LABOR DAY SALE IS ON 🔥 | FEW HOURS LEFT | BUY 2 & GET ADDITIONAL 25% OFF | Use Coupon - LABORDAY

SKILLCERTPRO

IT CERTIFICATION TRAININGS

0

Microsoft Azure / By SkillCertPro

Practice Set 14

Your results are here!! for" Microsoft Azure AZ-305 Practice Test 14 "

45 of 65 questions answered correctly

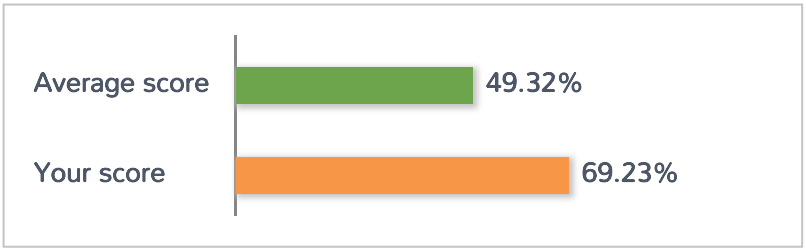
Your time: 01:52:55

Your Final Score is : 45

You have attempted : 65

Number of Correct Questions : 45 and scored 45

Number of Incorrect Questions : 20 and Negative marks 0

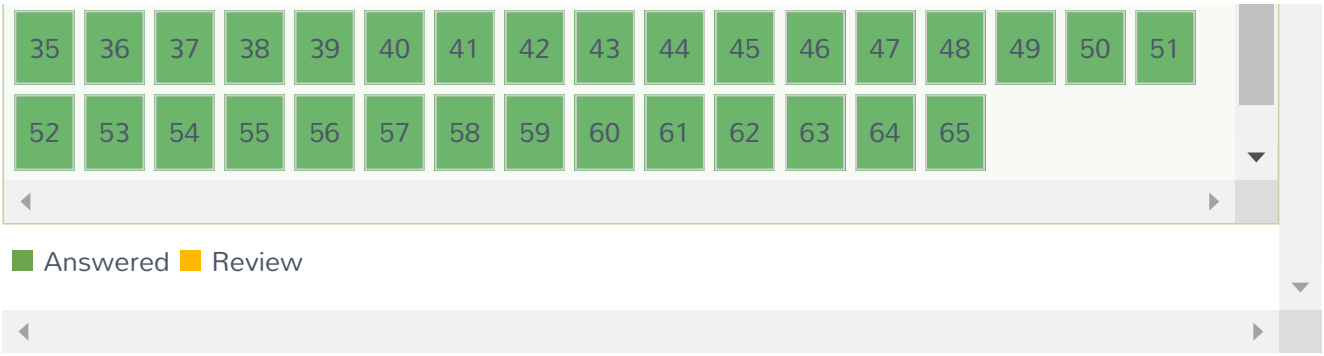


You can review your answers by clicking on “View Answers” option.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

Restart Test View Answers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34



1. Question

You are designing an Azure solution.

The network traffic for the solution must be securely distributed by providing the following features:

? HTTPS protocol

? Round robin routing

? SSL offloading

You need to recommend a load balancing option.

What should you recommend?

- A. Azure Load Balancer
- B. Azure Internal Load Balancer (ILB)
- C. Azure Traffic Manager
- **D. Azure Application Gateway**

Correct

Application Gateway supports autoscaling, TLS offloading, and end-to-end TLS, a web application firewall (WAF), cookie-based session affinity, URL path-based routing, multisite hosting, and other features.

Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS, WebSocket, and HTTP/2). It supports capabilities such as TLS termination, cookie-based session affinity, and round robin for load-balancing traffic. Load Balancer load-balances traffic at layer 4 (TCP or UDP).

Application Gateway provides Transport Layer Security (TLS) protocol termination ("SSL offload") or per-HTTP/HTTPS request.

Incorrect Answers:

A. Azure Load Balancer

Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. It does not provide SSL offloading capabilities.

B. Azure Internal Load Balancer (ILB)

Internal load balancing (ILB) enables you to run highly available services behind a private IP address which is accessible only within a cloud service or Virtual Network (VNet), giving additional security on that endpoint.

C. Azure Traffic Manager

Azure Traffic Manager is a DNS-based traffic load balancer. It allows you to distribute traffic to your public facing applications across the global Azure regions. It does not provide SSL offloading capabilities.

Reference:

https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq

https://docs.microsoft.com/en-us/azure/application-gateway/overview

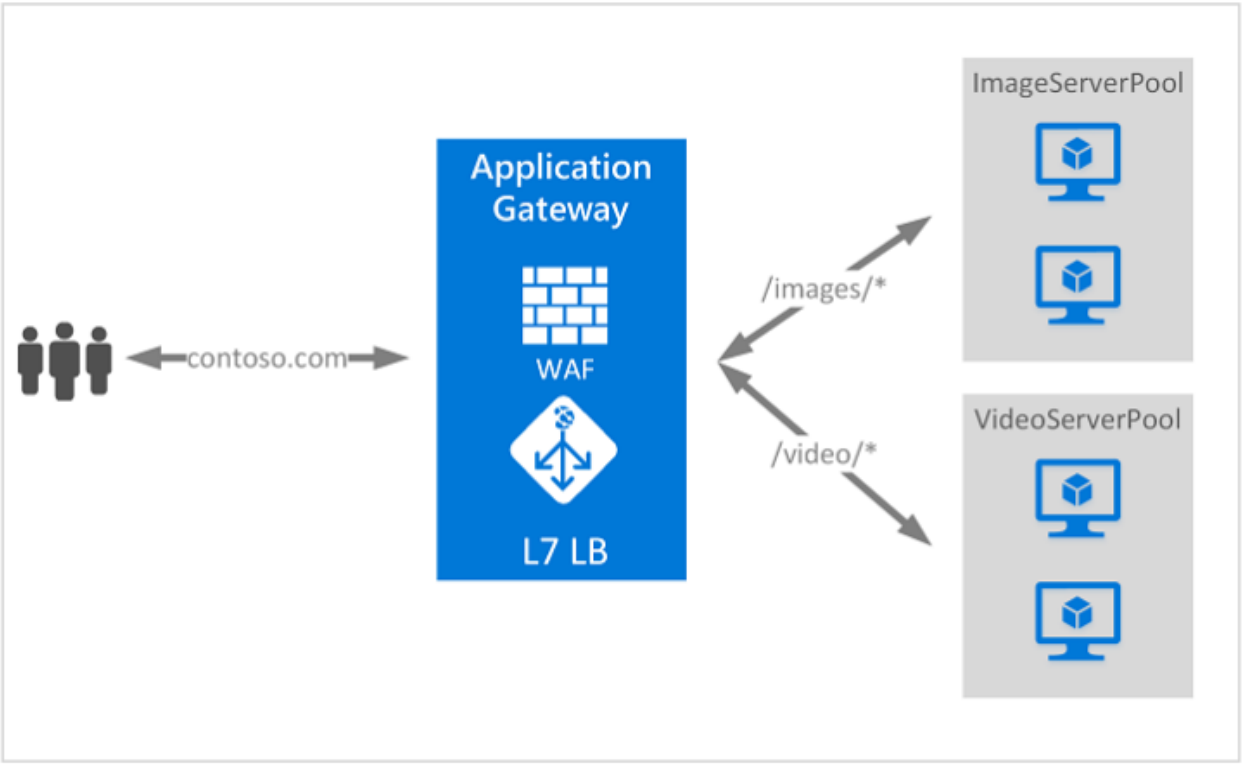
https://docs.microsoft.com/en-us/azure/application-gateway/features

What is Azure Application Gateway?

08/26/2020 • 2 minutes to read • +5

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So if `/images` is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If `/video` is in the URL, that traffic is routed to another pool that's optimized for videos.



This type of routing is known as application layer (OSI layer 7) load balancing. Azure Application Gateway can do URL-based routing and more.

Note

Azure provides a suite of fully managed load-balancing solutions for your scenarios.

- If you are looking to do DNS based global routing and do **not** have requirements for

Transport Layer Security (TLS) protocol termination ("SSL offload"), per-HTTP/HTTPS request or application-layer processing, review **Traffic Manager**.

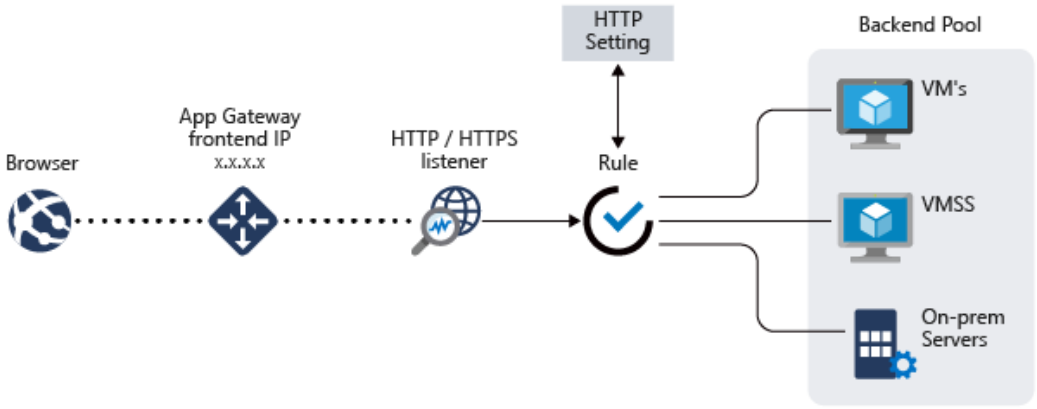
- If you need to optimize global routing of your web traffic and optimize top-tier end-user performance and reliability through quick global failover, see **Front Door**.
- To do network layer load balancing, review **Load Balancer**.

Your end-to-end scenarios may benefit from combining these solutions as needed. For an Azure load-balancing options comparison, see **Overview of load-balancing options in Azure**.

Azure Application Gateway features

09/25/2020 • 8 minutes to read •

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.



Application Gateway includes the following features:

- Secure Sockets Layer (SSL/TLS) termination
- Autoscaling
- Zone redundancy
- Static VIP
- Web Application Firewall
- Ingress Controller for AKS
- URL-based routing
- Multiple-site hosting
- Redirection
- Session affinity
- Websocket and HTTP/2 traffic
- Connection draining
- Custom error pages
- Rewrite HTTP headers and URL
- Sizing

2. Question

You have an on-premises network that uses an IP address space of 172.16.0.0/16.

You plan to deploy 25 virtual machines to a new Azure subscription.

You identify the following technical requirements:

? All Azure virtual machines must be placed on the same subnet named Subnet1.

? All the Azure virtual machines must be able to communicate with all on-premises servers.

? The servers must be able to communicate between the on-premises network and Azure by using a site-to-site VPN.

You need to recommend a subnet design that meets the technical requirements.

Which of the following would go into Slot1?

- A. 172.16.0.0/16
- B. 172.16.1.0/28
- C. 192.168.0.0/24
- D. 192.168.1.0/28

Correct

The range 192.168.1.0/28 is from 192.168.1.1 to 192.168.1.15, only 16 ips and we need 25 IPs, so the only valid answer for subnet1 is 192.168.0.0/24

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We recommend that you create a gateway subnet that uses a /27 or /28.

Incorrect Answers:

The range for the new subnet can't overlap the on-premise subnet range. The on-premise network is 172.16.0.0/16, that is from 172.16.0.1 to 172.16.255.255, so the answers 172.16.0.0/16 and 172.16.1.0/28 are not valid (overlap with on-pemise subnet)

Reference:

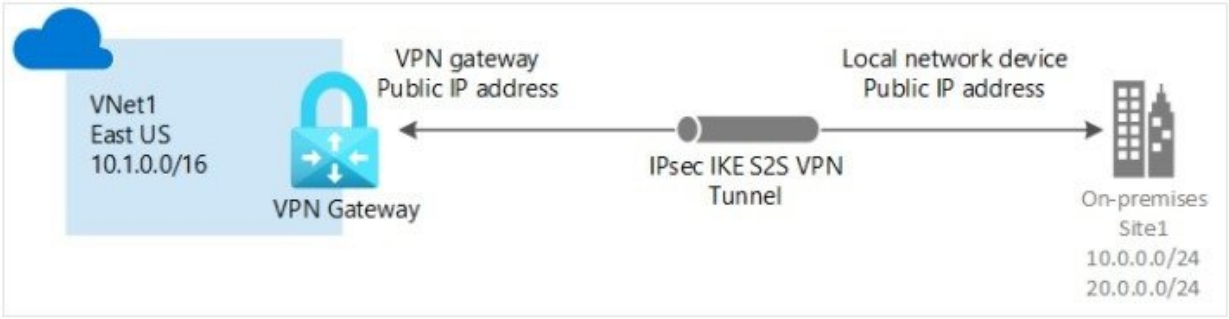
https://docs.microsoft.com/es-es/azure/vpn-gateway/tutorial-site-to-site-portal

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal#VNetGateway

Tutorial: Create a Site-to-Site connection in the Azure portal

07/21/2021 • 19 minutes to read •

Azure VPN gateways provide cross-premises connectivity between customer premises and Azure. This tutorial shows you how to use the Azure portal to create a Site-to-Site VPN gateway connection from your on-premises network to the VNet. You can also create this configuration using Azure PowerShell or Azure CLI.



Create a VPN gateway

In this step, you create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

About the gateway subnet

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We recommend that you create a gateway subnet that uses a /27 or /28.

If you see an error that specifies that the address space overlaps with a subnet, or that the subnet is not contained within the address space for your virtual network, check your VNet address range. You may not have enough IP addresses available in the address range you created for your virtual network. For example, if your default subnet encompasses the entire address range, there are no IP addresses left to create additional subnets. You can either adjust your subnets within the existing address space to free up IP addresses, or specify an additional address range and create the gateway subnet there.

3. Question

You have an on-premises network that uses an IP address space of 172.16.0.0/16.

You plan to deploy 25 virtual machines to a new Azure subscription.

You identify the following technical requirements:

? All Azure virtual machines must be placed on the same subnet named Subnet1.

? All the Azure virtual machines must be able to communicate with all on-premises servers.

? The servers must be able to communicate between the on-premises network and Azure by using a site-to-site VPN.

You need to recommend a subnet design that meets the technical requirements.

Which of the following would go into Slot2?

- A. 172.16.0.0/16
- B. 172.16.1.0/28
- C. 192.168.0.0/24
- D. 192.168.1.0/28

Incorrect

The range for the gateway can‘t ovelap with on-premise, and Microsoft recommend that would be /27 or /28, so the answer valid for gateway is 192.168.1.0/28

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We recommend that you create a gateway subnet that uses a /27 or /28.

Incorrect Answers:

he range for the new subnet can‘t overlap the on-premise subnet range. The on-premise network is 172.16.0.0/16, that is from 172.16.0.1 to 172.16.255.255, so the answers 172.16.0.0/16 and 172.16.1.0/28 are not valid (overlap with on-pemise subnet)

Reference:

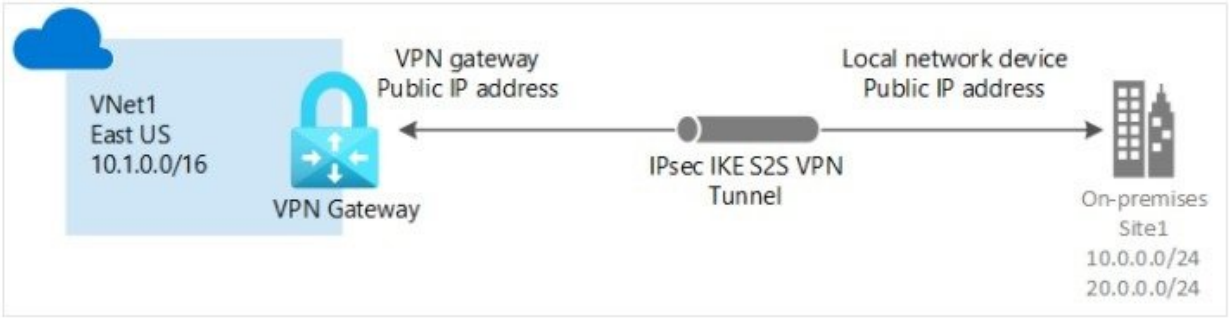
https://docs.microsoft.com/es-es/azure/vpn-gateway/tutorial-site-to-site-portal

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal#VNetGateway

Tutorial: Create a Site-to-Site connection in the Azure portal

07/21/2021 • 19 minutes to read •

Azure VPN gateways provide cross-premises connectivity between customer premises and Azure. This tutorial shows you how to use the Azure portal to create a Site-to-Site VPN gateway connection from your on-premises network to the VNet. You can also create this configuration using Azure PowerShell or Azure CLI.



Create a VPN gateway

In this step, you create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

About the gateway subnet

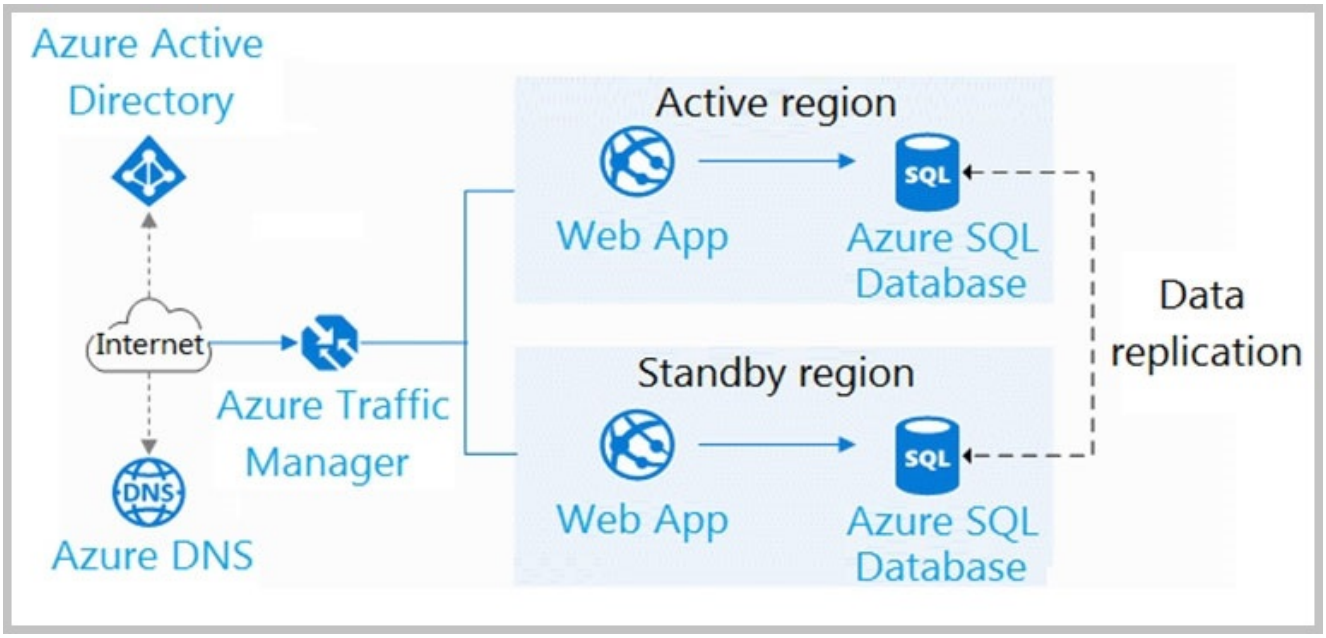
The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We recommend that you create a gateway subnet that uses a /27 or /28.

If you see an error that specifies that the address space overlaps with a subnet, or that the subnet is not contained within the address space for your virtual network, check your VNet address range. You may not have enough IP addresses available in the address range you created for your virtual network. For example, if your default subnet encompasses the entire address range, there are no IP addresses left to create additional subnets. You can either adjust your subnets within the existing address space to free up IP addresses, or specify an additional address range and create the gateway subnet there.

4. Question

You have the application architecture shown in the following exhibit:



Select the answer choice that completes the following statement based on the information presented in the graphic.

To change the front end to an active/active architecture in which both regions process incoming connections, you must .....

- A. add a load balancer to each region
- B. add an Azure Application Gateway to each region
- C. add an Azure content delivery network (CDN)
- **D. modify the Azure Traffic Manager routing method**

Correct

Azure Traffic Manager supports six traffic-routing methods to determine how to route network traffic to the various service endpoints.

Incorrect Answers:

A. add a load balancer to each region

Microsoft Azure Traffic Manager balances the traffic across regions and Azure Web App will have its own load balancer.

B. add an Azure Application Gateway to each region

Microsoft Azure Traffic Manager balances the traffic across regions and Azure Web App will have its own load balancer.

C. add an Azure content delivery network (CDN)

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs' store cached content on edge servers in point-of-presence (POP) locations that

are close to end users, to minimize latency.

Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

Traffic Manager routing methods

01/21/2021 • 13 minutes to read • +6

Azure Traffic Manager supports six traffic-routing methods to determine how to route network traffic to the various service endpoints. For any profile, Traffic Manager applies the traffic-routing method associated to it to each DNS query it receives. The traffic-routing method determines which endpoint is returned in the DNS response.

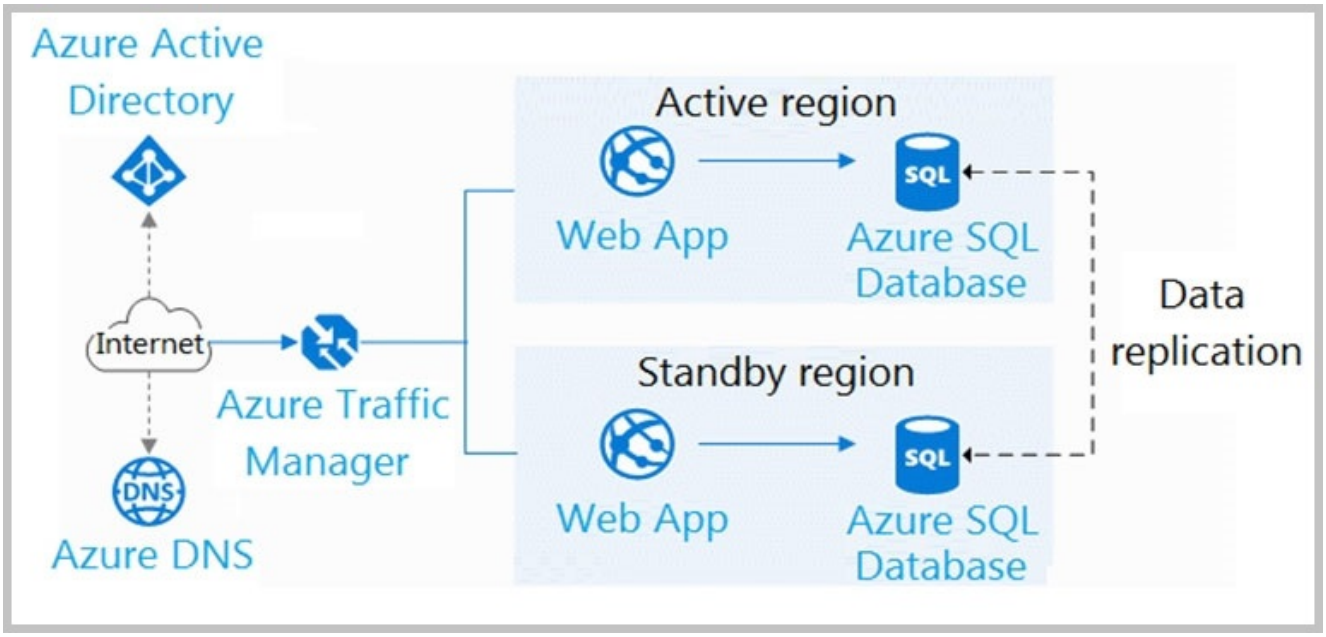
The following traffic routing methods are available in Traffic Manager:

- **Priority**: Select **Priority** routing when you want to have a primary service endpoint for all traffic. You can provide multiple backup endpoints in case the primary or one of the backup endpoints is unavailable.
- **Weighted**: Select **Weighted** routing when you want to distribute traffic across a set of endpoints based on their weight. Set the weight the same to distribute evenly across all endpoints.
- **Performance**: Select **Performance** routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.
- **Geographic**: Select **Geographic** routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.
- **Multivalue**: Select **MultiValue** for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, all healthy endpoints are returned.
- **Subnet**: Select **Subnet** traffic-routing method to map sets of end-user IP address ranges to a specific endpoint. When a request is received, the endpoint returned will be the one mapped for that request's source IP address.

All Traffic Manager profiles have health monitoring and automatic failover of endpoints. For more information, see Traffic Manager Endpoint Monitoring. Within a Traffic Manager profile, you can only configure one traffic routing method at a time. You can select a different traffic routing method for your profile at any time. Your changes will be applied within a minute without any downtime. You can combine traffic routing methods by using nested Traffic Manager profiles. Nesting profiles allows for sophisticated traffic-routing configurations that meet the needs of larger and complex applications. For more information, see nested Traffic Manager profiles.

5. Question

You have the application architecture shown in the following exhibit:



Select the answer choice that completes the following statement based on the information presented in the graphic.

To control the threshold for failing over the front end to the standby region. you must configure the ----------.

- A. Application Insights availability test
- B. Azure SQL Database failover groups
- C. Connection Monitor in Azure Network Watcher
- **D. Endpoint monitor settings in Azure Traffic Manager**

Correct

Azure Traffic Manager includes built-in endpoint monitoring and automatic endpoint failover. This feature helps you deliver high-availability applications that are resilient to endpoint failure, including Azure region failures.

To configure endpoint monitoring, you must specify the following settings on your Traffic Manager profile: Protocol, Port, Path, custom header settings, etc.

Incorrect Answers:

A. Application Insights availability test

This is a simple test through the portal to validate whether an endpoint is responding and measure performance associated with that response.

B. Azure SQL Database failover groups

A failover group is a named group of databases managed by a single server or within a managed instance that can fail over as a unit to another region in case all or some primary databases become unavailable due to an outage in the primary region. In this scenario, the requirement is front-end failover.

C. Connection Monitor in Azure Network Watcher

Connection Monitor provides unified end-to-end connection monitoring in Azure Network Watcher. The Connection Monitor feature supports hybrid and Azure cloud deployments. Network Watcher provides

tools to monitor, diagnose, and view connectivity-related metrics for your Azure deployments. For example, Your front-end web server VM communicates with a database server VM in a multi-tier application. You want to check network connectivity between the two VMs.

Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring

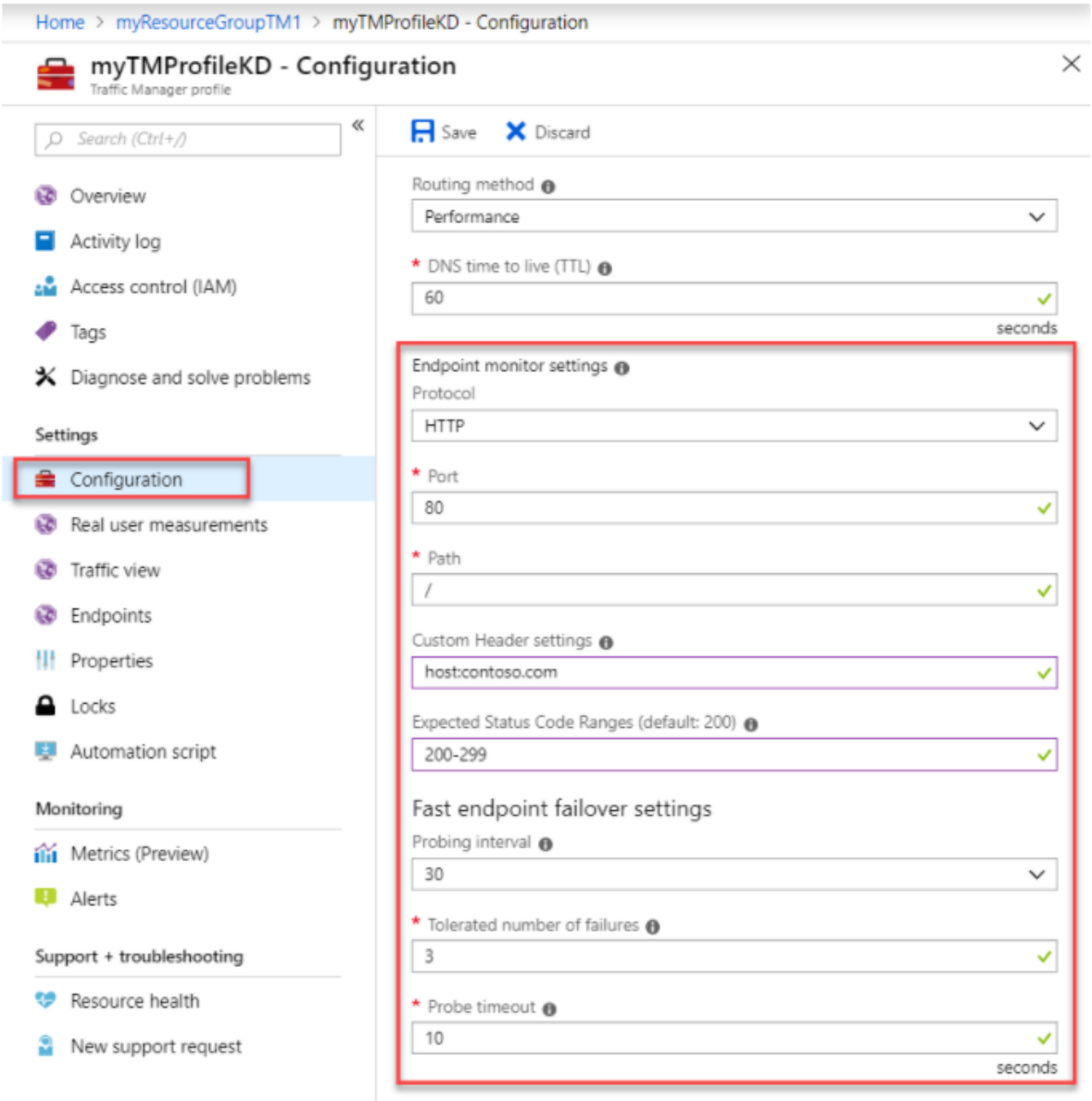
Traffic Manager endpoint monitoring

01/22/2021 • 15 minutes to read • +7

Azure Traffic Manager includes built-in endpoint monitoring and automatic endpoint failover. This feature helps you deliver high-availability applications that are resilient to endpoint failure, including Azure region failures.

Configure endpoint monitoring

To configure endpoint monitoring, you must specify the following settings on your Traffic Manager profile:



6. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam

time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

? Existing Environment

? Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

?Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

? Problem Statements

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

? Requirements

? Planned Changes

? Fabrikam plans to move most of its production workloads to Azure during the next few years.

? As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

? All R&D operations will remain on-premises.

? Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

? Technical Requirements

Fabrikam identifies the following technical requirements:

? Web site content must be easily updated from a single point.

? User input must be minimized when provisioning new web app instances.

? Whenever possible, existing on-premises licenses must be used to reduce cost.

? Users must always authenticate by using their corp.fabrikam.com UPN identity.

? Any new deployments to Azure must be redundant in case an Azure region fails.

? Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

? An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

? Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on- premises network.

? Database Requirements

Fabrikam identifies the following database requirements:

? Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

? To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

? Database backups must be retained for a minimum of seven years to meet compliance requirements.

? Security Requirements

Fabrikam identifies the following security requirements:

? Company information including policies, templates, and data must be inaccessible to anyone outside the company.

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

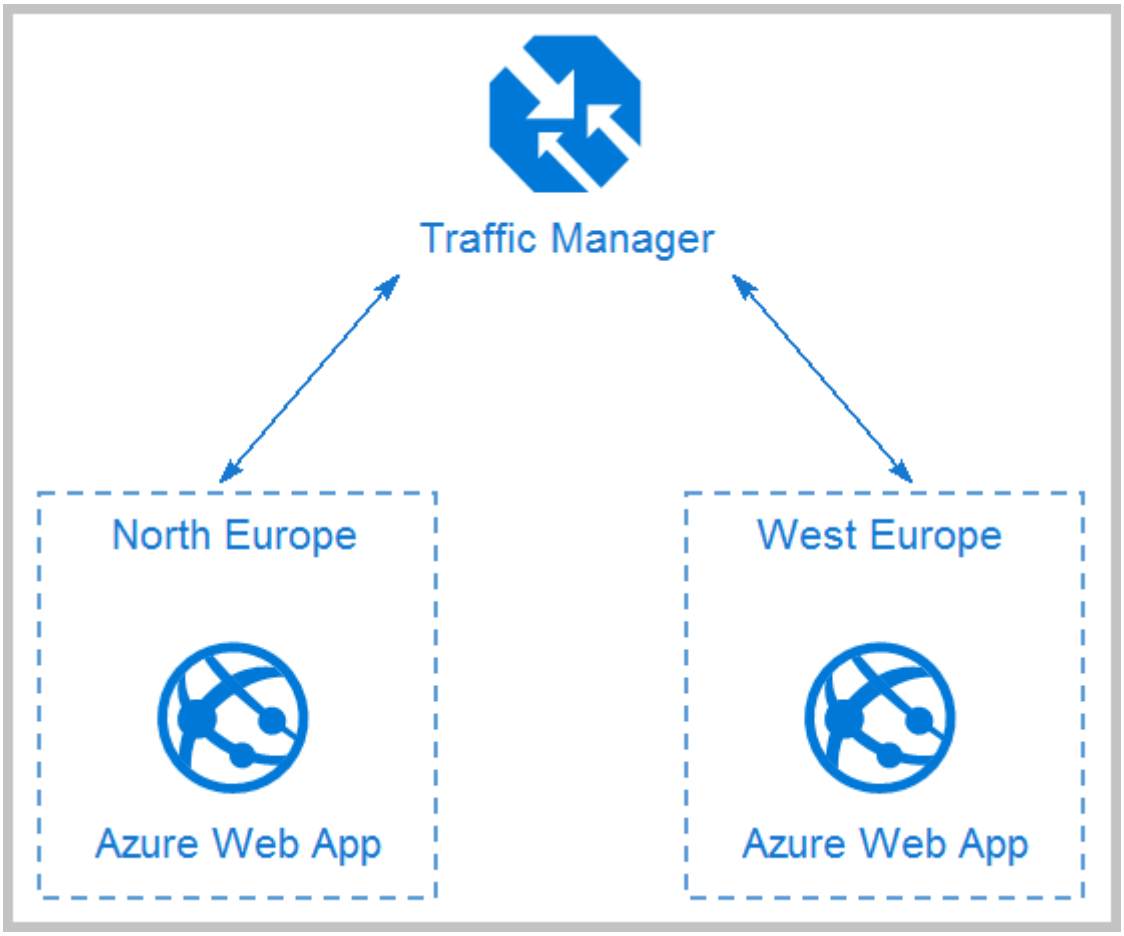
? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

? The testing of WebApp1 updates must not be visible to anyone outside the company.

Question

You design a solution for the web tier of WebApp1 as shown in the exhibit.



For the following statements, select Yes if the statement is true. Otherwise, select No.

The design supports the technical requirements for redundancy

- A. Yes
- B. No

Correct

Any new deployments to Azure must be redundant in case an Azure region fails.

Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-failover-and-recovery

https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans

What is Traffic Manager?

01/19/2021 • 2 minutes to read • +4

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Note

Azure provides a suite of fully managed load-balancing solutions for your scenarios.

- If you want to load balance between your servers in a region at the application layer, review **Application Gateway**.
- If you need to optimize global routing of your web traffic and optimize top-tier end-user performance and reliability through quick global failover, see **Front Door**.
- To do network layer load balancing, review **Load Balancer**.

Your end-to-end scenarios may benefit from combining these solutions as needed. For an Azure load-balancing options comparison, see **Overview of load-balancing options in Azure**.

7. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

? Existing Environment

? Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

?Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

? Problem Statements

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

? Requirements

? Planned Changes

? Fabrikam plans to move most of its production workloads to Azure during the next few years.

? As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

? All R&D operations will remain on-premises.

? Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

? Technical Requirements

Fabrikam identifies the following technical requirements:

? Web site content must be easily updated from a single point.

? User input must be minimized when provisioning new web app instances.

? Whenever possible, existing on-premises licenses must be used to reduce cost.

? Users must always authenticate by using their corp.fabrikam.com UPN identity.

? Any new deployments to Azure must be redundant in case an Azure region fails.

? Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

? An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

? Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on- premises network.

? Database Requirements

Fabrikam identifies the following database requirements:

? Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

? To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

? Database backups must be retained for a minimum of seven years to meet compliance requirements.

? Security Requirements

Fabrikam identifies the following security requirements:

? Company information including policies, templates, and data must be inaccessible to anyone outside the company.

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

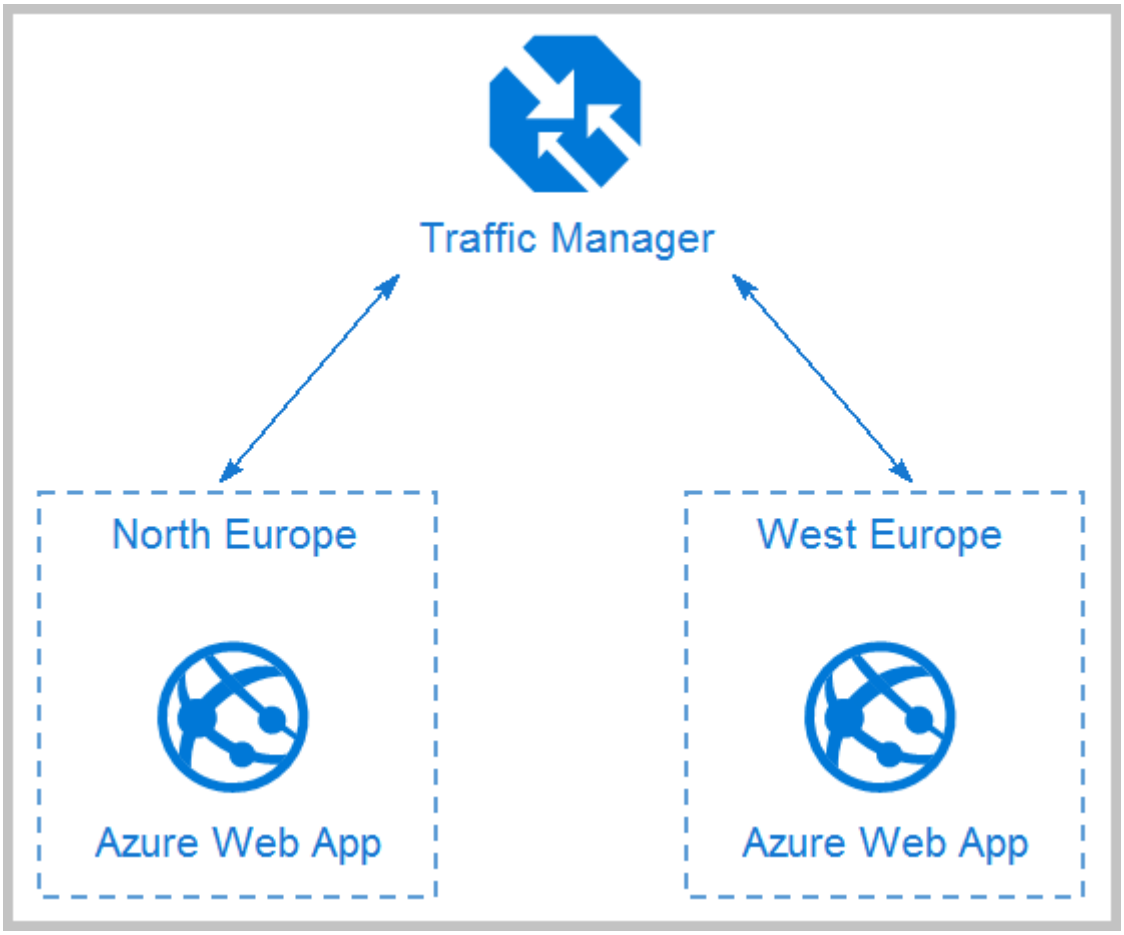
? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

? The testing of WebApp1 updates must not be visible to anyone outside the company.

Question

You design a solution for the web tier of WebApp1 as shown in the exhibit.



For the following statements, select Yes if the statement is true. Otherwise, select No.

The design supports autoscaling

A. Yes

B. No

Correct

Recent changes in Azure brought some significant changes in autoscaling options for Azure Web Apps (i.e. Azure App Service to be precise as scaling happens on App Service plan level and has effect on all Web Apps running in that App Service plan).

Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-failover-and-recovery

https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans

What is Traffic Manager?

01/19/2021 • 2 minutes to read • +4

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Note

Azure provides a suite of fully managed load-balancing solutions for your scenarios.

- If you want to load balance between your servers in a region at the application layer, review **Application Gateway**.
- If you need to optimize global routing of your web traffic and optimize top-tier end-user performance and reliability through quick global failover, see **Front Door**.
- To do network layer load balancing, review **Load Balancer**.

Your end-to-end scenarios may benefit from combining these solutions as needed. For an Azure load-balancing options comparison, see **Overview of load-balancing options in Azure**.

8. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

? Existing Environment

? Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

?Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

? Problem Statements

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

? Requirements

? Planned Changes

? Fabrikam plans to move most of its production workloads to Azure during the next few years.

? As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

? All R&D operations will remain on-premises.

? Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

? Technical Requirements

Fabrikam identifies the following technical requirements:

? Web site content must be easily updated from a single point.

? User input must be minimized when provisioning new web app instances.

? Whenever possible, existing on-premises licenses must be used to reduce cost.

? Users must always authenticate by using their corp.fabrikam.com UPN identity.

? Any new deployments to Azure must be redundant in case an Azure region fails.

? Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

? An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

? Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on- premises network.

? Database Requirements

Fabrikam identifies the following database requirements:

? Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

? To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

? Database backups must be retained for a minimum of seven years to meet compliance requirements.

? Security Requirements

Fabrikam identifies the following security requirements:

? Company information including policies, templates, and data must be inaccessible to anyone outside the company.

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

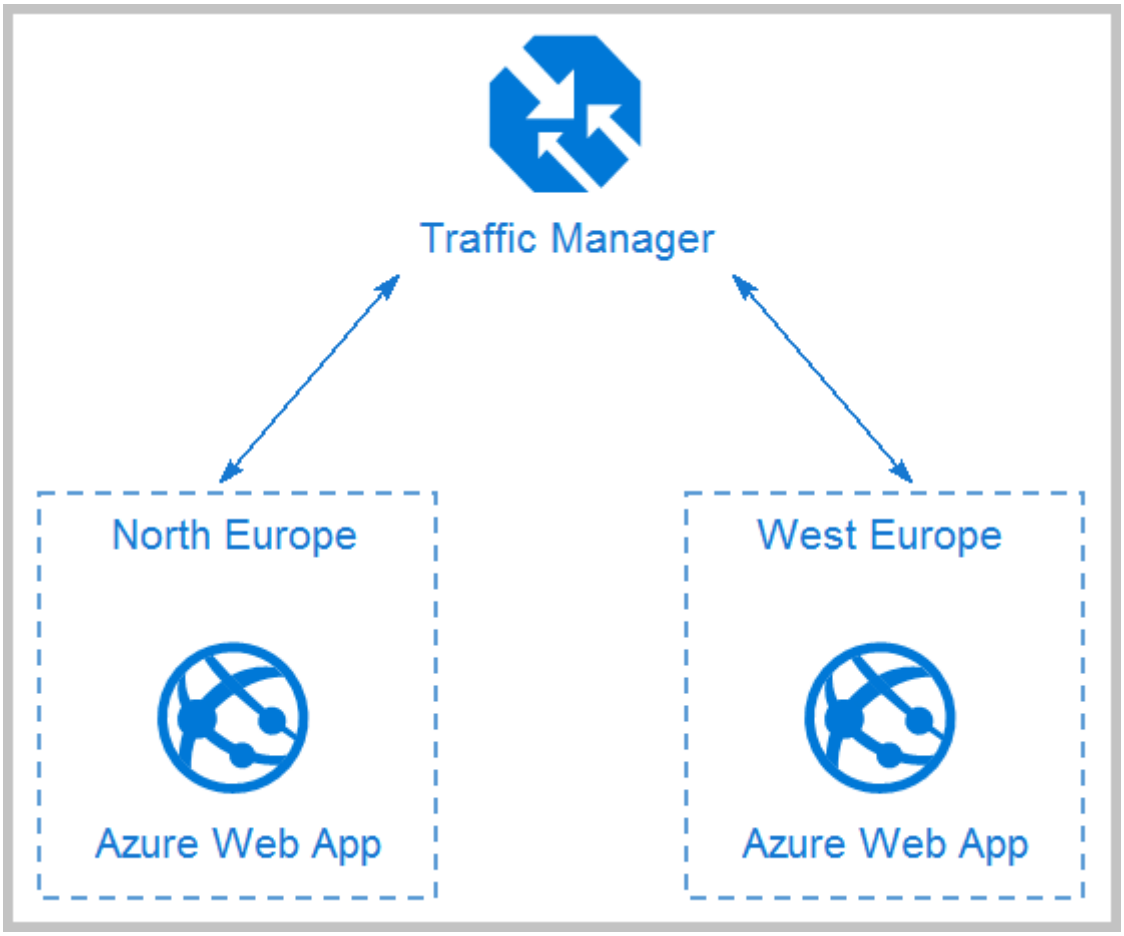
? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

? The testing of WebApp1 updates must not be visible to anyone outside the company.

Question

You design a solution for the web tier of WebApp1 as shown in the exhibit.



For the following statements, select Yes if the statement is true. Otherwise, select No.

The design requires a manual configuration if an Azure region fails

- A. Yes
- B. No

Correct

Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models.

Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Reference:

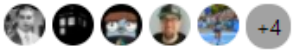
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-failover-and-recovery

https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans

What is Traffic Manager?

01/19/2021 • 2 minutes to read • 

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Note

Azure provides a suite of fully managed load-balancing solutions for your scenarios.

- If you want to load balance between your servers in a region at the application layer, review **Application Gateway**.
- If you need to optimize global routing of your web traffic and optimize top-tier end-user performance and reliability through quick global failover, see **Front Door**.
- To do network layer load balancing, review **Load Balancer**.

Your end-to-end scenarios may benefit from combining these solutions as needed. For an Azure load-balancing options comparison, see **Overview of load-balancing options in Azure**.

9. Question

Case Study

This is a case study. In the real exam, case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

Overview

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

? Existing Environment

? Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

?Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

? Problem Statements

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

? Requirements

? Planned Changes

? Fabrikam plans to move most of its production workloads to Azure during the next few years.

? As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft 365 deployment.

? All R&D operations will remain on-premises.

? Fabrikam plans to migrate the production and test instances of WebApp1 to Azure.

? Technical Requirements

Fabrikam identifies the following technical requirements:

? Web site content must be easily updated from a single point.

? User input must be minimized when provisioning new web app instances.

? Whenever possible, existing on-premises licenses must be used to reduce cost.

? Users must always authenticate by using their corp.fabrikam.com UPN identity.

? Any new deployments to Azure must be redundant in case an Azure region fails.

? Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.

? An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.

? Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the on- premises network.

? Database Requirements

Fabrikam identifies the following database requirements:

? Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.

? To avoid disrupting customer access, database downtime must be minimized when databases are migrated.

? Database backups must be retained for a minimum of seven years to meet compliance requirements.

? Security Requirements

Fabrikam identifies the following security requirements:

? Company information including policies, templates, and data must be inaccessible to anyone outside the company.

? Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.

? Administrators must be able authenticate to the Azure portal by using their corp.fabrikam.com credentials.

? All administrative access to the Azure portal must be secured by using multi-factor authentication.

? The testing of WebApp1 updates must not be visible to anyone outside the company.

Question

You need to recommend a data storage strategy for WebApp1.

What should you include in the recommendation?

- A. a vCore-based Azure SQL database
- B. an Azure virtual machine that runs SQL Server
- C. an Azure SQL Database elastic pool
- D. a fixed-size DTU Azure SQL database

Correct

If you use the vCore-based Azure SQL database, you are fulfilling the requirement of using Platform as service-based services. You can also use long term retention to ensure database backups are retained for seven years. By using the vCore model, you can save on costs by using existing licenses that are based on the Microsoft Enterprise Agreement.

Incorrect Answers:

B. an Azure virtual machine that runs SQL Server

PaaS services should be used whenever possible

C. an Azure SQL Database elastic pool

Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands.

D. a fixed-size DTU Azure SQL database

No because usage is unpredictable

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tiers-vcore?tabs=azure-portal

https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tiers-sql-database-vcore

vCore model overview - Azure SQL Database and Azure SQL Managed Instance

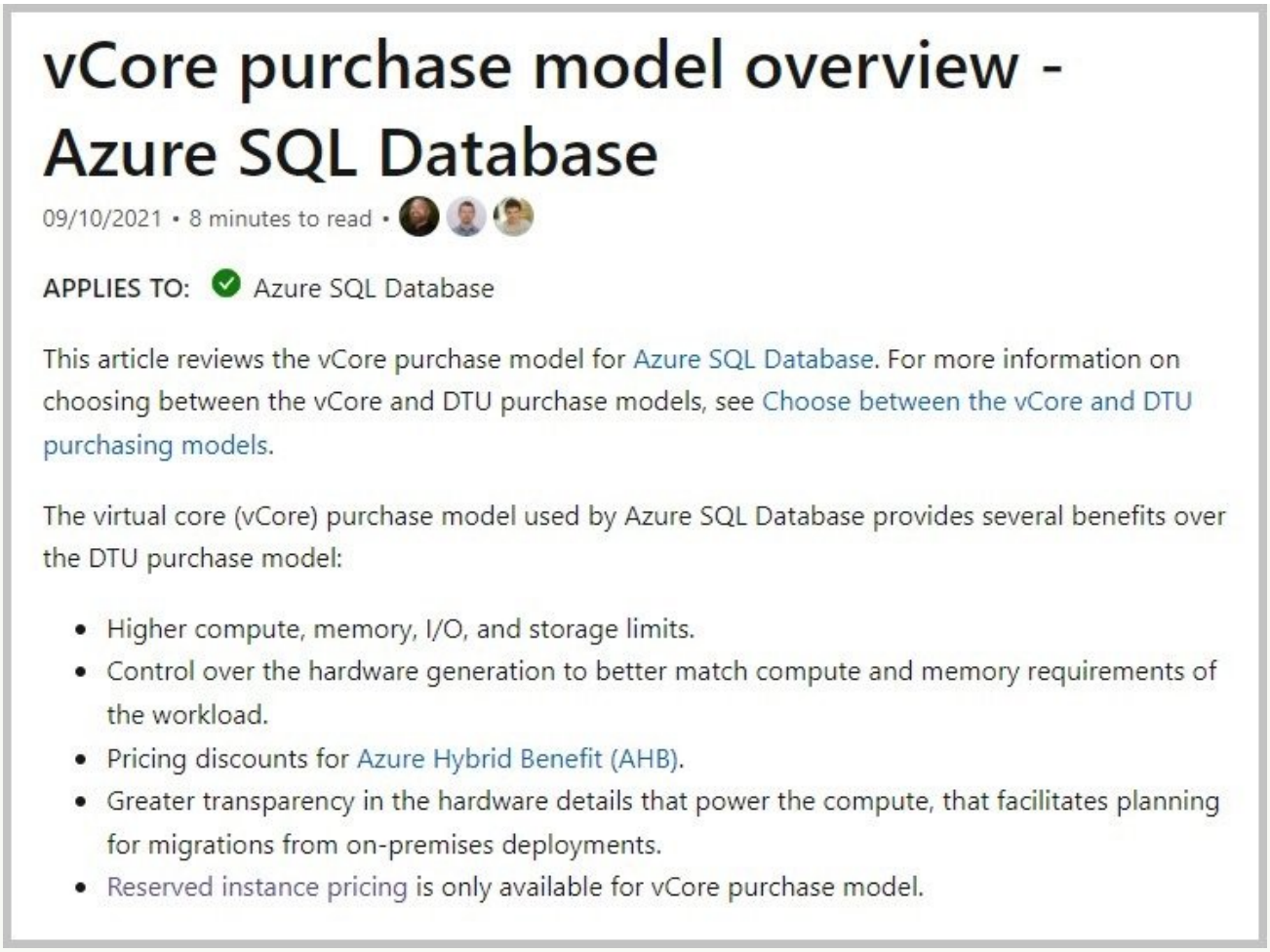
05/18/2021 • 2 minutes to read • +6

APPLIES TO: Azure SQL Database Azure SQL Managed Instance

The virtual core (vCore) purchasing model used by Azure SQL Database and Azure SQL Managed Instance provides several benefits:

- Control over the hardware generation to better match compute and memory requirements of the workload.
- Pricing discounts for Azure Hybrid Benefit (AHB) and Reserved Instance (RI).
- Greater transparency in the hardware details that power the compute, that facilitates planning for migrations from on-premises deployments.
- In the case of Azure SQL Database, vCore purchasing model provides higher compute, memory, I/O, and storage limits than the DTU model.

For more information on choosing between the vCore and DTU purchase models, see Choose between the vCore and DTU purchasing models.



vCore purchase model overview - Azure SQL Database

09/10/2021 • 8 minutes to read •

APPLIES TO: Azure SQL Database

This article reviews the vCore purchase model for Azure SQL Database. For more information on choosing between the vCore and DTU purchase models, see Choose between the vCore and DTU purchasing models.

The virtual core (vCore) purchase model used by Azure SQL Database provides several benefits over the DTU purchase model:

- Higher compute, memory, I/O, and storage limits.
- Control over the hardware generation to better match compute and memory requirements of the workload.
- Pricing discounts for Azure Hybrid Benefit (AHB).
- Greater transparency in the hardware details that power the compute, that facilitates planning for migrations from on-premises deployments.
- Reserved instance pricing is only available for vCore purchase model.

10. Question

You need to design a storage solution for an app that will store large amounts of frequently used data. The solution must meet the following requirements:

? Maximize data throughput.

? Prevent the modification of data for one year.

? Minimize latency for read and write operations.

Which Azure Storage account type should you recommend?

- A. BlobStorage
- **B. BlockBlobStorage**
- C. FileStorage
- D. StorageV2 with Premium performance
- E. StorageV2 with Standard performance

Incorrect

Block Blob is a premium storage account type for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.

The solution is B, because BlockBlobStorage provide a very low latency(x40) (Read and Write) and Throughput (x5).

Because One big file is splitted in “blobs“ that are processed in parallel (for read and write).

Reference:

https://azure.microsoft.com/en-us/blog/premium-block-blob-storage-a-new-level-of-performance/

https://docs.microsoft.com/en-us/azure/storage/blobs/archive-blob

Premium Block Blob Storage - a new level of performance

Posted on November 29, 2018

Claus Joergensen, Principal Program Manager, Azure Storage

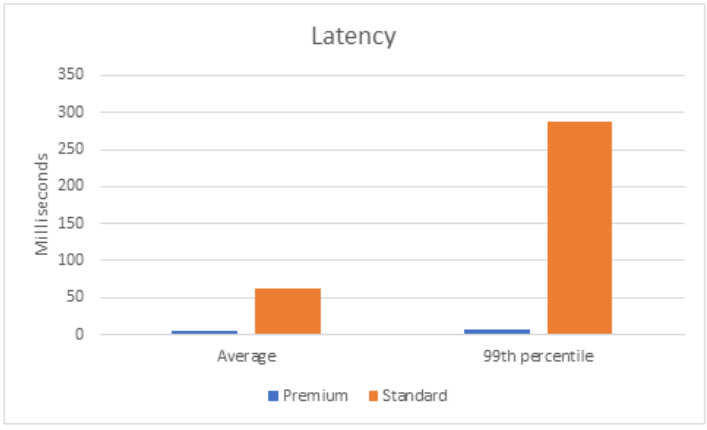
On March 25, 2019, Azure Premium Block Blob Storage became generally available. For more information, please refer to the blog post, “Azure Premium Block Blob Storage is now generally available.”

Premium Block Blob Storage, which is currently in limited public preview, unlocks a new level of performance in public cloud object storage. It uses a combination of solid-state drives in our storage clusters and enhancements to our blob storage software to provide high throughput and very fast response times. In this blog post we will take a closer look at some of these performance enhancements.

Low and consistent latency

Many enterprise applications and the users that use them require very fast response times. Storage response time, also known as latency, is often a significant portion of the overall time users must wait for a response.

At Microsoft Ignite 2018, I did a storage latency demonstration, comparing Premium Blob Storage to our Standard Blob Storage. The demo reads a random selection of 10,000 objects from a population of 1,000,000 64KB objects measuring time to last byte. Each object is a binary random byte array.



In the demo, the average latency for Standard is 61.4ms compared to Premium at 5.3ms, which is **more than an order of magnitude better**.

It is equally important to consistently provide low latency, which we measure by looking at the 99th percentile. In the demo, the 99th percentile for the standard is 287.3ms compared to 6.9ms for Premium, which is a whopping **40 times better**.

11. Question

You need to design a storage solution for an app that will store large amounts of frequently used data. The solution must meet the following requirements:

? Maximize data throughput.

? Prevent the modification of data for one year.

? Minimize latency for read and write operations.

Which Azure Storage service should you recommend?

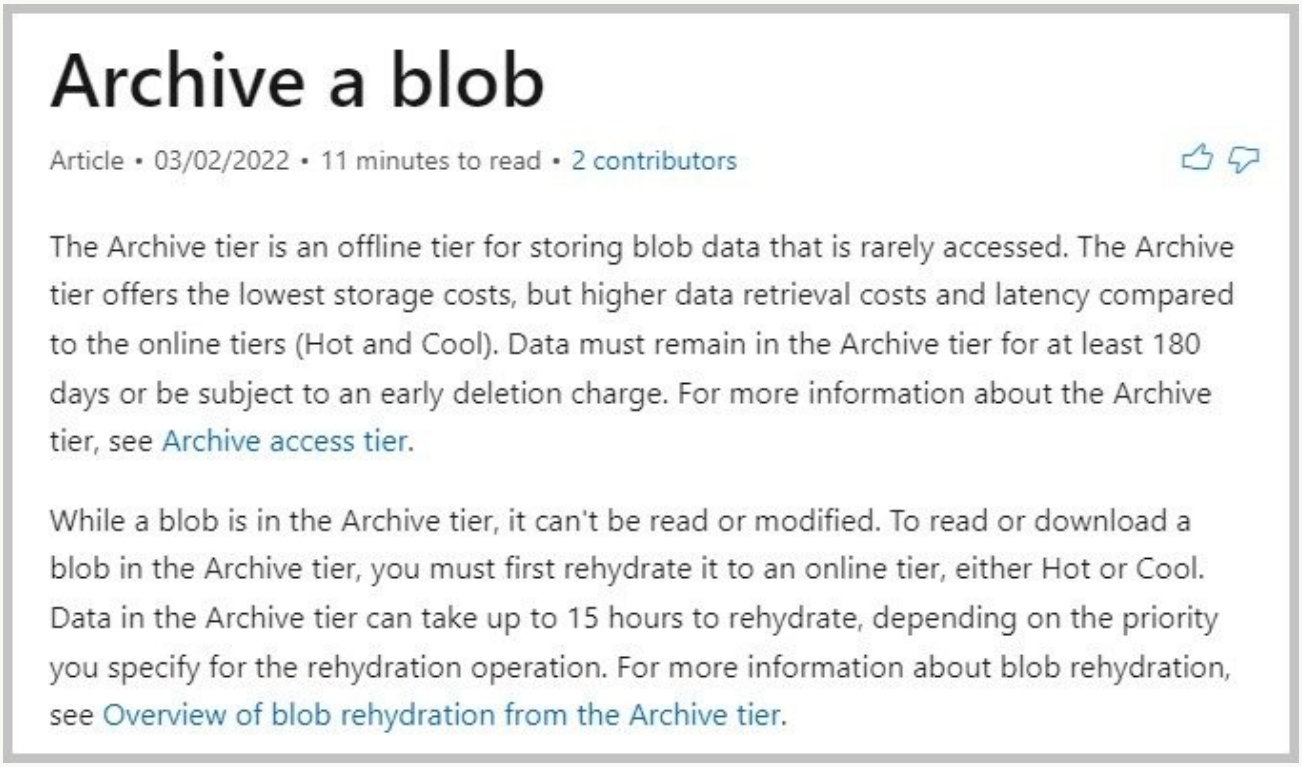
- A. Blob
- B. File
- C. Table

Correct

The Archive tier is an offline tier for storing blob data that is rarely accessed. The Archive tier offers the lowest storage costs, but higher data retrieval costs and latency compared to the online tiers (Hot and Cool). Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/archive-blob



Archive a blob

Article • 03/02/2022 • 11 minutes to read • 2 contributors

The Archive tier is an offline tier for storing blob data that is rarely accessed. The Archive tier offers the lowest storage costs, but higher data retrieval costs and latency compared to the online tiers (Hot and Cool). Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge. For more information about the Archive tier, see Archive access tier.

While a blob is in the Archive tier, it can't be read or modified. To read or download a blob in the Archive tier, you must first rehydrate it to an online tier, either Hot or Cool. Data in the Archive tier can take up to 15 hours to rehydrate, depending on the priority you specify for the rehydration operation. For more information about blob rehydration, see Overview of blob rehydration from the Archive tier.

12. Question

You are designing an application that will be hosted in Azure.

The application will host video files that range from 50 MB to 12 GB. The application will use certificate-based authentication and will be available to users on the internet.

You need to recommend a storage option for the video files. The solution must provide the fastest read performance and must minimize storage costs.

What should you recommend?

A. Azure Files

B. Azure Data Lake Storage Gen2

C. Azure Blob Storage

D. Azure SQL Database

Correct

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data.

Blob storage is ideal for:

? Serving images or documents directly to a browser.

? Storing files for distributed access.

? Streaming video and audio.

? Storing data for backup and restore, disaster recovery, and archiving.

? Storing data for analysis by an on-premises or Azure-hosted service.

Objects in Blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library.

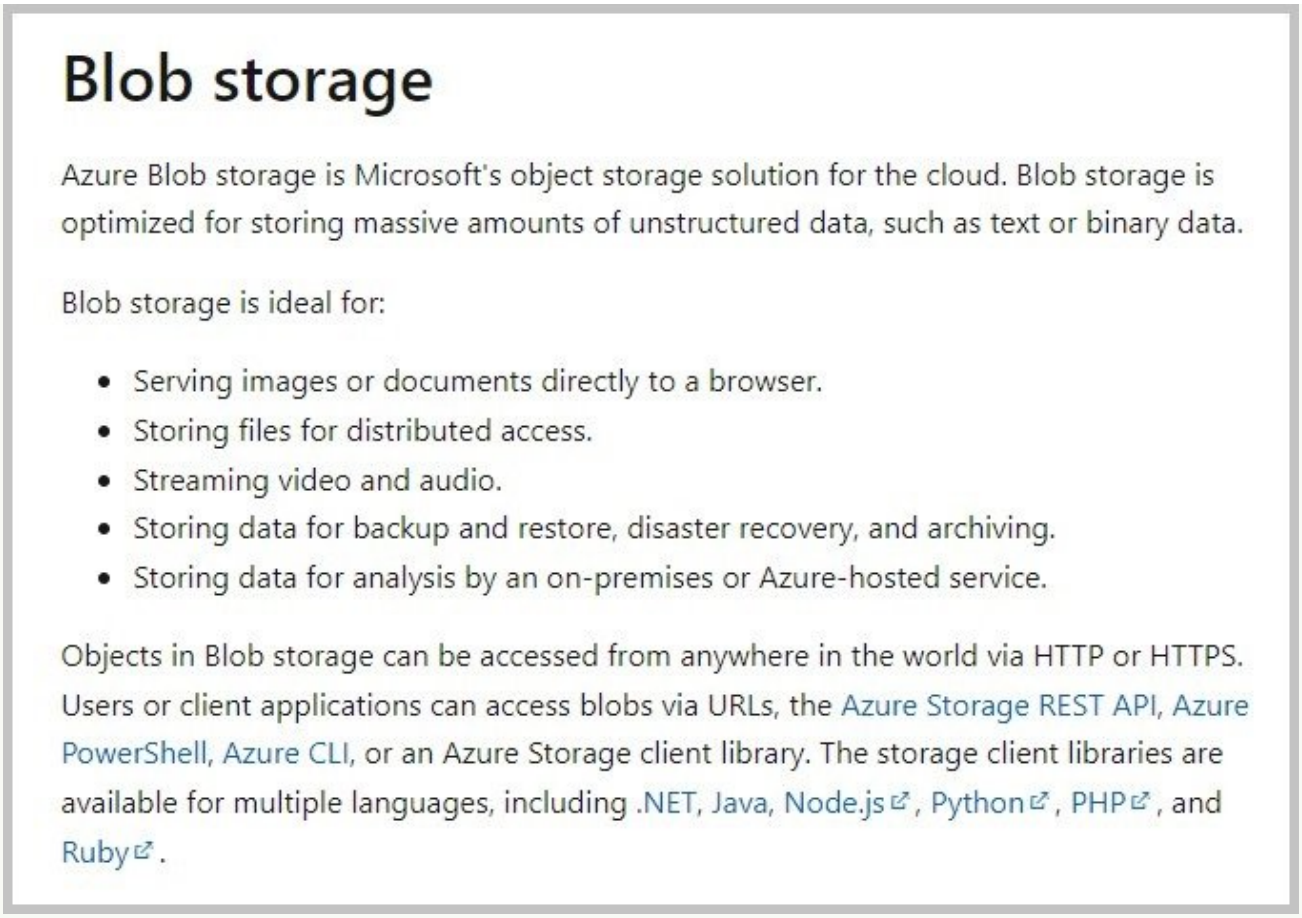
Note: Blob Storage: Stores large amounts of unstructured data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data publicly to the world, or to store application data privately.

Max file in Blob Storage. 4.77 TB.

Reference:

https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/digital-media-video

https://docs.microsoft.com/en-gb/azure/storage/common/storage-introduction#blob-storage



Blob storage

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data.

Blob storage is ideal for:

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

Objects in Blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

13. Question

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. The subscription contains 10 resource groups, one for each department at your company.

Each department has a specific spending limit for its Azure resources.

You need to ensure that when a department reaches its spending limit, the compute resources of the department shut down automatically.

Which two features should you include in the solution?

- [x] A. Azure Logic Apps
- [ ] B. Azure Monitor alerts
- [x] C. the spending limit of an Azure account
- [x] D. Cost Management budgets
- [ ] E. Azure Log Analytics alerts

Incorrect

Cost control is a critical component to maximizing the value of your investment in the cloud.

Budgets are commonly used as part of cost control. Budgets can be scoped in Azure. For instance, you

could narrow your budget view based on subscription, resource groups, or a collection of resources.

? Create an Azure Automation Runbook to stop VMs by using webhooks.

? Create an Azure Logic App to be triggered based on the budget threshold value and call the runbook with the right parameters.

? Create an Azure Monitor Action Group that will be configured to trigger the Azure Logic App when the budget threshold is met.

? Create the Azure budget with the wanted thresholds and wire it to the action group.

Incorrect Answers:

B. Azure Monitor alerts

Alerts proactively notify you when issues are found with your infrastructure or application using your monitoring data in Azure Monitor. They allow you to identify and address issues before the users of your system notice them. It is not required to trigger the logic app.

C. the spending limit of an Azure account

The spending limit in Azure prevents spending over your credit amount. When your usage results in charges that exhaust your spending limit, the services that you deployed are disabled for the rest of that billing period.

E. Azure Log Analytics alerts

Log alerts allow users to use a Log Analytics query to evaluate resources logs every set frequency, and fire an alert based on the results.

Reference:

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario

Manage costs with Azure Budgets

09/15/2021 • 17 minutes to read • +1

Cost control is a critical component to maximizing the value of your investment in the cloud. There are several scenarios where cost visibility, reporting, and cost-based orchestration are critical to continued business operations. Azure Cost Management APIs provide a set of APIs to support each of these scenarios. The APIs provide usage details, allowing you to view granular instance level costs.

Budgets are commonly used as part of cost control. Budgets can be scoped in Azure. For instance, you could narrow your budget view based on subscription, resource groups, or a collection of resources. In addition to using the budgets API to notify you via email when a budget threshold is reached, you can use Azure Monitor action groups to trigger an orchestrated set of actions resulting from a budget event.

A common budgets scenario for a customer running a non-critical workload could occur when they want to manage against a budget and also get to a predictable cost when looking at the monthly invoice. This scenario requires some cost-based orchestration of resources that are part of the Azure environment. In this scenario, a monthly budget of $1000 for the subscription is set. Also, notification thresholds are set to trigger a few orchestrations. This scenario starts with an 80% cost threshold, which will stop all VMs in the resource group **Optional**. Then, at the 100% cost threshold, all VM instances will be stopped.

To configure this scenario, you'll complete the following actions by using the steps provided in each section of this tutorial.

These actions included in this tutorial allow you to:

- Create an Azure Automation Runbook to stop VMs by using webhooks.
- Create an Azure Logic App to be triggered based on the budget threshold value and call the runbook with the right parameters.
- Create an Azure Monitor Action Group that will be configured to trigger the Azure Logic App when the budget threshold is met.
- Create the Azure budget with the wanted thresholds and wire it to the action group.

14. Question

You have an Azure subscription that contains the resources shown in the following table

Name	Type	Kind	Location
Storage1	Azure Storage Account	Storage	East US
Storage2	Azure Storage Account	StorageV2	East US
Workspace1	Azure Log Analytics Workspace	Not Applicable	East US
Workspace2	Azure Log Analytics Workspace	Not Applicable	East US
Hub1	Azure Event Hub	Not Applicable	East US

You create an Azure SQL database named DB1 that is hosted in the East US region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archives SQLInsights to storage1 and sends SQLInsights to Workspace1.

For the following statements, select Yes if the statement is true, Otherwise, select No.

You can add a new diagnostic setting that archives SQLInsights logs to storage2

- A. Yes
- B. No

Incorrect

You can create up to three parallel connections to stream diagnostic telemetry.

Platform logs and metrics can be sent to the destinations Log Analytics workspace, Event hubs, Azure storage account Only difference Azure storage account is referred for Archiving logs and metrics.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings

https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal

Create diagnostic settings to send platform logs and metrics to different destinations

06/09/2021 • 11 minutes to read •

Platform logs in Azure, including the Azure Activity log and resource logs, provide detailed diagnostic and auditing information for Azure resources and the Azure platform they depend on. Platform metrics are collected by default and typically stored in the Azure Monitor metrics database. This article provides details on creating and configuring diagnostic settings to send platform metrics and platform logs to different destinations.

> ⓘ **Important**
>
> Before you create a diagnostic setting for the Activity log, you should first disable any legacy configuration. See **Legacy collection methods** for details.

Each Azure resource requires its own diagnostic setting, which defines the following criteria:

- Categories of logs and metric data sent to the destinations defined in the setting. The available categories will vary for different resource types.
- One or more destinations to send the logs. Current destinations include Log Analytics workspace, Event Hubs, and Azure Storage.

A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings.

Destinations

Platform logs and metrics can be sent to the destinations in the following table.

Destination	Description
Log Analytics workspace	Sending logs and metrics to a Log Analytics workspace allows you to analyze them with other monitoring data collected by Azure Monitor using powerful log queries and also to leverage other Azure Monitor features such as alerts and visualizations.
Event hubs	Sending logs and metrics to Event Hubs allows you to stream data to external systems such as third-party SIEMs and other log analytics solutions.
Azure storage account	Archiving logs and metrics to an Azure storage account is useful for audit, static analysis, or backup. Compared to Azure Monitor Logs and a Log Analytics workspace, Azure storage is less expensive and logs can be kept there indefinitely.

15. Question

You have an Azure subscription that contains the resources shown in the following table

Name	Type	Kind	Location
Storage1	Azure Storage Account	Storage	East US
Storage2	Azure Storage Account	StorageV2	East US
Workspace1	Azure Log Analytics Workspace	Not Applicable	East US
Workspace2	Azure Log Analytics Workspace	Not Applicable	East US
Hub1	Azure Event Hub	Not Applicable	East US

You create an Azure SQL database named DB1 that is hosted in the East US region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archives SQLInsights to storage1 and sends SQLInsights to Workspace1.

For the following statements, select Yes if the statement is true, Otherwise, select No.

You can add a new diagnostic setting that sends SQLInsights logs to Workspace2

- A. Yes
- B. No

Correct

Platform logs and metrics can be sent to the destinations Log Analytics workspace, Event hubs, Azure storage account Only difference Azure storage account is referred for Archiving logs and metrics.

Note: Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings

https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal

Create diagnostic settings to send platform logs and metrics to different destinations

06/09/2021 • 11 minutes to read •

Platform logs in Azure, including the Azure Activity log and resource logs, provide detailed diagnostic and auditing information for Azure resources and the Azure platform they depend on. Platform metrics are collected by default and typically stored in the Azure Monitor metrics database. This article provides details on creating and configuring diagnostic settings to send platform metrics and platform logs to different destinations.

> ⓘ **Important**
>
> Before you create a diagnostic setting for the Activity log, you should first disable any legacy configuration. See **Legacy collection methods** for details.

Each Azure resource requires its own diagnostic setting, which defines the following criteria:

- Categories of logs and metric data sent to the destinations defined in the setting. The available categories will vary for different resource types.
- One or more destinations to send the logs. Current destinations include Log Analytics workspace, Event Hubs, and Azure Storage.

A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings.

Destinations

Platform logs and metrics can be sent to the destinations in the following table.

Destination	Description
Log Analytics workspace	Sending logs and metrics to a Log Analytics workspace allows you to analyze them with other monitoring data collected by Azure Monitor using powerful log queries and also to leverage other Azure Monitor features such as alerts and visualizations.
Event hubs	Sending logs and metrics to Event Hubs allows you to stream data to external systems such as third-party SIEMs and other log analytics solutions.
Azure storage account	Archiving logs and metrics to an Azure storage account is useful for audit, static analysis, or backup. Compared to Azure Monitor Logs and a Log Analytics workspace, Azure storage is less expensive and logs can be kept there indefinitely.

16. Question

You have an Azure subscription that contains the resources shown in the following table

Name	Type	Kind	Location
Storage1	Azure Storage Account	Storage	East US
Storage2	Azure Storage Account	StorageV2	East US
Workspace1	Azure Log Analytics Workspace	Not Applicable	East US
Workspace2	Azure Log Analytics Workspace	Not Applicable	East US
Hub1	Azure Event Hub	Not Applicable	East US

You create an Azure SQL database named DB1 that is hosted in the East US region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archives SQLInsights to storage1 and sends SQLInsights to Workspace1.

For the following statements, select Yes if the statement is true, Otherwise, select No.

You can add a new diagnostic setting that sends SQLInsights logs to Hub1

- A. Yes
- B. No

Correct

Sending logs to Event Hubs allows you to stream data to external systems such as third-party SIEMs and other log analytics solutions.

Note: A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings.

Note: Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings

https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal

Create diagnostic settings to send platform logs and metrics to different destinations

06/09/2021 • 11 minutes to read • 

Platform logs in Azure, including the Azure Activity log and resource logs, provide detailed diagnostic and auditing information for Azure resources and the Azure platform they depend on. Platform metrics are collected by default and typically stored in the Azure Monitor metrics database. This article provides details on creating and configuring diagnostic settings to send platform metrics and platform logs to different destinations.

> ⓘ **Important**
>
> Before you create a diagnostic setting for the Activity log, you should first disable any legacy configuration. See **Legacy collection methods** for details.

Each Azure resource requires its own diagnostic setting, which defines the following criteria:

- Categories of logs and metric data sent to the destinations defined in the setting. The available categories will vary for different resource types.
- One or more destinations to send the logs. Current destinations include Log Analytics workspace, Event Hubs, and Azure Storage.

A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings.

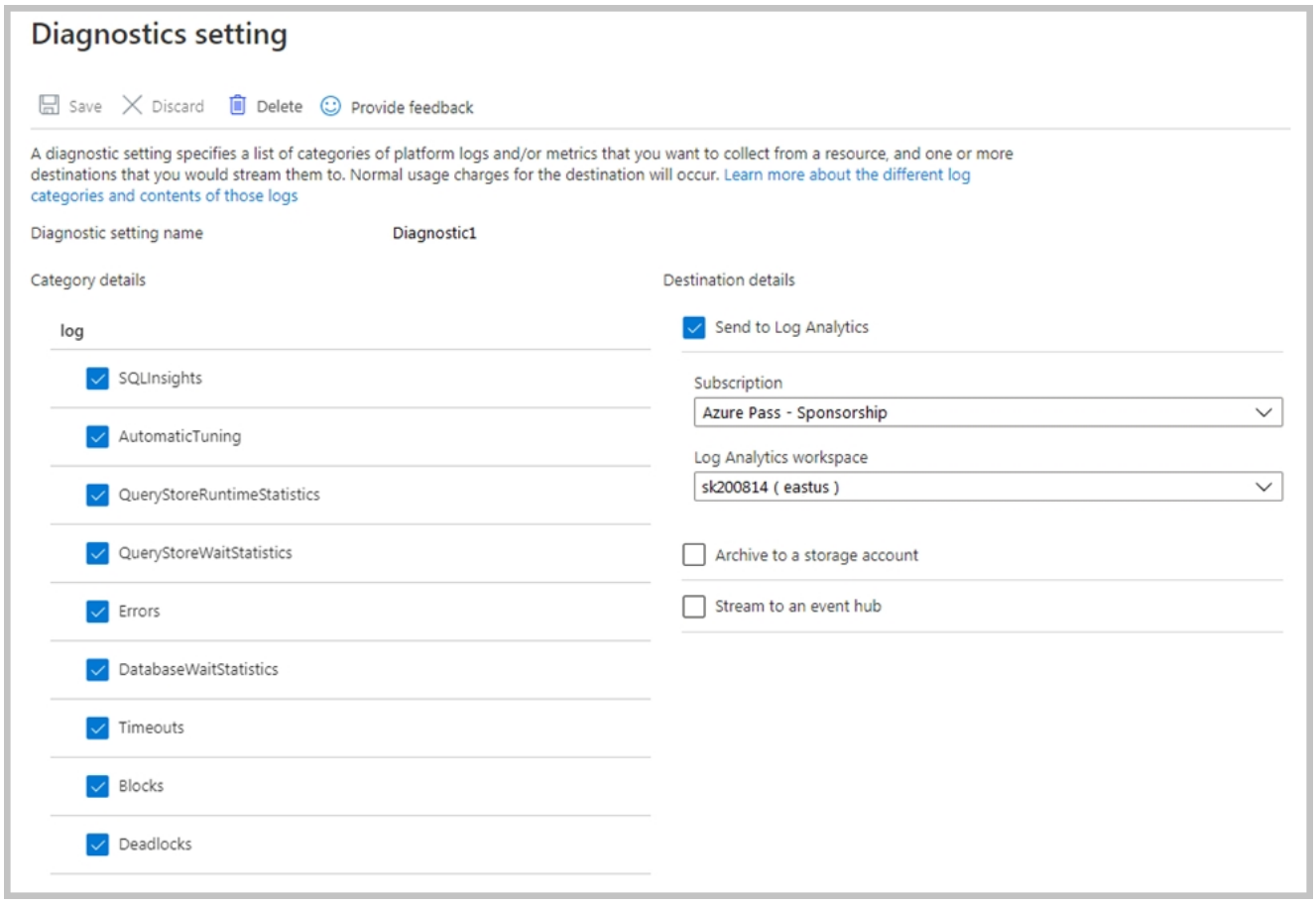
Destinations

Platform logs and metrics can be sent to the destinations in the following table.

Destination	Description
Log Analytics workspace	Sending logs and metrics to a Log Analytics workspace allows you to analyze them with other monitoring data collected by Azure Monitor using powerful log queries and also to leverage other Azure Monitor features such as alerts and visualizations.
Event hubs	Sending logs and metrics to Event Hubs allows you to stream data to external systems such as third-party SIEMs and other log analytics solutions.
Azure storage account	Archiving logs and metrics to an Azure storage account is useful for audit, static analysis, or backup. Compared to Azure Monitor Logs and a Log Analytics workspace, Azure storage is less expensive and logs can be kept there indefinitely.

17. Question

You configure the Diagnostics settings for an Azure SQL database as shown in the following exhibit.



Please select the answer choice that completes the following statement based on the information presented in the graphic.

To preform real-time reporting by using Microsoft Power BI, you must first _____

- A. clear Send to Log Analytics
- B. clear SQLInsights
- C. select Archive to a storage account
- D. select Stream to an event hub

Correct

You can stream Azure SQL Database and Azure SQL Managed Instance metrics and resource logs into Event Hubs by using the built-in Stream to an event hub option in the Azure portal. You also can enable the Service Bus rule ID by using diagnostics settings via PowerShell cmdlets, the Azure CLI, or the Azure Monitor REST API.

After the selected data is streamed into Event Hubs, you're one step closer to enabling advanced monitoring scenarios. Event Hubs acts as the front door for an event pipeline. After data is collected into an event hub, it can be transformed and stored by using a real-time analytics provider or a storage adapter. Event Hubs decouples the production of a stream of events from the consumption of those events. In this way, event consumers can access the events on their own schedule.

By using Event Hubs, Stream Analytics, and Power BI, you can easily transform your metrics and diagnostics data into near real-time insights on your Azure services.

Incorrect Answers:

A. clear Send to Log Analytics

No need to clear log analytics.

B. clear SQLInsights

No need to clear SQLInsights.

C. select Archive to a storage account

It is used to archive logs in Azure storage accounts for a long time.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal#stream-into-event-hubs

Stream into Event Hubs

You can stream Azure SQL Database and Azure SQL Managed Instance metrics and resource logs into Event Hubs by using the built-in **Stream to an event hub** option in the Azure portal. You also can enable the Service Bus rule ID by using diagnostics settings via PowerShell cmdlets, the Azure CLI, or the Azure Monitor REST API. Be sure that the event hub is in the same region as your database and server.

What to do with metrics and resource logs in Event Hubs

After the selected data is streamed into Event Hubs, you're one step closer to enabling advanced monitoring scenarios. Event Hubs acts as the front door for an event pipeline. After data is collected into an event hub, it can be transformed and stored by using a real-time analytics provider or a storage adapter. Event Hubs decouples the production of a stream of events from the consumption of those events. In this way, event consumers can access the events on their own schedule. For more information on Event Hubs, see:

- What are Azure Event Hubs?
- Get started with Event Hubs

You can use streamed metrics in Event Hubs to:

- **View service health by streaming hot-path data to Power BI**

  By using Event Hubs, Stream Analytics, and Power BI, you can easily transform your metrics and diagnostics data into near real-time insights on your Azure services. For an overview of how to set up an event hub, process data with Stream Analytics, and use Power BI as an output, see Stream Analytics and Power BI.

- **Stream logs to third-party logging and telemetry streams**

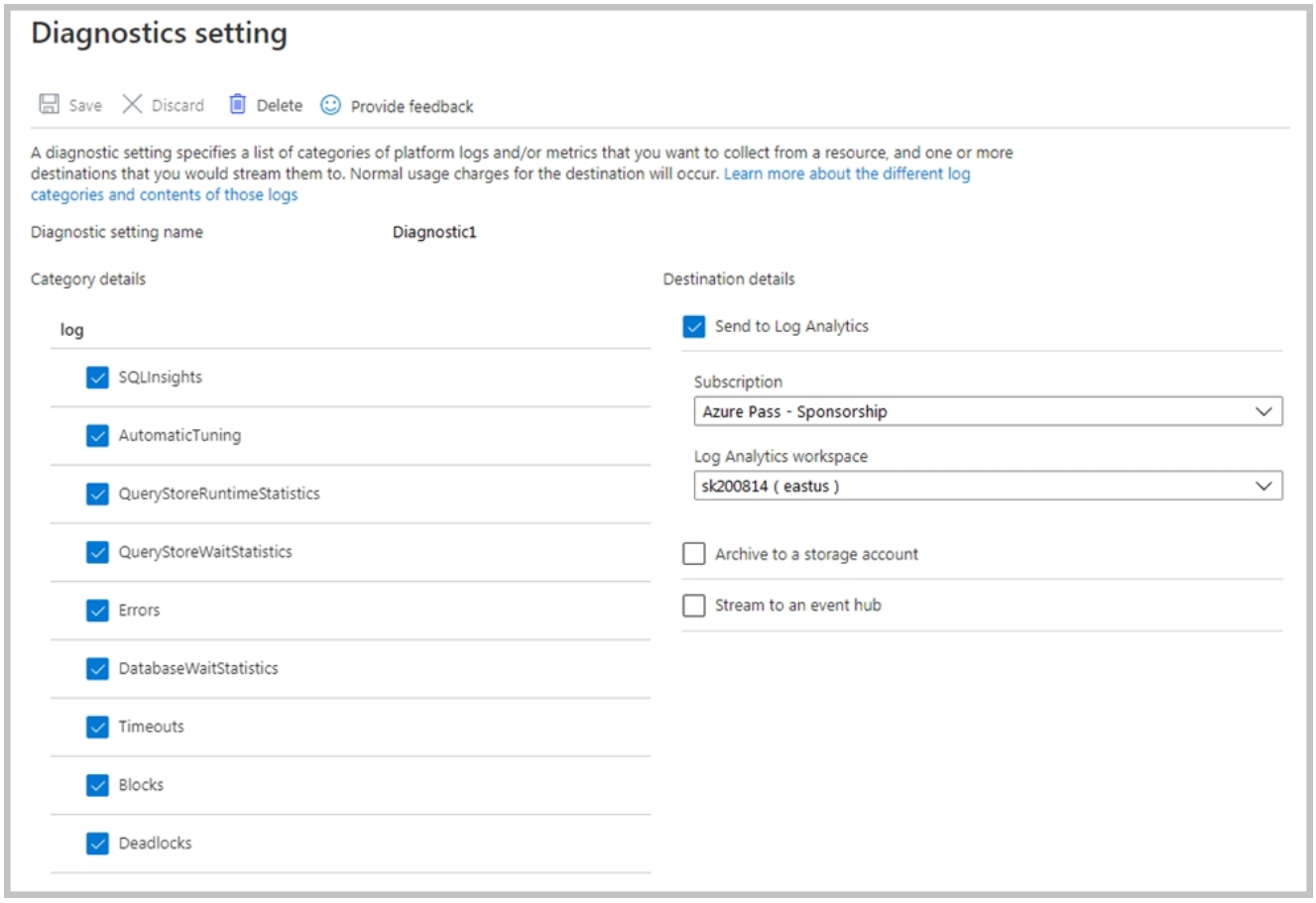
  By using Event Hubs streaming, you can get your metrics and resource logs into various third-party monitoring and log analytics solutions.

- **Build a custom telemetry and logging platform**

  Do you already have a custom-built telemetry platform or are considering building one? The highly scalable publish-subscribe nature of Event Hubs allows you to flexibly ingest metrics and resource logs. See Dan Rosanova's guide to using Event Hubs in a global-scale telemetry platform.

18. Question

You configure the Diagnostics settings for an Azure SQL database as shown in the following exhibit.



Please select the answer choice that completes the following statement based on the information presented in the graphic.

Diagnostics data can be reviewed in _____.

- A. Azure Analysis Services
- B. Azure Application Insights
- C. Azure SQL Analytics
- D. Microsoft SQL Server Analysis Services (SSAS)
- E. SQL Health Check

Incorrect

Azure SQL Analytics is an advanced cloud monitoring solution for monitoring performance of all of your Azure SQL databases at scale and across multiple subscriptions in a single view. Azure SQL Analytics collects and visualizes key performance metrics with built-in intelligence for performance troubleshooting.

By using these collected metrics, you can create custom monitoring rules and alerts. Azure SQL Analytics helps you to identify issues at each layer of your application stack. It uses Azure Diagnostic metrics along with Azure Monitor views to present data about all your Azure SQL databases in a single Log Analytics workspace. Azure Monitor helps you to collect, correlate, and visualize structured and unstructured data.

Incorrect Answers:

A. Azure Analysis Services

Azure Analysis Services is a fully managed platform as a service (PaaS) that provides enterprise-grade data models in the cloud.

B. Azure Application Insights

Application Insights is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.

D. Microsoft SQL Server Analysis Services (SSAS)

Analysis Services is an analytical data engine (VertiPaq) used in decision support and business analytics. It provides enterprise-grade semantic data models for business reports and client applications such as Power BI, Excel, Reporting Services reports, and other data visualization tools.

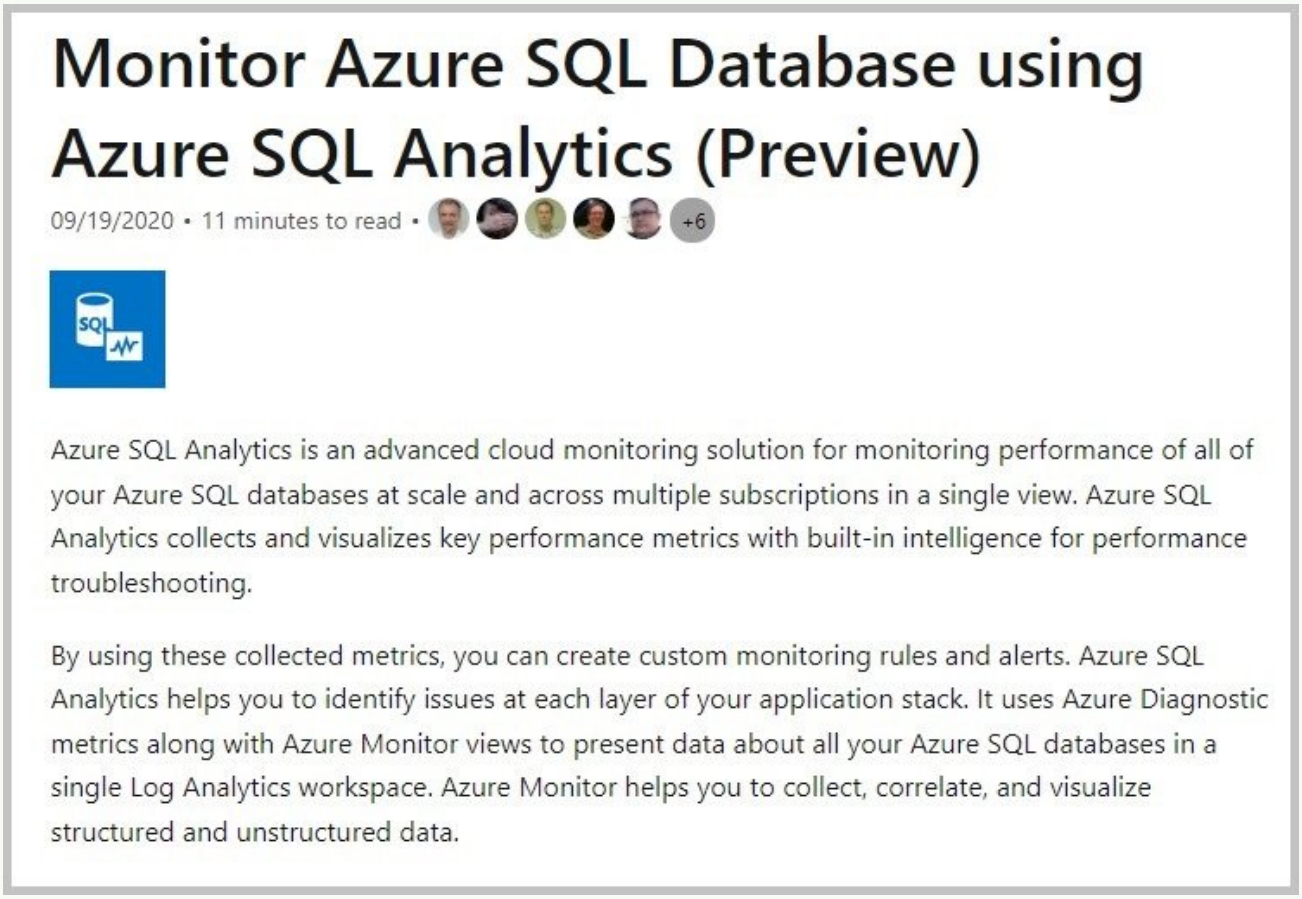
Installed as an on-premises server instance, SQL Server Analysis Services supports tabular models at all compatibility levels (depending on version), multidimensional models, data mining, and Power Pivot for SharePoint.

E. SQL Health Check

You can use the SQL Health Check solution to assess the risk and health of your server environments on a regular interval.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql



Monitor Azure SQL Database using Azure SQL Analytics (Preview)

09/19/2020 • 11 minutes to read • +6

Azure SQL Analytics is an advanced cloud monitoring solution for monitoring performance of all of your Azure SQL databases at scale and across multiple subscriptions in a single view. Azure SQL Analytics collects and visualizes key performance metrics with built-in intelligence for performance troubleshooting.

By using these collected metrics, you can create custom monitoring rules and alerts. Azure SQL Analytics helps you to identify issues at each layer of your application stack. It uses Azure Diagnostic metrics along with Azure Monitor views to present data about all your Azure SQL databases in a single Log Analytics workspace. Azure Monitor helps you to collect, correlate, and visualize structured and unstructured data.

Azure SQL Analytics options

The below table outlines supported options for two versions of the Azure SQL Analytics dashboard, one for Azure SQL Database, and the other one for Azure SQL Managed Instance databases.

Azure SQL Analytics option	Description	SQL Database support	SQL Managed Instance support
Resource by type	Perspective that counts all the resources monitored.	Yes	Yes
Insights	Provides hierarchical drill-down into Intelligent Insights into performance.	Yes	Yes
Errors	Provides hierarchical drill-down into SQL errors that happened on the databases.	Yes	Yes
Timeouts	Provides hierarchical drill-down into SQL timeouts that happened on the databases.	Yes	No
Blockings	Provides hierarchical drill-down into SQL blockings that happened on the databases.	Yes	No
Database waits	Provides hierarchical drill-down into SQL wait statistics on the database level. Includes summaries of total waiting time and the waiting time per wait type.	Yes	No
Query duration	Provides hierarchical drill-down into the query execution statistics such as query duration, CPU usage, Data IO usage, Log IO usage.	Yes	Yes
Query waits	Provides hierarchical drill-down into the query wait statistics by wait category.	Yes	Yes

19. Question

You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.

You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:

? Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.

? Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines

? Avoid storing secrets and certificates on the virtual machines.

? Minimize administrative effort for managing identities.

Which type of identity should you include in the recommendation?

- A. a service principal that is configured to use a certificate
- B. a system-assigned managed identity
- C. a service principal that is configured to use a client secret
- D. a user-assigned managed identity

Incorrect

Managed identities for Azure resources is a feature of Azure Active Directory.

User-assigned managed identity can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.

There are two types of managed identities:

System-assigned Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity an identity is created in Azure AD that is tied to the lifecycle of that service instance. So when the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Azure AD.

User-assigned You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more instances of an Azure service. In the case of user-assigned managed identities, the identity is managed separately from the resources that use it.

Incorrect Answers:

A. a service principal that is configured to use a certificate

It is used to authenticate to an application registered with Azure AD.

B. a system-assigned managed identity

System-assigned managed identity cannot be shared. It can only be associated with a single Azure resource.

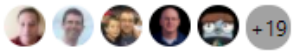
C. a service principal that is configured to use a client secret

It is used to authenticate to an application registered with Azure AD.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

What are managed identities for Azure resources?

08/26/2021 • 3 minutes to read • 

A common challenge for developers is the management of secrets and credentials used to secure communication between different components making up a solution. Managed identities eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. For example, an application may use a managed identity to access resources like Azure Key Vault where developers can store credentials in a secure manner or to access storage accounts.

Here are some of the benefits of using Managed identities:

- You don't need to manage credentials. Credentials are not even accessible to you.
- You can use managed identities to authenticate to any resource that supports Azure Active Directory authentication including your own applications.
- Managed identities can be used without any additional cost.

> ⓘ Note
>
> Managed identities for Azure resources is the new name for the service formerly known as Managed Service Identity (MSI).

Managed identity types

There are two types of managed identities:

- **System-assigned** Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity an identity is created in Azure AD that is tied to the lifecycle of that service instance. So when the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Azure AD.
- **User-assigned** You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more instances of an Azure service. In the case of user-assigned managed identities, the identity is managed separately from the resources that use it.

20. Question

You are designing a large Azure environment that will contain many subscriptions.

You plan to use Azure Policy as part of a governance solution.

To which three scopes can you assign Azure Policy definitions?

- [x] A. management groups
- [x] B. subscriptions
- [ ] C. Azure Active Directory (Azure AD) tenants
- [x] D. resource groups
- [ ] E. Azure Active Directory (Azure AD) administrative units
- [ ] F. compute resources

Correct

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.

An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to. Assignments are inherited by all child resources. This design means that a definition applied to a resource group is also applied to resources in that resource group. However, you can exclude a subscope from the assignment.

For example, at the subscription scope, you can assign a definition that prevents the creation of networking resources. You could exclude a resource group in that subscription that is intended for networking infrastructure. You then grant access to this networking resource group to users that you trust with creating networking resources.

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/overview

What is Azure Policy?

07/27/2021 • 11 minutes to read • +4

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

All Azure Policy data and objects are encrypted at rest. For more information, see Azure data encryption at rest.

Assignments

An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term *scope* refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to. Assignments are inherited by all child resources. This design means that a definition applied to a resource group is also applied to resources in that resource group. However, you can exclude a subscope from the assignment.

For example, at the subscription scope, you can assign a definition that prevents the creation of networking resources. You could exclude a resource group in that subscription that is intended for networking infrastructure. You then grant access to this networking resource group to users that you trust with creating networking resources.

In another example, you might want to assign a resource type allowlist definition at the management group level. Then you assign a more permissive policy (allowing more resource types) on a child management group or even directly on subscriptions. However, this example wouldn't work because Azure Policy is an explicit deny system. Instead, you need to exclude the child management group or subscription from the management group-level assignment. Then, assign the more permissive definition on the child management group or subscription level. If any assignment results in a resource getting denied, then the only way to allow the resource is to modify the denying assignment.

21. Question

You are designing a microservices architecture that will be hosted in an Azure Kubernetes Service (AKS) cluster. Apps that will consume the microservices will be hosted on Azure virtual machines. The virtual machines and the AKS cluster will reside on the same virtual network.

You need to design a solution to expose the microservices to the consumer apps. The solution must meet the following requirements:

? Ingress access to the microservices must be restricted to a single private IP address and protected by using mutual TLS authentication.

? The number of incoming microservice calls must be rate-limited.

? Costs must be minimized.

What should you include in the solution?

- A. Azure App Gateway with Azure Web Application Firewall (WAF)
- B. Azure API Management Premium tier with virtual network connection
- C. Azure API Management Standard tier with a service endpoint
- D. Azure Front Door with Azure Web Application Firewall (WAF)

Incorrect

One option is to deploy APIM (API Management) inside the cluster VNet.

The AKS cluster and the applications that consume the microservices might reside within the same VNet, hence there is no reason to expose the cluster publicly as all API traffic will remain within the VNet. For these scenarios, you can deploy API Management into the cluster VNet. API Management Premium tier supports VNet deployment.

Incorrect Answers:

A. Azure App Gateway with Azure Web Application Firewall (WAF)

App Gateway does not support rate limiting.

C. Azure API Management Standard tier with a service endpoint

The AKS cluster and the applications that consume the microservices might reside within the same VNet. API Management Premium tier supports VNet deployment and rate limiting.

D. Azure Front Door with Azure Web Application Firewall (WAF)

Azure Front Door is a load balancing solution. It provides a range of traffic-routing methods and backend health monitoring options to suit different application needs and automatic failover scenarios.

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes

Use Azure API Management with microservices deployed in Azure Kubernetes Service

12/14/2019 • 7 minutes to read •

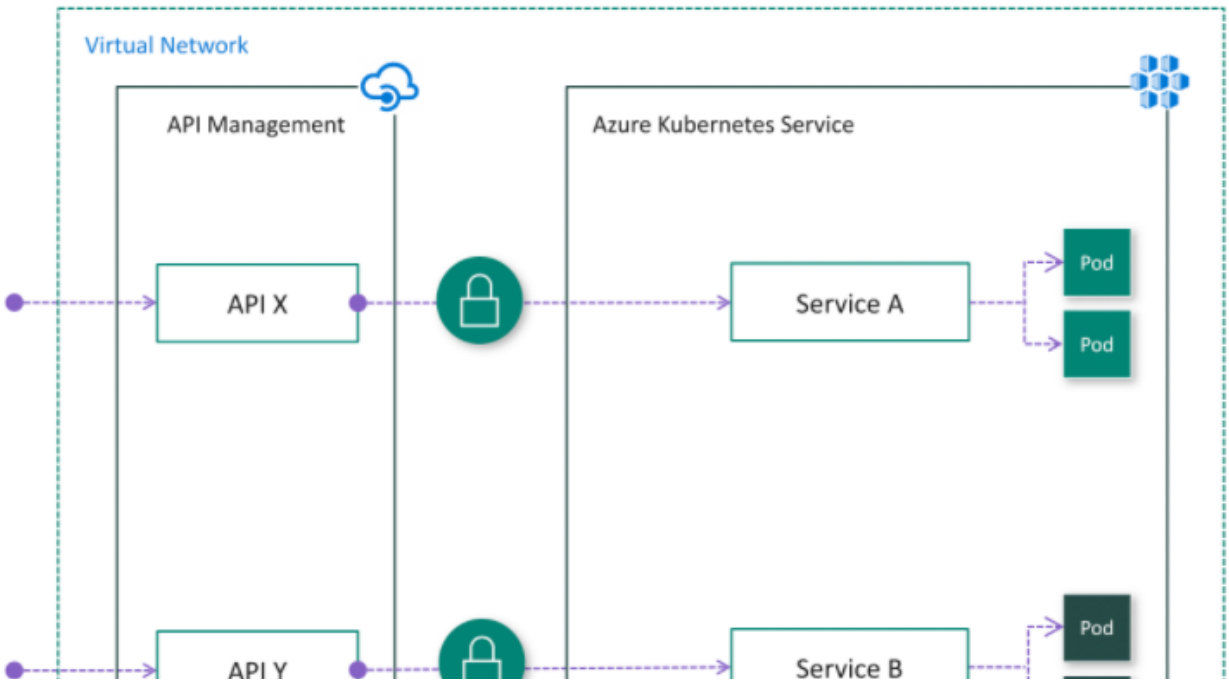
Microservices are perfect for building APIs. With Azure Kubernetes Service (AKS), you can quickly deploy and operate a microservices-based architecture in the cloud. You can then leverage Azure API Management (API Management) to publish your microservices as APIs for internal and external consumption. This article describes the options of deploying API Management with AKS. It assumes basic knowledge of Kubernetes, API Management, and Azure networking.

Option 3: Deploy APIM inside the cluster VNet

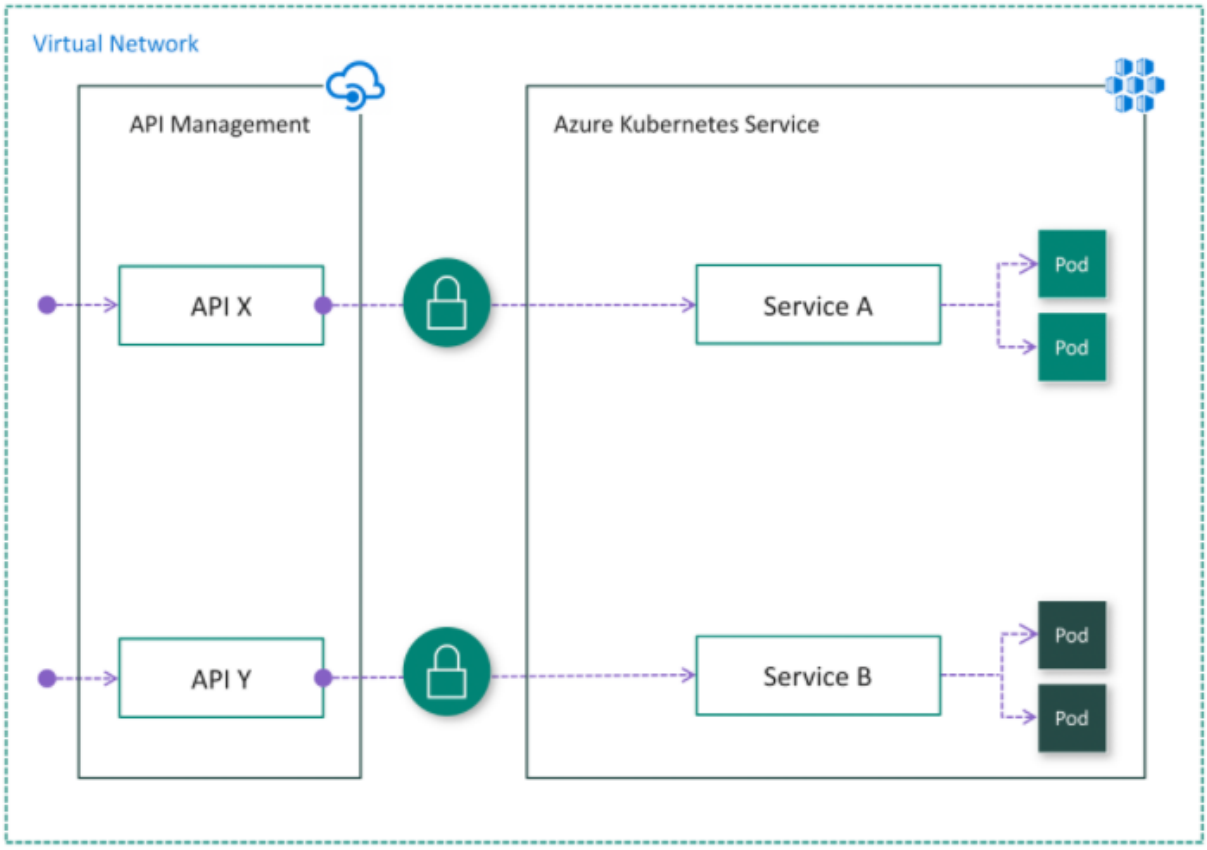
In some cases, customers with regulatory constraints or strict security requirements may find Option 1 and 2 not viable solutions due to publicly exposed endpoints. In others, the AKS cluster and the applications that consume the microservices might reside within the same VNet, hence there is no reason to expose the cluster publicly as all API traffic will remain within the VNet. For these scenarios, you can deploy API Management into the cluster VNet. API Management Developer and Premium tiers support VNet deployment.

There are two modes of deploying API Management into a VNet – External and Internal.

If API consumers do not reside in the cluster VNet, the External mode (Fig. 4) should be used. In this mode, the API Management gateway is injected into the cluster VNet but accessible from public internet via an external load balancer. It helps to hide the cluster completely while still allowing external clients to consume the microservices. Additionally, you can use Azure networking capabilities such as Network Security Groups (NSG) to restrict network traffic.



If all API consumers reside within the cluster VNet, then the Internal mode (Fig. 5) could be used. In this mode, the API Management gateway is injected into the cluster VNET and accessible only from within this VNet via an internal load balancer. There is no way to reach the API Management gateway or the AKS cluster from public internet.



In both cases, the AKS cluster is not publicly visible. Compared to Option 2, the Ingress Controller may not be necessary. Depending on your scenario and configuration, authentication might still be required between API Management and your microservices. For instance, if a Service Mesh is adopted, it always requires mutual TLS authentication.

22. Question

A company named Techzen Ltd., has a single-domain Active Directory forest named techzen-az304.com. Techzen is preparing to migrate all workloads to Azure. Techzen wants users to use single sign-on (SSO) when they access cloud-based services that integrate with Azure Active Directory (Azure AD).

You need to identify any objects in Active Directory that will fail to synchronize to Azure AD due to formatting issues. The solution must minimize costs.

What should you include in the solution?

- A. Azure AD Connect Health

B. Microsoft Office 365 IdFix

C. Azure Advisor

D. Password Export Server version 3.1 (PES v3.1) in Active Directory Migration Tool (ADMT)

Correct

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

Incorrect Answers:

A. Azure AD Connect Health

Azure Active Directory (Azure AD) Connect Health provides robust monitoring of your on-premises identity infrastructure. It enables you to maintain a reliable connection to Microsoft 365 and Microsoft Online Services.

C. Azure Advisor

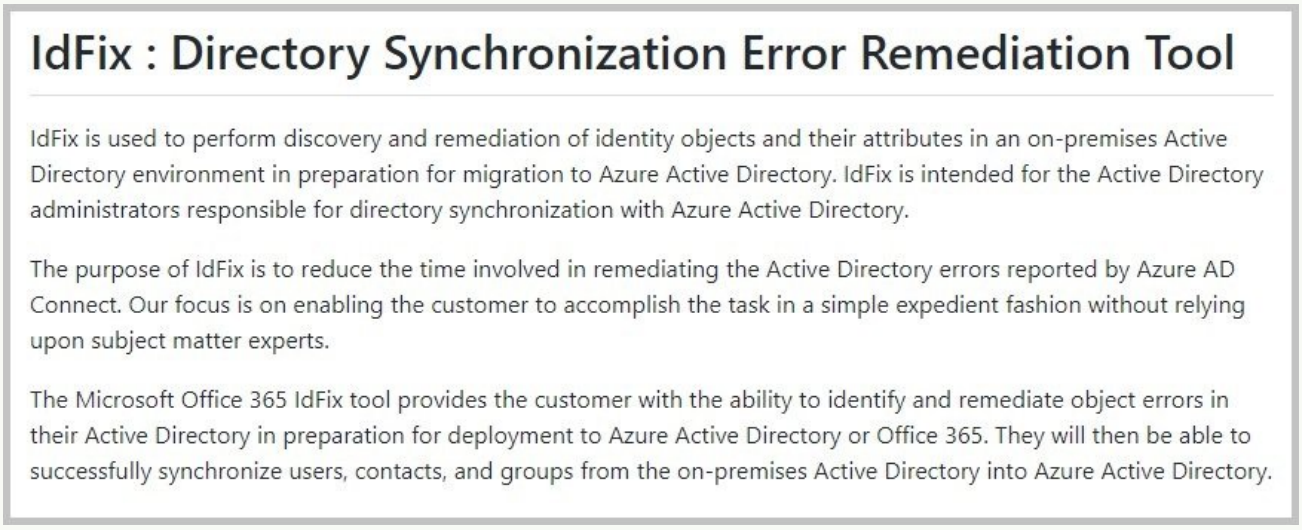
Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, Reliability (formerly called High availability), and security of your Azure resources.

D. Password Export Server version 3.1 (PES v3.1) in Active Directory Migration Tool (ADMT)

The Password Export Server version 3.1 (PES v3.1), x64 package, enables password migrations during account migrations in an Active Directory Domain Services infrastructure.

Reference:

https://github.com/Microsoft/idfix



IdFix : Directory Synchronization Error Remediation Tool

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

The purpose of IdFix is to reduce the time involved in remediating the Active Directory errors reported by Azure AD Connect. Our focus is on enabling the customer to accomplish the task in a simple expedient fashion without relying upon subject matter experts.

The Microsoft Office 365 IdFix tool provides the customer with the ability to identify and remediate object errors in their Active Directory in preparation for deployment to Azure Active Directory or Office 365. They will then be able to successfully synchronize users, contacts, and groups from the on-premises Active Directory into Azure Active Directory.

23. Question

You have an Azure subscription. The subscription has a blob container that contains multiple blobs.

Ten users in the finance department of your company plan to access the blobs during the month of April.

You need to recommend a solution to enable access to the blobs during the month of April only.

Which security solution should you include in the recommendation?

- A. access keys
- B. conditional access policies
- C. certificates
- **D. shared access signatures (SAS)**

Correct

A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:

? What resources the client may access.

? What permissions they have to those resources.

? How long the SAS is valid.

Incorrect Answers:

A. access keys

When you create a storage account, Azure generates two 512-bit storage account access keys. These keys can be used to authorize access to data in your storage account via Shared Key authorization. Rotate your keys if you believe they may have been compromised.

B. conditional access policies

Conditional Access in Azure Active Directory (Azure AD) controls access to cloud apps based on specific conditions that you specify. To allow access, you create Conditional Access policies that allow or block access based on whether or not the requirements in the policy are met.

C. certificates

Certificate based authentication cannot provide temporary access.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

Grant limited access to Azure Storage resources using shared access signatures (SAS)

12/28/2020 • 12 minutes to read • +3

A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:

- What resources the client may access.
- What permissions they have to those resources.
- How long the SAS is valid.

Types of shared access signatures

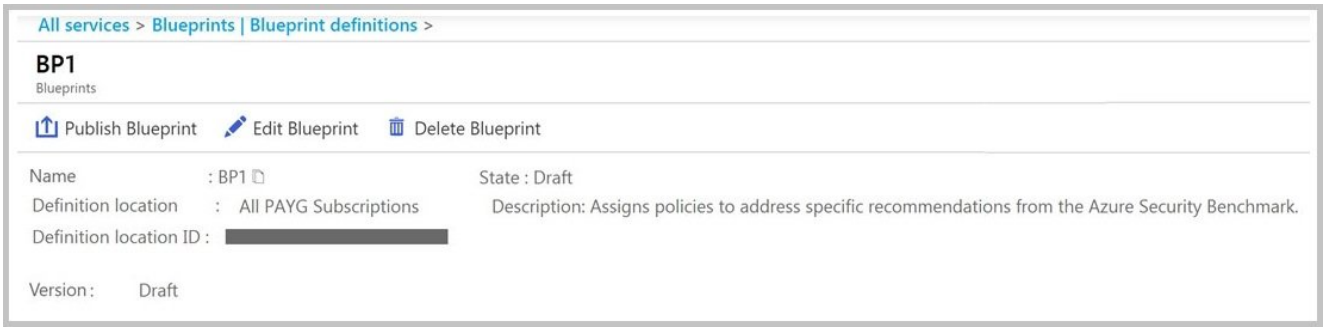
Azure Storage supports three types of shared access signatures:

- User delegation SAS
- Service SAS
- Account SAS

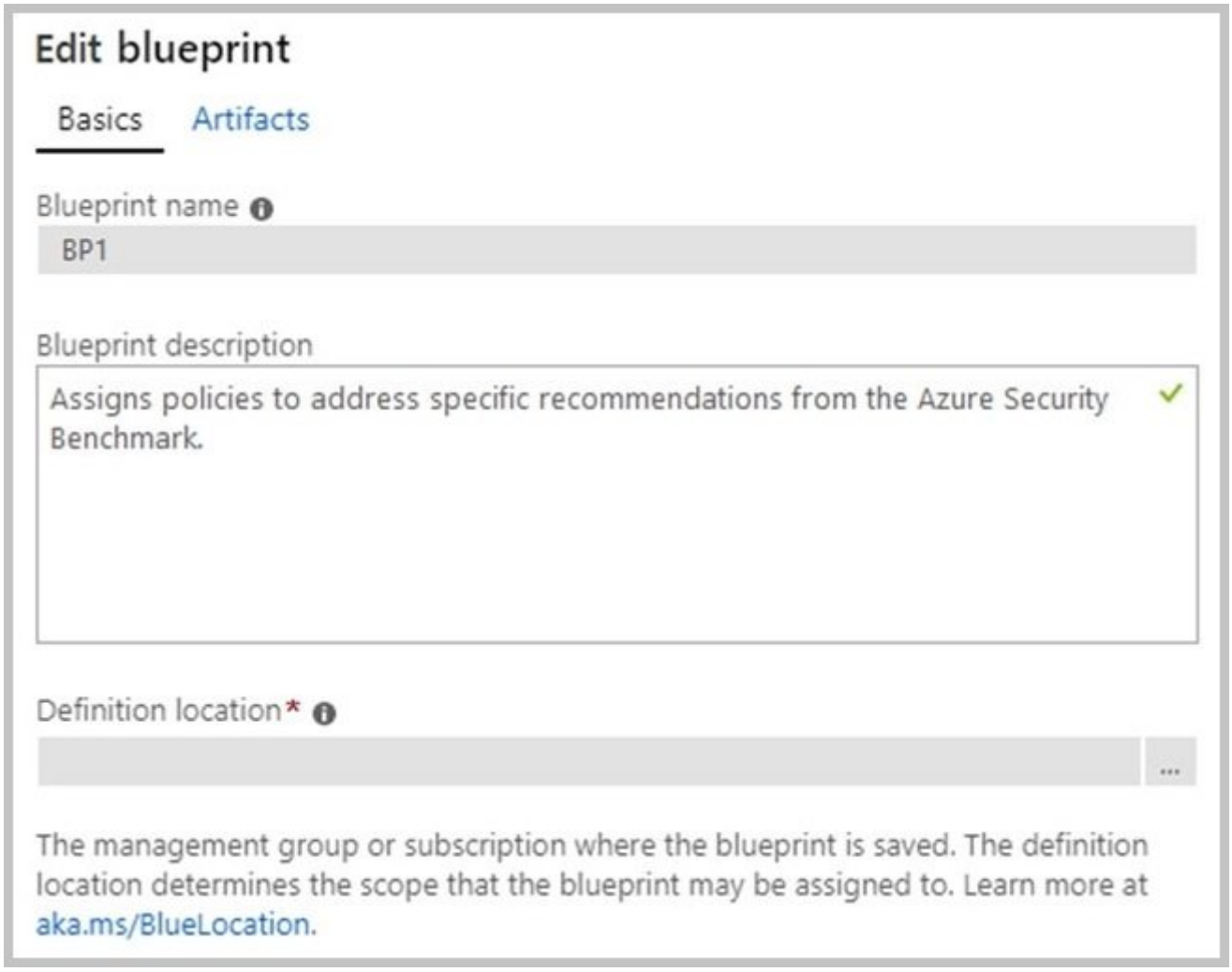
24. Question

You have an Azure blueprint named BP1.

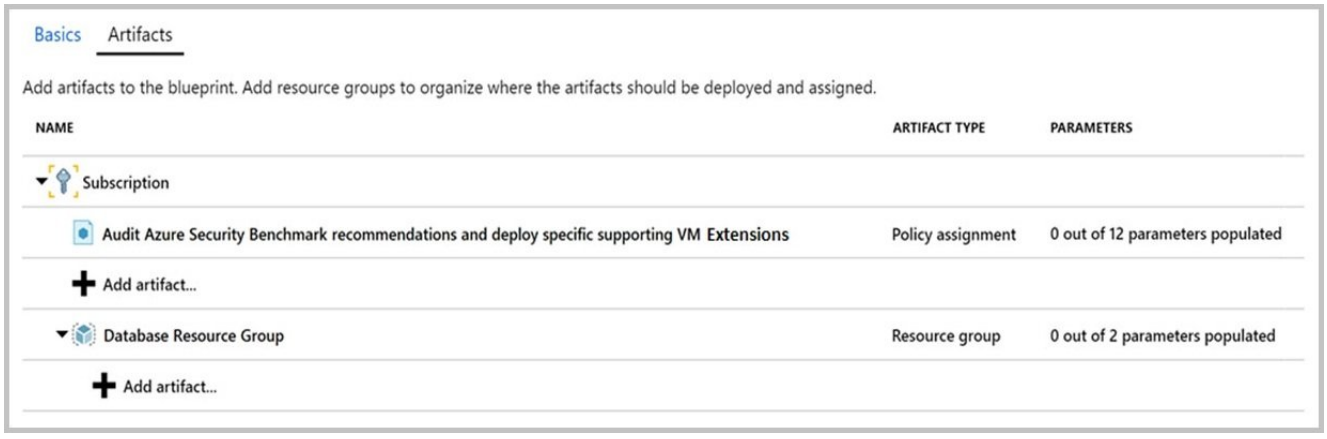
The properties of BP1 are shown in the Properties exhibit



The basic configuration of the blueprint is shown in the Basics exhibit.



The artifacts attached to BP1 are shown in the Artifacts exhibit.



For the following statements, select Yes if the statement is true. Otherwise, select No.

You can assign BP1 in its current state

- A. Yes
- B. No

Correct

BP1 is in draft mode.

When a blueprint is first created, it's considered to be in Draft mode. When it's ready to be assigned, it needs to be Published.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal

What is Azure Blueprints?

06/21/2021 • 8 minutes to read •

Important

Azure Blueprints is currently in PREVIEW. The **Supplemental Terms of Use for Microsoft Azure Previews** include additional legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

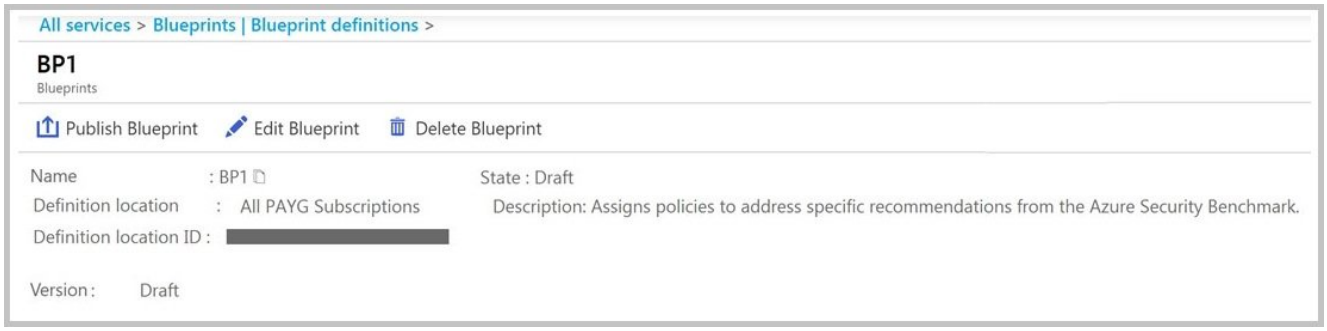
- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed Azure Cosmos DB. Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Azure Blueprints deploys your resources to.

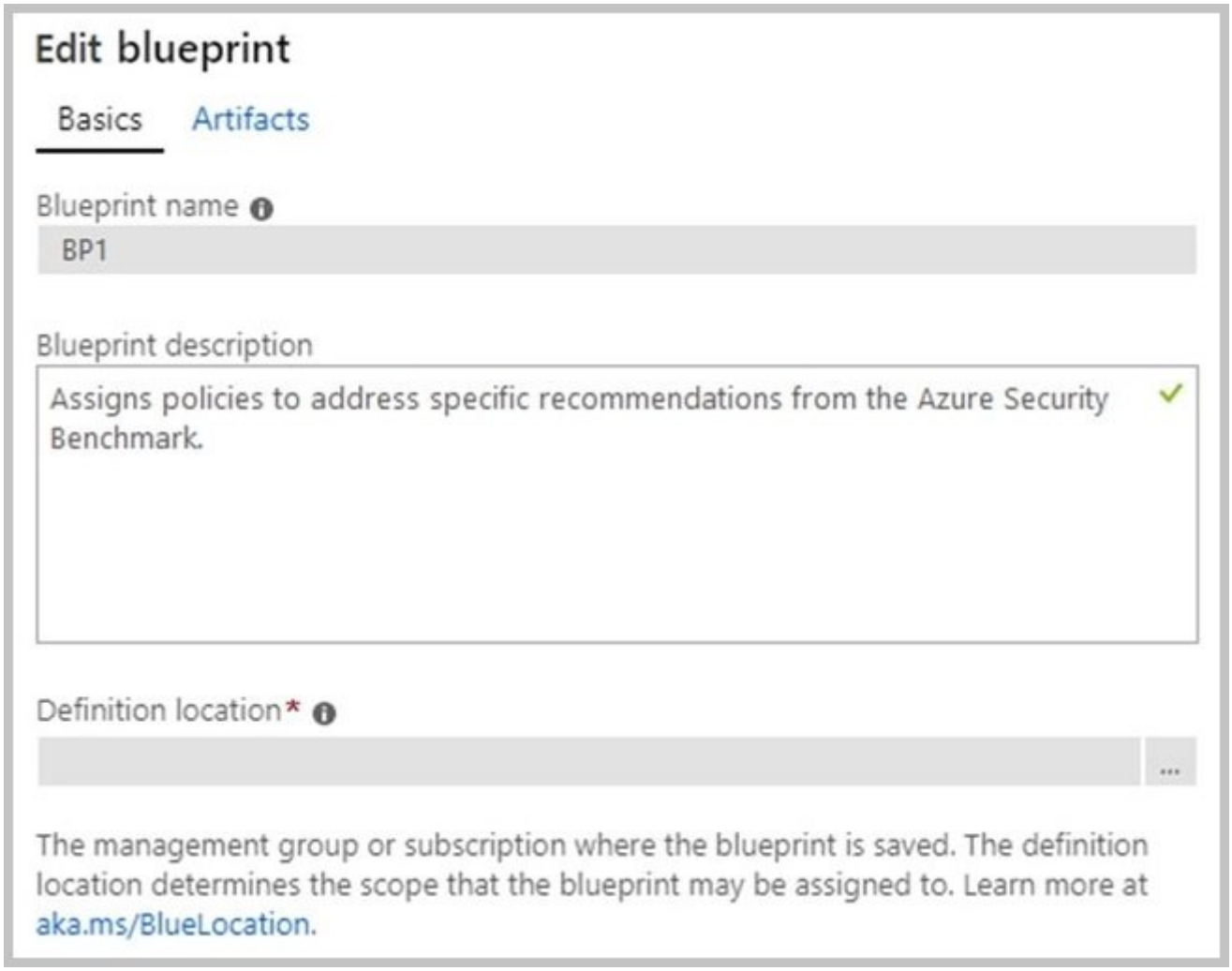
25. Question

You have an Azure blueprint named BP1.

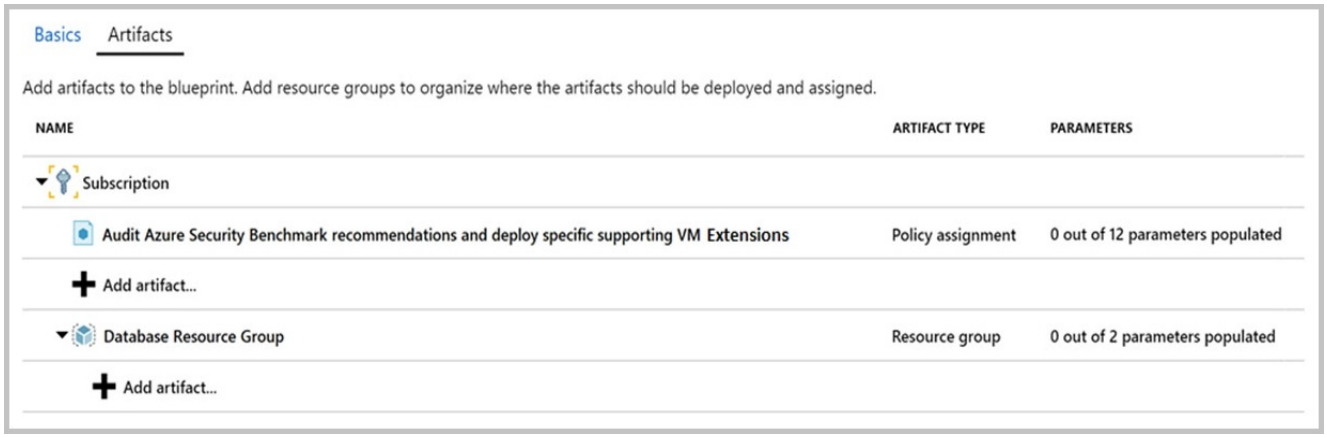
The properties of BP1 are shown in the Properties exhibit



The basic configuration of the blueprint is shown in the Basics exhibit.



The artifacts attached to BP1 are shown in the Artifacts exhibit.



For the following statements, select Yes if the statement is true. Otherwise, select No.

BP1 has a role assignment defined

A. Yes

B. No

Correct

The BP1 artifacts include one Policy assignment and a Resource group, but no Role assignments.

Note: Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

? Role Assignments

? Policy Assignments

? Azure Resource Manager templates (ARM templates)

? Resource Groups

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal

What is Azure Blueprints?

06/21/2021 • 8 minutes to read •

Important

Azure Blueprints is currently in PREVIEW. The **Supplemental Terms of Use for Microsoft Azure Previews** include additional legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

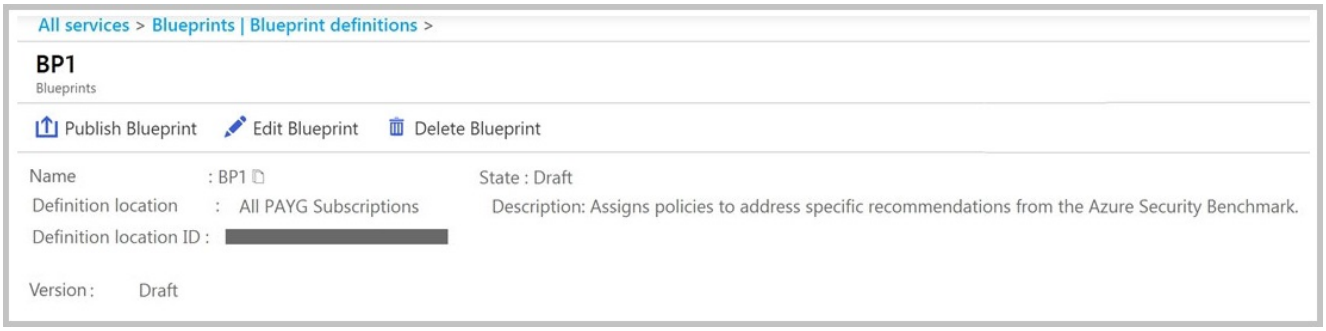
- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed Azure Cosmos DB. Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Azure Blueprints deploys your resources to.

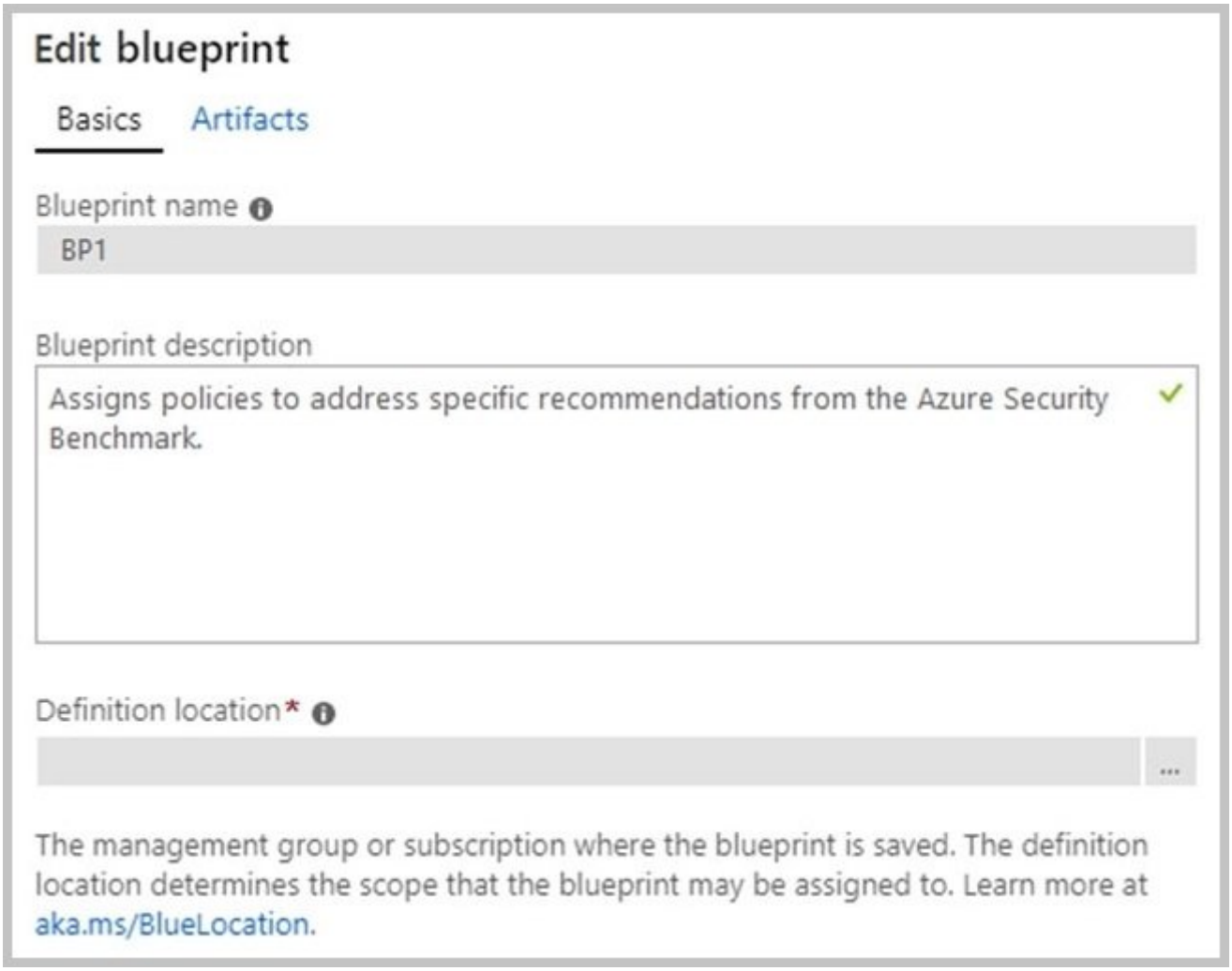
26. Question

You have an Azure blueprint named BP1.

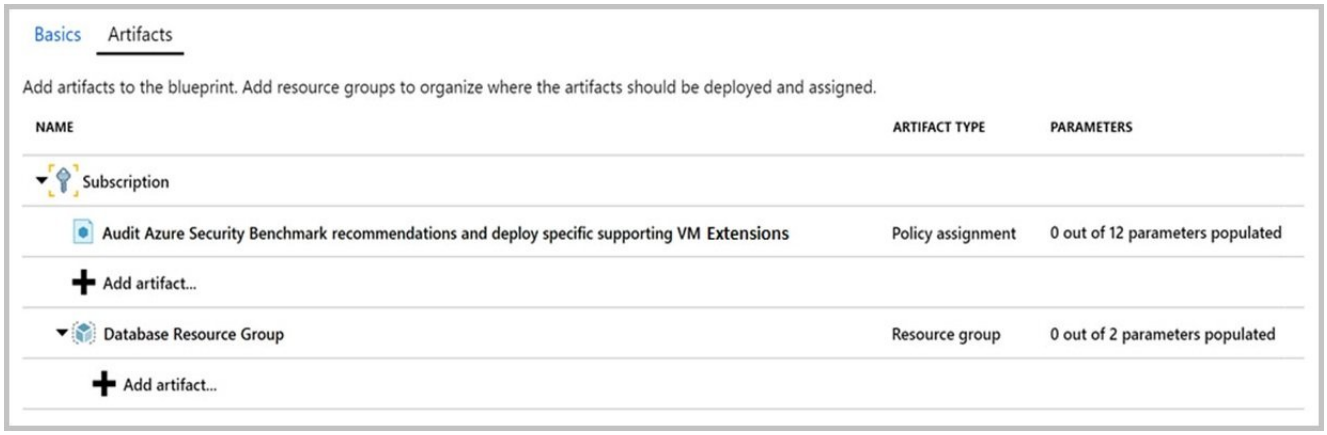
The properties of BP1 are shown in the Properties exhibit



The basic configuration of the blueprint is shown in the Basics exhibit.



The artifacts attached to BP1 are shown in the Artifacts exhibit.



For the following statements, select Yes if the statement is true. Otherwise, select No.

When BP1 is assigned, you will need to provide a resource group name

- A. Yes
- B. No

Incorrect

Yes, the BP1 artifacts include a Resource group. You must provide resource group name at the time of assignment.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal

What is Azure Blueprints?

06/21/2021 • 8 minutes to read •

ⓘ Important

Azure Blueprints is currently in PREVIEW. The **Supplemental Terms of Use for Microsoft Azure Previews** include additional legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed Azure Cosmos DB. Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Azure Blueprints deploys your resources to.

27. Question

Your company wants to use an Azure Active Directory (Azure AD) hybrid identity solution.

You need to ensure that users can authenticate if the internet connection to the on-premises Active Directory is unavailable. The solution must minimize authentication prompts for the users.

What should you include in the solution?

- A. password hash synchronization and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- B. pass-through authentication and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- C. an Active Directory Federation Services (AD FS) server

Correct

With Password hash synchronization + Seamless SSO the authentication is in the cloud.

Azure AD password hash synchronization is the simplest way to enable authentication for on-premises directory objects in Azure AD. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure.

Incorrect Answers:

B. pass-through authentication and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)

Pass-through Authentication rely on on-premises infrastructure.

C. an Active Directory Federation Services (AD FS) server

Federation rely on on-premises infrastructure.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#authentication-methods

Authentication methods

When the Azure AD hybrid identity solution is your new control plane, authentication is the foundation of cloud access. Choosing the correct authentication method is a crucial first decision in setting up an Azure AD hybrid identity solution. Implement the authentication method that is configured by using Azure AD Connect, which also provisions users in the cloud.

To choose an authentication method, you need to consider the time, existing infrastructure, complexity, and cost of implementing your choice. These factors are different for every organization and might change over time.

Cloud authentication

When you choose this authentication method, Azure AD handles users' sign-in process. Coupled with seamless single sign-on (SSO), users can sign in to cloud apps without having to reenter their credentials. With cloud authentication, you can choose from two options:

Azure AD password hash synchronization. The simplest way to enable authentication for on-premises directory objects in Azure AD. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure. Some premium features of Azure AD, like Identity Protection and Azure AD Domain Services, require password hash synchronization, no matter which authentication method you choose.

> ⓘ Note
>
> Passwords are never stored in clear text or encrypted with a reversible algorithm in Azure AD. For more information on the actual process of password hash synchronization, see **Implement password hash synchronization with Azure AD Connect sync**.

Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method. For more information on the actual pass-through authentication process, see User sign-in with Azure AD pass-through authentication.

28. Question

You need to design an Azure policy that will implement the following functionality:

? For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.

? For existing resources, identify whether the tags and values match the tags and values of the resource

group that contains the resources.

? For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values.

The solution must use the principle of least privilege.

Which of the following would go into Slot1?

- A. Append
- B. EnforceOPAConstraint
- C. EnforceRegoPolicy
- D. Modify

Incorrect

Modify is used to add, update, or remove properties or tags on a resource during creation or update. A common example is updating tags on resources such as costCenter. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations.

Incorrect Answers:

A. Append

Append is used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.

BC: The following effects are deprecated: EnforceOPAConstraint, EnforceRegoPolicy

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#modify

Modify

Modify is used to add, update, or remove properties or tags on a subscription or resource during creation or update. A common example is updating tags on resources such as costCenter. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations.

The following operations are supported by Modify:

- Add, replace, or remove resource tags. For tags, a Modify policy should have `mode` set to *Indexed* unless the target resource is a resource group.
- Add or replace the value of managed identity type (`identity.type`) of virtual machines and virtual machine scale sets.
- Add or replace the values of certain aliases.
  - Use `Get-AzPolicyAlias | Select-Object -ExpandProperty 'Aliases' | Where-Object { $_.DefaultMetadata.Attributes -eq 'Modifiable' }` in Azure PowerShell **4.6.0** or higher to get a list of aliases that can be used with Modify.

ⓘ Important

If you're managing tags, it's recommended to use Modify instead of Append as Modify provides additional operation types and the ability to remediate existing resources. However, Append is recommended if you aren't able to create a managed identity or Modify doesn't yet support the alias for the resource property.

29. Question

You need to design an Azure policy that will implement the following functionality:

? For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.

? For existing resources, identify whether the tags and values match the tags and values of the resource group that contains the resources.

? For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values.

The solution must use the principle of least privilege.

Which of the following would go into Slot2?

- A. A managed identity with the Contributor role
- B. A managed identity with the User Access Administrator role
- C. A service principal with the Contributor role
- D. A service principal with the User Access Administrator role

Correct

Resources that are non-compliant to a deployIfNotExists or modify policy can be put into a compliant state through Remediation. Remediation is accomplished by instructing Azure Policy to run the deployIfNotExists effect or the modify operations of the assigned policy on your existing resources and subscriptions, whether that assignment is to a management group, a subscription, a resource group, or an individual resource.

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity. If the managed identity is missing roles, an error is displayed during the assignment of the policy or an initiative.

Incorrect Answers:

B. A managed identity with the User Access Administrator role

Contributor role is required to remediate non-compliant resources.

C. A service principal with the Contributor role

Azure Policy uses a managed identity.

D. A service principal with the User Access Administrator role

Azure Policy uses a managed identity.

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

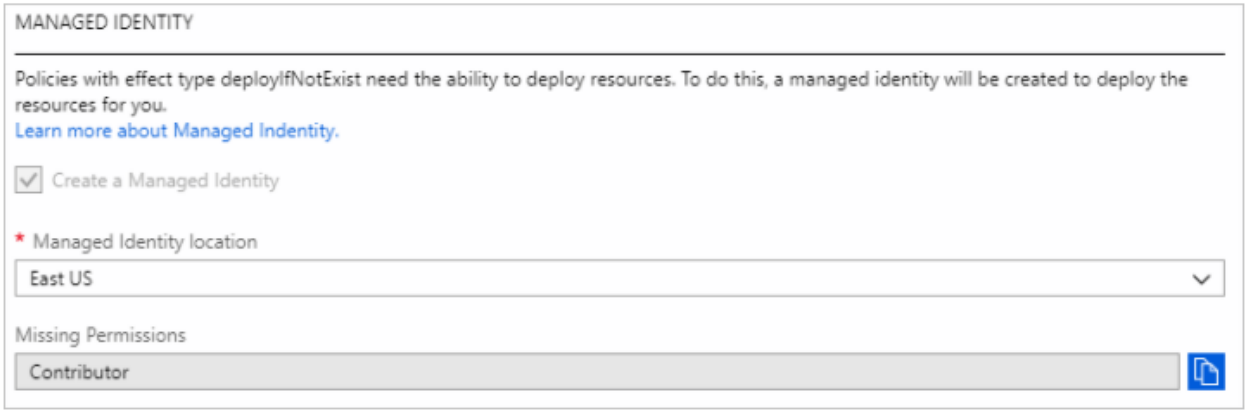
Remediate non-compliant resources with Azure Policy

08/17/2021 • 7 minutes to read •

Resources that are non-compliant to a **deployIfNotExists** or **modify** policy can be put into a compliant state through **Remediation**. Remediation is accomplished by instructing Azure Policy to run the **deployIfNotExists** effect or the **modify operations** of the assigned policy on your existing resources and subscriptions, whether that assignment is to a management group, a subscription, a resource group, or an individual resource. This article shows the steps needed to understand and accomplish remediation with Azure Policy.

How remediation security works

When Azure Policy runs the template in the **deployIfNotExists** policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity. If the managed identity is missing roles, an error is displayed during the assignment of the policy or an initiative. When using the portal, Azure Policy automatically grants the managed identity the listed roles once assignment starts. When using SDK, the roles must manually be granted to the managed identity. The *location* of the managed identity doesn't impact its operation with Azure Policy.



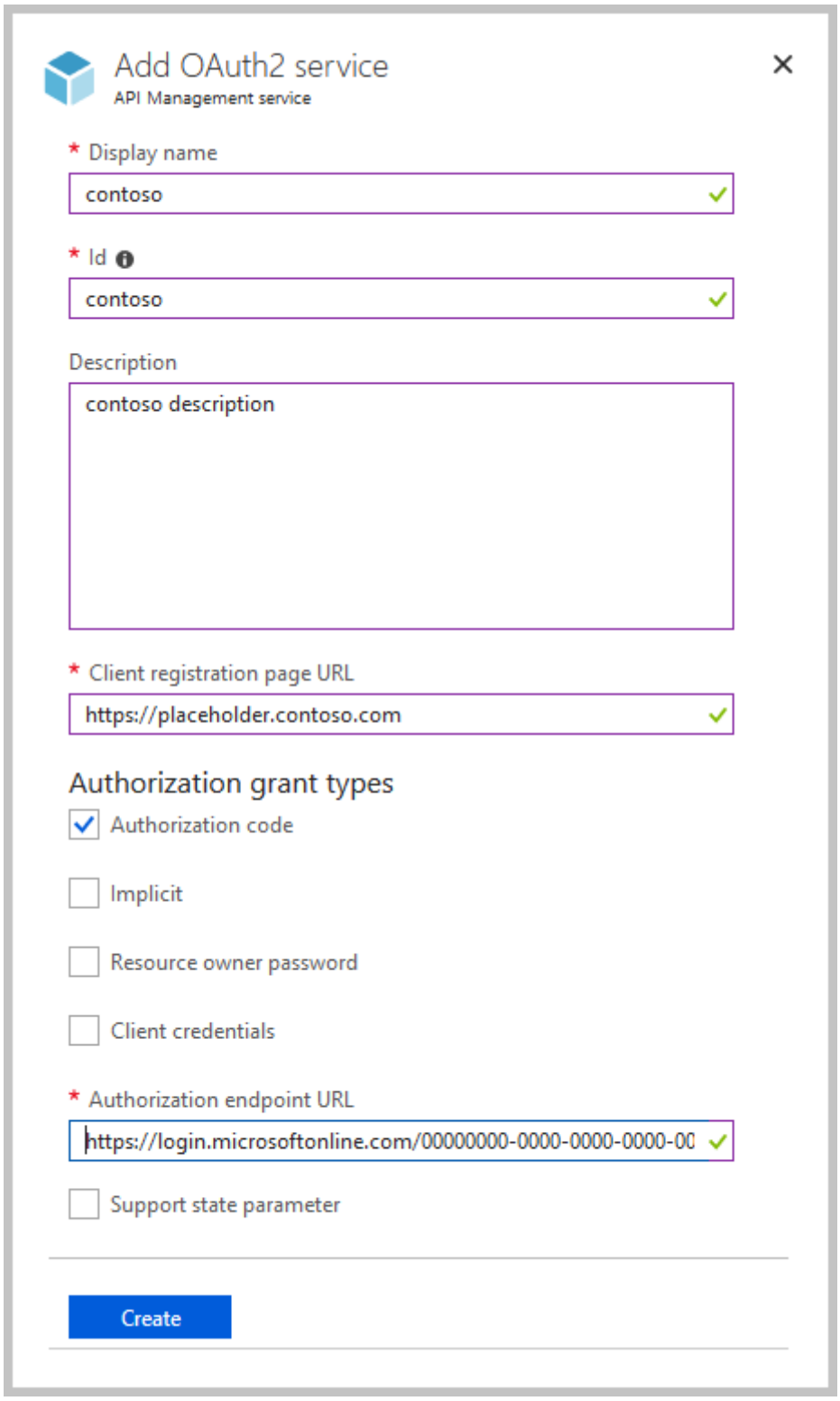
Important

In the following scenarios, the assignment's managed identity must be **manually granted access** or the remediation deployment fails:

- If the assignment is created through SDK
- If a resource modified by **deployIfNotExists** or **modify** is outside the scope of the policy assignment
- If the template accesses properties on resources outside the scope of the policy assignment

30. Question

You configure OAuth2 authorization in API Management as shown in the following exhibit.



Select the answer choice that completes the following statement based on the information presented in the graphic.

The selected authorization grant type is for _____

- A. Background services
- B. Headless device authentication

C. Web applications

Correct

The Authorization Code Grant Type is used by both web apps and native apps to get an access token after a user authorizes an app.

Note: The Authorization Code grant type is used by confidential and public clients to exchange an authorization code for an access token.

After the user returns to the client via the redirect URL, the application will get the authorization code from the URL and use it to request an access token.

Incorrect Answers:

A. Background services

Several applications run as background tasks that do not require user interaction. They run independently without needing assistance from the user interface. Background jobs start the interaction and keep taking interactive user requests. It minimizes the load that applications generally put on the user interface.

B. Headless device authentication

A headless system is a computer that operates without a monitor, graphical user interface (GUI) or peripheral devices, such as keyboard and mouse.

Headless computers are usually embedded systems in various devices or servers in multi-server data center environments. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys are among the myriad possible hosts of embedded systems.

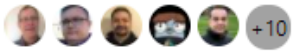
Reference:

https://developer.okta.com/blog/2018/04/10/oauth-authorization-code-grant-type

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2

https://docs.pivotal.io/p-identity/1-11/grant-types.html#client-cred-roles

How to authorize developer accounts using OAuth 2.0 in Azure API Management

08/14/2020 • 5 minutes to read • 

Many APIs support OAuth 2.0 to secure the API and ensure that only valid users have access, and they can only access resources to which they're entitled. In order to use Azure API Management's interactive Developer Console with such APIs, the service allows you to configure your service instance to work with your OAuth 2.0 enabled API.

Prerequisites

This guide shows you how to configure your API Management service instance to use OAuth 2.0 authorization for developer accounts, but does not show you how to configure an OAuth 2.0 provider. The configuration for each OAuth 2.0 provider is different, although the steps are similar, and the required pieces of information used in configuring OAuth 2.0 in your API Management service instance are the same. This topic shows examples using Azure Active Directory as an OAuth 2.0 provider.

> ⓘ Note
>
> For more information on configuring OAuth 2.0 using Azure Active Directory, see the **WebApp-GraphAPI-DotNet** sample.

Client Credentials Grant Type

This grant type is for apps that can request an access token and access resources on its own. These apps often use services that call APIs without users.

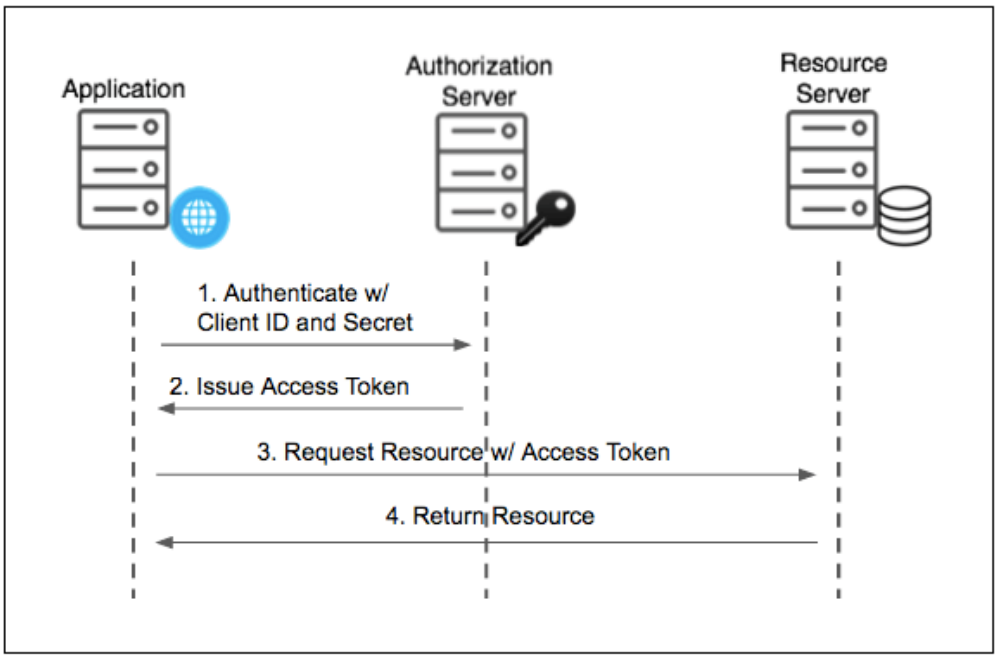
Client Credentials Grant Type Roles

The Client Credentials grant type uses the following roles:

- **Application**: A client that makes protected requests using the authorization of the resource owner.
- **Authorization Server**: The Single Sign-On server that issues access tokens to client apps after successfully authenticating the resource owner.
- **Resource Server**: The server that hosts protected resources and accepts and responds to protected resource requests using access tokens. Apps access the server through APIs.

Client Credentials Flow

The following diagram shows the flow for the Client Credentials grant type:

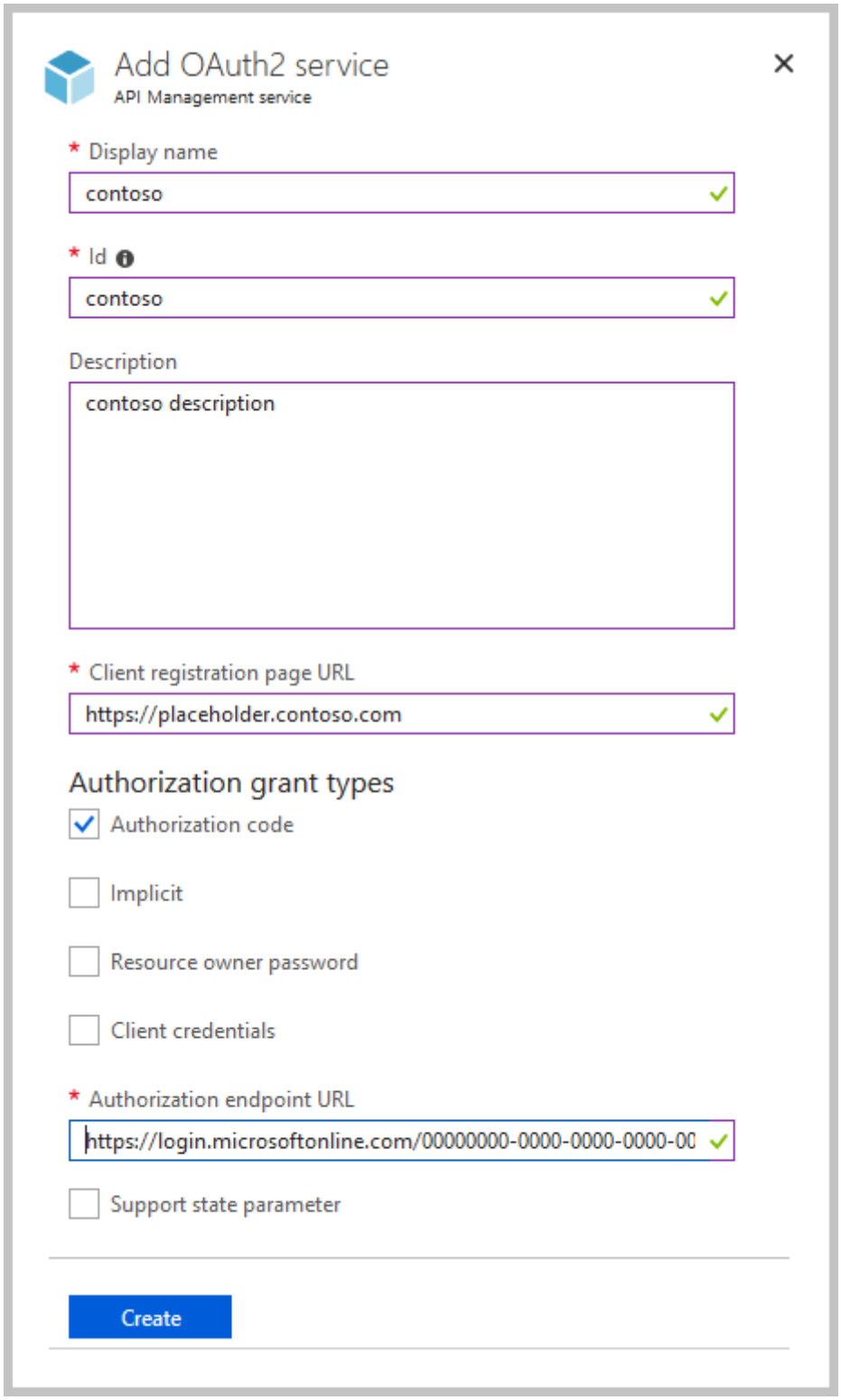


1. **Authenticate w/ Client ID and Secret**: The app authenticates with the authorization server using its client ID and client secret.
2. **Issue Access Token**: The authorization server validates the client ID and client secret and issues an access token.
3. **Request Resource w/ Access Token**: The app attempts to access the resource from the resource server by presenting the access token.
4. **Return Resource**: If the access token is valid, the resource server returns the resources to the app.

The resource server runs in Single Sign-On under a given space and org. Developers set the permissions for the resource server API endpoints. To do this, developers create resources that correspond to API endpoints secured by Single Sign-On. Administrators can create admin clients to perform automated management actions without a user. See **Create Admin Client.**

31. Question

You configure OAuth2 authorization in API Management as shown in the following exhibit.



Select the answer choice that completes the following statement based on the information presented in the graphic.

To enable custom data in the grant flow, select .....

- A. Client credentials
- B. Resource owner password
- C. Support state parameter

Correct

How to include additional client data?

In case you need to store additional details about a client that don't fit into the standard parameter set the custom data parameter comes to help:

POST /c2id/clients HTTP/1.1 –

Host: demo.c2id.com –

Content-Type: application/json –

Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

{

"redirect_uris" : ["https://myapp.example.com/callback"],

"data" : { "reg_type" : "3rd-party",

"approved" : true,

"author_id" : 792440 }

}

The data parameter permits arbitrary content packaged in a JSON object. To set it you will need the master registration token or a one-time access token with a client-reg:data scope.

Incorrect Answers:

B. Resource owner password

The resource owner password credentials grant workflow allows for the exchanging of the user name and password of a user for an access token. When using the resource owner password credentials grant, the user provides the credentials (user name and password) directly to the application.

C. Support state parameter

Authorization protocols provide a state parameter that allows you to restore the previous state of your application. The state parameter preserves some state object set by the client in the Authorization request and makes it available to the client in the response.

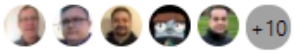
Reference:

https://connect2id.com/products/server/docs/guides/client-registration

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2

https://connect2id.com/products/server/docs/guides/client-registration#example-client-credentials-grant

How to authorize developer accounts using OAuth 2.0 in Azure API Management

08/14/2020 • 5 minutes to read • 

Many APIs support OAuth 2.0 to secure the API and ensure that only valid users have access, and they can only access resources to which they're entitled. In order to use Azure API Management's interactive Developer Console with such APIs, the service allows you to configure your service instance to work with your OAuth 2.0 enabled API.

Prerequisites

This guide shows you how to configure your API Management service instance to use OAuth 2.0 authorization for developer accounts, but does not show you how to configure an OAuth 2.0 provider. The configuration for each OAuth 2.0 provider is different, although the steps are similar, and the required pieces of information used in configuring OAuth 2.0 in your API Management service instance are the same. This topic shows examples using Azure Active Directory as an OAuth 2.0 provider.

> ⓘ Note
>
> For more information on configuring OAuth 2.0 using Azure Active Directory, see the **WebApp-GraphAPI-DotNet** sample.

4.7 How to register a client for the client credentials grant

The client credentials grant is intended for clients that act on their own behalf (the client is also the resource owner), as opposed to the general OAuth case where the client acts on behalf of an end-user. This grant type is often used in microservice and B2B service scenarios.

An initial registration token is always required.

Minimal registration request:

```
POST /clients HTTP/1.1
Host: demo.c2id.com
Content-Type: application/json
Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

{
  "grant_types" : [ "client_credentials" ]
}
```

As with the password grant client, the scope parameter can be required by the grant handler to bound the permitted access for the client:

```
POST /clients HTTP/1.1
Host: demo.c2id.com
Content-Type: application/json
Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

{
  "grant_types" : [ "client_credentials" ],
  "scope"       : "myapi:post myapi:get myapi:delete"
}
```

JWT and mutual TLS based authentication at the token endpoint is recommended for best security. Example registration for a client which is going to authenticate with a JWT signed with an EC private key using the `EC256` algorithm, the client's public key(s) for validating the JWT signature are published at an URL:

```
POST /clients HTTP/1.1
Host: demo.c2id.com
Content-Type: application/json
Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

{
  "grant_types"                    : [ "client_credentials" ],
  "token_endpoint_auth_method"     : "private_key_jwt",
  "token_endpoint_auth_signing_alg" : "EC256",
  "jwks_uri"                       : "https://client.example.com/jwks.json",
  "scope"                          : "myapi:post myapi:get myapi:delete"
}
```

32. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen,

IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

Reference:

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

What is Azure Network Watcher?

01/04/2021 • 8 minutes to read • +6

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. Network Watcher is designed to monitor and repair the network health of IaaS (Infrastructure-as-a-Service) products which includes Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc. Note: It is not intended for and will not work for PaaS monitoring or Web analytics.

Monitoring

Monitor communication between a virtual machine and an endpoint

Endpoints can be another virtual machine (VM), a fully qualified domain name (FQDN), a uniform resource identifier (URI), or IPv4 address. The *connection monitor* capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint. For example, you might have a web server VM that communicates with a database server VM. Someone in your organization may, unknown to you, apply a custom route or network security rule to the web server or database server VM or subnet.

If an endpoint becomes unreachable, connection troubleshoot informs you of the reason. Potential reasons are a DNS name resolution problem, the CPU, memory, or firewall within the operating system of a VM, or the hop type of a custom route, or security rule for the VM or subnet of the outbound connection. Learn more about security rules and route hop types in Azure.

Connection monitor also provides the minimum, average, and maximum latency observed over time. After learning the latency for a connection, you may find that you're able to decrease the latency by moving your Azure resources to different Azure regions. Learn more about determining relative latencies between Azure regions and internet service providers and how to monitor communication between a VM and an endpoint with connection monitor. If you'd rather test a connection at a point in time, rather than monitor the connection over time, like you do with connection monitor, use the connection troubleshoot capability.

Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute. Network performance monitor detects network issues like traffic blackholing, routing errors, and issues that conventional network monitoring methods aren't able to detect. The solution generates alerts and notifies you when a threshold is breached for a network link. It also ensures timely detection of network performance issues and localizes the source of the problem to a particular network segment or device. Learn more about network performance monitor.

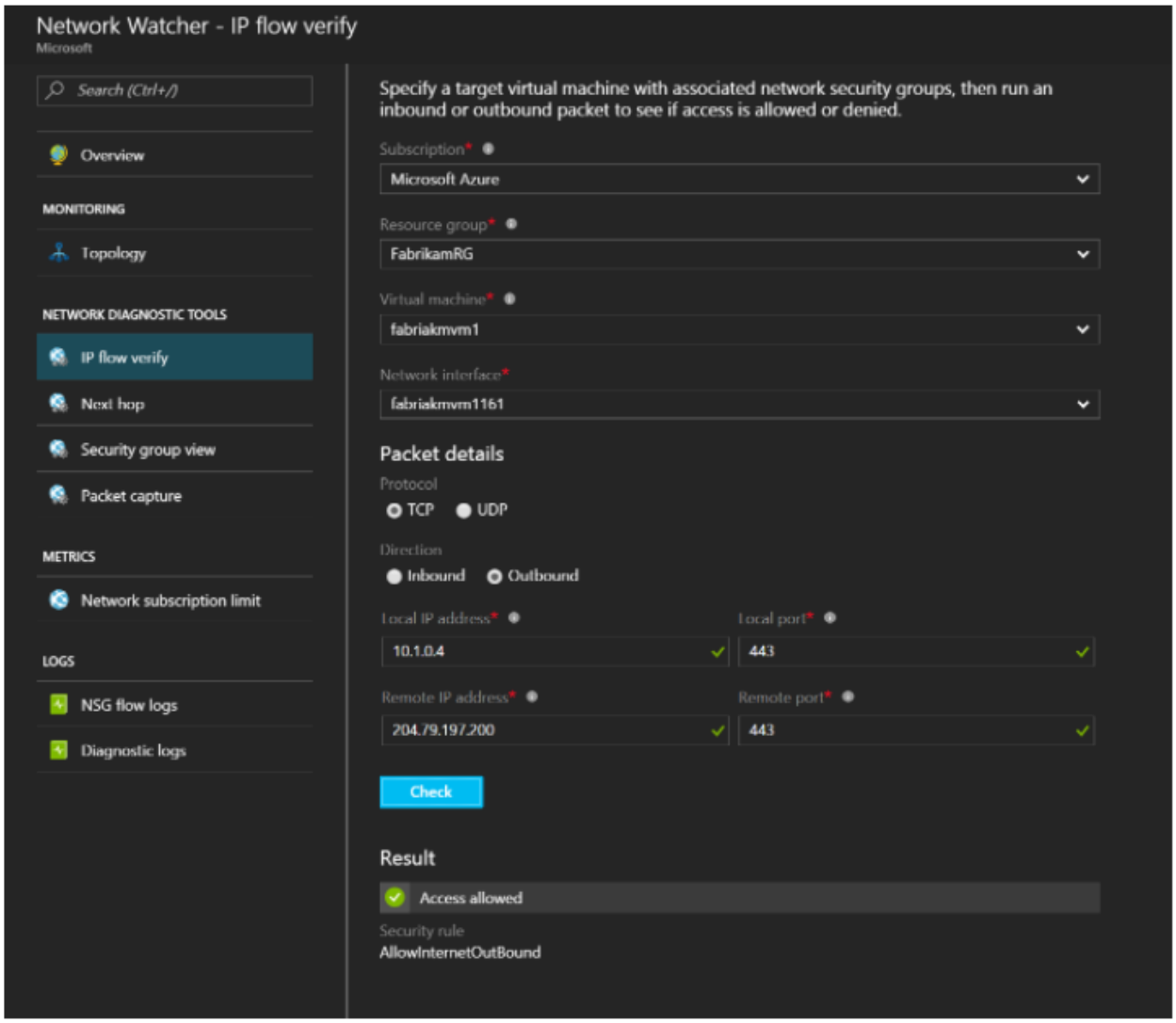
Introduction to IP flow verify in Azure Network Watcher

01/04/2021 • 2 minutes to read •

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

An instance of Network Watcher needs to be created in all regions that you plan to run IP flow verify. Network Watcher is a regional service and can only be ran against resources in the same region. The instance used does not affect the results of IP flow verify, as any route associated with the NIC or subnet is still be returned.



33. Question

You manage a network that includes an on-premises Active Directory domain and an Azure Active Directory (Azure AD).

Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider.

You need to provide guidance on the different identity providers.

How should you describe synchronized identity provider?

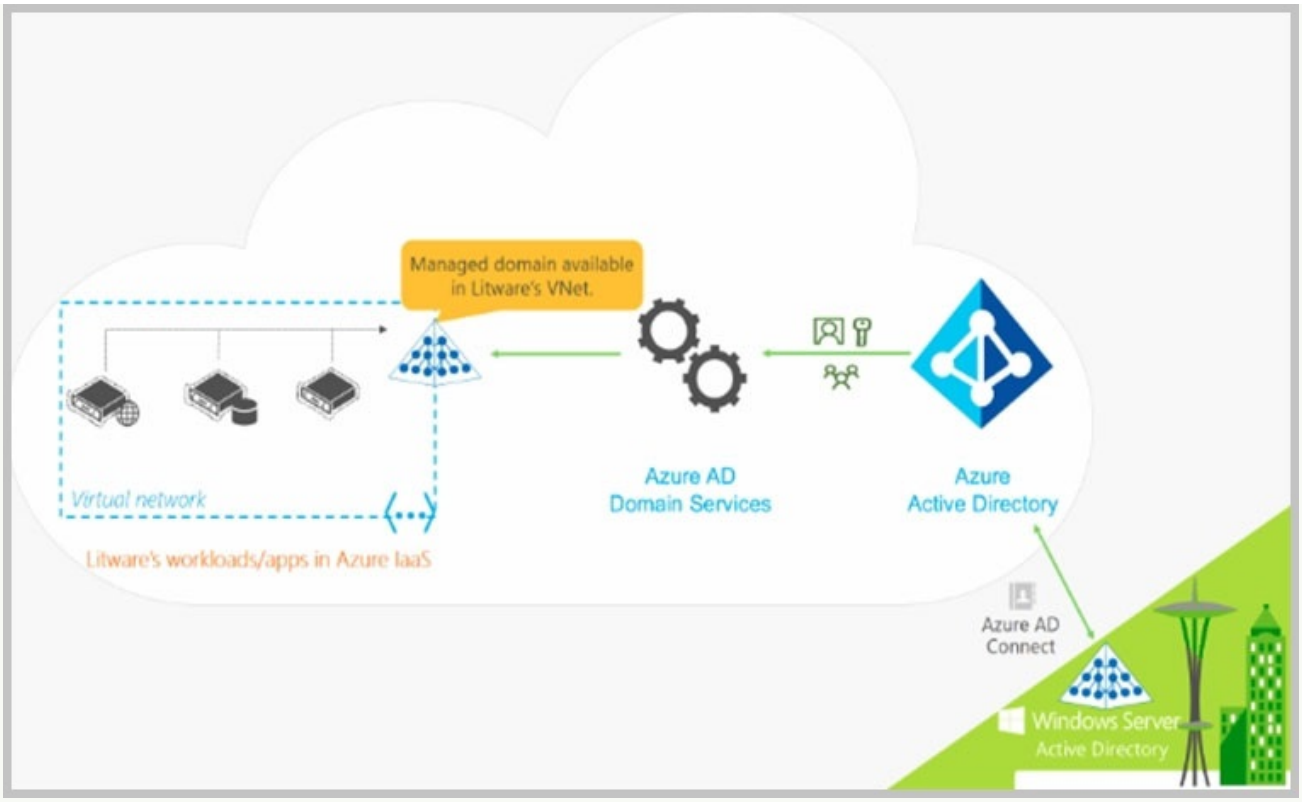
- A. User management occurs on-premises. Azure AD authenticates employees by using on-premise passwords.
- B. User management occurs on-premises. The on-premise domain controller authenticates employee credentials.
- C. Both user management and authentication occur in Azure AD

Incorrect

Azure AD Domain Services for hybrid organizations

Organizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the cloud, especially legacy directory-aware applications, Azure AD Domain Services can be useful to them.

Example: Litware Corporation has deployed Azure AD Connect, to synchronize identity information from their on-premises directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, their credential hashes for authentication (password hash sync) and group memberships.



User accounts, group memberships, and credentials from Litware's on-premises directory are synchronized to Azure AD via Azure AD Connect. These user accounts, group memberships, and credentials are automatically available within the managed domain.

Note: In a hybrid environment, objects and credentials from an on-premises AD DS domain can be synchronized to Azure AD using Azure AD Connect. Once those objects are successfully synchronized to Azure AD, the automatic background sync then makes those objects and credentials available to applications using the managed domain.

Incorrect Answers:

B. User management occurs on-premises. The on-premise domain controller authenticates employee credentials

In this model the user identity is managed in an on-premises server and the accounts and password hashes are synchronized to the cloud. The user enters the same password on-premises as they do in the cloud, and at sign-in the password is verified by Azure Active Directory

C. Both user management and authentication occur in Azure AD

User management occurs in on-premise environment.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization

How objects and credentials are synchronized in an Azure Active Directory Domain Services managed domain

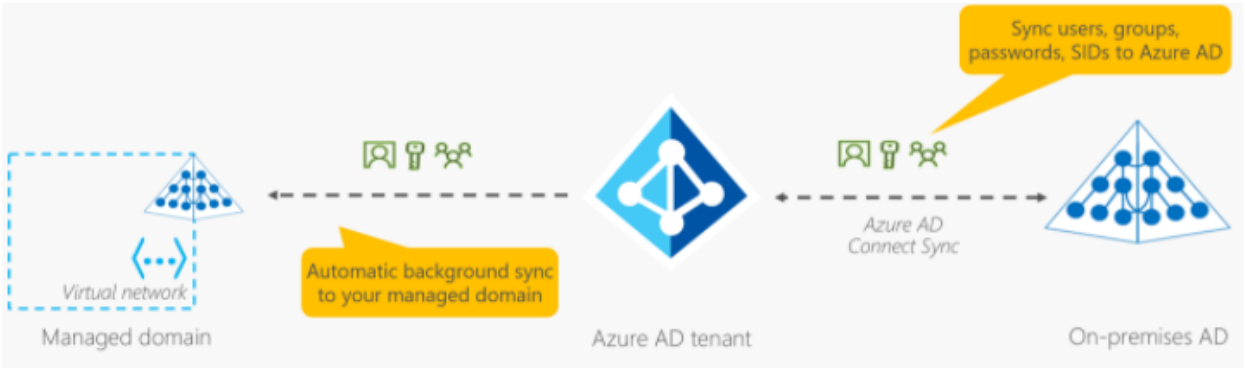
03/26/2021 • 9 minutes to read •

Objects and credentials in an Azure Active Directory Domain Services (Azure AD DS) managed domain can either be created locally within the domain, or synchronized from an Azure Active Directory (Azure AD) tenant. When you first deploy Azure AD DS, an automatic one-way synchronization is configured and started to replicate the objects from Azure AD. This one-way synchronization continues to run in the background to keep the Azure AD DS managed domain up-to-date with any changes from Azure AD. No synchronization occurs from Azure AD DS back to Azure AD.

In a hybrid environment, objects and credentials from an on-premises AD DS domain can be synchronized to Azure AD using Azure AD Connect. Once those objects are successfully synchronized to Azure AD, the automatic background sync then makes those objects and credentials available to applications using the managed domain.

If on-prem AD DS and Azure AD are configured for federated authentication using ADFS then there is no (current/valid) password hash available in Azure DS. Azure AD user accounts created before fed auth was implemented might have an old password hash but this likely doesn't match a hash of their on-prem password. Hence Azure AD DS won't be able to validate the users credentials.

The following diagram illustrates how synchronization works between Azure AD DS, Azure AD, and an optional on-premises AD DS environment:



34. Question

You manage a network that includes an on-premises Active Directory domain and an Azure Active Directory (Azure AD).

Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider.

You need to provide guidance on the different identity providers.

How should you describe federated identity provider?

- A. User management occurs on-premises. Azure AD authenticates employees by using on-premise passwords.
- **B. User management occurs on-premises. The on-premise domain controller authenticates employee credentials.**
- C. Both user management and authentication occur in Azure AD

Correct

Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. This method allows administrators to implement more rigorous levels of access control. Federation with AD FS and PingFederate is available.

Incorrect Answers:

A. User management occurs on-premises. Azure AD authenticates employees by using on-premise passwords.

In federated environment, authentication occurs in on-premise domain controllers.

C. Both user management and authentication occur in Azure AD

Both user management and authentication occurs in on-premise domain controllers.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview

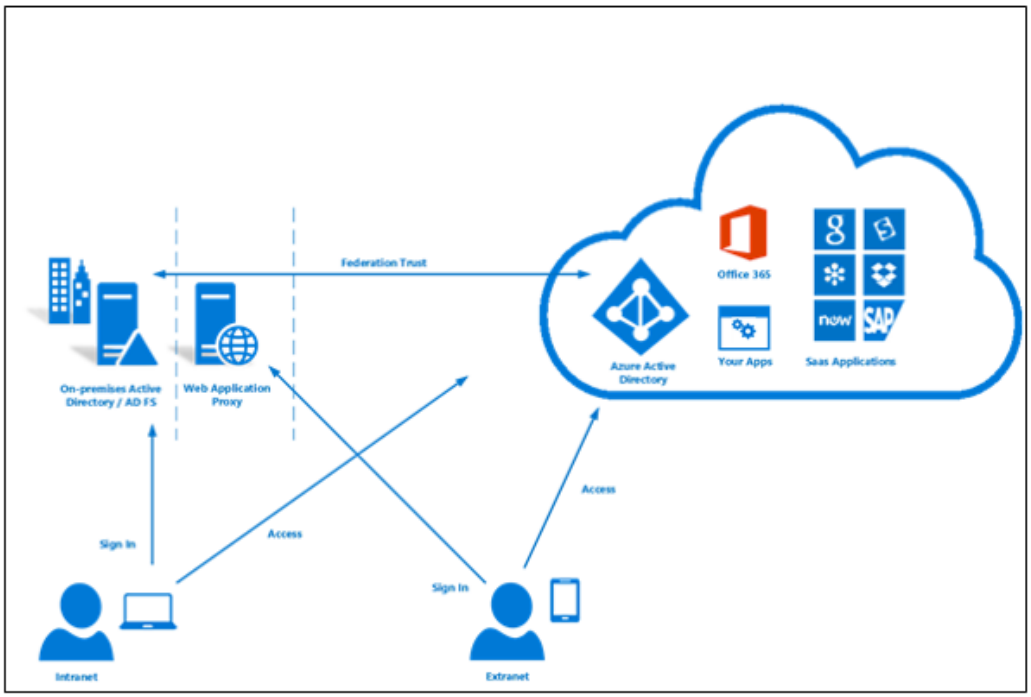
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

What is federation with Azure AD?

11/28/2018 • 2 minutes to read •

Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. This method allows administrators to implement more rigorous levels of access control. Federation with AD FS and PingFederate is available.



Tip

If you decide to use Federation with Active Directory Federation Services (AD FS), you can optionally set up password hash synchronization as a backup in case your AD FS infrastructure fails.

35. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You have an Azure Active Directory (Azure AD) tenant named pass-az304.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT

work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Create an Access Review for Group1.

Does this solution meet the goal?

- A. Yes
- B. No

Correct

Instead configure conditional access policies in Azure Active Directory.

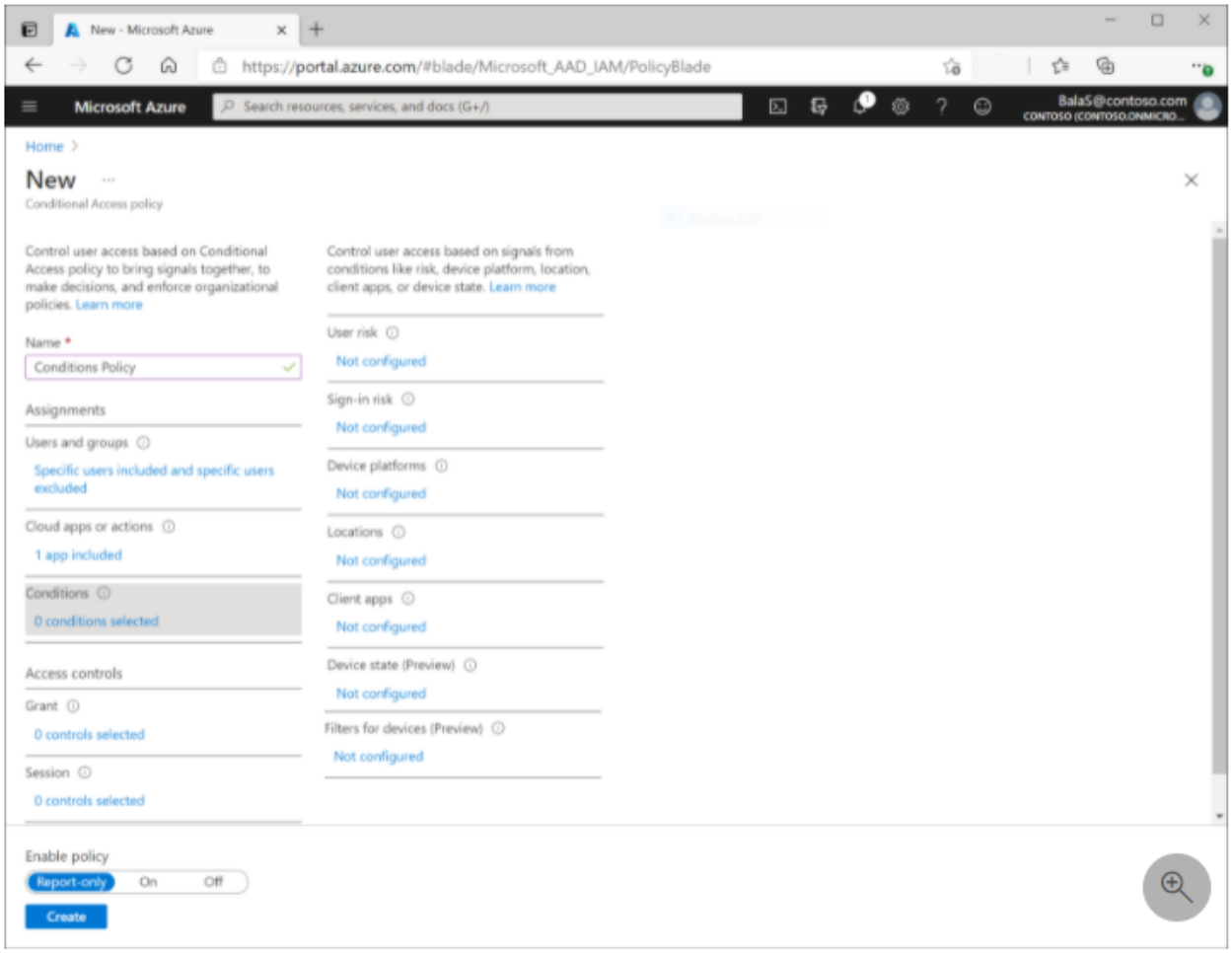
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#sign-in-risk

Conditional Access: Conditions

09/13/2021 • 10 minutes to read •

Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.



Multiple conditions can be combined to create fine-grained and specific Conditional Access policies.

For example, when accessing a sensitive application an administrator may factor sign-in risk information from Identity Protection and location into their access decision in addition to other controls like multi-factor authentication.

Sign-in risk

For customers with access to Identity Protection, sign-in risk can be evaluated as part of a Conditional Access policy. Sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. More information about sign-in risk can be found in the articles, What is risk and How To: Configure and enable risk policies.

36. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more

than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You have an Azure Active Directory (Azure AD) tenant named pass-az304.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Implement Azure AD Identity Protection for Group1.

Does this solution meet the goal?

- A. Yes
- B. No

Incorrect

Instead configure conditional access policies in Azure Active Directory.

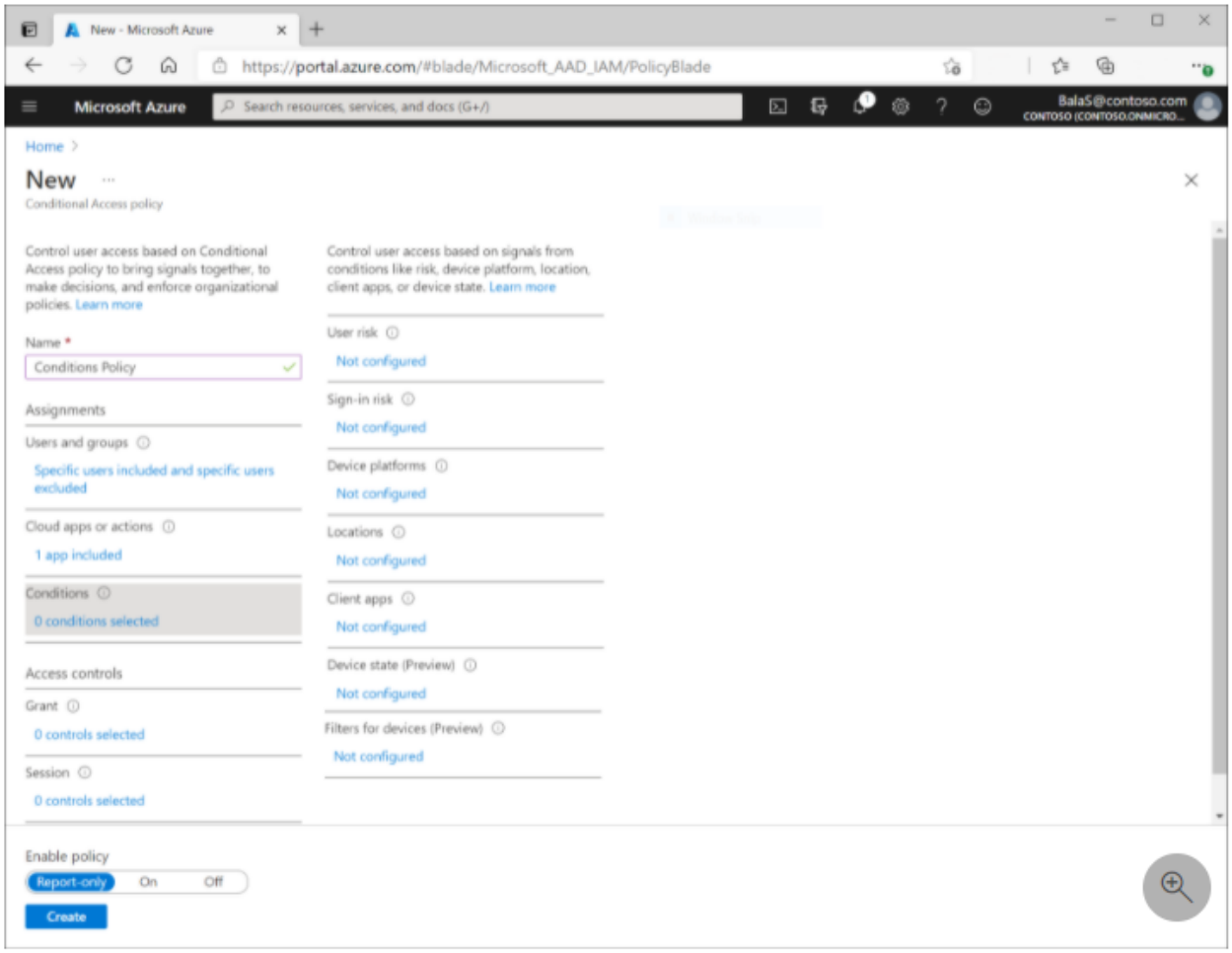
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#sign-in-risk

Conditional Access: Conditions

09/13/2021 • 10 minutes to read •

Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.



Multiple conditions can be combined to create fine-grained and specific Conditional Access policies.

For example, when accessing a sensitive application an administrator may factor sign-in risk information from Identity Protection and location into their access decision in addition to other controls like multi-factor authentication.

Sign-in risk

For customers with access to Identity Protection, sign-in risk can be evaluated as part of a Conditional Access policy. Sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. More information about sign-in risk can be found in the articles, What is risk and How To: Configure and enable risk policies.

37. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more

than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You have an Azure Active Directory (Azure AD) tenant named pass-az304.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: You implement an access package.

Does this solution meet the goal?

- A. Yes
- B. No

Correct

Instead configure conditional access policies in Azure Active Directory.

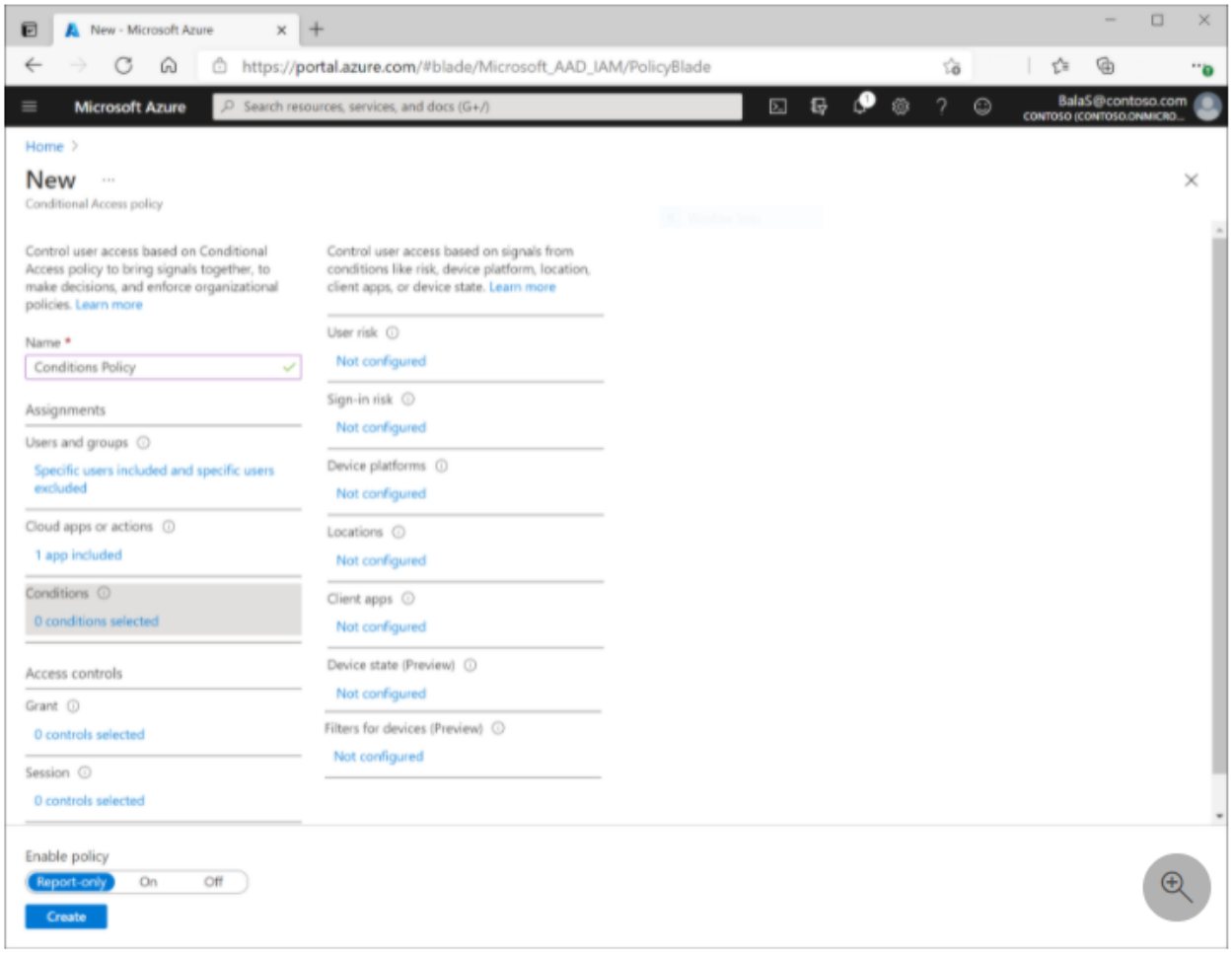
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#sign-in-risk

Conditional Access: Conditions

09/13/2021 • 10 minutes to read •

Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.



Multiple conditions can be combined to create fine-grained and specific Conditional Access policies.

For example, when accessing a sensitive application an administrator may factor sign-in risk information from Identity Protection and location into their access decision in addition to other controls like multi-factor authentication.

Sign-in risk

For customers with access to Identity Protection, sign-in risk can be evaluated as part of a Conditional Access policy. Sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. More information about sign-in risk can be found in the articles, What is risk and How To: Configure and enable risk policies.

38. Question

Your company has the divisions shown in the following table.

Division	Azure Subscription	Azure Active Directory (Azure AD) Tenant
East	Sub1, Sub2	east.pass-az304.com
West	Sub3, Sub4	west.pass-az-304.com

You plan to deploy a custom application to each subscription. The application will contain the following:

? A resource group

? An Azure web app

? Custom role assignments

? An Azure Cosmos DB account

You need to use Azure Blueprints to deploy the application to each subscription.

What is the minimum number of management groups required to deploy the application?

- 1
- 2
- 3
- 4

Correct

One management group for East, and one for West.

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

You need 2 Management Groups as there is to AAD involved.

Note: Each Azure AD tenant is given a single top-level management group called the root management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This group allows global policies and Azure role assignments to be applied at the directory level.

Note: Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. All subscriptions within a single management group must trust the same Azure Active Directory tenant.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/security-center/security-center-management-groups

https://docs.microsoft.com/en-us/azure/governance/management-groups/overview

What is Azure Blueprints?

06/21/2021 • 8 minutes to read • 

> ⓘ **Important**
>
> Azure Blueprints is currently in PREVIEW. The **Supplemental Terms of Use for Microsoft Azure Previews** include additional legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed Azure Cosmos DB. Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Azure Blueprints deploys your resources to.

What are Azure management groups?

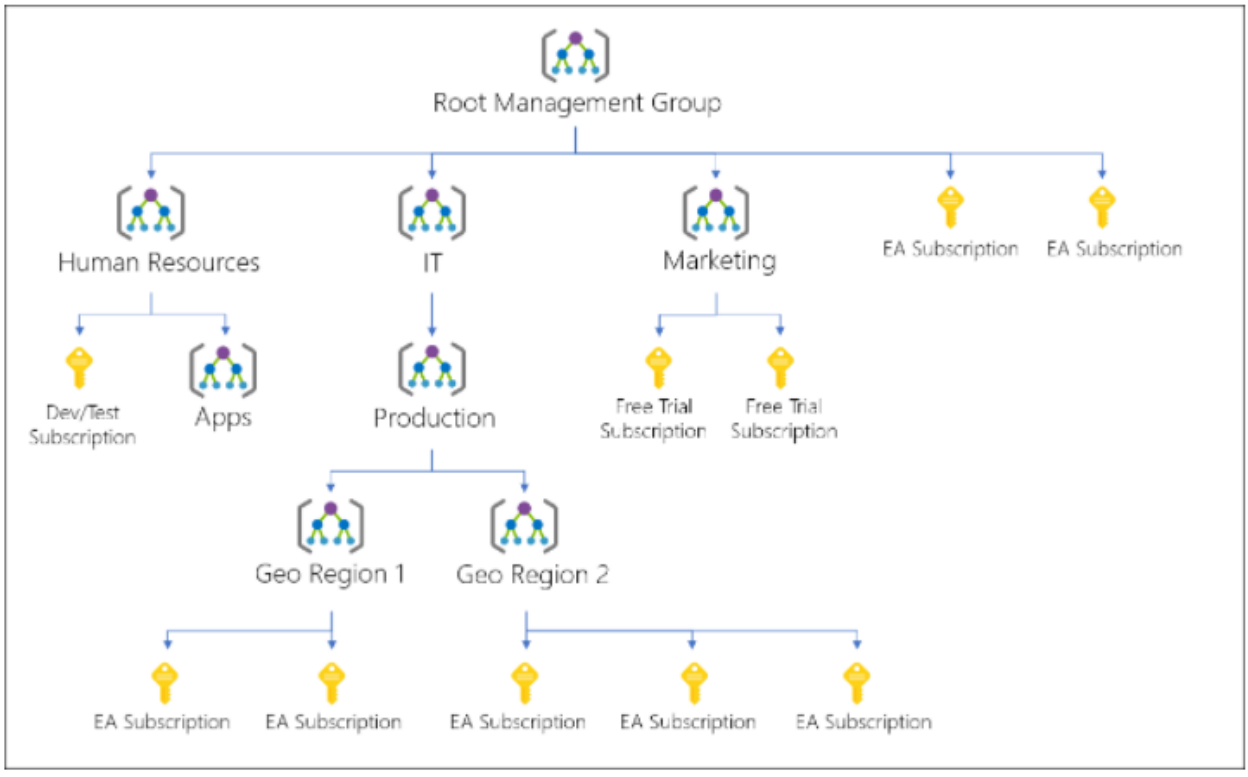
08/17/2021 • 12 minutes to read • +7

If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. All subscriptions within a single management group must trust the same Azure Active Directory tenant.

For example, you can apply policies to a management group that limits the regions available for virtual machine (VM) creation. This policy would be applied to all management groups, subscriptions, and resources under that management group by only allowing VMs to be created in that region.

Hierarchy of management groups and subscriptions

You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management. The following diagram shows an example of creating a hierarchy for governance using management groups.



39. Question

Your company has the divisions shown in the following table.

Division	Azure Subscription	Azure Active Directory (Azure AD) Tenant
East	Sub1, Sub2	east.pass-az304.com
West	Sub3, Sub4	west.pass-az-304.com

You plan to deploy a custom application to each subscription. The application will contain the following:

? A resource group

? An Azure web app

? Custom role assignments

? An Azure Cosmos DB account

You need to use Azure Blueprints to deploy the application to each subscription.

What is the minimum number of blue print definitions required to deploy the application?

- 1
- 2
- 3
- 4

Incorrect

You need 2 Blueprint as you will need one definition in each root management group.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved.

Note: Each Azure AD tenant is given a single top-level management group called the root management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This group allows global policies and Azure role assignments to be applied at the directory level.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/security-center/security-center-management-groups

What is Azure Blueprints?

06/21/2021 • 8 minutes to read •

Important

Azure Blueprints is currently in PREVIEW. The **Supplemental Terms of Use for Microsoft Azure Previews** include additional legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed Azure Cosmos DB. Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Azure Blueprints deploys your resources to.

Blueprint definition

A blueprint is composed of *artifacts*. Azure Blueprints currently supports the following resources as artifacts:

Resource	Hierarchy options	Description
Resource Groups	Subscription	Create a new resource group for use by other artifacts within the blueprint. These placeholder resource groups enable you to organize resources exactly the way you want them structured and provides a scope limiter for included policy and role assignment artifacts and ARM templates.
ARM template	Subscription, Resource Group	Templates, including nested and linked templates, are used to compose complex environments. Example environments: a SharePoint farm, Azure Automation State Configuration, or a Log Analytics workspace.
Policy Assignment	Subscription, Resource Group	Allows assignment of a policy or initiative to the subscription the blueprint is assigned to. The policy or initiative must be within the scope of the blueprint definition location. If the policy or initiative has parameters, these parameters are assigned at creation of the blueprint or during blueprint assignment.
Role Assignment	Subscription, Resource Group	Add an existing user or group to a built-in role to make sure the right people always have the right access to your resources. Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.

40. Question

Your company has the divisions shown in the following table.

Division	Azure Subscription	Azure Active Directory (Azure AD) Tenant
East	Sub1, Sub2	east.pass-az304.com
West	Sub3, Sub4	west.pass-az-304.com

You plan to deploy a custom application to each subscription. The application will contain the following:

? A resource group

? An Azure web app

? Custom role assignments

? An Azure Cosmos DB account

You need to use Azure Blueprints to deploy the application to each subscription.

What is the minimum number of blue print assignments required to deploy the application?

- 1
- 2

3

4

Correct

Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription.

You need 2 Assignments as you can assign the blueprints to the root management group though the REST API.

Note: Each Azure AD tenant is given a single top-level management group called the root management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This group allows global policies and Azure role assignments to be applied at the directory level.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

https://docs.microsoft.com/en-us/azure/security-center/security-center-management-groups

What is Azure Blueprints?

06/21/2021 • 8 minutes to read •

Important

Azure Blueprints is currently in PREVIEW. The **Supplemental Terms of Use for Microsoft Azure Previews** include additional legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed Azure Cosmos DB. Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Azure Blueprints deploys your resources to.

Blueprint assignment

Each **Published Version** of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription. In the portal, the blueprint defaults the **Version** to the one **Published** most recently. If there are artifact parameters or blueprint parameters, then the parameters are defined during the assignment process.

Note

Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the **Create Or Update REST API** must be used and the request body must include a value for `properties.scope` to define the target subscription.

41. Question

You have an Azure Active Directory (Azure AD) tenant.

You plan to deploy Azure Cosmos DB databases that will use the SQL API.

You need to recommend a solution to provide specific Azure AD user accounts with read access to the Cosmos DB databases.

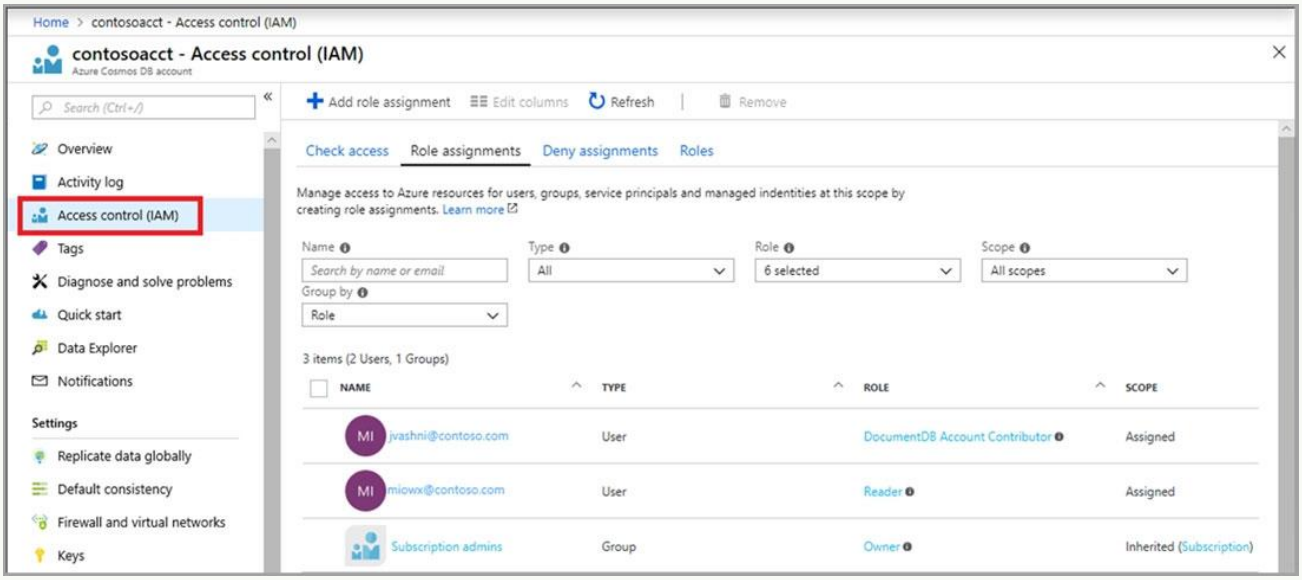
What should you include in the recommendation?

- A. shared access signatures (SAS) and conditional access policies
- B. certificates and Azure Key Vault
- C. a resource token and an Access control (IAM) role assignment
- D. master keys and Azure Information Protection policies

Correct

Azure Cosmos DB provides built-in Azure role-based access control (Azure RBAC) for common management scenarios in Azure Cosmos DB. An individual who has a profile in Azure Active Directory can assign these Azure roles to users, groups, service principals, or managed identities to grant or deny access to resources and operations on Azure Cosmos DB resources. Role assignments are scoped to control-plane access only, which includes access to Azure Cosmos accounts, databases, containers, and offers (throughput).

The Access control (IAM) pane in the Azure portal is used to configure Azure role-based access control on Azure Cosmos resources. The roles are applied to users, groups, service principals, and managed identities in Active Directory. You can use built-in roles or custom roles for individuals and groups. The following screenshot shows Active Directory integration (Azure RBAC) using access control (IAM) in the Azure portal:



Incorrect Answers:

A. shared access signatures (SAS) and conditional access policies

SAS is not applicable for Azure Cosmos DB.

B. certificates and Azure Key Vault

Certificates based authentication is not applicable for Azure Cosmos DB.

D. master keys and Azure Information Protection policies

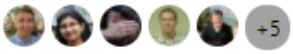
Azure Information Protection enables organizations to discover, classify, and protect documents and emails by applying labels to content. This is not a valid option for data protection in Azure Cosmos DB.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control

https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data#resource-tokens

Azure role-based access control in Azure Cosmos DB

06/17/2021 • 4 minutes to read • 

APPLIES TO: SQL API Cassandra API Gremlin API Table API Azure Cosmos DB API for MongoDB

> **Note**
>
> Azure RBAC support in Azure Cosmos DB applies to management plane operations only. This article is about role-based access control for management plane operations in Azure Cosmos DB. If you are using data plane operations, data is secured using primary keys, resource tokens, or the Azure Cosmos DB RBAC. To learn more about role-based access control applied to data plane operations, see **Secure access to data** and **Azure Cosmos DB RBAC** articles.

Azure Cosmos DB provides built-in Azure role-based access control (Azure RBAC) for common management scenarios in Azure Cosmos DB. An individual who has a profile in Azure Active Directory can assign these Azure roles to users, groups, service principals, or managed identities to grant or deny access to resources and operations on Azure Cosmos DB resources. Role assignments are scoped to control-plane access only, which includes access to Azure Cosmos accounts, databases, containers, and offers (throughput).

Built-in roles

The following are the built-in roles supported by Azure Cosmos DB:

Built-in role	Description
DocumentDB Account Contributor	Can manage Azure Cosmos DB accounts.
Cosmos DB Account Reader	Can read Azure Cosmos DB account data.
Cosmos Backup Operator	Can submit a restore request for Azure portal for a periodic backup enabled database or a container. Can modify the backup interval and retention on the Azure portal. Cannot access any data or use Data Explorer.
CosmosRestoreOperator	Can perform restore action for Azure Cosmos DB account with continuous backup mode.
Cosmos DB Operator	Can provision Azure Cosmos accounts, databases, and containers. Cannot access any data or use Data Explorer.

Resource tokens

Resource tokens provide access to the application resources within a database. Resource tokens:

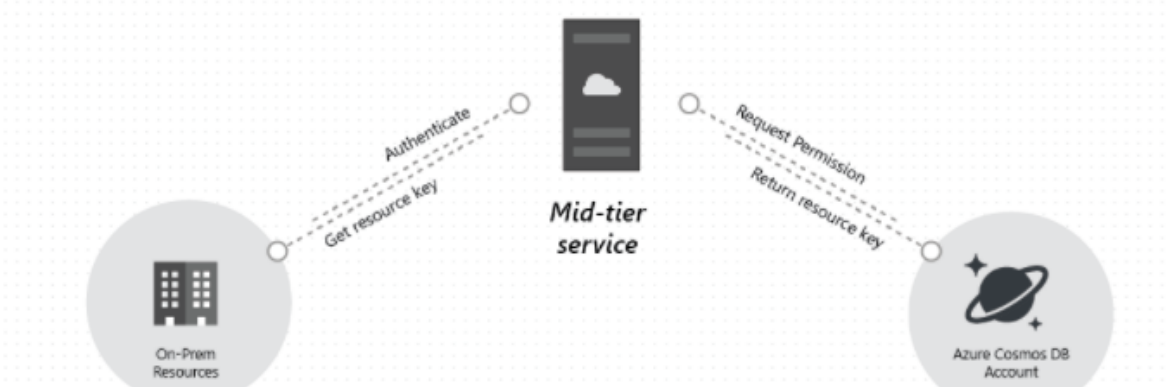
- Provide access to specific containers, partition keys, documents, attachments, stored procedures, triggers, and UDFs.
- Are created when a user is granted permissions to a specific resource.
- Are recreated when a permission resource is acted upon on by POST, GET, or PUT call.
- Use a hash resource token specifically constructed for the user, resource, and permission.
- Are time bound with a customizable validity period. The default valid time span is one hour. Token lifetime, however, may be explicitly specified, up to a maximum of five hours.
- Provide a safe alternative to giving out the primary key.
- Enable clients to read, write, and delete resources in the Cosmos DB account according to the permissions they've been granted.

You can use a resource token (by creating Cosmos DB users and permissions) when you want to provide access to resources in your Cosmos DB account to a client that cannot be trusted with the primary key.

Cosmos DB resource tokens provide a safe alternative that enables clients to read, write, and delete resources in your Cosmos DB account according to the permissions you've granted, and without need for either a primary or read only key.

Here is a typical design pattern whereby resource tokens may be requested, generated, and delivered to clients:

1. A mid-tier service is set up to serve a mobile application to share user photos.
2. The mid-tier service possesses the primary key of the Cosmos DB account.
3. The photo app is installed on end-user mobile devices.
4. On login, the photo app establishes the identity of the user with the mid-tier service. This mechanism of identity establishment is purely up to the application.
5. Once the identity is established, the mid-tier service requests permissions based on the identity.
6. The mid-tier service sends a resource token back to the phone app.
7. The phone app can continue to use the resource token to directly access Cosmos DB resources with the permissions defined by the resource token and for the interval allowed by the resource token.
8. When the resource token expires, subsequent requests receive a 401 unauthorized exception. At this point, the phone app re-establishes the identity and requests a new resource token.



Resource token generation and management are handled by the native Cosmos DB client libraries; however, if you use REST you must construct the request/authentication headers. For more information on creating authentication headers for REST, see Access Control on Cosmos DB Resources or the source code for our .NET SDK or Node.js SDK.

For an example of a middle tier service used to generate or broker resource tokens, see the ResourceTokenBroker app.

42. Question

You need to design a resource governance solution for an Azure subscription. The solution must meet the following requirements:

? Ensure that all ExpressRoute resources are created in a resource group named RG1.

? Delegate the creation of the ExpressRoute resources to an Azure Active Directory (Azure AD) group named Networking.

? Use the principle of least privilege.

Ensure that all ExpressRoute resources are created in RG1:	SLOT-1
Delegate the creation of the ExpressRoute resources to Networking:	SLOT-2

Which of the following would go into Slot1?

- A. A custom RBAC role assignment at the level of RG1
- B. A custom RBAC role assignment at the subscription level
- C. An Azure Blueprints assignment that sets locking mode for the level of RG1
- **D. An Azure Policy assignment at the subscription level that has an exclusion**
- E. Multiple Azure Policy assignments at the resource group level except for RG1

Correct

You should create a custom Azure policy to restrict ExpressRoute resources and add RG1 as exclusion.

Incorrect Answers:

A. A custom RBAC role assignment at the level of RG1

Custom RBAC roles cannot restrict the type of resources to be created in a specific resource group.

B. A custom RBAC role assignment at the subscription level

Custom RBAC roles cannot restrict the type of resources to be created in a specific resource group.

C. An Azure Blueprints assignment that sets locking mode for the level of RG1

Locking Mode applies to the blueprint assignment and it has three options: Don't Lock, Read Only, or Do Not Delete. The locking mode is configured during artifact deployment during a blueprint assignment. A different locking mode can be set by updating the blueprint assignment. Locking modes, however, can't be changed outside of Azure Blueprints.

E. Multiple Azure Policy assignments at the resource group level except for RG1

We can meet the need using a single Azure policy.

Reference:

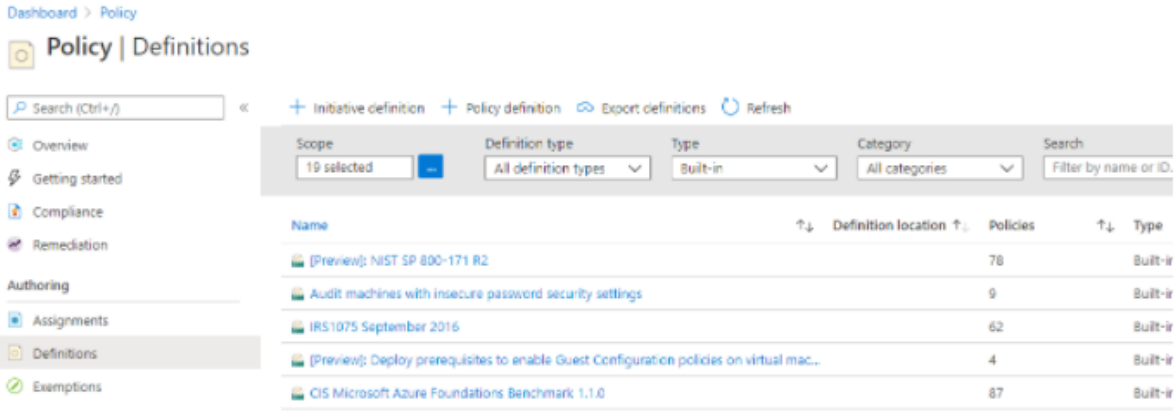
https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#implement-a-new-custom-policy

Implement a new custom policy

Now that you've assigned a built-in policy definition, you can do more with Azure Policy. Next, create a new custom policy to save costs by validating that virtual machines created in your environment can't be in the G series. This way, every time a user in your organization tries to create a virtual machine in the G series, the request is denied.

1. Select **Definitions** under **Authoring** in the left side of the Azure Policy page.



2. Select + **Policy definition** at the top of the page. This button opens to the **Policy definition** page.

3. Enter the following information:

   - The management group or subscription in which the policy definition is saved. Select by using the ellipsis on **Definition location**.

     ⓘ Note

     If you plan to apply this policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to. The same is true for an initiative definition.

   - The name of the policy definition - *Require VM SKUs not in the G series*
   - The description of what the policy definition is intended to do - *This policy definition*

enforces that all virtual machines created in this scope have SKUs other than the G series to reduce cost.

- Choose from existing options (such as *Compute*), or create a new category for this policy definition.
- Copy the following JSON code and then update it for your needs with:
  - The policy parameters.
  - The policy rules/conditions, in this case - VM SKU size equal to G series
  - The policy effect, in this case - **Deny**.

Here's what the JSON should look like. Paste your revised code into the Azure portal.

JSON Copy

```
{
    "policyRule": {
        "if": {
            "allOf": [{
                    "field": "type",
                    "equals": "Microsoft.Compute/virtualMachines"
                },
                {
                    "field": "Microsoft.Compute/virtualMachines/sku.name",
                    "like": "Standard_G*"
                }
            ]
        },
        "then": {
            "effect": "deny"
        }
    }
}
```

The *field* property in the policy rule must be a supported value. A full list of values is found on policy definition structure fields. An example of an alias might be `"Microsoft.Compute/VirtualMachines/Size"`.

To view more Azure Policy samples, see Azure Policy samples.

4. Select **Save**.

43. Question

You need to design a resource governance solution for an Azure subscription. The solution must meet the following requirements:

? Ensure that all ExpressRoute resources are created in a resource group named RG1.

? Delegate the creation of the ExpressRoute resources to an Azure Active Directory (Azure AD) group named Networking.

? Use the principle of least privilege.

Ensure that all ExpressRoute resources are created in RG1:	SLOT-1
Delegate the creation of the ExpressRoute resources to Networking:	SLOT-2

Which of the following would go into Slot2?

- A. A custom RBAC role assignment at the level of RG1
- B. A custom RBAC role assignment at the subscription level
- C. An Azure Blueprints assignment that sets locking mode for the level of RG1
- D. An Azure Policy assignment at the subscription level that has an exclusion
- E. Multiple Azure Policy assignments at the resource group level except for RG1

Incorrect

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

Incorrect Answers:

B. A custom RBAC role assignment at the subscription level

The scope must be resource group level

C. An Azure Blueprints assignment that sets locking mode for the level of RG1

Locking Mode applies to the blueprint assignment and it has three options: Don‘t Lock, Read Only, or Do Not Delete. The locking mode is configured during artifact deployment during a blueprint assignment. A different locking mode can be set by updating the blueprint assignment. Locking modes, however, can‘t be changed outside of Azure Blueprints.

As the option suggests, these are used to apply read only or do no delete locks.

D. An Azure Policy assignment at the subscription level that has an exclusion

Azure policies are not used to delegate access.

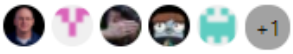
E. Multiple Azure Policy assignments at the resource group level except for RG1

Azure policies are not used to delegate access.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

Azure custom roles

08/27/2021 • 9 minutes to read • 

Important

Adding a management group to `AssignableScopes` is currently in preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see **Supplemental Terms of Use for Microsoft Azure Previews**.

If the Azure built-in roles don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group (in preview only), subscription, and resource group scopes.

Custom roles can be shared between subscriptions that trust the same Azure AD directory. There is a limit of **5,000** custom roles per directory. (For Azure Germany and Azure China 21Vianet, the limit is 2,000 custom roles.) Custom roles can be created using the Azure portal, Azure PowerShell, Azure CLI, or the REST API.

Steps to create a custom role

Here are the basic steps to create a custom role.

1. Determine the permissions you need.

   When you create a custom role, you need to know the operations that are available to define your permissions. Typically, you start with an existing built-in role and then modify it for your needs. You will add the operations to the `Actions` or `NotActions` properties of the role definition. If you have data operations, you will add those to the `DataActions` or `NotDataActions` properties.

   For more information, see the next section How to determine the permissions you need.

2. Decide how you want to create the custom role.

   You can create custom roles using Azure portal, Azure PowerShell, Azure CLI, or the REST API.

3. Create the custom role.

   The easiest way is to use the Azure portal. For steps on how to create a custom role using the Azure portal, see Create or update Azure custom roles using the Azure portal.

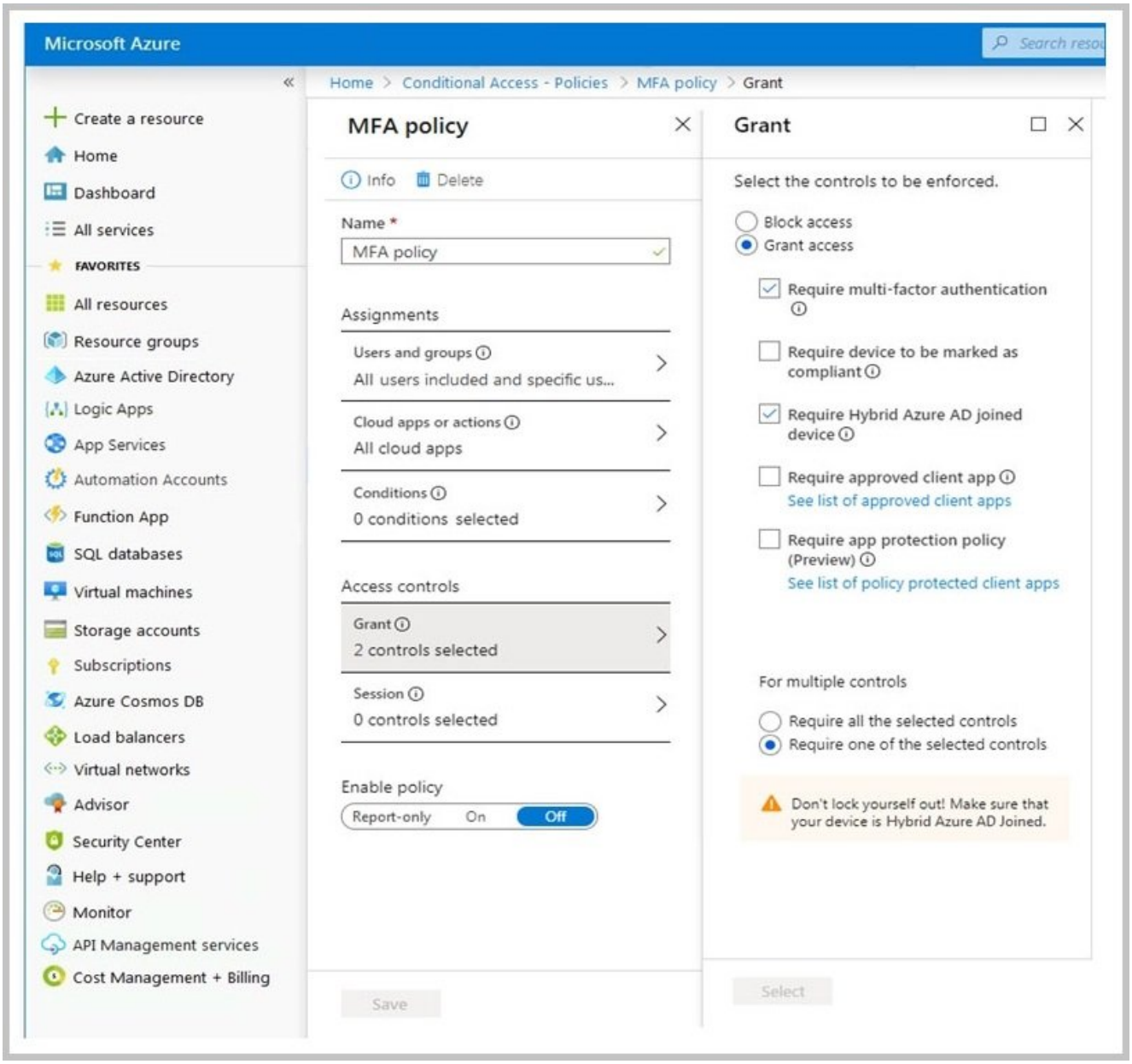
4. Test the custom role.

   Once you have your custom role, you have to test it to verify that it works as you expect. If you need to make adjustments later, you can update the custom role.

44. Question

You have an Azure Active Directory (Azure AD) tenant and Windows 10 devices.

You configure a conditional access policy as shown in the exhibit.



What is the result of the policy?

- A. All users will always be prompted for multi-factor authentication (MFA)
- B. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are NOT joined to Azure AD
- C. All users will be able to sign in without using multi-factor authentication (MFA)
- D. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are joined to Azure AD

Incorrect

In this scenario, the enable policy is set to Off in the image. So, this policy will have no impact.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

What is Conditional Access?

01/27/2021 • 2 minutes to read •

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can utilize these identity signals as part of their access control decisions.

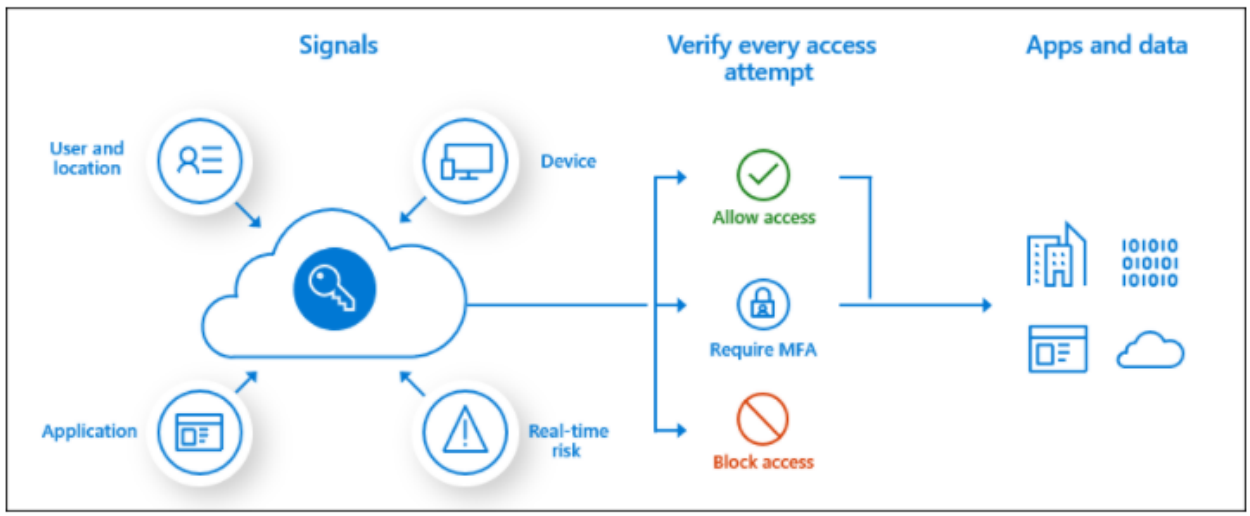
Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Important

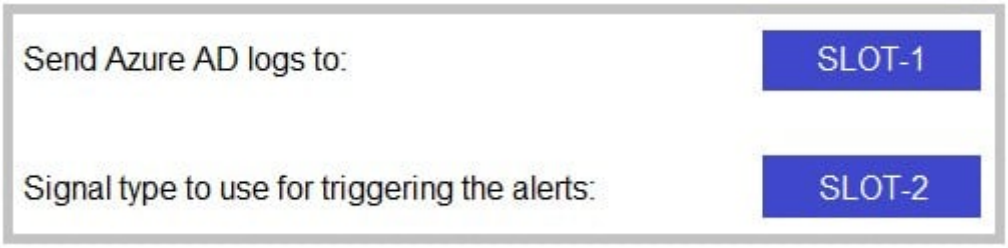
Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

45. Question

You have an Azure Active Directory (Azure AD) tenant.

You plan to use Azure Monitor to monitor user sign-ins and generate alerts based on specific user sign-in events.

You need to recommend a solution to trigger the alerts based on the events.



Which of the following would go into Slot1?

- A. An Azure event hub
- **B. An Azure Log Analytics workspace**
- C. An Azure Storage account

Correct

To be able to create an alert we send the Azure AD logs to An Azure Log Analytics workspace.

Note: You can forward your AAD logs and events to either an Azure Storage Account, an Azure Event Hub, Log Analytics, or a combination of all of these.

Incorrect Answers:

A. An Azure event hub

Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching/storage adapters. In this scenario, you need to send logs to Azure log analytics workspace to monitor and raise alerts in Azure monitor.

C. An Azure Storage account

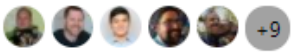
An Azure storage account contains all of your Azure Storage data objects: blobs, file shares, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. In this scenario, you need to send logs to Azure log analytics workspace to monitor and raise alerts in Azure monitor.

Reference:

https://4sysops.com/archives/how-to-create-an-azure-ad-admin-login-alert/

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

Integrate Azure AD logs with Azure Monitor logs

07/09/2021 • 3 minutes to read • 

Follow the steps in this article to integrate Azure Active Directory (Azure AD) logs with Azure Monitor.

Use the integration of Azure AD activity logs in Azure Monitor logs to perform tasks like:

- Compare your Azure AD sign-in logs against security logs published by Azure Security Center.
- Troubleshoot performance bottlenecks on your application's sign-in page by correlating application performance data from Azure Application Insights.
- Analyze Identity Protection risky users and risk detections logs to detect threats in your environment (public preview)
- Identify sign-ins from applications that use the Active Directory Authentication Library (ADAL) for authentication. ADAL is nearing end-of-support.

Supported reports

You can route audit activity logs and sign-in activity logs to Azure Monitor logs for further analysis.

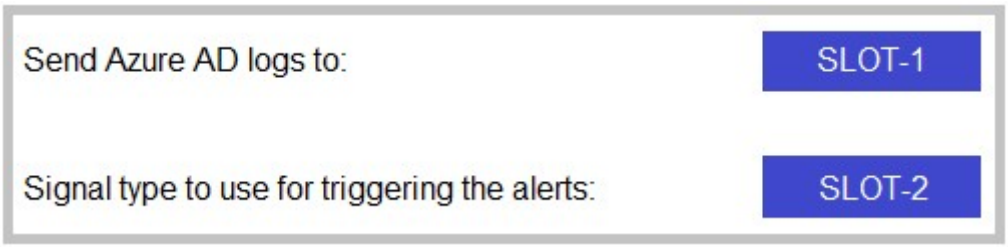
- **Audit logs**: The audit logs activity report gives you access to the history of every task that's performed in your tenant.
- **Sign-in logs**: With the sign-in activity report, you can determine who performed the tasks that are reported in the audit logs.
- **Provisioning logs**: With the provisioning logs, you can monitor which users have been created, updated, and deleted in all your third-party applications.
- **Risky users logs (public preview)**: With the risky users logs, you can monitor changes in user risk level and remediation activity.
- **Risk detections logs (public preview)**: With the risk detections logs, you can monitor user's risk detections and analyze trends in risk activity detected in your organization.

46. Question

You have an Azure Active Directory (Azure AD) tenant.

You plan to use Azure Monitor to monitor user sign-ins and generate alerts based on specific user sign-in events.

You need to recommend a solution to trigger the alerts based on the events.



Which of the following would go into Slot2?

- A. Activity log
- B. Log
- C. Metric

Incorrect

Ensure Resource Type is an analytics source like Log Analytics or Application Insights and signal type as Log.

Incorrect Answers:

A. Activity log

The Activity log is a platform log in Azure that provides insight into subscription-level events.

C. Metric

Azure Monitor Metrics is a feature of Azure Monitor that collects numeric data from monitored resources into a time series database. Metrics are numerical values that are collected at regular intervals and describe some aspect of a system at a particular time.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log

Create, view, and manage log alerts using Azure Monitor

09/22/2020 • 12 minutes to read • 

Overview

Log alerts allow users to use a Log Analytics query to evaluate resources logs every set frequency, and fire an alert based on the results. Rules can trigger one or more actions using Action Groups. Learn more about functionality and terminology of log alerts.

This article shows you how to create and manage log alerts using Azure Monitor. Alert rules are defined by three components:

- Target: A specific Azure resource to monitor.
- Criteria: Logic to evaluate. If met, the alert fires.
- Action: Notifications or automation - email, SMS, webhook, and so on.

You can also create log alert rules using Azure Resource Manager templates, which are described in a separate article.

ⓘ **Note**

Log data from a **Log Analytics workspace** can be sent to the Azure Monitor metrics store. Metrics alerts have **different behavior**, which may be more desirable depending on the data you are working with. For information on what and how you can route logs to metrics, see **Metric Alert for Logs.**

47. Question

You deploy Azure App Service Web Apps that connect to on-premises Microsoft SQL Server instances by using Azure ExpressRoute. You plan to migrate the SQL Server instances to Azure.

Migration of the SQL Server instances to Azure must:

? Support automatic patching and version updates to SQL Server.

? Provide automatic backup services.

? Allow for high-availability of the instances.

? Provide a native VNET with private IP addressing.

? Encrypt all data in transit.

? Be in a single-tenant environment with dedicated underlying infrastructure (compute, storage).

You need to migrate the SQL Server instances to Azure.

Which Azure service should you use?

○ A. SQL Server in a Docker container running on Azure Container Instances (ACI)

B. SQL Server in Docker containers running on Azure Kubernetes Service (AKS)

C. SQL Server Infrastructure-as-a-Service (IaaS) virtual machine (VM)

D. Azure SQL Database Managed Instance

E. Azure SQL Database with elastic pools

Correct

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine.

Azure SQL Managed Instance is designed for customers looking to migrate a large number of apps from an on-premises or IaaS, self-built, or ISV provided environment to a fully managed PaaS cloud environment, with as low a migration effort as possible. Using the fully automated Azure Data Migration Service, customers can lift and shift their existing SQL Server instance to SQL Managed Instance, which offers compatibility with SQL Server and complete isolation of customer instances with native VNet support.

Reference:

https://docs.microsoft.com/en-us/azure/dms/resource-network-topologies

https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview

What is Azure SQL Managed Instance?

01/14/2021 • 15 minutes to read • +10

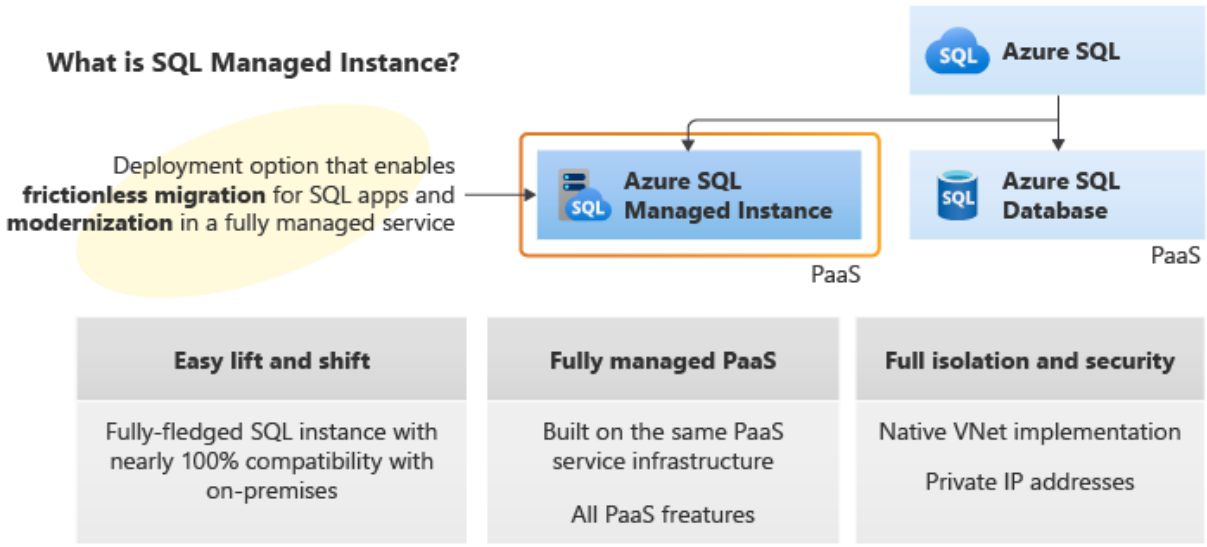
APPLIES TO: Azure SQL Managed Instance

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

Important

For a list of regions where SQL Managed Instance is currently available, see **Supported regions.**

The following diagram outlines key features of SQL Managed Instance:



48. Question

You are designing a SQL database solution. The solution will include 20 databases that will be 20 GB each and have varying usage patterns.

You need to recommend a database platform to host the databases. The solution must meet the following requirements:

? The compute resources allocated to the databases must scale dynamically.

? The solution must meet an SLA of 99.99% uptime.

? The solution must have reserved capacity.

? Compute charges must be minimized.

What should you include in the recommendation?

- A. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine in an availability set
- B. 20 instances of Azure SQL Database serverless
- C. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine
- **D. an elastic pool that contains 20 Azure SQL databases**

Correct

Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands. The databases in an elastic pool are on a single server and share a set number of resources at a set price. Elastic pools in Azure SQL Database enable SaaS developers to optimize the price performance for a group of databases within a prescribed budget while delivering performance elasticity for each database.

Guaranteed 99.995 percent uptime for SQL Database

Incorrect Answers:

A. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine in an availability set

This option causes higher computing costs.

B. 20 instances of Azure SQL Database serverless

Elastic pool is a cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands as compared with individual instances.

C. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine

It cannot provide 99.99% uptime.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview

https://azure.microsoft.com/en-us/pricing/details/sql-database/elastic/

Elastic pools help you manage and scale multiple databases in Azure SQL Database

06/23/2021 • 10 minutes to read • +3

APPLIES TO: Azure SQL Database

Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands. The databases in an elastic pool are on a single server and share a set number of resources at a set price. Elastic pools in Azure SQL Database enable SaaS developers to optimize the price performance for a group of databases within a prescribed budget while delivering performance elasticity for each database.

What are SQL elastic pools

SaaS developers build applications on top of large scale data-tiers consisting of multiple databases. A common application pattern is to provision a single database for each customer. But different customers often have varying and unpredictable usage patterns, and it's difficult to predict the resource requirements of each individual database user. Traditionally, you had two options:

- Over-provision resources based on peak usage and over pay, or
- Under-provision to save cost, at the expense of performance and customer satisfaction during peaks.

Elastic pools solve this problem by ensuring that databases get the performance resources they need when they need it. They provide a simple resource allocation mechanism within a predictable budget. To learn more about design patterns for SaaS applications using elastic pools, see Design Patterns for Multi-tenant SaaS Applications with Azure SQL Database.

Important

There is no per-database charge for elastic pools. You are billed for each hour a pool exists at the highest eDTU or vCores, regardless of usage or whether the pool was active for less than an hour.

49. Question

You have an app named App1 that uses two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to migrate DB1 and DB2 to Azure.

You need to recommend an Azure solution to host DB1 and DB2. The solution must meet the following requirements:

? Support server-side transactions across DB1 and DB2.

? Minimize administrative effort to update the solution.

What should you recommend?

- A. two Azure SQL databases in an elastic pool
- B. two Azure SQL databases on different Azure SQL Database servers
- C. two Azure SQL databases on the same Azure SQL Database managed instance
- D. two SQL Server databases on an Azure virtual machine

Incorrect

SQL Managed Instance enables system administrators to spend less time on administrative tasks because the service either performs them for you or greatly simplifies those tasks.

Note: Azure SQL Managed Instance is designed for customers looking to migrate a large number of apps from an on-premises or IaaS, self-built, or ISV provided environment to a fully managed PaaS cloud environment, with as low a migration effort as possible. Using the fully automated Azure Data Migration Service, customers can lift and shift their existing SQL Server instance to SQL Managed Instance, which offers compatibility with SQL Server and complete isolation of customer instances with native VNet support. With Software Assurance, you can exchange your existing licenses for discounted rates on SQL Managed Instance using the Azure Hybrid Benefit for SQL Server. SQL Managed Instance is the best migration destination in the cloud for SQL Server instances that require high security and a rich programmability surface.

Incorrect Answers:

A. two Azure SQL databases in an elastic pool

Distributed transactions are not supported in Azure SQL, because this feature is still in preview.

B. two Azure SQL databases on different Azure SQL Database servers

This option increases administrative effort.

D. two SQL Server databases on an Azure virtual machine

This option increases administrative effort.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview

What is Azure SQL Managed Instance?

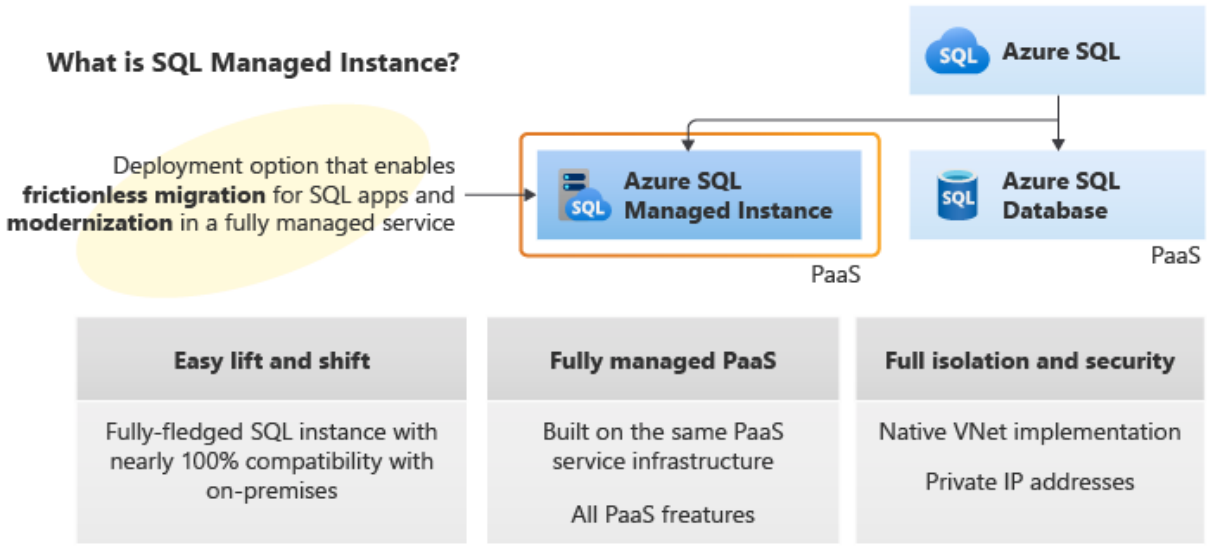
01/14/2021 • 15 minutes to read • +10

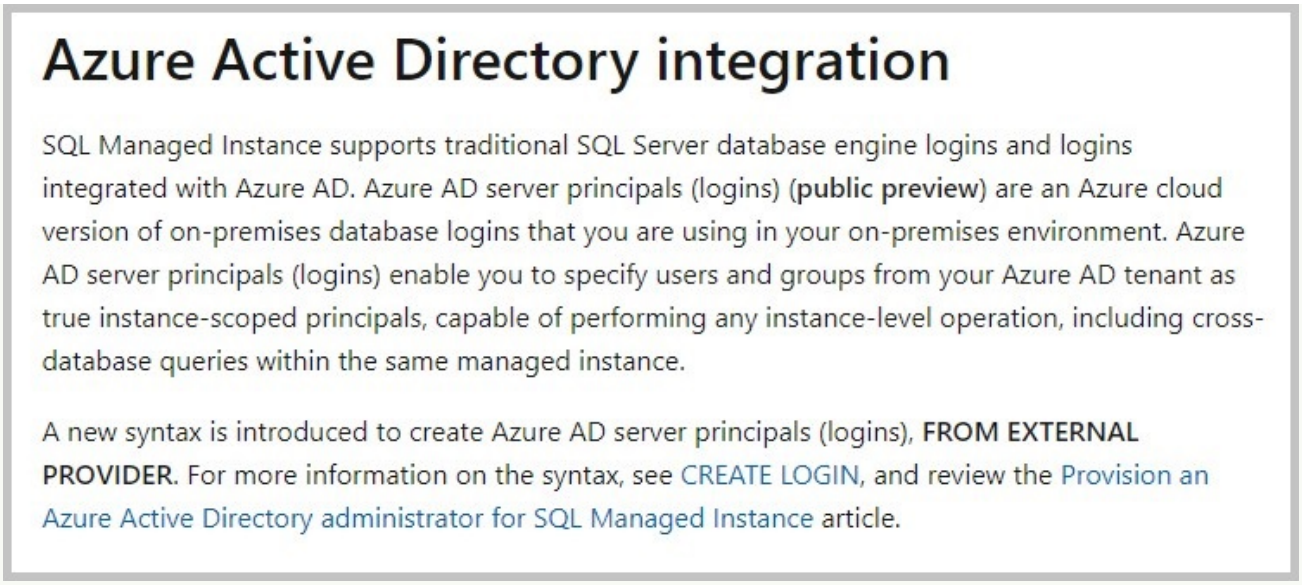
APPLIES TO: Azure SQL Managed Instance

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

> **Important**
>
> For a list of regions where SQL Managed Instance is currently available, see **Supported regions.**

The following diagram outlines key features of SQL Managed Instance:





50. Question

You are planning an Azure Storage solution for sensitive data. The data will be accessed daily. The data set is less than 10 GB.

You need to recommend a storage solution that meets the following requirements:

? All the data written to storage must be retained for five years.

? Once the data is written, the data can only be read. Modifications and deletion must be prevented.

? After five years, the data can be deleted, but never modified.

? Data access charges must be minimized.

Which of the following would go into Slot1?

- A. General purpose v2 with Archive access tier for blobs
- B. General purpose v2 with Cool access tier for blobs
- **C. General purpose v2 with Hot access tier for blobs**

Correct

Requirement: The data will be accessed daily

Hot access tier is optimized for storing data that is accessed frequently

Incorrect Answers:

A. General purpose v2 with Archive access tier for blobs

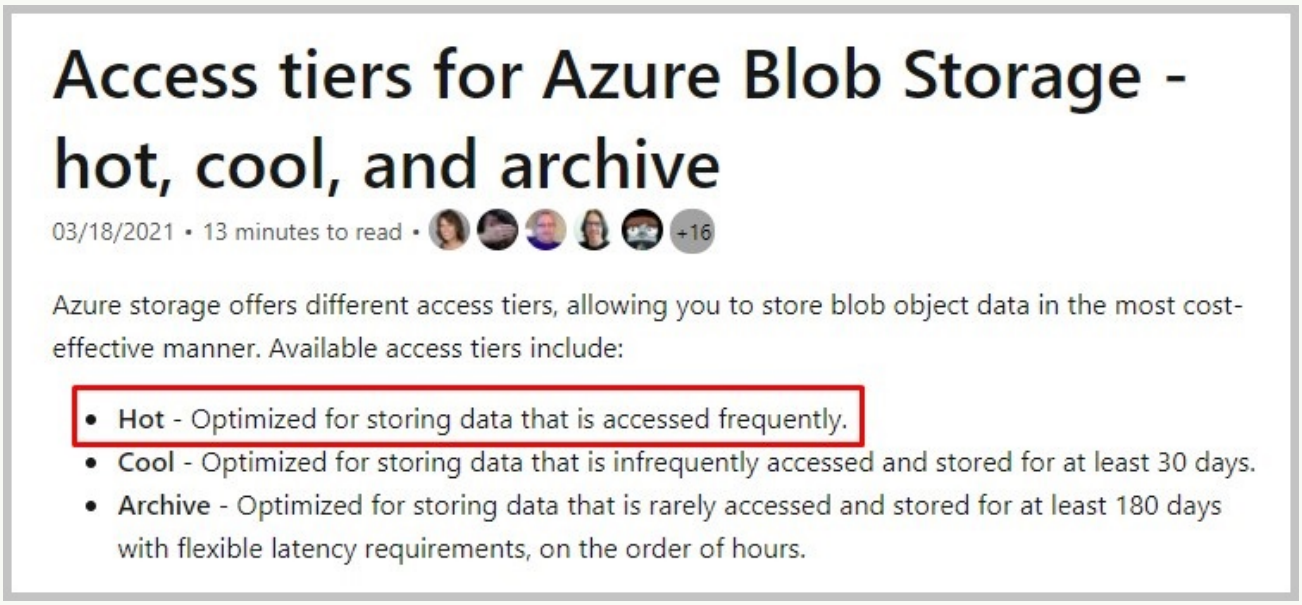
Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.

B. General purpose v2 with Cool access tier for blobs

Optimized for storing data that is infrequently accessed and stored for at least 30 days.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers



51. Question

You are planning an Azure Storage solution for sensitive data. The data will be accessed daily. The data set is less than 10 GB.

You need to recommend a storage solution that meets the following requirements:

? All the data written to storage must be retained for five years.

? Once the data is written, the data can only be read. Modifications and deletion must be prevented.

? After five years, the data can be deleted, but never modified.

? Data access charges must be minimized.

Which of the following would go into Slot2?

- A. Container access level
- B. Container access policy
- C. Storage account resource lock

Incorrect

Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Note: A read-only lock on a storage account doesn't prevent data within that account from being deleted or modified. This type of lock only protects the storage account itself from being deleted or modified, and doesn't protect blob, queue, table, or file data within that storage account.

Incorrect Answers:

A. Container access level

Restricting access at the container level does not prevent modifying or deleting blobs.

C. Storage account resource lock

Storage account resource lock does not prevent you from modification/deletion of data within container. This will only prevent from modification or deletion of storage account

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-policy-configure-container-scope?tabs=azure-portal

https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview

https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview#scenarios-with-container-level-scope

Store business-critical blob data with immutable storage

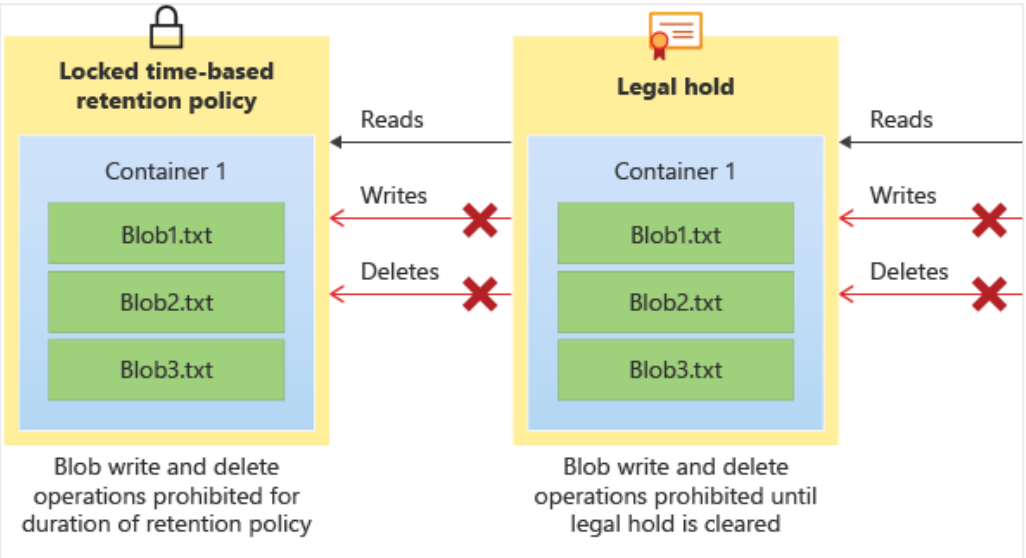
08/31/2021 • 10 minutes to read •

Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Immutable storage for Azure Blob storage supports two types of immutability policies:

- **Time-based retention policies**: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten. To learn more about time-based retention policies, see Time-based retention policies for immutable blob data.
- **Legal hold policies**: A legal hold stores immutable data until the legal hold is explicitly cleared. When a legal hold is set, objects can be created and read, but not modified or deleted. To learn more about legal hold policies, see Legal holds for immutable blob data.

The following diagram shows how time-based retention policies and legal holds prevent write and delete operations while they are in effect.



52. Question

You have an Azure subscription that contains an Azure SQL database.

You plan to use Azure reservations on the Azure SQL database.

To which resource type will the reservation discount be applied?

A. vCore compute

B. DTU compute

C. Storage

D. License

Correct

Quantity: The amount of compute resources being purchased within the capacity reservation. The quantity is a number of vCores in the selected Azure region and Performance tier that are being reserved and will get the billing discount. For example, if you run or plan to run multiple databases with the total compute capacity of Gen5 16 vCores in the East US region, then you would specify the quantity as 16 to maximize the benefit for all the databases.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/reserved-capacity-overview

Save costs for resources with reserved capacity - Azure SQL Database & SQL Managed Instance

10/13/2020 • 6 minutes to read • +4

APPLIES TO: Azure SQL Database Azure SQL Managed Instance

Save money with Azure SQL Database and SQL Managed Instance by committing to a reservation for compute resources compared to pay-as-you-go prices. With reserved capacity, you make a commitment for SQL Database and/or SQL Managed Instance use for a period of one or three years to get a significant discount on the compute costs. To purchase reserved capacity, you need to specify the Azure region, deployment type, performance tier, and term.

You do not need to assign the reservation to a specific database or managed instance. Matching existing deployments that are already running or ones that are newly deployed automatically get the benefit. By purchasing a reservation, you commit to usage for the compute costs for a period of one or three years. As soon as you buy a reservation, the compute charges that match the reservation attributes are no longer charged at the pay-as-you go rates.

A reservation applies to both primary and billable secondary compute replicas, but does not cover software, networking, or storage charges associated with the service. At the end of the reservation term, the billing benefit expires and the database or managed instance is billed at the pay-as-you go price. Reservations do not automatically renew. For pricing information, see the reserved capacity offering.

You can buy reserved capacity in the Azure portal. Pay for the reservation up front or with monthly payments. To buy reserved capacity:

- You must be in the owner role for at least one Enterprise or individual subscription with pay-as-you-go rates.
- For Enterprise subscriptions, **Add Reserved Instances** must be enabled in the EA portal. Or, if that setting is disabled, you must be an EA Admin on the subscription. Reserved capacity.

For more information about how enterprise customers and Pay-As-You-Go customers are charged for reservation purchases, see Understand Azure reservation usage for your Enterprise enrollment and Understand Azure reservation usage for your Pay-As-You-Go subscription.

> ⓘ Note
>
> Purchasing reserved capacity does not pre-allocate or reserve specific infrastructure resources (virtual machines or nodes) for your use.

53. Question

You have an Azure Storage v2 account named storage1. You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

What should you do?

- A. You create an Azure Blob storage container, and you configure a legal hold access policy
- B. You create a file share and snapshots
- C. You create a file share, and you configure an access policy
- **D. You create an Azure Blob storage container, and you configure a time-based retention policy and lock the policy**

Correct

Time-based retention policy support: Users can set policies to store data for a specified interval. When a time-based retention policy is set, blobs can be created and read, but not modified or deleted. After the retention period has expired, blobs can be deleted but not overwritten.

Note: Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. For the duration of the retention interval, blobs can be created and read, but cannot be modified or deleted. Immutable storage is available for general-purpose v2 and Blob storage accounts in all Azure regions.

Incorrect Answers:

A. You create an Azure Blob storage container, and you configure a legal hold access policy

A legal hold stores immutable data until the legal hold is explicitly cleared. When a legal hold is set, objects can be created and read, but not modified or deleted. It is used when you do not know how long you need to keep the data without editing/deleting it.

B. You create a file share and snapshots

Azure Files provides the capability to take share snapshots of file shares. Share snapshots capture the share state at that point in time. It can be used as a solution for recovering data after accidental deletion or corruption.

C. You create a file share, and you configure an access policy

A stored access policy provides an additional level of control over service-level shared access signatures (SAS) on the server side. Establishing a stored access policy serves to group shared access signatures and to provide additional restrictions for signatures that are bound by the policy.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

Store business-critical blob data with immutable storage

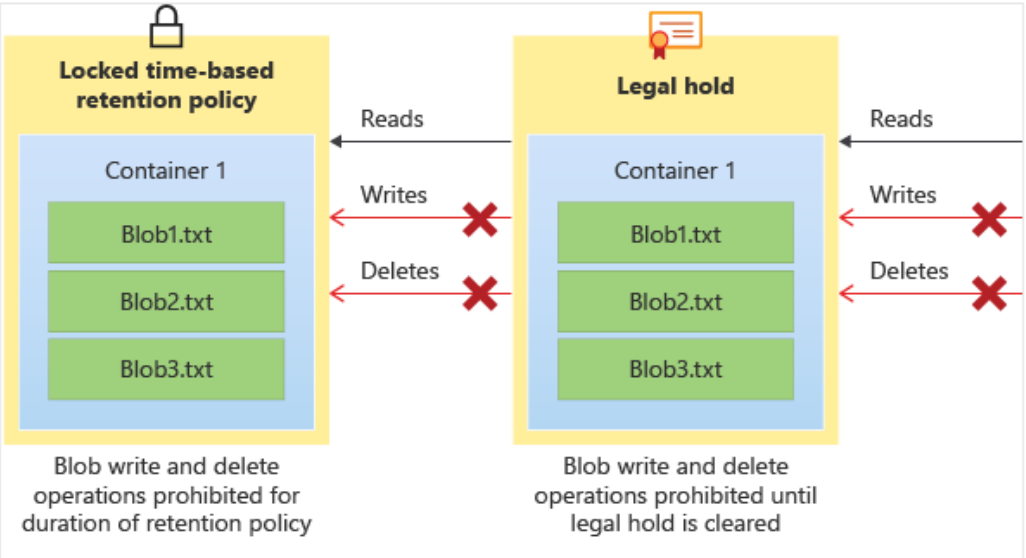
08/31/2021 • 10 minutes to read •

Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Immutable storage for Azure Blob storage supports two types of immutability policies:

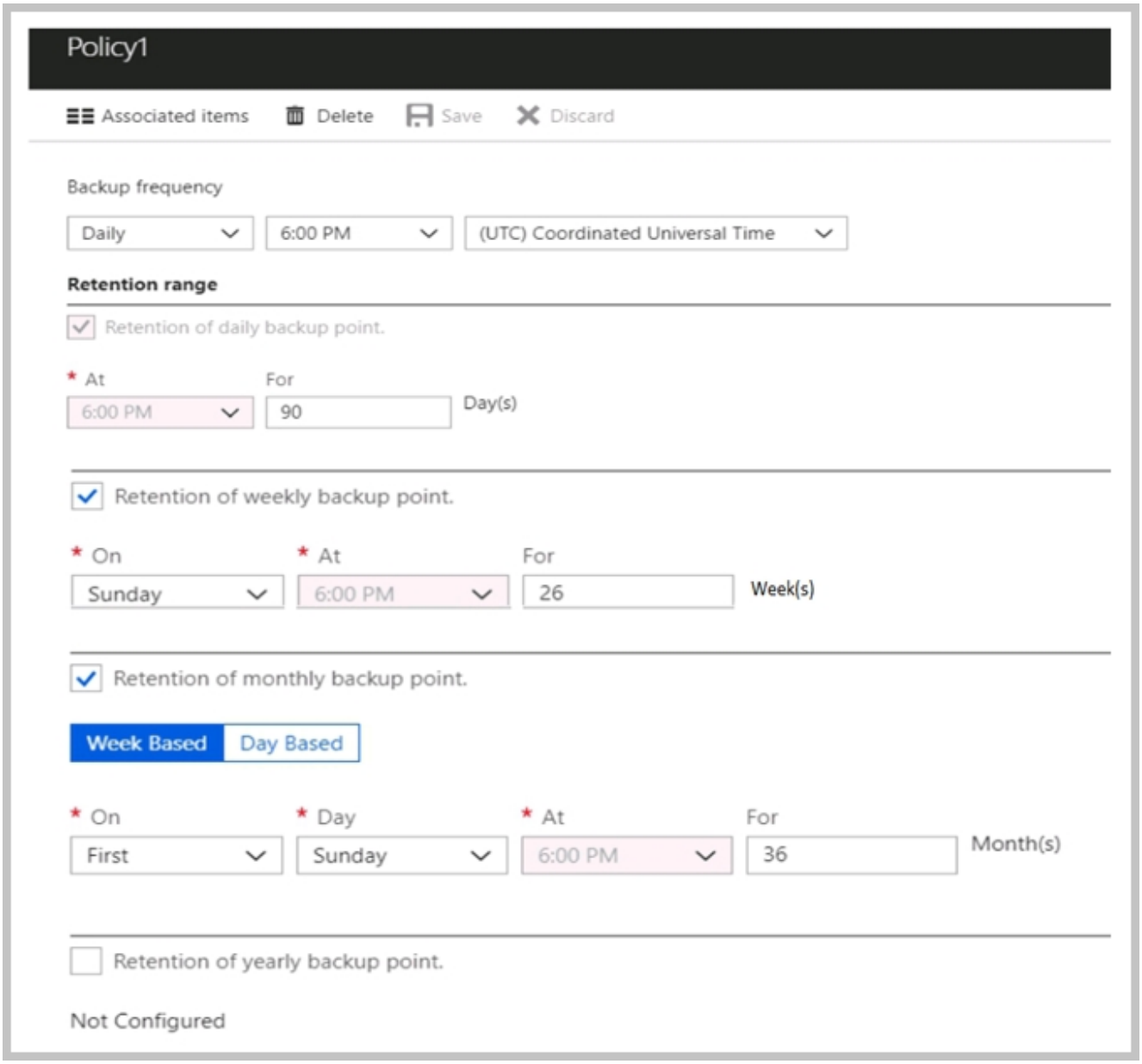
- **Time-based retention policies**: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten. To learn more about time-based retention policies, see Time-based retention policies for immutable blob data.
- **Legal hold policies**: A legal hold stores immutable data until the legal hold is explicitly cleared. When a legal hold is set, objects can be created and read, but not modified or deleted. To learn more about legal hold policies, see Legal holds for immutable blob data.

The following diagram shows how time-based retention policies and legal holds prevent write and delete operations while they are in effect.



54. Question

You plan to deploy the backup policy shown in the following exhibit.



Select the answer that completes the following statement based on the information presented in the graphic.

Virtual machines that are backed up by using the policy can be recovered for up to a maximum of _____.

- A. 90 days
- B. 26 weeks
- C. 36 months
- D. 45 months

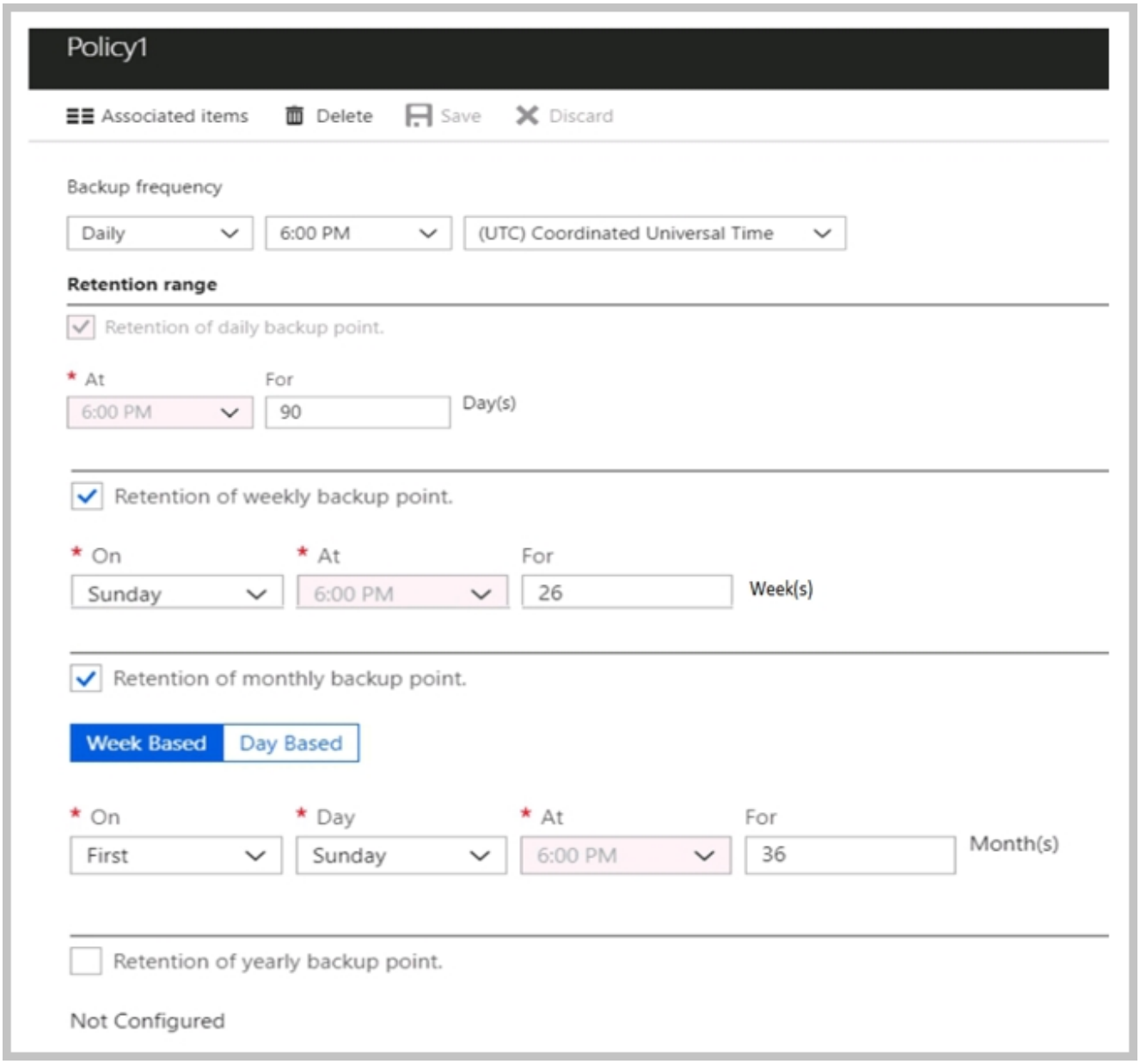
Correct

The monthly backups are configured to retain for 36 months.

Note: 36 months is monthly retention, not yearly

55. Question

You plan to deploy the backup policy shown in the following exhibit.



Select the answer that completes the following statement based on the information presented in the graphic.

The minimum recovery point objective (RPO) for virtual machines that are backed up by using the policy is _____.

- A. 1 hour
- B. 1 day
- C. 1 week
- D. 1 month
- E. 1 year

Correct

With daily backup at 6:00 pm, it is acceptable to lose the data up to a day old. you will lose no more than 1 days data. RPO should be 1 day

56. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You have an Azure Storage v2 account named storage1. You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create an Azure Blob storage container, and you configure a legal hold access policy.

Does this meet the goal?

- A. Yes
- B. No

Correct

Use an Azure Blob storage container, but use a time-based retention policy instead of a legal hold.

Note: Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. For the duration of the retention interval, blobs can be created and read, but cannot be modified or deleted. Immutable storage is available for general-purpose v2 and Blob storage accounts in all Azure regions.

Note: Set retention policies and legal holds

? Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general- purpose v2 or Blob storage account.

? Select Access policy in the container settings. Then select Add policy under Immutable blob storage.

? To enable time-based retention, select Time-based retention from the drop-down menu.

? Enter the retention interval in days (acceptable values are 1 to 146000 days).

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutability-policies-manage

Store business-critical blob data with immutable storage

08/31/2021 • 10 minutes to read •

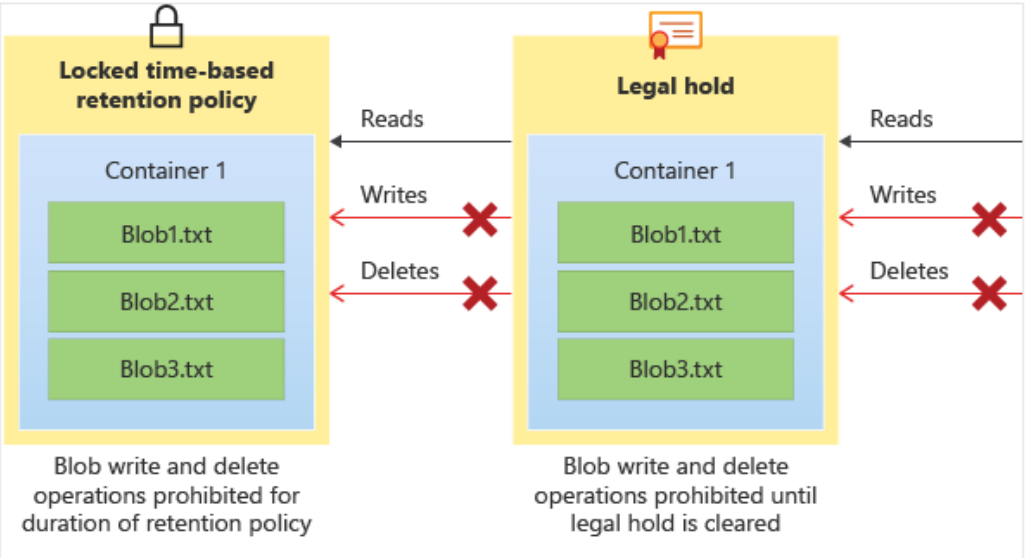
Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Immutable storage for Azure Blob storage supports two types of immutability policies:

- **Time-based retention policies**: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten. To learn more about time-based retention policies, see Time-based retention policies for immutable blob data.

- **Legal hold policies**: A legal hold stores immutable data until the legal hold is explicitly cleared. When a legal hold is set, objects can be created and read, but not modified or deleted. To learn more about legal hold policies, see Legal holds for immutable blob data.

The following diagram shows how time-based retention policies and legal holds prevent write and delete operations while they are in effect.



About immutable storage for blobs

Immutable storage helps healthcare organization, financial institutions, and related industries—particularly broker-dealer organizations—to store data securely. Immutable storage can be leveraged in any scenario to protect critical data against modification or deletion.

Typical applications include:

- **Regulatory compliance**: Immutable storage for Azure Blob storage helps organizations address SEC 17a-4(f), CFTC 1.31(d), FINRA, and other regulations.
- **Secure document retention**: Immutable storage for blobs ensures that data can't be modified or deleted by any user, not even by users with account administrative privileges.
- **Legal hold**: Immutable storage for blobs enables users to store sensitive information that is critical to litigation or business use in a tamper-proof state for the desired duration until the hold is removed. This feature is not limited only to legal use cases but can also be thought of as an event-based hold or an enterprise lock, where the need to protect data based on event triggers or corporate policy is required.

57. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You have an Azure Storage v2 account named storage1. You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create a file share and snapshots.

Does this meet the goal?

- A. Yes
- B. No

Correct

Instead use an immutable Blob Storage with a time-based retention policy

Note: Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. For the duration of the retention interval, blobs can be created and read, but cannot be modified or deleted. Immutable storage is available for general-purpose v2 and Blob storage accounts in all Azure regions.

Note: Set retention policies and legal holds

? Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general- purpose v2 or Blob storage account.

? Select Access policy in the container settings. Then select Add policy under Immutable blob storage.

? To enable time-based retention, select Time-based retention from the drop-down menu.

? Enter the retention interval in days (acceptable values are 1 to 146000 days).

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutability-policies-manage

Store business-critical blob data with immutable storage

08/31/2021 • 10 minutes to read •

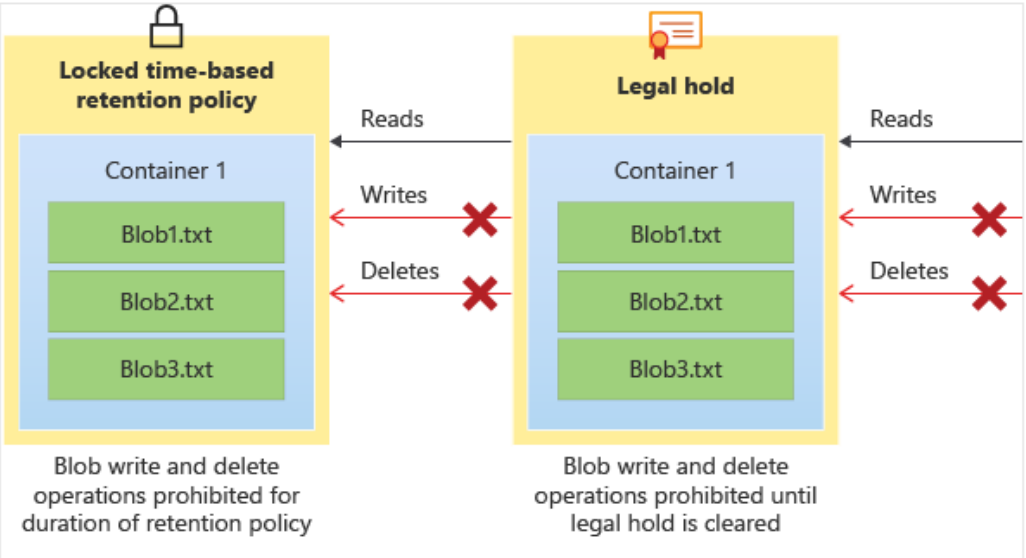
Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Immutable storage for Azure Blob storage supports two types of immutability policies:

- **Time-based retention policies**: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten. To learn more about time-based retention policies, see Time-based retention policies for immutable blob data.

- **Legal hold policies**: A legal hold stores immutable data until the legal hold is explicitly cleared. When a legal hold is set, objects can be created and read, but not modified or deleted. To learn more about legal hold policies, see Legal holds for immutable blob data.

The following diagram shows how time-based retention policies and legal holds prevent write and delete operations while they are in effect.



About immutable storage for blobs

Immutable storage helps healthcare organization, financial institutions, and related industries—particularly broker-dealer organizations—to store data securely. Immutable storage can be leveraged in any scenario to protect critical data against modification or deletion.

Typical applications include:

- **Regulatory compliance:** Immutable storage for Azure Blob storage helps organizations address SEC 17a-4(f), CFTC 1.31(d), FINRA, and other regulations.
- **Secure document retention:** Immutable storage for blobs ensures that data can't be modified or deleted by any user, not even by users with account administrative privileges.
- **Legal hold:** Immutable storage for blobs enables users to store sensitive information that is critical to litigation or business use in a tamper-proof state for the desired duration until the hold is removed. This feature is not limited only to legal use cases but can also be thought of as an event-based hold or an enterprise lock, where the need to protect data based on event triggers or corporate policy is required.

58. Question

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

In the real exam, after you answer a question in this section, you will NOT be able to return to it.

You have an Azure Storage v2 account named storage1. You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create a file share, and you configure an access policy.

Does this meet the goal?

- A. Yes
- B. No

Correct

Instead of a file share, an immutable Blob storage is required and Time-based retention policy support

Time-based retention policy support: Users can set policies to store data for a specified interval. When a time-based retention policy is set, blobs can be created and read, but not modified or deleted. After the retention period has expired, blobs can be deleted but not overwritten.

Note: Set retention policies and legal holds

? Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general- purpose v2 or Blob storage account.

? Select Access policy in the container settings. Then select Add policy under Immutable blob storage.

? To enable time-based retention, select Time-based retention from the drop-down menu.

? Enter the retention interval in days (acceptable values are 1 to 146000 days).

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutability-policies-manage

Store business-critical blob data with immutable storage

08/31/2021 • 10 minutes to read •

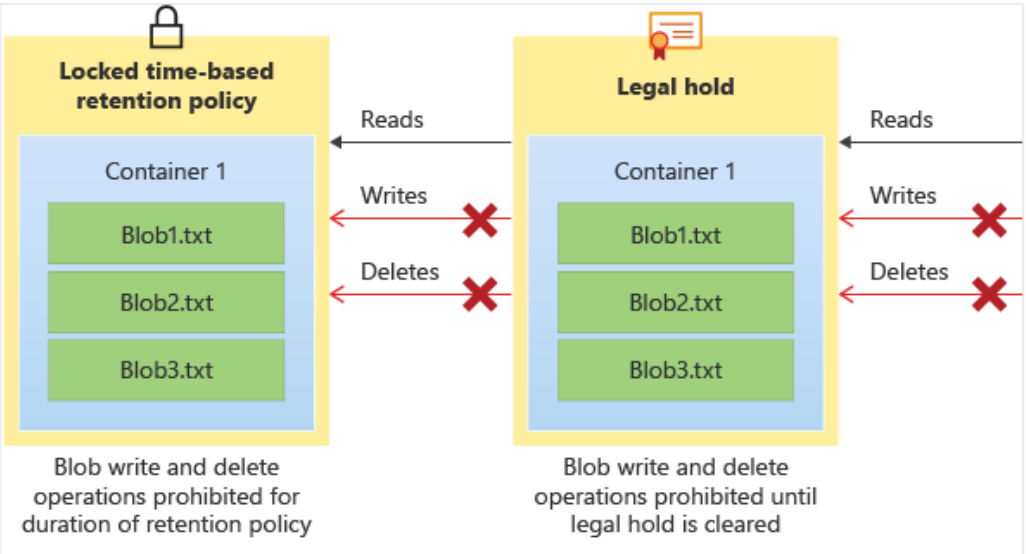
Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.

Immutable storage for Azure Blob storage supports two types of immutability policies:

- **Time-based retention policies**: With a time-based retention policy, users can set policies to store data for a specified interval. When a time-based retention policy is set, objects can be created and read, but not modified or deleted. After the retention period has expired, objects can be deleted but not overwritten. To learn more about time-based retention policies, see Time-based retention policies for immutable blob data.

- **Legal hold policies**: A legal hold stores immutable data until the legal hold is explicitly cleared. When a legal hold is set, objects can be created and read, but not modified or deleted. To learn more about legal hold policies, see Legal holds for immutable blob data.

The following diagram shows how time-based retention policies and legal holds prevent write and delete operations while they are in effect.



About immutable storage for blobs

Immutable storage helps healthcare organization, financial institutions, and related industries—particularly broker-dealer organizations—to store data securely. Immutable storage can be leveraged in any scenario to protect critical data against modification or deletion.

Typical applications include:

- **Regulatory compliance**: Immutable storage for Azure Blob storage helps organizations address SEC 17a-4(f), CFTC 1.31(d), FINRA, and other regulations.
- **Secure document retention**: Immutable storage for blobs ensures that data can't be modified or deleted by any user, not even by users with account administrative privileges.
- **Legal hold**: Immutable storage for blobs enables users to store sensitive information that is critical to litigation or business use in a tamper-proof state for the desired duration until the hold is removed. This feature is not limited only to legal use cases but can also be thought of as an event-based hold or an enterprise lock, where the need to protect data based on event triggers or corporate policy is required.

59. Question

Your network contains an on-premises Active Directory domain. The domain contains the Hyper-V clusters shown in the following table.

Name	Number of Nodes	Number of Virtual Machines running on Cluster
Cluster1	4	2
Cluster2	3	15

You plan to implement Azure Site Recovery to protect six virtual machines running on Cluster1 and three virtual machines running on Cluster2. Virtual machines are running on all Cluster1 and Cluster2 nodes.
You need to identify the minimum number of Azure Site Recovery Providers that must be installed on premises.
How many Providers should you identify?

- A. 1
- B. 7
- C. 9
- D. 16

Incorrect

Install it on all seven nodes.

Note: Install the Azure Site Recovery Provider

Run the Provider setup file on each VMM server. If VMM is deployed in a cluster, install for the first time as follows:

? Install the Provider on an active node, and finish the installation to register the VMM server in the vault.

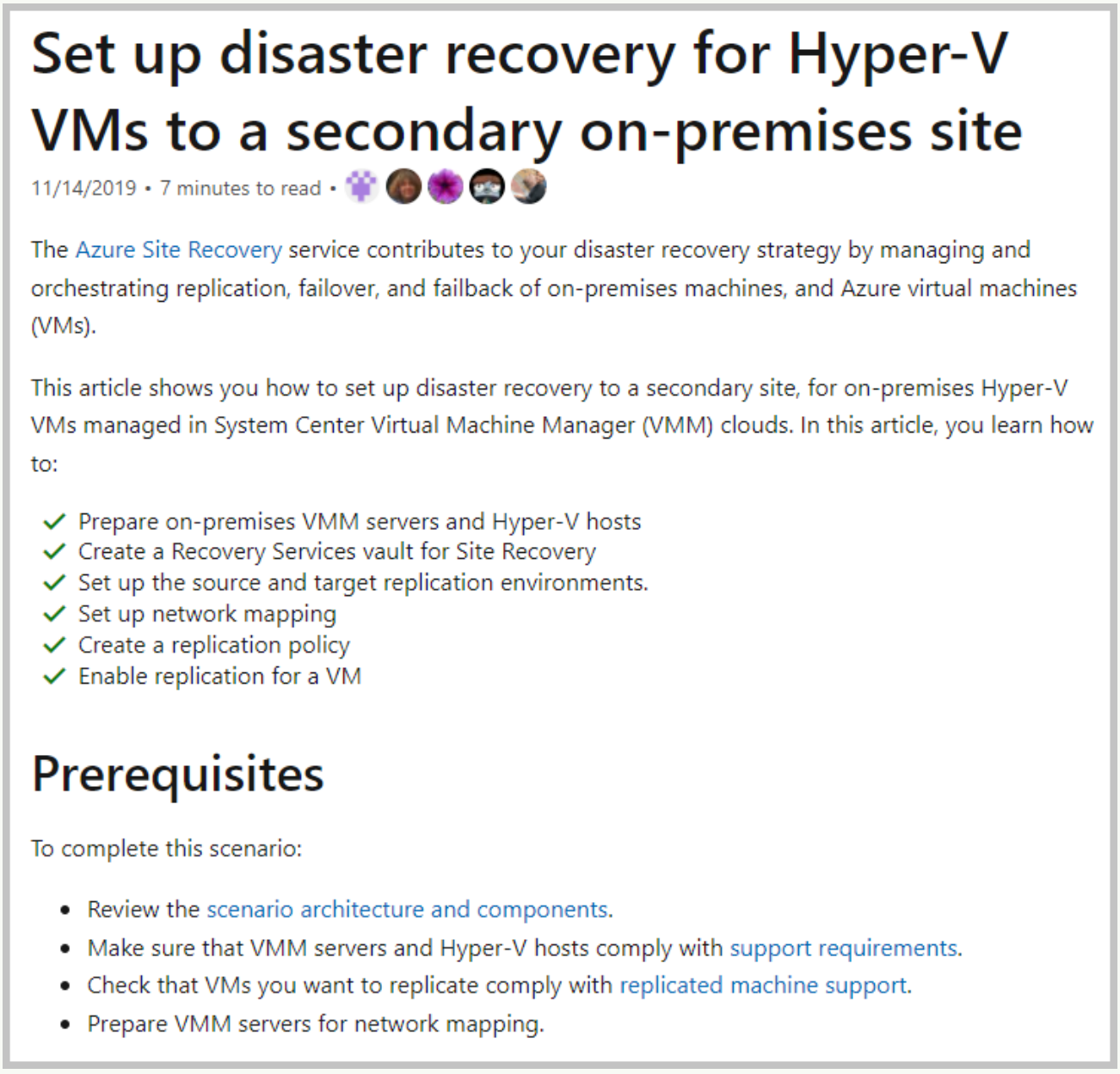
? Then, install the Provider on the other nodes. Cluster nodes should all run the same version of the Provider.

Note: During Site Recovery deployment, you gather Hyper-V hosts and clusters into Hyper-V sites. You install the Azure Site Recovery Provider and Recovery Services agent on each standalone Hyper-V host, or on each Hyper-V cluster node.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-vmm-disaster-recovery

https://developer.microsoft.com/en-us/graph/blogs/retrieving-azure-ad-access-reviews/



Set up disaster recovery for Hyper-V VMs to a secondary on-premises site

11/14/2019 • 7 minutes to read •

The Azure Site Recovery service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and failback of on-premises machines, and Azure virtual machines (VMs).

This article shows you how to set up disaster recovery to a secondary site, for on-premises Hyper-V VMs managed in System Center Virtual Machine Manager (VMM) clouds. In this article, you learn how to:

- ✓ Prepare on-premises VMM servers and Hyper-V hosts
- ✓ Create a Recovery Services vault for Site Recovery
- ✓ Set up the source and target replication environments.
- ✓ Set up network mapping
- ✓ Create a replication policy
- ✓ Enable replication for a VM

Prerequisites

To complete this scenario:

- Review the scenario architecture and components.
- Make sure that VMM servers and Hyper-V hosts comply with support requirements.
- Check that VMs you want to replicate comply with replicated machine support.
- Prepare VMM servers for network mapping.

60. Question

You are designing a message application that will run on an on-premises Ubuntu virtual machine. The application will use Azure Storage queues.

You need to recommend a processing solution for the application to interact with the storage queues. The solution must meet the following requirements:

? Create and delete queues daily.

? Be scheduled by using a CRON job.

? Upload messages every five minutes.

What should developers use to interact with the queues?

- A. Azure CLI
- B. AzCopy
- C. Azure Data Factory
- D. .NET Core

Incorrect

Build applications using .NET Core to communicate with storage queues.

Incorrect Answers:

A. Azure CLI

The Azure CLI is a cross-platform command-line tool to connect to Azure and execute administrative commands on Azure resources.

B. AzCopy

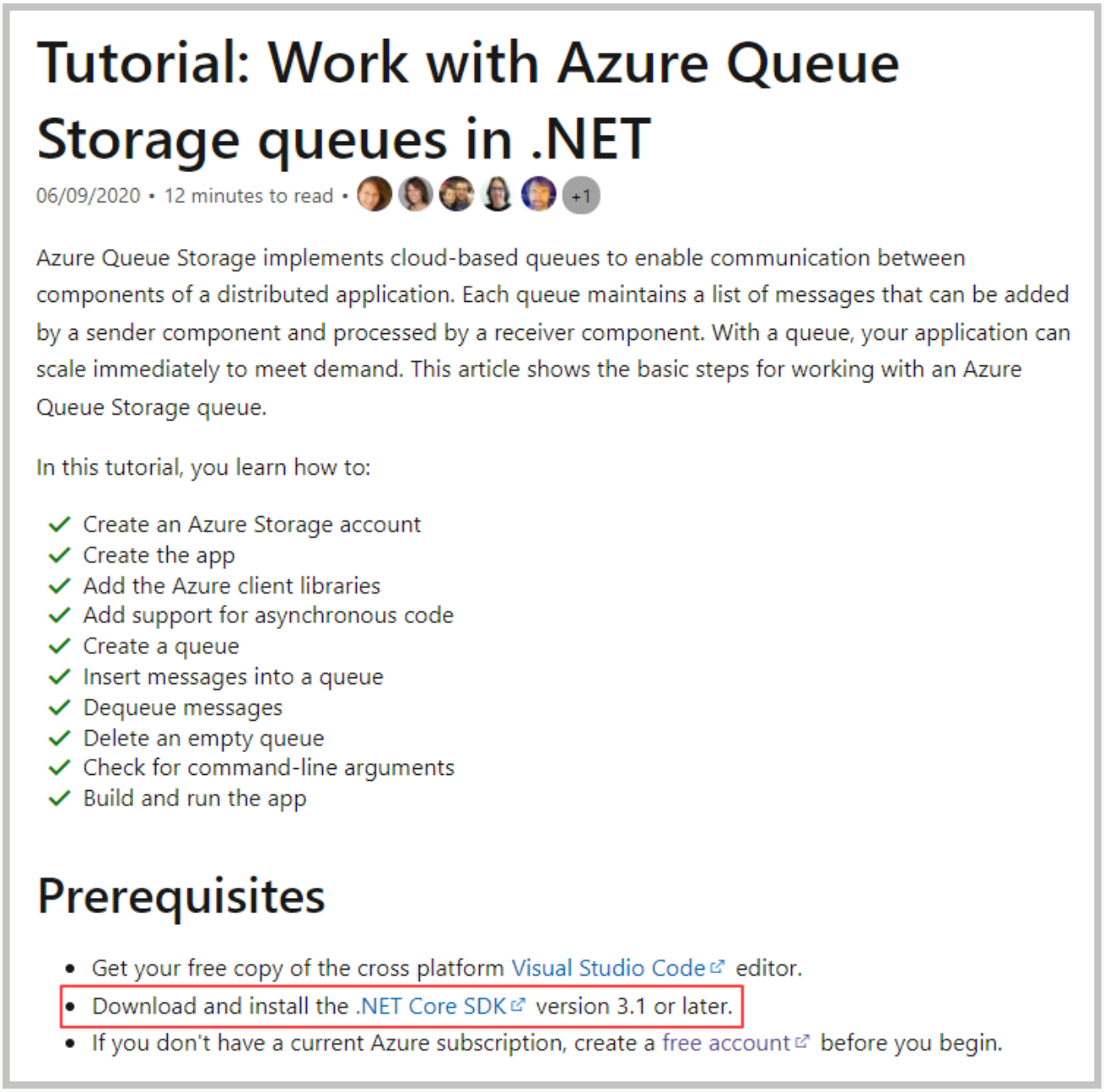
AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

C. Azure Data Factory

Azure Data Factory is Azure's cloud ETL service for scale-out serverless data integration and data transformation.

Reference:

https://docs.microsoft.com/en-us/azure/storage/queues/storage-tutorial-queues



Tutorial: Work with Azure Queue Storage queues in .NET

06/09/2020 • 12 minutes to read • +1

Azure Queue Storage implements cloud-based queues to enable communication between components of a distributed application. Each queue maintains a list of messages that can be added by a sender component and processed by a receiver component. With a queue, your application can scale immediately to meet demand. This article shows the basic steps for working with an Azure Queue Storage queue.

In this tutorial, you learn how to:

- ✓ Create an Azure Storage account
- ✓ Create the app
- ✓ Add the Azure client libraries
- ✓ Add support for asynchronous code
- ✓ Create a queue
- ✓ Insert messages into a queue
- ✓ Dequeue messages
- ✓ Delete an empty queue
- ✓ Check for command-line arguments
- ✓ Build and run the app

Prerequisites

- Get your free copy of the cross platform Visual Studio Code editor.
- Download and install the .NET Core SDK version 3.1 or later.
- If you don't have a current Azure subscription, create a free account before you begin.

61. Question

You have a .NET web service named Service1 that has the following requirements:

? Must read and write temporary files to the local file system.

? Must write to the Application event log.

You need to recommend a solution to host Service1 in Azure. The solution must meet the following requirements:

? Minimize maintenance overhead.

? Minimize costs.

What should you include in the recommendation?

- A. an App Service Environment
- B. an Azure web app
- C. an Azure virtual machine scale set

D. an Azure function

Correct

Azure provides built-in diagnostics to assist with debugging an App Service app.

There are three main types of files that an Azure Web App can deal with

? Persisted files

? Temporary files

? Machine level read-only files

Logs messages generated by your application code. The messages can be generated by the web framework you choose, or from your application code directly using the standard logging pattern of your language. Each message is assigned one of the following

categories: Critical, Error, Warning, Info, Debug, and Trace. You can select how verbose you want the logging to be by setting the severity level when you enable application logging.

Incorrect Answers:

A. an App Service Environment

The Azure App Service Environment is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale.

C. an Azure virtual machine scale set

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. in this scenario, there is no need to load balance.

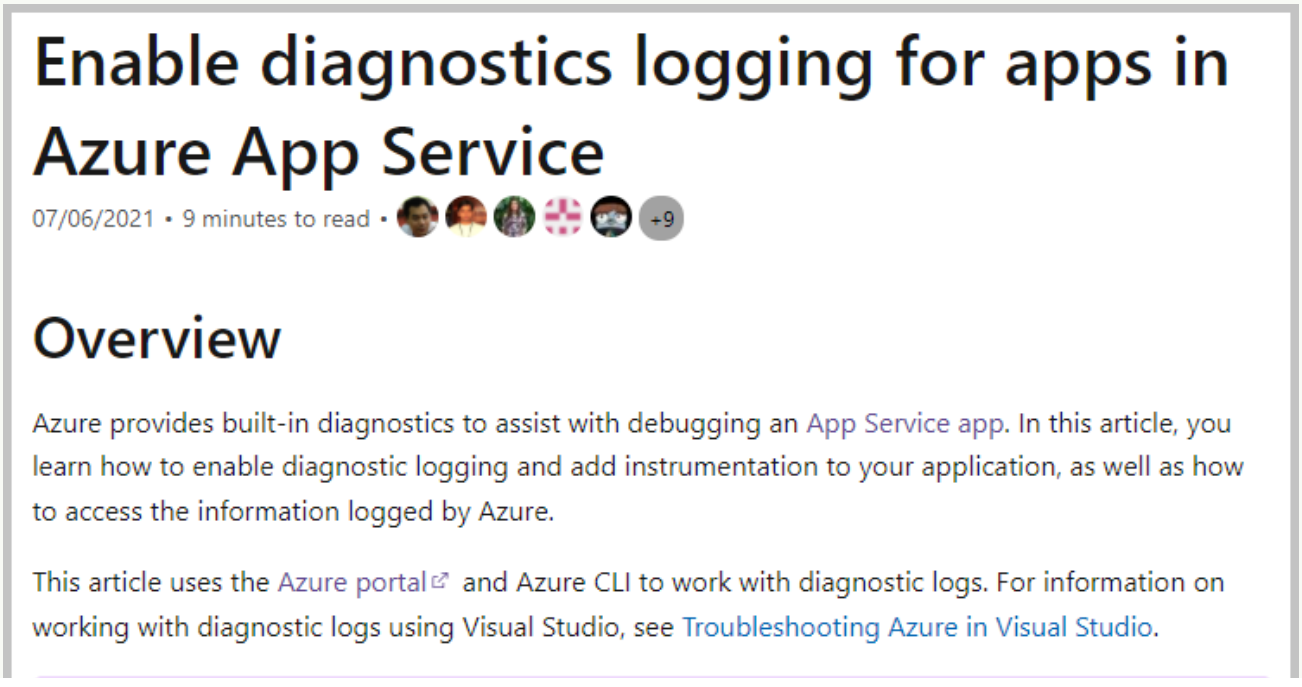
D. an Azure function

Azure Functions is a cloud service available on-demand that provides all the continually updated infrastructure and resources needed to run your applications.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs

https://github.com/projectkudu/kudu/wiki/Understanding-the-Azure-App-Service-file-system



Enable diagnostics logging for apps in Azure App Service

07/06/2021 • 9 minutes to read • +9

Overview

Azure provides built-in diagnostics to assist with debugging an App Service app. In this article, you learn how to enable diagnostic logging and add instrumentation to your application, as well as how to access the information logged by Azure.

This article uses the Azure portal and Azure CLI to work with diagnostic logs. For information on working with diagnostic logs using Visual Studio, see Troubleshooting Azure in Visual Studio.

> ⓘ Note
>
> In addition to the logging instructions in this article, there's new, integrated logging capability with Azure Monitoring. You'll find more on this capability in the **Send logs to Azure Monitor (preview)** section.

Type	Platform	Location	Description
Application logging	Windows, Linux	App Service file system and/or Azure Storage blobs	Logs messages generated by your application code. The messages can be generated by the web framework you choose, or from your application code directly using the standard logging pattern of your language. Each message is assigned one of the following categories: **Critical**, **Error**, **Warning**, **Info**, **Debug**, and **Trace**. You can select how verbose you want the logging to be by setting the severity level when you enable application logging.
Web server logging	Windows	App Service file system or Azure Storage blobs	Raw HTTP request data in the W3C extended log file format. Each log message includes data such as the HTTP method, resource URI, client IP, client port, user agent, response code, and so on.
Detailed Error Messages	Windows	App Service file system	Copies of the *.htm* error pages that would have been sent to the client browser. For security reasons, detailed error pages shouldn't be sent to clients in production, but App Service can save the error page each time an application error occurs that has HTTP code 400 or greater. The page may contain information that can help determine why the server returns the error code.
Failed request tracing	Windows	App Service file system	Detailed tracing information on failed requests, including a trace of the IIS components used to process the request and the time taken in each component. It's useful if you want to improve site performance or isolate a specific HTTP error. One folder is generated for each failed request, which contains the XML log file, and the XSL stylesheet to view the log file with.
Deployment logging	Windows, Linux	App Service file system	Logs for when you publish content to an app. Deployment logging happens automatically and there are no configurable settings for deployment logging. It helps you determine why a deployment failed. For example, if you use a custom deployment script, you might use deployment logging to determine why the script is failing.

> ⓘ Note
>
> App Service provides a dedicated, interactive diagnostics tool to help you troubleshoot your application. For more information, see **Azure App Service diagnostics overview**.
>
> In addition, you can use other Azure services to improve the logging and monitoring capabilities of your app, such as **Azure Monitor**.

62. Question

You are designing a network connectivity strategy for a new Azure subscription. You identify the following requirements:

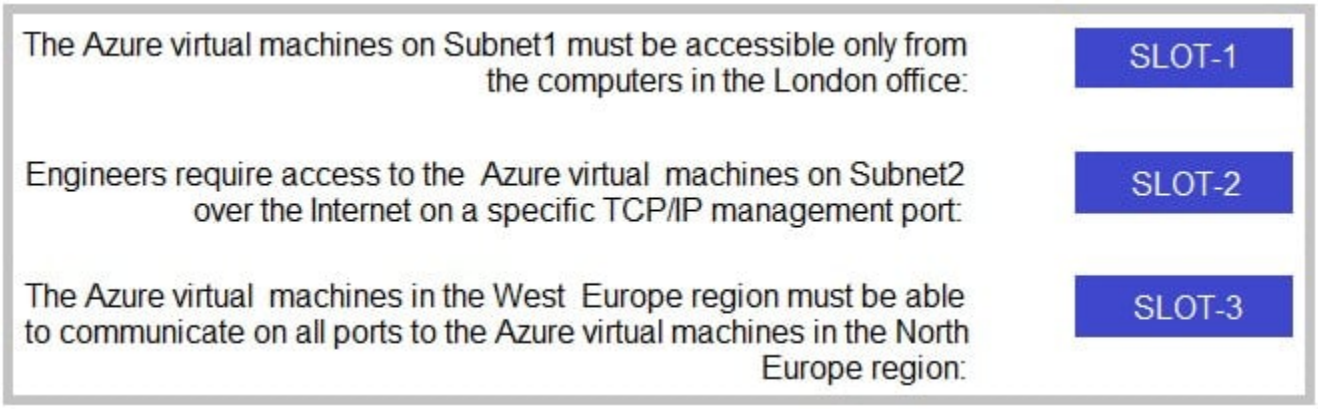
? The Azure virtual machines on a subnet named Subnet1 must be accessible only from the computers in your London office.

? Engineers require access to the Azure virtual machines on a subnet named Subnet2 over the Internet on a specific TCP/IP management port.

? The Azure virtual machines in the West Europe Azure region must be able to communicate on all ports to the Azure virtual machines in the North Europe Azure region.

? Azure virtual machines on Subnet1 and Subnet2 have public IP addresses.

You need to recommend which components must be used to meet the requirements. The solution must minimize costs and administrative effort whenever possible.



Which of the following would go into Slot1?

- A. An Azure ExpressRoute connection
- B. A network security group (NSG)
- C. A new virtual network
- D. A site-to-site VPN
- E. Virtual network peering

Correct

A VPN device is required to configure a Site-to-Site (S2S) cross-premises VPN connection using a VPN gateway.

Site-to-Site connections can be used to create a hybrid solution, or whenever you want secure connections between your on-premises networks and your virtual networks.

Incorrect Answers:

A. An Azure ExpressRoute connection

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet and they offer more reliability, faster speeds and lower latencies than typical Internet connections. This is an expensive option and involves significant administrative effort.

B. A network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

C. A new virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

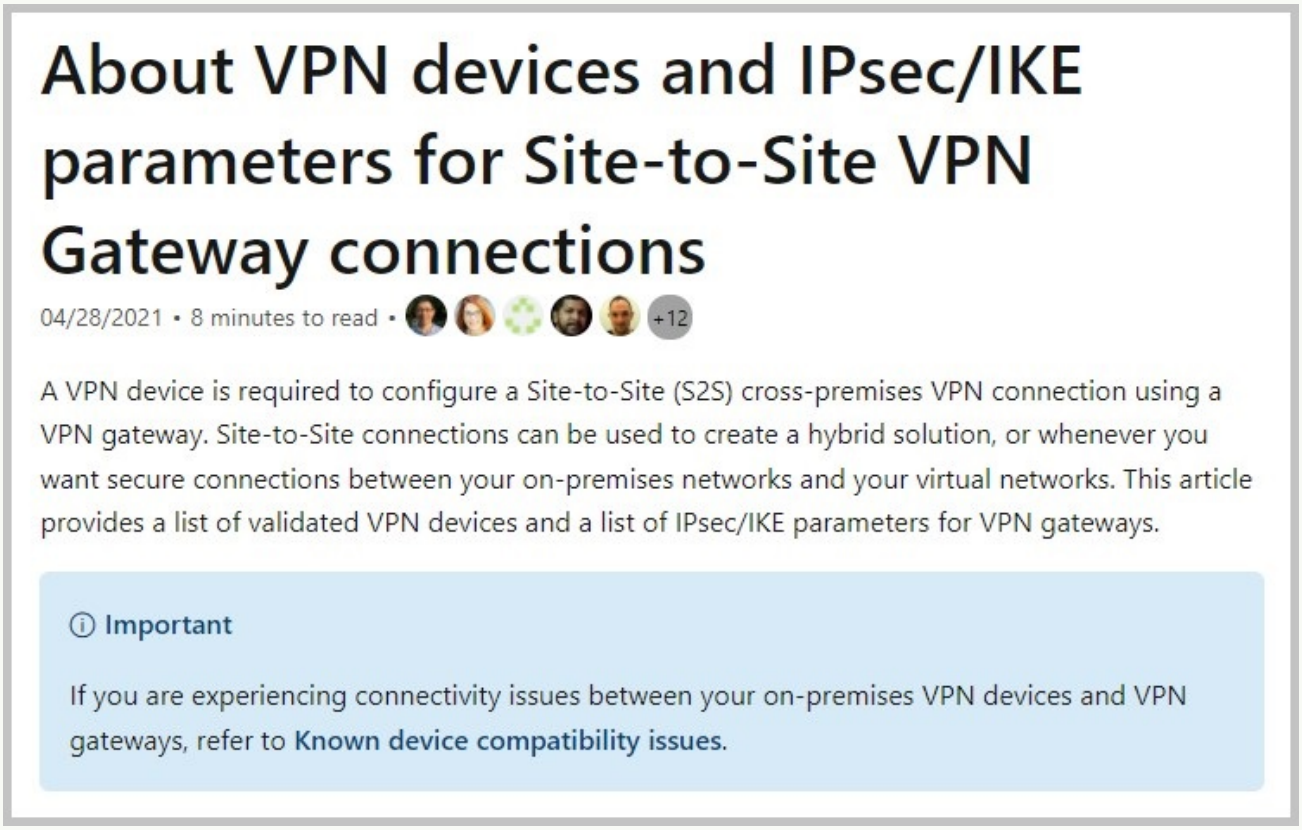
E. Virtual network peering

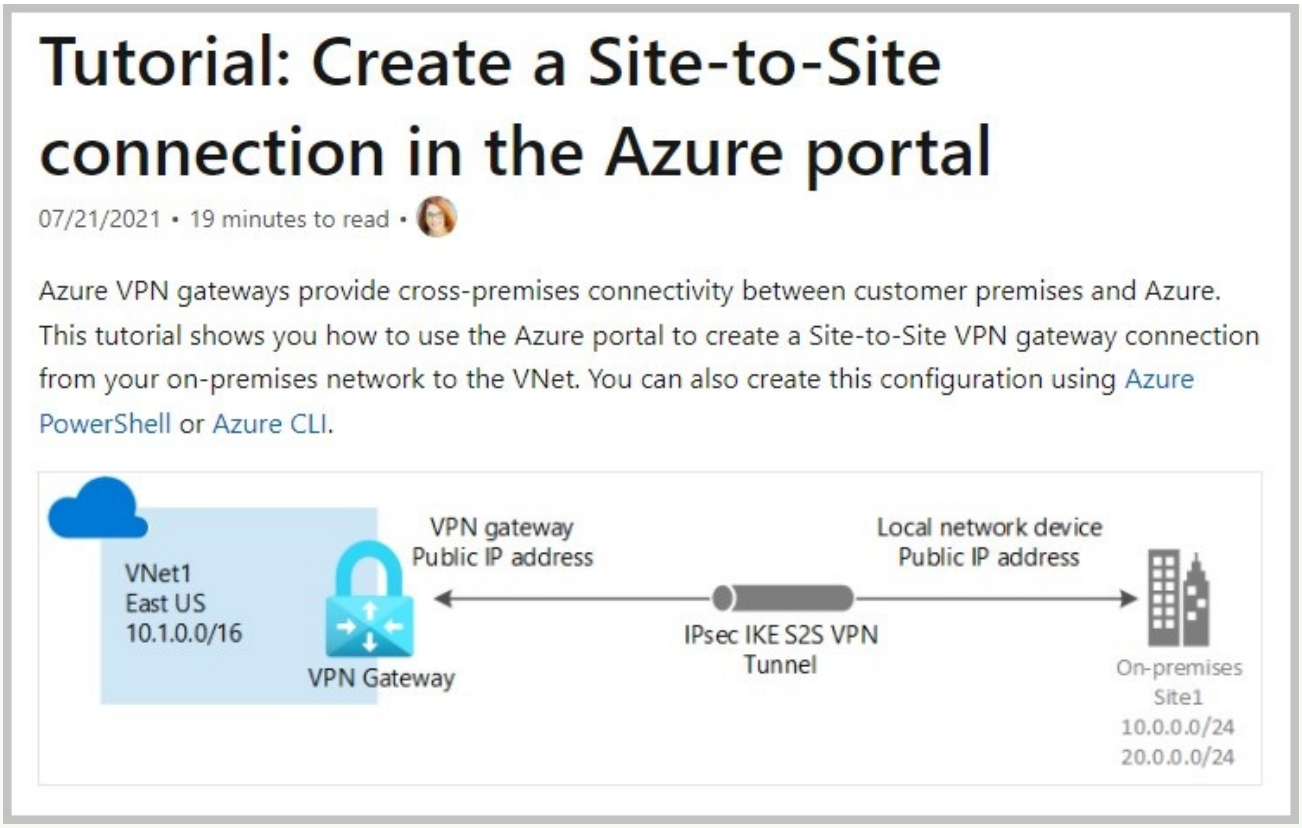
Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices

https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal





63. Question

You are designing a network connectivity strategy for a new Azure subscription. You identify the following requirements:

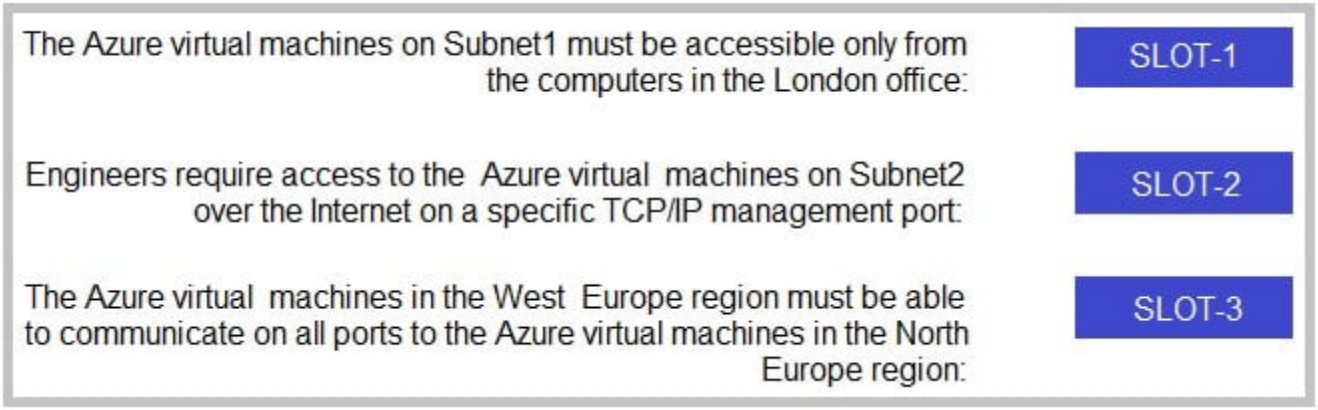
? The Azure virtual machines on a subnet named Subnet1 must be accessible only from the computers in your London office.

? Engineers require access to the Azure virtual machines on a subnet named Subnet2 over the Internet on a specific TCP/IP management port.

? The Azure virtual machines in the West Europe Azure region must be able to communicate on all ports to the Azure virtual machines in the North Europe Azure region.

? Azure virtual machines on Subnet1 and Subnet2 have public IP addresses.

You need to recommend which components must be used to meet the requirements. The solution must minimize costs and administrative effort whenever possible.



Which of the following would go into Slot2?

A. An Azure ExpressRoute connection

B. A network security group (NSG)

C. A new virtual network

D. A site-to-site VPN

E. Virtual network peering

Correct

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Incorrect Answers:

A. An Azure ExpressRoute connection

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don‘t go over the public Internet and they offer more reliability, faster speeds and lower latencies than typical Internet connections. This is an expensive option and involves significant administrative effort.

C. A new virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you‘d operate in your own data center, but brings with it additional benefits of Azure‘s infrastructure such as scale, availability, and isolation.

D. A site-to-site VPN

Site-to-Site connections can be used to create a hybrid solution, or whenever you want secure connections between your on-premises networks and your virtual networks.

E. Virtual network peering

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft‘s private network only.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Network security groups

09/08/2020 • 9 minutes to read • 

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes properties of a network security group rule, the default security rules that are applied, and the rule properties that you can modify to create an augmented security rule.

Default security rules

Azure creates the following default rules in each network security group that you create:

Inbound

AllowVNetInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowAzureLoadBalancerInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

DenyAllInbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Outbound

AllowVnetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access

65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowInternetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

DenyAllOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

64. Question

You are designing a network connectivity strategy for a new Azure subscription. You identify the following requirements:

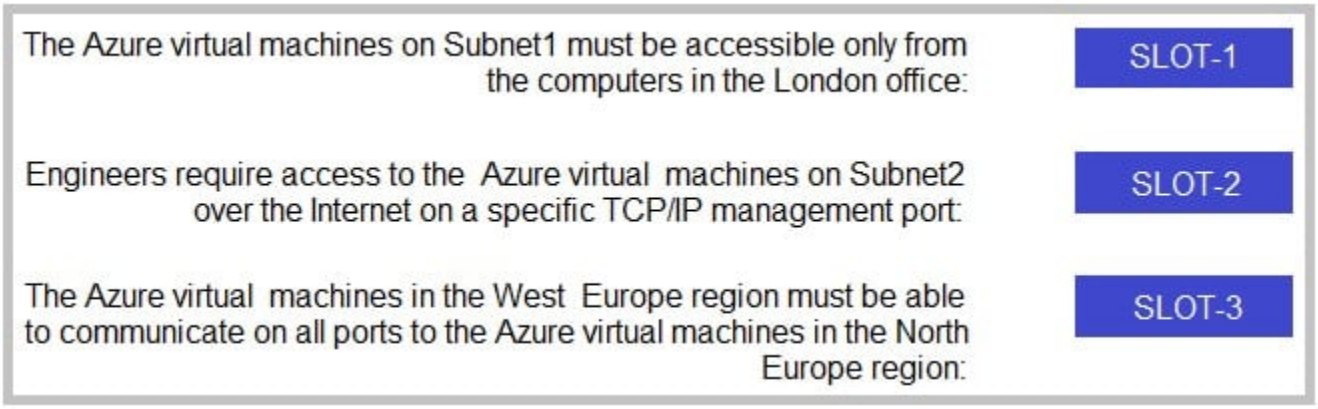
? The Azure virtual machines on a subnet named Subnet1 must be accessible only from the computers in your London office.

? Engineers require access to the Azure virtual machines on a subnet named Subnet2 over the Internet on a specific TCP/IP management port.

? The Azure virtual machines in the West Europe Azure region must be able to communicate on all ports to the Azure virtual machines in the North Europe Azure region.

? Azure virtual machines on Subnet1 and Subnet2 have public IP addresses.

You need to recommend which components must be used to meet the requirements. The solution must minimize costs and administrative effort whenever possible.



Which of the following would go into Slot3?

- A. An Azure ExpressRoute connection
- B. A network security group (NSG)
- C. A new virtual network

D. A site-to-site VPN

E. Virtual network peering

Incorrect

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

Azure supports the following types of peering:

? Virtual network peering: Connect virtual networks within the same Azure region.

? Global virtual network peering: Connecting virtual networks across Azure regions.

Incorrect Answers:

A. An Azure ExpressRoute connection

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet and they offer more reliability, faster speeds and lower latencies than typical Internet connections. This is an expensive option and involves significant administrative effort.

B. A network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

C. A new virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

D. A site-to-site VPN

Site-to-Site connections can be used to create a hybrid solution, or whenever you want secure connections between your on-premises networks and your virtual networks.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

https://azure.microsoft.com/en-us/pricing/details/virtual-network/

Virtual network peering

11/15/2019 • 6 minutes to read • +16

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's *private* network only.

Azure supports the following types of peering:

- **Virtual network peering**: Connect virtual networks within the same Azure region.
- **Global virtual network peering**: Connecting virtual networks across Azure regions.

The benefits of using virtual network peering, whether local or global, include:

- A low-latency, high-bandwidth connection between resources in different virtual networks.
- The ability for resources in one virtual network to communicate with resources in a different virtual network.
- The ability to transfer data between virtual networks across Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions.
- The ability to peer virtual networks created through the Azure Resource Manager.
- The ability to peer a virtual network created through Resource Manager to one created through the classic deployment model. To learn more about Azure deployment models, see Understand Azure deployment models.
- No downtime to resources in either virtual network when creating the peering, or after the peering is created.

Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.

65. Question

You are designing a solution that will include containerized applications running in an Azure Kubernetes Service (AKS) cluster.

You need to recommend a load balancing solution for HTTPS traffic. The solution must meet the following requirements:

? Automatically configure load balancing rules as the applications are deployed to the cluster.

? Support Azure Web Application Firewall (WAF).

? Support cookie-based affinity.

? Support URL routing.

What should you include the recommendation?

- A. an NGINX ingress controller

B. Application Gateway Ingress Controller (AGIC)

C. an HTTP application routing ingress controller

D. the Kubernetes load balancer service

Correct

Much like the most popular Kubernetes Ingress Controllers, the Application Gateway Ingress Controller provides several features, leveraging Azure's native Application Gateway L7 load balancer.

Application Gateway Ingress Controller (AGIC) allows you to use Application Gateway as the ingress for an Azure Kubernetes Service (AKS) cluster.

The ingress controller runs as a pod within the AKS cluster and consumes Kubernetes Ingress Resources and converts them to an Application Gateway configuration, which allows the gateway to load-balance traffic to the Kubernetes pods. The ingress controller only supports Application Gateway Standard_v2 and WAF_v2 SKUs.

Incorrect Answers:

A. an NGINX ingress controller

NGINX Ingress Controller is a best-in-class traffic management solution for cloud?native apps in Kubernetes and containerized environments.

C. an HTTP application routing ingress controller

The HTTP application routing solution makes it easy to access applications that are deployed to your Azure Kubernetes Service (AKS) cluster. When the solution's enabled, it configures an Ingress controller in your AKS cluster. As applications are deployed, the solution also creates publicly accessible DNS names for application endpoints.

D. the Kubernetes load balancer service

The Kubernetes load balancer sends connections to the first server in the pool until it is at capacity, and then sends new connections to the next available server. To take advantage of the load balancer that is available in your host environment, simply edit your service configuration file to set the type field to LoadBalancer. You will also need to specify a port value for the port field.

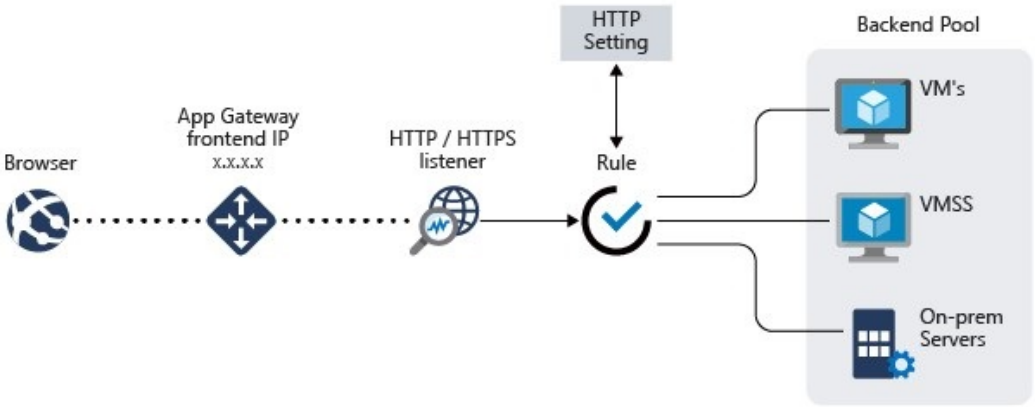
Reference:

https://docs.microsoft.com/en-us/azure/application-gateway/features

Azure Application Gateway features

09/25/2020 • 8 minutes to read •

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.



Ingress Controller for AKS

Application Gateway Ingress Controller (AGIC) allows you to use Application Gateway as the ingress for an Azure Kubernetes Service (AKS) cluster.

The ingress controller runs as a pod within the AKS cluster and consumes Kubernetes Ingress Resources and converts them to an Application Gateway configuration, which allows the gateway to load-balance traffic to the Kubernetes pods. The ingress controller only supports Application Gateway Standard_v2 and WAF_v2 SKUs.

For more information, see Application Gateway Ingress Controller (AGIC).

Use Page numbers below to navigate to other practice tests

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

← Previous Post

Next Post →

We help you to succeed in your certification exams

We have helped over thousands of working professionals to achieve their certification goals with our practice tests.

Skillcertpro

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY