APPENDIX

January 2021 Exam Update

On January 27, 2021, Microsoft updated the AZ-500 Exam objectives to add new topics to the existing areas of the exam. This appendix covers the new additions per skill measure section.

Skill: Implement advance network security

In this section of the exam, Azure Firewall Manager was the only addition for this exam's update.

Implement Azure Firewall Manager

Azure Firewall Manager provides security management for two types of Azure network architectures: secured virtual hub and hub virtual network. The diagram shown in Figure A-1 has a representation of these options.

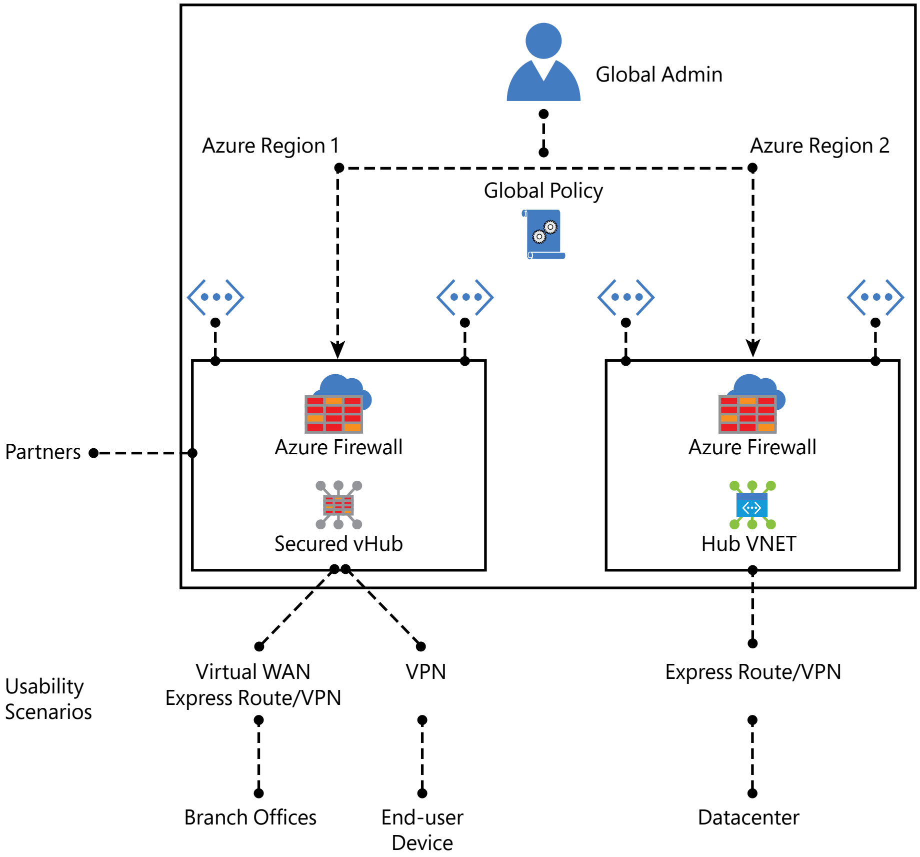


FIGURE A-1 Azure Firewall Manager deployment options

When you need to create a hub-and-spoke architecture, you use an Azure Virtual WAN Hub. When you apply security and routing policies (that are managed by Azure Firewall Manager) to this hub, you call it a secured virtual hub. A secured virtual hub is recommended in scenarios where you need to filter traffic between virtual networks, virtual networks and branch offices, and traffic to the internet. When security policies created by Azure Firewall Manager are associated with an Azure virtual network, you use a hub virtual network. You can't have more than one hub per virtual WAN per region, but you can add multiple virtual WANs in the region to accomplish this.

One of the advantages of using Azure Firewall Manager is the capability for central deployment and configuration of multiple Azure Firewall instances, and these instances can span across different Azure regions and subscriptions. When implementing secured virtual hub deployments, you can choose to route the traffic to your secured hub to filter and for logging without manually configuring User Defined Routes (UDR) on spoke virtual networks.

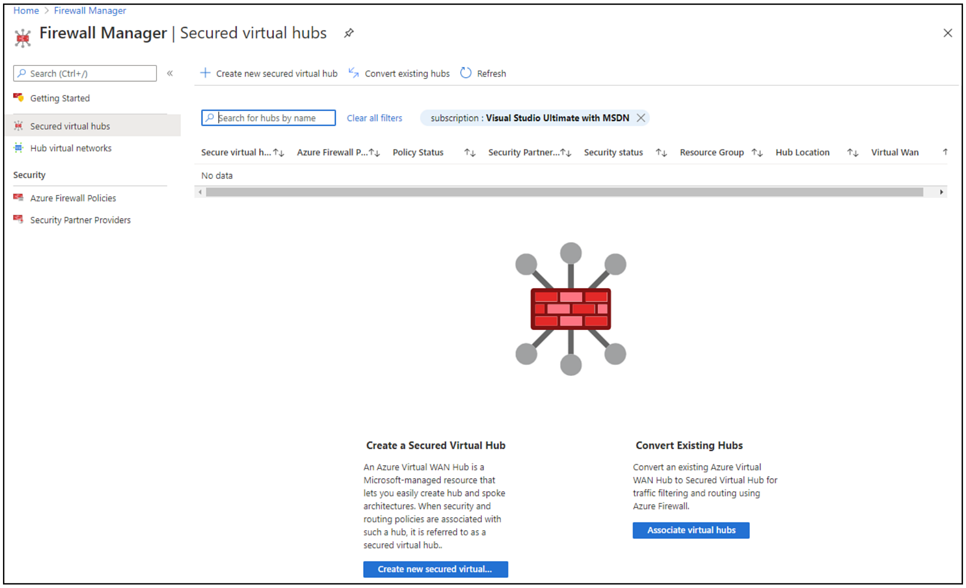
Azure Firewall Manager supports integration with security partner providers (SECaaS), including Zscaler, Check Point, and iboss. With this integration, you can secure a hub with a security partner and perform routing and filtering of internet traffic from your virtual networks (VNets) or branch locations within a region. Again, there is no need to configure UDRs because the route management process is automated.

> ***TIP*** **ARCHITECTURE OPTIONS**
>
> **For more details about the architecture options to implement Azure Firewall Manager, visit *http://aka.ms/az500fwmanager*.**

Deployment

After choosing the deployment option, you can start configuring your Azure Firewall Manager. First, ensure that you already have your virtual networks created and configured. In the following example, you create a secured virtual hub using Azure portal:

1. Navigate to the Azure portal at *https://portal.azure.com*.
2. In the search bar, type *firewall* and under **Services**, click **Firewall Manager**.
3. On the left navigation pane, click **Secured Virtual Hubs** and the **Firewall Manager | Secured Virtual Hubs** page displays as shown in Figure A-2.



Create a Secured Virtual Hub

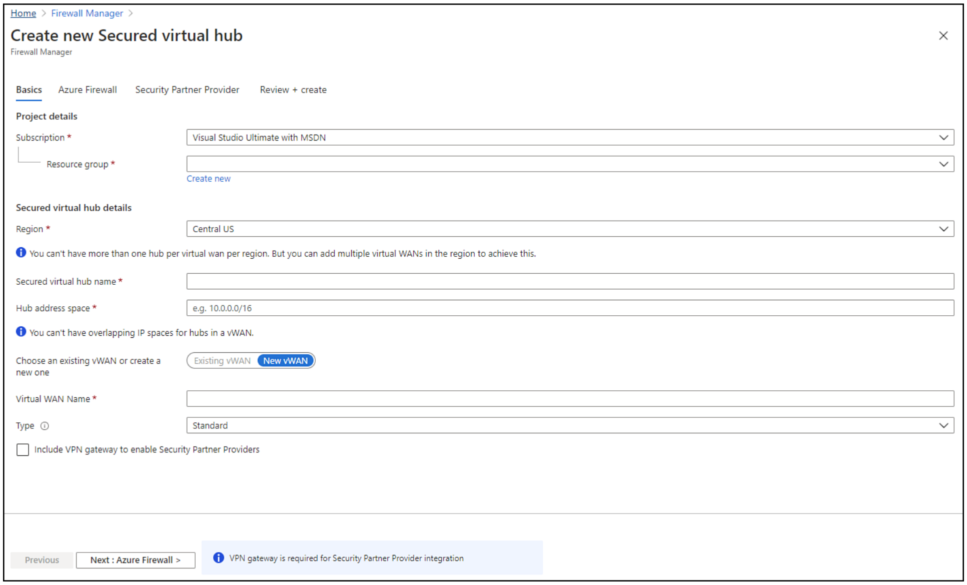
An Azure Virtual WAN Hub is a Microsoft-managed resource that lets you easily create hub and spoke architectures. When security and routing policies are associated with such a hub, it is referred to as a secured virtual hub..

Convert Existing Hubs

Convert an existing Azure Virtual WAN Hub to Secured Virtual Hub for traffic filtering and routing using Azure Firewall.

FIGURE A-2 Configuring secured virtual hubs

4. Click the **Create New Secured Virtual Hub** button and the **Create New Secured Virtual Hub** page appears as shown in Figure A-3.



Home > Firewall Manager >

Create new Secured virtual hub

Firewall Manager

Basics | Azure Firewall | Security Partner Provider | Review + create

Project details

Subscription * : Visual Studio Ultimate with MSDN

Resource group * :

Create new

Secured virtual hub details

Region * : Central US

You can't have more than one hub per virtual wan per region. But you can add multiple virtual WANs in the region to achieve this.

Secured virtual hub name * :

Hub address space * : e.g. 10.0.0.0/16

You can't have overlapping IP spaces for hubs in a vWAN.

Choose an existing vWAN or create a new one: Existing vWAN [✓ New vWAN]

Virtual WAN Name * :

Type : Standard

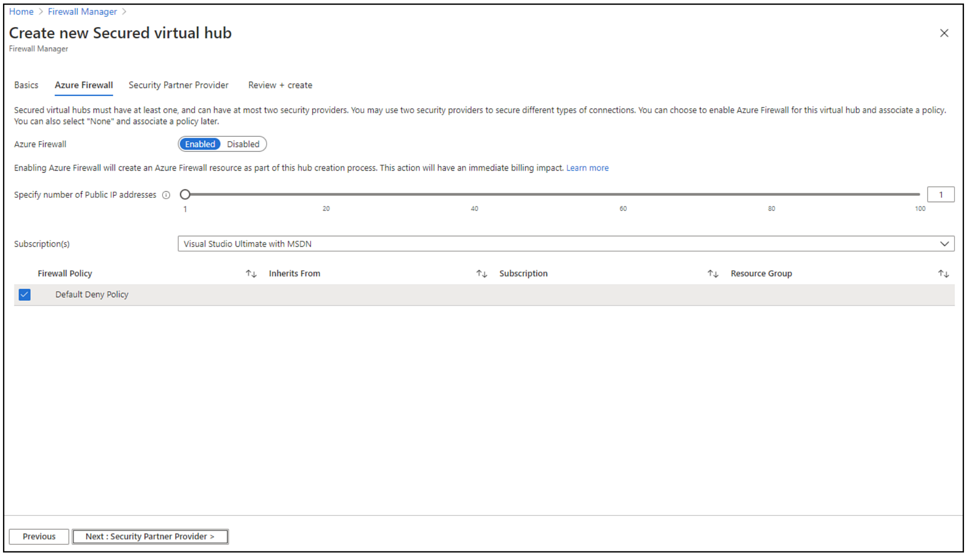
□ Include VPN gateway to enable Security Partner Providers

Previous | Next : Azure Firewall >

VPN gateway is required for Security Partner Provider integration

FIGURE A-3 Configuring the parameters for the new secured virtual hub

5. On the Create New Secured Virtual Hub page, make the appropriate selections from the **Resource Group** and **Region** drop-down menus, give a name to this secured virtual hub, and type an IP address space that doesn't overlap with the IP space used by hubs in a vWAN. You also have the option to use an existing vWAN or create a new one. Once you finish filling all the options, click **Next: Azure Firewall** and the **Azure Firewall** tab appears as shown in Figure A-4.



Home > Firewall Manager >

Create new Secured virtual hub

Firewall Manager

Basics | Azure Firewall | Security Partner Provider | Review + create

Secured virtual hubs must have at least one, and can have at most two security providers. You may use two security providers to secure different types of connections. You can choose to enable Azure Firewall for this virtual hub and associate a policy. You can also select "None" and associate a policy later.

Azure Firewall: [✓ Enabled] Disabled

Enabling Azure Firewall will create an Azure Firewall resource as part of this hub creation process. This action will have an immediate billing impact. Learn more

Specify number of Public IP addresses: 1

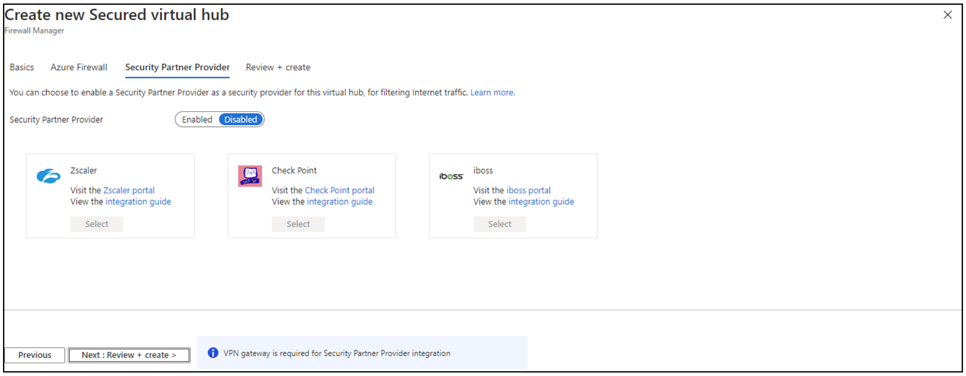
Subscription(s): Visual Studio Ultimate with MSDN

	Firewall Policy	Inherits From	Subscription	Resource Group
☑	Default Deny Policy			

Previous | Next : Security Partner Provider >

FIGURE A-4 Configuring Azure Firewall parameters

6. On this page, you either enable the Azure Firewall or disable it in case you want to use another security provider. You can also select the number of public IP addresses that can be used. For this demonstration, leave the default selection and click **Next: Security Partner Provider**. The **Security Partner Provider** tab appears as shown in Figure A-5.



Create new Secured virtual hub

Firewall Manager

You can choose to enable a Security Partner Provider as a security provider for this virtual hub, for filtering Internet traffic. Learn more.

Security Partner Provider: Enabled [✓ Disabled]

Zscaler
Visit the Zscaler portal
View the integration guide

Check Point
Visit the Check Point portal
View the integration guide

iboss
Visit the iboss portal
View the integration guide

VPN gateway is required for Security Partner Provider integration

FIGURE A-5 Selecting the security partner provider

7. You can optionally select a security partner provider to integrate with. In this case there is no integration, therefore leave the default selection and click **Next: Review + Create** and then click **Create**.

It can take up to 30 minutes for this new secured virtual hub to be deployed. Once it is finished, you can get the firewall public IP address. After that, the next steps are

1. Connect the hub and spoke virtual networks.
2. Deploy the resources (VMs, for example).
3. Create a firewall policy according to your organization's needs.
4. Change the route to ensure that network traffic gets routed through your firewall.

> ***TIP*** **SECURITY PARTNER PROVIDERS**
>
> **For more information about security partner providers, visit *http://aka.ms/az500secpartners*.**

Skill: Secure data and applications

In this section of the exam, Azure Defender for Storage, Azure Defender for SQL, and Azure Defender for Key Vault were added for this exam's update.

Although these were the only additions, is important to emphasize that at Ignite 2020, Microsoft announced the change in the Azure Security Center Standard brand. What used to be called Azure Security Center Standard tier is now called Azure Defender. The Azure Security Center Free tier is still functional, and all capabilities are still the same.

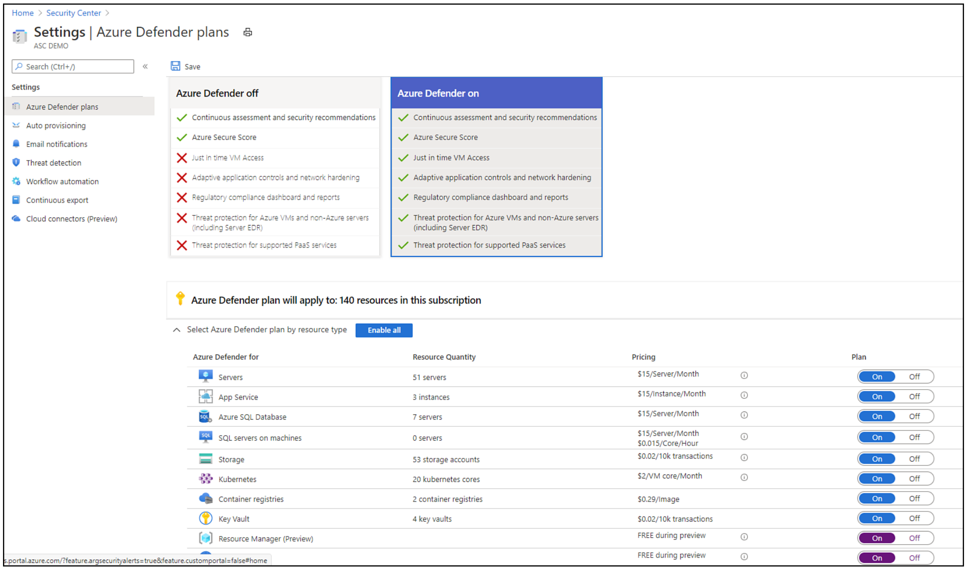
With this new brand, the features that were part of Azure Security Center Standard tier are now part of Azure Defender for Servers, which includes the following:

- Vulnerability Assessment (powered by Qualys)
- File Integrity Monitoring
- Just in time VM access
- Adaptive Application Control
- Adaptive Network Hardening

In addition, all plans that were called *Advanced Threat Protection* are now under the Azure Defender brand, which includes the following:

- Azure Defender for Kubernetes
- Azure Defender for Container registries
- Azure Defender for SQL (this used to be called Advanced Data Security for SQL)
- Azure Defender for App Service
- Azure Defender for Storage

These options are available to be enabled under the pricing and settings page in Azure Security Center, as shown in Figure A-6.



Azure Defender off	Azure Defender on
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Azure Secure Score	✓ Azure Secure Score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

Azure Defender plan will apply to: 140 resources in this subscription

Select Azure Defender plan by resource type

Azure Defender for	Resource Quantity	Pricing	Plan
Servers	51 servers	$15/Server/Month	On Off
App Service	3 instances	$15/Instance/Month	On Off
Azure SQL Database	7 servers	$15/Server/Month	On Off
SQL servers on machines	0 servers	$15/Server/Month $0.015/Core/Hour	On Off
Storage	53 storage accounts	$0.02/10k transactions	On Off
Kubernetes	20 kubernetes cores	$2/VM core/Month	On Off
Container registries	2 container registries	$0.29/Image	On Off
Key Vault	4 key vaults	$0.02/10k transactions	On Off
Resource Manager (Preview)		FREE during preview	On Off
		FREE during preview	On Off

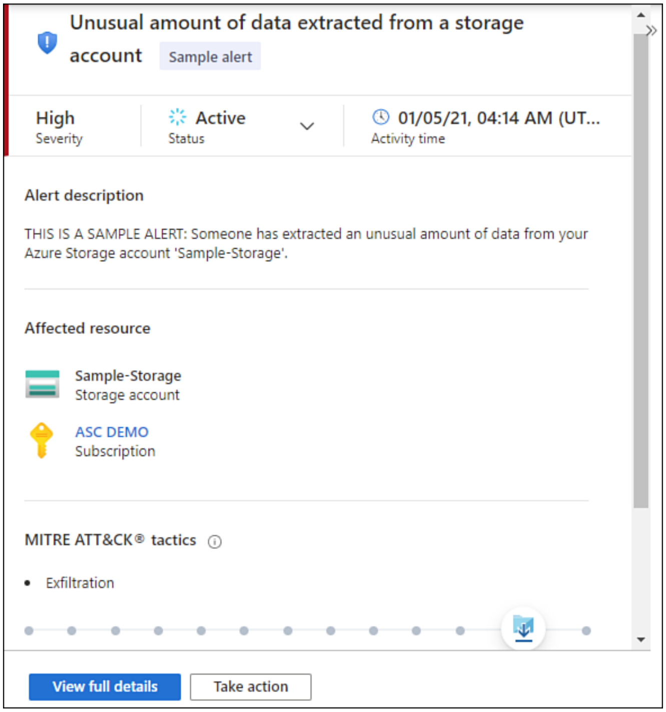
FIGURE A-6 Azure Defender plans

The sections that follow cover the details of the three Azure Defender additions for the January 2021 update of the AZ-500 Exam.

Azure Defender for Storage

Azure Defender for Storage can be enabled for data stored in Azure Blob, Azure Files, and Azure Data Lakes Storage (ADLS) Gen2. You can enable Azure Defender for Storage on the subscription level, just like any other plan, or you can enable it only on the storage accounts that you want to protect.

Alerts generated by Azure Defender for Storage can occur when there are suspicious access patterns—for example, an access from a Tor exit node. Another scenario that can trigger an alert is when there are suspicious activities in the storage account—for example, an unusual change of access permission. Figure A-7 has a sample alert for Azure Defender for Storage.



Unusual amount of data extracted from a storage account Sample alert

High Severity | Active Status | 01/05/21, 04:14 AM (UT... Activity time

Alert description

THIS IS A SAMPLE ALERT: Someone has extracted an unusual amount of data from your Azure Storage account 'Sample-Storage'.

Affected resource

Sample-Storage
Storage account

ASC DEMO
Subscription

MITRE ATT&CK® tactics

- Exfiltration

FIGURE A-7 Sample alert for Azure Defender for Storage

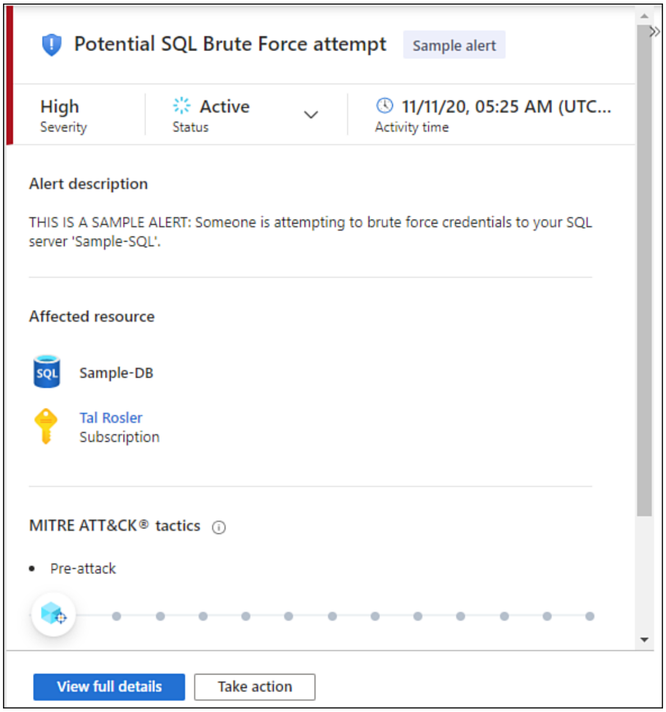
In 2020, a major addition to Azure Defender for Storage was announced: the hash reputation analysis for malware. To add an extra layer of security, Azure Defender for Storage analyzes files that are uploaded using hash reputation, which leverages Microsoft Threat Intelligence. Is very important to emphasize that this is not an anti-malware scan for storage. This feature inspects the storage logs and compares the hashes of newly uploaded files with information about known viruses, trojans, spyware, and ransomware.

Azure Defender for SQL

Azure Defender for SQL is a protection plan that helps you mitigate potential database vulnerabilities and detect anomalous activities that may indicate threats against your databases. Azure Defender for SQL has evolved over the years and currently has two major plans:

- Azure Defender for Azure SQL database servers, which includes Azure SQL Database, Azure SQL Managed Instance, and Dedicated SQL pool in Azure Synapse
- Azure Defender for SQL servers on machines, which includes SQL Server running on VMs in Azure, on-premises, or in another cloud provider

Azure Defender for SQL provides threat detects for anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. Figure A-8 has an example of an alert triggered by this plan.



Potential SQL Brute Force attempt Sample alert

High
Severity

Active
Status

11/11/20, 05:25 AM (UTC...
Activity time

Alert description

THIS IS A SAMPLE ALERT: Someone is attempting to brute force credentials to your SQL server 'Sample-SQL'.

Affected resource

Sample-DB

Tal Rosler
Subscription

MITRE ATT&CK® tactics

- Pre-attack

FIGURE A-8 Sample alert for Azure Defender for SQL

The Azure Defender for Azure SQL database servers can be easily enabled on the subscription level on the Azure SQL database that you want to be protected; no agent is required. However, to use the Azure Defender for SQL servers on machines, you need to enable the plan on the subscription level, and you must onboard the server, which means provision the Log Analytics agent on SQL Server. If your VMs are in Azure, you just need to use the auto-provisioning option in Azure Security Center to onboard the Log Analytics Agent automatically to your Azure VMs.

Another recently announced scenario is the integration with Azure Arc, which allows a deeper integration across different scenarios. It is recommended that you use Azure Arc for your SQL Servers on-premises or in different cloud providers (AWS and GCP). Once they are fully onboard, you can deploy the Log Analytics Agent. In summary, follow the sequence below to fully onboard:

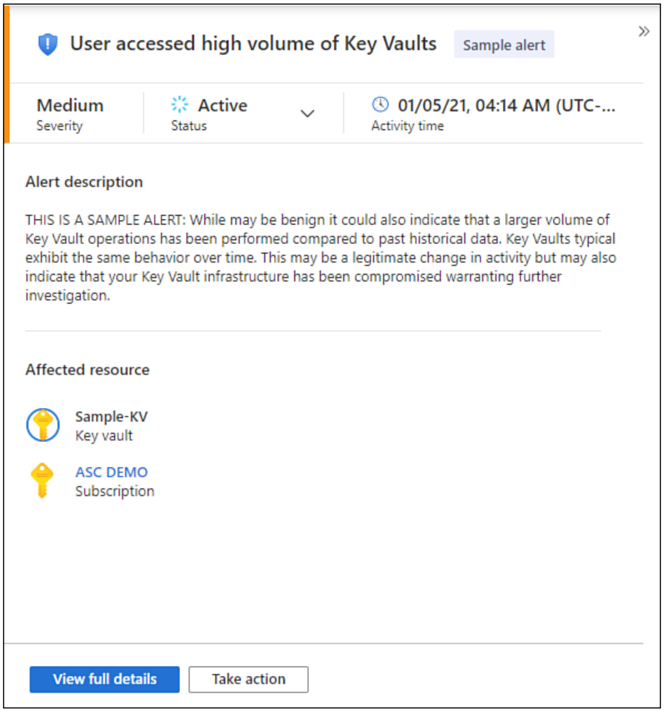
1. Enable Azure Arc on your machines (follow the steps at *http://aka.ms/az500enablearc*).
2. Install the Log Analytics agent to this machine. You can easily identify which machines are missing the agent by reviewing the recommendation **Log Analytics Agent Should Be Installed On Your Windows-Based Azure Arc Machines**.
3. Enable the **SQL Servers On Machines** pricing plan in the pricing and settings page of Azure Security Center. The plan will be enabled on all SQL servers and will be fully active after the first restart of the SQL Server instance.

TIP **IDENTIFYING AZURE ARC–ENABLED MACHINES**

You can quickly identify which machines are Azure Arc enabled by using the Inventory dashboard. Create a filter based on Resource Type and change the criteria to Servers – Azure Arc.

Azure Defender for Key Vault

Azure Defender for Key Vault uses machine learning to detect unusual and potentially harmful attempts to access or exploit Key Vault accounts. By the time this appendix was written, the only option to enable Azure Defender for Key Vault was to enable it on the entire subscription. Figure A-9 has an Azure Defender for Key Vault sample alert.


User accessed high volume of Key Vaults

Medium
Severity

Active
Status

01/05/21, 04:14 AM (UTC-...
Activity time

Alert description

THIS IS A SAMPLE ALERT: While may be benign it could also indicate that a larger volume of Key Vault operations has been performed compared to past historical data. Key Vaults typical exhibit the same behavior over time. This may be a legitimate change in activity but may also indicate that your Key Vault infrastructure has been compromised warranting further investigation.

Affected resource

Sample-KV
Key vault

ASC DEMO
Subscription

FIGURE A-9 Azure Defender for Key Vault sample alert

TIP **LIST OF ALERTS**

You can see the list of all alerts that can be generated by Azure Defender for Key Vault at *http://aka.ms/AzDefKeyVaultAlerts*.