SKILLCERTPRO

IT CERTIFICATION TRAININGS

0

Microsoft Azure / By SkillCertPro

Practice Set 13

Your results are here!! for" Microsoft Azure AZ-305 Practice Test 13 "

51 of 65 questions answered correctly

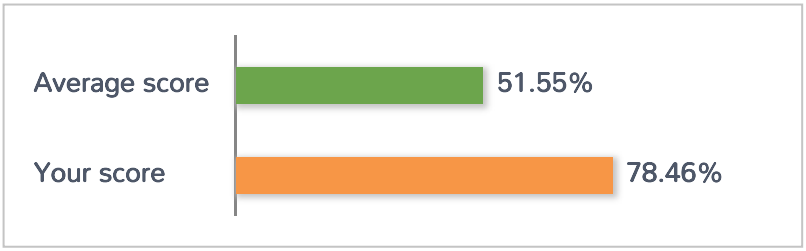
Your time: 03:09:05

Your Final Score is : 51

You have attempted : 65

Number of Correct Questions : 51 and scored 51

Number of Incorrect Questions : 14 and Negative marks 0

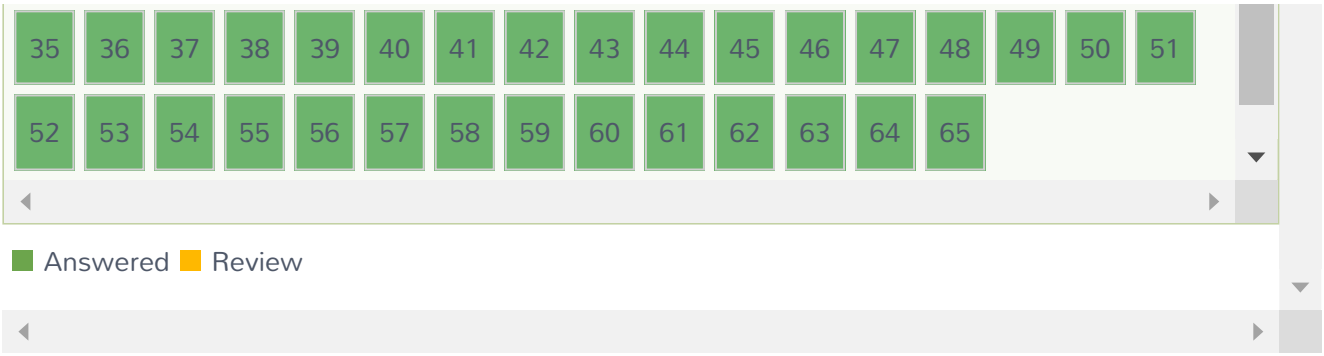


You can review your answers by clicking on “View Answers” option.

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 need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.

What should you include in the recommendation?

- A. the Change Tracking management solution
- B. Application Insights
- C. Azure Monitor action groups
- D. Azure Activity Log

Correct

Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.

Through activity logs, you can determine:

? what operations were taken on the resources in your subscription

? who started the operation

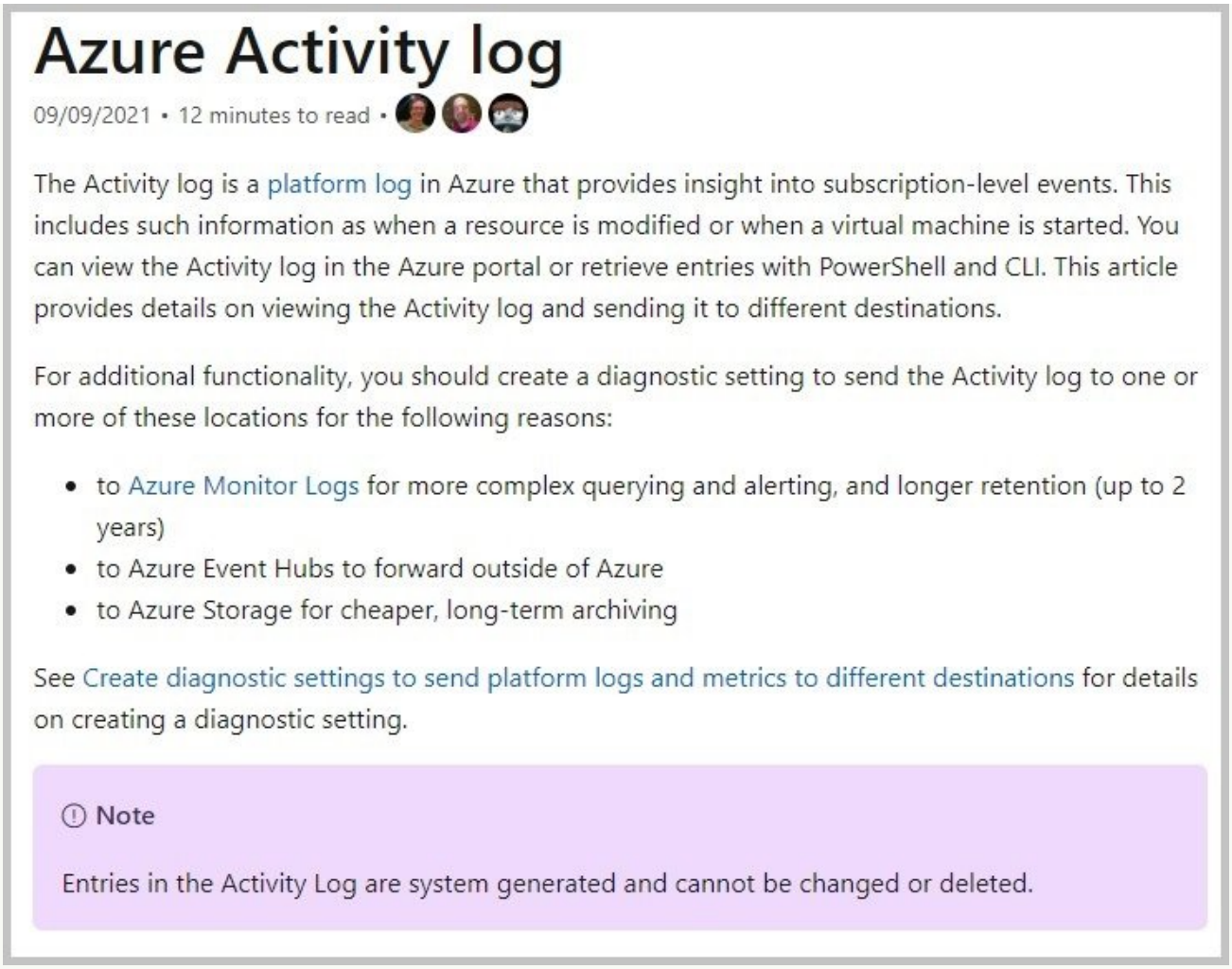
? when the operation occurred

? the status of the operation

? the values of other properties that might help you research the operation

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs



Azure Activity log

09/09/2021 • 12 minutes to read •

The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started. You can view the Activity log in the Azure portal or retrieve entries with PowerShell and CLI. This article provides details on viewing the Activity log and sending it to different destinations.

For additional functionality, you should create a diagnostic setting to send the Activity log to one or more of these locations for the following reasons:

- to Azure Monitor Logs for more complex querying and alerting, and longer retention (up to 2 years)
- to Azure Event Hubs to forward outside of Azure
- to Azure Storage for cheaper, long-term archiving

See Create diagnostic settings to send platform logs and metrics to different destinations for details on creating a diagnostic setting.

Note

Entries in the Activity Log are system generated and cannot be changed or deleted.

2. Question

You have an Azure App Service Web App that includes Azure Blob storage and an Azure SQL Database instance. The application is instrumented by using the Application Insights SDK.

You need to design a monitoring solution for the web app.

Which Azure monitoring service should you use for the following?

Correlate Azure resource usage and performance data with application configuration and performance data

- A. Azure Application Insights
- B. Azure Service Map
- C. Azure Log Analytics
- D. Azure Activity Log

Correct

Log Analytics helps correlate the usage and performance data collected by Application Insights with configuration and performance data across the Azure resources that support the app.

Incorrect Answers:

A. Azure Application Insights

It is used 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. It's designed to help you continuously improve performance and usability.

B. Azure Service Map

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services.

D. Azure Activity Log

The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/custom-data-correlation

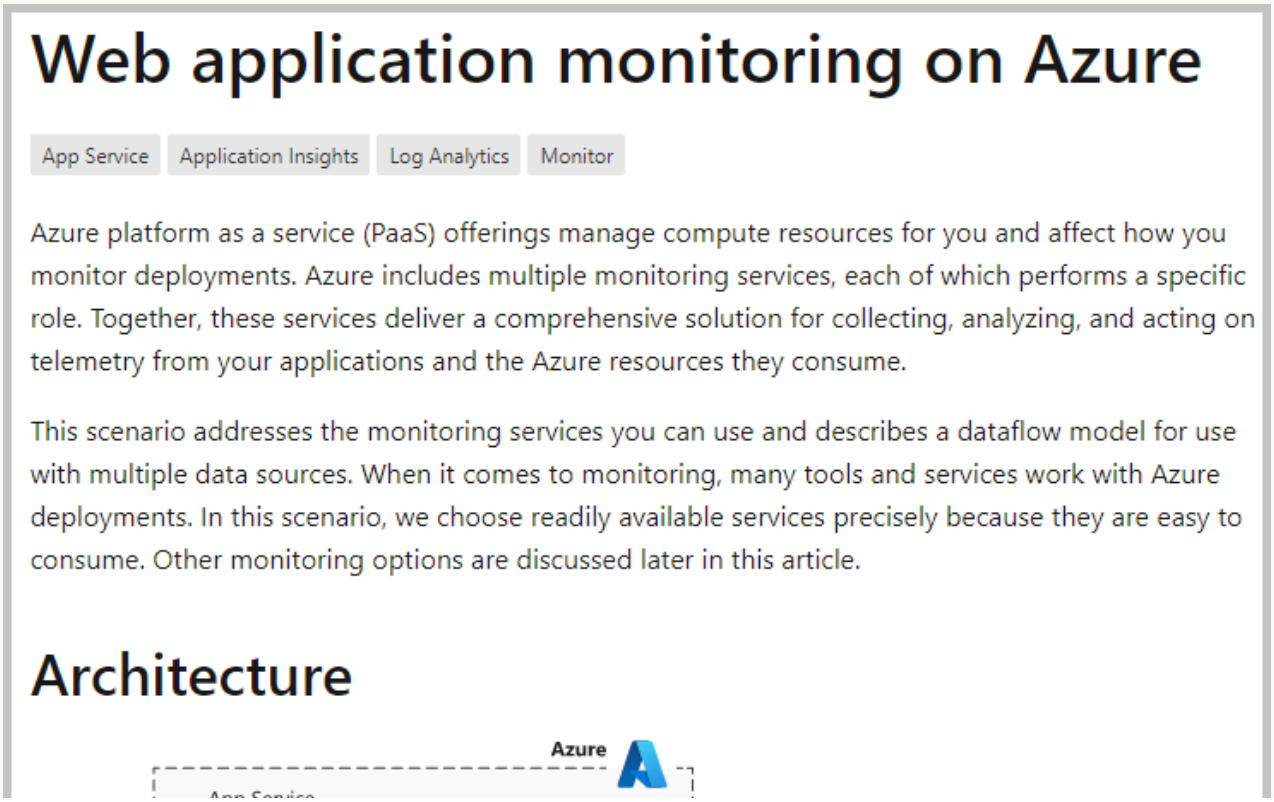
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/app-service-web-app/app-monitoring

Correlating Application Insights data with custom data sources

08/08/2018 • 2 minutes to read • +2

Application Insights collects several different data types: exceptions, traces, page views, and others. While this is often sufficient to investigate your application's performance, reliability, and usage, there are cases when it is useful to correlate the data stored in Application Insights to other completely custom datasets.



Web application monitoring on Azure

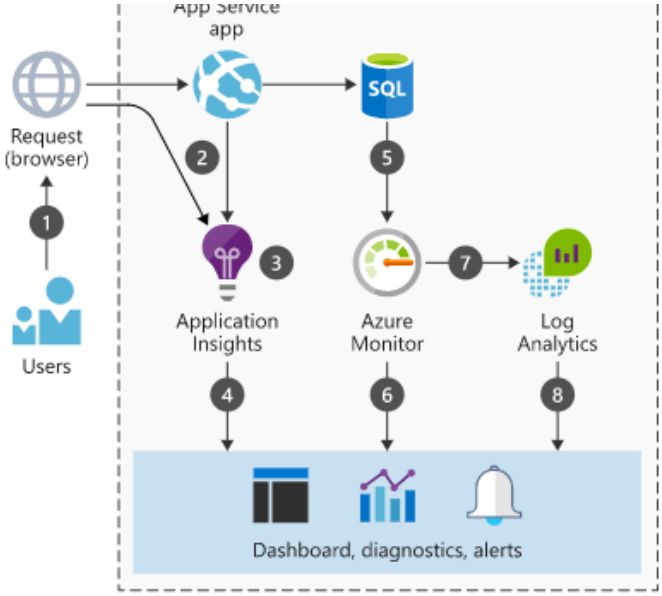
App Service | Application Insights | Log Analytics | Monitor

Azure platform as a service (PaaS) offerings manage compute resources for you and affect how you monitor deployments. Azure includes multiple monitoring services, each of which performs a specific role. Together, these services deliver a comprehensive solution for collecting, analyzing, and acting on telemetry from your applications and the Azure resources they consume.

This scenario addresses the monitoring services you can use and describes a dataflow model for use with multiple data sources. When it comes to monitoring, many tools and services work with Azure deployments. In this scenario, we choose readily available services precisely because they are easy to consume. Other monitoring options are discussed later in this article.

Architecture

Azure



Components

- Azure App Service is a PaaS service for building and hosting apps in managed virtual machines. The underlying compute infrastructures on which your apps run is managed for you. App Service provides monitoring of resource usage quotas and app metrics, logging of diagnostic information, and alerts based on metrics. Even better, you can use Application Insights to create availability tests for testing your application from different regions.
- Application Insights is an extensible Application Performance Management (APM) service for developers and supports multiple platforms. It monitors the application, detects application anomalies such as poor performance and failures, and sends telemetry to the Azure portal. Application Insights can also be used for logging, distributed tracing, and custom application metrics.
- Azure Monitor provides base-level infrastructure metrics and logs for most services in Azure. You can interact with the metrics in several ways, including charting them in Azure portal, accessing them through the REST API, or querying them using PowerShell or CLI. Azure Monitor also offers its data directly into Log Analytics and other services, where you can query and combine it with data from other sources on premises or in the cloud.
- Log Analytics helps correlate the usage and performance data collected by Application Insights with configuration and performance data across the Azure resources that support the app. This scenario uses the Azure Log Analytics agent to push SQL Server audit logs into Log Analytics. You can write queries and view data in the Log Analytics blade of the Azure portal.

3. Question

You have an Azure App Service Web App that includes Azure Blob storage and an Azure SQL Database instance. The application is instrumented by using the Application Insights SDK.

You need to design a monitoring solution for the web app.

Which Azure monitoring service should you use for the following?

Visualize the relationships between application components

- A. Azure Application Insights

B. Azure Service Map

C. Azure Log Analytics

D. Azure Activity Log

Correct

Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. You can see the full application topology across multiple levels of related application components. Components could be different Application Insights resources, or different roles in a single resource. The app map finds components by following HTTP dependency calls made between servers with the Application Insights SDK installed.

Incorrect Answers:

B. Azure Service Map

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services.

C. Azure Log Analytics

Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor Logs and interactively analyze their results.

D. Azure Activity Log

The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map?tabs=net

Application Map: Triage Distributed Applications

03/15/2019 • 8 minutes to read • +14

Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status. You can click through from any component to more detailed diagnostics, such as Application Insights events. If your app uses Azure services, you can also click through to Azure diagnostics, such as SQL Database Advisor recommendations.

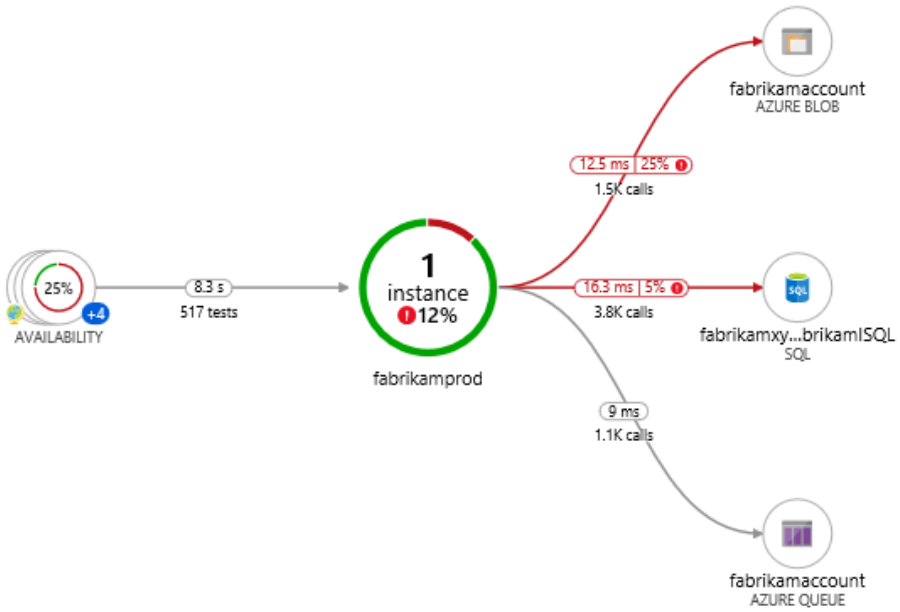
Composite Application Map

You can see the full application topology across multiple levels of related application components. Components could be different Application Insights resources, or different roles in a single resource. The app map finds components by following HTTP dependency calls made between servers with the Application Insights SDK installed.

This experience starts with progressive discovery of the components. When you first load the application map, a set of queries is triggered to discover the components related to this component. A button at the top-left corner will update with the number of components in your application as they are discovered.

On clicking "Update map components", the map is refreshed with all components discovered until that point. Depending on the complexity of your application, this may take a minute to load.

If all of the components are roles within a single Application Insights resource, then this discovery step is not required. The initial load for such an application will have all its components.



4. Question

You have an Azure App Service Web App that includes Azure Blob storage and an Azure SQL Database instance. The application is instrumented by using the Application Insights SDK.

You need to design a monitoring solution for the web app.

Which Azure monitoring service should you use for the following?

Track requests and exceptions to a specific line of code within the application

- A. Azure Application Insights
- B. Azure Service Map
- C. Azure Log Analytics
- D. Azure Activity Log

Correct

Application Insights, a feature of Azure Monitor, 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. It's designed to help you continuously improve performance and usability. It works for apps on a wide variety of platforms including .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

Incorrect Answers:

B. Azure Service Map

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services.

C. Azure Log Analytics

Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor Logs and interactively analyze their results.

D. Azure Activity Log

The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

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

What is Application Insights?

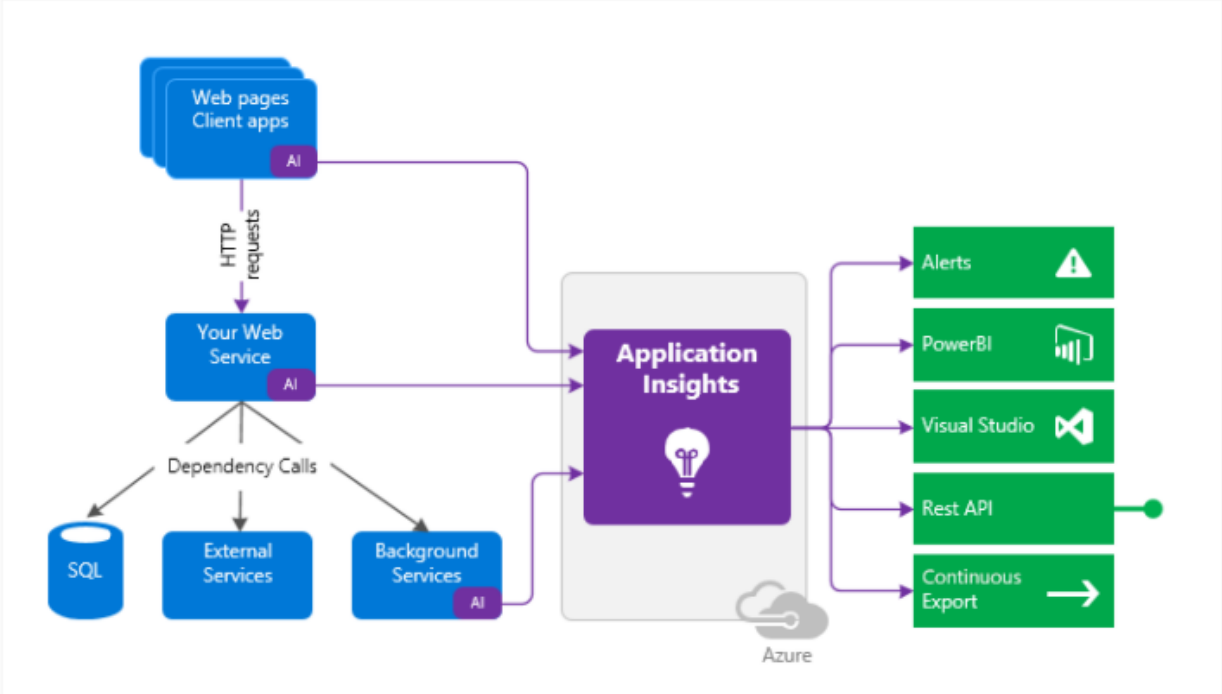
06/03/2019 • 5 minutes to read • +10

Application Insights, a feature of Azure Monitor, 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. It's designed to help you continuously improve performance and usability. It works for apps on a wide variety of platforms including .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

How does Application Insights work?

You install a small instrumentation package (SDK) in your application or enable Application Insights using the Application Insights Agent when supported. The instrumentation monitors your app and directs the telemetry data to an Azure Application Insights Resource using a unique GUID that we refer to as an Instrumentation Key.

You can instrument not only the web service application, but also any background components, and the JavaScript in the web pages themselves. The application and its components can run anywhere - it doesn't have to be hosted in Azure.



5. Question

You have an Azure App Service Web App that includes Azure Blob storage and an Azure SQL Database instance. The application is instrumented by using the Application Insights SDK.

You need to design a monitoring solution for the web app.

Which Azure monitoring service should you use for the following?

Analyze how many users return to the application and how often they select a particular dropdown value

- A. Azure Application Insights
- B. Azure Service Map
- C. Azure Log Analytics
- D. Azure Activity Log

Correct

Custom events and metrics in App insights allow you write yourself in the client or server code, to track business events such as items sold or games won.

Incorrect Answers:

B. Azure Service Map

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services.

C. Azure Log Analytics

Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor Logs and interactively analyze their results.

D. Azure Activity Log

The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started.

Reference:

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

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

What is Application Insights?

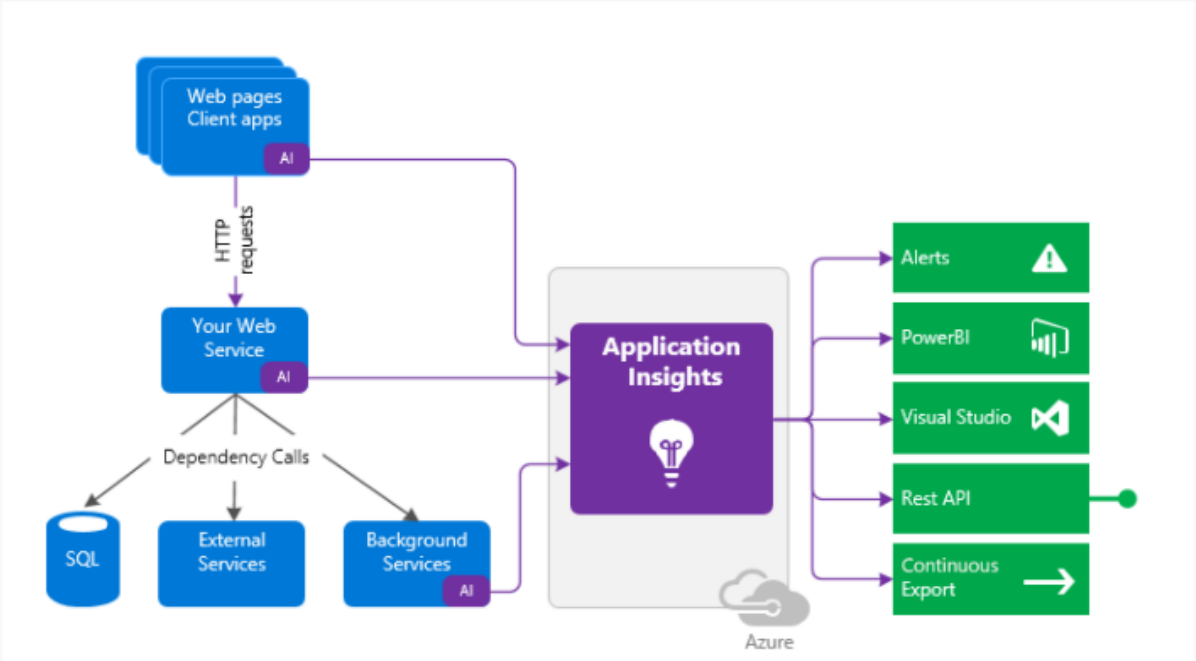
06/03/2019 • 5 minutes to read • +10

Application Insights, a feature of Azure Monitor, 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. It's designed to help you continuously improve performance and usability. It works for apps on a wide variety of platforms including .NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

How does Application Insights work?

You install a small instrumentation package (SDK) in your application or enable Application Insights using the Application Insights Agent when supported. The instrumentation monitors your app and directs the telemetry data to an Azure Application Insights Resource using a unique GUID that we refer to as an Instrumentation Key.

You can instrument not only the web service application, but also any background components, and the JavaScript in the web pages themselves. The application and its components can run anywhere - it doesn't have to be hosted in Azure.



6. Question

You are designing an Azure resource deployment that will use Azure Resource Manager templates. The deployment will use Azure Key Vault to store secrets.

You need to recommend a solution to meet the following requirements:

? Prevent the IT staff that will perform the deployment from retrieving the secrets directly from Key Vault.

? Use the principle of least privilege.

Which two actions should you recommend?

- [ ] A. Create a Key Vault access policy that allows all get key permissions, get secret permissions, and get certificate permissions
- [ ] **B. From Access policies in Key Vault, enable access to the Azure Resource Manager for template deployment**
- [ ] C. Create a Key Vault access policy that allows all list key permissions, list secret permissions, and list certificate permissions
- [x] **D. Assign the IT staff a custom role that includes the Microsoft.KeyVault/Vaults/Deploy/Action permission**
- [ ] E. Assign the Key Vault Contributor role to the IT staff

Incorrect

Instead of putting a secure value (like a password) directly in your template or parameter file, you can retrieve the value from an Azure Key Vault during a deployment. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID.

To access a key vault during template deployment, set enabledForTemplateDeployment on the key vault to true

If you already have a key vault, make sure it allows template deployments.

az keyvault update –name ExampleVault –enabled-for-template-deployment true

The user who deploys the template must have the Microsoft.KeyVault/vaults/deploy/action permission for the scope of the resource group and key vault.

{

“Name“: “Key Vault resource manager template deployment operator“,

“IsCustom“: true,

“Description“: “Lets you deploy a resource manager template with the access to the secrets in the Key Vault.“,

“Actions“: [

“Microsoft.KeyVault/vaults/deploy/action“

],

“NotActions“: [],

“DataActions“: [],

“NotDataActions“: [],

“AssignableScopes“: [

“/subscriptions/00000000-0000-0000-0000-000000000000“

]

}

Incorrect Answers:

A. Create a Key Vault access policy that allows all get key permissions, get secret permissions, and get certificate permissions

This is not a recommended option to refer in ARM template deployments.

C. Create a Key Vault access policy that allows all list key permissions, list secret permissions, and list certificate permissions

This is not a recommended option to refer in ARM template deployments.

E. Assign the Key Vault Contributor role to the IT staff

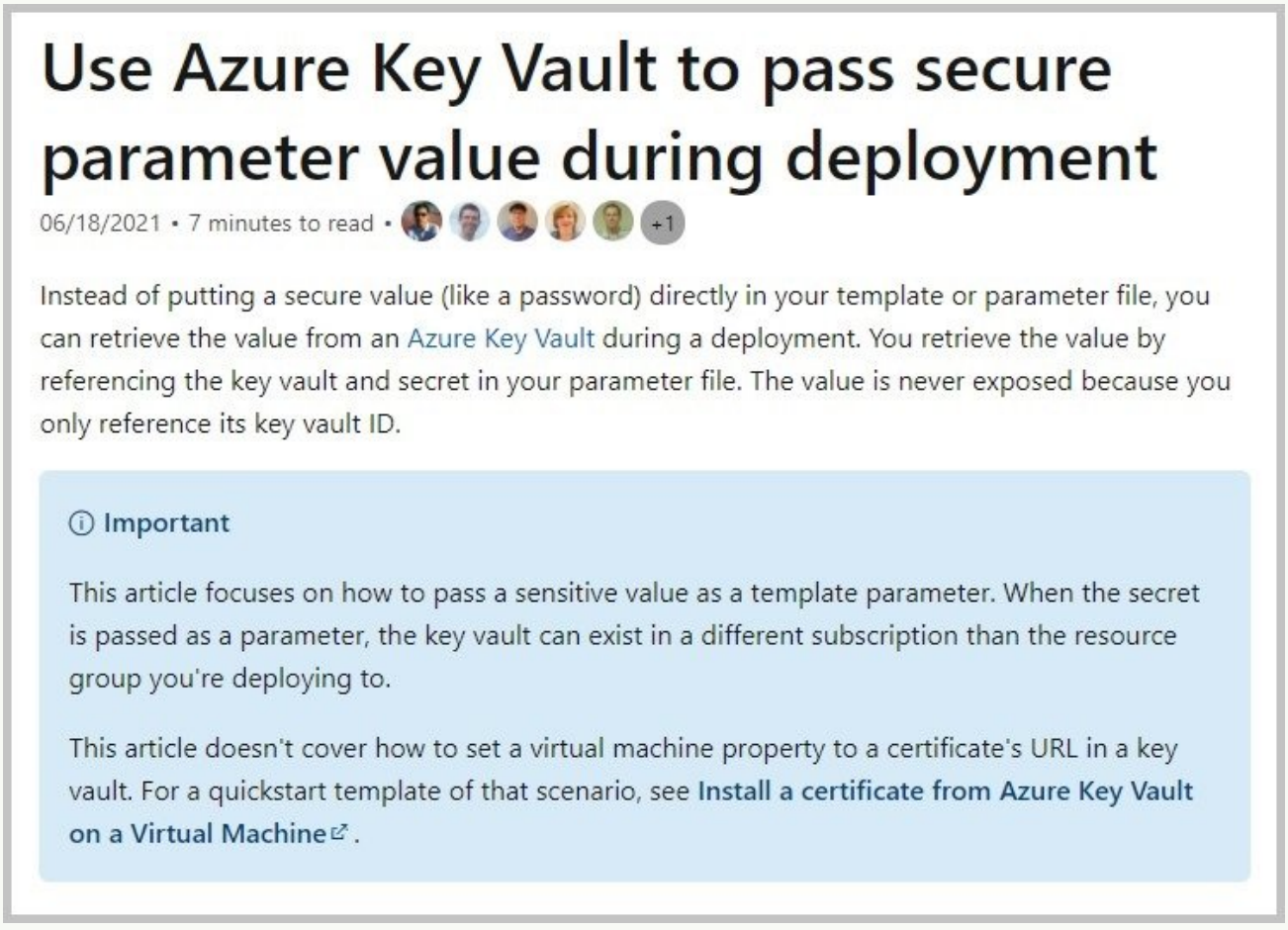
To grant access to a user to manage key vaults, you assign a predefined key vault Contributor role to the user at a specific scope.

If a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has Contributor role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli



Use Azure Key Vault to pass secure parameter value during deployment

06/18/2021 • 7 minutes to read • +1

Instead of putting a secure value (like a password) directly in your template or parameter file, you can retrieve the value from an Azure Key Vault during a deployment. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID.

Important

This article focuses on how to pass a sensitive value as a template parameter. When the secret is passed as a parameter, the key vault can exist in a different subscription than the resource group you're deploying to.

This article doesn't cover how to set a virtual machine property to a certificate's URL in a key vault. For a quickstart template of that scenario, see **Install a certificate from Azure Key Vault on a Virtual Machine**.

7. Question

You have an Azure subscription that contains web apps in three Azure regions.

You need to implement Azure Key Vault to meet the following requirements:

? In the event of a regional outage, all keys must be readable.

? All the web apps in the subscription must be able to access Key Vault.

? The number of Key Vault resources to be deployed and managed must be minimized.

How many instances of Key Vault should you implement?

- A. 1
- B. 2
- C. 3
- D. 4

Incorrect

Azure Key Vault features multiple layers of redundancy to make sure that your keys and secrets remain available to your application even if individual components of the service fail.

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away but within the same geography. This maintains high durability of your keys and secrets. See the Azure paired regions document for details on specific region pairs.

Example: Secrets that must be shared by your application in both Europe West and Europe North. Minimize these as much as you can. Put these in a key vault in either of the two regions. Use the same URI from both regions. Microsoft will fail over the Key Vault service internally.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance

Azure Key Vault availability and redundancy

03/31/2021 • 2 minutes to read • +1

Azure Key Vault features multiple layers of redundancy to make sure that your keys and secrets remain available to your application even if individual components of the service fail.

> **Note**
>
> This guide applies to vaults. Managed HSM pools use a different high availability and disaster recovery model. See **Managed HSM Disaster Recovery Guide** for more information.

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away, but within the same geography to maintain high durability of your keys and secrets. For details about specific region pairs, see Azure paired regions. The exception to the paired regions model is single region geo, for example Brazil South, Qatar Central. Such regions allow only the option to keep data resident within the same region. Both Brazil South and Qatar Central use zone redundant storage (ZRS) to replicate your data three times within the single location/region. For AKV Premium, only 2 of the 3 regions are used to replicate data from the HSM's.

If individual components within the key vault service fail, alternate components within the region step in to serve your request to make sure that there is no degradation of functionality. You don't need to take any action to start this process, it happens automatically and will be transparent to you.

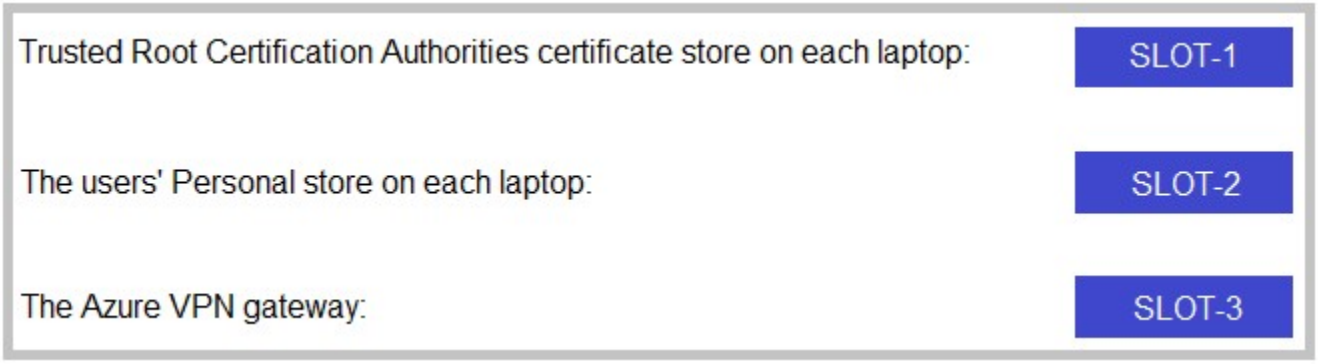
In the rare event that an entire Azure region is unavailable, the requests that you make of Azure Key Vault in that region are automatically routed (*failed over*) to a secondary region except in the case of the Brazil South and Qatar Central region. When the primary region is available again, requests are routed back (*failed back*) to the primary region. Again, you don't need to take any action because this happens automatically.

8. Question

Your company has users who work remotely from laptops.

You plan to move some of the applications accessed by the remote users to Azure virtual machines. The users will access the applications in Azure by using a point-to-site VPN connection. You will use certificates generated from an on-premises-based Certification authority (CA).

You need to recommend which certificates are required for the deployment.



Which of the following would go into Slot1?

- A. A root CA certificate that has the private key
- B. A root CA certificate that has the public key only
- C. A user certificate that has the private key
- D. A user certificate that has the public key only

Incorrect

Certificates are used by Azure to authenticate clients connecting to a VNet over a Point-to-Site VPN connection. Once you obtain a root certificate, you upload the public key information to Azure. The root certificate is then considered 'trusted' by Azure for connection over P2S to the virtual network. You also generate client certificates from the trusted root certificate, and then install them on each client computer. The client certificate is used to authenticate the client when it initiates a connection to the VNet.

Reference:

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

Generate certificates

Certificates are used by Azure to authenticate clients connecting to a VNet over a Point-to-Site VPN connection. Once you obtain a root certificate, you upload the public key information to Azure. The root certificate is then considered 'trusted' by Azure for connection over P2S to the virtual network. You also generate client certificates from the trusted root certificate, and then install them on each client computer. The client certificate is used to authenticate the client when it initiates a connection to the VNet.

Generate a root certificate

Obtain the .cer file for the root certificate. You can use either a root certificate that was generated with an enterprise solution (recommended), or generate a self-signed certificate. After you create the root certificate, export the public certificate data (not the private key) as a Base64 encoded X.509 .cer file. You upload this file later to Azure.

- **Enterprise certificate:** If you're using an enterprise solution, you can use your existing certificate chain. Acquire the .cer file for the root certificate that you want to use.
- **Self-signed root certificate:** If you aren't using an enterprise certificate solution, create a self-signed root certificate. Otherwise, the certificates you create won't be compatible with your P2S connections and clients will receive a connection error when they try to connect. You can use Azure PowerShell, MakeCert, or OpenSSL. The steps in the following articles describe how to generate a compatible self-signed root certificate:
  - Windows 10 PowerShell instructions: These instructions require Windows 10 and PowerShell to generate certificates. Client certificates that are generated from the root certificate can be installed on any supported P2S client.
  - MakeCert instructions: Use MakeCert if you don't have access to a Windows 10 computer to use to generate certificates. Although MakeCert is deprecated, you can still use it to generate certificates. Client certificates that you generate from the root certificate can be installed on any supported P2S client.
  - Linux instructions.

9. Question

Your company has users who work remotely from laptops.

You plan to move some of the applications accessed by the remote users to Azure virtual machines. The users will access the applications in Azure by using a point-to-site VPN connection. You will use certificates generated from an on-premises-based Certification authority (CA).

You need to recommend which certificates are required for the deployment.

Trusted Root Certification Authorities certificate store on each laptop:	SLOT-1
The users' Personal store on each laptop:	SLOT-2
The Azure VPN gateway:	SLOT-3

Which of the following would go into Slot2?

- A. A root CA certificate that has the private key
- B. A root CA certificate that has the public key only
- C. A user certificate that has the private key
- D. A user certificate that has the public key only

Correct

Each client computer that you connect to a VNet with a Point-to-Site connection must have a client certificate installed. You generate it from the root certificate and install it on each client computer. If you don't install a valid client certificate, authentication will fail when the client tries to connect to the VNet. You can either generate a unique certificate for each client, or you can use the same certificate for multiple clients. The advantage to generating unique client certificates is the ability to revoke a single certificate. Otherwise, if multiple clients use the same client certificate to authenticate and you revoke it, you'll need to generate and install new certificates for every client that uses that certificate.

Reference:

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

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site#clientcert

Generate client certificates

Each client computer that you connect to a VNet with a Point-to-Site connection must have a client certificate installed. You generate it from the root certificate and install it on each client computer. If you don't install a valid client certificate, authentication will fail when the client tries to connect to the VNet.

You can either generate a unique certificate for each client, or you can use the same certificate for multiple clients. The advantage to generating unique client certificates is the ability to revoke a single certificate. Otherwise, if multiple clients use the same client certificate to authenticate and you revoke it, you'll need to generate and install new certificates for every client that uses that certificate.

You can generate client certificates by using the following methods:

- **Enterprise certificate**:
  - If you're using an enterprise certificate solution, generate a client certificate with the common name value format *name@yourdomain.com*. Use this format instead of the *domain name\username* format.
  - Make sure the client certificate is based on a user certificate template that has *Client Authentication* listed as the first item in the user list. Check the certificate by double-clicking it and viewing **Enhanced Key Usage** in the **Details** tab.
- **Self-signed root certificate**: Follow the steps in one of the following P2S certificate articles so that the client certificates you create will be compatible with your P2S connections.

  When you generate a client certificate from a self-signed root certificate, it's automatically installed on the computer that you used to generate it. If you want to install a client certificate on another client computer, export it as a .pfx file, along with the entire certificate chain. Doing so will create a .pfx file that contains the root certificate information required for the client to authenticate.

  The steps in these articles generate a compatible client certificate, which you can then export and distribute.
  - Windows 10 PowerShell instructions: These instructions require Windows 10 and PowerShell to generate certificates. The generated certificates can be installed on any supported P2S client.
  - MakeCert instructions: Use MakeCert if you don't have access to a Windows 10 computer for generating certificates. Although MakeCert is deprecated, you can still use it to generate certificates. You can install the generated certificates on any supported P2S client.
  - Linux instructions.

10. Question

Your company has users who work remotely from laptops.

You plan to move some of the applications accessed by the remote users to Azure virtual machines. The users will access the applications in Azure by using a point-to-site VPN connection. You will use certificates

generated from an on-premises-based Certification authority (CA).

You need to recommend which certificates are required for the deployment.

Trusted Root Certification Authorities certificate store on each laptop:	SLOT-1
The users' Personal store on each laptop:	SLOT-2
The Azure VPN gateway:	SLOT-3

Which of the following would go into Slot3?

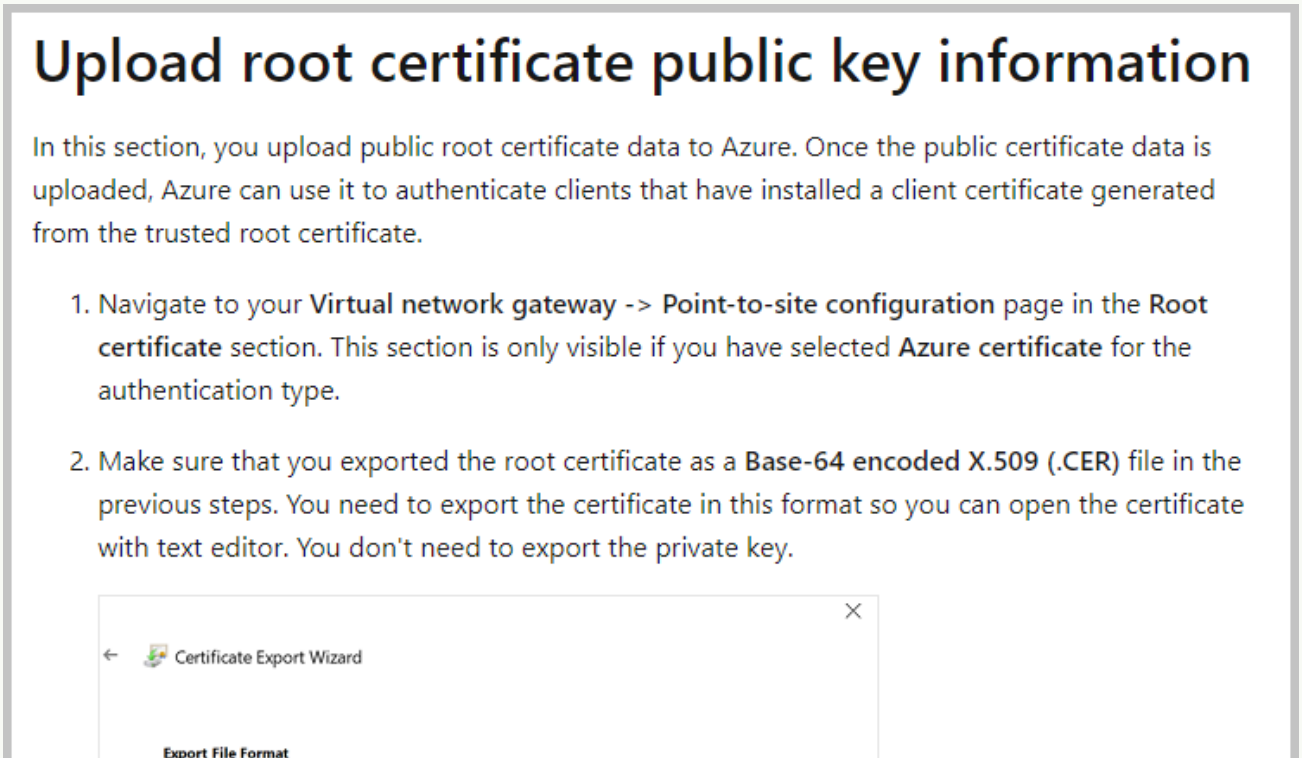
- A. A root CA certificate that has the private key
- B. A root CA certificate that has the public key only
- C. A user certificate that has the private key
- D. A user certificate that has the public key only

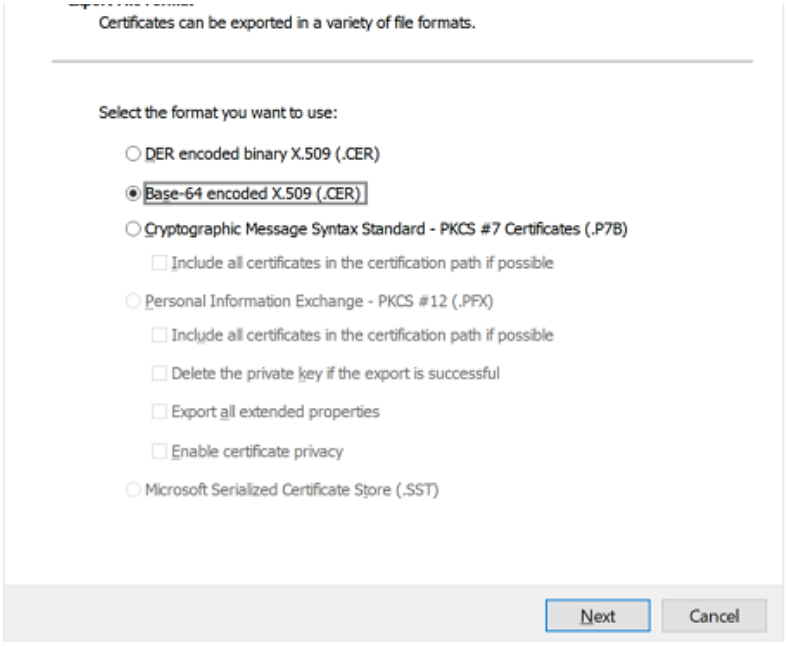
Correct

You upload public root certificate data to Azure. Once the public certificate data is uploaded, Azure can use it to authenticate clients that have installed a client certificate generated from the trusted root certificate.

Reference:

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



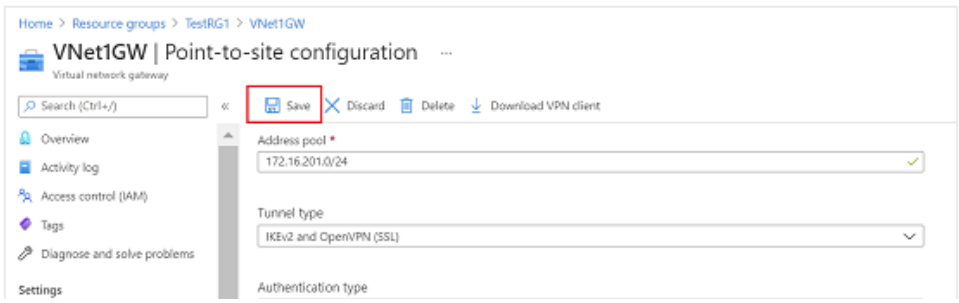


3. Open the certificate with a text editor, such as Notepad. When copying the certificate data, make sure that you copy the text as one continuous line without carriage returns or line feeds. You may need to modify your view in the text editor to 'Show Symbol/Show all characters' to see the carriage returns and line feeds. Copy only the following section as one continuous line:

4. In the **Root certificate** section, you can add up to 20 trusted root certificates.

   - Paste the certificate data into the **Public certificate data** field.
   - **Name** the certificate.

5. Select **Save** at the top of the page to save all of the configuration settings.



11. Question

You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365 E5 plan.

You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:

? To the manager of the developers, send a monthly email message that lists the access permissions to Application1.

? If the manager does not verify an access permission, automatically revoke that permission.

? Minimize development effort.

What should you recommend?

- A. Create an Azure Automation runbook that runs the Get-AzureADUserAppRoleAssignment cmdlet
- B. Create an Azure Automation runbook that runs the Get-AzRoleAssignment cmdlet
- **C. In Azure Active Directory (Azure AD), create an access review of Application1**
- D. In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources

Correct

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Incorrect Answers:

A. Create an Azure Automation runbook that runs the Get-AzureADUserAppRoleAssignment cmdlet

With this approach, we implement the membership management functionality ourselves. It takes a lot of hard work.

B. Create an Azure Automation runbook that runs the Get-AzRoleAssignment cmdlet

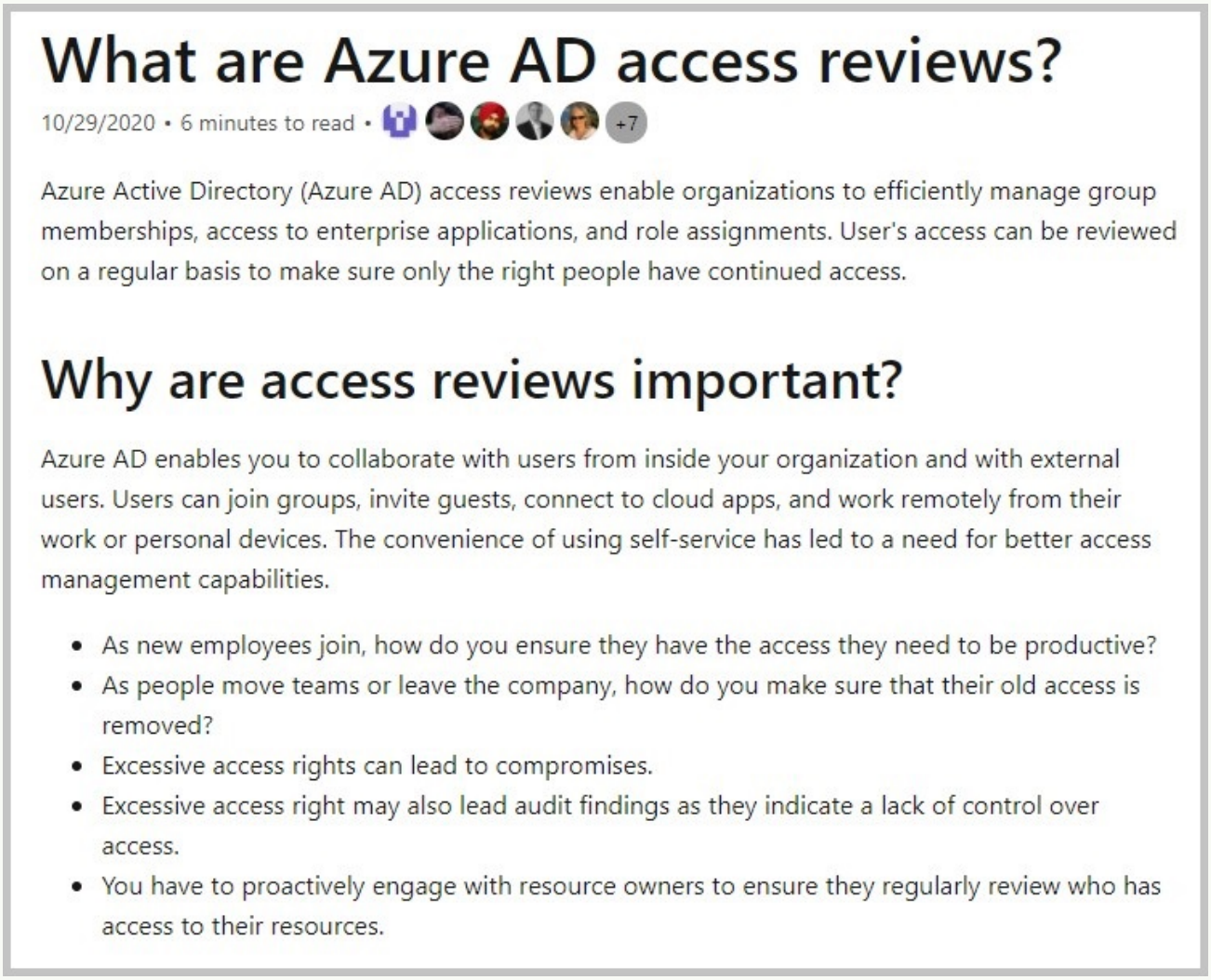
With this approach, we implement the membership management functionality ourselves. It takes a lot of hard work.

D. In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview



What are Azure AD access reviews?

10/29/2020 • 6 minutes to read • +7

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Why are access reviews important?

Azure AD enables you to collaborate with users from inside your organization and with external users. Users can join groups, invite guests, connect to cloud apps, and work remotely from their work or personal devices. The convenience of using self-service has led to a need for better access management capabilities.

- As new employees join, how do you ensure they have the access they need to be productive?
- As people move teams or leave the company, how do you make sure that their old access is removed?
- Excessive access rights can lead to compromises.
- Excessive access right may also lead audit findings as they indicate a lack of control over access.
- You have to proactively engage with resource owners to ensure they regularly review who has access to their resources.

12. Question

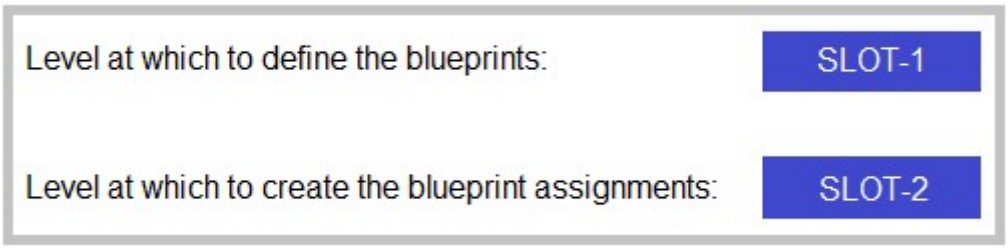
You plan to create an Azure environment that will contain a root management group and 10 child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription.

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

? Use Azure Blueprints to control governance across all the subscriptions and resource groups.

? Ensure that Blueprints-based configurations are consistent across all the subscriptions and resource groups.

? Minimize the number of blueprint definitions and assignments.



Which of the following would go into Slot1?

A. The child management groups

B. The root management group

C. The subscriptions

Correct

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.

Incorrect Answers:

A. The child management groups

To reduce the number of blueprint assignments, you must define it at root management group level.

C. The subscriptions

To reduce the number of blueprint assignments, you must define it at root management group level.

Reference:

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

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.

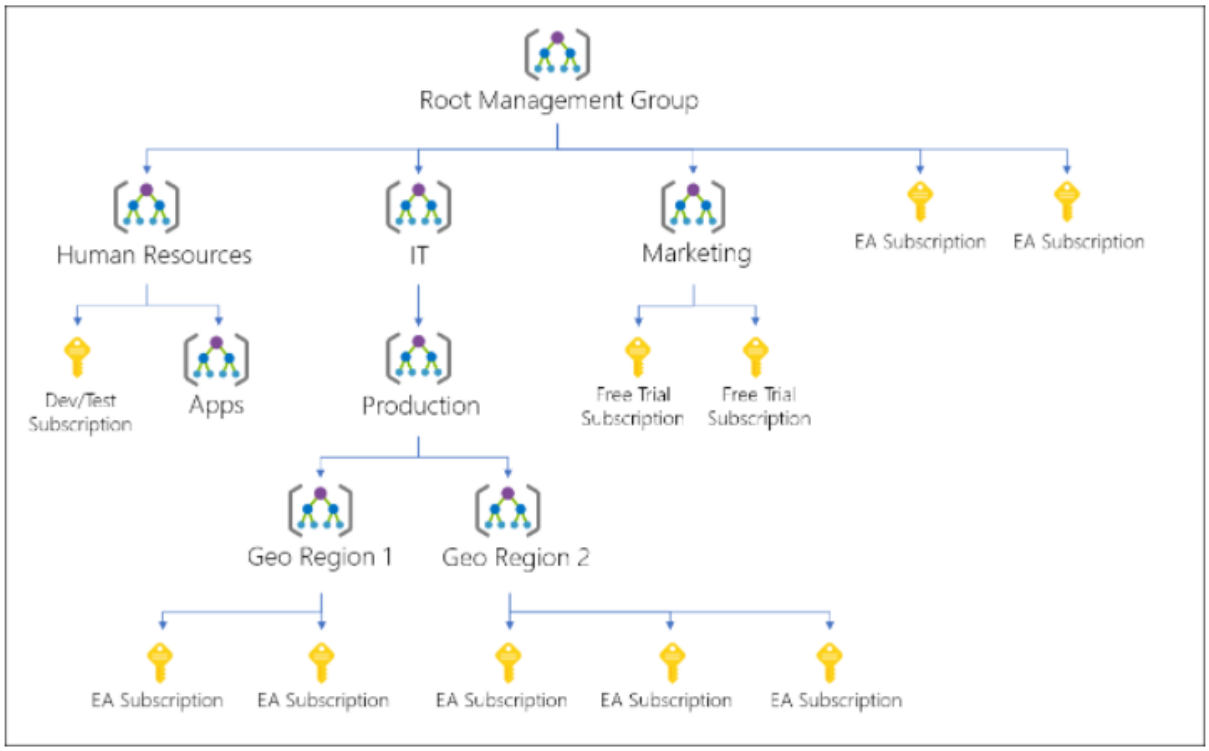
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- 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.

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.



13. Question

You plan to create an Azure environment that will contain a root management group and 10 child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription.

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

? Use Azure Blueprints to control governance across all the subscriptions and resource groups.

? Ensure that Blueprints-based configurations are consistent across all the subscriptions and resource groups.

? Minimize the number of blueprint definitions and assignments.

Level at which to define the blueprints:	SLOT-1
Level at which to create the blueprint assignments:	SLOT-2

Which of the following would go into Slot2?

A. The child management groups

B. The root management group

C. The subscriptions

Incorrect

Each directory 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 root management group allows for global policies and Azure role assignments to be applied at the directory level.

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

Incorrect Answers:

A. The child management groups

To reduce the number of blueprint assignments, you must define it at root management group level.

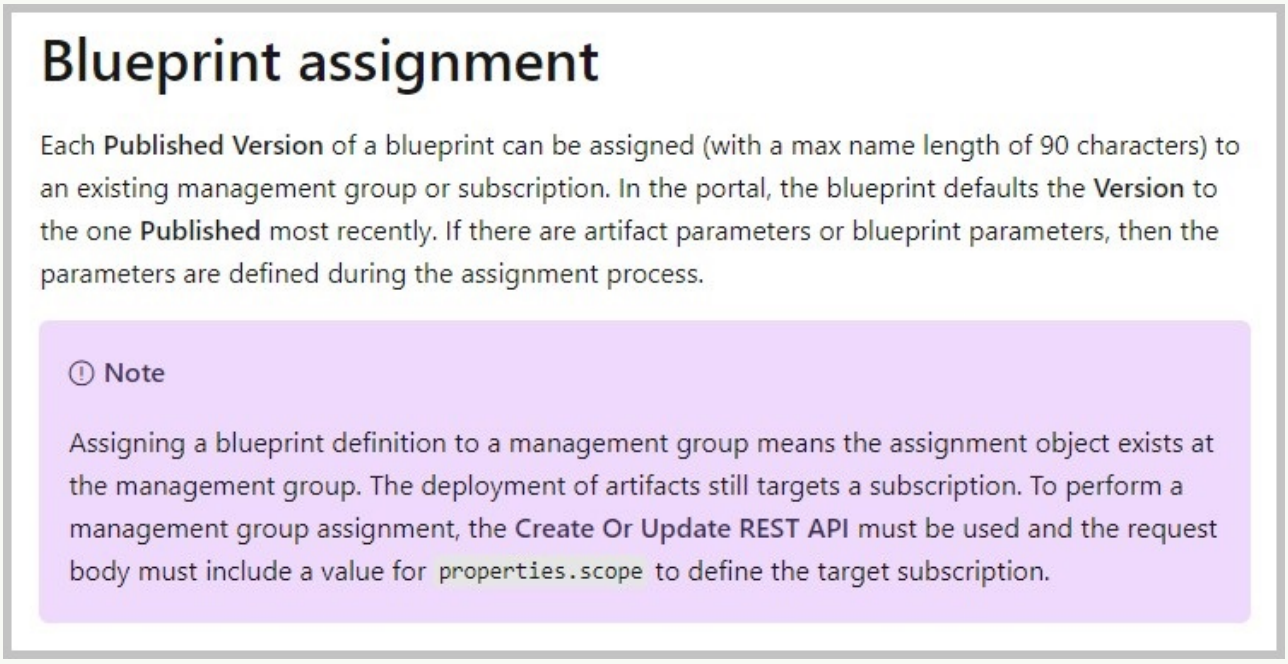
C. The subscriptions

To reduce the number of blueprint assignments, you must define it at root management group level.

Reference:

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

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



Blueprint assignment

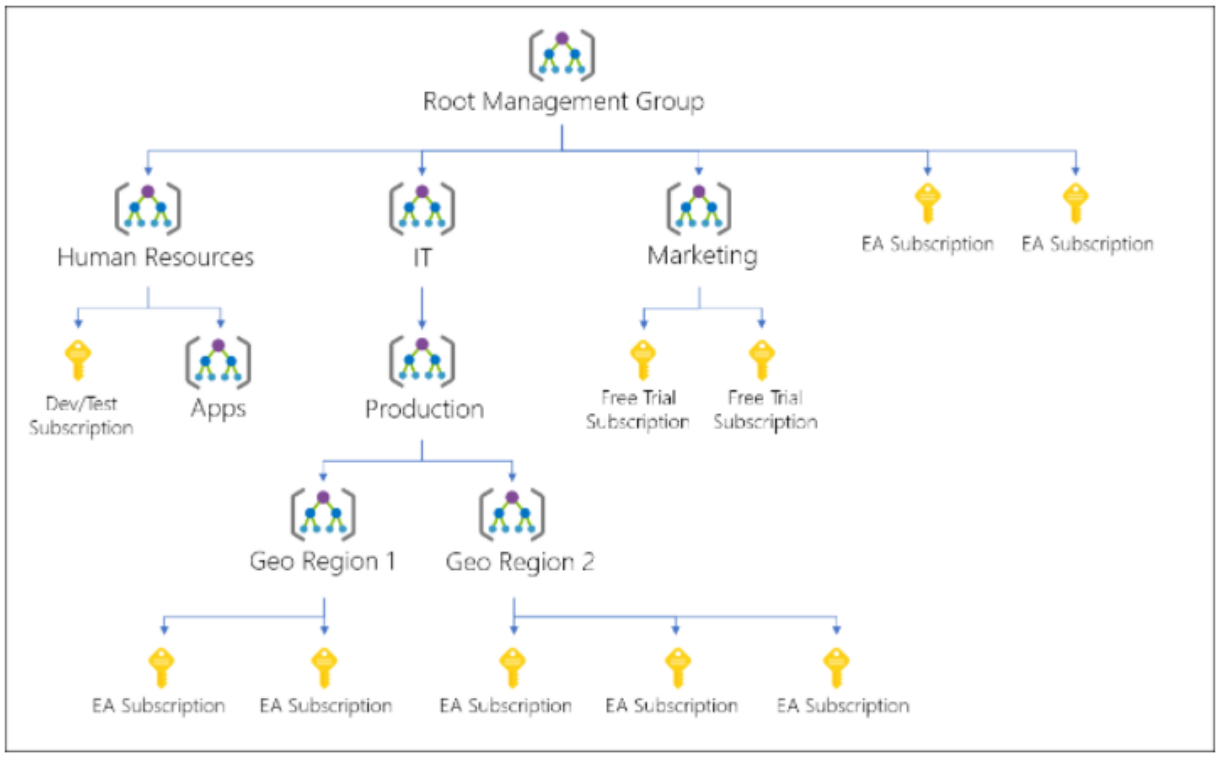
Each **Published Version** of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription. In the portal, the blueprint defaults the **Version** to the one **Published** most recently. If there are artifact parameters or blueprint parameters,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

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.



14. Question

Your organization has developed and deployed several Azure App Service Web and API applications. The applications use Azure Key Vault to store several authentication, storage account, and data encryption keys. Several departments have the following requests to support the applications:

Department	Request
Security	• Review membership of administrative roles and require users to provide a justification for continued membership • Get alerts about changes in administrator assignments. • See a history of administrator activation, including which changes administrators made to Azure resources.
Development	• Enable the applications to access Azure Key Vault and retrieve keys for use in code.
Quality Assurance	• Receive temporary administrator access to create and configure additional Web and API applications in the test environment.

You need to recommend the appropriate Azure service for each department request.

What should you recommend for security department?

A. Azure AD Privileged Identity Management

B. Azure Managed Identity

C. Azure AD Connect

D. Azure AD Identity Protection

Incorrect

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Incorrect Answers:

B. Azure Managed Identity

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.

C. Azure AD Connect

Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals.

D. Azure AD Identity Protection

Azure Active Directory (Azure AD) Identity Protection provides you advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

15. Question

Your organization has developed and deployed several Azure App Service Web and API applications. The applications use Azure Key Vault to store several authentication, storage account, and data encryption keys. Several departments have the following requests to support the applications:

Department	Request
Security	• Review membership of administrative roles and require users to provide a justification for continued membership • Get alerts about changes in administrator assignments. • See a history of administrator activation, including which changes administrators made to Azure resources.
Development	• Enable the applications to access Azure Key Vault and retrieve keys for use in code.
Quality Assurance	• Receive temporary administrator access to create and configure additional Web and API applications in the test environment.

You need to recommend the appropriate Azure service for each department request.

What should you recommend for development department?

- A. Azure AD Privileged Identity Management
- B. Azure Managed Identity
- C. Azure AD Connect
- D. Azure AD Identity Protection

Correct

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.

Incorrect Answers:

A. Azure AD Privileged Identity Management

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization.

C. Azure AD Connect

Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals.

D. Azure AD Identity Protection

Azure Active Directory (Azure AD) Identity Protection provides you advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications.

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 • +19

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).

16. Question

Your organization has developed and deployed several Azure App Service Web and API applications. The applications use Azure Key Vault to store several authentication, storage account, and data encryption keys. Several departments have the following requests to support the applications:

Department	Request
Security	• Review membership of administrative roles and require users to provide a justification for continued membership • Get alerts about changes in administrator assignments. • See a history of administrator activation, including which changes administrators made to Azure resources.
Development	• Enable the applications to access Azure Key Vault and retrieve keys for use in code.
Quality Assurance	• Receive temporary administrator access to create and configure additional Web and API applications in the test environment.

You need to recommend the appropriate Azure service for each department request.

What should you recommend for quality assurance department?

- A. Azure AD Privileged Identity Management
- B. Azure Managed Identity
- C. Azure AD Connect
- D. Azure AD Identity Protection

Correct

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Incorrect Answers:

B. Azure Managed Identity

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.

C. Azure AD Connect

Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals.

D. Azure AD Identity Protection

Azure Active Directory (Azure AD) Identity Protection provides you advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

What is Azure AD Privileged Identity Management?

06/25/2021 • 8 minutes to read •

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. The following video introduces you to important PIM concepts and features.

What does it do?

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit
- Prevents removal of the **last active Global Administrator** role assignment

17. Question

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains two administrative user accounts named Admin1 and Admin2. You create two Azure virtual machines named VM1 and VM2.

You need to ensure that Admin1 and Admin2 are notified when more than five events are added to the security log of VM1 or VM2 during a period of 120 seconds.

The solution must minimize administrative tasks.

What should you create?

- A. two action groups and two alert rules
- B. one action group and one alert rule
- C. five action groups and one alert rule
- D. two action groups and one alert rule

Correct

An alert rule can have multiple VMs as target. Also mentioned here at Azure documentation:

The following are key attributes of an alert rule:

Target Resource – Defines the scope and signals available for alerting. A target can be any Azure resource. Example targets:

? Virtual machines.

? Storage accounts.

? Log Analytics workspace.

? Application Insights.

For certain resources (like virtual machines), you can specify multiple resources as the target of the alert rule.

Also, as per another Azure documentation – Various alerts may use the same action group or different action groups depending on the user's requirements.

In Summary, you just need one 1 alert rule and 1 action group and thus option B seems to be correct.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview

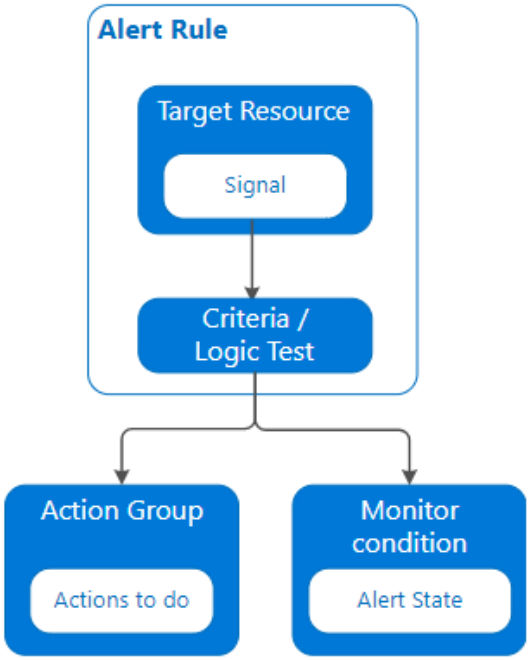
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

What are alerts in Microsoft Azure?

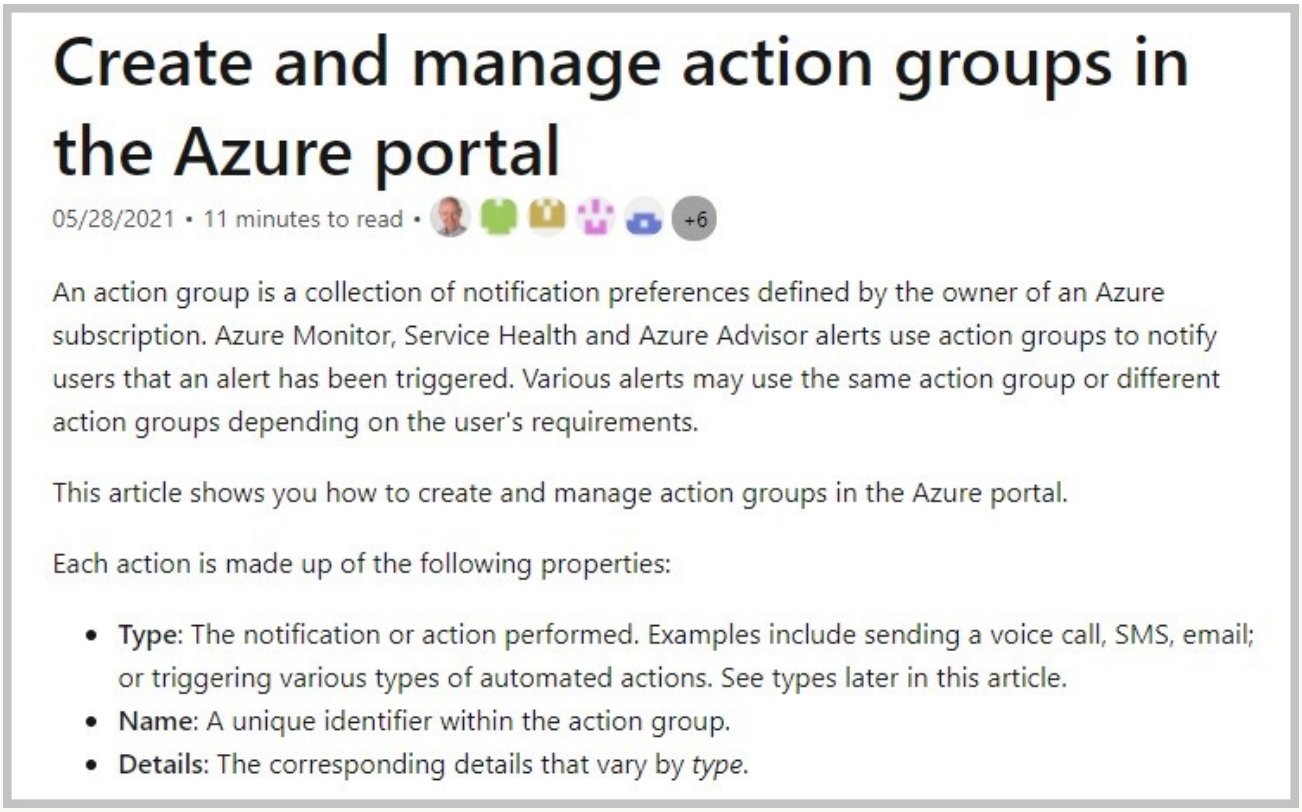
Alerts proactively notify you when issues are found with your infrastructure or application using your monitoring data in Azure Monitor. They allow you to identify and address issues before the users of your system notice them.

Overview

The diagram below represents the flow of alerts.



Alert rules are separated from alerts and the actions taken when an alert fires. The alert rule captures the target and criteria for alerting. The alert rule can be in an enabled or a disabled state. Alerts only fire when enabled.



Create and manage action groups in the Azure portal

05/28/2021 • 11 minutes to read • +6

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered. Various alerts may use the same action group or different action groups depending on the user's requirements.

This article shows you how to create and manage action groups in the Azure portal.

Each action is made up of the following properties:

- **Type**: The notification or action performed. Examples include sending a voice call, SMS, email; or triggering various types of automated actions. See types later in this article.
- **Name**: A unique identifier within the action group.
- **Details**: The corresponding details that vary by *type*.

18. Question

You have an Azure Active Directory (Azure AD) tenant named techzen-az304.com that has a security group named Group1. Group1 is configured for assigned membership. Group1 has 50 members, including 20 guest users.

You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:

? The evaluation must be repeated automatically every three months.

? Every member must be able to report whether they need to be in Group1.

? Users who report that they do not need to be in Group1 must be removed from Group1 automatically.

? Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

What should you include in the recommendation?

- A. Change the Membership type of Group1 to Dynamic User
- B. Implement Azure AD Privileged Identity Management
- C. Implement Azure AD Identity Protection
- D. Create an access review

Correct

You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#when-should-you-use-access-reviews

When should you use access reviews?

- **Too many users in privileged roles:** It's a good idea to check how many users have administrative access, how many of them are Global Administrators, and if there are any invited guests or partners that have not been removed after being assigned to do an administrative task. You can recertify the role assignment users in Azure AD roles such as Global Administrators, or Azure resources roles such as User Access Administrator in the Azure AD Privileged Identity Management (PIM) experience.
- **When automation is not possible:** You can create rules for dynamic membership on security groups or Microsoft 365 Groups, but what if the HR data is not in Azure AD or if users still need access after leaving the group to train their replacement? You can then create a review on that group to ensure those who still need access should have continued access.
- **When a group is used for a new purpose:** If you have a group that is going to be synced to Azure AD, or if you plan to enable the application Salesforce for everyone in the Sales team group, it would be useful to ask the group owner to review the group membership prior to the group being used in a different risk content.
- **Business critical data access:** for certain resources, it might be required to ask people outside of IT to regularly sign out and give a justification on why they need access for auditing purposes.
- **To maintain a policy's exception list:** In an ideal world, all users would follow the access policies to secure access to your organization's resources. However, sometimes there are business cases that require you to make exceptions. As the IT admin, you can manage this task, avoid oversight of policy exceptions, and provide auditors with proof that these exceptions are reviewed regularly.
- **Ask group owners to confirm they still need guests in their groups:** Employee access might be automated with some on premises Identity and Access Management (IAM), but not invited guests. If a group gives guests access to business sensitive content, then it's the group owner's responsibility to confirm the guests still have a legitimate business need for access.
- **Have reviews recur periodically:** You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.

ⓘ Note

If you are ready to try Access reviews take a look at **Create an access review of groups or applications**

19. Question

You have 200 resource groups across 20 Azure subscriptions.

Your company's security policy states that the security administrator must verify all assignments of the Owner role for the subscriptions and resource groups once a month. All assignments that are not approved by the security administrator must be removed automatically. The security administrator must be prompted

every month to perform the verification.

What should you use to implement the security policy?

- A. Identity Secure Score in Azure Security Center
- **B. Access reviews in Identity Governance**
- C. the user risk policy in Azure Active Directory (Azure AD) Identity Protection
- D. role assignments in Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Correct

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Incorrect Answers:

A. Identity Secure Score in Azure Security Center

The identity secure score is percentage that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security.

C. the user risk policy in Azure Active Directory (Azure AD) Identity Protection

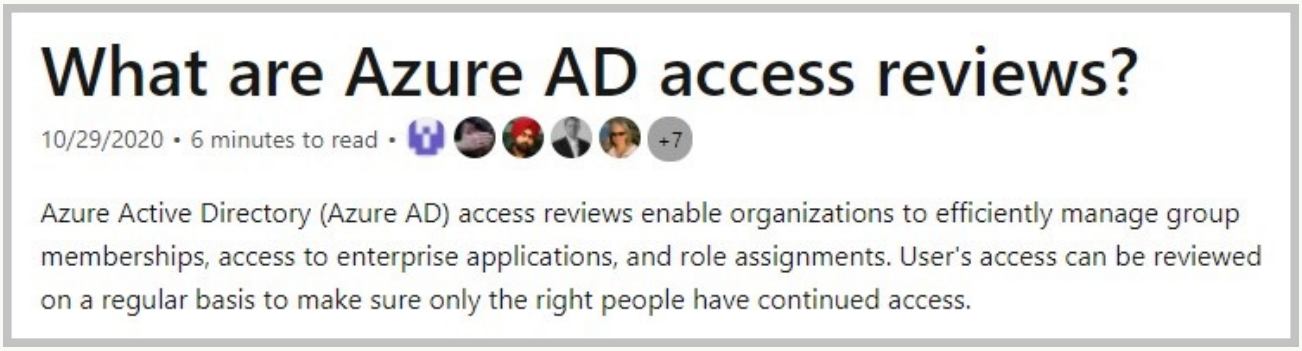
The user risk policy helps to know whether Azure AD recognizes the likelihood that a user account has been compromised.

D. role assignments in Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview



When should you use access reviews?

- **Too many users in privileged roles:** It's a good idea to check how many users have administrative access, how many of them are Global Administrators, and if there are any invited guests or partners that have not been removed after being assigned to do an administrative task. You can recertify the role assignment users in Azure AD roles such as Global Administrators, or Azure resources roles such as User Access Administrator in the Azure AD Privileged Identity Management (PIM) experience.
- **When automation is not possible:** You can create rules for dynamic membership on security groups or Microsoft 365 Groups, but what if the HR data is not in Azure AD or if users still need access after leaving the group to train their replacement? You can then create a review on that group to ensure those who still need access should have continued access.
- **When a group is used for a new purpose:** If you have a group that is going to be synced to Azure AD, or if you plan to enable the application Salesforce for everyone in the Sales team group, it would be useful to ask the group owner to review the group membership prior to the group being used in a different risk content.
- **Business critical data access:** for certain resources, it might be required to ask people outside of IT to regularly sign out and give a justification on why they need access for auditing purposes.
- **To maintain a policy's exception list:** In an ideal world, all users would follow the access policies to secure access to your organization's resources. However, sometimes there are business cases that require you to make exceptions. As the IT admin, you can manage this task, avoid oversight of policy exceptions, and provide auditors with proof that these exceptions are reviewed regularly.
- **Ask group owners to confirm they still need guests in their groups:** Employee access might be automated with some on premises Identity and Access Management (IAM), but not invited guests. If a group gives guests access to business sensitive content, then it's the group owner's responsibility to confirm the guests still have a legitimate business need for access.
- **Have reviews recur periodically:** You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.

ⓘ Note

If you are ready to try Access reviews take a look at **Create an access review of groups or applications**

20. Question

Your company has 20 web APIs that were developed in-house.

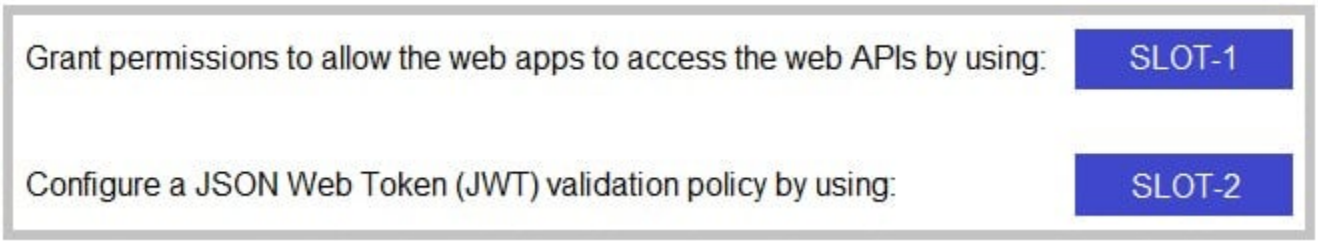
The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company's Azure Active Directory (Azure AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from

reaching the web APIs. The solution must meet the following requirements:

? Use Azure AD-generated claims.

? Minimize configuration and management effort.



Which of the following would go into Slot1?

- A. Azure AD
- B. Azure API Management
- C. The web APIs

Correct

Steps to take:

1 – In Azure AD, register an application (backend-app) to represent the API.

2 – In Azure AD, register another application (client-app) to represent a client application that needs to call the API.

3 – In Azure AD, grant permissions to allow the client-app to call the backend-app.

4 – In APIM, configure the Developer Console to call the API using OAuth 2.0 user authorization.

5 – In APIM, add the validate-jwt policy to validate the OAuth token for every incoming request.

Grant permissions by using: Azure AD (Step 3)

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad

21. Question

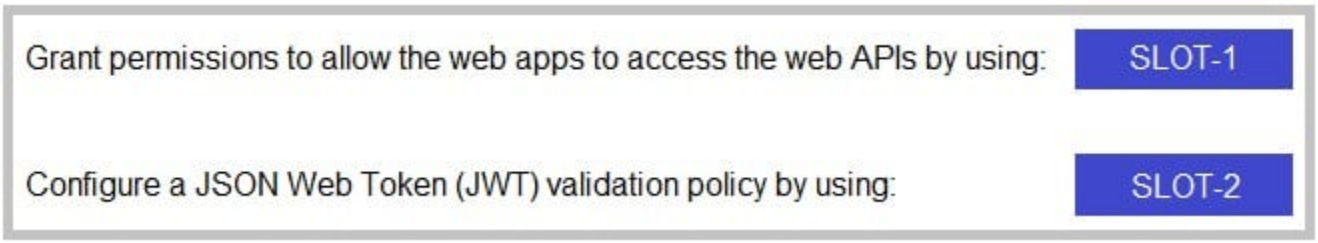
Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company's Azure Active Directory (Azure AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

? Use Azure AD-generated claims.

? Minimize configuration and management effort.



Which of the following would go into Slot2?

- A. Azure AD
- B. Azure API Management
- C. The web APIs

Incorrect

Steps to take:

1 – In Azure AD, register an application (backend-app) to represent the API.

2 – In Azure AD, register another application (client-app) to represent a client application that needs to call the API.

3 – In Azure AD, grant permissions to allow the client-app to call the backend-app.

4 – In APIM, configure the Developer Console to call the API using OAuth 2.0 user authorization.

5 – In APIM, add the validate-jwt policy to validate the OAuth token for every incoming request.

Configure JWT validation policy by using: Azure APIM (Step 5)

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad

https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies#ValidateJWT

22. Question

Your company is designing a multi-tenant application that will use elastic pools and Azure SQL databases. The application will be used by 30 customers.

You need to design a storage solution for the application. The solution must meet the following requirements:

? Operational costs must be minimized.

? All customers must have their own database.

The customer databases will be in one of the following three Azure regions: East US, North Europe, or South Africa North.

What is the minimum number of elastic pools required?

- 1

- 3
- 6
- 10
- 30

Correct

The server, its pools & databases must be in the same Azure region under the same subscription.

If the customers can be in one of the three Azure Regions, this means that it will probably have customers in all regions, these are the regions where the customers will be, so you will need 3 elastic pools, one for each region and one sql server for each region.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview

https://vincentlauzon.com/2016/12/18/azure-sql-elastic-pool-overview/

23. Question

Your company is designing a multi-tenant application that will use elastic pools and Azure SQL databases.

The application will be used by 30 customers.

You need to design a storage solution for the application. The solution must meet the following requirements:

? Operational costs must be minimized.

? All customers must have their own database.

The customer databases will be in one of the following three Azure regions: East US, North Europe, or South Africa North.

What is the minimum number of Azure SQL Database servers required?

- 1
- 3
- 6
- 10
- 30

Correct

If the customers can be in one of the three Azure Regions, this means that it will probably have customers in all regions, these are the regions where the customers will be, so you will need 3 elastic pools, one for each region and one sql server for each region.

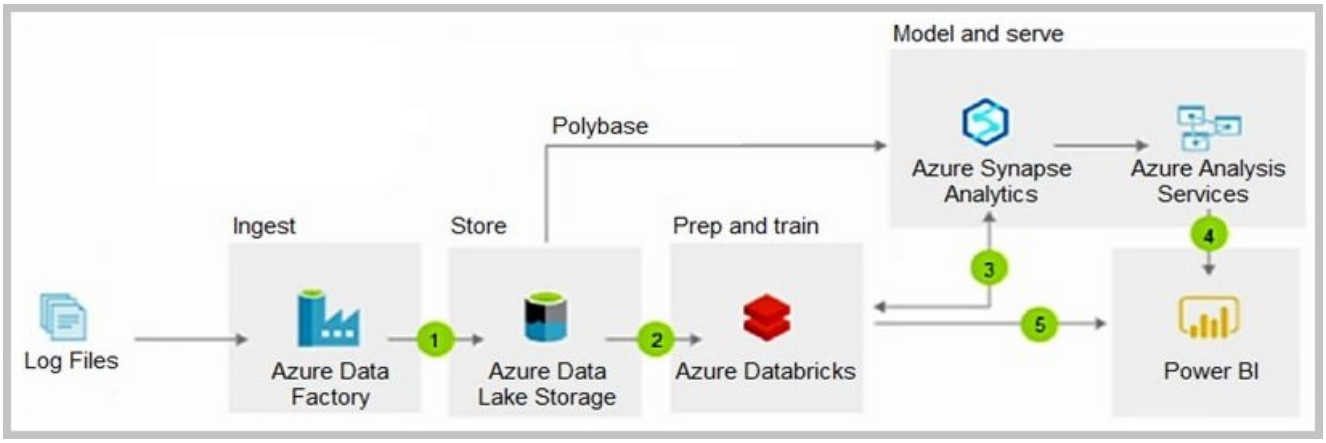
Reference:

https://vincentlauzon.com/2016/12/18/azure-sql-elastic-pool-overview/

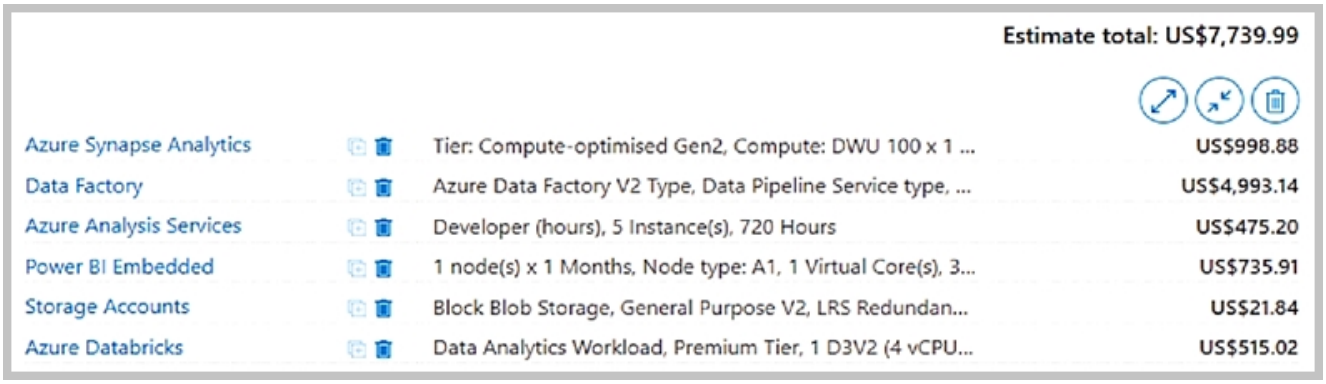
https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview

24. Question

You are reviewing an Azure architecture as shown in the Architecture exhibit.



The estimated monthly costs for the architecture are shown in the Costs exhibit.



Estimate total: US$7,739.99

Azure Synapse Analytics	Tier: Compute-optimised Gen2, Compute: DWU 100 x 1 ...	US$998.88
Data Factory	Azure Data Factory V2 Type, Data Pipeline Service type, ...	US$4,993.14
Azure Analysis Services	Developer (hours), 5 Instance(s), 720 Hours	US$475.20
Power BI Embedded	1 node(s) x 1 Months, Node type: A1, 1 Virtual Core(s), 3...	US$735.91
Storage Accounts	Block Blob Storage, General Purpose V2, LRS Redundan...	US$21.84
Azure Databricks	Data Analytics Workload, Premium Tier, 1 D3V2 (4 vCPU...	US$515.02

The log files are generated by user activity to Apache web servers. The log files are in a consistent format.

Approximately 1 GB of logs are generated per day.

Microsoft Power BI is used to display weekly reports of the user activity.

You need to recommend a solution to minimize costs while maintaining the functionality of the architecture.

What should you recommend?

- A. Replace Azure Synapse Analytics and Azure Analysis Services with SQL Server on an Azure virtual machine
- B. Replace Azure Synapse Analytics with Azure SQL Database Hyperscale
- **C. Replace Azure Data Factory with CRON jobs that use AzCopy**
- D. Replace Azure Databricks with Azure Machine Learning

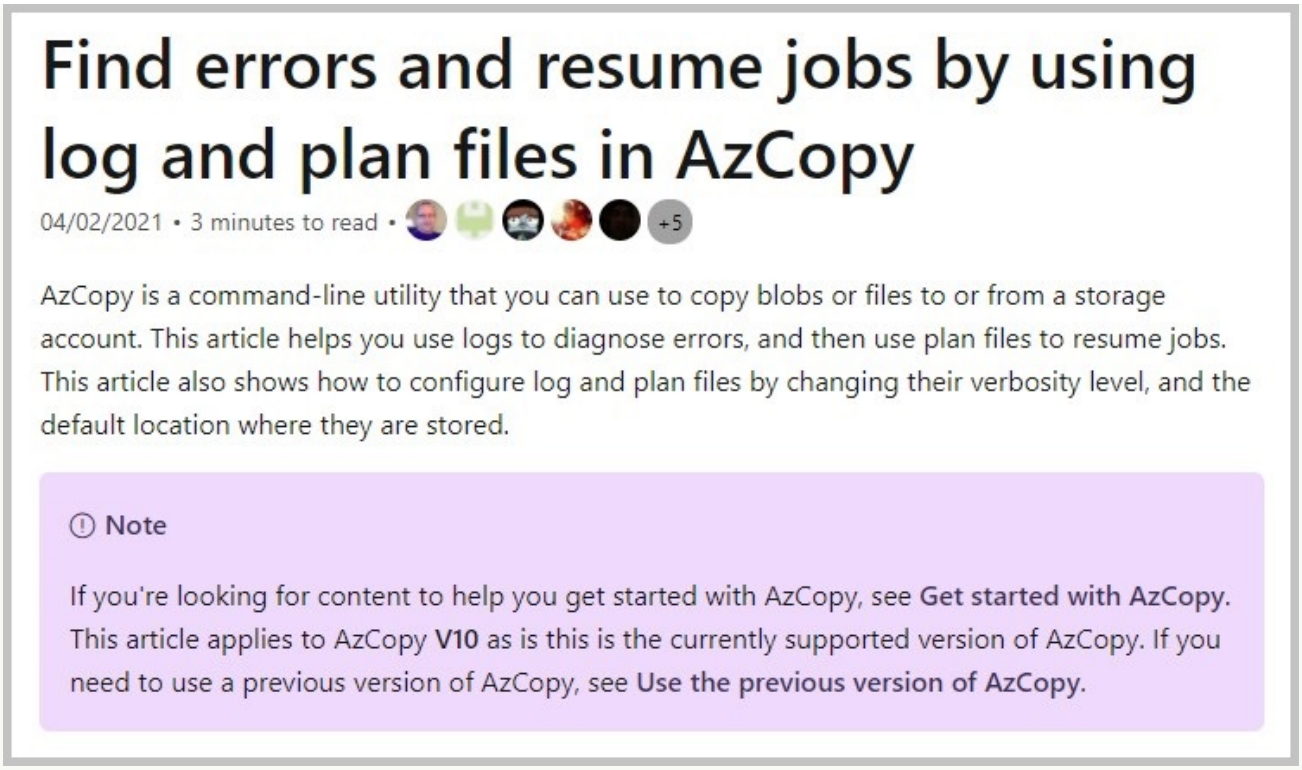
Correct

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Cron is one of the most useful utility that you can find in any Unix-like operating system. It is used to schedule commands at a specific time. These scheduled commands or tasks are known as “Cron Jobs“.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-configure



Find errors and resume jobs by using log and plan files in AzCopy

04/02/2021 • 3 minutes to read • +5

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account. This article helps you use logs to diagnose errors, and then use plan files to resume jobs. This article also shows how to configure log and plan files by changing their verbosity level, and the default location where they are stored.

Note

If you're looking for content to help you get started with AzCopy, see **Get started with AzCopy**. This article applies to AzCopy **V10** as is this is the currently supported version of AzCopy. If you need to use a previous version of AzCopy, see **Use the previous version of AzCopy**.

25. 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 account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier.

You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: For File1, you set Access tier to Hot.

Does this meet the goal?

- A. Yes
- B. No

Correct

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs.

Example usage scenarios for the hot access tier include:

? Data that‘s in active use or expected to be accessed (read from and written to) frequently.

? Data that‘s staged for processing and eventual migration to the cool access tier.

While a blob is in the archive access tier, it‘s considered to be offline and can‘t be read or modified. In order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#comparing-block-blob-storage-options

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

Comparing block blob storage options

The following table shows a comparison of premium performance block blob storage, and the hot, cool, and archive access tiers.

	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

Overview of blob rehydration from the archive tier

08/31/2021 • 8 minutes to read •

While a blob is in the archive access tier, it's considered to be offline and can't be read or modified. In order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier. There are two options for rehydrating a blob that is stored in the archive tier:

- Copy an archived blob to an online tier: You can rehydrate an archived blob by copying it to a new blob in the hot or cool tier with the Copy Blob or Copy Blob from URL operation. Microsoft recommends this option for most scenarios.
- Change a blob's access tier to an online tier: You can rehydrate an archived blob to hot or cool by changing its tier using the Set Blob Tier operation.

Rehydrating a blob from the archive tier can take several hours to complete. Microsoft recommends rehydrating larger blobs for optimal performance. Rehydrating several small blobs concurrently may require additional time.

26. 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 account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier.

You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: You add a new file share to the storage account.

Does this meet the goal?

- A. Yes
- B. No

Correct

Instead use the hot access tier.

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs.

Example usage scenarios for the hot access tier include:

? Data that‘s in active use or expected to be accessed (read from and written to) frequently.

? Data that‘s staged for processing and eventual migration to the cool access tier.

While a blob is in the archive access tier, it‘s considered to be offline and can‘t be read or modified. In

order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#comparing-block-blob-storage-options

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

Comparing block blob storage options

The following table shows a comparison of premium performance block blob storage, and the hot, cool, and archive access tiers.

	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

Overview of blob rehydration from the archive tier

08/31/2021 • 8 minutes to read •

While a blob is in the archive access tier, it's considered to be offline and can't be read or modified. In order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier. There are two options for rehydrating a blob that is stored in the archive tier:

- Copy an archived blob to an online tier: You can rehydrate an archived blob by copying it to a new blob in the hot or cool tier with the Copy Blob or Copy Blob from URL operation. Microsoft recommends this option for most scenarios.
- Change a blob's access tier to an online tier: You can rehydrate an archived blob to hot or cool by changing its tier using the Set Blob Tier operation.

Rehydrating a blob from the archive tier can take several hours to complete. Microsoft recommends rehydrating larger blobs for optimal performance. Rehydrating several small blobs concurrently may require additional time.

27. 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 account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier.

You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: You move File1 to a new storage account. For File1, you set Access tier to Archive.

Does this meet the goal?

- A. Yes
- B. No

Correct

Instead use the hot access tier.

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs.

Example usage scenarios for the hot access tier include:

? Data that‘s in active use or expected to be accessed (read from and written to) frequently.

? Data that‘s staged for processing and eventual migration to the cool access tier.

While a blob is in the archive access tier, it‘s considered to be offline and can‘t be read or modified. In

order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#comparing-block-blob-storage-options

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

Comparing block blob storage options

The following table shows a comparison of premium performance block blob storage, and the hot, cool, and archive access tiers.

	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

Overview of blob rehydration from the archive tier

08/31/2021 • 8 minutes to read •

While a blob is in the archive access tier, it's considered to be offline and can't be read or modified. In order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier. There are two options for rehydrating a blob that is stored in the archive tier:

- Copy an archived blob to an online tier: You can rehydrate an archived blob by copying it to a new blob in the hot or cool tier with the Copy Blob or Copy Blob from URL operation. Microsoft recommends this option for most scenarios.
- Change a blob's access tier to an online tier: You can rehydrate an archived blob to hot or cool by changing its tier using the Set Blob Tier operation.

Rehydrating a blob from the archive tier can take several hours to complete. Microsoft recommends rehydrating larger blobs for optimal performance. Rehydrating several small blobs concurrently may require additional time.

28. Question

You have an Azure subscription that contains an Azure SQL database.

You are evaluating whether to use Azure reservations on the Azure SQL database.

Which tool should you use to estimate the potential savings?

- A. The Purchase reservations blade in the Azure portal
- B. The Advisor blade in the Azure portal
- C. The SQL database blade in the Azure portal

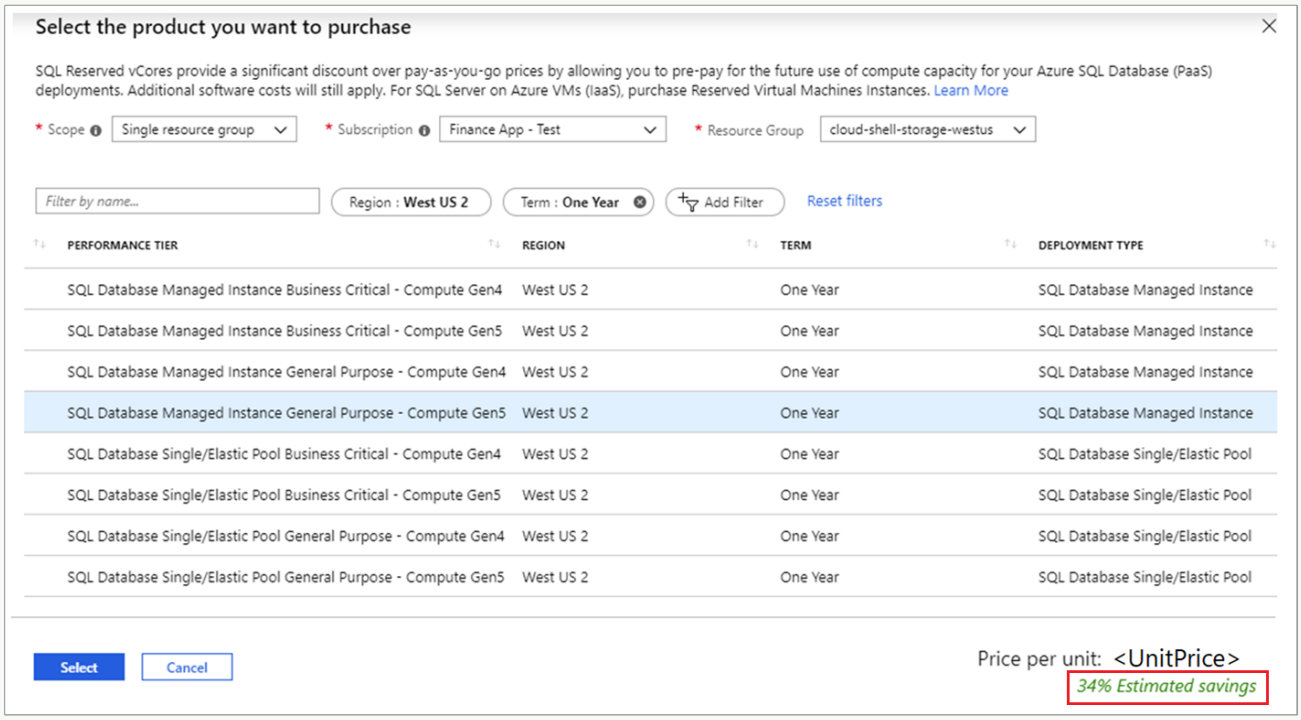
Correct

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.

Buy reserved capacity

1. Sign in to the Azure portal.
2. Select All services > Reservations.
3. Select Add and then in the Purchase Reservations pane, select SQL Database to purchase a new reservation for SQL Database.

4. Fill in the required fields. Existing databases in SQL Database and SQL Managed Instance that match the attributes you select qualify to get the reserved capacity discount. The actual number of databases or managed instances that get the discount depends on the scope and quantity selected.



5. Review the cost of the capacity reservation in the Costs section.

6. Select Purchase.

7. Select View this Reservation to see the status of your purchase.

Reference:

https://docs.microsoft.com/en-us/azure/cost-management-billing/reservations/save-compute-costs-reservations

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 • +3

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.

29. Question

Your company identifies the following business continuity and disaster recovery objectives for virtual machines that host sales, finance, and reporting applications in the company's on-premises data center:

? The sales application must be able to fail over to a second on-premises data center.

? The finance application requires that data be retained for seven years. In the event of a disaster, the application must be able to run from Azure. The recovery time objective (RTO) is 10 minutes.

? The reporting application must be able to recover point-in-time data at a daily granularity. The RTO is eight hours.

You need to recommend which Azure services meet the business continuity and disaster recovery objectives. The solution must minimize costs.

What should you recommend for Sales Application?

- A. Azure Backup only
- B. Azure Site Recovery only
- C. Azure Site Recovery and Azure Backup

Correct

Azure Site Recovery is able to meet the needs. There are no special requirements for backup, but it is mentioned that you should minimize costs.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview#what-does-site-recovery-provide

What does Site Recovery provide?

Feature	Details
Simple BCDR solution	Using Site Recovery, you can set up and manage replication, failover, and failback from a single location in the Azure portal.
Azure VM replication	You can set up disaster recovery of Azure VMs from a primary region to a secondary region.
VMware VM replication	You can replicate VMware VMs to Azure using the improved Azure Site Recovery replication appliance that offers better security and resilience than the configuration server. For more information, see Disaster recovery of VMware VMs.
On-premises VM replication	You can replicate on-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter. Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter.
Workload replication	Replicate any workload running on supported Azure VMs, on-premises Hyper-V and VMware VMs, and Windows/Linux physical servers.
Data resilience	Site Recovery orchestrates replication without intercepting application data. When you replicate to Azure, data is stored in Azure storage, with the resilience that provides.

	When failover occurs, Azure VMs are created, based on the replicated data.
RTO and RPO targets	Keep recovery time objectives (RTO) and recovery point objectives (RPO) within organizational limits. Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V. You can reduce RTO further by integrating with Azure Traffic Manager.
Keep apps consistent over failover	You can replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process.
Testing without disruption	You can easily run disaster recovery drills, without affecting ongoing replication.
Flexible failovers	You can run planned failovers for expected outages with zero-data loss. Or, unplanned failovers with minimal data loss, depending on replication frequency, for unexpected disasters. You can easily fail back to your primary site when it's available again.
Customized recovery plans	Using recovery plans, you can customize and sequence the failover and recovery of multi-tier applications running on multiple VMs. You group machines together in a recovery plan, and optionally add scripts and manual actions. Recovery plans can be integrated with Azure automation runbooks.
BCDR integration	Site Recovery integrates with other BCDR technologies. For example, you can use Site Recovery to protect the SQL Server backend of corporate workloads, with native support for SQL Server AlwaysOn, to manage the failover of availability groups.
Azure automation integration	A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery.
Network integration	Site Recovery integrates with Azure for application network management. For example, to reserve IP addresses, configure load-balancers, and use Azure Traffic Manager for efficient network switchovers.

30. Question

Your company identifies the following business continuity and disaster recovery objectives for virtual machines that host sales, finance, and reporting applications in the company's on-premises data center:

? The sales application must be able to fail over to a second on-premises data center.

? The finance application requires that data be retained for seven years. In the event of a disaster, the application must be able to run from Azure. The recovery time objective (RTO) is 10 minutes.

? The reporting application must be able to recover point-in-time data at a daily granularity. The RTO is eight hours.

You need to recommend which Azure services meet the business continuity and disaster recovery objectives. The solution must minimize costs.

What should you recommend for finance application?

- A. Azure Backup only

B. Azure Site Recovery only

C. Azure Site Recovery and Azure Backup

Correct

Azure Site Recovery is able to perform the fail over, and Azure Backup is able to perform the backup specifying daily, weekly, monthly and yearly retention, up to 10 years.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview#what-does-site-recovery-provide

https://azure.microsoft.com/en-us/support/legal/sla/site-recovery/

https://docs.microsoft.com/en-us/azure/backup/backup-overview#what-can-i-back-up

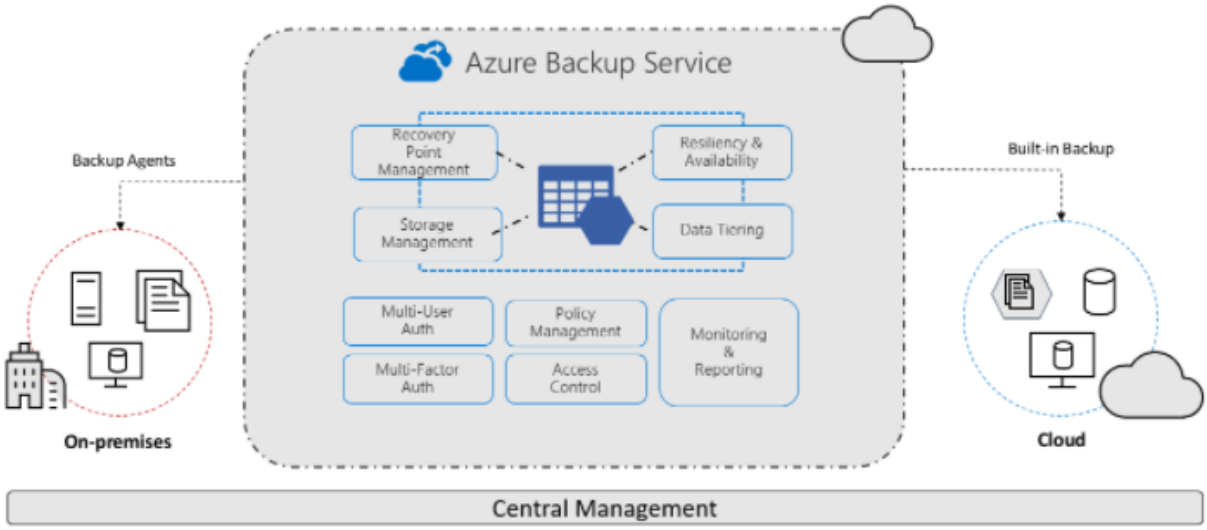
What does Site Recovery provide?

Feature	Details
Simple BCDR solution	Using Site Recovery, you can set up and manage replication, failover, and failback from a single location in the Azure portal.
Azure VM replication	You can set up disaster recovery of Azure VMs from a primary region to a secondary region.
VMware VM replication	You can replicate VMware VMs to Azure using the improved Azure Site Recovery replication appliance that offers better security and resilience than the configuration server. For more information, see Disaster recovery of VMware VMs.
On-premises VM replication	You can replicate on-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter. Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter.
Workload replication	Replicate any workload running on supported Azure VMs, on-premises Hyper-V and VMware VMs, and Windows/Linux physical servers.
Data resilience	Site Recovery orchestrates replication without intercepting application data. When you replicate to Azure, data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created, based on the replicated data.
RTO and RPO targets	Keep recovery time objectives (RTO) and recovery point objectives (RPO) within organizational limits. Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V. You can reduce RTO further by integrating with Azure Traffic Manager.
Keep apps consistent over failover	You can replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process.
Testing without disruption	You can easily run disaster recovery drills, without affecting ongoing replication.

Flexible failovers	You can run planned failovers for expected outages with zero-data loss. Or, unplanned failovers with minimal data loss, depending on replication frequency, for unexpected disasters. You can easily fail back to your primary site when it's available again.
Customized recovery plans	Using recovery plans, you can customize and sequence the failover and recovery of multi-tier applications running on multiple VMs. You group machines together in a recovery plan, and optionally add scripts and manual actions. Recovery plans can be integrated with Azure automation runbooks.
BCDR integration	Site Recovery integrates with other BCDR technologies. For example, you can use Site Recovery to protect the SQL Server backend of corporate workloads, with native support for SQL Server AlwaysOn, to manage the failover of availability groups.
Azure automation integration	A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery.
Network integration	Site Recovery integrates with Azure for application network management. For example, to reserve IP addresses, configure load-balancers, and use Azure Traffic Manager for efficient network switchovers.

What can I back up?

- **On-premises** - Back up files, folders, system state using the Microsoft Azure Recovery Services (MARS) agent. Or use the DPM or Azure Backup Server (MABS) agent to protect on-premises VMs (Hyper-V and VMware) and other on-premises workloads
- **Azure VMs** - Back up entire Windows/Linux VMs (using backup extensions) or back up files, folders, and system state using the MARS agent.
- **Azure Managed Disks** - Back up Azure Managed Disks
- **Azure Files shares** - Back up Azure File shares to a storage account
- **SQL Server in Azure VMs** - Back up SQL Server databases running on Azure VMs
- **SAP HANA databases in Azure VMs** - Backup SAP HANA databases running on Azure VMs
- **Azure Database for PostgreSQL servers (preview)** - Back up Azure PostgreSQL databases and retain the backups for up to 10 years
- **Azure Blobs** - Overview of operational backup for Azure Blobs



31. Question

Your company identifies the following business continuity and disaster recovery objectives for virtual machines that host sales, finance, and reporting applications in the company's on-premises data center:

? The sales application must be able to fail over to a second on-premises data center.

? The finance application requires that data be retained for seven years. In the event of a disaster, the application must be able to run from Azure. The recovery time objective (RTO) is 10 minutes.

? The reporting application must be able to recover point-in-time data at a daily granularity. The RTO is eight hours.

You need to recommend which Azure services meet the business continuity and disaster recovery objectives. The solution must minimize costs.

What should you recommend for reporting application?

- A. Azure Backup only
- B. Azure Site Recovery only

C. Azure Site Recovery and Azure Backup

Correct

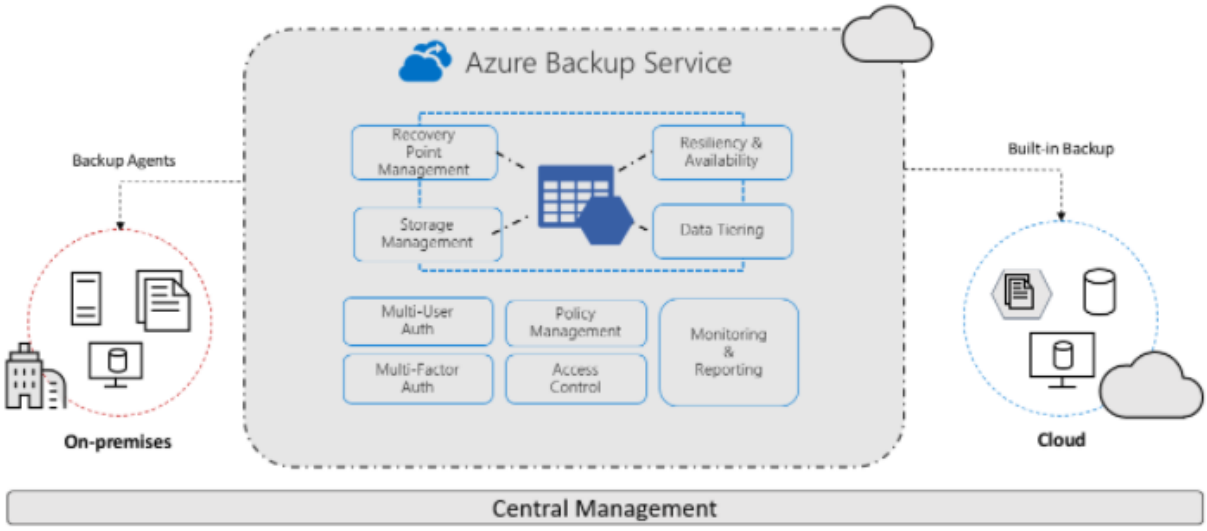
The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.

Reference:

https://docs.microsoft.com/en-us/azure/backup/backup-overview#what-can-i-back-up

What can I back up?

- **On-premises** - Back up files, folders, system state using the Microsoft Azure Recovery Services (MARS) agent. Or use the DPM or Azure Backup Server (MABS) agent to protect on-premises VMs (Hyper-V and VMware) and other on-premises workloads
- **Azure VMs** - Back up entire Windows/Linux VMs (using backup extensions) or back up files, folders, and system state using the MARS agent.
- **Azure Managed Disks** - Back up Azure Managed Disks
- **Azure Files shares** - Back up Azure File shares to a storage account
- **SQL Server in Azure VMs** - Back up SQL Server databases running on Azure VMs
- **SAP HANA databases in Azure VMs** - Backup SAP HANA databases running on Azure VMs
- **Azure Database for PostgreSQL servers (preview)** - Back up Azure PostgreSQL databases and retain the backups for up to 10 years
- **Azure Blobs** - Overview of operational backup for Azure Blobs



32. Question

Your company purchases an app named App1.

You plan to run App1 on seven Azure virtual machines in an Availability Set. The number of fault domains is set to 3. The number of update domains is set to 20.

You need to identify how many App1 instances will remain available during a period of planned

maintenance.

How many App1 instances should you identify?

- A. 1
- B. 2
- C. 6
- D. 7

Correct

Only one update domain is rebooted at a time. Here there are 7 update domain with one VM each (and 13 update domain with no VM), so remaining six virtual machines will be up and running.

Note1: An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not updated at the same time.

Note2: Each virtual machine in your availability set is assigned an update domain and a fault domain by the underlying Azure platform. For a given availability set, five non-user-configurable update domains are assigned by default (Resource Manager deployments can then be increased to provide up to 20 update domains) to indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability

Availability options for Azure Virtual Machines

03/08/2021 • 3 minutes to read • +1

Applies to: ✔ Linux VMs ✔ Windows VMs ✔ Flexible scale sets ✔ Uniform scale sets

This article provides an overview of the availability options for Azure virtual machines (VMs).

Availability zones

Availability zones expands the level of control you have to maintain the availability of the applications and data on your VMs. An Availability Zone is a physically separate zone, within an Azure region. There are three Availability Zones per supported Azure region.

Each Availability Zone has a distinct power source, network, and cooling. By designing your solutions to use replicated VMs in zones, you can protect your apps and data from the loss of a data center. If one zone is compromised, then replicated apps and data are instantly available in another zone.

Availability sets

An availability set is a logical grouping of VMs that allows Azure to understand how your application is built to provide for redundancy and availability. We recommended that two or more VMs are created within an availability set to provide for a highly available application and to meet the 99.95% Azure SLA. There is no cost for the Availability Set itself, you only pay for each VM instance that you create.

33. Question

You need to design a solution that will execute custom C# code in response to an event routed to Azure Event Grid. The solution must meet the following requirements:

? The executed code must be able to access the private IP address of a Microsoft SQL Server instance that runs on an Azure virtual machine.

? Costs must be minimized.

What should you include in the solution?

- A. Azure Logic Apps in the integrated service environment
- B. Azure Functions in the Dedicated plan and the Basic Azure App Service plan
- C. Azure Logic Apps in the Consumption plan
- D. Azure Functions in the Consumption plan

Correct

To connect to Azure virtual machines using private IP address, we must do Virtual network integration.

Incorrect Answers:

A. Azure Logic Apps in the integrated service environment

Azure Functions dedicated plan is cheaper than Azure Logic Apps ISE.

C. Azure Logic Apps in the Consumption plan

Virtual network integration is supported only on Azure Functions Dedicated plan and Azure Logics Apps ISE.

D. Azure Functions in the Consumption plan

Virtual network integration is supported only on Azure Functions Dedicated plan and Azure Logics Apps ISE.

Reference:

https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale

Overview of plans

The following is a summary of the benefits of the three main hosting plans for Functions:

Plan	Benefits
Consumption plan	Scale automatically and only pay for compute resources when your functions are running. On the Consumption plan, instances of the Functions host are dynamically added and removed based on the number of incoming events. ✓ Default hosting plan. ✓ Pay only when your functions are running. ✓ Scales automatically, even during periods of high load.
Premium plan	Automatically scales based on demand using pre-warmed workers which run applications with no delay after being idle, runs on more powerful instances, and connects to virtual networks. Consider the Azure Functions Premium plan in the following situations: ✓ Your function apps run continuously, or nearly continuously. ✓ You have a high number of small executions and a high execution bill, but low GB seconds in the Consumption plan. ✓ You need more CPU or memory options than what is provided by the Consumption plan. ✓ Your code needs to run longer than the maximum execution time allowed on the Consumption plan. ✓ You require features that aren't available on the Consumption plan, such as virtual network connectivity. ✓ You want to provide a custom Linux image on which to run your functions.
Dedicated plan	Run your functions within an App Service plan at regular App Service plan rates. Best for long-running scenarios where Durable Functions can't be used. Consider an App Service plan in the following situations: ✓ You have existing, underutilized VMs that are already running other App Service instances. ✓ Predictive scaling and costs are required.

Networking features

Feature	Consumption plan	Premium plan	Dedicated plan	ASE	Kubernetes
Inbound IP restrictions and private site access	✅ Yes	✅ Yes	✅ Yes	✅ Yes	✅ Yes
Virtual network integration	❌ No	✅ Yes (Regional)	✅ Yes (Regional and Gateway)	✅ Yes	✅ Yes
Virtual network triggers (non-HTTP)	❌ No	✅ Yes	✅ Yes	✅ Yes	✅ Yes
Hybrid connections (Windows only)	❌ No	✅ Yes	✅ Yes	✅ Yes	✅ Yes
Outbound IP restrictions	❌ No	✅ Yes	✅ Yes	✅ Yes	✅ Yes

34. Question

The developers at your company are building a containerized Python Django app.

You need to recommend platform to host the app. The solution must meet the following requirements:

? Support autoscaling.

? Support continuous deployment from an Azure Container Registry.

? Provide built-in functionality to authenticate app users by using Azure Active Directory (Azure AD).

Which platform should you include in the recommendation?

- A. Azure Container instances
- B. an Azure App Service instance that uses containers
- C. Azure Kubernetes Service (AKS)

Correct

Azure Web Apps for Containers which gives us the flexibility to customize our application dependencies by wrapping those needed libraries in a Docker container.

Azure App Services can be integrated with AAD for app level authentication while AKS can also be integrated with AAD but for components of Kubernetes not the app itself.

Incorrect Answers:

A. Azure Container instances

Azure Container instances does not allow Autoscaling.

C. Azure Kubernetes Service (AKS)

Azure Kubernetes Service (AKS) offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. Unite your development and operations teams on a single platform to rapidly build, deliver, and scale applications with confidence.

Reference:

https://azure.microsoft.com/en-au/services/app-service/containers/

https://azure.microsoft.com/en-gb/services/app-service/#overview

https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization

https://docs.microsoft.com/en-us/azure/developer/python/azure-sdk-authenticate

https://docs.microsoft.com/en-us/azure/app-service/deploy-ci-cd-custom-container

https://docs.microsoft.com/en-us/dotnet/architecture/modernize-with-azure-containers/modernize-existing-apps-to-cloud-optimized/choosing-azure-compute-options-for-container-based-applications

https://devblogs.microsoft.com/premier-developer/running-django-on-azure-web-apps-for-containers-with-docker/

https://docs.microsoft.com/en-us/azure/app-service/configure-authentication-provider-aad

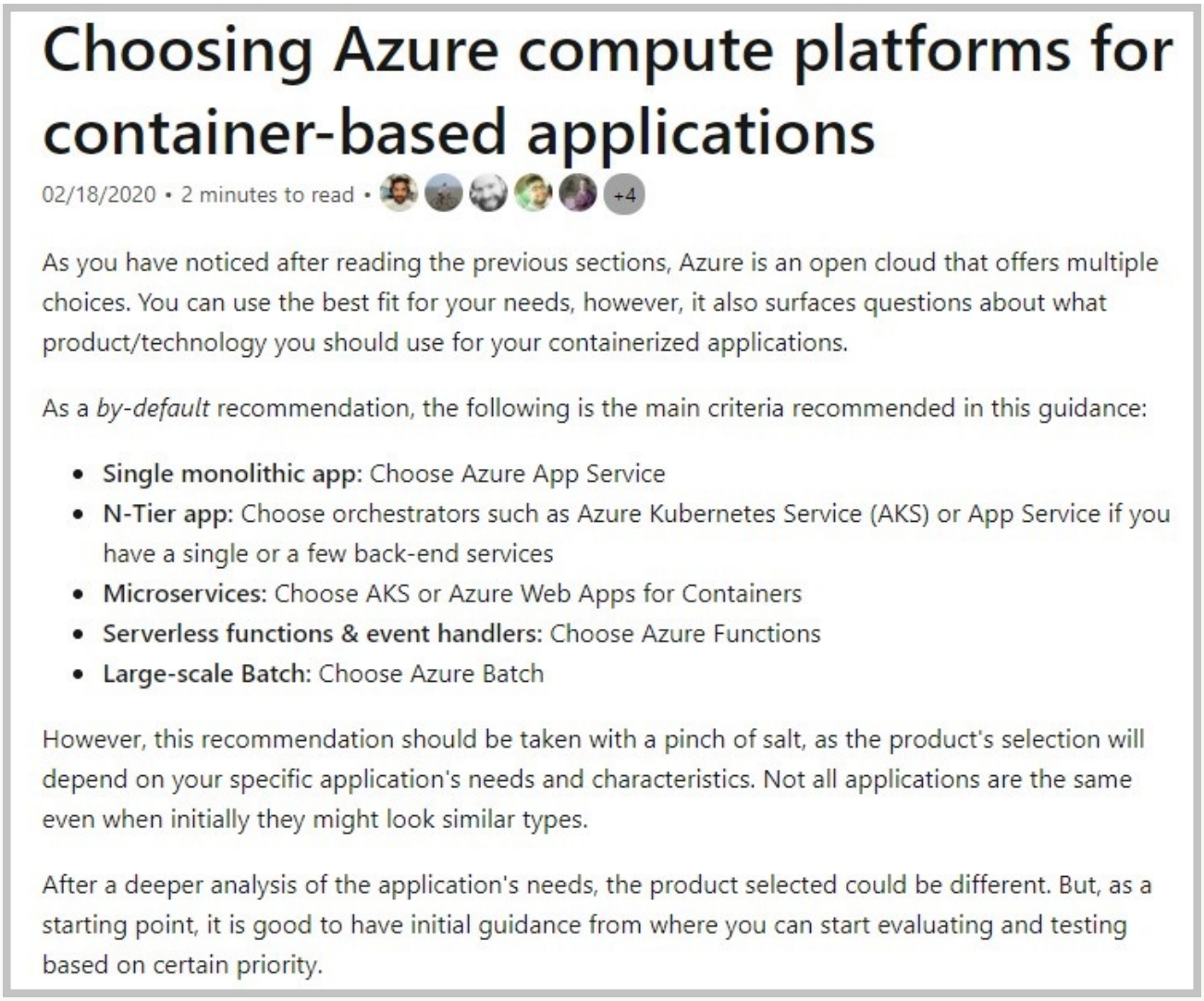
https://docs.microsoft.com/en-us/azure/app-service/environment/app-service-environment-auto-scale

How to authenticate and authorize Python applications on Azure

08/10/2021 • 6 minutes to read • +1

Most cloud applications deployed to Azure need to access other Azure resources such as storage, databases, stored secrets, and so on. To access those resources, the application must be both authenticated and authorized:

- **Authentication** verifies the app's identity with Azure Active Directory.
- **Authorization** determines which operations the authenticated app can perform on any given resource. The authorized operations are defined by the **roles** assigned to the app identity for that resource. In a few cases, such as Azure Key Vault, authorization is also determined by additional **access policies** that are assigned to the app identity.



Choosing Azure compute platforms for container-based applications

02/18/2020 • 2 minutes to read • +4

As you have noticed after reading the previous sections, Azure is an open cloud that offers multiple choices. You can use the best fit for your needs, however, it also surfaces questions about what product/technology you should use for your containerized applications.

As a *by-default* recommendation, the following is the main criteria recommended in this guidance:

- **Single monolithic app:** Choose Azure App Service
- **N-Tier app:** Choose orchestrators such as Azure Kubernetes Service (AKS) or App Service if you have a single or a few back-end services
- **Microservices:** Choose AKS or Azure Web Apps for Containers
- **Serverless functions & event handlers:** Choose Azure Functions
- **Large-scale Batch:** Choose Azure Batch

However, this recommendation should be taken with a pinch of salt, as the product's selection will depend on your specific application's needs and characteristics. Not all applications are the same even when initially they might look similar types.

After a deeper analysis of the application's needs, the product selected could be different. But, as a starting point, it is good to have initial guidance from where you can start evaluating and testing based on certain priority.

35. Question

You have an on-premises network to which you deploy a virtual appliance.

You plan to deploy several Azure virtual machines and connect the on-premises network to Azure by using a Site-to-Site connection.

All network traffic that will be directed from the Azure virtual machines to a specific subnet must flow through the virtual appliance.

You need to recommend solutions to manage network traffic.

Which two options should you recommend? Each correct answer presents a complete solution.

- [ ] A. Configure Azure Traffic Manager
- [x] B. Implement Azure ExpressRoute
- [x] C. Configure a routing table
- [x] D. Implement an Azure virtual network

Incorrect

B: Forced tunneling lets you redirect or “force“ all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing.

This is a critical security requirement for most enterprise IT policies. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic.

Forced tunneling in Azure is configured via virtual network user-defined routes.

C: ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co- location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet.

Note: Scenario is similar to question in the last reference link. Take a look at the two diagrams.

Reference:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm#requirements-and-considerations

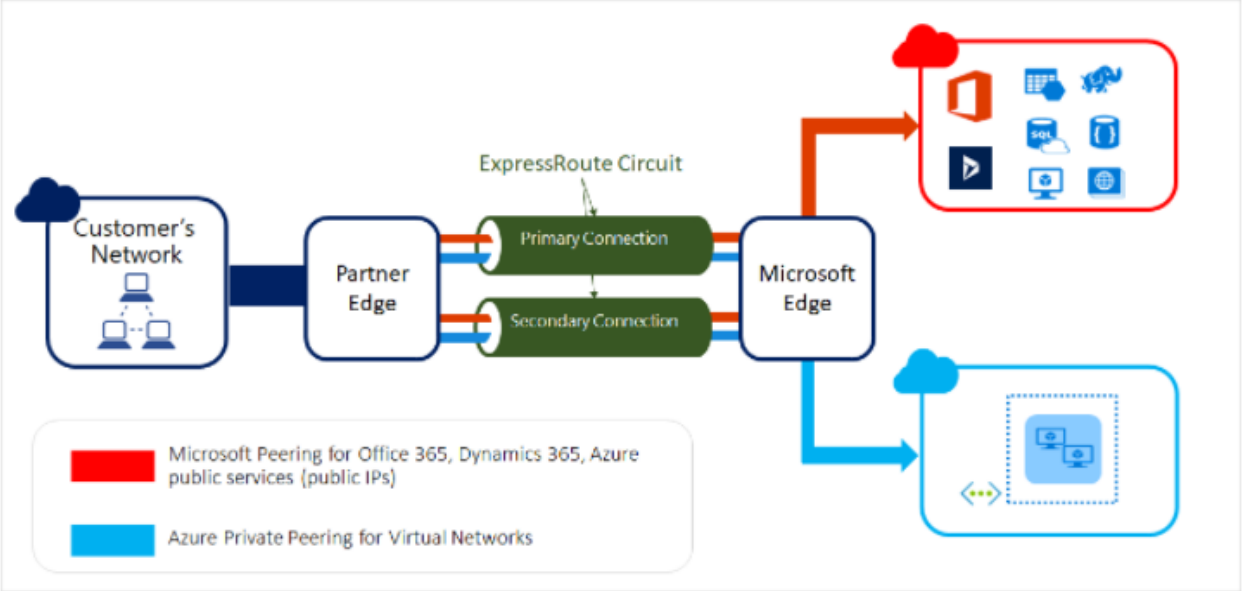
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute#security-considerations

What is Azure ExpressRoute?

10/05/2020 • 5 minutes to read • +9

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections don't go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using ExpressRoute, see ExpressRoute connectivity models.



Note

In the context of ExpressRoute, the Microsoft Edge describes the edge routers on the Microsoft side of the ExpressRoute circuit. This is the ExpressRoute circuit's point of entry into Microsoft's network.

Requirements and considerations

Forced tunneling in Azure is configured using virtual network custom user-defined routes. Redirecting traffic to an on-premises site is expressed as a Default Route to the Azure VPN gateway. For more information about user-defined routing and virtual networks, see Custom user-defined routes.

- Each virtual network subnet has a built-in, system routing table. The system routing table has the following three groups of routes:
  - **Local VNet routes:** Directly to the destination VMs in the same virtual network.
  - **On-premises routes:** To the Azure VPN gateway.
  - **Default route:** Directly to the Internet. Packets destined to the private IP addresses not covered by the previous two routes are dropped.
- This procedure uses user-defined routes (UDR) to create a routing table to add a default route, and then associate the routing table to your VNet subnet(s) to enable forced tunneling on those subnets.
- Forced tunneling must be associated with a VNet that has a route-based VPN gateway. You need to set a "default site" among the cross-premises local sites connected to the virtual network. Also, the on-premises VPN device must be configured using 0.0.0.0/0 as traffic selectors.
- ExpressRoute forced tunneling is not configured via this mechanism, but instead, is enabled by advertising a default route via the ExpressRoute BGP peering sessions. For more information, see the ExpressRoute Documentation.
- When having both VPN Gateway and ExpressRoute Gateway deployed in the same VNet, user-defined routes (UDR) is no longer needed as ExpressRoute Gateway will advertise configured "default site" into VNet.

36. Question

You are developing a sales application that will contain several Azure cloud services and will handle different components of a transaction. Different cloud services will process customer orders, billing, payment, inventory, and shipping.

You need to recommend a solution to enable the cloud services to asynchronously communicate transaction information by using REST messages.

What should you include in the recommendation?

- A. Azure Service Bus
- B. Azure Data Lake
- C. Azure Traffic Manager
- D. Azure Application Gateway

Correct

Asynchronous messaging can be implemented in a variety of different ways: with queues, topics, and subscriptions. Azure Service Bus supports asynchronism via a store and forward mechanism.

Service Bus is a transactional message broker and ensures transactional integrity for all internal operations against its message stores. All transfers of messages inside of Service Bus, such as moving messages to a dead-letter queue or automatic forwarding of messages between entities, are transactional.

Data is transferred between different applications and services using mess ages. A message is a container decorated with metadata, and contains data. The data can be any kind of information, including structured data encoded with the common formats such as the following ones: JSON, XML, Apache Avro, Plain Text.

Some common messaging scenarios are:

Messaging. Transfer business data, such as sales or purchase orders, journals, or inventory movements.

Decouple applications. Improve reliability and scalability of applications and services. Producer and consumer don‘t have to be online or readily available at the same time.

Topics and subscriptions. Enable 1:n relationships between publishers and subscribers, allowing subscribers to select particular messages from a published message stream.

Message sessions. Implement high-scale coordination of workflows and multiplexed transfers that require strict message ordering or message deferral.

Incorrect Answers:

B. Azure Data Lake

Azure Data Lake works with existing IT investments for identity, management, and security for simplified data management and governance. It also integrates seamlessly with operational stores and data warehouses so you can extend current data applications.

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. Traffic Manager also provides your public endpoints with high availability and quick responsiveness

D. Azure Application Gateway

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

Reference:

https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-transactions

https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-async-messaging

https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/messaging

https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview

What is Azure Service Bus?

06/11/2021 • 6 minutes to read • 

Microsoft Azure Service Bus is a fully managed enterprise message broker with message queues and publish-subscribe topics. Service Bus is used to decouple applications and services from each other, providing the following benefits:

- Load-balancing work across competing workers
- Safely routing and transferring data and control across service and application boundaries
- Coordinating transactional work that requires a high-degree of reliability

Asynchronous messaging patterns and high availability

04/23/2021 • 4 minutes to read • 

Asynchronous messaging can be implemented in a variety of different ways. With queues, topics, and subscriptions, Azure Service Bus supports asynchronism via a store and forward mechanism. In normal (synchronous) operation, you send messages to queues and topics, and receive messages from queues and subscriptions. Applications you write depend on these entities always being available. When the entity health changes, due to a variety of circumstances, you need a way to provide a reduced capability entity that can satisfy most needs.

Applications typically use asynchronous messaging patterns to enable a number of communication scenarios. You can build applications in which clients can send messages to services, even when the service is not running. For applications that experience bursts of communications, a queue can help level the load by providing a place to buffer communications. Finally, you can get a simple but effective load balancer to distribute messages across multiple machines.

In order to maintain availability of any of these entities, consider a number of different ways in which these entities can appear unavailable for a durable messaging system. Generally speaking, we see the entity become unavailable to applications we write in the following different ways:

- Unable to send messages.
- Unable to receive messages.
- Unable to manage entities (create, retrieve, update, or delete entities).
- Unable to contact the service.

For each of these failures, different failure modes exist that enable an application to continue to perform work at some level of reduced capability. For example, a system that can send messages but not receive them can still receive orders from customers but cannot process those orders. This topic discusses potential issues that can occur, and how those issues are mitigated. Service Bus has introduced a number of mitigations which you must opt into, and this topic also discusses the rules governing the use of those opt-in mitigations.

Transactions in Service Bus

A *transaction* groups two or more operations together into an *execution scope*. By nature, such a transaction must ensure that all operations belonging to a given group of operations either succeed or fail jointly. In this respect transactions act as one unit, which is often referred to as *atomicity*.

Service Bus is a transactional message broker and ensures transactional integrity for all internal operations against its message stores. All transfers of messages inside of Service Bus, such as moving messages to a dead-letter queue or automatic forwarding of messages between entities, are transactional. As such, if Service Bus accepts a message, it has already been stored and labeled with a sequence number. From then on, any message transfers within Service Bus are coordinated operations across entities, and will neither lead to loss (source succeeds and target fails) or to duplication (source fails and target succeeds) of the message.

Service Bus supports grouping operations against a single messaging entity (queue, topic, subscription) within the scope of a transaction. For example, you can send several messages to one queue from within a transaction scope, and the messages will only be committed to the queue's log when the transaction successfully completes.

37. Question

You plan to run an image rendering workload in Azure. The workload uses parallel compute processes. What is the best service to use to run the workload? More than one answer choice may achieve the goal. Select the BEST answer.

- A. an Azure virtual machine scale set
- B. Azure Function App
- C. Azure Kubernetes Service (AKS)
- D. Azure Batch

Correct

Azure Batch works well with intrinsically parallel (also known as “embarrassingly parallel“) workloads. Intrinsically parallel workloads are those where the applications can run independently, and each instance completes part of the work. When the applications are executing, they might access some common data, but they do not communicate with other instances of the application. Intrinsically parallel workloads can therefore run at a large scale, determined by the amount of compute resources available to run applications simultaneously.

Some examples of intrinsically parallel workloads you can bring to Batch:

? Financial risk modeling using Monte Carlo simulations

? VFX and 3D image rendering

? Image analysis and processing

? Media transcoding

? Genetic sequence analysis

? Optical character recognition (OCR)

? Data ingestion, processing, and ETL operations

? Software test execution

Incorrect Answers:

A. 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. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs.

B. Azure Function App

This option may work for simple to medium compute workloads. high-performance computing is recommended.

C. Azure Kubernetes Service (AKS)

Azure Kubernetes Service (AKS) offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. Unite your development and operations teams on a single platform to rapidly build, deliver, and scale applications with confidence.

Reference:

https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview

What is Azure Batch?

06/11/2021 • 5 minutes to read • +10

Use Azure Batch to run large-scale parallel and high-performance computing (HPC) batch jobs efficiently in Azure. Azure Batch creates and manages a pool of compute nodes (virtual machines), installs the applications you want to run, and schedules jobs to run on the nodes. There's no cluster or job scheduler software to install, manage, or scale. Instead, you use Batch APIs and tools, command-line scripts, or the Azure portal to configure, manage, and monitor your jobs.

Developers can use Batch as a platform service to build SaaS applications or client apps where large-scale execution is required. For example, you can build a service with Batch to run a Monte Carlo risk simulation for a financial services company, or a service to process many images.

There is no additional charge for using Batch. You only pay for the underlying resources consumed, such as the virtual machines, storage, and networking.

For a comparison between Batch and other HPC solution options in Azure, see High Performance Computing (HPC) on Azure.

Run parallel workloads

Batch works well with intrinsically parallel (also known as "embarrassingly parallel") workloads. These workloads have applications which can run independently, with each instance completing part of the work. When the applications are executing, they might access some common data, but they don't communicate with other instances of the application. Intrinsically parallel workloads can therefore run at a large scale, determined by the amount of compute resources available to run applications simultaneously.

Some examples of intrinsically parallel workloads you can bring to Batch:

- Financial risk modeling using Monte Carlo simulations
- VFX and 3D image rendering
- Image analysis and processing
- Media transcoding
- Genetic sequence analysis
- Optical character recognition (OCR)
- Data ingestion, processing, and ETL operations
- Software test execution

38. Question

You are designing a microservices architecture that will use Azure Kubernetes Service (AKS) to host pods that run containers. Each pod deployment will host a separate API. Each API will be implemented as a separate service.

You need to recommend a solution to make the APIs available to external users from Azure API Management. The solution must meet the following requirements:

? Control access to the APIs by using mutual TLS authentication between API Management and the AKS-based APIs.

? Provide access to the APIs by using a single IP address.

What should you recommend to provide access to the APIs?

- A. the LoadBalancer service in AKS
- B. custom network security groups (NSGs)
- C. the Ingress Controller in AKS

Correct

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. Kubernetes ingress resources are used to configure the ingress rules and routes for individual Kubernetes services. Using an ingress controller and ingress rules, a single IP address can be used to route traffic to multiple services in a Kubernetes cluster.

Incorrect Answers:

A. the LoadBalancer service

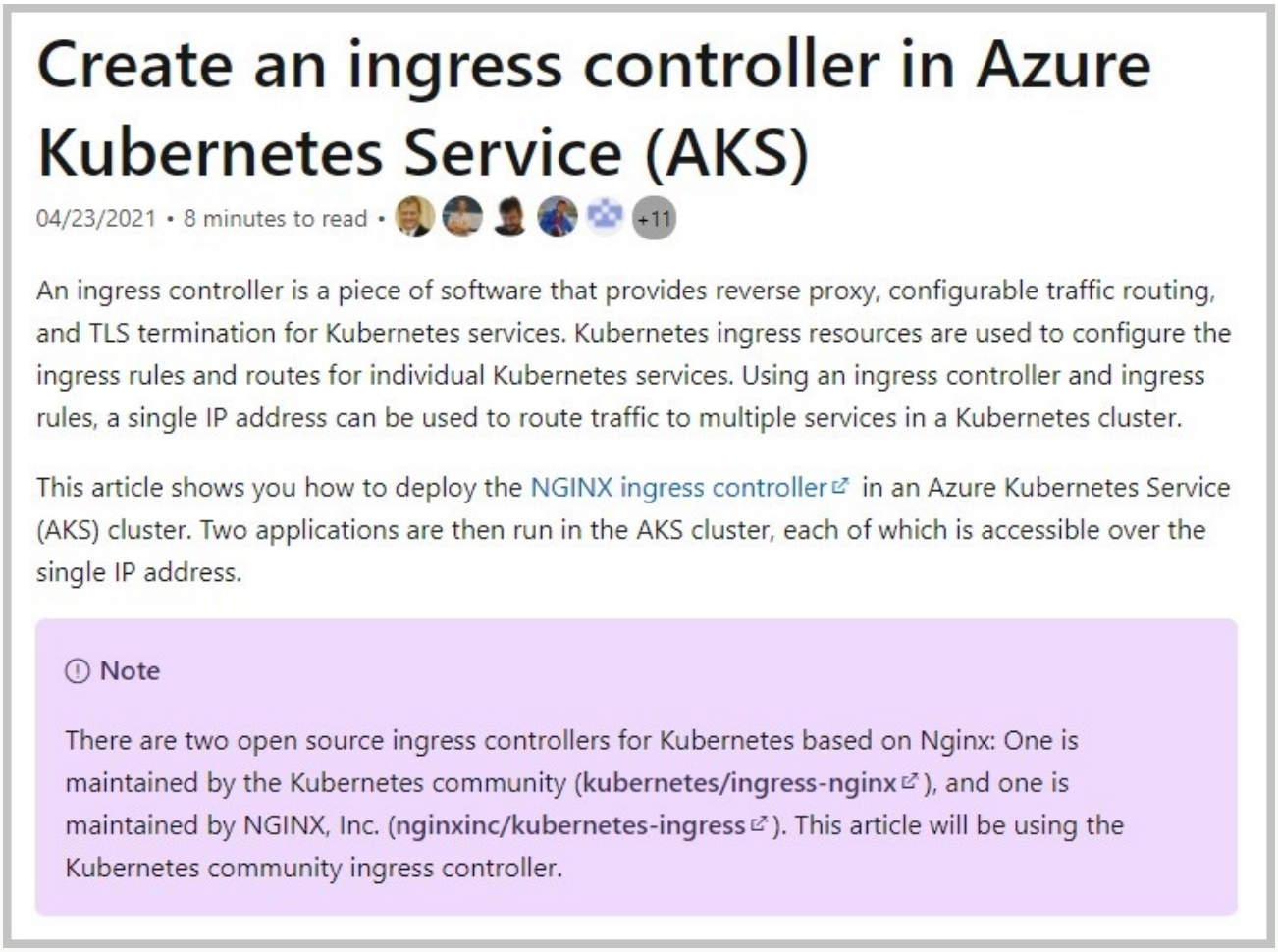
Mutual authentication is not supported.

B. custom network security groups (NSGs)

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.

Reference:

https://docs.microsoft.com/en-us/azure/aks/ingress-basic



Create an ingress controller in Azure Kubernetes Service (AKS)

04/23/2021 • 8 minutes to read • +11

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. Kubernetes ingress resources are used to configure the ingress rules and routes for individual Kubernetes services. Using an ingress controller and ingress rules, a single IP address can be used to route traffic to multiple services in a Kubernetes cluster.

This article shows you how to deploy the NGINX ingress controller in an Azure Kubernetes Service (AKS) cluster. Two applications are then run in the AKS cluster, each of which is accessible over the single IP address.

Note

There are two open source ingress controllers for Kubernetes based on Nginx: One is maintained by the Kubernetes community (**kubernetes/ingress-nginx**), and one is maintained by NGINX, Inc. (**nginxinc/kubernetes-ingress**). This article will be using the Kubernetes community ingress controller.

39. Question

You are designing a cost-optimized solution that uses Azure Batch to run two types of jobs on Linux nodes. The first job type will consist of short-running tasks for a development environment. The second job type will consist of long running Message Passing Interface (MPI) applications for a production environment that requires timely job completion.

You need to recommend the pool type and node type for each job type. The solution must minimize compute charges and leverage Azure Hybrid Benefit whenever possible.

What should you recommend for first job?

- A. Batch service and dedicated virtual machines
- **B. Batch service and low-priority virtual machines**
- C. User subscription and dedicated virtual machines
- D. User subscription and low-priority virtual machines

Correct

In an Azure Batch workflow, a compute node (or node) is a virtual machine that processes a portion of your application's workload. A pool is a collection of these nodes for your application to runs on. This article explains more about nodes and pools, along with considerations when creating and using them in an Azure Batch workflow.

Batch accounts

All processing and resources are associated with a Batch account. When your application makes a request against the Batch service, it authenticates the request using the Azure Batch account name, the URL of the account, and either an access key or an Azure Active Directory token.

Node type and target

When you create a pool, you can specify which types of nodes you want and the target number for each. The two types of nodes are:

Dedicated nodes. Dedicated compute nodes are reserved for your workloads. They are more expensive than low-priority nodes, but they are guaranteed to never be preempted.

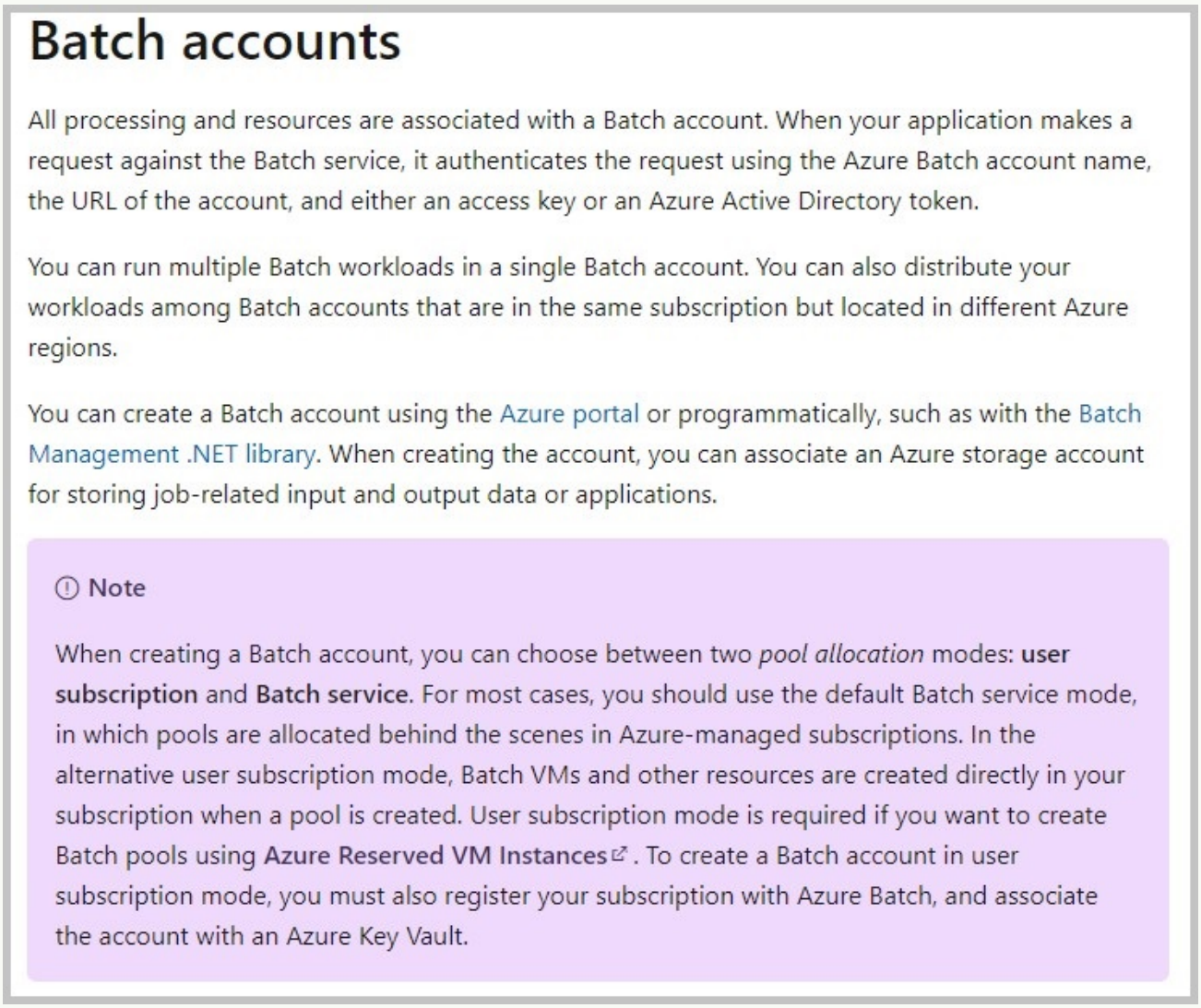
Low-priority nodes. Low-priority nodes take advantage of surplus capacity in Azure to run your Batch workloads. Low-priority nodes are less expensive per hour than dedicated nodes, and enable workloads requiring significant compute power. For more information, see Use low-priority VMs with Batch.

Reference:

https://docs.microsoft.com/en-us/azure/batch/accounts#batch-accounts

https://docs.microsoft.com/en-us/azure/batch/batch-low-pri-vms#batch-support-for-low-priority-vms

https://docs.microsoft.com/en-us/azure/batch/nodes-and-pools#node-type-and-target



Batch accounts

All processing and resources are associated with a Batch account. When your application makes a request against the Batch service, it authenticates the request using the Azure Batch account name, the URL of the account, and either an access key or an Azure Active Directory token.

You can run multiple Batch workloads in a single Batch account. You can also distribute your workloads among Batch accounts that are in the same subscription but located in different Azure regions.

You can create a Batch account using the Azure portal or programmatically, such as with the Batch Management .NET library. When creating the account, you can associate an Azure storage account for storing job-related input and output data or applications.

Note

When creating a Batch account, you can choose between two *pool allocation* modes: **user subscription** and **Batch service**. For most cases, you should use the default Batch service mode, in which pools are allocated behind the scenes in Azure-managed subscriptions. In the alternative user subscription mode, Batch VMs and other resources are created directly in your subscription when a pool is created. User subscription mode is required if you want to create Batch pools using **Azure Reserved VM Instances**. To create a Batch account in user subscription mode, you must also register your subscription with Azure Batch, and associate the account with an Azure Key Vault.

Node type and target

When you create a pool, you can specify which types of nodes you want and the target number for each. The two types of nodes are:

- **Dedicated nodes**. Dedicated compute nodes are reserved for your workloads. They are more expensive than low-priority nodes, but they are guaranteed to never be preempted.
- **Low-priority nodes**. Low-priority nodes take advantage of surplus capacity in Azure to run your Batch workloads. Low-priority nodes are less expensive per hour than dedicated nodes, and enable workloads requiring significant compute power. For more information, see Use low-priority VMs with Batch.

Low-priority nodes may be preempted when Azure has insufficient surplus capacity. If a node is preempted while running tasks, the tasks are requeued and run again once a compute node becomes available again. Low-priority nodes are a good option for workloads where the job completion time is flexible and the work is distributed across many nodes. Before you decide to use low-priority nodes for your scenario, make sure that any work lost due to preemption will be minimal and easy to recreate.

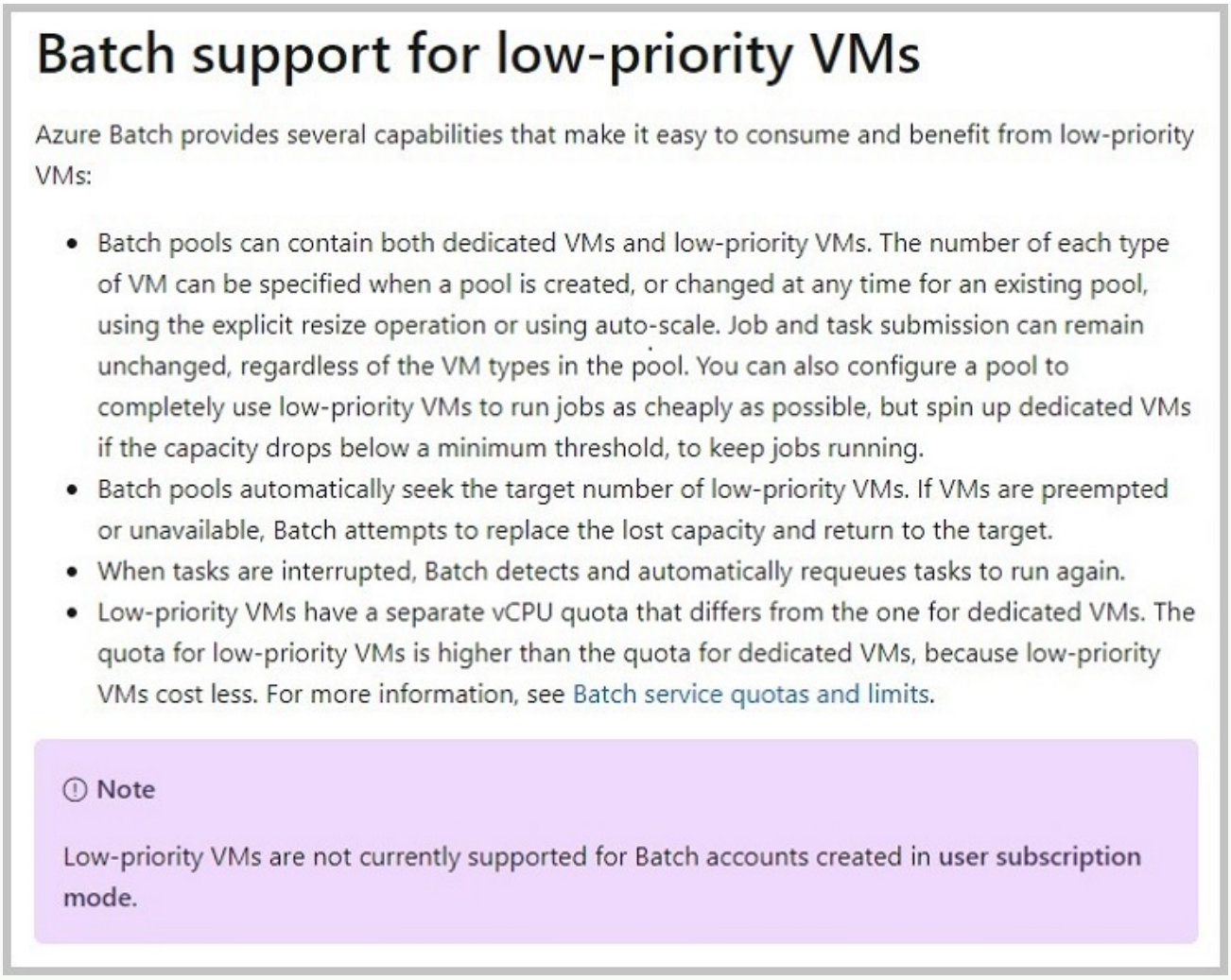
You can have both low-priority and dedicated compute nodes in the same pool. Each type of node has its own target setting, for which you can specify the desired number of nodes.

The number of compute nodes is referred to as a *target* because, in some situations, your pool might not reach the desired number of nodes. For example, a pool might not achieve the target if it reaches the core quota for your Batch account first. Or, the pool might not achieve the target if you have applied an automatic scaling formula to the pool that limits the maximum number of nodes.

For pricing information for both low-priority and dedicated nodes, see Batch Pricing.

Node size

When you create an Azure Batch pool, you can choose from among almost all the VM families and sizes available in Azure. Azure offers a range of VM sizes for different workloads, including specialized HPC or GPU-enabled VM sizes. Note that node sizes can only be chosen at the time a pool is created. In other words, once a pool is created, its node size cannot be changed.



Batch support for low-priority VMs

Azure Batch provides several capabilities that make it easy to consume and benefit from low-priority VMs:

- Batch pools can contain both dedicated VMs and low-priority VMs. The number of each type of VM can be specified when a pool is created, or changed at any time for an existing pool, using the explicit resize operation or using auto-scale. Job and task submission can remain unchanged, regardless of the VM types in the pool. You can also configure a pool to completely use low-priority VMs to run jobs as cheaply as possible, but spin up dedicated VMs if the capacity drops below a minimum threshold, to keep jobs running.
- Batch pools automatically seek the target number of low-priority VMs. If VMs are preempted or unavailable, Batch attempts to replace the lost capacity and return to the target.
- When tasks are interrupted, Batch detects and automatically requeues tasks to run again.
- Low-priority VMs have a separate vCPU quota that differs from the one for dedicated VMs. The quota for low-priority VMs is higher than the quota for dedicated VMs, because low-priority VMs cost less. For more information, see Batch service quotas and limits.

Note

Low-priority VMs are not currently supported for Batch accounts created in user subscription mode.

40. Question

You are designing a cost-optimized solution that uses Azure Batch to run two types of jobs on Linux nodes. The first job

type will consist of short-running tasks for a development environment. The second job type will consist of long

running Message Passing Interface (MPI) applications for a production environment that requires timely job completion.

You need to recommend the pool type and node type for each job type. The solution must minimize compute charges

and leverage Azure Hybrid Benefit whenever possible.

What should you recommend for second job?

- A. Batch service and dedicated virtual machines
- B. Batch service and low-priority virtual machines
- C. User subscription and dedicated virtual machines
- D. User subscription and low-priority virtual machines

Incorrect

When creating a Batch account, you can choose between two pool allocation modes: user subscription and Batch service. For most cases, you should use the default Batch service mode, in which pools are allocated behind the scenes in Azure-managed subscriptions. In the alternative user subscription mode, Batch VMs and other resources are created directly in your subscription when a pool is created. User subscription mode is required if you want to create Batch pools using Azure Reserved VM Instances. To create a Batch account in user subscription mode, you must also register your subscription with Azure Batch, and associate the account with an Azure Key Vault.

Dedicated nodes. Dedicated compute nodes are reserved for your workloads. They are more expensive than low-priority nodes, but they are guaranteed to never be preempted.

See the requirement leverage Azure Hybrid Benefit whenever possible

Reference:

https://docs.microsoft.com/en-us/azure/batch/accounts#batch-accounts

https://docs.microsoft.com/en-us/azure/batch/batch-low-pri-vms#batch-support-for-low-priority-vms

https://docs.microsoft.com/en-us/azure/batch/nodes-and-pools#node-type-and-target

Node type and target

When you create a pool, you can specify which types of nodes you want and the target number for each. The two types of nodes are:

- **Dedicated nodes**. Dedicated compute nodes are reserved for your workloads. They are more expensive than low-priority nodes, but they are guaranteed to never be preempted.
- **Low-priority nodes**. Low-priority nodes take advantage of surplus capacity in Azure to run your Batch workloads. Low-priority nodes are less expensive per hour than dedicated nodes, and enable workloads requiring significant compute power. For more information, see Use low-priority VMs with Batch.

Low-priority nodes may be preempted when Azure has insufficient surplus capacity. If a node is preempted while running tasks, the tasks are requeued and run again once a compute node becomes available again. Low-priority nodes are a good option for workloads where the job completion time is flexible and the work is distributed across many nodes. Before you decide to use low-priority nodes for your scenario, make sure that any work lost due to preemption will be minimal and easy to recreate.

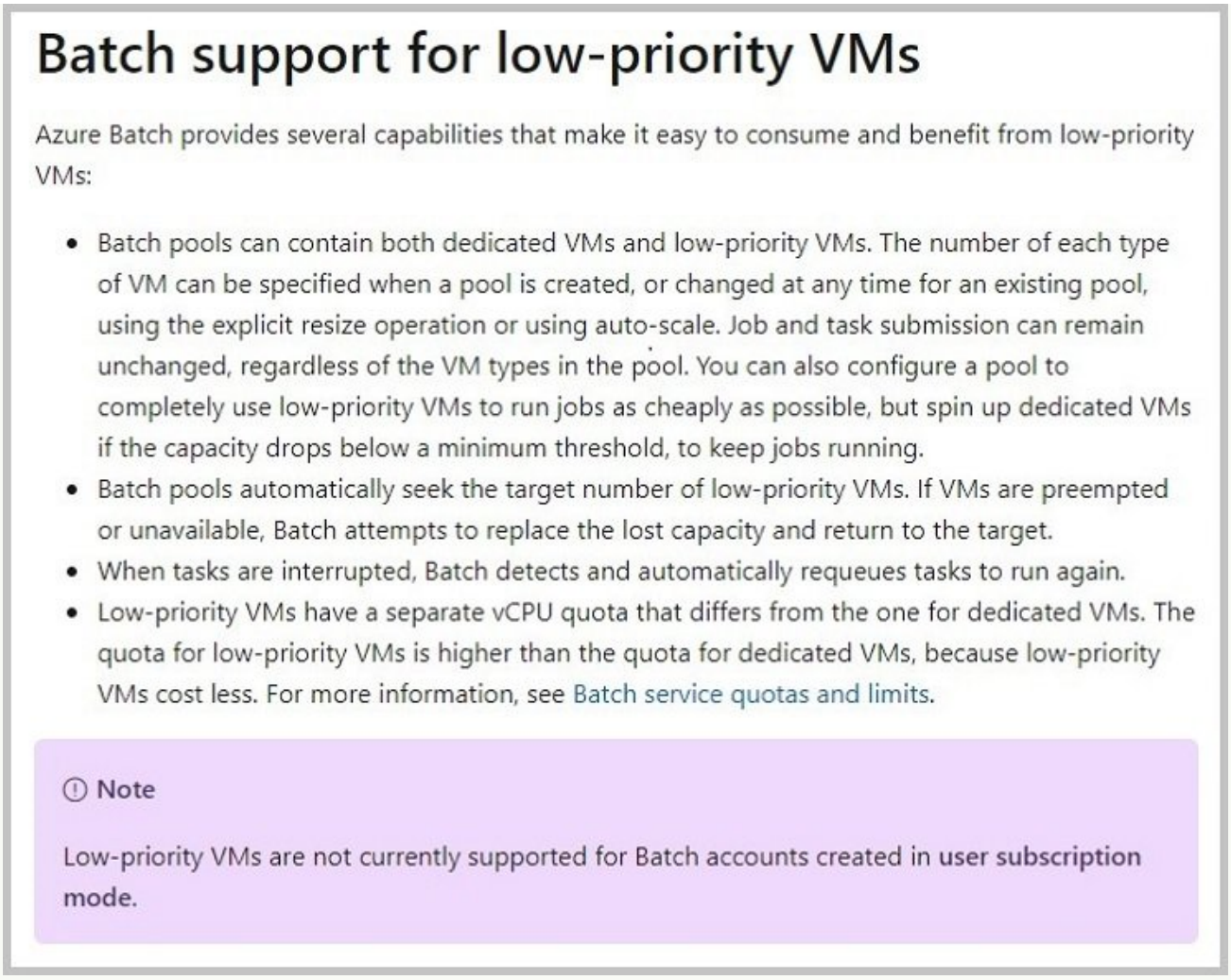
You can have both low-priority and dedicated compute nodes in the same pool. Each type of node has its own target setting, for which you can specify the desired number of nodes.

The number of compute nodes is referred to as a *target* because, in some situations, your pool might not reach the desired number of nodes. For example, a pool might not achieve the target if it reaches the core quota for your Batch account first. Or, the pool might not achieve the target if you have applied an automatic scaling formula to the pool that limits the maximum number of nodes.

For pricing information for both low-priority and dedicated nodes, see Batch Pricing.

Node size

When you create an Azure Batch pool, you can choose from among almost all the VM families and sizes available in Azure. Azure offers a range of VM sizes for different workloads, including specialized HPC or GPU-enabled VM sizes. Note that node sizes can only be chosen at the time a pool is created. In other words, once a pool is created, its node size cannot be changed.



Batch support for low-priority VMs

Azure Batch provides several capabilities that make it easy to consume and benefit from low-priority VMs:

- Batch pools can contain both dedicated VMs and low-priority VMs. The number of each type of VM can be specified when a pool is created, or changed at any time for an existing pool, using the explicit resize operation or using auto-scale. Job and task submission can remain unchanged, regardless of the VM types in the pool. You can also configure a pool to completely use low-priority VMs to run jobs as cheaply as possible, but spin up dedicated VMs if the capacity drops below a minimum threshold, to keep jobs running.
- Batch pools automatically seek the target number of low-priority VMs. If VMs are preempted or unavailable, Batch attempts to replace the lost capacity and return to the target.
- When tasks are interrupted, Batch detects and automatically requeues tasks to run again.
- Low-priority VMs have a separate vCPU quota that differs from the one for dedicated VMs. The quota for low-priority VMs is higher than the quota for dedicated VMs, because low-priority VMs cost less. For more information, see Batch service quotas and limits.

ⓘ Note

Low-priority VMs are not currently supported for Batch accounts created in user subscription mode.

41. 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 plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

? Support rate limiting.

? Balance requests between all instances.

? Ensure that users can access the app in the event of a regional outage.

Solution: You use Azure Front Door to provide access to the app.

Does this meet the goal?

- A. Yes
- B. No

Correct

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications.

The Azure Web Application Firewall (WAF) rate limit rule for Azure Front Door controls the number of requests allowed from clients during a one-minute duration.

Reference:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell

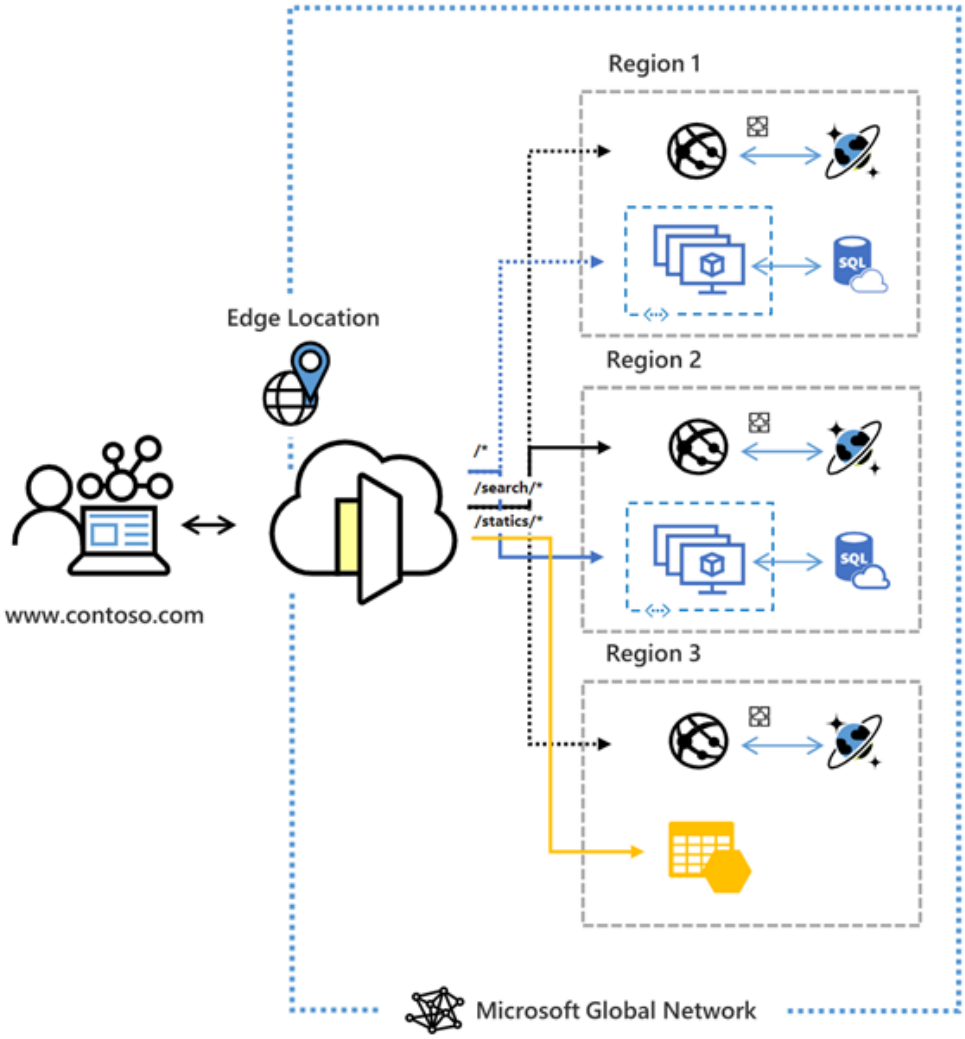
What is Azure Front Door?

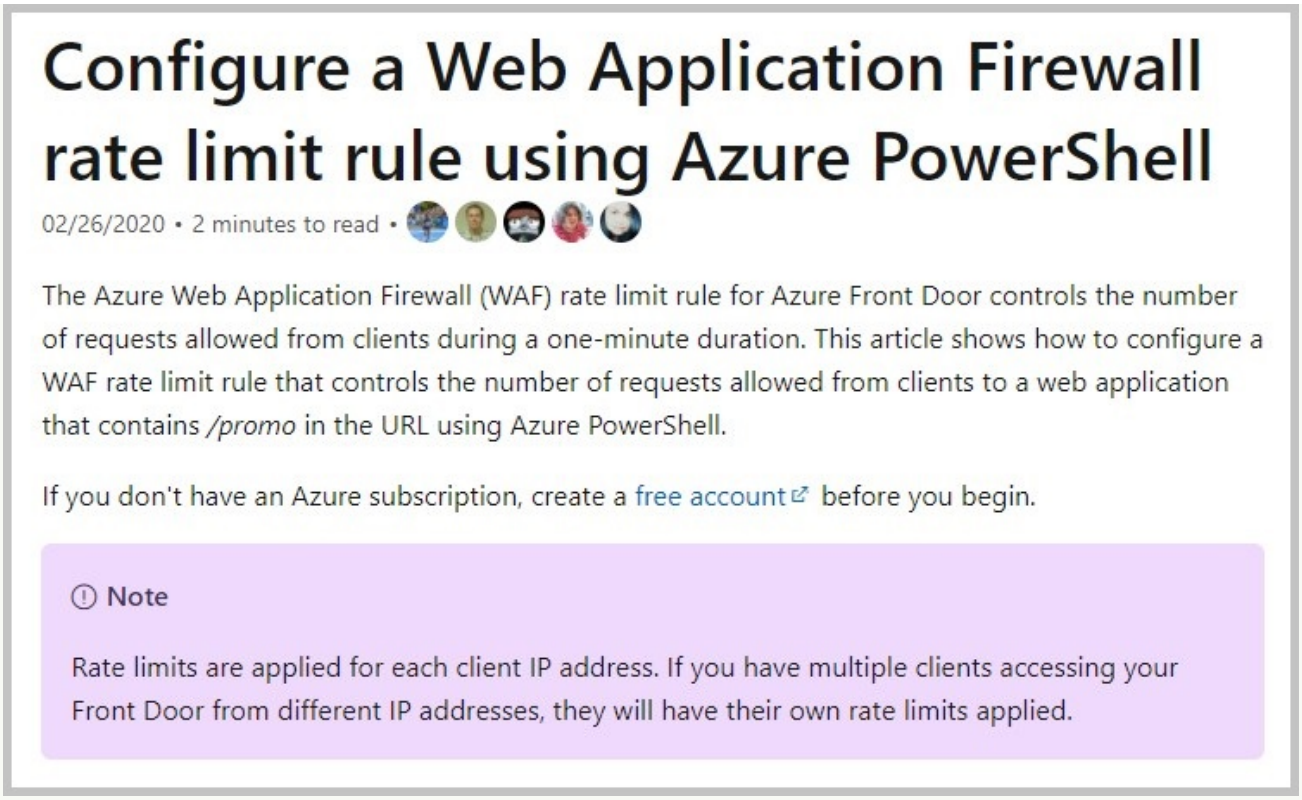
03/09/2021 • 2 minutes to read • +6

Important

This documentation is for Azure Front Door. Looking for information on Azure Front Door Standard/Premium (Preview)? View here.

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.





Configure a Web Application Firewall rate limit rule using Azure PowerShell

02/26/2020 • 2 minutes to read •

The Azure Web Application Firewall (WAF) rate limit rule for Azure Front Door controls the number of requests allowed from clients during a one-minute duration. This article shows how to configure a WAF rate limit rule that controls the number of requests allowed from clients to a web application that contains */promo* in the URL using Azure PowerShell.

If you don't have an Azure subscription, create a free account before you begin.

Note

Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied.

42. 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 plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

? Support rate limiting.

? Balance requests between all instances.

? Ensure that users can access the app in the event of a regional outage.

Solution: You use Azure Load Balancer to provide access to the app.

Does this meet the goal?

- A. Yes
- B. No

Correct

Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances but it does not provide high availability at the regional level.

Instead use Azure Front Door to provide access to the app

Reference:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell

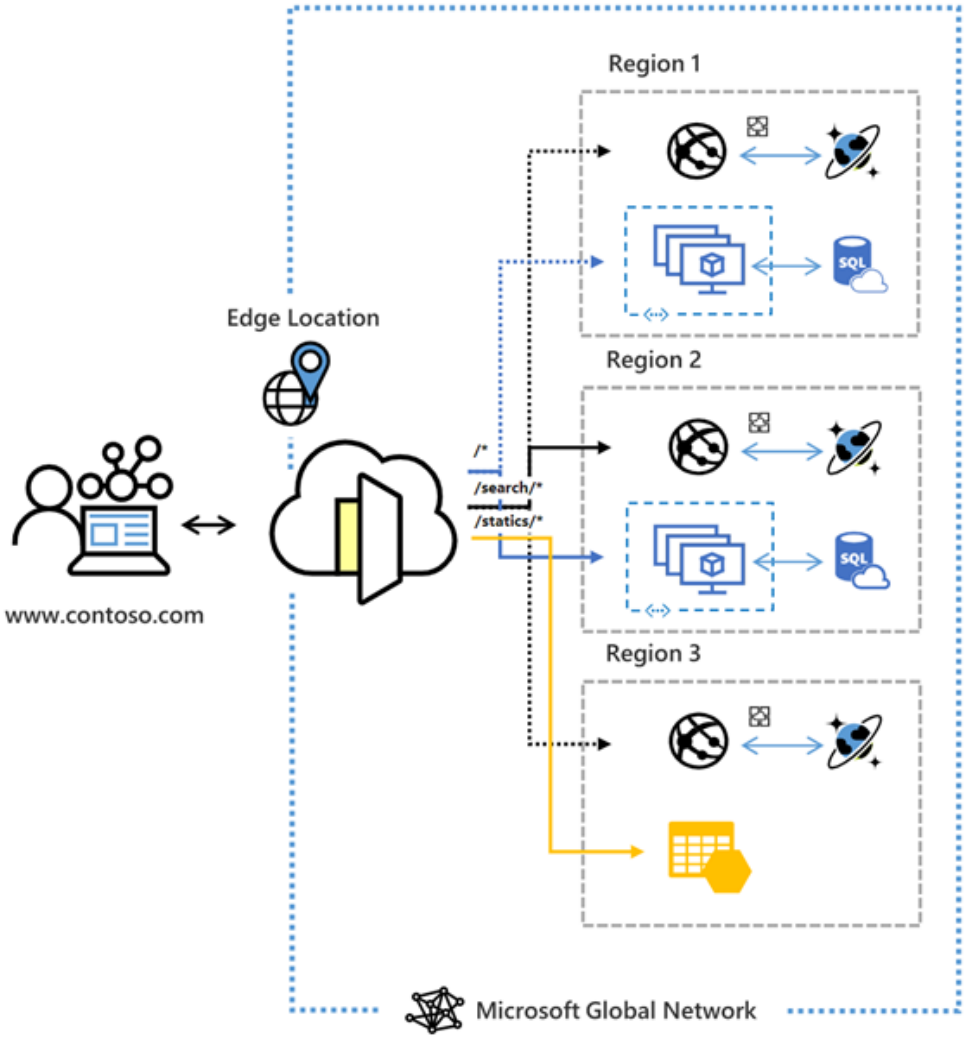
What is Azure Front Door?

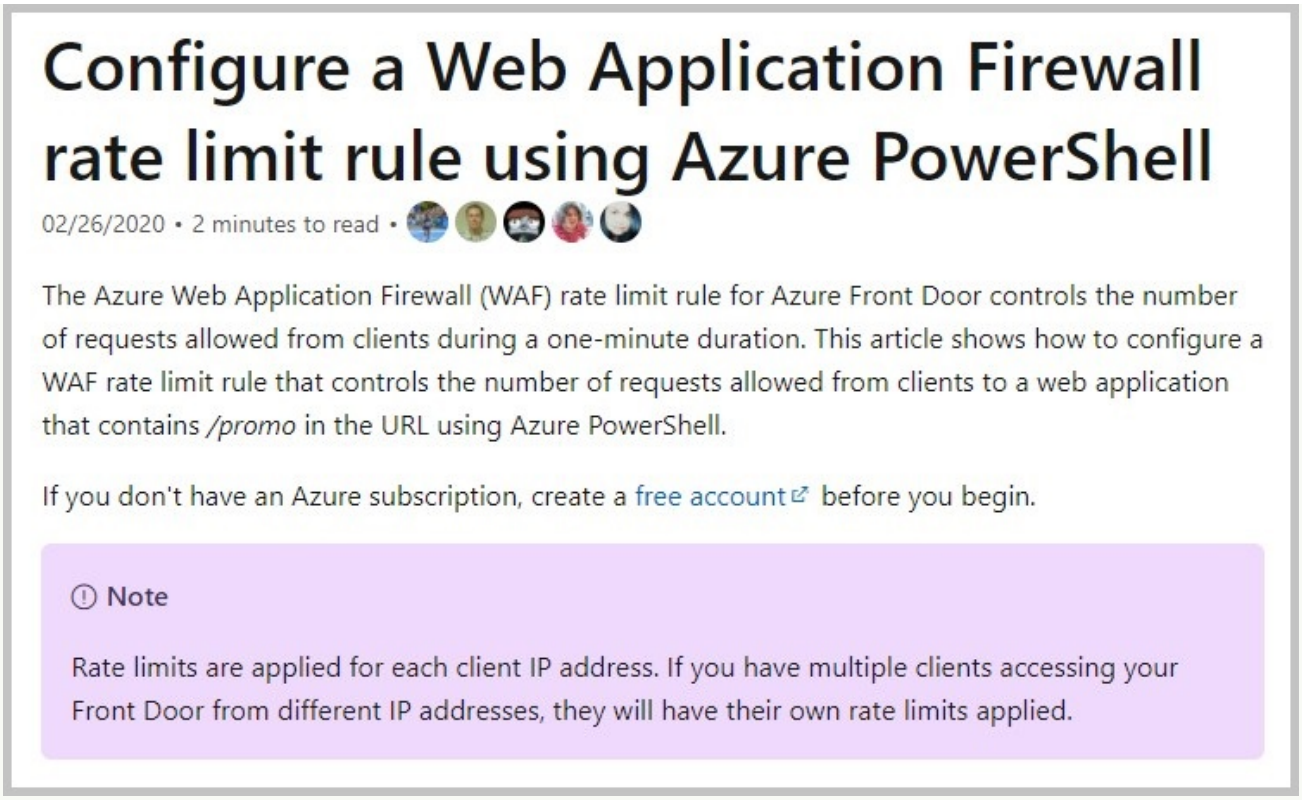
03/09/2021 • 2 minutes to read • +6

Important

This documentation is for Azure Front Door. Looking for information on Azure Front Door Standard/Premium (Preview)? View here.

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.





Configure a Web Application Firewall rate limit rule using Azure PowerShell

02/26/2020 • 2 minutes to read •

The Azure Web Application Firewall (WAF) rate limit rule for Azure Front Door controls the number of requests allowed from clients during a one-minute duration. This article shows how to configure a WAF rate limit rule that controls the number of requests allowed from clients to a web application that contains */promo* in the URL using Azure PowerShell.

If you don't have an Azure subscription, create a free account before you begin.

Note

Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied.

43. 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 plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

? Support rate limiting.

? Balance requests between all instances.

? Ensure that users can access the app in the event of a regional outage.

Solution: You use Azure Traffic Manager to provide access to the app.

Does this meet the goal?

- A. Yes
- B. No

Correct

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. It does not provide rate limiting.

Instead use Azure Front Door to provide access to the app

Reference:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell

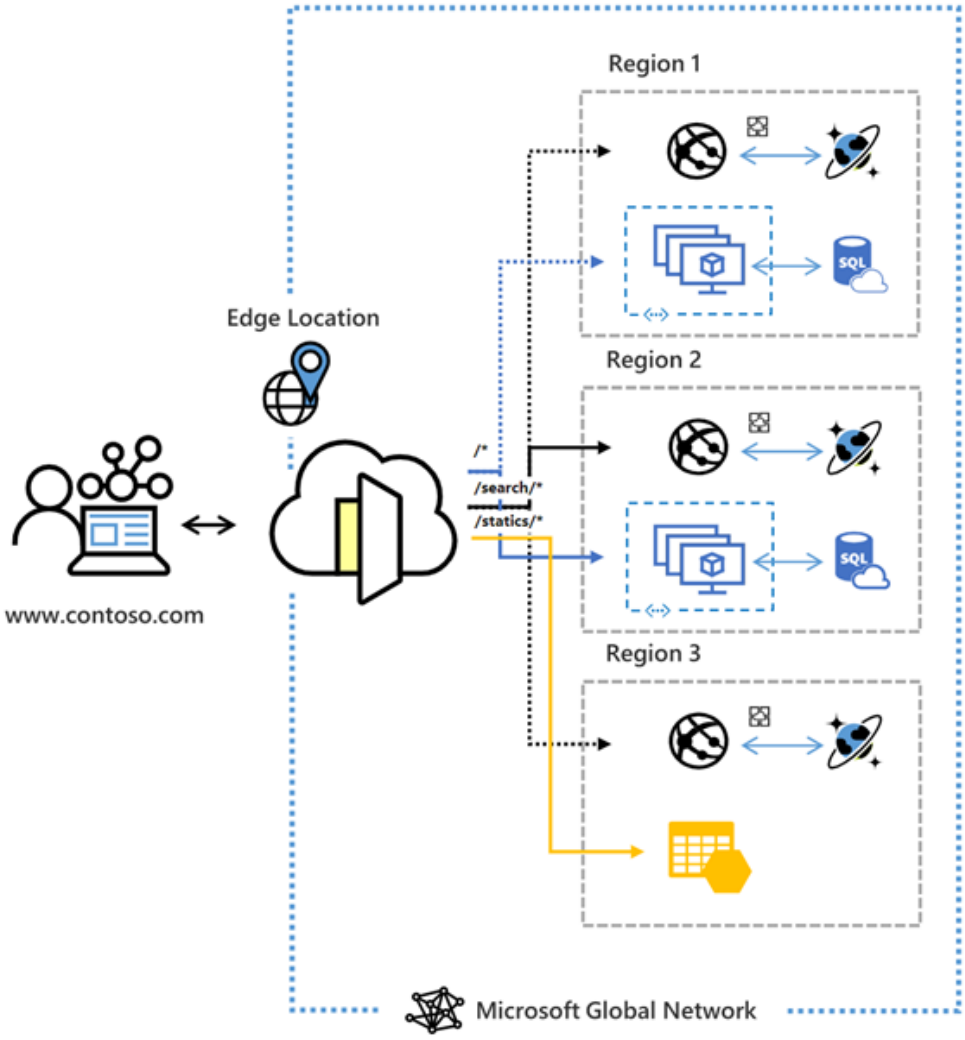
What is Azure Front Door?

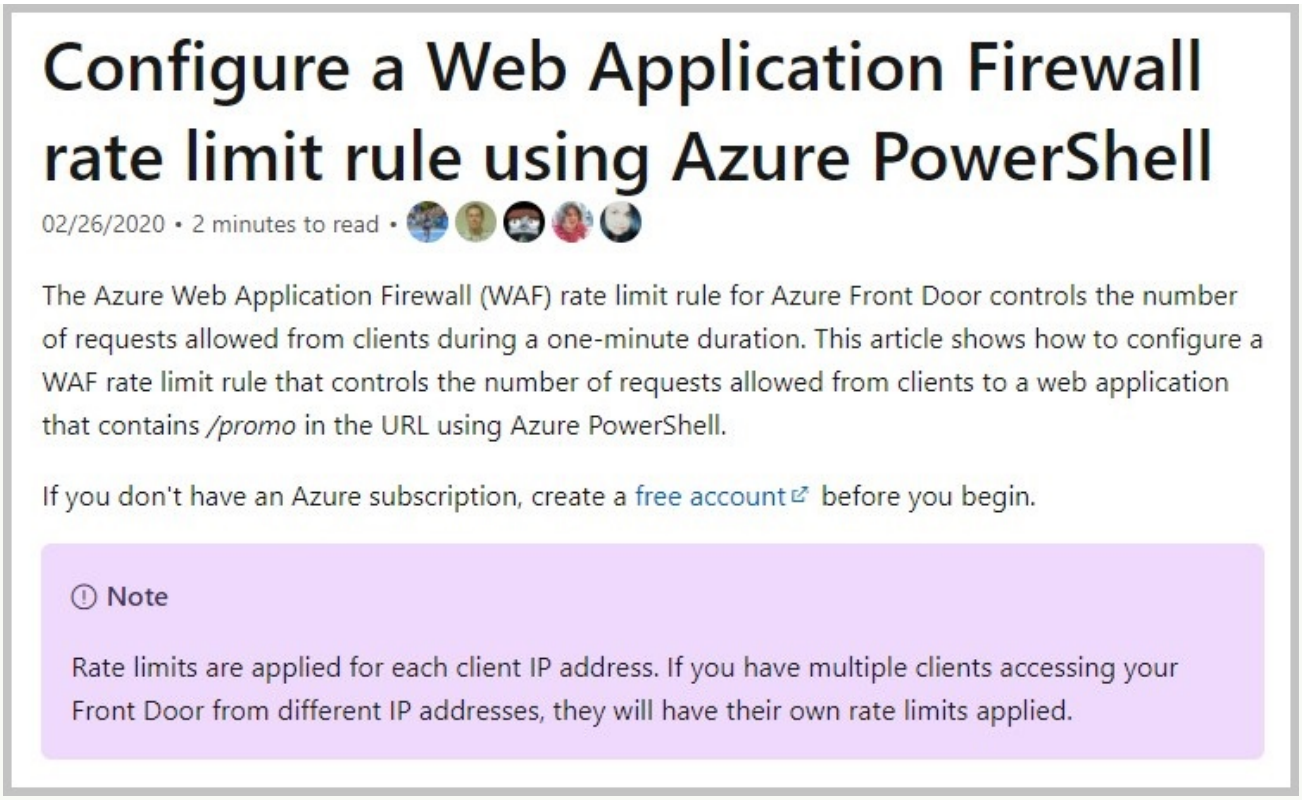
03/09/2021 • 2 minutes to read • +6

Important

This documentation is for Azure Front Door. Looking for information on Azure Front Door Standard/Premium (Preview)? View here.

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.





Configure a Web Application Firewall rate limit rule using Azure PowerShell

02/26/2020 • 2 minutes to read •

The Azure Web Application Firewall (WAF) rate limit rule for Azure Front Door controls the number of requests allowed from clients during a one-minute duration. This article shows how to configure a WAF rate limit rule that controls the number of requests allowed from clients to a web application that contains */promo* in the URL using Azure PowerShell.

If you don't have an Azure subscription, create a free account before you begin.

Note

Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied.

44. 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 plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

? Support rate limiting.

? Balance requests between all instances.

? Ensure that users can access the app in the event of a regional outage.

Solution: You use Azure Application Gateway to provide access to the app

Does this meet the goal?

- A. Yes
- B. No

Correct

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

Instead use Azure Front Door to provide access to the app

Reference:

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell

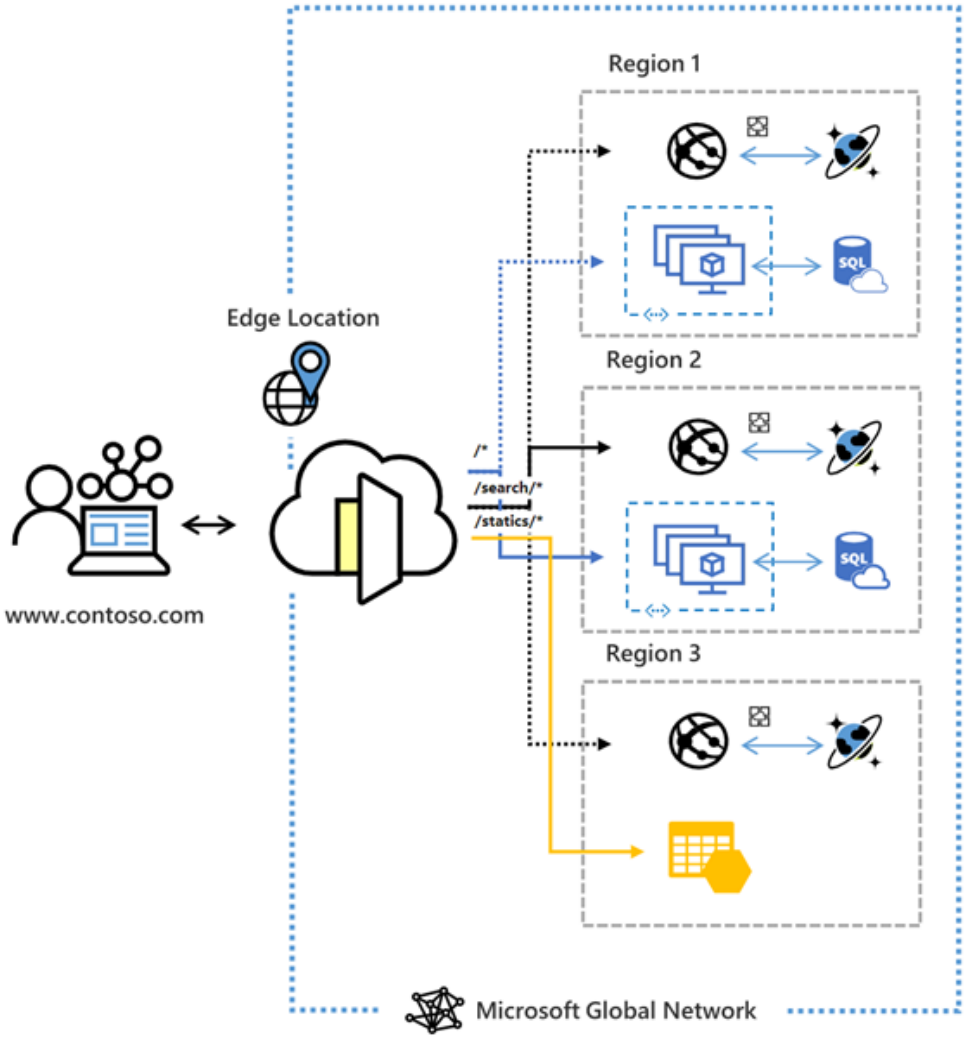
What is Azure Front Door?

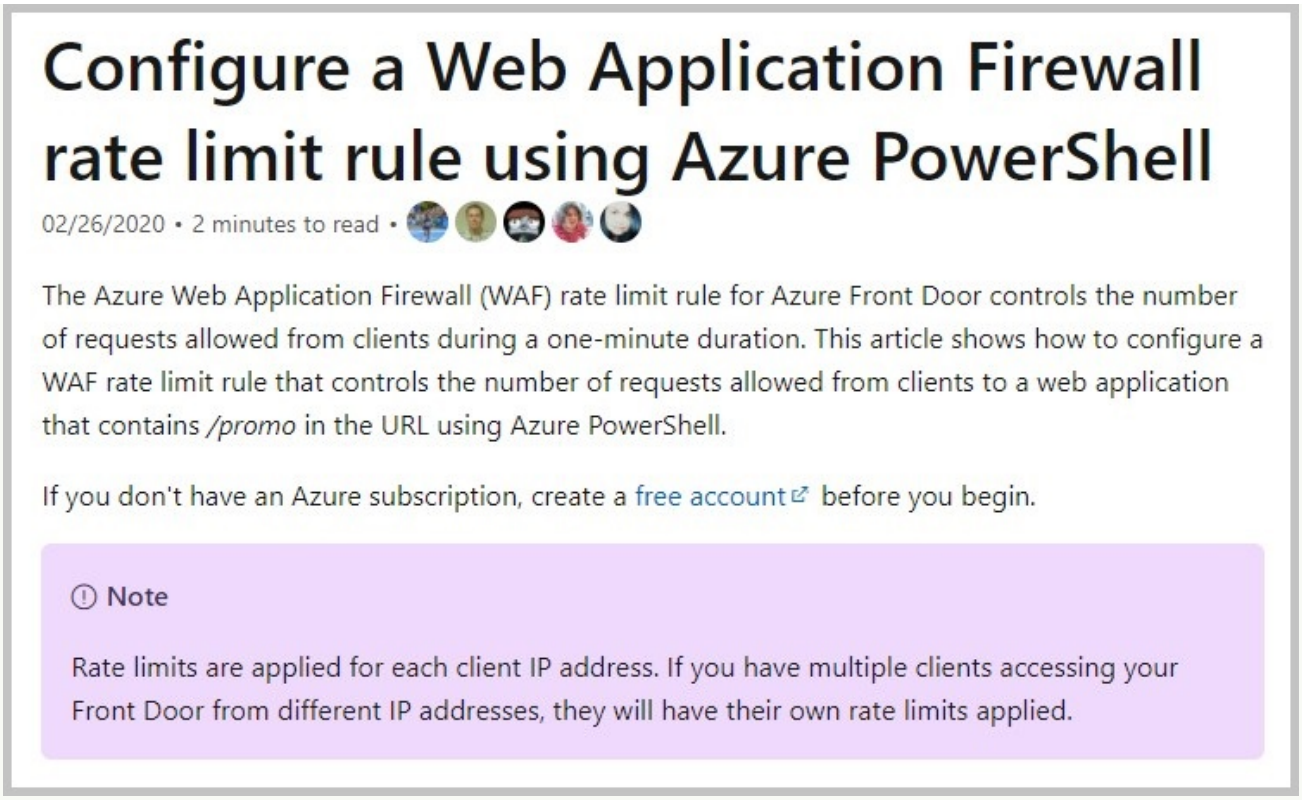
03/09/2021 • 2 minutes to read • +6

Important

This documentation is for Azure Front Door. Looking for information on Azure Front Door Standard/Premium (Preview)? View here.

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.





Configure a Web Application Firewall rate limit rule using Azure PowerShell

02/26/2020 • 2 minutes to read •

The Azure Web Application Firewall (WAF) rate limit rule for Azure Front Door controls the number of requests allowed from clients during a one-minute duration. This article shows how to configure a WAF rate limit rule that controls the number of requests allowed from clients to a web application that contains */promo* in the URL using Azure PowerShell.

If you don't have an Azure subscription, create a free account before you begin.

Note

Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied.

45. Question

You plan to deploy an application that will run in a Linux-based Docker container.

You need to recommend a solution to host the application in Azure. The solution must meet the following requirements:

? Support a custom domain name and an associated SSL certificate.

? Scale-out automatically based on demand.

? Minimize administrative effort and costs.

What should you include in the recommendation?

- A. Azure App Service
- B. Azure Container Instances
- C. an Azure virtual machine
- D. Azure Kubernetes Service (AKS)

Incorrect

App Service not only adds the power of Microsoft Azure to your application, such as security, load balancing, autoscaling, and automated management. You can also take advantage of its DevOps capabilities, such as continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domain, and TLS/SSL certificates.

Key features of App Service include:

? Containerization and Docker – Dockerize your app and host a custom Windows or Linux container in App Service.

? Global scale with high availability – Scale up or out manually or automatically. Host your apps anywhere in Microsoft's global datacenter infrastructure, and the App Service SLA promises high availability.

App Service can also host web apps natively on Linux for supported application stacks. It can also run custom Linux containers (also known as Web App for Containers).

Incorrect Answers:

B. Azure Container Instances

Does not provide auto scaling.

C. an Azure virtual machine

This is not an option to deploy containers with minimal effort and cost.

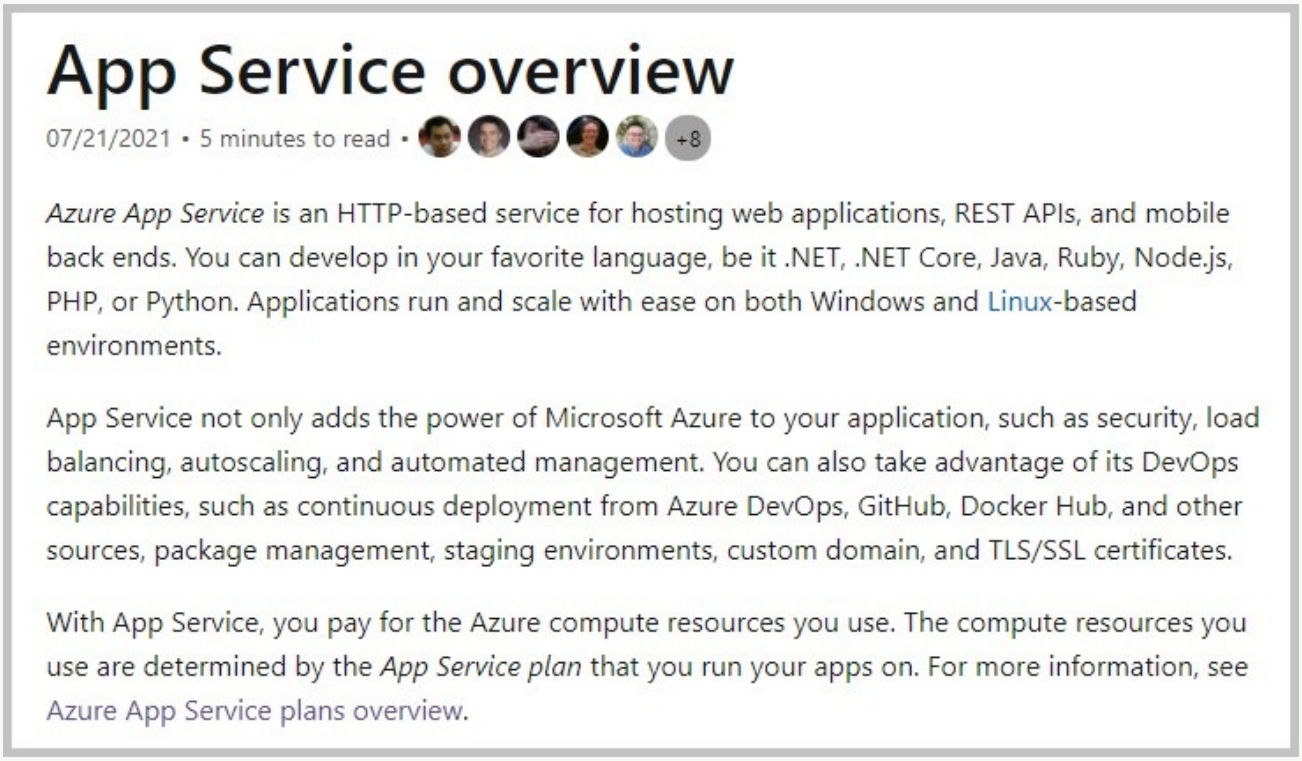
D. Azure Kubernetes Service (AKS)

It requires more administrative effort as compared with App Service for containers.

Reference:

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

https://docs.microsoft.com/en-us/learn/modules/deploy-run-container-app-service/



App Service overview

07/21/2021 • 5 minutes to read • +8

Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. You can develop in your favorite language, be it .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. Applications run and scale with ease on both Windows and Linux-based environments.

App Service not only adds the power of Microsoft Azure to your application, such as security, load balancing, autoscaling, and automated management. You can also take advantage of its DevOps capabilities, such as continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domain, and TLS/SSL certificates.

With App Service, you pay for the Azure compute resources you use. The compute resources you use are determined by the *App Service plan* that you run your apps on. For more information, see Azure App Service plans overview.

46. Question

You are designing an Azure web app.

You plan to deploy the web app to the North Europe Azure region and the West Europe Azure region.

You need to recommend a solution for the web app. The solution must meet the following requirements:

? Users must always access the web app from the North Europe region, unless the region fails.

? The web app must be available to users if an Azure region is unavailable.

? Deployment costs must be minimized.

Which of the following would go into Slot1?

- A. A Traffic Manager profile
- B. Azure Application Gateway
- C. Azure Load Balancer

Correct

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.

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.

Incorrect Answers:

B. Azure Application Gateway

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

C. Azure Load Balancer

Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load-balancing rules and health probes.

Reference:

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

https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

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.

47. Question

You are designing an Azure web app.

You plan to deploy the web app to the North Europe Azure region and the West Europe Azure region.

You need to recommend a solution for the web app. The solution must meet the following requirements:

? Users must always access the web app from the North Europe region, unless the region fails.

? The web app must be available to users if an Azure region is unavailable.

? Deployment costs must be minimized.

Which of the following would go into Slot2?

- A. Cookie-based session affinity
- B. Performance traffic routing
- C. Priority traffic routing
- D. Weighted traffic routing

Correct

Priority routing is used 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.

Incorrect Answers:

A. Cookie-based session affinity

The cookie-based session affinity feature is useful when you want to keep a user session on the same server. By using gateway-managed cookies, the Application Gateway can direct subsequent traffic from a user session to the same server for processing.

B. Performance traffic routing

Performance routing is used when you have endpoints in different geographic locations and you want end users to use the “closest“ endpoint for the lowest network latency.

D. Weighted traffic routing

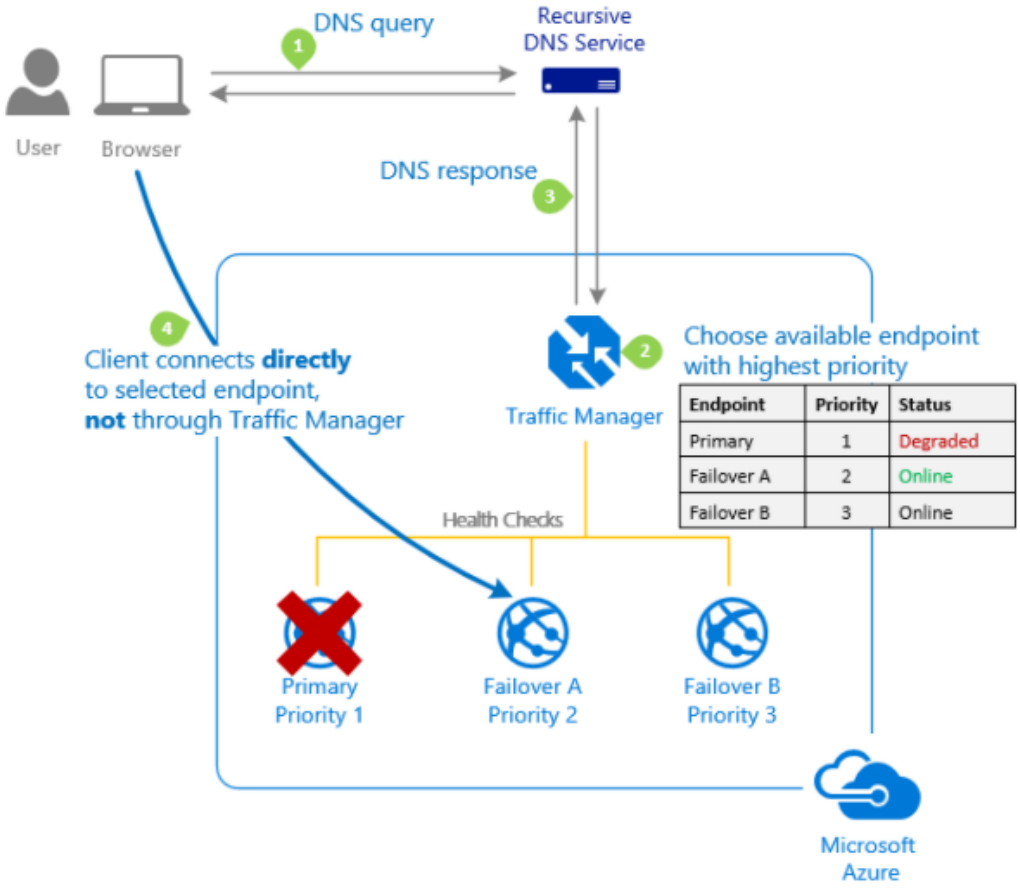
Weighted routing is used when you want to distribute traffic across a set of endpoints based on their weight. Set the weight the same to distribute evenly across all endpoints.

Reference:

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

Priority traffic-routing method

Often an organization wants to provide reliability for their services. To do so, they deploy one or more backup services in case their primary goes down. The 'Priority' traffic-routing method allows Azure customers to easily implement this failover pattern.



The Traffic Manager profile contains a prioritized list of service endpoints. By default, Traffic Manager sends all traffic to the primary (highest-priority) endpoint. If the primary endpoint isn't available, Traffic Manager routes the traffic to the second endpoint. In a situation where the primary and secondary endpoints aren't available, the traffic goes to the third, and so on. Availability of the endpoint is based on the configured status (enabled or disabled) and the ongoing endpoint monitoring.

48. Question

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

You plan to provide users with access to shared files by using Azure Storage. The users will be provided with different levels of access to various Azure file shares based on their user account or their group membership.

You need to recommend which additional Azure services must be used to support the planned deployment.

What should you include in the recommendation?

A. an Azure AD enterprise application

B. Azure Information Protection

C. an Azure AD Domain Services (Azure AD DS) instance

D. an Azure Front Door instance

Correct

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Incorrect Answers:

A. an Azure AD enterprise application

It is used to register an application with Azure AD tenant.

B. Azure Information Protection

Azure Information Protection (AIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content.

D. an Azure Front Door instance

Azure Front Door is a fast, reliable, and secure modern cloud CDN with intelligent threat protection. It provides static and dynamic content acceleration, global load balancing, and enhanced security for your global hyper-scale applications, APIs, websites, and cloud services with intelligent threat protection.

Reference:

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable

Enable Azure Active Directory Domain Services authentication on Azure Files

07/22/2021 • 13 minutes to read • +6

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).We strongly recommend you to review the How it works section to select the right domain service for authentication. The setup is different depending on the domain service you choose. This article focuses on enabling and configuring Azure AD DS for authentication with Azure file shares.

If you are new to Azure file shares, we recommend reading our planning guide before reading the following series of articles.

Note

Azure Files supports Kerberos authentication with Azure AD DS with RC4-HMAC and AES-256 encryption.

Azure Files supports authentication for Azure AD DS with full synchronization with Azure AD. If you have enabled scoped synchronization in Azure AD DS which only sync a limited set of identities from Azure AD, authentication and authorization is not supported.

49. 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 notification solution for the IT Support distribution group.

What should you include in the recommendation?

- A. a SendGrid account with advanced reporting
- B. Azure AD Connect Health
- C. Azure Network Watcher
- D. an action group

Incorrect

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

Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Incorrect Answers:

A. a SendGrid account with advanced reporting

SendGrid is used to send email. You need Azure AD Connect Health to find and alert sync issues.

C. Azure Network Watcher

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.

D. an action group

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.

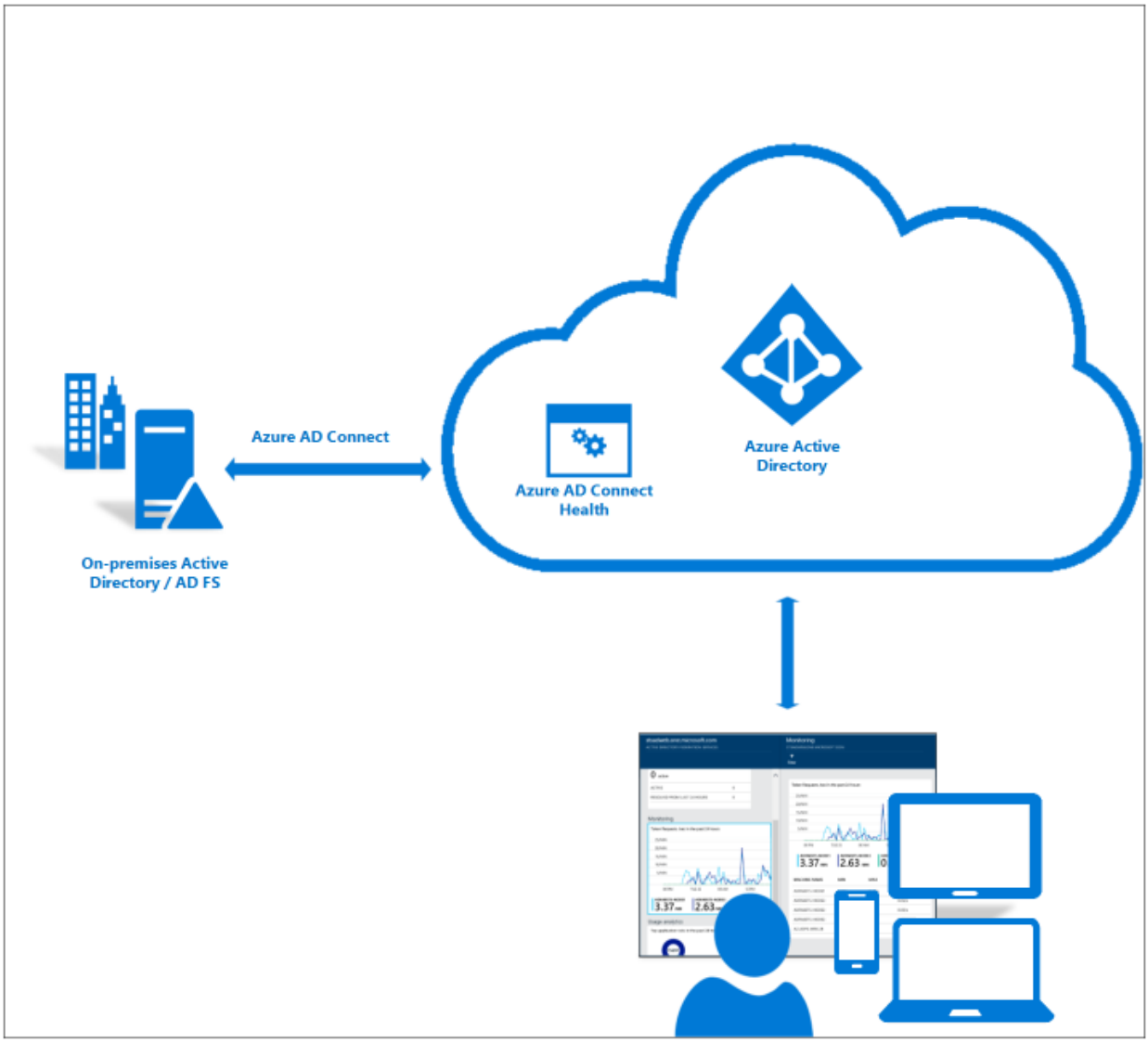
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect#what-is-azure-ad-connect-health

What is 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. This reliability is achieved by providing monitoring capabilities for your key identity components. Also, it makes the key data points about these components easily accessible.

The information is presented in the Azure AD Connect Health portal. Use the Azure AD Connect Health portal to view alerts, performance monitoring, usage analytics, and other information. Azure AD Connect Health enables the single lens of health for your key identity components in one place.



50. 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 strategy for migrating the database content of WebApp1 to Azure.

What should you include in the recommendation?

- A. Use Azure Site Recovery to replicate the SQL servers to Azure
- B. Copy the BACPAC file that contains the Azure SQL database files to Azure Blob storage
- C. Use SQL Server transactional replication
- D. Copy the VHD that contains the Azure SQL database files to Azure Blob storage

Incorrect

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

When you can‘t afford to remove your SQL Server database from production while the migration is

occurring, you can use SQL Server transactional replication as your migration solution. To use this method, the source database must meet the requirements for transactional replication and be compatible for Azure SQL Database.

Incorrect Answers:

A. Use Azure Site Recovery to replicate the SQL servers to Azure

It does not cover the “Any new deployments to Azure must be redundant in case an Azure region fails“ technical requirement.

B. Copy the BACPAC file that contains the Azure SQL database files to Azure Blob storage

This solution required to stop current Database, copy the information and setup the VM, so we are not minimizing downtime with this solution.

D. Copy the VHD that contains the Azure SQL database files to Azure Blob storage

This solution required to stop current Database, copy the information and setup the VM, so we are not minimizing downtime with this solution.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/migrate-to-database-from-sql-server#method-2-use-transactional-replication

https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview

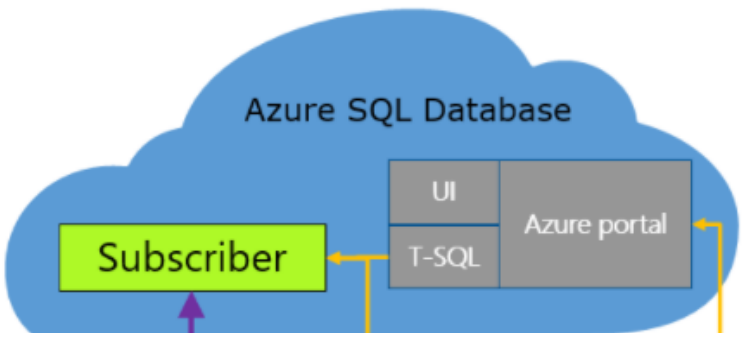
https://docs.microsoft.com/en-us/azure/azure-sql/database/long-term-backup-retention-configure

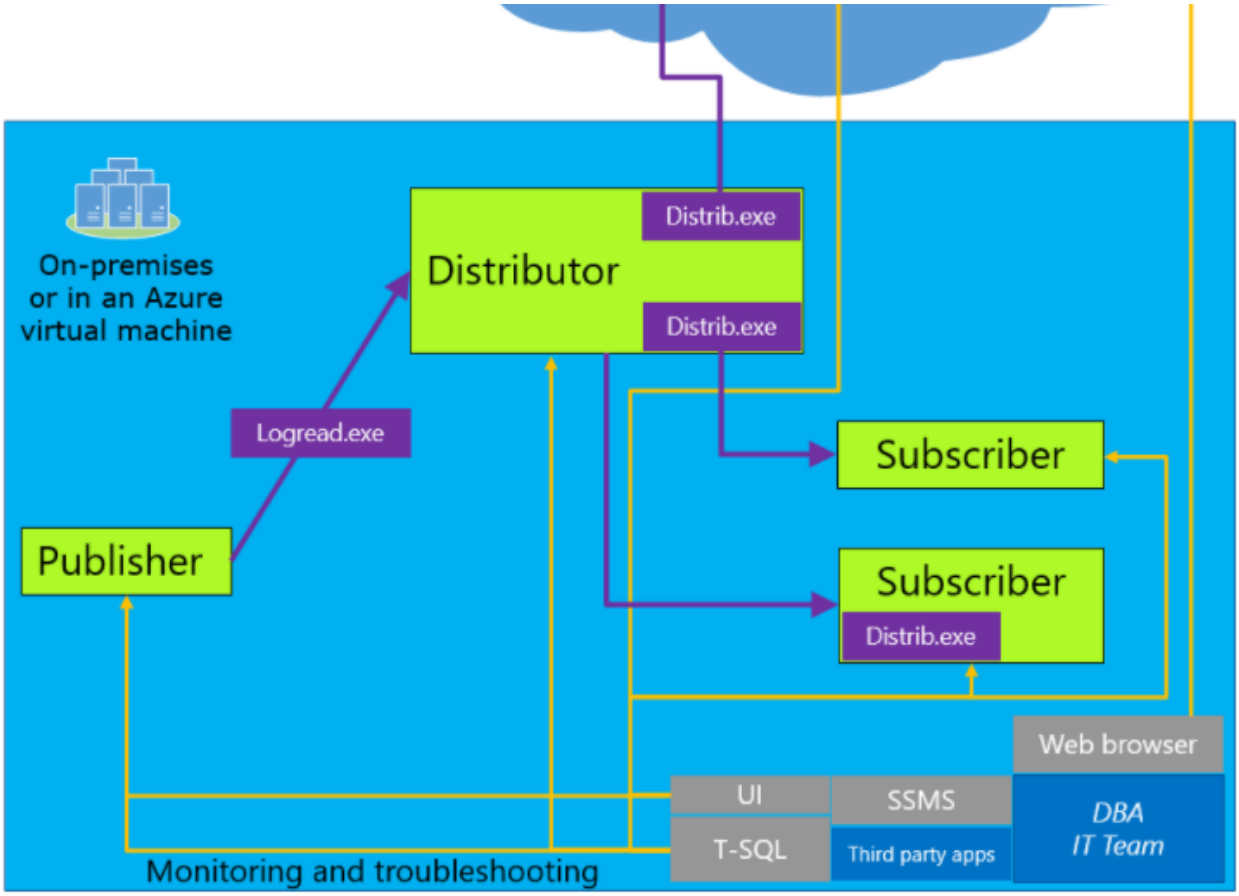
Method 2: Use Transactional Replication

When you can't afford to remove your SQL Server database from production while the migration is occurring, you can use SQL Server transactional replication as your migration solution. To use this method, the source database must meet the requirements for transactional replication and be compatible for Azure SQL Database. For information about SQL replication with Always On, see Configure Replication for Always On Availability Groups (SQL Server).

To use this solution, you configure your database in Azure SQL Database as a subscriber to the SQL Server instance that you wish to migrate. The transactional replication distributor synchronizes data from the database to be synchronized (the publisher) while new transactions continue occur.

With transactional replication, all changes to your data or schema show up in your database in Azure SQL Database. Once the synchronization is complete and you're ready to migrate, change the connection string of your applications to point them to your database. Once transactional replication drains any changes left on your source database and all your applications point to Azure DB, you can uninstall transactional replication. Your database in Azure SQL Database is now your production system.





Tip

You can also use transactional replication to migrate a subset of your source database. The publication that you replicate to Azure SQL Database can be limited to a subset of the tables in the database being replicated. For each table being replicated, you can limit the data to a subset of the rows and/or a subset of the columns.

51. 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

What should you include in the identity management strategy to support the planned changes?

- A. Move all the domain controllers from corp.fabrikam.com to virtual networks in Azure
- B. Deploy domain controllers for the rd.fabrikam.com forest to virtual networks in Azure
- **C. Deploy domain controllers for corp.fabrikam.com to virtual networks in Azure**
- D. Deploy a new Azure AD tenant for the authentication of new R&D projects

Correct

You can create additional domain controllers to a virtual network in Azure. Azure AD can then sync from these domain controllers. We don t need an Azure setup for test.cloudportalhub.com.

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. (This requires domain controllers in Azure)

Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails. (This requires domain controllers on-premises)

Reference:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/virtualized-domain-controller-architecture

Virtualized domain controller cloning architecture

Overview

Virtualized domain controller cloning relies on the hypervisor platform to expose an identifier called **VM-Generation ID** to detect creation of a virtual machine. AD DS initially stores the value of this identifier in its database (NTDS.DIT) during domain controller promotion. When the virtual machine boots up, the current value of the VM-Generation ID from the virtual machine is compared against the value in the database. If the two values are different, the domain controller resets the Invocation ID and discards the RID pool, thereby preventing USN re-use or the potential creation of duplicate security-principals. The domain controller then looks for a DCCloneConfig.xml file in the locations called out in Step 3 in Cloning Detailed Processing. If it finds a DCCloneConfig.xml file, it concludes that it is being deployed as a clone, so it initiates cloning to provision itself as an additional domain controller by re-promoting using the existing NTDS.DIT and SYSVOL contents copied from source media.

In a mixed environment where some hypervisors support VM-GenerationID and others do not, it is possible for a clone media to be accidentally deployed on a hypervisor that does not support VM-GenerationID. The presence of DCCloneConfig.xml file indicates administrative intent to clone a DC. Therefore, if a DCCloneConfig.xml file is found during boot but a VM-GenerationID is not provided from the host, the clone DC is booted into Directory Services Restore Mode (DSRM) to prevent any impact to the rest of the environment. The clone media can be subsequently moved to a hypervisor that supports VM-GenerationID and then cloning can be retried.

If the clone media is deployed on a hypervisor that supports VM-GenerationID but a DCCloneConfig.xml file is not provided, as the DC detects a VM-GenerationID change between its DIT and the one from the new VM, it will trigger safeguards to prevent USN re-use and avoid duplicate SIDs. However, cloning will not be initiated, so the secondary DC will continue to run under the same identity as the source DC. This secondary DC should be removed from the network at the earliest possible time to avoid any inconsistencies in the environment.

52. 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 solution to meet the database retention requirement.

What should you recommend?

- A. Configure geo-replication of the database
- **B. Configure a long-term retention policy for the database**
- C. Configure Azure Site Recovery
- D. Use automatic Azure SQL Database backups

Correct

Scenario:

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

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

Many applications have regulatory, compliance, or other business purposes that require you to retain database backups beyond the 7-35 days provided by Azure SQL Database and Azure SQL Managed Instance automatic backups. By using the long-term retention (LTR) feature, you can store specified SQL Database and SQL Managed Instance full backups in Azure Blob storage with read-access geo-redundant storage for up to 10 years. You can then restore any backup as a new database.

Incorrect Answers:

A. Configure geo-replication of the database

Active geo-replication is an Azure SQL Database feature that allows you to create readable secondary databases of individual databases on a server in the same or different data center (region).

C. Configure Azure Site Recovery

It is not required for Azure SQL database.

D. Use automatic Azure SQL Database backups

Database backups are an essential part of any business continuity and disaster recovery strategy, because they protect your data from corruption or deletion. These backups enable database restore to a point in time within the configured retention period. If your data protection rules require that your backups are available for an extended time (up to 10 years), you can configure long-term retention for both single and pooled databases.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/long-term-retention-overview

https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview#backup-storage-redundancy

Long-term retention - Azure SQL Database and Azure SQL Managed Instance

07/13/2021 • 4 minutes to read •

Many applications have regulatory, compliance, or other business purposes that require you to retain database backups beyond the 7-35 days provided by Azure SQL Database and Azure SQL Managed Instance automatic backups. By using the long-term retention (LTR) feature, you can store specified SQL Database and SQL Managed Instance full backups in Azure Blob storage with configured redundancy for up to 10 years. LTR backups can then be restored as a new database.

Long-term retention can be enabled for Azure SQL Database, and is available in public preview for Azure SQL Managed Instance. This article provides a conceptual overview of long-term retention. To configure long-term retention, see Configure Azure SQL Database LTR and Configure Azure SQL Managed Instance LTR.

Note

You can use SQL Agent jobs to schedule **copy-only database backups** as an alternative to LTR beyond 35 days.

Important

Long-term retention on Managed Instance is currently available in public preview in Azure Public regions only.

53. Question

You have an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain.

You have an internal web app named WebApp1 that is hosted on-premises. WebApp1 uses Integrated Windows authentication.

Some users work remotely and do NOT have VPN access to the on-premises network.

You need to provide the remote users with single sign-on (SSO) access to WebApp1.

Which two features should you include in the solution?

- [x] A. Azure AD Application Proxy
- [ ] B. Azure AD Privileged Identity Management (PIM)
- [ ] C. Conditional Access policies

D. Azure Arc

E. Azure AD enterprise applications

F. Azure Application Gateway

Correct

It's required to download connector under Application Proxy and create a new application under Enterprise Application, however for Pre Authentication option, you can choose "Passthrough" or "Azure Active Directory", and both will work, but it's recommended to use "Azure Active Directory" so you can take advantage of using conditional access and MFA.

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. You can configure single sign-on to an Application Proxy application.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-config-sso-how-to

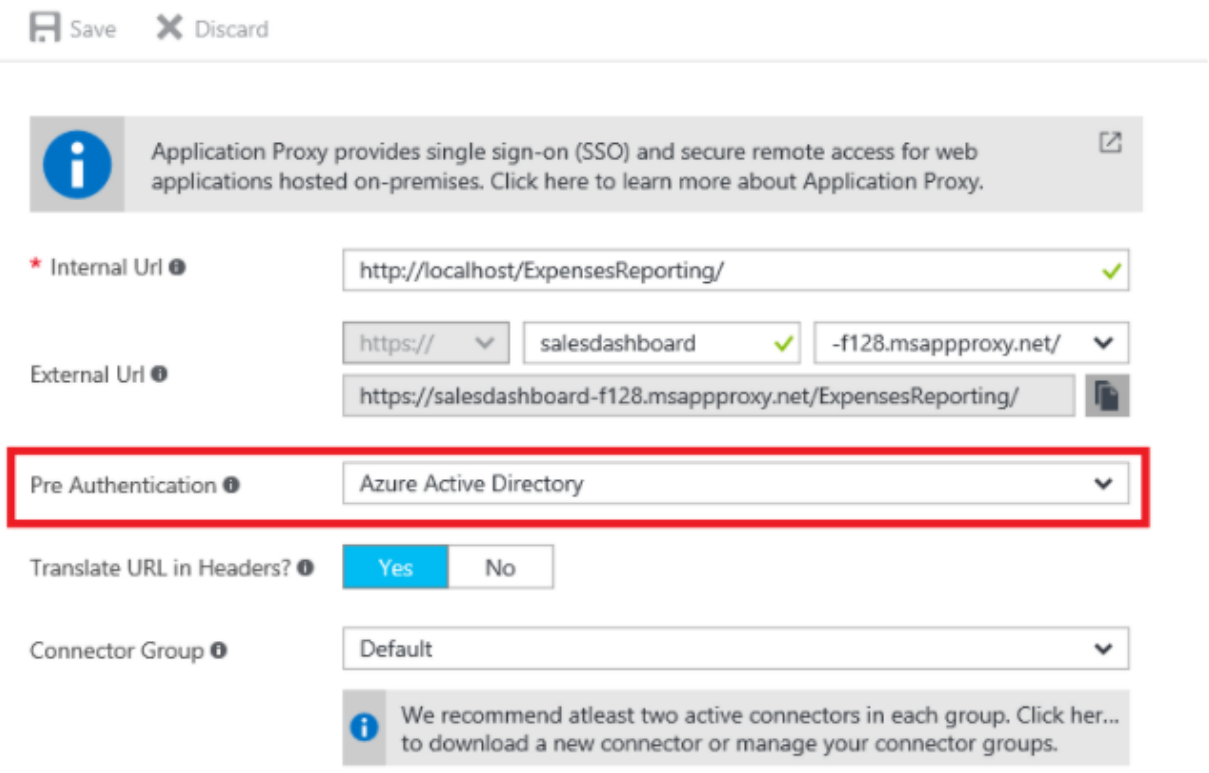
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd

How to configure single-sign on

To configure SSO, first make sure that your application is configured for Pre-Authentication through Azure Active Directory. To do this configuration, go to **Azure Active Directory** -> **Enterprise Applications** -> **All Applications** -> Your application -> **Application Proxy**. On this page, you see the "Pre Authentication" field, and make sure that is set to "Azure Active Directory.

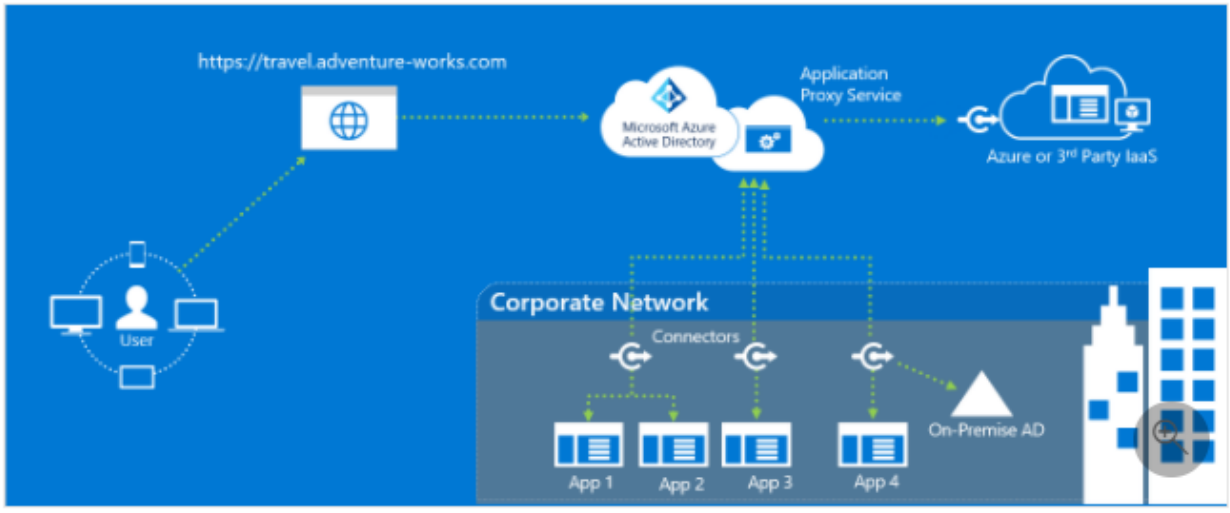
For more information on the Pre-Authentication methods, see step 4 of the app publishing document.



Tutorial: Add an on-premises application for remote access through Application Proxy in Azure Active Directory

Article • 12/30/2021 • 14 minutes to read • 6 contributors

Azure Active Directory (Azure AD) has an Application Proxy service that enables users to access on-premises applications by signing in with their Azure AD account. To learn more about Application Proxy, see What is App Proxy?. This tutorial prepares your environment for use with Application Proxy. Once your environment is ready, you'll use the Azure portal to add an on-premises application to your Azure AD tenant.



54. Question

You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system. Permissions to folders are granted directly to the data engineers.

You need to recommend a design for the planned Databrick deployment. The solution must meet the following requirements:

? Ensure that the data engineers can only access folders to which they have permissions.

? Minimize development effort.

? Minimize costs.

What should you include in the recommendation for Databricks SKU?

A. Premium

B. Standard

Correct

Databricks SKU should be a Premium plan. As the doc states both cloud storage access and credential passthrough features will need a Premium plan.

? Configure access to cloud storage

Requirements

? Azure Databricks account on the Premium plan

? A Databricks SQL endpoint

? Groups representing users who you will give access to data

? Access Azure Data Lake Storage using Azure Active Directory credential passthrough

Requirements

? Azure Databricks Premium Plan. See Upgrade or Downgrade an Azure Databricks Workspace for details on upgrading a standard plan to a premium plan.

? An Azure Data Lake Storage Gen1 or Gen2 storage account. Azure Data Lake Storage Gen2 storage accounts must use the hierarchical namespace to work with Azure Data Lake Storage credential passthrough. See Create a storage account for instructions on creating a new ADLS Gen2 account, including how to enable the hierarchical namespace.

? Properly configured user permissions to Azure Data Lake Storage. An Azure Databricks administrator needs to ensure that users have the correct roles, for example, Storage Blob Data Contributor, to read and write data stored in Azure Data Lake Storage. See Use the Azure portal to assign an Azure role for access to blob and queue data.

? You cannot use a cluster configured with ADLS credentials, for example, service principal credentials, with credential passthrough.

Reference:

https://docs.microsoft.com/en-us/azure/databricks/sql/user/security/cloud-storage-access

https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adls-passthrough#adls-aad-credentials

Configure access to cloud storage

Article • 01/26/2022 • 3 minutes to read • 3 contributors

This article describes how Databricks SQL administrators configure a new workspace for access to data objects.

> ⓘ Note
>
> - If you are using Azure Databricks **managed tables** you do not need to configure access to cloud storage.
> - Databricks SQL endpoints all share the same cloud storage access credentials.

To configure data access for Databricks SQL, follow the steps in this section:

- Requirements
- Step 1: (Optional) Create a service principal for each Azure Data Lake Storage Gen2 storage account
- Step 2: Grant service principals access to the Azure Data Lake Storage Gen2 accounts
- Step 3: Configure Databricks SQL to use service principals for data access
- Step 4: Define data access privileges using table access control
- Step 5: (Optional) Set owner

Requirements

- Azure Databricks account on the Premium plan
- A Databricks SQL endpoint
- Groups representing users who you will give access to data

Access Azure Data Lake Storage using Azure Active Directory credential passthrough

Article • 01/26/2022 • 11 minutes to read • 6 contributors

> **Note**
>
> This article contains references to the term *whitelisted*, a term that Azure Databricks no longer uses. When the term is removed from the software, we'll remove it from this article.

You can authenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.

Azure Data Lake Storage credential passthrough is supported with Azure Data Lake Storage Gen1 and Gen2 only. Azure Blob storage does not support credential passthrough.

Notebooks are included to provide examples of using credential passthrough with ADLS Gen1 and ADLS Gen2 storage accounts.

Requirements

- Azure Databricks Premium Plan. See Upgrade or Downgrade an Azure Databricks Workspace for details on upgrading a standard plan to a premium plan.
- An Azure Data Lake Storage Gen1 or Gen2 storage account. Azure Data Lake Storage Gen2 storage accounts must use the hierarchical namespace to work with Azure Data Lake Storage credential passthrough. See Create a storage account for instructions on creating a new ADLS Gen2 account, including how to enable the hierarchical namespace.
- Properly configured user permissions to Azure Data Lake Storage. An Azure Databricks administrator needs to ensure that users have the correct roles, for example, Storage Blob Data Contributor, to read and write data stored in Azure Data Lake Storage. See Use the Azure portal to assign an Azure role for access to blob and queue data.
- You cannot use a cluster configured with ADLS credentials, for example, service principal credentials, with credential passthrough.

55. Question

You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system. Permissions to folders are granted directly to the data engineers.

You need to recommend a design for the planned Databrick deployment. The solution must meet the following requirements:

? Ensure that the data engineers can only access folders to which they have permissions.

? Minimize development effort.

? Minimize costs.

What should you include in the recommendation for Cluster Configuration?

- A. Credential passthrough
- B. Managed identites
- C. MLflow
- D. A runtime that contains Photon
- E. Secret scope

Correct

Athenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.

Reference:

https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adls-passthrough

Access Azure Data Lake Storage using Azure Active Directory credential passthrough

Article • 01/26/2022 • 11 minutes to read • 6 contributors

Note

This article contains references to the term *whitelisted*, a term that Azure Databricks no longer uses. When the term is removed from the software, we'll remove it from this article.

You can authenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.

Azure Data Lake Storage credential passthrough is supported with Azure Data Lake Storage Gen1 and Gen2 only. Azure Blob storage does not support credential passthrough.

56. Question

You have an Azure subscription that contains an Azure SQL database named DB1.

Several queries that query the data in DB1 take a long time to execute.

You need to recommend a solution to identify the queries that take the longest to execute.

What should you include in the recommendation?

- A. SQL Database Advisor
- B. Azure Monitor
- C. Performance Recommendations
- D. Query Performance Insight

Correct

Query Performance Insight provides intelligent query analysis for single and pooled databases. It helps identify the top resource consuming and long-running queries in your workload. This helps you find the queries to optimize to improve overall workload performance and efficiently use the resource that you are paying for.

Incorrect Answers:

A. SQL Database Advisor

Azure SQL Database has a number of database advisors that provide customized recommendations that enable you to maximize performance. These database advisors continuously assess and analyze the usage history and provide recommendations based on workload patterns that help improve performance.

B. Azure Monitor

Azure Monitor helps you maximize the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.

C. Performance Recommendations

You can use the Azure portal to find performance recommendations that can optimize performance of your database in Azure SQL Database or to correct some issue identified in your workload.

The Performance recommendation page in the Azure portal enables you to find the top recommendations based on their potential impact.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/query-performance-insight-use

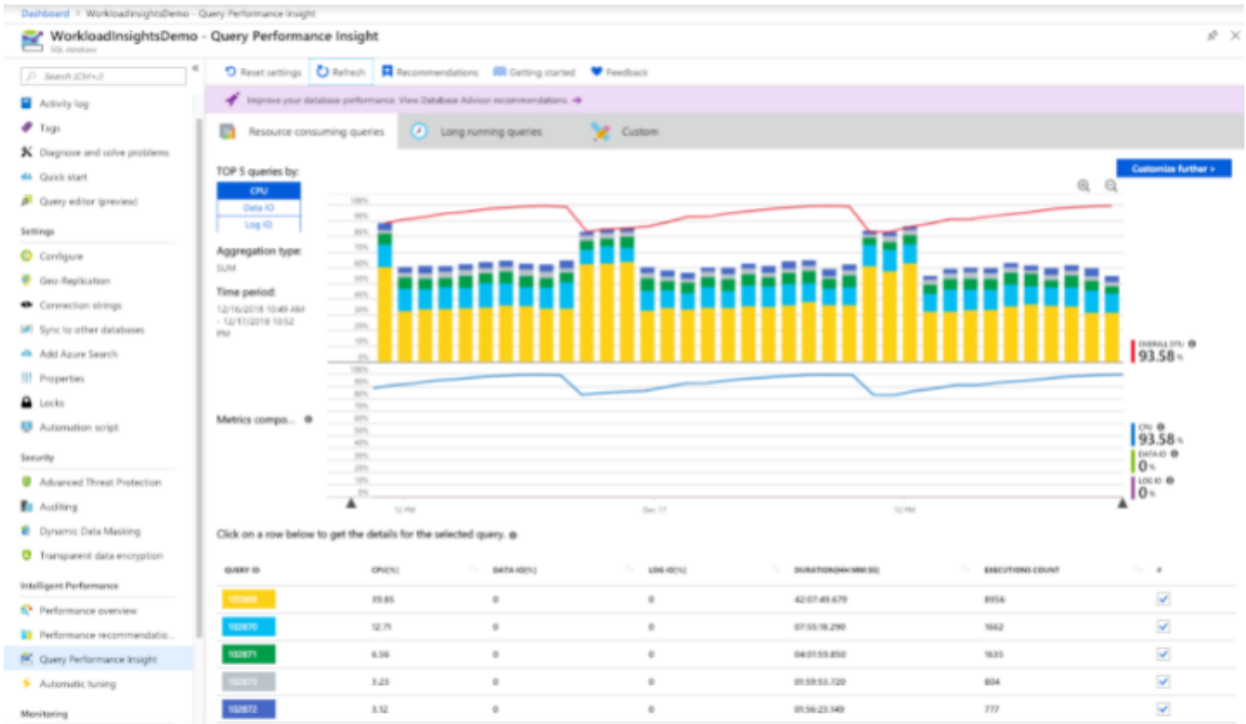
Query Performance Insight for Azure SQL Database

01/14/2021 • 10 minutes to read • +1

APPLIES TO: Azure SQL Database

Query Performance Insight provides intelligent query analysis for single and pooled databases. It helps identify the top resource consuming and long-running queries in your workload. This helps you find the queries to optimize to improve overall workload performance and efficiently use the resource that you are paying for. Query Performance Insight helps you spend less time troubleshooting database performance by providing:

- Deeper insight into your databases resource (DTU) consumption
- Details on top database queries by CPU, duration, and execution count (potential tuning candidates for performance improvements)
- The ability to drill down into details of a query, to view the query text and history of resource utilization
- Annotations that show performance recommendations from database advisors



57. Question

You have an on-premises Hyper-V cluster. The cluster contains Hyper-V hosts that run Windows Server 2016 Datacenter. The hosts are licensed under a Microsoft Enterprise Agreement that has Software Assurance.

The Hyper-V cluster contains 30 virtual machines that run Windows Server 2012 R2. Each virtual machine runs a different workload. The workloads have predictable consumption patterns.

You plan to replace the virtual machines with Azure virtual machines that run Windows Server 2016. The

virtual machines will be sized according to the consumption pattern of each workload.

You need to recommend a solution to minimize the compute costs of the Azure virtual machines.

Which two recommendations should you include in the solution?

- [ ] A. Configure a spending limit in the Azure account center
- [ ] B. Create a virtual machine scale set that uses autoscaling
- [x] C. Activate Azure Hybrid Benefit for the Azure virtual machines
- [x] D. Purchase Azure Reserved Virtual Machine Instances for the Azure virtual machines
- [ ] E. Create a lab in Azure DevTest Labs and place the Azure virtual machines in the lab

Correct

C: For customers with Software Assurance, Azure Hybrid Benefit for Windows Server allows you to use your on-premises Windows Server licenses and run Windows virtual machines on Azure at a reduced cost. You can use Azure Hybrid Benefit for Windows Server to deploy new virtual machines with Windows OS.

D: With Azure Reserved VM Instances (RIs) you reserve virtual machines in advance and save up to 80 percent.

Incorrect Answers:

A. Configure a spending limit in the Azure account center

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. It will not provide discount or reduce the costs.

B. Create a virtual machine scale set that uses autoscaling

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.

E. Create a lab in Azure DevTest Labs and place the Azure virtual machines in the lab

Azure DevTest Labs enables developers on teams to efficiently self-manage virtual machines (VMs) and PaaS resources without waiting for approvals.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing

https://docs.microsoft.com/en-us/azure/cost-management-billing/reservations/save-compute-costs-reservations

Azure Hybrid Benefit for Windows Server

04/22/2018 • 5 minutes to read • +9

Applies to: ✔ Windows VMs ✔ Flexible scale sets

For customers with Software Assurance, Azure Hybrid Benefit for Windows Server allows you to use your on-premises Windows Server licenses and run Windows virtual machines on Azure at a reduced cost. You can use Azure Hybrid Benefit for Windows Server to deploy new virtual machines with Windows OS. This article goes over the steps on how to deploy new VMs with Azure Hybrid Benefit for Windows Server and how you can update existing running VMs. For more information about Azure Hybrid Benefit for Windows Server licensing and cost savings, see the Azure Hybrid Benefit for Windows Server licensing page.

Each 2-processor license or each set of 16-core licenses are entitled to two instances of up to 8 cores, or one instance of up to 16 cores. The Azure Hybrid Benefit for Standard Edition licenses can only be used once either on-premises or in Azure. Datacenter Edition benefits allow for simultaneous usage both on-premises and in Azure.

Using Azure Hybrid Benefit for Windows Server with any VMs running Windows Server OS are now supported in all regions, including VMs with additional software such as SQL Server or third-party marketplace software.

What are Azure Reservations?

02/24/2021 • 6 minutes to read • +3

Azure Reservations help you save money by committing to one-year or three-year plans for multiple products. Committing allows you to get a discount on the resources you use. Reservations can significantly reduce your resource costs by up to 72% from pay-as-you-go prices. Reservations provide a billing discount and don't affect the runtime state of your resources. After you purchase a reservation, the discount automatically applies to matching resources.

You can pay for a reservation up front or monthly. The total cost of up-front and monthly reservations is the same and you don't pay any extra fees when you choose to pay monthly. Monthly payment is available for Azure reservations, not third-party products.

58. Question

You have an Azure subscription that contains the SQL servers on Azure shown in the following table

Name	Resource Group	Location
SQLsvr1	RG1	East US
SQLsvr2	RG2	West US

The subscription contains the storage accounts shown in the following table.

Name	Resource Group	Location	Account Kind
storage1	RG1	East US	StorageV2 (General Purpose v2)
storage2	RG2	West US	BlobStorage

You create the Azure SQL databases shown in the following table.

Name	Resource Group	Server	Pricing Tier
SQLdb1	RG1	SQLsvr1	Standard
SQLdb2	RG1	SQLsvr1	Standard
SQLdb3	RG2	SQLsvr2	Premium

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

When you enable auditing for SQLdb1, you can store the audit information on storage1

- A. Yes
- B. No

Correct

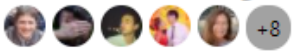
Both SQLsvr1 and Storage1 are in same location East US

Note: Be sure that the destination is in the same region as your database and server.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

Auditing for Azure SQL Database and Azure Synapse Analytics

08/25/2021 • 14 minutes to read • 

APPLIES TO: Azure SQL Database Azure Synapse Analytics

Auditing for Azure SQL Database and Azure Synapse Analytics tracks database events and writes them to an audit log in your Azure storage account, Log Analytics workspace, or Event Hubs.

Auditing also:

- Helps you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
- Enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance. For more information about Azure programs that support standards compliance, see the Azure Trust Center where you can find the most current list of Azure SQL compliance certifications.

> **Note**
>
> For information on Azure SQL Managed Instance auditing, see the following article, **Get started with SQL Managed Instance auditing.**

Overview

You can use SQL Database auditing to:

- **Retain** an audit trail of selected events. You can define categories of database actions to be audited.
- **Report** on database activity. You can use pre-configured reports and a dashboard to get started quickly with activity and event reporting.
- **Analyze** reports. You can find suspicious events, unusual activity, and trends.

> **Important**
>
> Auditing for Azure SQL Database, Azure Synapse and Azure SQL Managed Instance is optimized for availability and performance. During very high activity, or high network load, Azure SQL Database, Azure Synapse and Azure SQL Managed Instance allow operations to proceed and may not record some audited events.

59. Question

You have an Azure subscription that contains the SQL servers on Azure shown in the following table

Name	Resource Group	Location
SQLsvr1	RG1	East US
SQLsvr2	RG2	West US

The subscription contains the storage accounts shown in the following table.

Name	Resource Group	Location	Account Kind
storage1	RG1	East US	StorageV2 (General Purpose v2)
storage2	RG2	West US	BlobStorage

You create the Azure SQL databases shown in the following table.

Name	Resource Group	Server	Pricing Tier
SQLdb1	RG1	SQLsvr1	Standard
SQLdb2	RG1	SQLsvr1	Standard
SQLdb3	RG2	SQLsvr2	Premium

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

When you enable auditing for SQLdb2, you can store the audit information on storage2

- A. Yes
- B. No

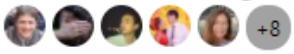
Correct

SQLsvr2 and Storage2 are in different locations

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

Auditing for Azure SQL Database and Azure Synapse Analytics

08/25/2021 • 14 minutes to read • 

APPLIES TO: Azure SQL Database Azure Synapse Analytics

Auditing for Azure SQL Database and Azure Synapse Analytics tracks database events and writes them to an audit log in your Azure storage account, Log Analytics workspace, or Event Hubs.

Auditing also:

- Helps you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
- Enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance. For more information about Azure programs that support standards compliance, see the Azure Trust Center where you can find the most current list of Azure SQL compliance certifications.

> ⓘ Note
>
> For information on Azure SQL Managed Instance auditing, see the following article, **Get started with SQL Managed Instance auditing.**

Overview

You can use SQL Database auditing to:

- **Retain** an audit trail of selected events. You can define categories of database actions to be audited.
- **Report** on database activity. You can use pre-configured reports and a dashboard to get started quickly with activity and event reporting.
- **Analyze** reports. You can find suspicious events, unusual activity, and trends.

> ⓘ Important
>
> Auditing for Azure SQL Database, Azure Synapse and Azure SQL Managed Instance is optimized for availability and performance. During very high activity, or high network load, Azure SQL Database, Azure Synapse and Azure SQL Managed Instance allow operations to proceed and may not record some audited events.

60. Question

You have an Azure subscription that contains the SQL servers on Azure shown in the following table

Name	Resource Group	Location
SQLsvr1	RG1	East US
SQLsvr2	RG2	West US

The subscription contains the storage accounts shown in the following table.

Name	Resource Group	Location	Account Kind
storage1	RG1	East US	StorageV2 (General Purpose v2)
storage2	RG2	West US	BlobStorage

You create the Azure SQL databases shown in the following table.

Name	Resource Group	Server	Pricing Tier
SQLdb1	RG1	SQLsvr1	Standard
SQLdb2	RG1	SQLsvr1	Standard
SQLdb3	RG2	SQLsvr2	Premium

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

When you enable auditing for SQLdb3, you can store the audit information on storage2

- A. Yes
- B. No

Correct

Both SQLsvr2 and Storage2 are in same location West US

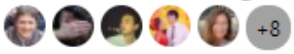
There has been some talk about whether the Premium refers to the storage type, but BlobStorage (specified in the question) can ONLY be Standard, so the mention of Premium must relate to SQL only.

From the link specified in the answer, under “Audit to storage destination“ it states in the Remarks sub-section “Audit logs are written to Append Blobs in an Azure Blob storage on your Azure subscription“. So It must be YES.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

Auditing for Azure SQL Database and Azure Synapse Analytics

08/25/2021 • 14 minutes to read • 

APPLIES TO: Azure SQL Database Azure Synapse Analytics

Auditing for Azure SQL Database and Azure Synapse Analytics tracks database events and writes them to an audit log in your Azure storage account, Log Analytics workspace, or Event Hubs.

Auditing also:

- Helps you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
- Enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance. For more information about Azure programs that support standards compliance, see the Azure Trust Center where you can find the most current list of Azure SQL compliance certifications.

> **Note**
>
> For information on Azure SQL Managed Instance auditing, see the following article, **Get started with SQL Managed Instance auditing.**

Overview

You can use SQL Database auditing to:

- **Retain** an audit trail of selected events. You can define categories of database actions to be audited.
- **Report** on database activity. You can use pre-configured reports and a dashboard to get started quickly with activity and event reporting.
- **Analyze** reports. You can find suspicious events, unusual activity, and trends.

> **Important**
>
> Auditing for Azure SQL Database, Azure Synapse and Azure SQL Managed Instance is optimized for availability and performance. During very high activity, or high network load, Azure SQL Database, Azure Synapse and Azure SQL Managed Instance allow operations to proceed and may not record some audited events.

61. Question

You are building an application that will run in a virtual machine (VM). The application will use Azure Managed Identity.

The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authorization method would go into Slot1?

- A. Hash-based message authentication code (HMAC)
- B. Azure Managed Identity
- C. Role-Based Access Controls (RBAC)
- D. HTTPS encryption

Incorrect

Access to a key vault is controlled through two interfaces: the management plane and the data plane. The management plane is where you manage Key Vault itself. Operations in this plane include creating and deleting key vaults, retrieving Key Vault properties, and updating access policies. The data plane is where you work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.

Both planes use Azure Active Directory (Azure AD) for authentication. For authorization, the management plane uses Azure role-based access control (Azure RBAC) and the data plane uses a Key Vault access policy and Azure RBAC for Key Vault data plane operations.

Note:

Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources.

Incorrect Answers:

A. Hash-based message authentication code (HMAC)

HMAC (Hash-based Message Authentication Code) is a type of a message authentication code (MAC) that is acquired by executing a cryptographic hash function on the data (that is) to be authenticated and a secret shared key.

It's not a valid authentication method for Azure Key Vault.

B. Azure Managed Identity

Managed identities for Azure resources is a feature of Azure Active Directory. Each of the Azure services that support managed identities for Azure resources are subject to their own timeline.

D. HTTPS encryption

It's not an authentication method.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#access-model-overview

62. Question

You are building an application that will run in a virtual machine (VM). The application will use Azure Managed Identity.

The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authorization method would go into Slot2?

- A. Hash-based message authentication code (HMAC)
- B. Azure Managed Identity
- C. Role-Based Access Controls (RBAC)
- D. HTTPS encryption

Incorrect

Authorization refers to controlling access on resources and commands within a database. This is done by assigning permissions to a user within a database in Azure SQL Database or Azure SQL Managed Instance. Permissions are ideally managed by adding user accounts to database roles and assigning database-level permissions to those roles. Alternatively an individual user can also be granted certain object-level permissions.

Note:

Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources.

Incorrect Answers:

A. Hash-based message authentication code (HMAC)

HMAC (Hash-based Message Authentication Code) is a type of a message authentication code (MAC) that is acquired by executing a cryptographic hash function on the data (that is) to be authenticated and a secret shared key.

It's not a valid authentication method for Azure Key Vault.

B. Azure Managed Identity

Managed identities for Azure resources is a feature of Azure Active Directory. Each of the Azure services that support managed identities for Azure resources are subject to their own timeline.

D. HTTPS encryption

It's not an authentication method.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/security-overview#authorization

63. Question

You are building an application that will run in a virtual machine (VM). The application will use Azure Managed Identity.

The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authorization method would go into Slot3?

- A. Hash-based message authentication code (HMAC)
- B. Azure Managed Identity
- C. Role-Based Access Controls (RBAC)
- D. HTTPS encryption

Incorrect

Azure Cosmos DB uses hash-based message authentication code (HMAC) for authorization.
Each request is hashed using the secret account key, and the subsequent base-64 encoded hash is sent with each call to Azure Cosmos DB. To validate the request, the Azure Cosmos DB service uses the correct secret key and properties to generate a hash, then it compares the value with the one in the request. If the two values match, the operation is authorized successfully and the request is processed, otherwise there is an authorization failure and the request is rejected.
Incorrect Answers:
B. Azure Managed Identity
Managed identities for Azure resources is a feature of Azure Active Directory. Each of the Azure services that support managed identities for Azure resources are subject to their own timeline.
C. Role-Based Access Controls (RBAC)
Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.
Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources.
D. HTTPS encryption
It's not an authentication method.
Reference:
https://docs.microsoft.com/en-us/azure/cosmos-db/database-security?tabs=sql-api#how-does-azure-cosmos-db-secure-my-database

64. Question

A company named Techzen, Ltd. has an Azure Active Directory (Azure AD) tenant that uses the Basic license.
You plan to deploy two applications to Azure. The applications have the requirements shown in the following table.

Application Name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authentication
Reporting	Users must authenticate by using either Techzen credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

Which authentication strategy should you recommend for Customer application?

- A. An Azure AD B2C tenant
- B. An Azure AD v1.0 endpoint
- C. An Azure AD V2.0 endpoint

Correct

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure Multi-Factor Authentication so that you can add a second layer of security to sign-up and sign-in experiences in your applications.

Note: Personal accounts are obviously supported, also enable B2C for MFA seems possible, AAD v1 or v2 requires premium P1 license to enable MFA, we have only Basic

Incorrect Answers:

B. An Azure AD v1.0 endpoint

The v1.0 endpoint allows only work and school accounts to sign in to your application (Azure AD)

C. An Azure AD V2.0 endpoint

The Microsoft identity platform endpoint allows work and school accounts from Azure AD and personal Microsoft accounts (MSA), such as hotmail.com, outlook.com, and msn.com, to sign in.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-mfa

https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview

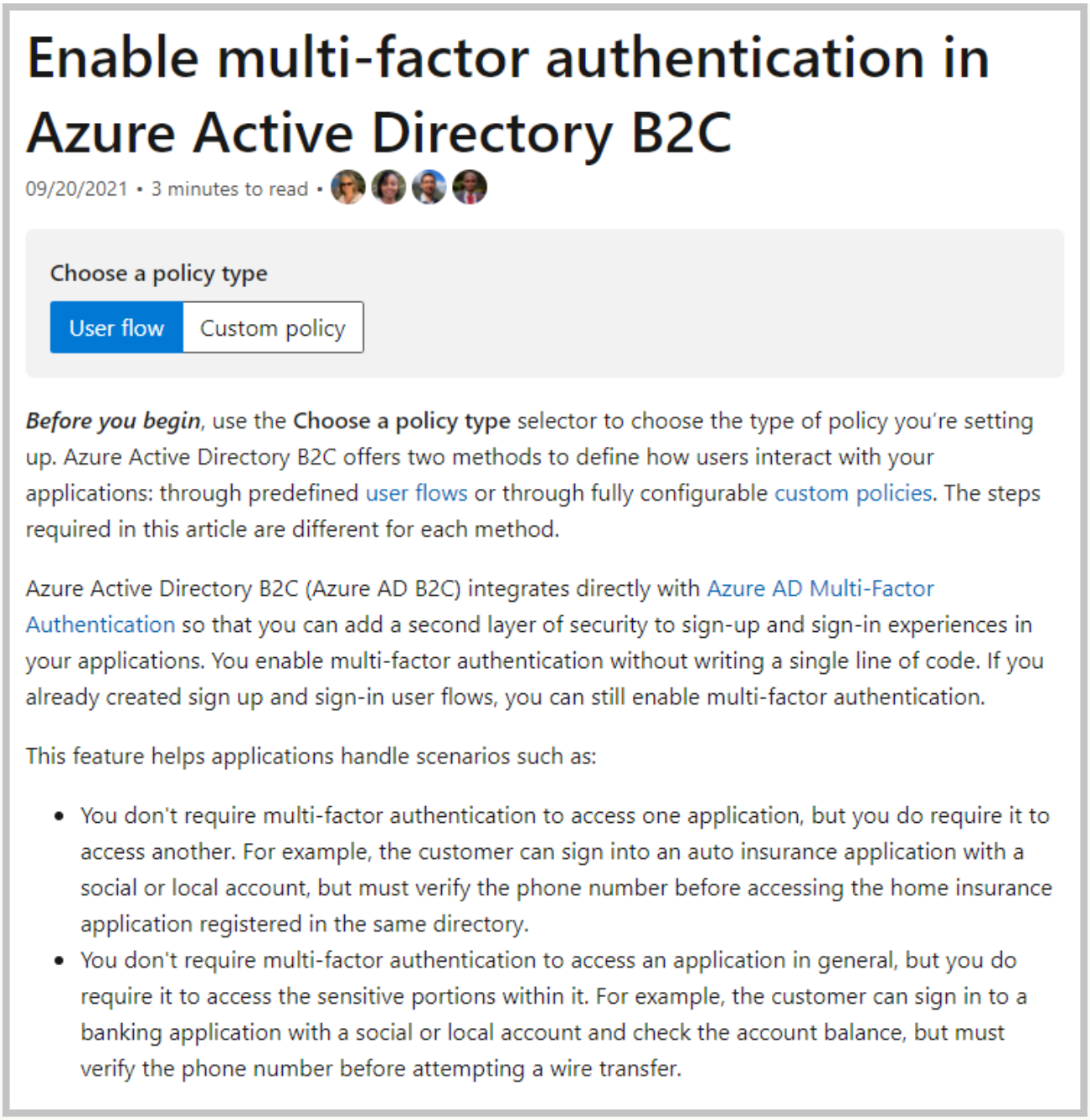
https://docs.microsoft.com/en-us/azure/active-directory-b2c/multi-factor-authentication?pivots=b2c-user-flow

What is Azure Active Directory B2C?

09/19/2019 • 5 minutes to read •

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

Azure Active Directory B2C (Azure AD B2C) is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring and automatically handling threats like denial-of-service, password spray, or brute force attacks.



Enable multi-factor authentication in Azure Active Directory B2C

09/20/2021 • 3 minutes to read •

Choose a policy type

User flow | Custom policy

Before you begin, use the **Choose a policy type** selector to choose the type of policy you're setting up. Azure Active Directory B2C offers two methods to define how users interact with your applications: through predefined user flows or through fully configurable custom policies. The steps required in this article are different for each method.

Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure AD Multi-Factor Authentication so that you can add a second layer of security to sign-up and sign-in experiences in your applications. You enable multi-factor authentication without writing a single line of code. If you already created sign up and sign-in user flows, you can still enable multi-factor authentication.

This feature helps applications handle scenarios such as:

- You don't require multi-factor authentication to access one application, but you do require it to access another. For example, the customer can sign into an auto insurance application with a social or local account, but must verify the phone number before accessing the home insurance application registered in the same directory.
- You don't require multi-factor authentication to access an application in general, but you do require it to access the sensitive portions within it. For example, the customer can sign in to a banking application with a social or local account and check the account balance, but must verify the phone number before attempting a wire transfer.

65. Question

A company named Techzen, Ltd. has an Azure Active Directory (Azure AD) tenant that uses the Basic license.

You plan to deploy two applications to Azure. The applications have the requirements shown in the following table.

Application Name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authentication
Reporting	Users must authenticate by using either Techzen credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

Which authentication strategy should you recommend for Reporting application?

A. An Azure AD B2C tenant

B. An Azure AD v1.0 endpoint

C. An Azure AD V2.0 endpoint

Correct

OAuth 2.0 and OpenID Connect standard-compliant authentication service enabling developers to authenticate several identity types, including:

? Work or school accounts, provisioned through Azure AD

? Personal Microsoft account, like Skype, Xbox, and Outlook.com

? Social or local accounts, by using Azure AD B2C

v1.0 does not support personal accounts, v2 – does. At the same time, integrating internal Techzen, Ltd accounts to B2C would be more difficult. B2C local accounts can't be named as Techzen, Ltd accounts, as there would be limited use of these accounts when managing Azure, or other usually internal services.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview

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 →

Skillcertpro

Quick Links

ABOUT US
FAQ
BROWSE ALL PRACTICE TESTS
CONTACT FORM

Important Links

REFUND POLICY
REFUND REQUEST
TERMS & CONDITIONS
PRIVACY POLICY