A dropdown menu set to 'greater than'.
- * Threshold:** A text input field containing the value '1'. Below the field is the unit 'count'.
- * Period:** A dropdown menu set to 'Over the last 5 minutes'.
- Email owners, contributors, and readers:** An unchecked checkbox.
- Additional administrator email(s):** A text input field with the placeholder text `Add email addresses separated by semicolons`.

Azure Security Controls & Pentesting – Auditing & Monitoring

++

Monitoring – Azure Storage

+ Monitoring of various events based on configured rules.



Azure Security Controls & Pentesting –
Azure Security Centre

++

Azure Security Centre

+ Prevention

- Centralised management of deployed security controls.
- Immediate mitigation of defects through the interface.

+ Detection

- Monitoring of systems' security status.
- Identification of potential threats.

Azure Security Controls & Pentesting - Azure Security Centre

++

Azure Security Centre - Prevention



Azure Security Controls & Pentesting – Azure Security Centre

++

Azure Security Centre – Prevention

+ Security Policy

- Recommendations based on specific security policy e.g. baseline rules, web application firewall
- The results represent the health of the deployed resources.
- Provides recommendations for remedial actions to be taken.

The screenshot shows the 'Security policy' configuration page in Azure Security Centre. At the top, there are three buttons: 'Save', 'Discard', and 'Delete agents'. Below this, the 'Data collection' section has a toggle for 'Collect data from virtual machines' set to 'On'. A note indicates 'Choose a storage account per region' with 'Nothing to configure'. The 'Show recommendations for' section lists several security features, all of which are currently turned 'On': System updates, Baseline rules, Antimalware, Access Control List on endpoints, Network Security Groups, Web Application Firewall, SQL Auditing, and SQL Transparent Data Encryption.

Recommendation	On	Off
System updates	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Baseline rules	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Antimalware	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Access Control List on endpoints	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Network Security Groups	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web Application Firewall	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SQL Auditing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SQL Transparent Data Encryption	<input checked="" type="checkbox"/>	<input type="checkbox"/>

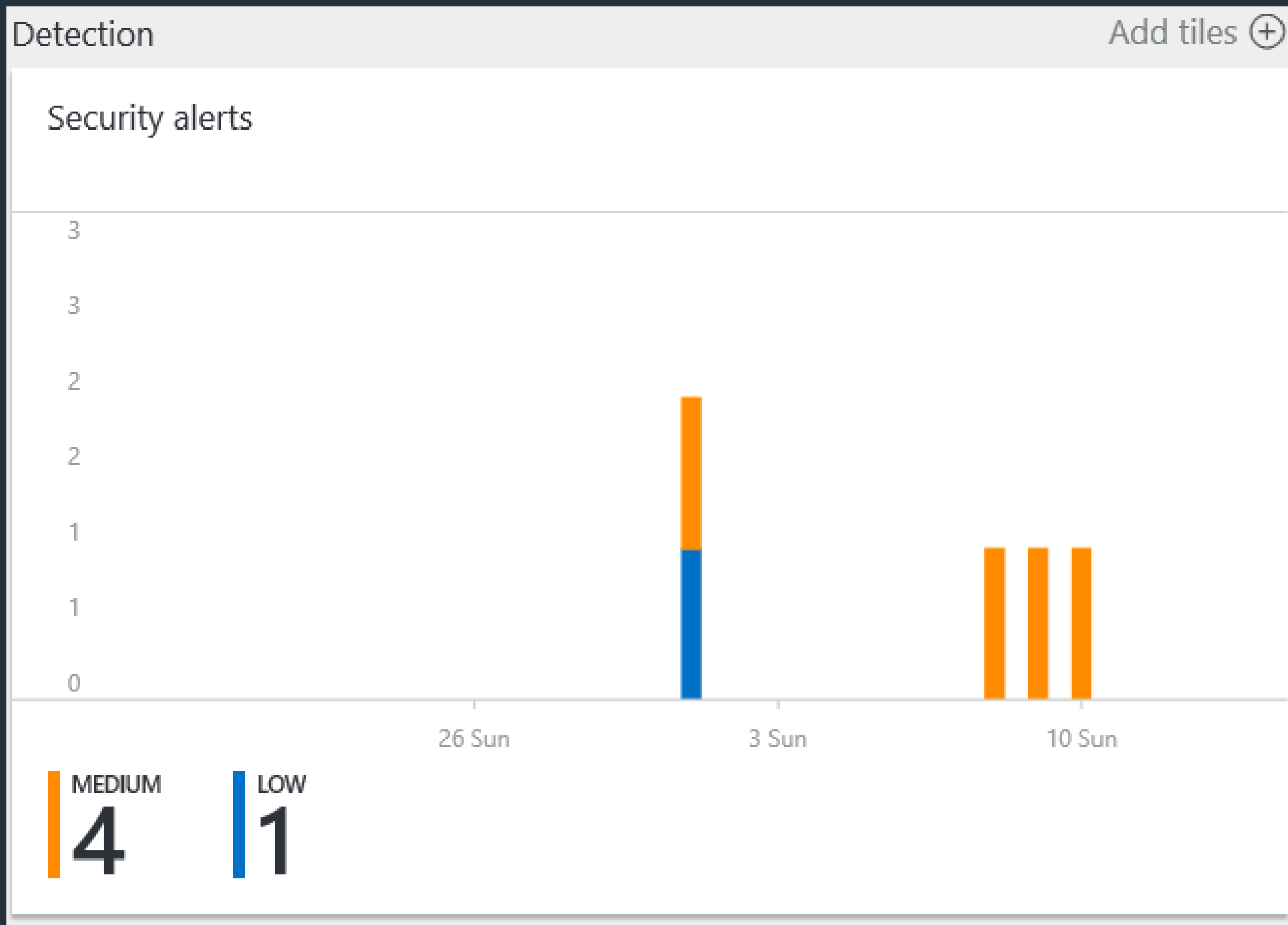
PUBLIC



Azure Security Controls & Pentesting –
Azure Security Centre

++

Azure Security Centre - Detection



Azure Security Controls & Pentesting – Azure Security Centre

++

Azure Security Centre – Detection

+ Detailed description of any unauthorised and/or malicious attempts and actions that took place to address an attack.

Failed RDP Brute Force Attack
windows1 - PREVIEW

Failed RDP Brute Force Attack
PREVIEW

Filter

ATTACKED RESOURCE	COUNT	DETECTION...	ST...	SEVERI...
windows1	1	08:59:26 AM	Active	⚠ Medium ...



DESCRIPTION	Several Remote Desktop login attempts were detected from Windows7, none of them succeeded. Event logs analysis shows that in the last 46 minutes there were 153 failed attempts. 152 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.
DETECTION TIME	Friday, 1 July 2016 08:59:26
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	windows1
DETECTED BY	Microsoft
ACTION TAKEN	Detected
SOURCE	Windows7
ALERT START TIME (UTC)	07/01/2016 07:13:55
NON-EXISTENT USERS	152
EXISTING USERS	1
FAILED ATTEMPTS	153
SUCCESSFUL LOGINS	0
ATTACK DURATION	46 minutes

Azure Security Controls & Pentesting – Azure Security Centre

++

Azure Security Centre – Detection

+ Integration with the Azure extensions and reporting of identified issues.

Antimalware Action Taken
PREVIEW

Filter

ATTACKED RESOURCE	COUNT	DETECTION...	ST...	SEVERI...
windows1	1	14:49:11	Active	Low
windows1	1	13:28:48	Active	Low



Antimalware Action Taken
windows1 - PREVIEW

Microsoft Antimalware has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
http://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=1

DESCRIPTION
Name: Virus:DOS/EICAR_Test_File
ID: 2147519003
Severity: Severe
Category: Virus
Path:
file:_C:\Users\vmuser\AppData\Local\Microsoft\Windows\INetCache\IE\PKETD7EM\eicar[1].com
Detection Origin: Internet
Detection Type

DETECTION TIME Friday, 1 July 2016 13:28:48

SEVERITY Low

STATE Active

ATTACKED RESOURCE windows1

DETECTED BY Microsoft Antimalware

ACTION TAKEN Blocked



Contents

1. Cloud Services Trends, Challenges & Azure
2. Azure Security Controls & Pentesting
3. Azurite – Explore & Visualize
4. Conclusions

PUBLIC

MWR
LABS

—| Azurite Explorer & Azurite
visualizer

++

Azurite Explorer

+ <https://www.youtube.com/watch?v=Ntm-VagQiJQ>

PUBLIC



—| Azurite Explorer & Azurite
visualizer

++

Azurite visualizer

+ https://www.youtube.com/watch?v=PvzSc28_NLA

Conclusions

- + Familiarisation with Azure terms, building blocks and security controls is required.
- + Azure provides various tools to support testing activities.
- + Azure provides functionality to apply best practices and secure deployments.
- + Not the most mature Cloud platform, but it's getting there gradually at least from a security perspective.



PUBLIC



```
PS> Listen-ToTheAudience
```

```
+ @mwr1abs
```

```
https://labs.mwrinfosecurity.com
```

```
+ Azurite Explorer and  
Azurite Visualizer code on Github
```

```
https://github.com/mwr1abs/Azurite
```