PUBLIC

A Penetration Tester's Guide to the Azure Cloud

Apostolos Mastoris

22nd July 2016

MWR LABS

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.

MWR LABS

Contents

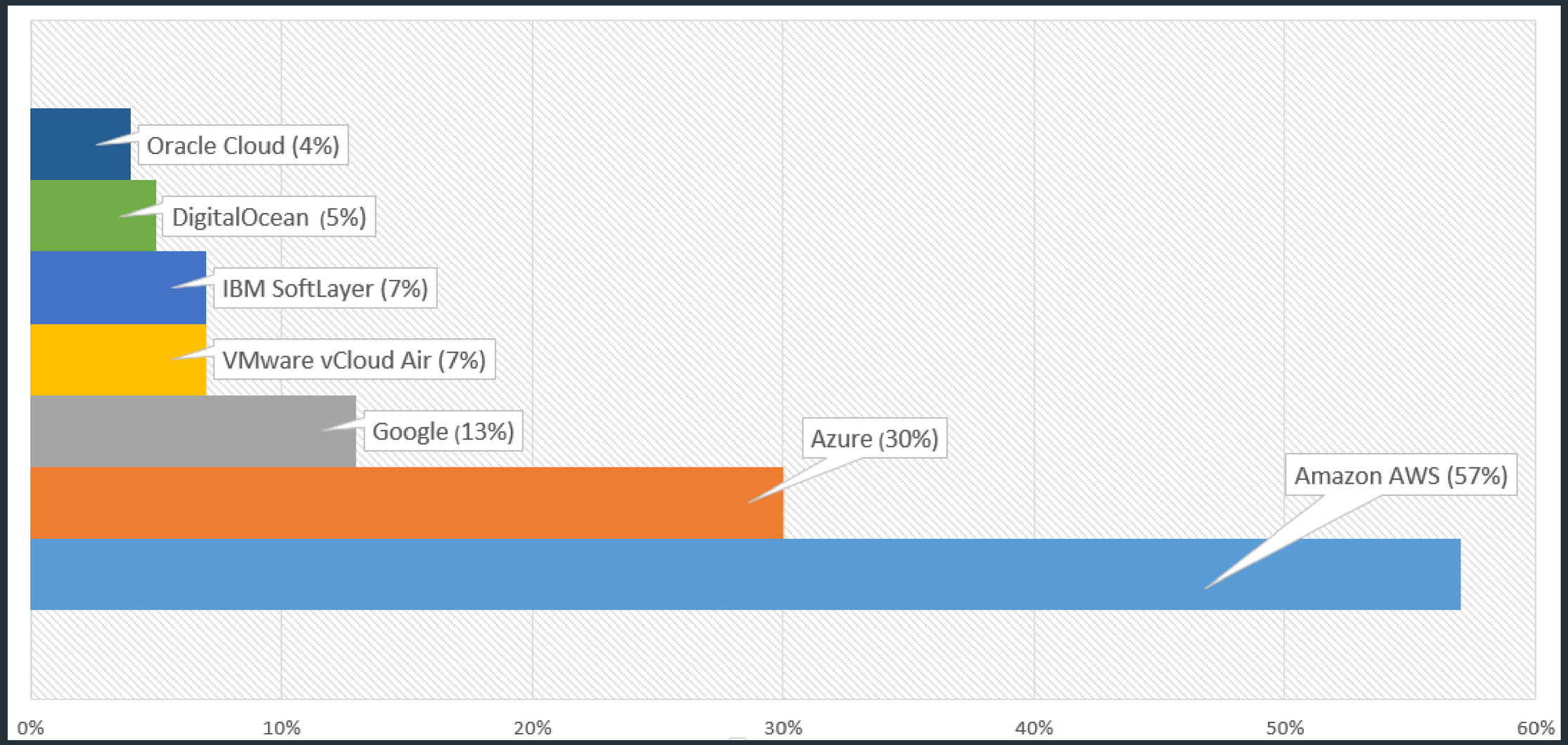
1. Cloud Services Trends, Challenges & Azure
2. Azure Security Controls & Pentesting
3. Azurite - Explore & Visualize
4. Conclusions

Cloud Services Trends, Challenges & Azure

MWR LABS

++

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



Source: RightScale 2016 State of the Cloud Report

++

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

MWR LABS

++ Azure Service Models & Responsibilities

MWR LABS

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)

++

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

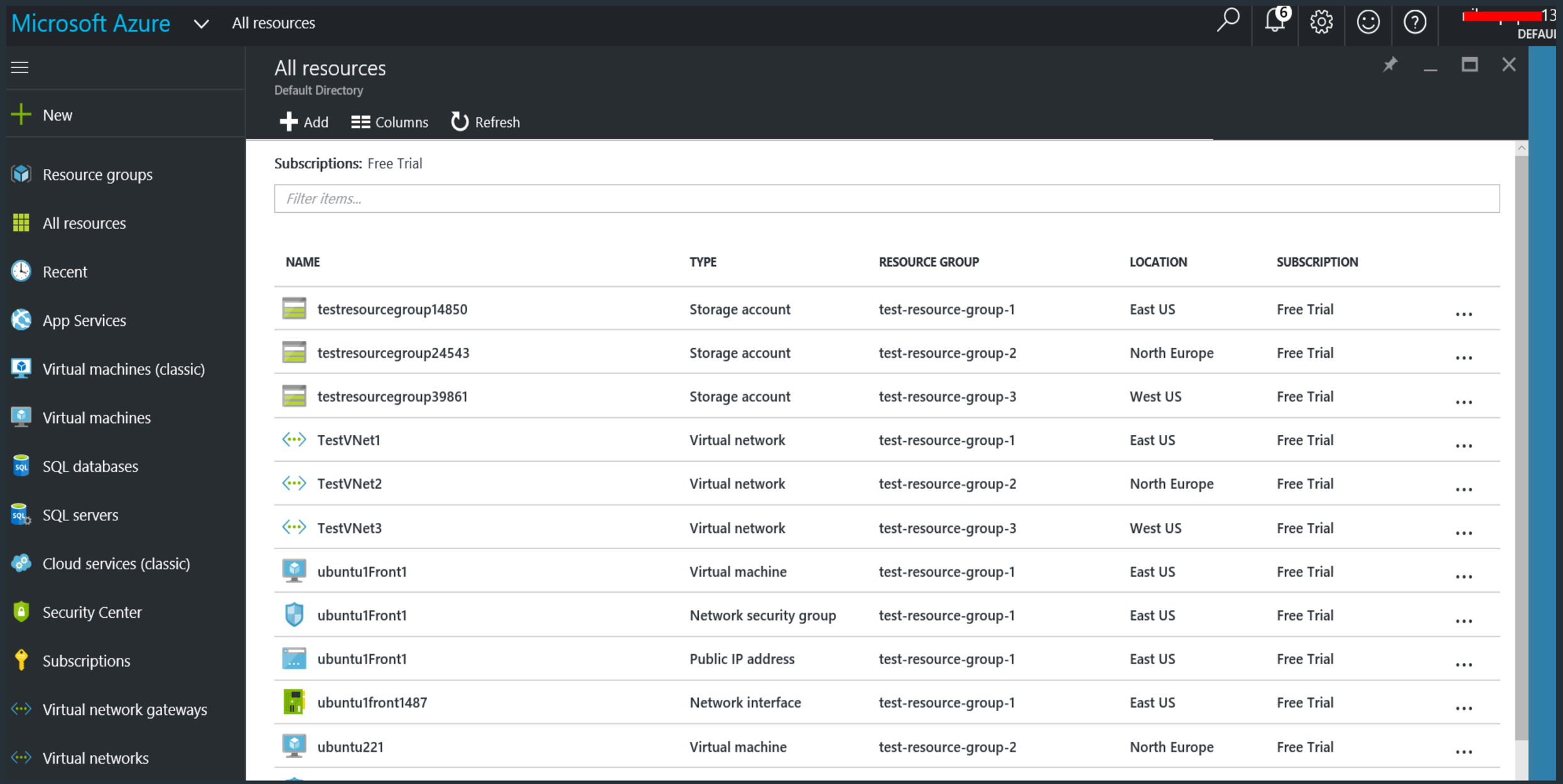
PUBLIC

Cloud Services Trends, Challenges & Azure – Azure Management

MWR LABS

++

Azure Portal



MWR LABS

Contents

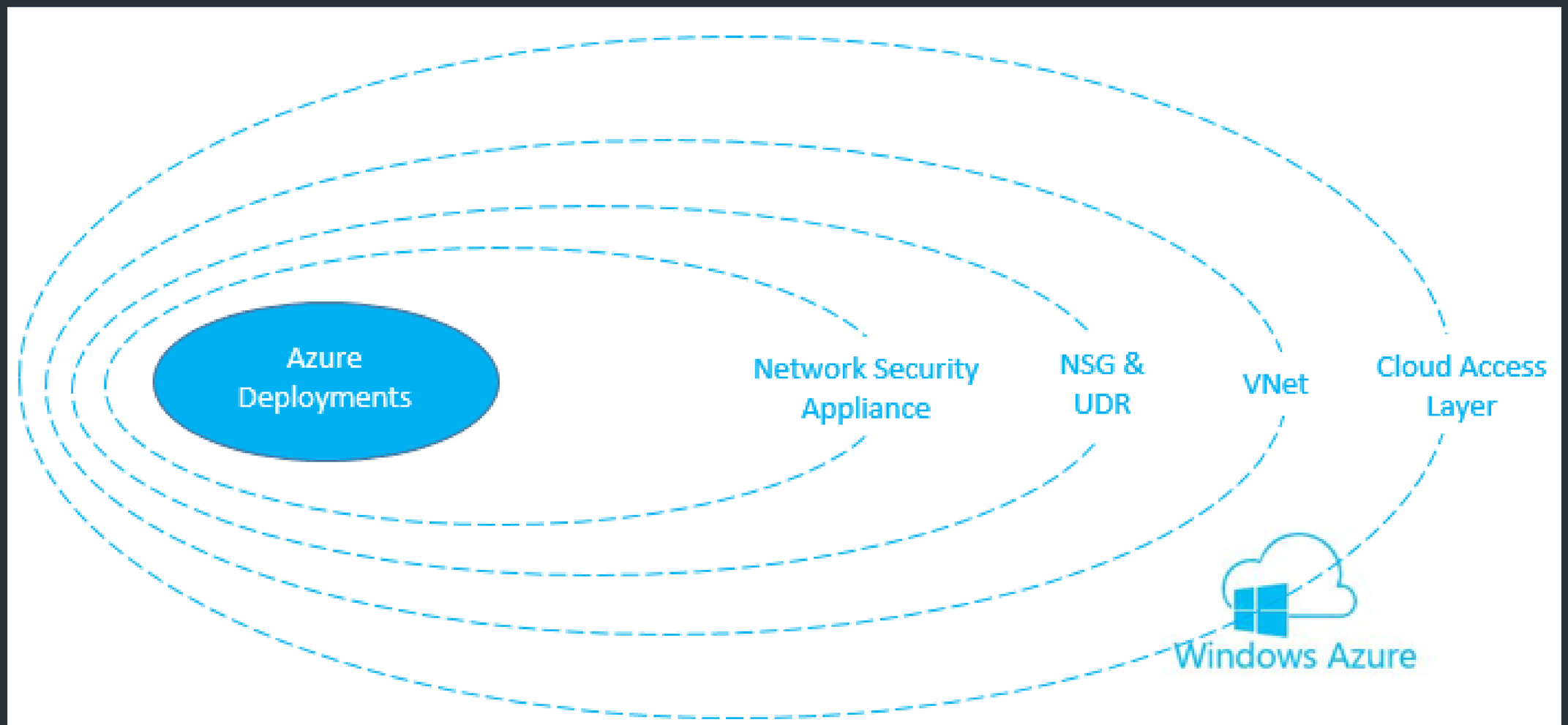
1. Cloud Services Trends, Challenges & Azure
2. Azure Security Controls & Pentesting
3. Azurite - Explore & Visualize
4. Conclusions

MWR LABS

++

Network Security

+ Azure provides controls to secure each network layer:



Source: Microsoft Azure

++

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)

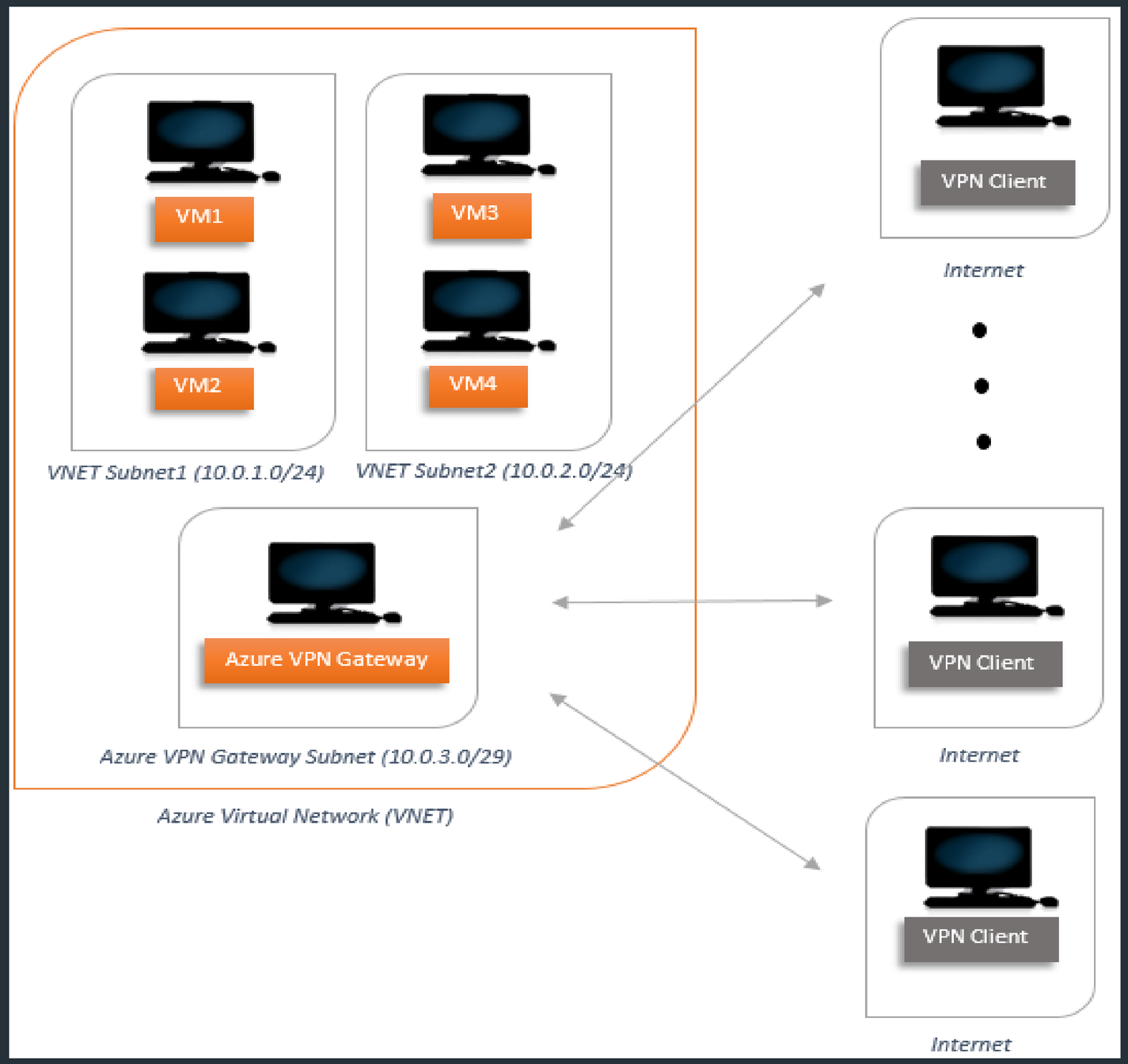
++

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

++

VNet – Point-to-Site VPN



Azure Security Controls & Pentesting - Network Security

MWR LABS

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

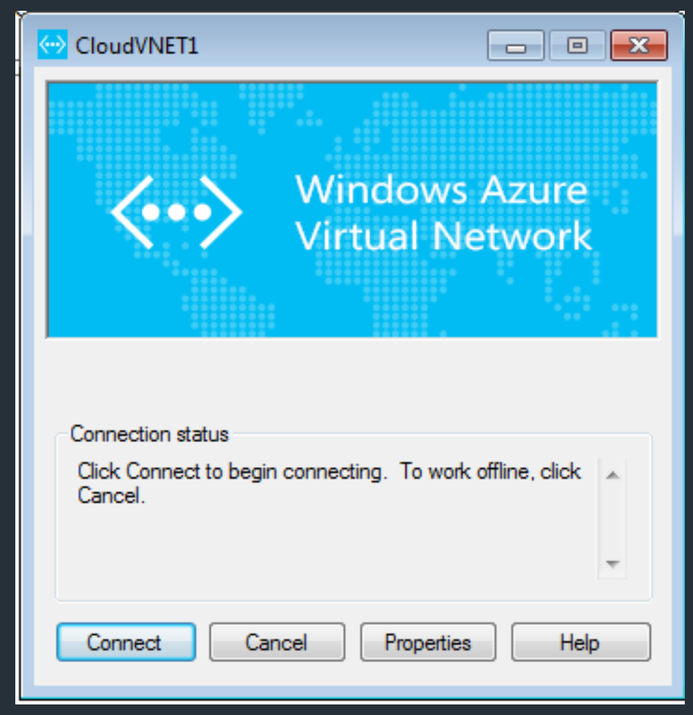
+ Tenant to generate client certificate for authentication to VPN service.

+ 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.

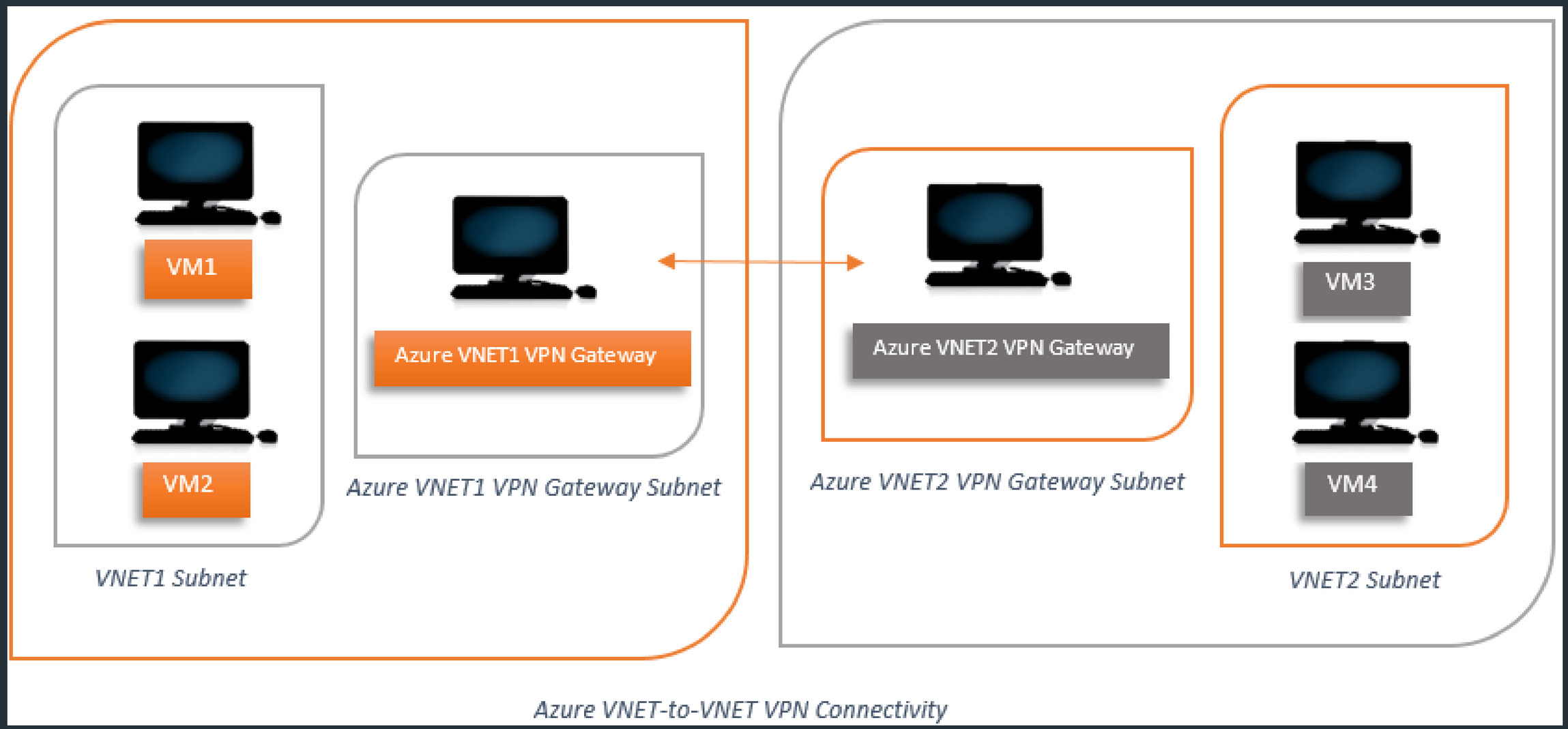


Azure Security Controls & Pentesting - Network Security

MWR LABS

++

VNet – Site-to-Site (S2S) VPN

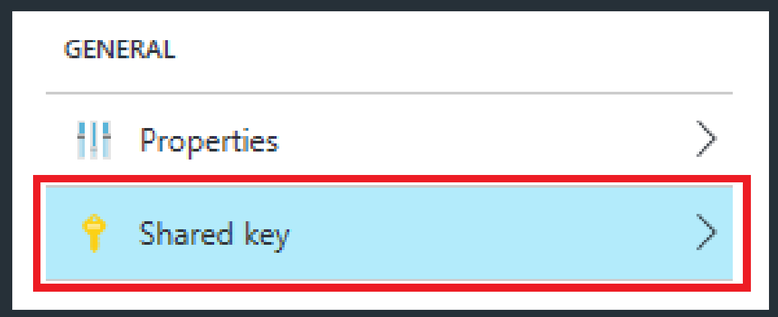


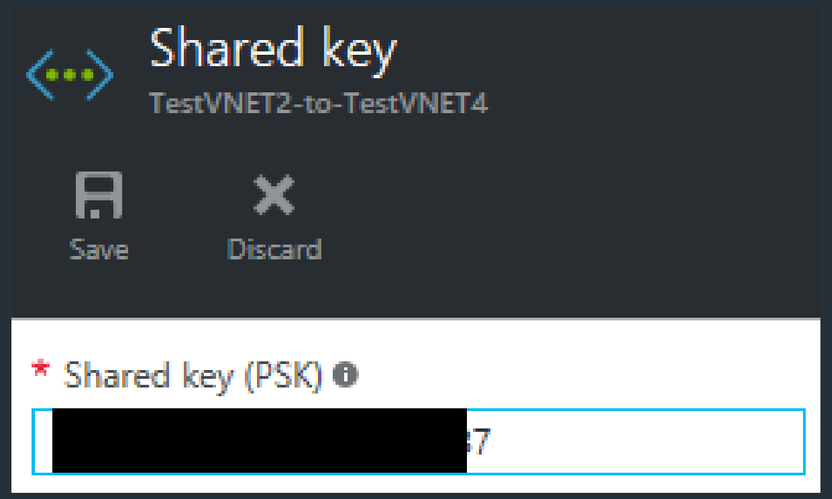
Azure VNET-to-VNET VPN Connectivity

++

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:





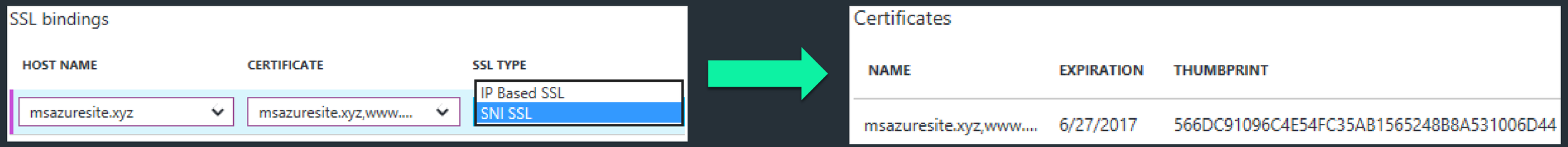
Azure Security Controls & Pentesting - Transport Security

MWR LABS

++

Transport Security - Web Apps

+ SSL/TLS Certificate



- IP-based or SNI-based

+ Extensions for ‘Let’s encrypt’ CA support

+ Extension to enforce HTTPS access.

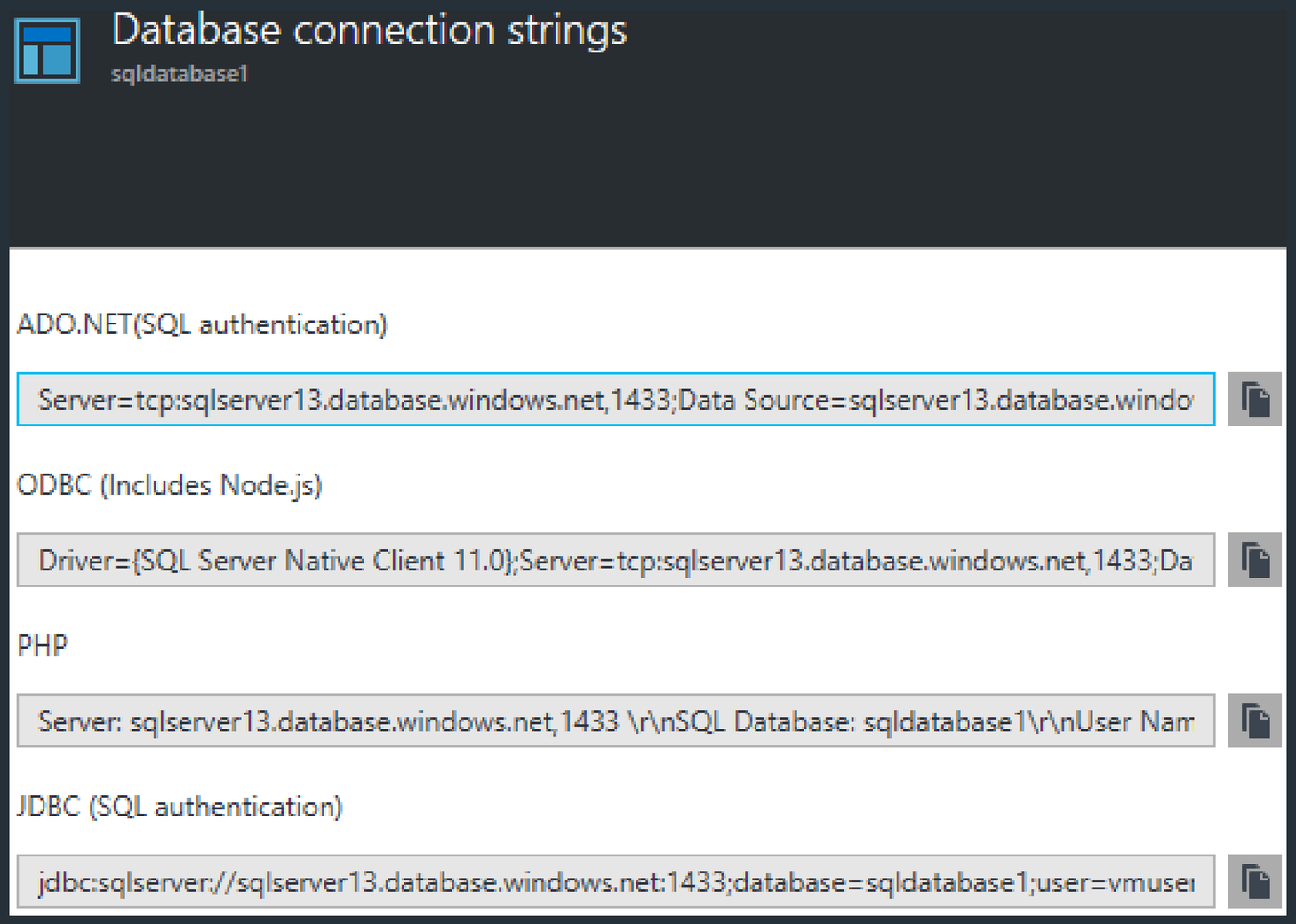
+ Configuration to redirect from HTTP to HTTPS: https://azure.microsoft.com/en-us/documentation/articles/web-sites-configure-ssl-certificate/

Azure Security Controls & Pentesting - Transport Security

MWR LABS

++ Transport Security – Azure SQL Database

+ Azure SQL Database connection strings



Azure Security Controls & Pentesting - Transport Security

MWR LABS

++ 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

MWR LABS

++ 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

MWR LABS

++ 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

++

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.

++

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.

Azure Security Controls & Pentesting – Network Access Control

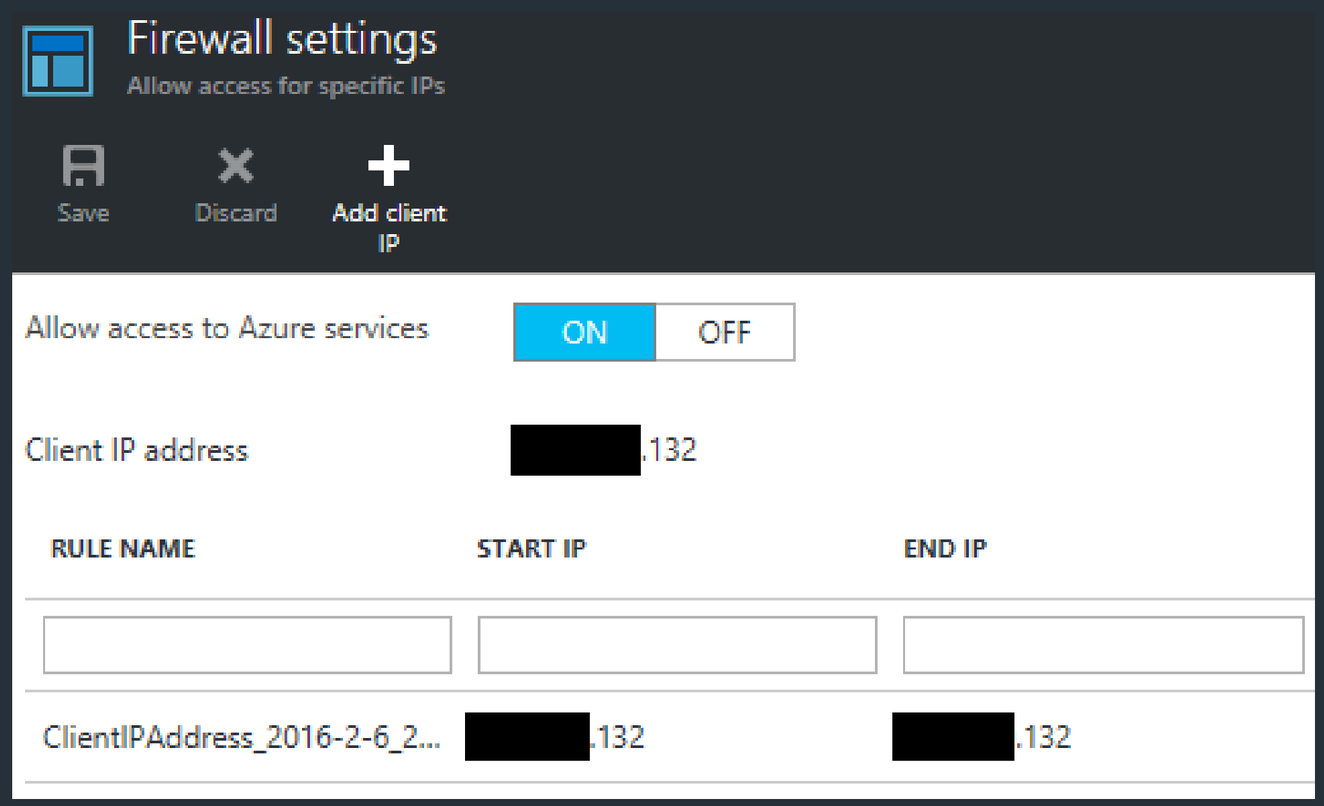
MWR LABS

++ 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.



Azure Security Controls & Pentesting – Network Access Control

MWR LABS

++ 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

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

++ 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 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 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 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.

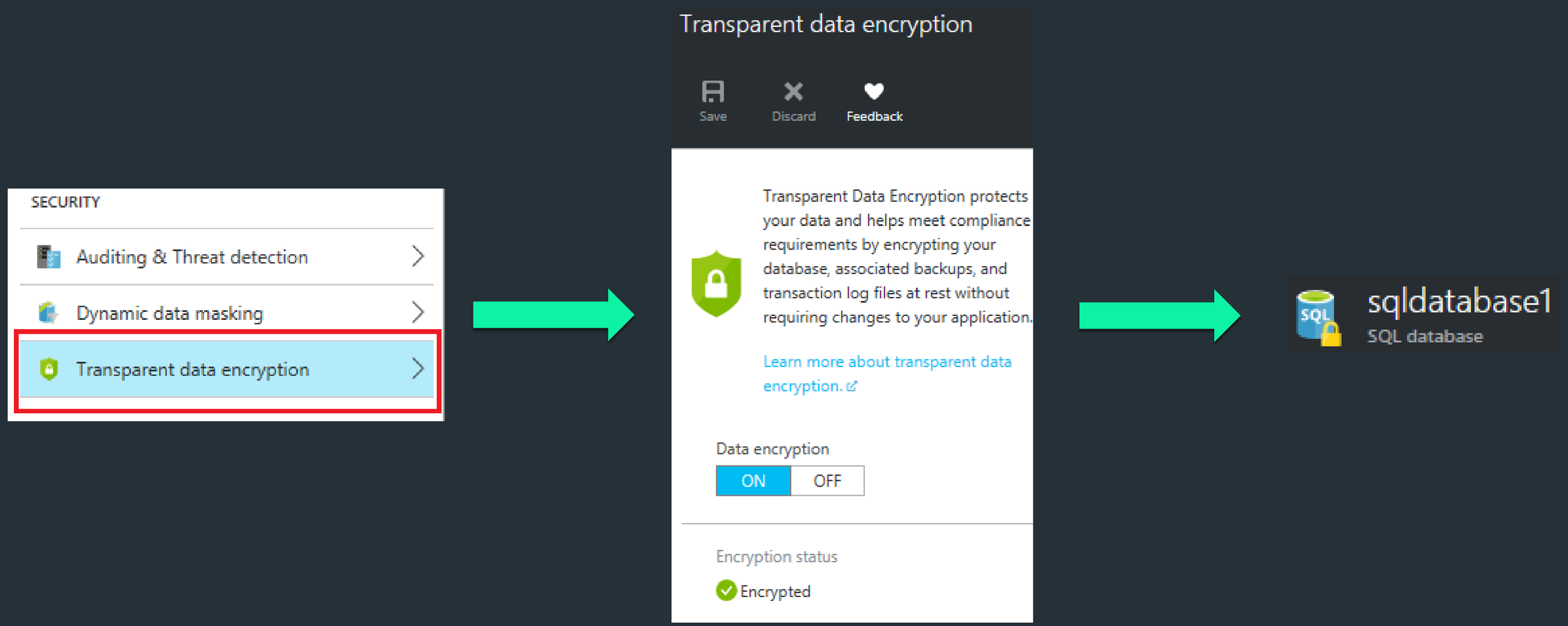
+ Key operations:

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

++

Azure SQL Database

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



++

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:

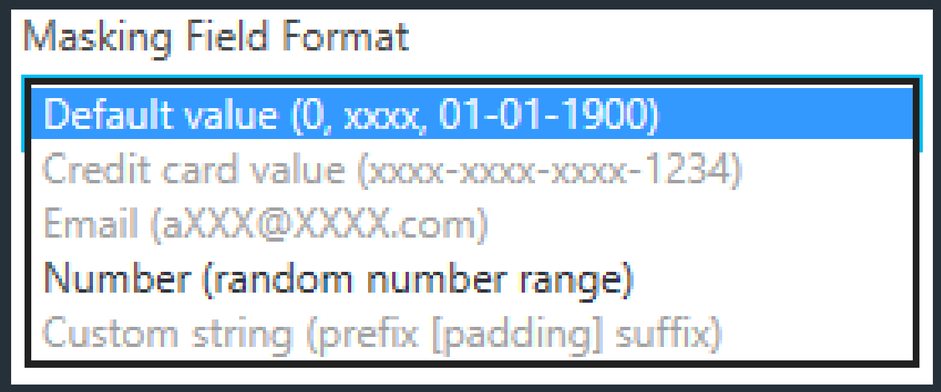
	database_id	encryption_state	create_date	regenerate_date	modify_date	set_date	opened_date	key_algorithm	key_length	encryptor_thumbprint	encryptor_type
1	2	3	2016-07-10 20:09:28.457	2016-07-10 20:09:28.457	2016-07-10 20:09:28.457	1900-01-01 00:00:00.000	2016-07-10 20:09:28.457	AES	256	0x	ASYMMETRIC KEY
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]515B	CERTIFICATE

++

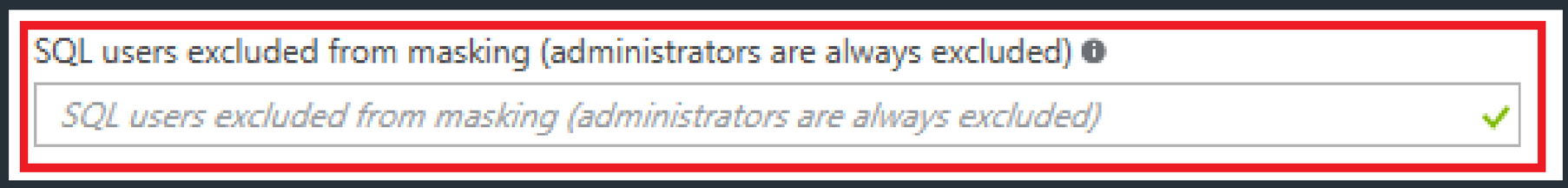
Database Data Masking

+ 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:



MWR LABS

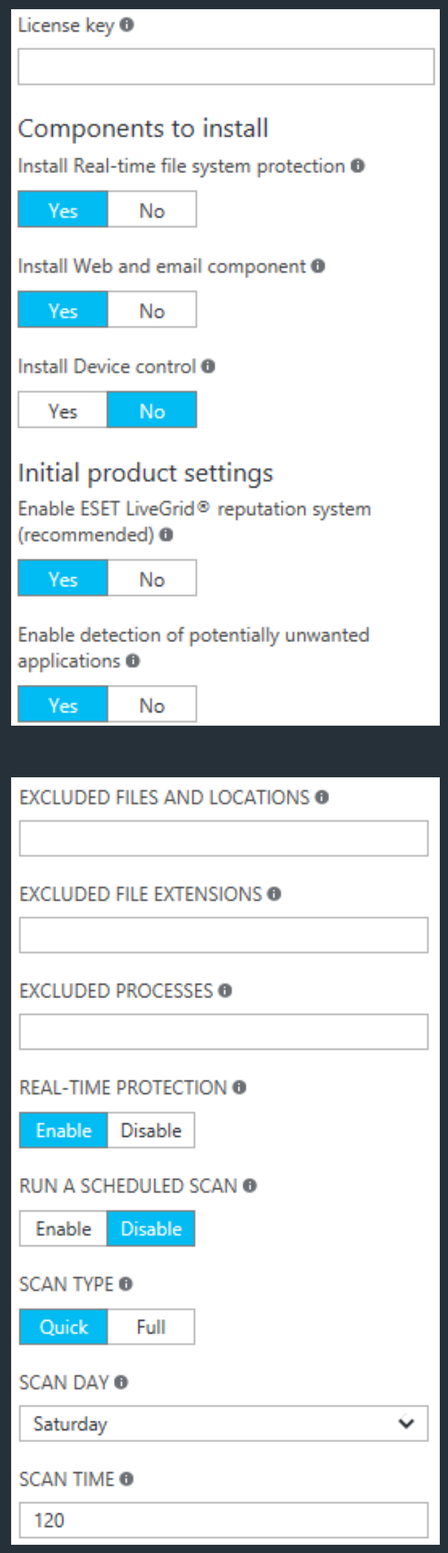
Azure Security Controls & Pentesting

++

Endpoint Protection

+ Anti-virus & Anti-Malware Extensions

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

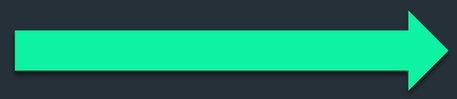


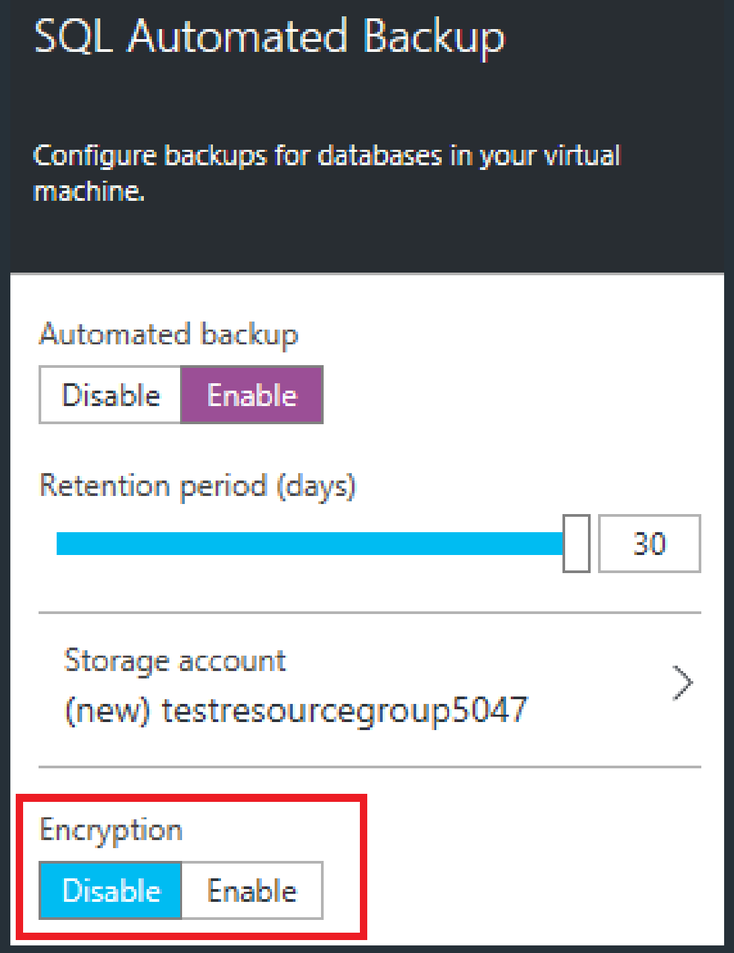
Azure Security Controls & Pentesting – Backup Security

MWR LABS

++ Backup Security

+ MSSQL – Configuration during VM creation:





+ Azure SQL Database

MWR LABS

++

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)

PUBLIC

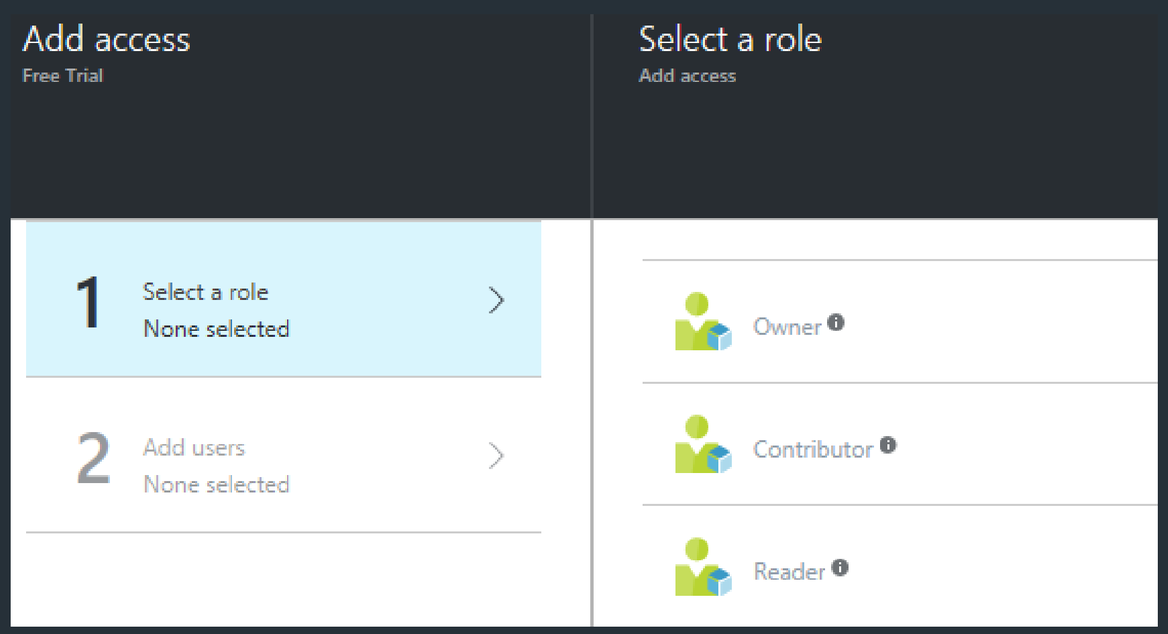
Azure Security Controls & Pentesting – User Access Controls

MWR LABS

++

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

MWR LABS

++ Authentication/Authorisation – Azure SQL Database

+ Administrator – dbo (member of the db_owner group)

+ Other Groups:

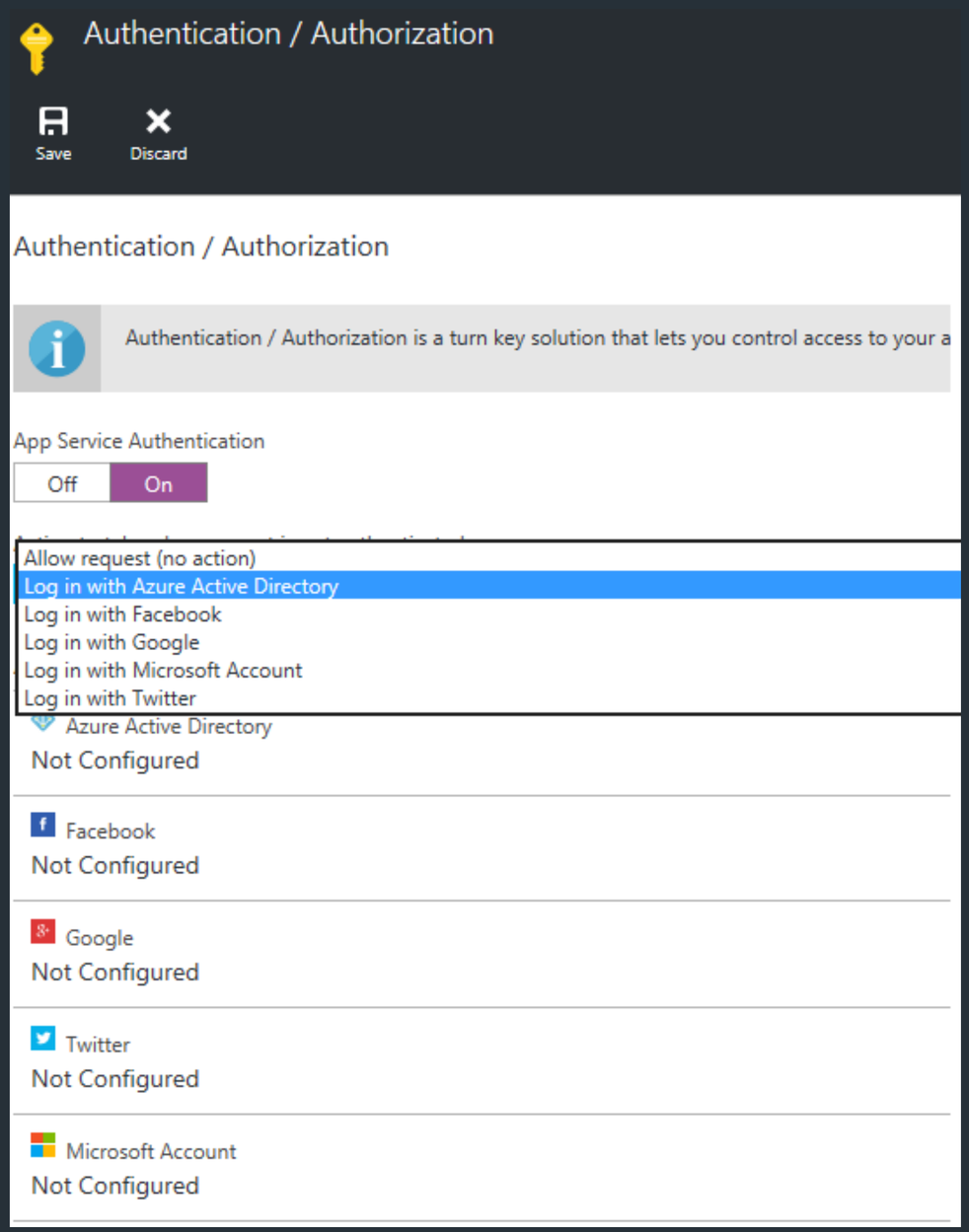
- db_datareader – Grants read access to every table in the database.
- dbmanager – Permissions to create new databases.
- db_owner – Full control of a database.

PUBLIC

Azure Security Controls & Pentesting – Access Controls

MWR LABS

++ Authentication/Authorisation – Web Apps



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
```

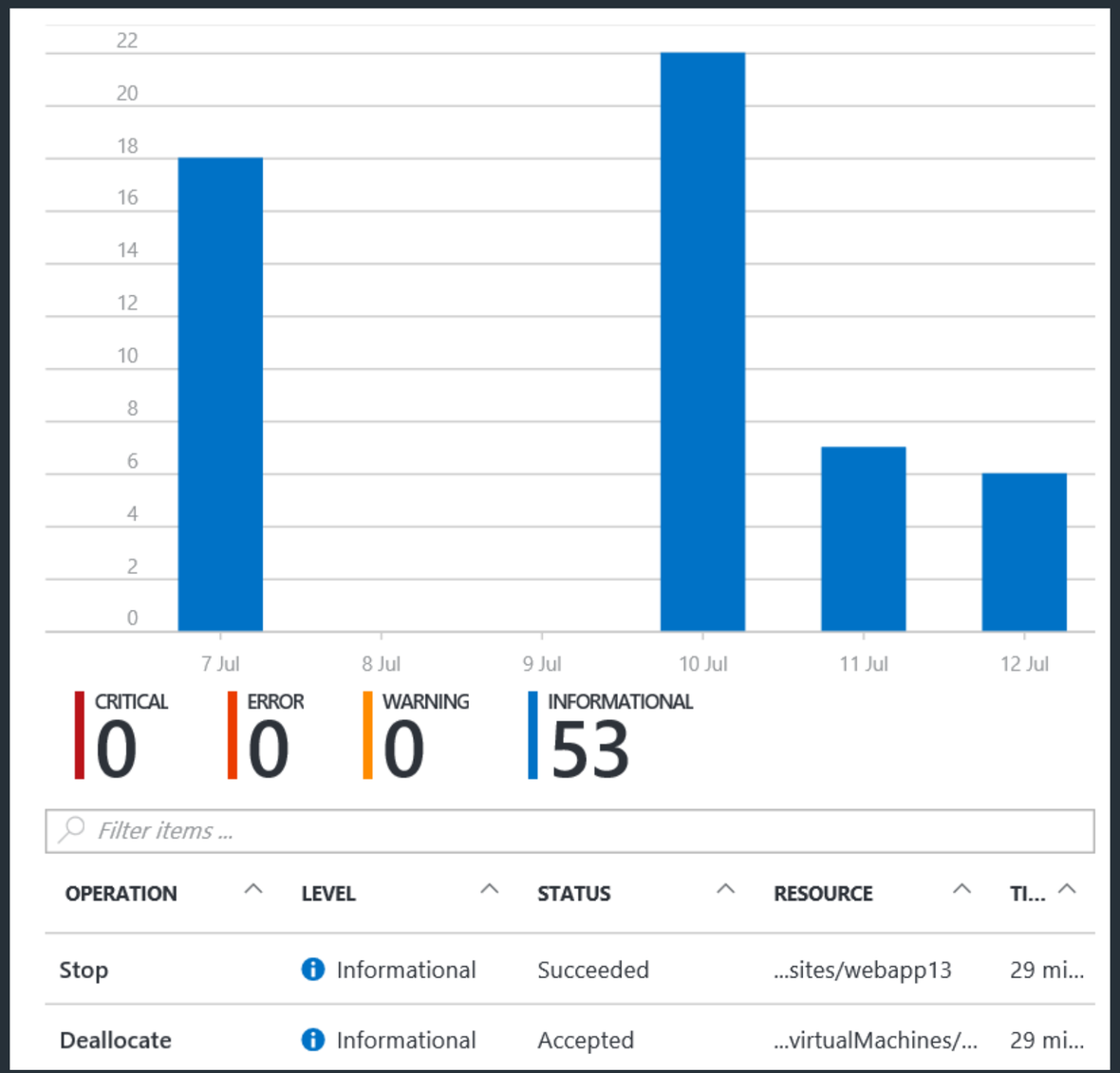
+ Azure Web App (65535 ports TCP)
  - 80/tcp, 443/tcp , 454/tcp, 455/tcp , 1221/tcp, 4016/tcp, 4018/tcp, 4020/tcp

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

MWR LABS

++

Auditing & Monitoring

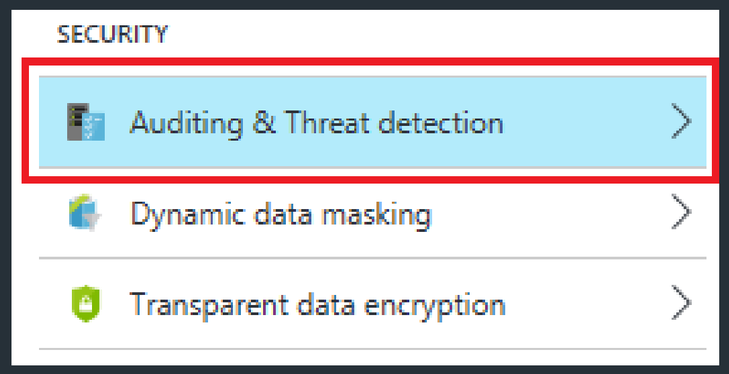


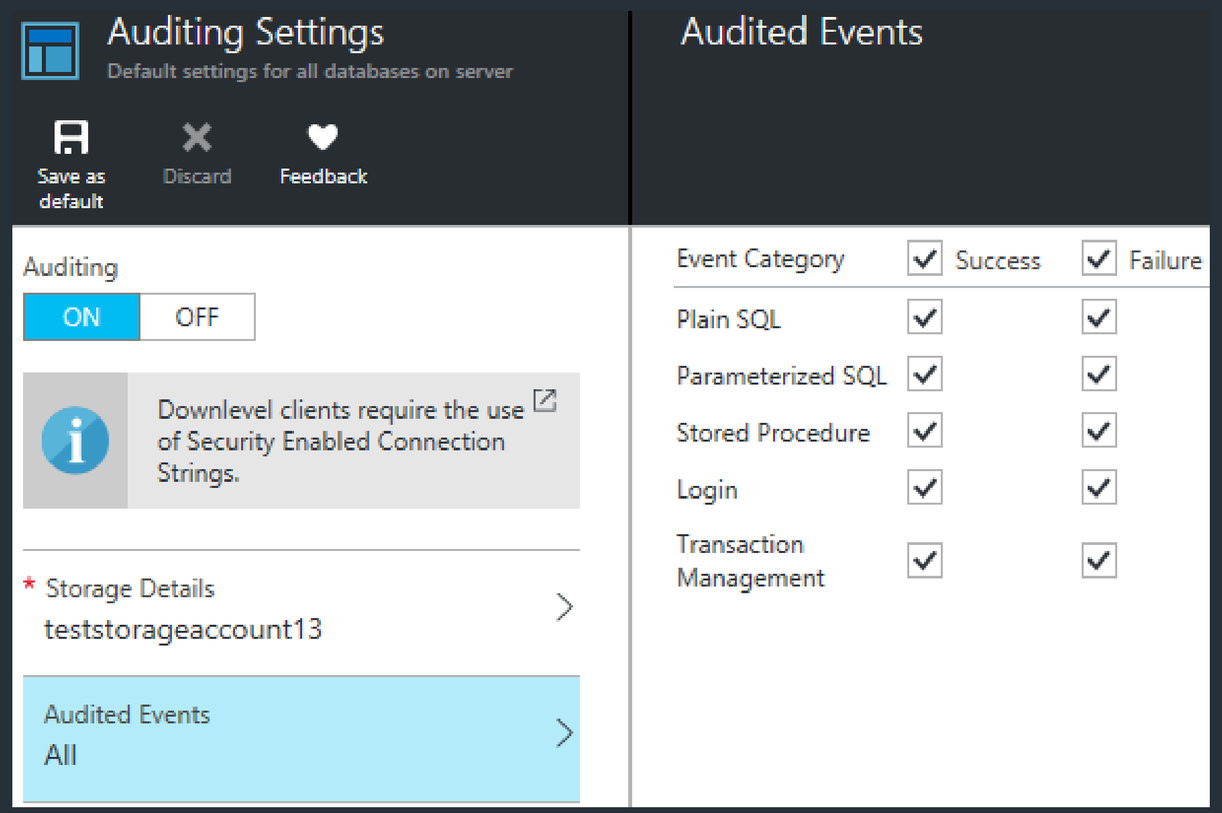
MWR LABS

++

Auditing - Azure SQL Server

+ Auditing configuration





PUBLIC

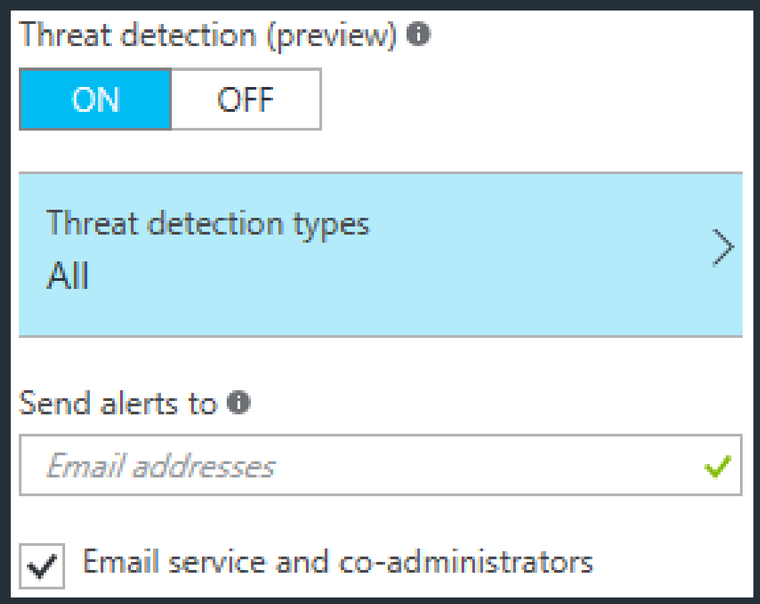
Azure Security Controls & Pentesting – Auditing & Monitoring

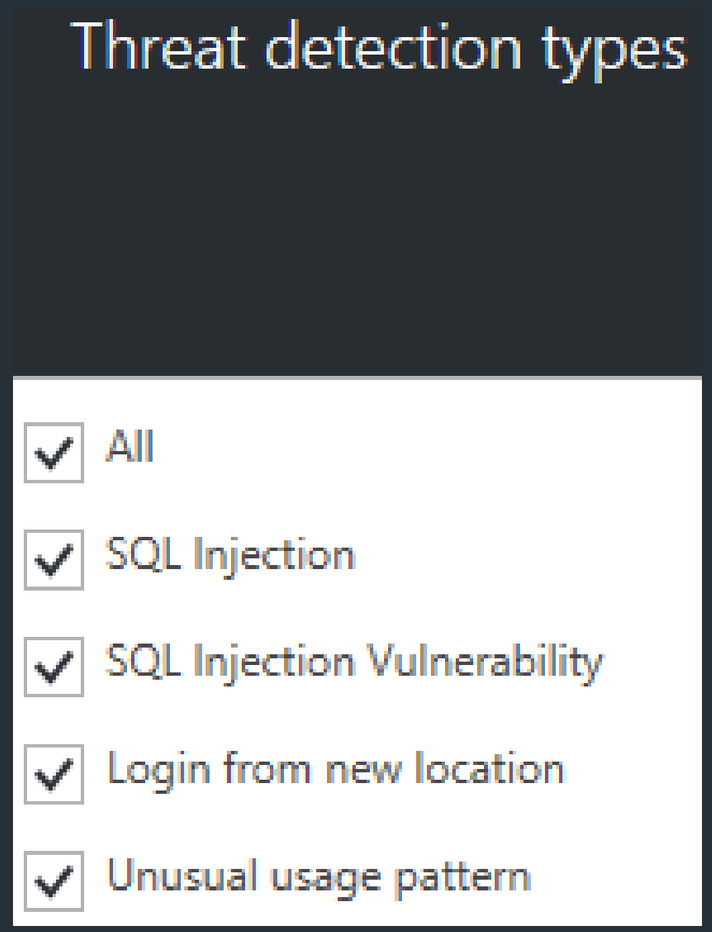
MWR LABS

++

Threat Detection - Azure SQL Server

\+ Threat detection





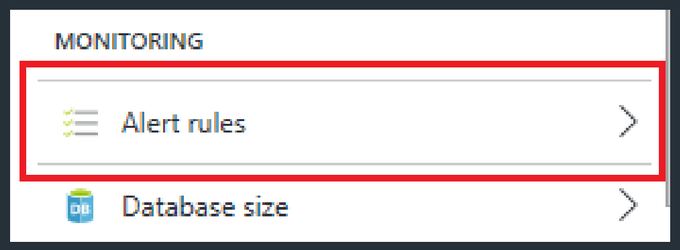
Azure Security Controls & Pentesting – Auditing & Monitoring

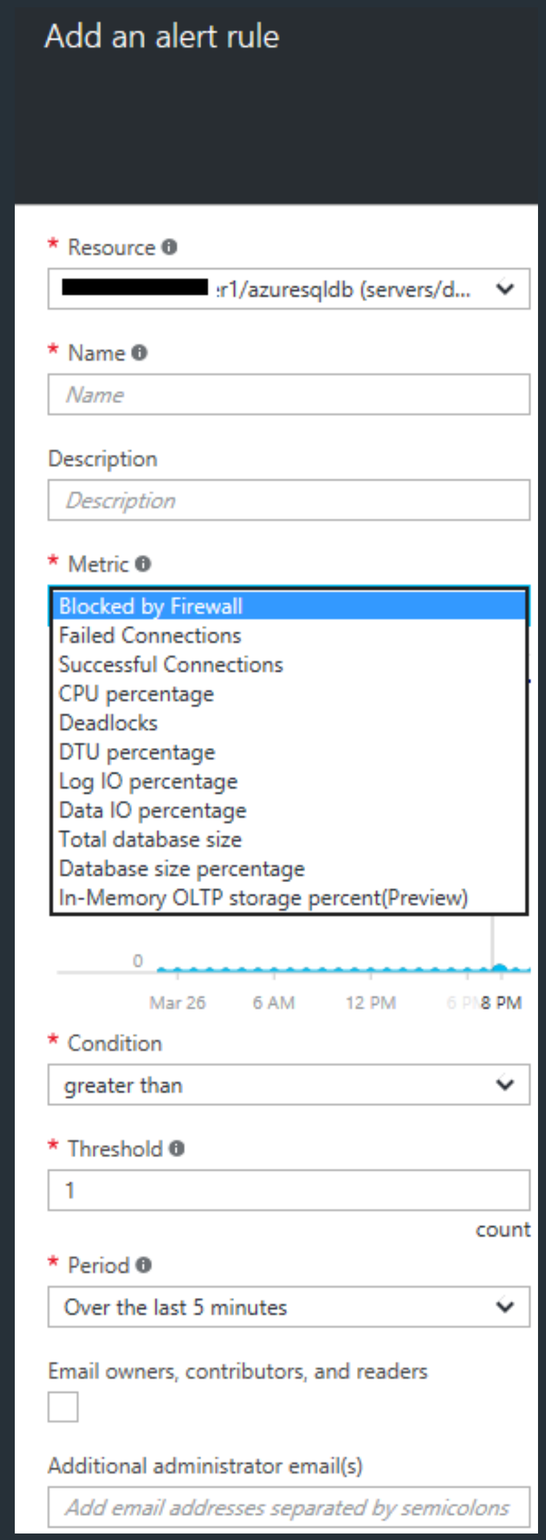
MWR LABS

++

Monitoring - Azure SQL Server

+ Monitoring of various events based on configured rules.





PUBLIC

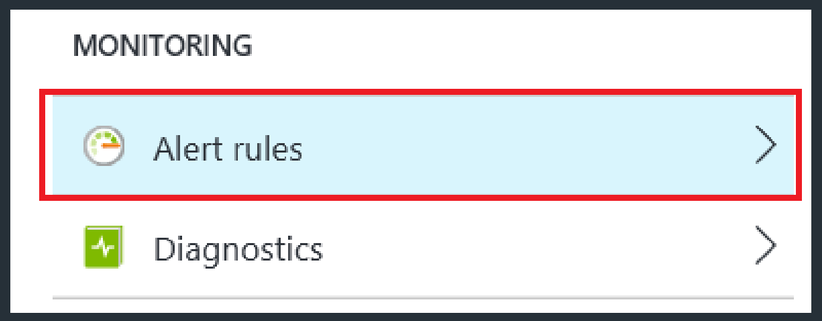
Azure Security Controls & Pentesting – Auditing & Monitoring

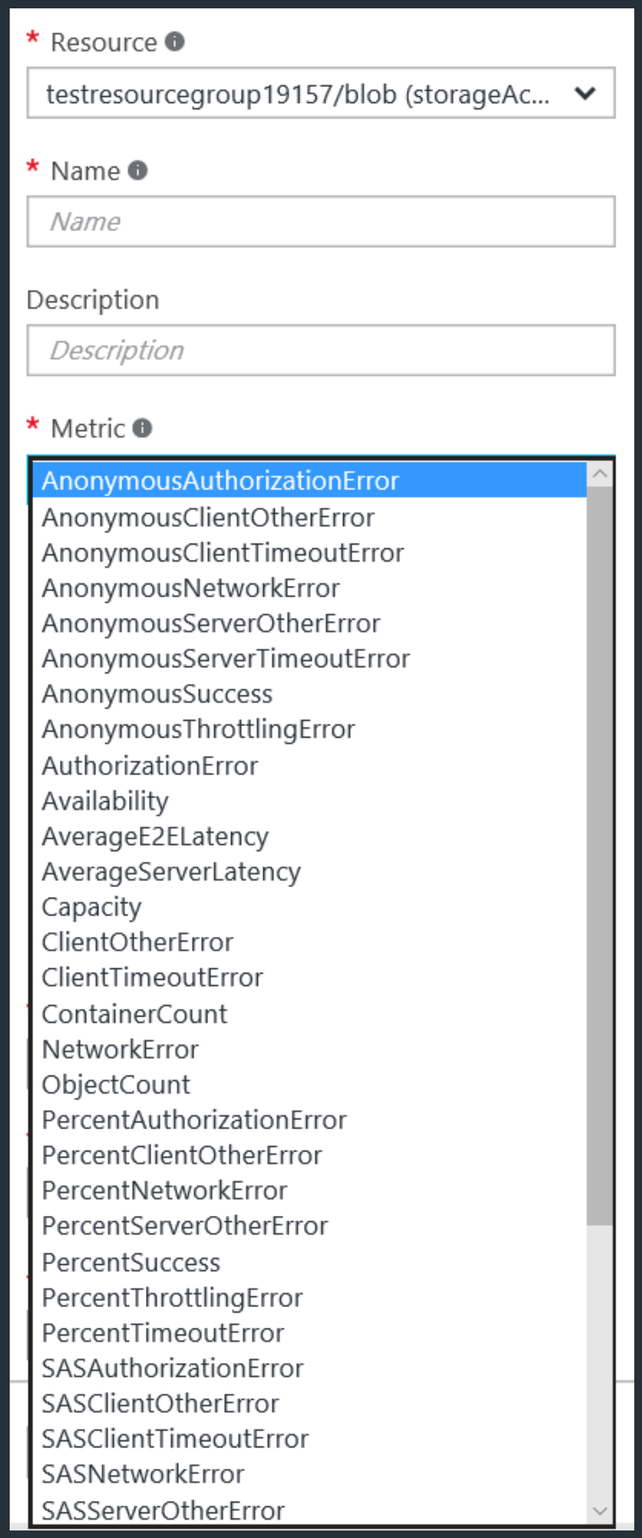
MWR LABS

++

Monitoring - Azure Storage

+ Monitoring of various events based on configured rules.





++ 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

MWR LABS

++

Azure Security Centre - Prevention

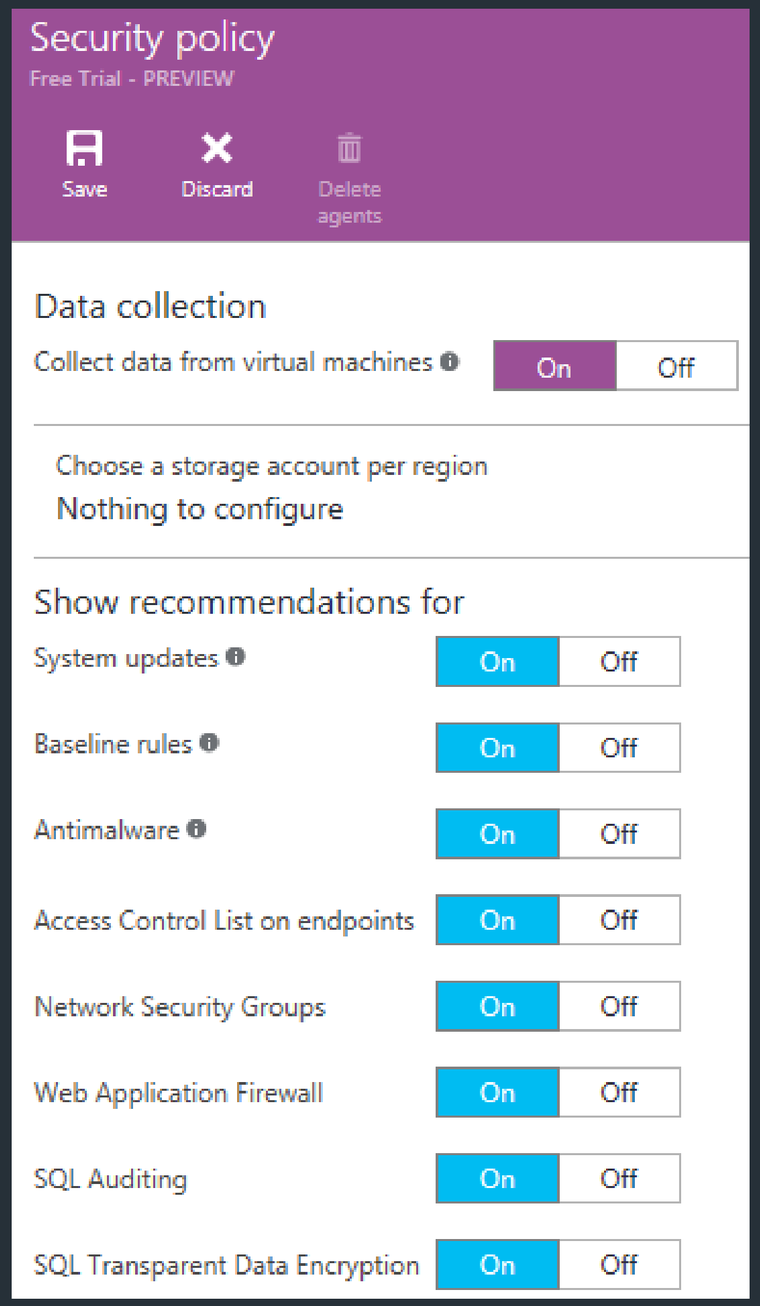
Azure Security Controls & Pentesting – Azure Security Centre

MWR LABS

++ 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.



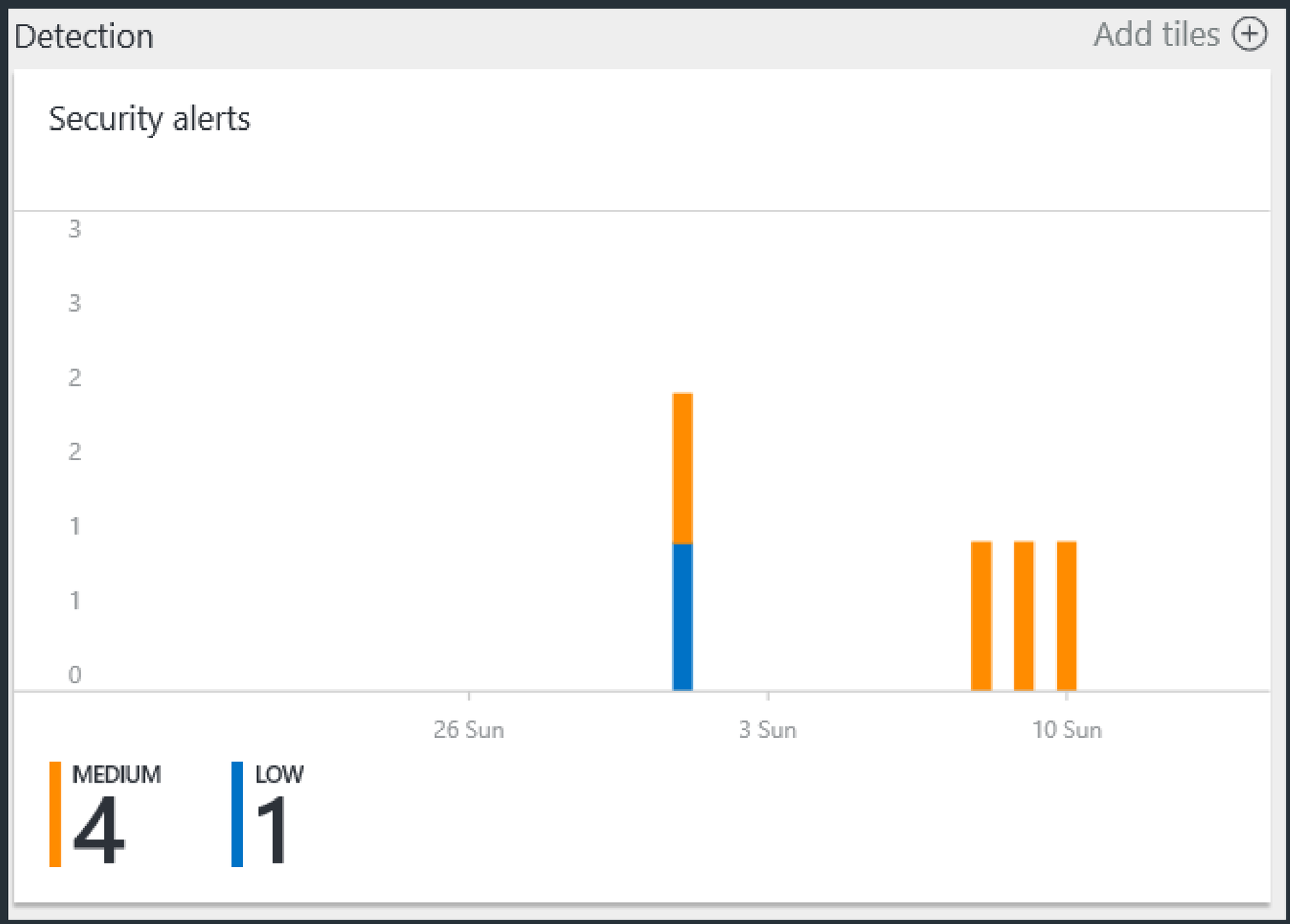
PUBLIC

Azure Security Controls & Pentesting – Azure Security Centre

MWR LABS

++

Azure Security Centre - Detection



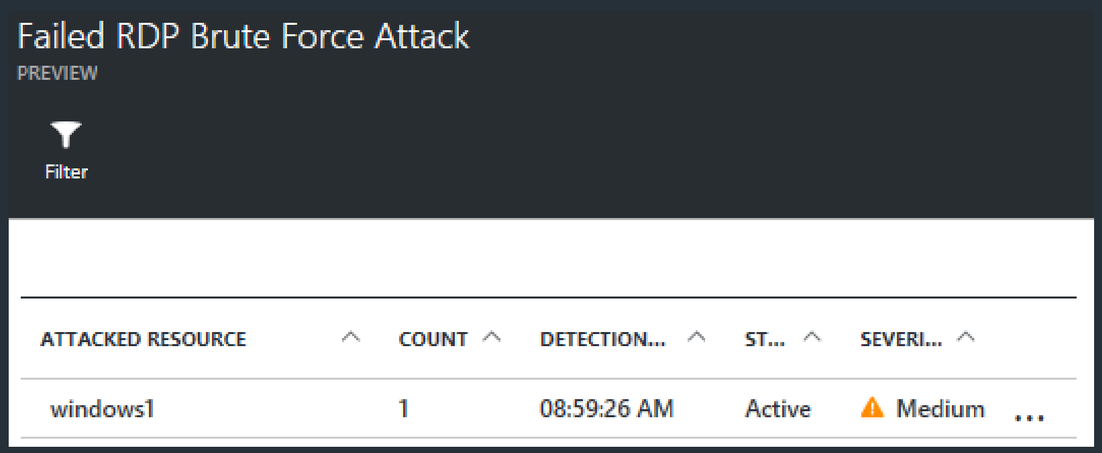
Azure Security Controls & Pentesting – Azure Security Centre

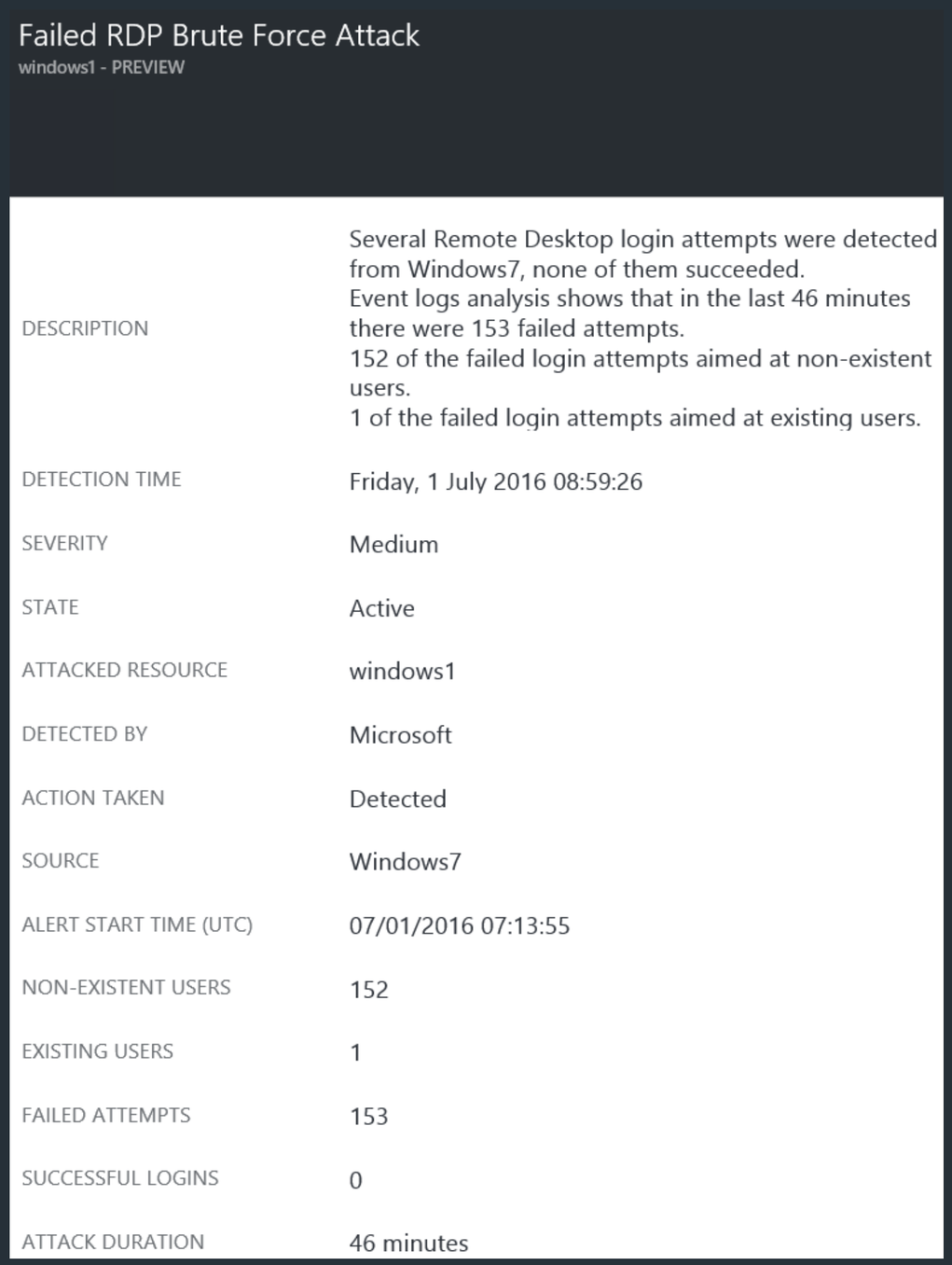
MWR LABS

++

Azure Security Centre - Detection

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



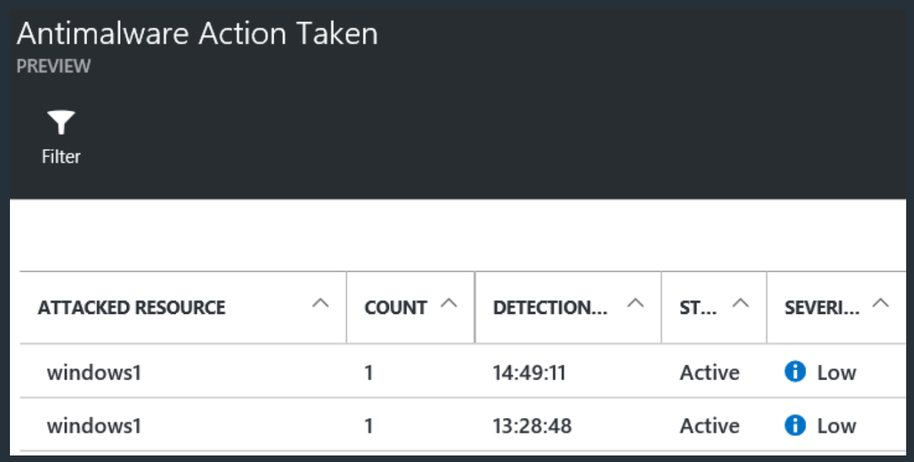


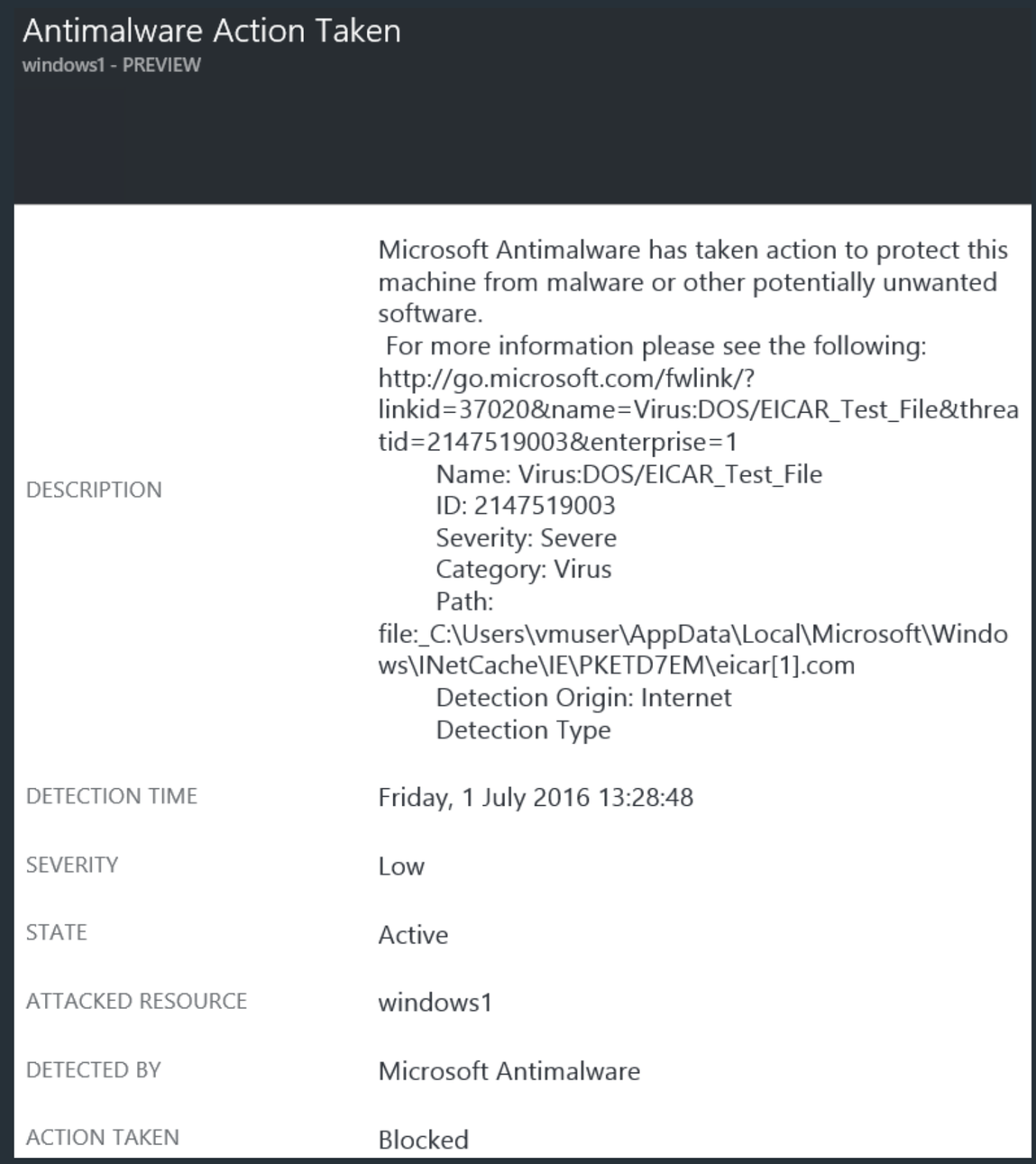
MWR LABS

++

Azure Security Centre - Detection

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





MWR LABS

Contents

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

MWR LABS

Azurite Explorer & Azurite Visualizer

++

Azurite Explorer

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

++

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.

MWR LABS

PS> Listen-ToTheAudience

+ @mwrlabs

  https://labs.mwrinfosecurity.com

+ Azurite Explorer and Azurite Visualizer code on Github

  https://github.com/mwrlabs/Azurite