SKILLCERTPRO

IT CERTIFICATION TRAININGS

0

Microsoft Azure / By SkillCertPro

Practice Set 15

Your results are here!! for" Microsoft Azure AZ-305 Practice Test 15 "

42 of 65 questions answered correctly

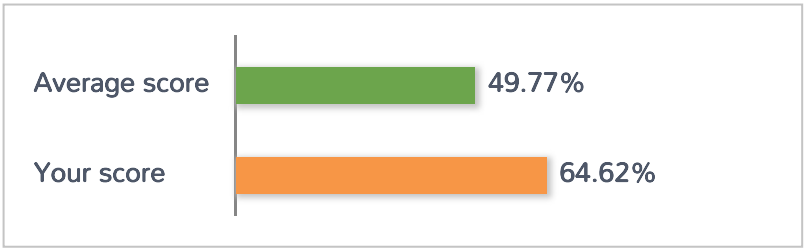
Your time: 01:24:50

Your Final Score is : 42

You have attempted : 65

Number of Correct Questions : 42 and scored 42

Number of Incorrect Questions : 23 and Negative marks 0

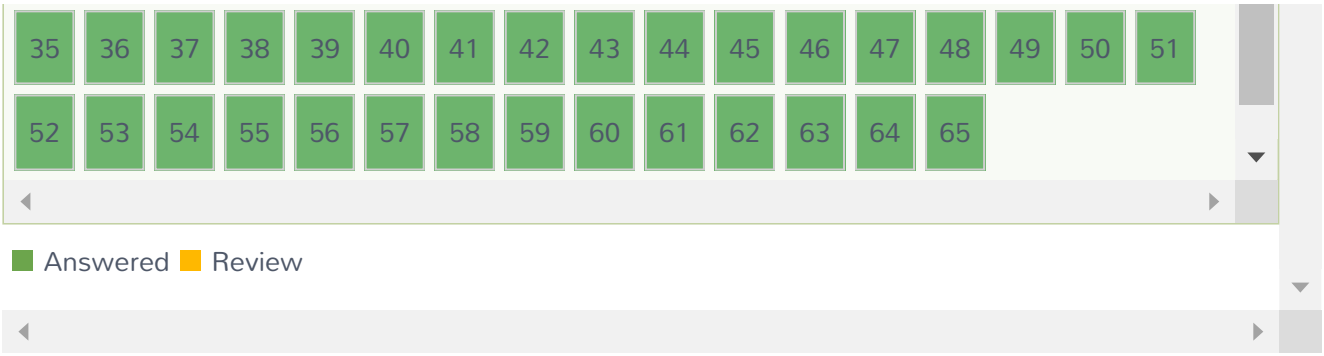


You can review your answers by clicking on “View Answers” option.

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

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

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

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

Several VMs are exhibiting network connectivity issues.

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

Solution: Use the Azure Advisor to analyze the network traffic.

Does the solution meet the goal?

- A. Yes
- **B. No**

Correct

Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

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

With Advisor, you can:

? Get proactive, actionable, and personalized best practices recommendations.

? Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.

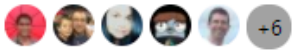
? Get recommendations with proposed actions inline.

Reference:

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

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

What is Azure Network Watcher?

01/04/2021 • 8 minutes to read • 

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

Monitoring

Monitor communication between a virtual machine and an endpoint

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

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

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

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

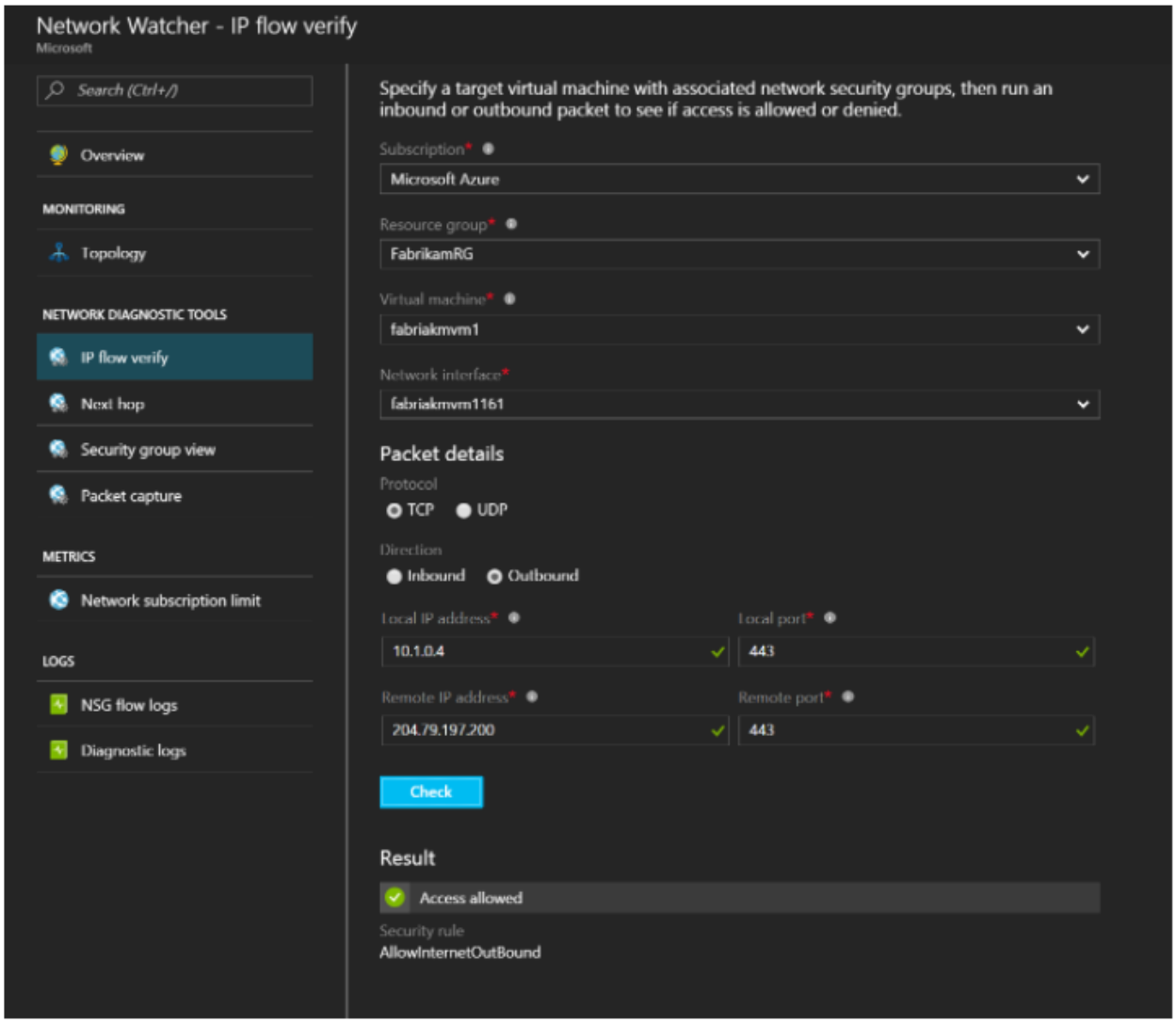
Introduction to IP flow verify in Azure Network Watcher

01/04/2021 • 2 minutes to read •

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

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

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



2. Question

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

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

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

Several VMs are exhibiting network connectivity issues.

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

Solution: Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.

Does the solution meet the goal?

- A. Yes
- **B. No**

Correct

Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

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

With Advisor, you can:

? Get proactive, actionable, and personalized best practices recommendations.

? Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.

? Get recommendations with proposed actions inline.

Reference:

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

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

What is Azure Network Watcher?

01/04/2021 • 8 minutes to read • +6

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

Monitoring

Monitor communication between a virtual machine and an endpoint

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

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

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

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

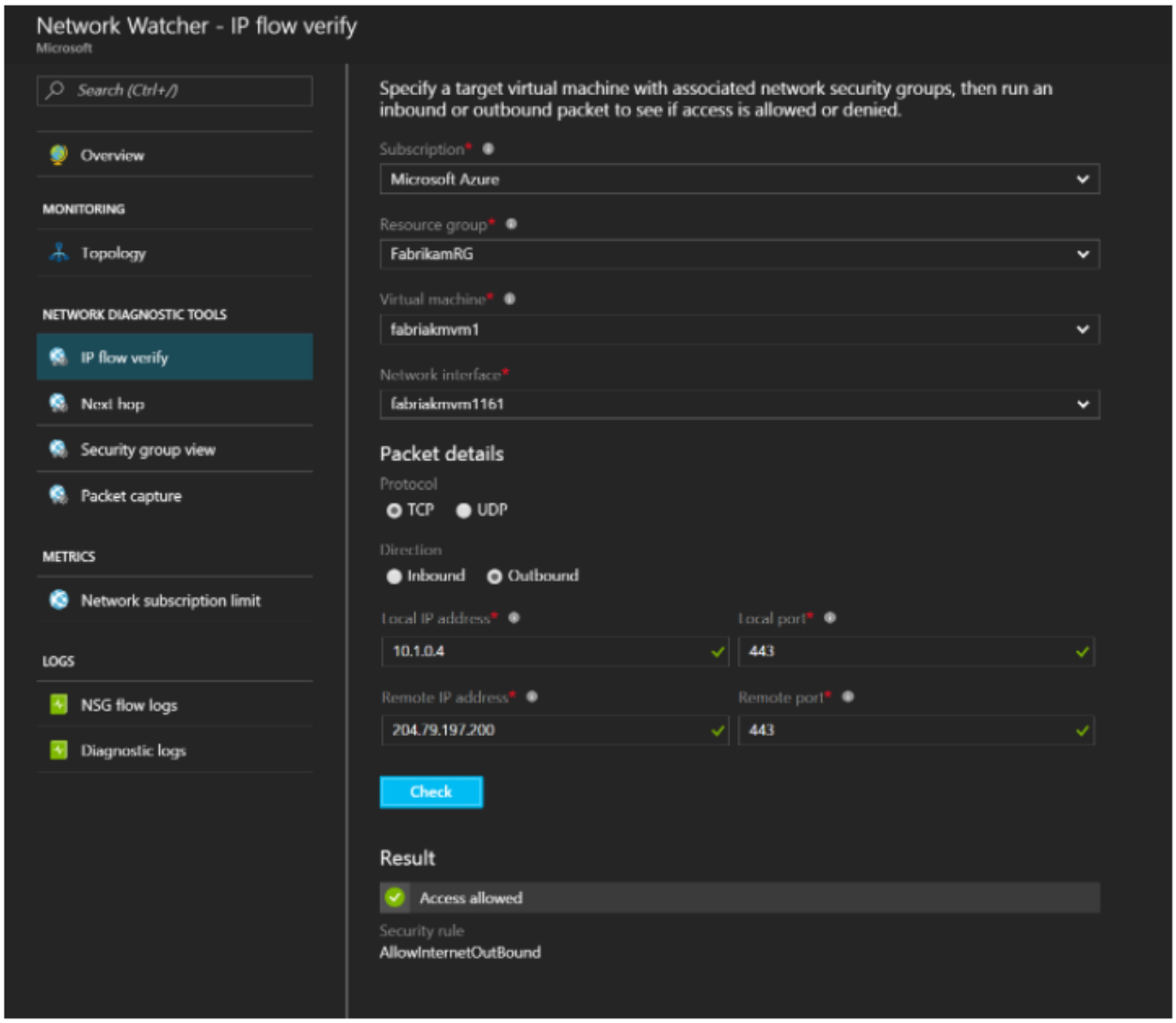
Introduction to IP flow verify in Azure Network Watcher

01/04/2021 • 2 minutes to read •

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

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

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



3. Question

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

Name	Type	Location
VNET1	Virtual Network	West US
Workspace1	Azure Log Analytics Workspace	West US
Storage1	Storage Account	West US
Storage2	Storage Account	East US

You need to archive the diagnostic data for VNET1 for 365 days. The solution must minimize costs.

Where should you archive the data?

- A. Workspace1
- B. storage1
- C. storage2

Correct

Diagnostics data can be:

? Written to an Azure Storage account, for auditing or manual inspection. You can specify the retention time (in days) using resource diagnostic settings.

? Streamed to an Event hub for ingestion by a third-party service, or custom analytics solution, such as PowerBI.

? Written to Azure Monitor logs.

Archiving logs and metrics to an Azure storage account is useful for audit, static analysis, or backup. Compared to Azure Monitor Logs and a Log Analytics workspace, Azure storage is less expensive and logs can be kept there indefinitely.

The storage account needs to be in the same region as the resource being monitored if the resource is regional.

Incorrect Answers:

A. Workspace1

The workspace is the top-level resource for Azure Machine Learning, providing a centralized place to work with all the artifacts you create when you use Azure Machine Learning. The workspace keeps a history of all training runs, including logs, metrics, output, and a snapshot of your scripts. It is not a ideal solution to store archival data.

C. storage2

The storage account needs to be in the same region as the resource being monitored. it will incur additional egress charges to transfer data.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log#log-destinations

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings?tabs=CMD

Destinations

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

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

Destination requirements

Any destinations for the diagnostic setting must be created before creating the diagnostic settings. The destination does not have to be in the same subscription as the resource sending logs as long as the user who configures the setting has appropriate Azure RBAC access to both subscriptions. Using Azure Lighthouse, it is also possible to have diagnostic settings sent to a workspace in another Azure Active Directory tenant. The following table provides unique requirements for each destination including any regional restrictions.

Destination	Requirements
Log Analytics workspace	The workspace does not need to be in the same region as the resource being monitored.
Event hubs	The shared access policy for the namespace defines the permissions that the streaming mechanism has. Streaming to Event Hubs requires Manage, Send, and Listen permissions. To update the diagnostic setting to include streaming, you must have the ListKey permission on that Event Hubs authorization rule. The event hub namespace needs to be in the same region as the resource being monitored if the resource is regional.
Azure storage account	You should not use an existing storage account that has other, non-monitoring data stored in it so that you can better control access to the data. If you are archiving the Activity log and resource logs together though, you may choose to use the same storage account to keep all monitoring data in a central location. To send the data to immutable storage, set the immutable policy for the storage account as described in Set and manage immutability policies for Blob storage. You must follow all steps in this article including enabling protected append blobs writes. The storage account needs to be in the same region as the resource being monitored if

the resource is regional.

Note

Azure Data Lake Storage Gen2 accounts are not currently supported as a destination for diagnostic settings even though they may be listed as a valid option in the Azure portal.

Note

Azure Monitor (Diagnostic Settings) can't access Event Hubs resources when virtual networks are enabled. You have to enable the Allow trusted Microsoft services to bypass this firewall setting in Event Hub, so that Azure Monitor (Diagnostic Settings) service is granted access to your Event Hubs resources.

4. Question

You plan to create an Azure Cosmos DB account that uses the SQL API. The account will contain data added by a web application. The web application will send data daily.

You need to recommend a notification solution that meets the following requirements:

? Sends email notifications when data is received from the web application

? Minimizes compute cost

What should you include in the recommendation?

- A. Deploy an Azure logic app that has a SendGrid connector configured to use an Azure Cosmos DB action
- B. Deploy a function app that is configured to use the Consumption plan and an Azure Event Hubs binding
- **C. Deploy a function app that is configured to use the Consumption plan and a SendGrid binding**
- D. Deploy an Azure logic app that has a webhook configured to use a SendGrid action

Incorrect

You can send email by using SendGrid bindings in Azure Functions. Azure Functions supports an output binding for SendGrid.

Note: When you're using the Consumption plan, instances of the Azure Functions host are dynamically added and removed based on the number of incoming events.

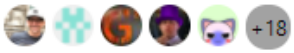
Reference:

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

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

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

Azure Functions triggers and bindings concepts

02/18/2019 • 6 minutes to read • 

In this article you learn the high-level concepts surrounding functions triggers and bindings.

Triggers are what cause a function to run. A trigger defines how a function is invoked and a function must have exactly one trigger. Triggers have associated data, which is often provided as the payload of the function.

Binding to a function is a way of declaratively connecting another resource to the function; bindings may be connected as *input bindings*, *output bindings*, or both. Data from bindings is provided to the function as parameters.

You can mix and match different bindings to suit your needs. Bindings are optional and a function might have one or multiple input and/or output bindings.

Triggers and bindings let you avoid hardcoding access to other services. Your function receives data (for example, the content of a queue message) in function parameters. You send data (for example, to create a queue message) by using the return value of the function.

Consider the following examples of how you could implement different functions.

Example scenario	Trigger	Input binding	Output binding
A new queue message arrives which runs a function to write to another queue.	Queue*	*None*	Queue*
A scheduled job reads Blob Storage contents and creates a new Cosmos DB document.	Timer	Blob Storage	Cosmos DB
The Event Grid is used to read an image from Blob Storage and a document from Cosmos DB to send an email.	Event Grid	Blob Storage and Cosmos DB	SendGrid
A webhook that uses Microsoft Graph to update an Excel sheet.	HTTP	*None*	Microsoft Graph

* Represents different queues

These examples are not meant to be exhaustive, but are provided to illustrate how you can use triggers and bindings together.

Azure Functions SendGrid bindings

11/29/2017 • 6 minutes to read • 

This article explains how to send email by using SendGrid bindings in Azure Functions. Azure Functions supports an output binding for SendGrid.

This is reference information for Azure Functions developers. If you're new to Azure Functions, start with the following resources:

- Create your first function: C#, JavaScript, Java, or Python.
- Azure Functions developer reference.
- Language-specific reference: C#, C# script, F#, Java, JavaScript, or Python.
- Azure Functions triggers and bindings concepts.
- Code and test Azure Functions locally.

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.

5. Question

You on-premises network contains a file server named Server1 that stores 500 GB of data.

You need to use Azure Data Factory to copy the data from Server1 to Azure Storage.

You add a new data factory.

Which of the following would go into Slot1?

- A. Install an Azure File Sync agent
- **B. Install a self-hosted integration runtime**
- C. Install the File Server Resource Manager role service

Correct

The Integration Runtime is a customer-managed data integration infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

Reference:

https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-sql-azure-adf

https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime?tabs=data-factory

Create and configure a self-hosted integration runtime

09/09/2021 • 23 minutes to read • +30

APPLIES TO: Azure Data Factory Azure Synapse Analytics

The integration runtime (IR) is the compute infrastructure that Azure Data Factory and Synapse pipelines use to provide data-integration capabilities across different network environments. For details about IR, see Integration runtime overview.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

This article describes how you can create and configure a self-hosted IR.

Note

This article has been updated to use the Azure Az PowerShell module. The Az PowerShell module is the recommended PowerShell module for interacting with Azure. To get started with the Az PowerShell module, see **Install Azure PowerShell**. To learn how to migrate to the Az PowerShell module, see **Migrate Azure PowerShell from AzureRM to Az.**

6. Question

You on-premises network contains a file server named Server1 that stores 500 GB of data.

You need to use Azure Data Factory to copy the data from Server1 to Azure Storage.

You add a new data factory.

Which of the following would go into Slot2?

- A. Create a pipeline
- B. Create an import/export job
- C. Provision an Azure-SQL Server Integration Services (SSIS) integration runtime

Correct

With ADF, existing data processing services can be composed into data pipelines that are highly available and managed in the cloud. These data pipelines can be scheduled to ingest, prepare, transform, analyze, and publish data, and ADF manages and orchestrates the complex data and processing dependencies

A pipeline is a logical grouping of activities that together perform a task. For example, a pipeline could contain a set of activities that ingest and clean log data, and then kick off a mapping data flow to analyze the log data. The pipeline allows you to manage the activities as a set instead of each one individually. You deploy and schedule the pipeline instead of the activities independently.

Reference:

https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-sql-azure-adf

https://docs.microsoft.com/en-us/azure/data-factory/concepts-pipelines-activities

https://docs.microsoft.com/en-us/azure/data-factory/connector-file-system

Introduction: What is ADF and when should it be used to migrate data?

Azure Data Factory is a fully managed cloud-based data integration service that orchestrates and automates the movement and transformation of data. The key concept in the ADF model is pipeline. A pipeline is a logical grouping of Activities, each of which defines the actions to perform on the data contained in Datasets. Linked services are used to define the information needed for Data Factory to connect to the data resources.

With ADF, existing data processing services can be composed into data pipelines that are highly available and managed in the cloud. These data pipelines can be scheduled to ingest, prepare, transform, analyze, and publish data, and ADF manages and orchestrates the complex data and processing dependencies. Solutions can be quickly built and deployed in the cloud, connecting a growing number of on-premises and cloud data sources.

Consider using ADF:

- when data needs to be continually migrated in a hybrid scenario that accesses both on-premises and cloud resources
- when the data needs transformations or have business logic added to it when being migrated.

ADF allows for the scheduling and monitoring of jobs using simple JSON scripts that manage the movement of data on a periodic basis. ADF also has other capabilities such as support for complex operations. For more information on ADF, see the documentation at Azure Data Factory (ADF).

Pipelines and activities in Azure Data Factory and Azure Synapse Analytics

09/09/2021 • 16 minutes to read • +19

Select the version of Data Factory service you're using: Current version

APPLIES TO: Azure Data Factory Azure Synapse Analytics

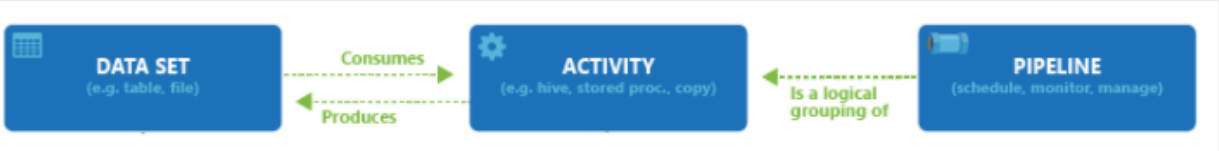
This article helps you understand pipelines and activities in Azure Data Factory and Azure Synapse Analytics and use them to construct end-to-end data-driven workflows for your data movement and data processing scenarios.

Overview

A Data Factory or Synapse Workspace can have one or more pipelines. A pipeline is a logical grouping of activities that together perform a task. For example, a pipeline could contain a set of activities that ingest and clean log data, and then kick off a mapping data flow to analyze the log data. The pipeline allows you to manage the activities as a set instead of each one individually. You deploy and schedule the pipeline instead of the activities independently.

The activities in a pipeline define actions to perform on your data. For example, you may use a copy activity to copy data from SQL Server to an Azure Blob Storage. Then, use a data flow activity or a Databricks Notebook activity to process and transform data from the blob storage to an Azure Synapse Analytics pool on top of which business intelligence reporting solutions are built.

Azure Data Factory and Azure Synapse Analytics have three groupings of activities: data movement activities, data transformation activities, and control activities. An activity can take zero or more input datasets and produce one or more output datasets. The following diagram shows the relationship between pipeline, activity, and dataset:



An input dataset represents the input for an activity in the pipeline, and an output dataset represents the output for the activity. Datasets identify data within different data stores, such as tables, files, folders, and documents. After you create a dataset, you can use it with activities in a pipeline. For example, a dataset can be an input/output dataset of a Copy Activity or an HDInsightHive Activity. For more information about datasets, see Datasets in Azure Data Factory article.

7. Question

You have an existing implementation of Microsoft SQL Server Integration Services (SSIS) packages stored in an SSISDB catalog on your on-premises network.

The on-premises network does not have hybrid connectivity to Azure by using Site-to-Site VPN or ExpressRoute.

You want to migrate the packages to Azure Data Factory.

You need to recommend a solution that facilitates the migration while minimizing changes to the existing packages. The solution must minimize costs.

Store the SSISDB catalog by using:	SLOT-1
Implement a runtime engine for package execution by using:	SLOT-2

Which of the following would go into Slot1?

- A. Azure SQL Database
- B. Azure Synapse Analytics
- C. SQL Server on an Azure virtual machine
- D. SQL Server on an on-premises computer

Incorrect

You can now move your SQL Server Integration Services (SSIS) projects, packages, and workloads to the Azure cloud. Deploy, run, and manage SSIS projects and packages in the SSIS Catalog (SSISDB) on Azure SQL Database or SQL Managed Instance with familiar tools such as SQL Server Management Studio (SSMS)

Note: You can't create the SSISDB Catalog database on Azure SQL Database at this time independently of creating the Azure-SSIS Integration Runtime in Azure Data Factory. The Azure-SSIS IR is the runtime environment that runs SSIS packages on Azure.

Incorrect Answers:

B. Azure Synapse Analytics

Azure Synapse is an enterprise analytics service that accelerates time to insight across data warehouses and big data systems.

C. SQL Server on an Azure virtual machine

You have to pay additional costs for managing virtual machine.

Reference:

https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-connect-to-catalog-database

https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-lift-shift-ssis-packages-overview?view=sql-server-ver15

Lift and shift SQL Server Integration Services workloads to the cloud

09/23/2018 • 7 minutes to read • +4

Applies to: SQL Server (all supported versions) SSIS Integration Runtime in Azure Data Factory

You can now move your SQL Server Integration Services (SSIS) projects, packages, and workloads to the Azure cloud. Deploy, run, and manage SSIS projects and packages in the SSIS Catalog (SSISDB) on Azure SQL Database or SQL Managed Instance with familiar tools such as SQL Server Management Studio (SSMS).

Benefits

Moving your on-premises SSIS workloads to Azure has the following potential benefits:

- **Reduce operational costs** and reduce the burden of managing infrastructure that you have when you run SSIS on-premises or on Azure virtual machines.
- **Increase high availability** with the ability to specify multiple nodes per cluster, as well as the high availability features of Azure and of Azure SQL Database.
- **Increase scalability** with the ability to specify multiple cores per node (scale up) and multiple nodes per cluster (scale out).

Architecture of SSIS on Azure

The following table highlights the differences between SSIS on premises and SSIS on Azure.

The most significant difference is the separation of storage from runtime. Azure Data Factory hosts the runtime engine for SSIS packages on Azure. The runtime engine is called the Azure-SSIS Integration Runtime (Azure-SSIS IR). For more info, see Azure-SSIS Integration Runtime.

Location	Storage	Runtime	Scalability
On premises	SQL Server	SSIS runtime hosted by SQL Server	SSIS Scale Out (in SQL Server 2017 and later) Custom solutions (in prior versions of SQL Server)
On Azure	SQL Database or SQL Managed Instance	Azure-SSIS Integration Runtime, a component of Azure Data Factory	Scaling options for the Azure-SSIS Integration Runtime

8. Question

You have an existing implementation of Microsoft SQL Server Integration Services (SSIS) packages stored in an SSISDB catalog on your on-premises network.

The on-premises network does not have hybrid connectivity to Azure by using Site-to-Site VPN or ExpressRoute.

You want to migrate the packages to Azure Data Factory.

You need to recommend a solution that facilitates the migration while minimizing changes to the existing packages. The solution must minimize costs.

Which of the following would go into Slot2?

- A. Self-hosted integration runtime only
- B. Azure-SQL Server Integration Services Integration Runtime (IR) only
- C. Azure-SQL Server Integration Services Integration Runtime and self-hosted integration runtime

Incorrect

The Integration Runtime (IR) is the compute infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments. Azure-SSIS Integration Runtime (IR) in Azure Data Factory (ADF) supports running SSIS packages.

Self-hosted integration runtime can be used for data movement in this scenario.

Why Self hosted IR?

This article describes how to run SQL Server Integration Services (SSIS) packages on an Azure-SSIS Integration Runtime (Azure-SSIS IR) in Azure Data Factory with a self-hosted integration runtime (self-hosted IR) configured as a proxy.

With this feature, you can access data on-premises without having to join your Azure-SSIS IR to a virtual network. The feature is useful when your corporate network has a configuration too complex or a policy too restrictive for you to inject your Azure-SSIS IR into it.

As Azure cloud does not connectivity to on Premise network you would need to implement self Hosted-IR as well

Reference:

https://docs.microsoft.com/en-us/azure/data-factory/create-azure-integration-runtime

https://docs.microsoft.com/en-us/azure/data-factory/self-hosted-integration-runtime-proxy-ssis

How to create and configure Azure Integration Runtime

09/09/2021 • 3 minutes to read • 

APPLIES TO: Azure Data Factory Azure Synapse Analytics

The Integration Runtime (IR) is the compute infrastructure used by Azure Data Factory and Synapse pipelines to provide data integration capabilities across different network environments. For more information about IR, see Integration runtime.

Azure IR provides a fully managed compute to natively perform data movement and dispatch data transformation activities to compute services like HDInsight. It is hosted in Azure environment and supports connecting to resources in public network environment with public accessible endpoints.

This document introduces how you can create and configure Azure Integration Runtime.

Note

This article has been updated to use the Azure Az PowerShell module. The Az PowerShell module is the recommended PowerShell module for interacting with Azure. To get started with the Az PowerShell module, see **Install Azure PowerShell**. To learn how to migrate to the Az PowerShell module, see **Migrate Azure PowerShell from AzureRM to Az**.

Configure a self-hosted IR as a proxy for an Azure-SSIS IR in Azure Data Factory

09/17/2021 • 11 minutes to read • +11

APPLIES TO: Azure Data Factory Azure Synapse Analytics

This article describes how to run SQL Server Integration Services (SSIS) packages on an Azure-SSIS Integration Runtime (Azure-SSIS IR) in Azure Data Factory (ADF) with a self-hosted integration runtime (self-hosted IR) configured as a proxy.

With this feature, you can access data and run tasks on premises without having to join your Azure-SSIS IR to a virtual network. The feature is useful when your corporate network has a configuration too complex or a policy too restrictive for you to inject your Azure-SSIS IR into it.

This feature can only be enabled on SSIS Data Flow Task and Execute SQL/Process Tasks for now.

Enabled on Data Flow Task, this feature will break it down into two staging tasks whenever applicable:

- **On-premises staging task**: This task runs your data flow component that connects to an on-premises data store on your self-hosted IR. It moves data from the on-premises data store into a staging area in your Azure Blob Storage or vice versa.
- **Cloud staging task**: This task runs your data flow component that doesn't connect to an on-premises data store on your Azure-SSIS IR. It moves data from the staging area in your Azure Blob Storage to a cloud data store or vice versa.

If your Data Flow Task moves data from on premises to cloud, then the first and second staging tasks will be on-premises and cloud staging tasks, respectively. If your Data Flow Task moves data from cloud to on premises, then the first and second staging tasks will be cloud and on-premises staging tasks, respectively. If your Data Flow Task moves data from on premises to on premises, then the first and second staging tasks will be both on-premises staging tasks. If your Data Flow Task moves data from cloud to cloud, then this feature isn't applicable.

Enabled on Execute SQL/Process Tasks, this feature will run them on your self-hosted IR.

Other benefits and capabilities of this feature allow you to, for example, set up your self-hosted IR in regions that are not yet supported by an Azure-SSIS IR, and allow the public static IP address of your self-hosted IR on the firewall of your data sources.

9. Question

You are designing an Azure Cosmos DB solution that will host multiple writable replicas in multiple Azure regions.

You need to recommend the strongest database consistency level for the design. The solution must meet the following requirements:

? Provide a latency-based Service Level Agreement (SLA) for writes.

? Support multiple regions.

Which consistency level should you recommend?

- A. bounded staleness
- B. strong
- C. session
- D. consistent prefix

Incorrect

Each level provides availability and performance tradeoffs. The following image shows the different consistency levels as a spectrum.

Note: The service offers comprehensive 99.99% SLAs which covers the guarantees for throughput, consistency, availability and latency for the Azure Cosmos DB Database Accounts scoped to a single Azure region configured with any of the five Consistency Levels or Database Accounts spanning multiple Azure regions, configured with any of the four relaxed Consistency Levels.

Incorrect Answers:

B. strong

Strong consistency for accounts with regions spanning more than 5000 miles (8000 kilometers) is blocked by default due to high write latency. To enable this capability please contact support.

C. session

In session consistency, within a single client session reads are guaranteed to honor the consistent-prefix, monotonic reads, monotonic writes, read-your-writes, and write-follows-reads guarantees.

D. consistent prefix

In consistent prefix option, updates that are returned contain some prefix of all the updates, with no gaps. Consistent prefix consistency level guarantees that reads never see out-of-order writes.

Reference:

https://azure.microsoft.com/en-us/support/legal/sla/cosmos-db/v1_3/

https://docs.microsoft.com/en-us/azure/cosmos-db/consistency-levels#consistency-levels-and-latency

Consistency levels in Azure Cosmos DB

09/20/2021 • 13 minutes to read • +10

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

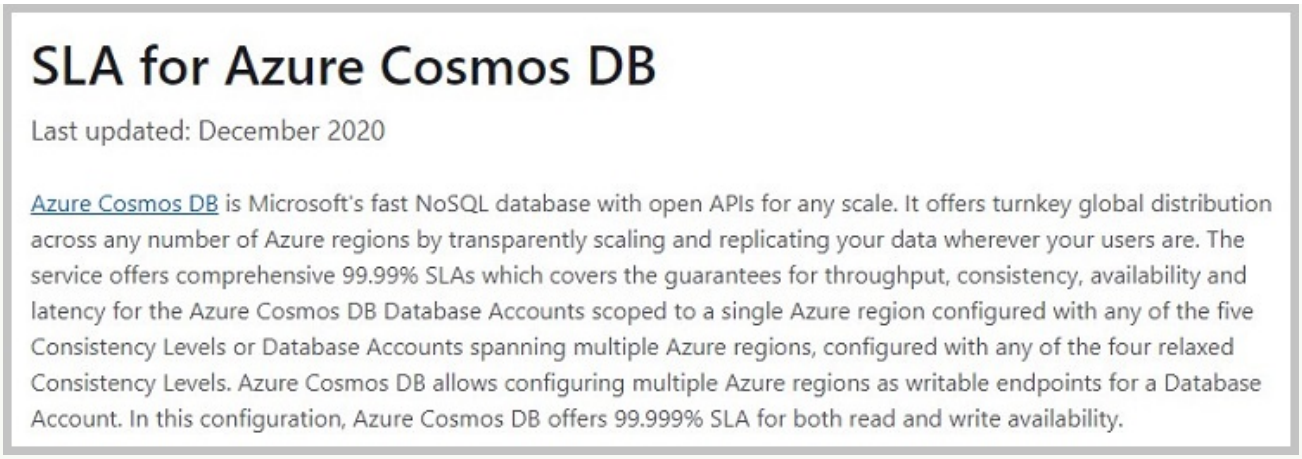
Distributed databases that rely on replication for high availability, low latency, or both, must make a fundamental tradeoff between the read consistency, availability, latency, and throughput as defined by the PACLC theorem. The linearizability of the strong consistency model is the gold standard of data programmability. But it adds a steep price from higher write latencies due to data having to replicate and commit across large distances. Strong consistency may also suffer from reduced availability (during failures) because data cannot replicate and commit in every region. Eventual consistency offers higher availability and better performance, but its more difficult to program applications because data may not be completely consistent across all regions.

Most commercially available distributed NoSQL databases available in the market today provide only strong and eventual consistency. Azure Cosmos DB offers five well-defined levels. From strongest to weakest, the levels are:

- *Strong*
- *Bounded staleness*
- *Session*
- *Consistent prefix*
- *Eventual*

Each level provides availability and performance tradeoffs. The following image shows the different consistency levels as a spectrum.

The consistency levels are region-agnostic and are guaranteed for all operations regardless of the region from which the reads and writes are served, the number of regions associated with your Azure Cosmos account, or whether your account is configured with a single or multiple write regions.



SLA for Azure Cosmos DB

Last updated: December 2020

Azure Cosmos DB is Microsoft's fast NoSQL database with open APIs for any scale. It offers turnkey global distribution across any number of Azure regions by transparently scaling and replicating your data wherever your users are. The service offers comprehensive 99.99% SLAs which covers the guarantees for throughput, consistency, availability and latency for the Azure Cosmos DB Database Accounts scoped to a single Azure region configured with any of the five Consistency Levels or Database Accounts spanning multiple Azure regions, configured with any of the four relaxed Consistency Levels. Azure Cosmos DB allows configuring multiple Azure regions as writable endpoints for a Database Account. In this configuration, Azure Cosmos DB offers 99.999% SLA for both read and write availability.

10. Question

You have an Azure web app named App1 and an Azure key vault named KV1.

App1 stores database connection strings in KV1.

App1 performs the following types of requests to KV1:

? Get

? List

? Wrap

? Delete

? Unwrap

? Backup

? Decrypt

? Encrypt

You are evaluating the continuity of service for App1.

You need to identify the following if the Azure region that hosts KV1 becomes unavailable:

Which of the following would go into Slot1?

- A. A server in the same Availability Set
- B. A server in the same fault domain
- C. A server in the same paired region
- D. A virtual machine in a scale set

Correct

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.

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.

Incorrect Answers:

A. A server in the same Availability Set

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. It is applicable for virtual machines.

B. A server in the same fault domain

A fault domain is a set of hardware components that share a single point of failure. To be fault tolerant to a certain level, you need multiple fault domains at that level. It is applicable for virtual machines.

D. A virtual machine in a 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. It is applicable for virtual machines.

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.

In the Brazil South and Qatar Central region, you must plan for the recovery of your Azure key vaults in a region failure scenario. To back up and restore your Azure key vault to a region of your choice, complete the steps that are detailed in Azure Key Vault backup.

Through this high availability design, Azure Key Vault requires no downtime for maintenance activities.

11. Question

You have an Azure web app named App1 and an Azure key vault named KV1.

App1 stores database connection strings in KV1.

App1 performs the following types of requests to KV1:

? Get

? List

? Wrap

? Delete

? Unwrap

? Backup

? Decrypt

? Encrypt

You are evaluating the continuity of service for App1.

You need to identify the following if the Azure region that hosts KV1 becomes unavailable:

Which of the following would go into Slot2?

- Backup
- Decrypt
- Delete
- Encrypt
- Get
- List

Incorrect

There are a few caveats to be aware of:

? In the event of a region failover, it may take a few minutes for the service to fail over. Requests that are made during this time before failover may fail.

? If you are using private link to connect to your key vault, it may take up to 20 minutes for the connection to be re-established in the event of a failover.

? During failover, your key vault is in read-only mode. Requests that are supported in this mode

? During failover, your key vault is in read-only mode. Requests that are supported in this mode are:

? List certificates

? Get certificates

? List secrets

? Get secrets

? List keys

? Get (properties of) keys

? Encrypt

? Decrypt

? Wrap

? Unwrap

? Verify

? Sign

? Backup

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.

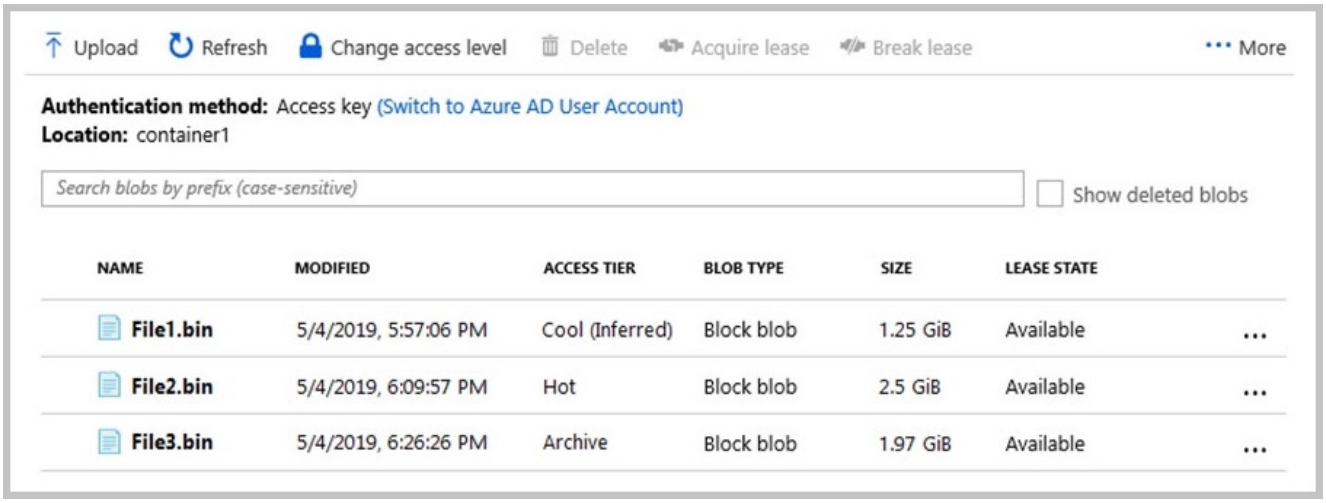
Note

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.

- During failover, your key vault is in read-only mode. Requests that are supported in this mode are:
  - List certificates
  - Get certificates
  - List secrets
  - Get secrets
  - List keys
  - Get (properties of) keys
  - Encrypt
  - Decrypt
  - Wrap
  - Unwrap
  - Verify
  - Sign
  - Backup

12. Question

You have an Azure Storage account that contains the data shown in the following exhibit.



You need to identify which files can be accessed immediately from the storage account.

Which files should you identify?

- A. File1.bin only
- B. File2.bin only
- C. File3.bin only
- **D. File1.bin and File2.bin only**
- E. File1.bin, File2.bin, and File3.bin

Correct

Hot – Optimized for storing data that is accessed frequently.

Cool – Optimized for storing data that is infrequently accessed and stored for at least 30 days.

Archive – Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

File1.bin and File2.bin are in Hot and Cool access tier and can be accessed immediately.

Note: You need to rehydrate data in archive tier to access.

Reference:

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

Access tiers for Azure Blob Storage - hot, cool, and archive

03/18/2021 • 13 minutes to read • +17

Azure storage offers different access tiers, allowing you to store blob object data in the most cost-effective manner. Available access tiers include:

- **Hot** - Optimized for storing data that is accessed frequently.
- **Cool** - Optimized for storing data that is infrequently accessed and stored for at least 30 days.
- **Archive** - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.

The following considerations apply to the different access tiers:

- The access tier can be set on a blob during or after upload.
- Only the hot and cool access tiers can be set at the account level. The archive access tier can only be set at the blob level.
- Data in the cool access tier has slightly lower availability, but still has high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, slightly lower availability and higher access costs are acceptable trade-offs for lower overall storage costs compared to hot data. For more information, see SLA for storage.
- Data in the archive access tier is stored offline. The archive tier offers the lowest storage costs but also the highest access costs and latency.
- The hot and cool tiers support all redundancy options. The archive tier supports only LRS, GRS, and RA-GRS.
- Data storage limits are set at the account level and not per access tier. You can choose to use all of your limit in one tier or across all three tiers.

13. 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 on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing an Azure Storage account, and then running AzCopy.

Does this meet the goal?

A. Yes

B. No

Correct

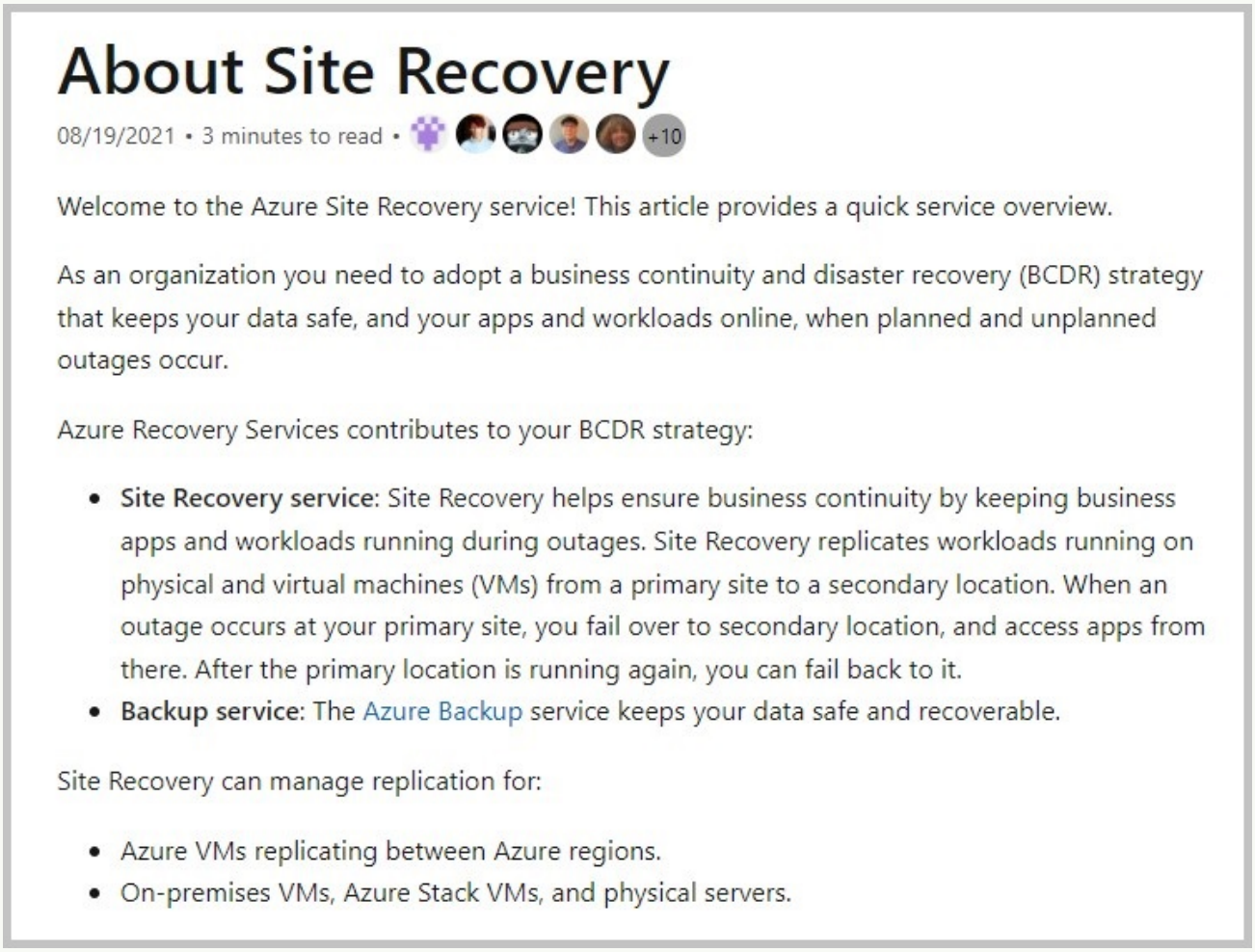
AzCopy only copy files, not the disks. Instead use Azure Site Recovery.

Note: To ensure that the virtual machines remain available during the migration, use Azure Site Recovery otherwise you can use Azure Migrate.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-hyper-v#replicate-hyper-v-vms



About Site Recovery

08/19/2021 • 3 minutes to read • +10

Welcome to the Azure Site Recovery service! This article provides a quick service overview.

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads online, when planned and unplanned outages occur.

Azure Recovery Services contributes to your BCDR strategy:

- **Site Recovery service**: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- **Backup service**: The Azure Backup service keeps your data safe and recoverable.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs, and physical servers.

14. 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 on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing an Azure Storage account that has a file service and a blob service, and then using the Data Migration Assistant.

Does this meet the goal?

- A. Yes
- B. No

Correct

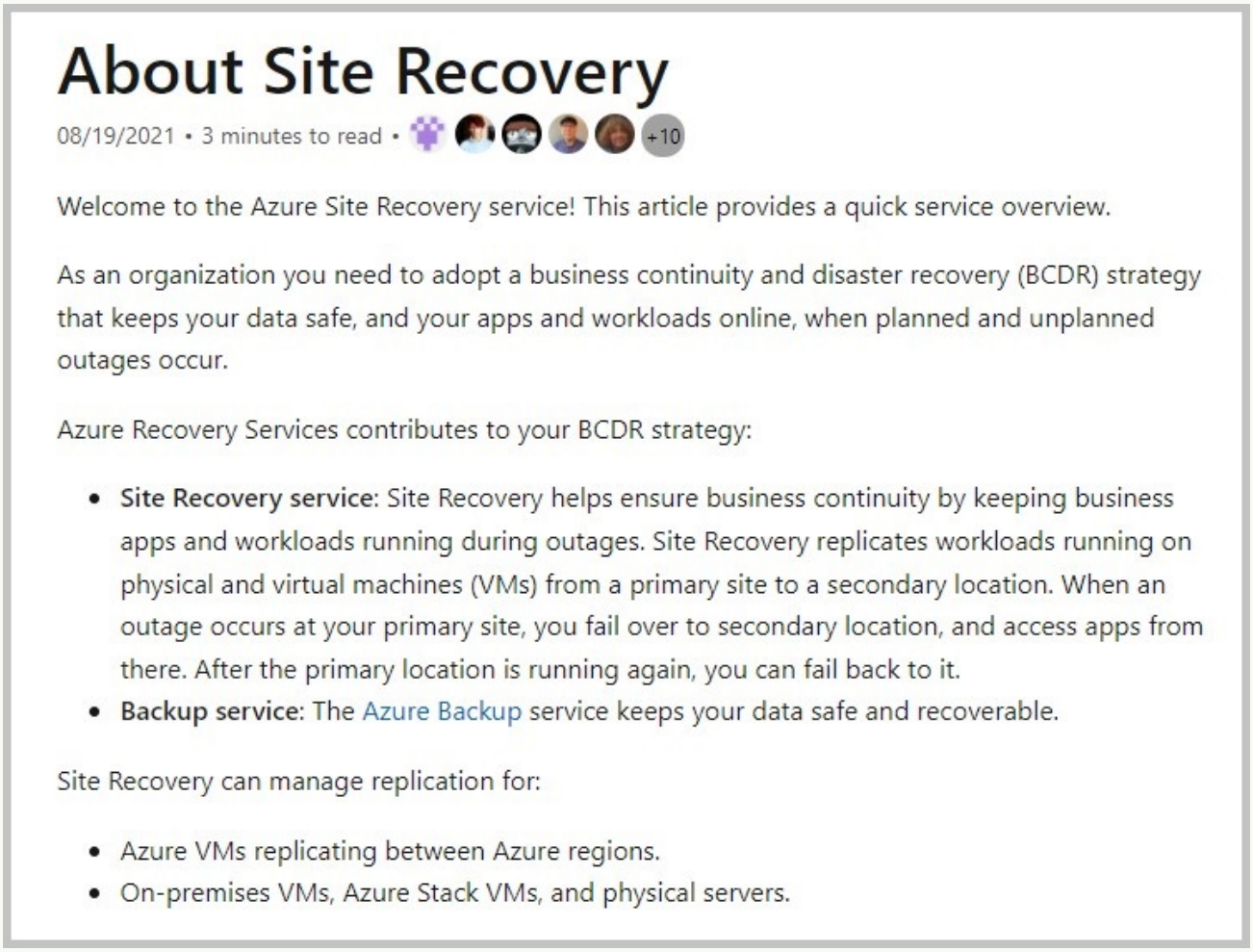
Data Migration Assistant is used to migrate SQL databases. Instead use Azure Site Recovery.

Note: To ensure that the virtual machines remain available during the migration, use Azure Site Recovery otherwise you can use Azure Migrate.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-hyper-v#replicate-hyper-v-vms



About Site Recovery

08/19/2021 • 3 minutes to read • +10

Welcome to the Azure Site Recovery service! This article provides a quick service overview.

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads online, when planned and unplanned outages occur.

Azure Recovery Services contributes to your BCDR strategy:

- **Site Recovery service**: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- **Backup service**: The Azure Backup service keeps your data safe and recoverable.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs, and physical servers.

15. 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 on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing a Recovery Services vault, and then using Azure Site Recovery.

Does this meet the goal?

- A. Yes
- B. No

Correct

Site Recovery can replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure.

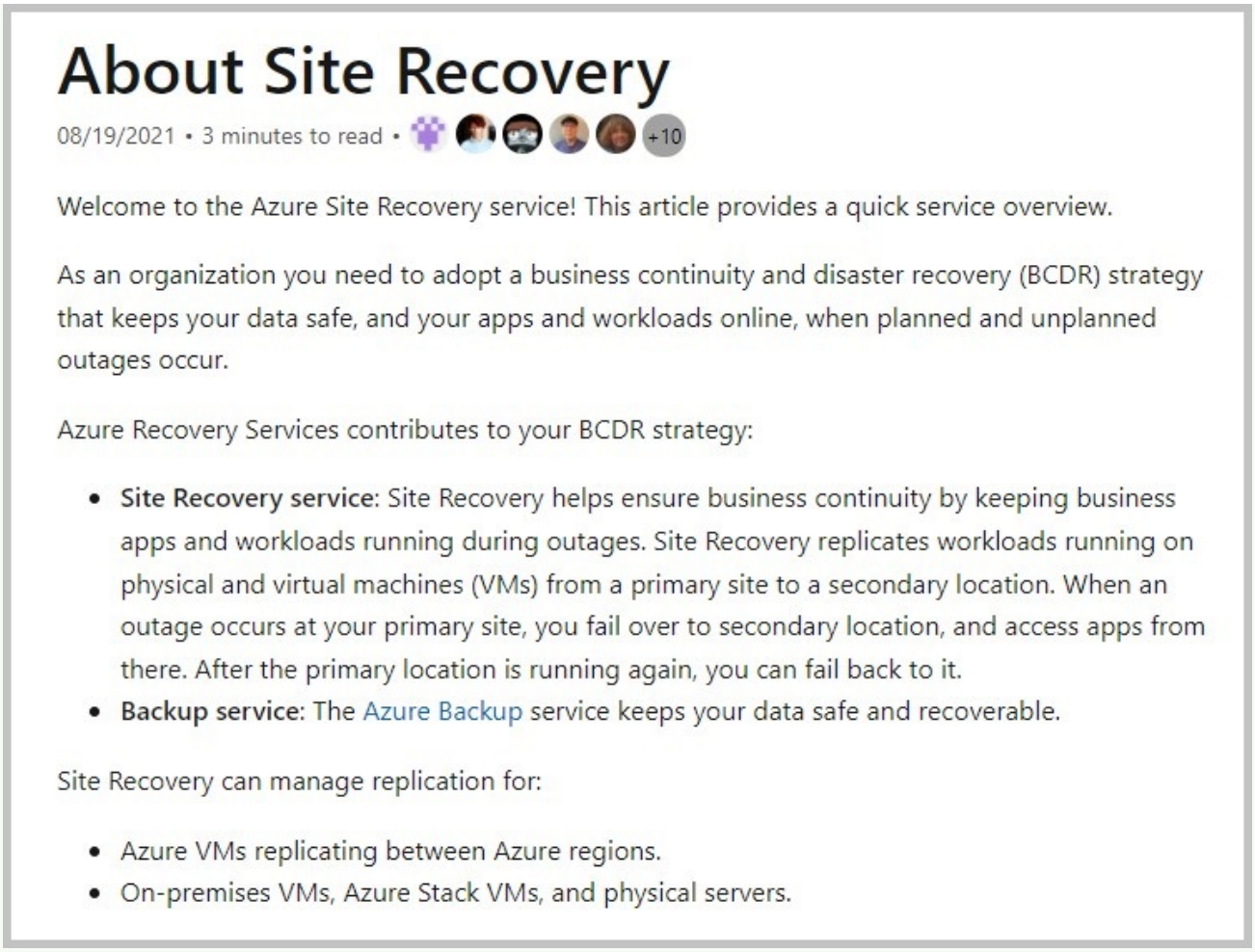
Note: To ensure that the virtual machines remain available during the migration, use Azure Site Recovery otherwise you can use Azure Migrate.

Note: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-hyper-v#replicate-hyper-v-vms



About Site Recovery

08/19/2021 • 3 minutes to read • +10

Welcome to the Azure Site Recovery service! This article provides a quick service overview.

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads online, when planned and unplanned outages occur.

Azure Recovery Services contributes to your BCDR strategy:

- **Site Recovery service**: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- **Backup service**: The Azure Backup service keeps your data safe and recoverable.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs, and physical servers.

16. 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 on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing an Azure Storage account, and then using Azure Migrate.

Does this meet the goal?

- A. Yes
- B. No

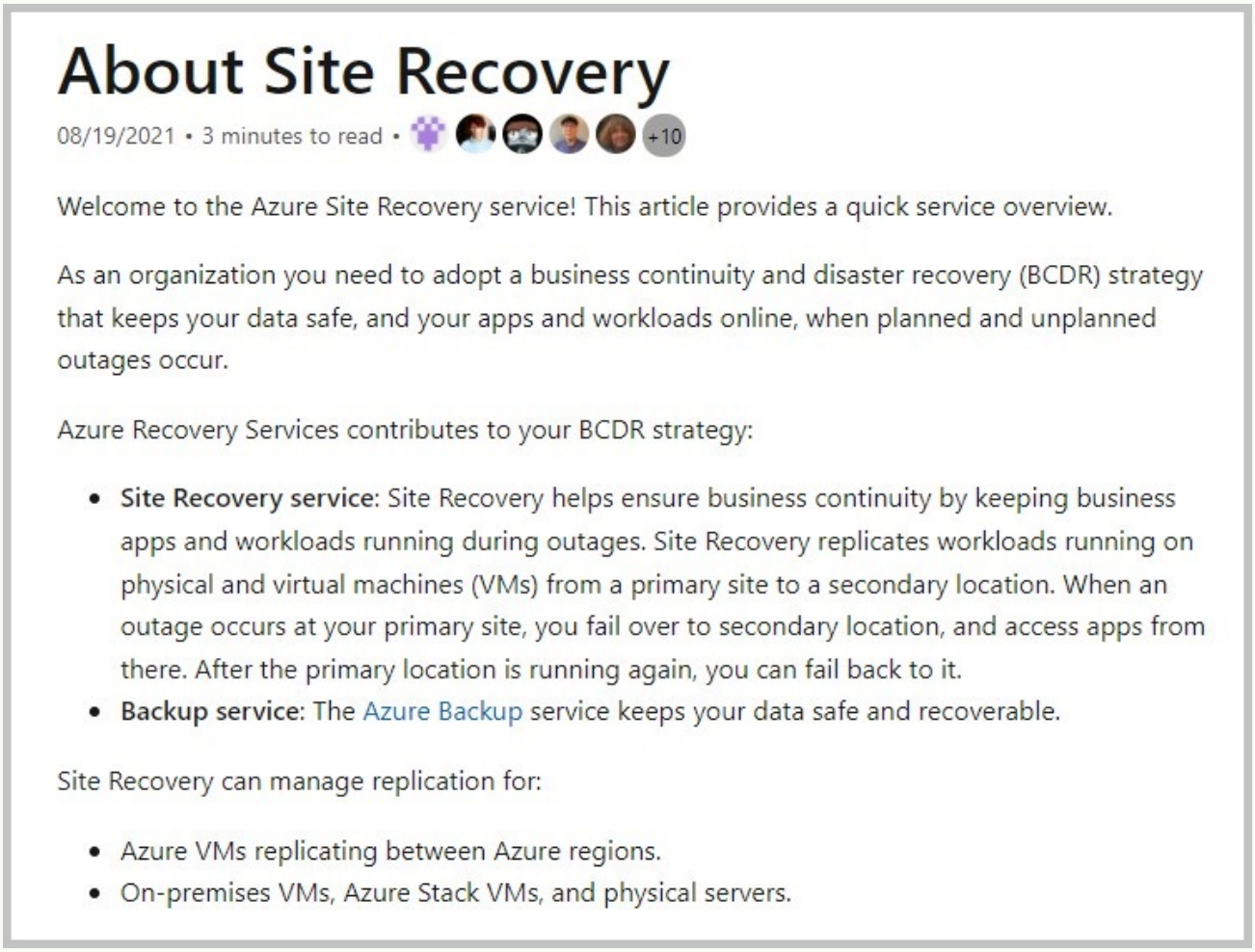
Correct

To ensure that the virtual machines remain available during the migration, use Azure Site Recovery otherwise you can use Azure Migrate.

Reference:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-hyper-v#replicate-hyper-v-vms



About Site Recovery

08/19/2021 • 3 minutes to read • +10

Welcome to the Azure Site Recovery service! This article provides a quick service overview.

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads online, when planned and unplanned outages occur.

Azure Recovery Services contributes to your BCDR strategy:

- **Site Recovery service**: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- **Backup service**: The Azure Backup service keeps your data safe and recoverable.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs, and physical servers.

17. Question

You plan to archive 10 TB of on-premises data files to Azure.

You need to recommend a data archival solution. The solution must minimize the cost of storing the data files.

Which Azure Storage account type should you include in the recommendation?

- A. Standard StorageV2 (general purpose v2)
- B. Standard Storage (general purpose v1)
- C. Premium StorageV2 (general purpose v2)
- D. Premium Storage (general purpose v1)

Incorrect

Standard StorageV2 supports the Archive access tier, which would be the cheapest solution.

Incorrect Answers:

C,D: Each Premium storage account offers 35 TB of disk and 10 TB of snapshot capacity

Reference:

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

Introduction to the core Azure Storage services

04/08/2020 • 11 minutes to read • +24

The Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Core storage services offer a massively scalable object store for data objects, disk storage for Azure virtual machines (VMs), a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store. The services are:

- **Durable and highly available.** Redundancy ensures that your data is safe in the event of transient hardware failures. You can also opt to replicate data across datacenters or geographical regions for additional protection from local catastrophe or natural disaster. Data replicated in this way remains highly available in the event of an unexpected outage.
- **Secure.** All data written to an Azure storage account is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data.
- **Scalable.** Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications.
- **Managed.** Azure handles hardware maintenance, updates, and critical issues for you.
- **Accessible.** Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides client libraries for Azure Storage in a variety of languages, including .NET, Java, Node.js, Python, PHP, Ruby, Go, and others, as well as a mature REST API. Azure Storage supports scripting in Azure PowerShell or Azure CLI. And the Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data.

18. Question

You are designing a microservices architecture that will support a web application.

The solution must meet the following requirements:

? Allow independent upgrades to each microservice.

? Deploy the solution on-premises and to Azure.

? Set policies for performing automatic repairs to the microservices.

? Support low-latency and hyper-scale operations.

You need to recommend a technology.

- A. Azure Container Instance
- B. Azure Virtual Machine Scale Set
- C. Azure Service Fabric

D. Azure Logic App

Correct

Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers. Service Fabric also addresses the significant challenges in developing and managing cloud native applications.

A key differentiator of Service Fabric is its strong focus on building stateful services. You can use the Service Fabric programming model or run containerized stateful services written in any language or code. You can create Service Fabric clusters anywhere, including Windows Server and Linux on premises and other public clouds, in addition to Azure.

You can use Azure Service Fabric to create Service Fabric clusters on any virtual machines or computers running Windows Server.

Incorrect Answers:

A. Azure Container Instance

Azure Container Instances offers the fastest and simplest way to run a container in Azure, without having to manage any virtual machines and without having to adopt a higher-level service.

B. 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.

D. Azure Logic App

Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems.

Reference:

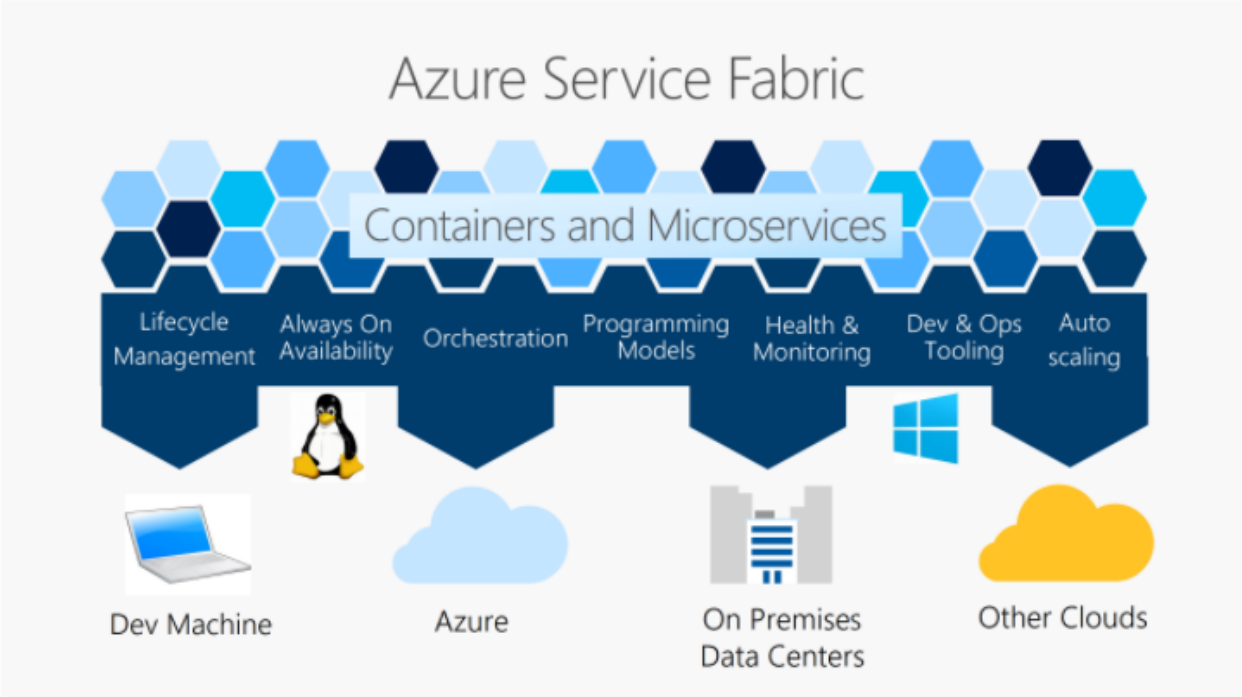
https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview

Overview of Azure Service Fabric

09/22/2020 • 2 minutes to read • +17

Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers. Service Fabric also addresses the significant challenges in developing and managing cloud native applications.

A key differentiator of Service Fabric is its strong focus on building stateful services. You can use the Service Fabric programming model or run containerized stateful services written in any language or code. You can create Service Fabric clusters anywhere, including Windows Server and Linux on premises and other public clouds, in addition to Azure.



Service Fabric powers many Microsoft services today, including Azure SQL Database, Azure Cosmos DB, Cortana, Microsoft Power BI, Microsoft Intune, Azure Event Hubs, Azure IoT Hub, Dynamics 365, Skype for Business, and many core Azure services.

19. Question

You use Azure virtual machines to run a custom application that uses an Azure SQL Database instance on the back end.

The IT department at your company recently enabled forced tunneling.

Since the configuration change, developers have noticed degraded performance when they access the database from the Azure virtual machine.

You need to recommend a solution to minimize latency when accessing the database. The solution must minimize costs.

What should you include in the recommendation?

- A. Virtual Network (VNET) service endpoints
- B. Azure virtual machines that run Microsoft SQL Server servers
- C. Azure SQL Database Managed Instance
- D. Always On availability groups

Correct

Any routes in your virtual network that force internet traffic to your on-premises and/or virtual appliances also force Azure service traffic to take the same route as the internet traffic. Service endpoints provide optimal routing for Azure traffic.

Note: Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

Incorrect Answers:

B. Azure virtual machines that run Microsoft SQL Server servers

SQL Server on Azure Virtual Machines enables you to use full versions of SQL Server in the cloud without having to manage any on-premises hardware. SQL Server virtual machines (VMs) also simplify licensing costs when you pay as you go.

C. Azure SQL Database Managed Instance

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service.

D. Always On availability groups

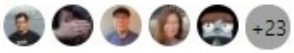
Always On availability groups provide high availability, disaster recovery, and read-scale balancing.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

https://docs.microsoft.com/en-us/azure/app-service/environment/forced-tunnel-support#configure-your-ase-with-service-endpoints

Virtual Network service endpoints

11/08/2019 • 11 minutes to read • 

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

> ⓘ Note
>
> Microsoft recommends use of Azure Private Link for secure and private access to services hosted on Azure platform. For more information, see **Azure Private Link**.

Configure your ASE with Service Endpoints

To route all outbound traffic from your ASE, except that which goes to Azure SQL and Azure Storage, perform the following steps:

1. Create a route table and assign it to your ASE subnet. Find the addresses that match your region here App Service Environment management addresses. Create routes for those addresses with a next hop of internet. These routes are needed because the App Service Environment inbound management traffic must reply from the same address it was sent to.

2. Enable Service Endpoints with Azure SQL and Azure Storage with your ASE subnet. After this step is completed, you can then configure your VNet with forced tunneling.

For details on deploying an ASE with a template, read Creating an App Service Environment using a template.

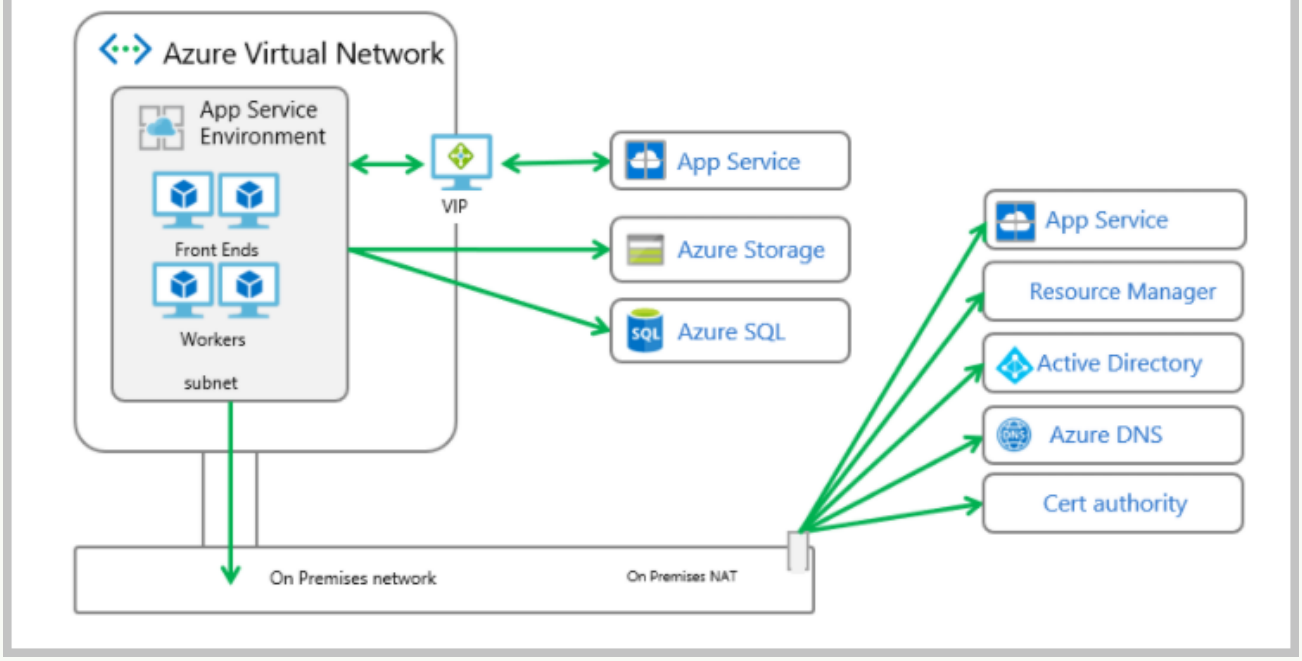
Service Endpoints enable you to restrict access to multi-tenant services to a set of Azure virtual networks and subnets. You can read more about Service Endpoints in the Virtual Network Service Endpoints documentation.

When you enable Service Endpoints on a resource, there are routes created with higher priority than all other routes. If you use Service Endpoints with a forced tunneled ASE, the Azure SQL and Azure Storage management traffic isn't forced tunneled. The other ASE dependency traffic is forced tunneled and can't be lost or the ASE would not function properly.

When Service Endpoints is enabled on a subnet with an Azure SQL instance, all Azure SQL instances connected to from that subnet must have Service Endpoints enabled. if you want to access multiple Azure SQL instances from the same subnet, you can't enable Service Endpoints on one Azure SQL instance and not on another. Azure Storage does not behave the same as Azure SQL. When you enable Service Endpoints with Azure Storage, you lock access to that resource from your subnet but can still access other Azure Storage accounts even if they do not have Service Endpoints enabled.

If you configure forced tunneling with a network filter appliance, then remember that the ASE has

dependencies in addition to Azure SQL and Azure Storage. If traffic is blocked to those dependencies, the ASE will not function properly.



20. Question

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.

You need to use Azure Monitor to design an alerting strategy for security-related events.

Which Azure Monitor Logs tables should you query for events from Windows event logs?

- A. AzureActivity
- B. AzureDiagnostics
- C. Event
- D. Syslog

Correct

Windows Event logs information sent to the Windows event logging system

Incorrect Answers:

A. AzureActivity

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.

B. AzureDiagnostics

Azure Diagnostics extension is an agent in Azure Monitor that collects monitoring data from the guest operating system of Azure compute resources including virtual machines.

D. Syslog

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may

be stored on the local machine or delivered to a Syslog collector.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events#log-queries-with-windows-events

Data collected

The following table lists the types of data you can configure a Log Analytics workspace to collect from all connected agents. See What is monitored by Azure Monitor? for a list of insights, solutions, and other solutions that use the Log Analytics agent to collect other kinds of data.

Data Source	Description
Windows Event logs	Information sent to the Windows event logging system.
Syslog	Information sent to the Linux event logging system.
Performance	Numerical values measuring performance of different aspects of operating system and workloads.
IIS logs	Usage information for IIS web sites running on the guest operating system.
Custom logs	Events from text files on both Windows and Linux computers.

Data destinations

The Log Analytics agent sends data to a Log Analytics workspace in Azure Monitor. The Windows agent can be multihomed to send data to multiple workspaces and System Center Operations Manager management groups. The Linux agent can send to only a single destination, either a workspace or management group.

Log queries with Windows Events

The following table provides different examples of log queries that retrieve Windows Event records.

Query	Description
Event	All Windows events.
Event | where EventLevelName == "error"	All Windows events with severity of error.
Event | summarize count() by Source	Count of Windows events by source.
Event | where EventLevelName == "error" | summarize count() by Source	Count of Windows error events by source.

21. Question

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.

You need to use Azure Monitor to design an alerting strategy for security-related events.

Which Azure Monitor Logs tables should you query for events from Linux system logging?

- A. AzureActivity
- B. AzureDiagnostics
- C. Event
- D. Syslog

Correct

Syslog information sent to the Linux event logging system.

Incorrect Answers:

A. AzureActivity

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.

B. AzureDiagnostics

Azure Diagnostics extension is an agent in Azure Monitor that collects monitoring data from the guest operating system of Azure compute resources including virtual machines.

C. Event

Windows Event logs information sent to the Windows event logging system.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-syslog

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent#data-collected

Data collected

The following table lists the types of data you can configure a Log Analytics workspace to collect from all connected agents. See What is monitored by Azure Monitor? for a list of insights, solutions, and other solutions that use the Log Analytics agent to collect other kinds of data.

Data Source	Description
Windows Event logs	Information sent to the Windows event logging system.
Syslog	Information sent to the Linux event logging system.
Performance	Numerical values measuring performance of different aspects of operating system and workloads.
IIS logs	Usage information for IIS web sites running on the guest operating system.
Custom logs	Events from text files on both Windows and Linux computers.

Data destinations

The Log Analytics agent sends data to a Log Analytics workspace in Azure Monitor. The Windows agent can be multihomed to send data to multiple workspaces and System Center Operations Manager management groups. The Linux agent can send to only a single destination, either a workspace or management group.

Log queries with Syslog records

The following table provides different examples of log queries that retrieve Syslog records.

Query	Description
Syslog	All Syslogs.
Syslog | where SeverityLevel == "error"	All Syslog records with severity of error.
Syslog | summarize AggregatedValue = count() by Computer	Count of Syslog records by computer.
Syslog | summarize AggregatedValue = count() by Facility	Count of Syslog records by facility.

22. Question

You are designing a container solution in Azure that will include two containers. One container will host a web API that will be available to the public. The other container will perform health monitoring of the web API and will remain private. The two containers will be deployed together as a group.

You need to recommend a compute service for the containers. The solution must minimize costs and maintenance overhead.

What should you include in the recommendation?

- A. Azure Service Fabric
- B. Azure Kubernetes Service (AKS)
- C. Azure Container Instances
- D. Azure Container registries

Incorrect

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Incorrect Answers:

A. Azure Service Fabric

Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers.

B. 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.

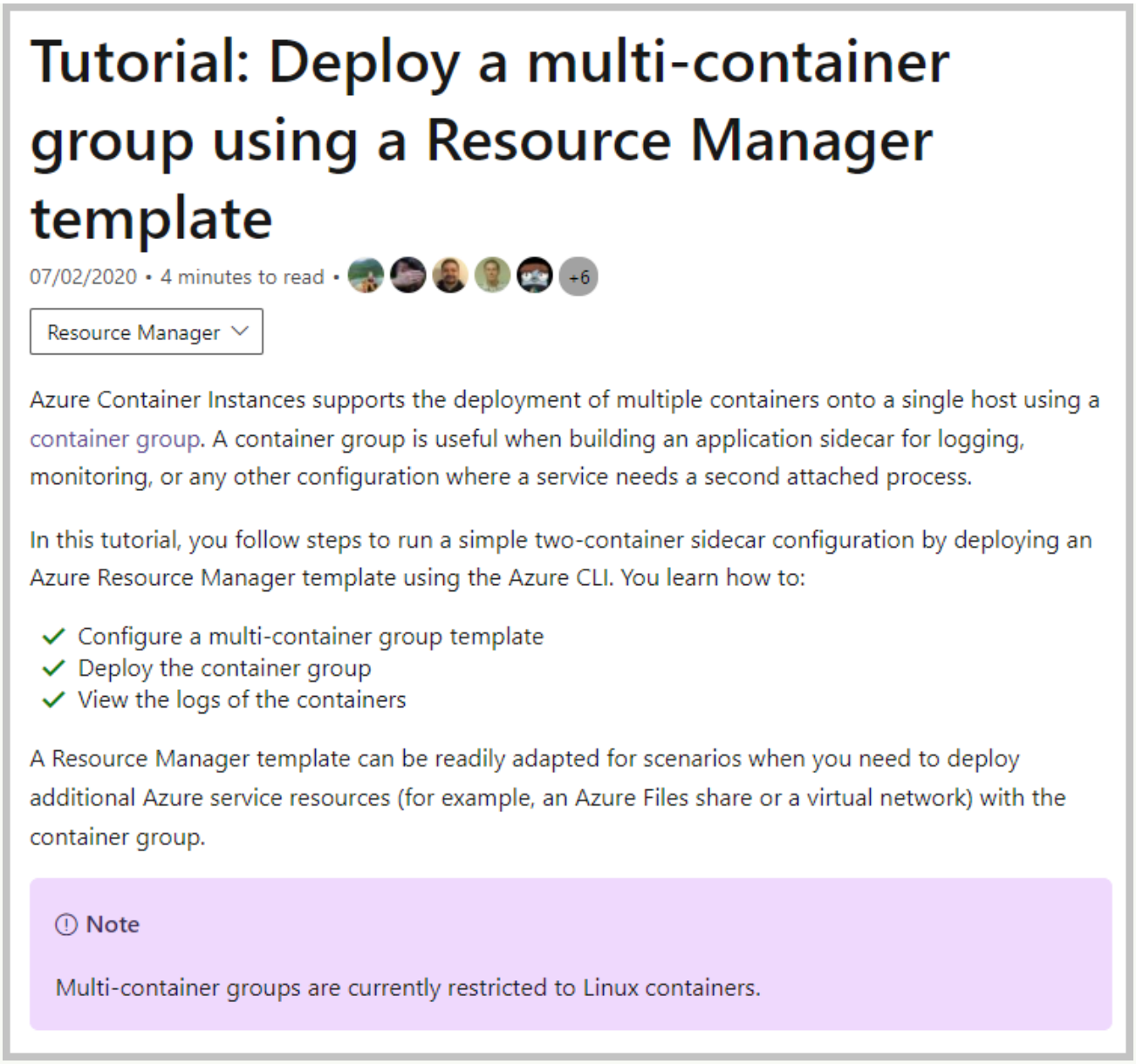
D. Azure Container registries

Azure Container Registry provides storage of private Docker container images, enabling fast, scalable retrieval, and network-close deployment of container workloads on Azure.

Reference:

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-multi-container-group

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups



Tutorial: Deploy a multi-container group using a Resource Manager template

07/02/2020 • 4 minutes to read • +6

Resource Manager

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

In this tutorial, you follow steps to run a simple two-container sidecar configuration by deploying an Azure Resource Manager template using the Azure CLI. You learn how to:

- ✓ Configure a multi-container group template
- ✓ Deploy the container group
- ✓ View the logs of the containers

A Resource Manager template can be readily adapted for scenarios when you need to deploy additional Azure service resources (for example, an Azure Files share or a virtual network) with the container group.

ⓘ Note

Multi-container groups are currently restricted to Linux containers.

23. Question

You plan to deploy an Azure App Service web app that will have multiple instances across multiple Azure regions.

You need to recommend a load balancing service for the planned deployment. The solution must meet the following requirements:

? Maintain access to the app in the event of a regional outage.

? Support Azure Web Application Firewall (WAF).

? Support cookie-based affinity.

? Support URL routing.

What should you include in the recommendation?

- A. Azure Front Door
- B. Azure Load Balancer
- C. Azure Traffic Manager

D. Azure Application Gateway

Correct

Front Door is an application delivery network that provides global load balancing and site acceleration service for web applications. It offers Layer 7 capabilities for your application like SSL offload, path-based routing, fast failover, caching, etc. to improve performance and high-availability of your applications.

Incorrect Answers:

B. Azure Load Balancer

Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. It is a regional load balancing service.

C. Azure Traffic Manager

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 support URL routing.

D. Azure Application Gateway

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

Reference:

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

https://microsoft.github.io/AzureTipsAndTricks/blog/tip192.html

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

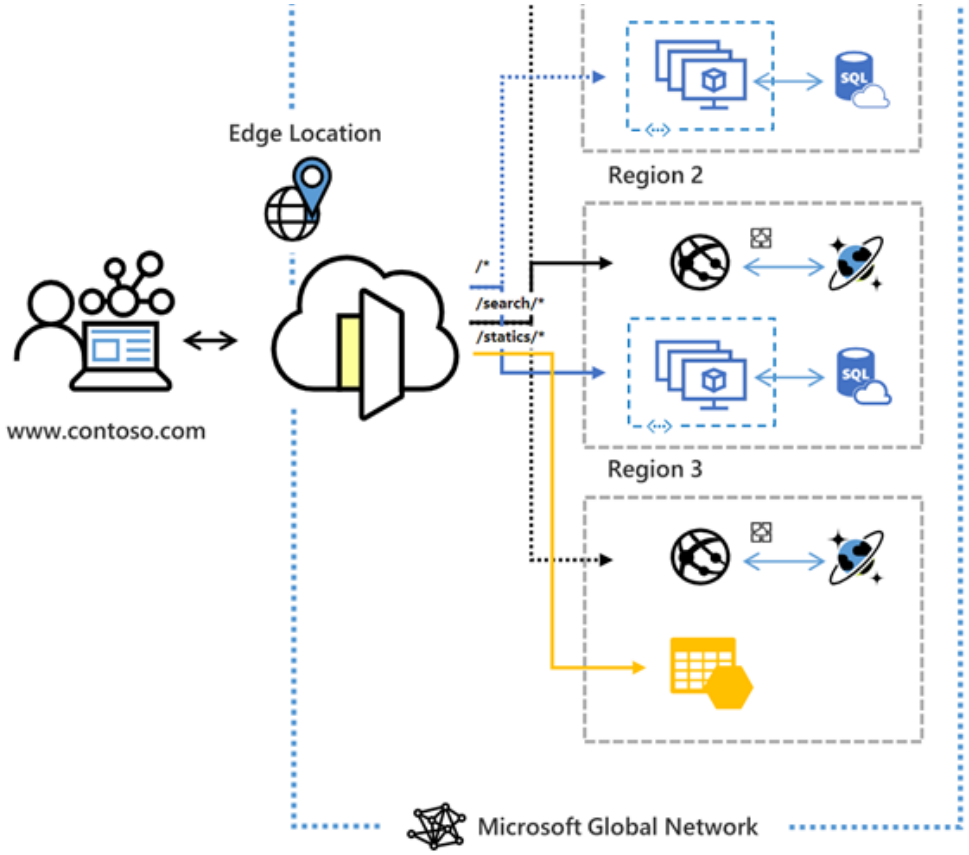
What is Azure Front Door?

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.



Front Door works at Layer 7 (HTTP/HTTPS layer) using anycast protocol with split TCP and Microsoft's global network to improve global connectivity. Based on your routing method you can ensure that Front Door will route your client requests to the fastest and most available application backend. An application backend is any Internet-facing service hosted inside or outside of Azure. Front Door provides a range of traffic-routing methods and backend health monitoring options to suit different application needs and automatic failover scenarios. Similar to Traffic Manager, Front Door is resilient to failures, including failures to an entire Azure region.

Azure load balancing services

Here are the main load-balancing services currently available in Azure:

Front Door is an application delivery network that provides global load balancing and site acceleration service for web applications. It offers Layer 7 capabilities for your application like SSL offload, path-based routing, fast failover, caching, etc. to improve performance and high-availability of your applications.

Note

At this time, Azure Front Door does not support Web Sockets.

Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Because Traffic Manager is a DNS-based load-balancing service, it load balances only at the domain level. For that reason, it can't fail over as quickly as Front Door, because of common challenges around DNS caching and systems not honoring DNS TTLs.

Application Gateway provides application delivery controller (ADC) as a service, offering various Layer 7 load-balancing capabilities. Use it to optimize web farm productivity by offloading CPU-intensive SSL termination to the gateway.

Azure Load Balancer is a high-performance, ultra low-latency Layer 4 load-balancing service (inbound and outbound) for all UDP and TCP protocols. It is built to handle millions of requests per second while ensuring your solution is highly available. Azure Load Balancer is zone-redundant, ensuring high availability across Availability Zones.

24. Question

Your company plans to publish APIs for its services by using Azure API Management.

You discover that service responses include the AspNet-Version header.

You need to recommend a solution to remove AspNet-Version from the response of the published APIs.

What should you include in the recommendation?

- A. a new product
- B. a modification to the URL scheme
- C. a new policy

Correct

Set a new transformation policy to transform an API to strip response headers.

API Management (APIM) is a way to create consistent and modern API gateways for existing back-end services. API Management helps organizations publish APIs to external, partner, and internal developers

to unlock the potential of their data and services.

The API gateway is the endpoint that:

? Accepts API calls and routes them to your backends.

? Verifies API keys, JWT tokens, certificates, and other credentials.

? Enforces usage quotas and rate limits.

? Transforms your API on the fly without code modifications.

? Caches backend responses where set up.

? Logs call metadata for analytics purposes.

Incorrect Answers:

A. a new product

Products in API Management have one or more APIs, and are configured with a title, description, and terms of use.

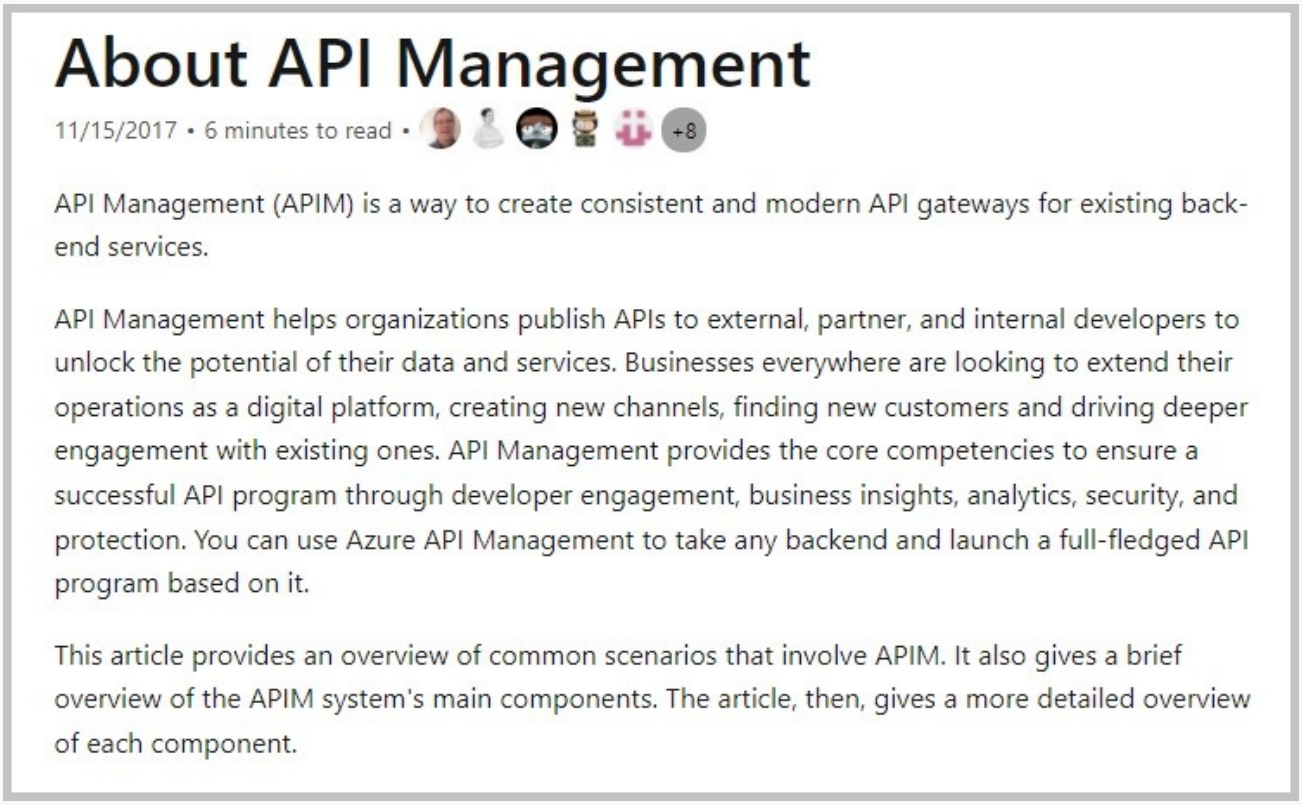
B. a modification to the URL scheme

This option lets you configure which protocols can access API.

Reference:

https://docs.microsoft.com/en-us/azure/api-management/transform-api#transform-an-api-to-strip-response-headers

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



About API Management

11/15/2017 • 6 minutes to read • +8

API Management (APIM) is a way to create consistent and modern API gateways for existing back-end services.

API Management helps organizations publish APIs to external, partner, and internal developers to unlock the potential of their data and services. Businesses everywhere are looking to extend their operations as a digital platform, creating new channels, finding new customers and driving deeper engagement with existing ones. API Management provides the core competencies to ensure a successful API program through developer engagement, business insights, analytics, security, and protection. You can use Azure API Management to take any backend and launch a full-fledged API program based on it.

This article provides an overview of common scenarios that involve APIM. It also gives a brief overview of the APIM system's main components. The article, then, gives a more detailed overview of each component.

Transform an API to strip response headers

This section shows how to hide the HTTP headers that you don't want to show to your users. This example shows how to delete the following headers in the HTTP response:

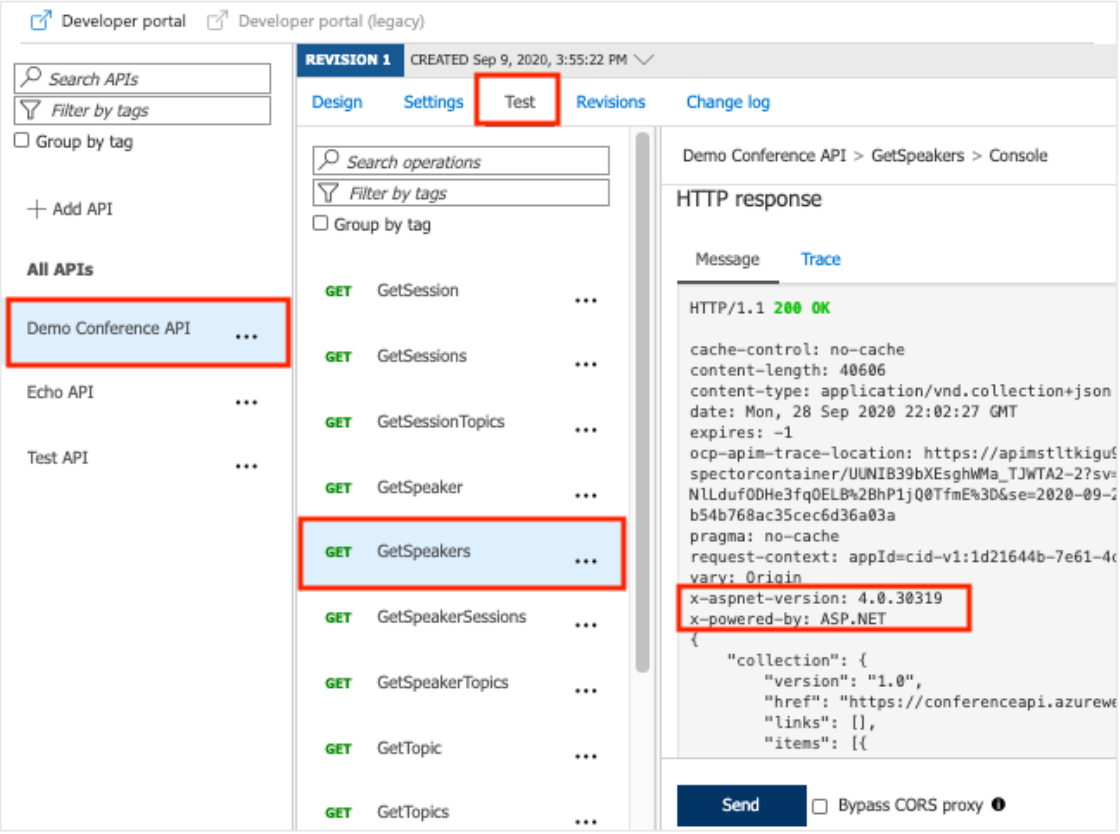
- X-Powered-By
- X-AspNet-Version

Test the original response

To see the original response:

1. In your API Management service instance, select **APIs**.
2. Select **Demo Conference API** from your API list.
3. Select the **Test** tab, on the top of the screen.
4. Select the **GetSpeakers** operation and select **Send**.

The original response should look similar to the following:



As you can see, the response includes the **X-AspNet-Version** and **X-Powered-By** headers.

25. Question

You have an Azure subscription named Subscription1 that is linked to a hybrid Azure Active Directory (Azure AD) tenant.

You have an on-premises datacenter that does NOT have a VPN connection to Subscription1. The

datacenter contains a computer named Server1 that has
Microsoft SQL Server 2016 installed. Server1 is prevented from accessing the internet.
An Azure logic app named LogicApp1 requires write access to a database on Server1.
You need to recommend a solution to provide LogicApp1 with the ability to access Server1.
What should you recommend deploying on-premises?

- A. A Web Application Proxy for Windows Server
- B. An Azure AD Application Proxy connector
- C. An On-premises data gateway
- D. Hybrid Connection Manager

Incorrect

Before you can connect to on-premises data sources from Azure Logic Apps, download and install the on-premises data gateway on a local computer. The gateway works as a bridge that provides quick data transfer and encryption between data sources on premises and your logic apps.
The on-premises data gateway depends on Azure Service Bus Messaging for cloud connectivity and establishes the corresponding outbound connections to the gateway's associated Azure region.
Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-connection
https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-install
https://docs.microsoft.com/en-us/azure/connectors/connectors-create-api-sqlazure

Install on-premises data gateway for Azure Logic Apps

03/16/2021 • 13 minutes to read • 

Before you can connect to on-premises data sources from Azure Logic Apps, download and install the on-premises data gateway on a local computer. The gateway works as a bridge that provides quick data transfer and encryption between data sources on premises and your logic apps. You can use the same gateway installation with other cloud services, such as Power Automate, Power BI, Power Apps, and Azure Analysis Services. For information about how to use the gateway with these services, see these articles:

- Microsoft Power Automate on-premises data gateway
- Microsoft Power BI on-premises data gateway
- Microsoft Power Apps on-premises data gateway
- Azure Analysis Services on-premises data gateway

This article shows how to download, install, and set up your on-premises data gateway so that you can access on-premises data sources from Azure Logic Apps. You can also learn more about how the data gateway works later in this topic. For more information about the gateway, see What is an on-premises gateway? To automate gateway installation and management tasks, visit the PowerShell gallery for the DataGateway PowerShell cmdlets.

Connect to on-premises data sources from Azure Logic Apps

07/14/2021 • 8 minutes to read • 

After you install the *on-premises data gateway* on a local computer and before you can access data sources on premises from your logic apps, you have to create a gateway resource in Azure for your gateway installation. You can then select this gateway resource in the triggers and actions that you want to use for the on-premises connectors available in Azure Logic Apps. Azure Logic Apps supports read and write operations through the data gateway. However, these operations have limits on their payload size.

This article shows how to create your Azure gateway resource for a previously installed gateway on your local computer. For more information about the gateway, see How the gateway works.

Tip

To directly access on-premises resources in Azure virtual networks without having to use the gateway, consider creating an ***integration service environment*** instead.

26. Question

You have an Azure subscription named Subscription1 that is linked to a hybrid Azure Active Directory (Azure AD) tenant.

You have an on-premises datacenter that does NOT have a VPN connection to Subscription1. The datacenter contains a computer named Server1 that has

Microsoft SQL Server 2016 installed. Server1 is prevented from accessing the internet.

An Azure logic app named LogicApp1 requires write access to a database on Server1.

You need to recommend a solution to provide LogicApp1 with the ability to access Server1.

What should you recommend deploying in Azure?

- A. A connection gateway resource
- B. An Azure Application Gateway
- C. An Azure Event Grid domain
- D. An enterprise application

Incorrect

Before you can connect to on-premises data sources from Azure Logic Apps, download and install the on-premises data gateway on a local computer. The gateway works as a bridge that provides quick data transfer and encryption between data sources on premises and your logic apps.

The on-premises data gateway depends on Azure Service Bus Messaging for cloud connectivity and establishes the corresponding outbound connections to the gateway‘s associated Azure region.

Reference:

https://docs.microsoft.com/en-us/azure/connectors/connectors-create-api-sqlazure

https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-connection

Connect to on-premises SQL Server

The first time that you add either a SQL trigger or SQL action, and you haven't previously created a connection to your database, you're prompted to complete these steps:

1. For connections to your on-premises SQL server that require the on-premises data gateway, make sure that you've completed these prerequisites.

   Otherwise, your data gateway resource won't appear in the **Connection Gateway** list when you create your connection.

2. For **Authentication Type**, select the authentication that's required and enabled on your SQL Server:

Authentication	Description
Windows Authentication	- Supports only the non-ISE SQL Server connector, which requires a data gateway resource that's previously created in Azure for your connection, regardless whether you use multi-tenant Azure or an ISE. - Requires a valid Windows user name and password to confirm your identity through your Windows account. For more information, see Windows Authentication
SQL Server Authentication	- Supports both the non-ISE and ISE SQL Server connector. - Requires a valid user name and strong password that are created and stored in your SQL Server. For more information, see SQL Server Authentication.

3. Select or provide the following values for your SQL database:

Property	Required	Description
SQL server name	Yes	The address for your SQL server, for example, `Fabrikam-Azure-SQL.database.windows.net`
SQL database name	Yes	The name for your SQL Server database, for example, `Fabrikam-Azure-SQL-DB`
Username	Yes	Your user name for the SQL server and database
Password	Yes	Your password for the SQL server and database
Subscription	Yes, for Windows authentication	The Azure subscription for the data gateway resource that you previously created in Azure
Connection Gateway	Yes, for Windows authentication	The name for the data gateway resource that you previously created in Azure **Tip:** If your gateway doesn't appear in the list, check that you correctly set up your gateway.

27. Question

You manage an application instance. The application consumes data from multiple databases. Application code references database tables using a combination of the server, database, and table name.

You need to migrate the application data to Azure.

To which two Azure services could you migrate the application to achieve the goal?

- [x] A. Azure SQL Managed Instance
- [ ] B. Azure SQL Database
- [x] C. SQL Server in an Azure virtual machine
- [ ] D. SQL Server Stretch Database

Correct

The managed instance deployment model is designed for customers looking to migrate a large number of apps from on-premises or IaaS, self-built, or ISV provided environment to fully managed PaaS cloud environment, with as low migration effort as possible. Using the fully automated Data Migration Service (DMS) in Azure, customers can lift and shift their on-premises SQL Server to a managed instance that offers compatibility with SQL Server on-premises and complete isolation of customer instances with native VNet support.

Both SQL Server on Azure VM and SQL Managed Instance support s cross-database queries wherein

server.dbName.tableName is used

Incorrect Answers:

B. Azure SQL Database

The elastic query feature (in preview) enables you to run a Transact-SQL query that spans multiple databases in Azure SQL Database. This feature is still in preview.

D. SQL Server Stretch Database

Stretch Database migrates your cold data transparently and securely to the Microsoft Azure cloud.

Reference:

https://docs.microsoft.com/en-us/sql/relational-databases/linked-servers/linked-servers-database-engine?view=sql-server-ver15

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance

What is Azure SQL Managed Instance?

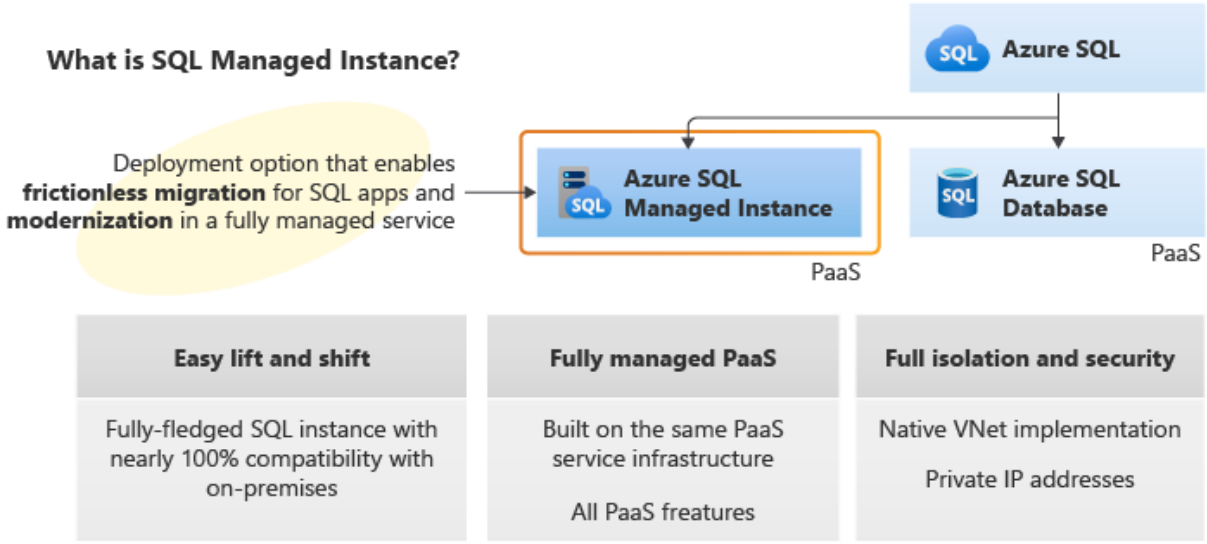
01/14/2021 • 15 minutes to read • +10

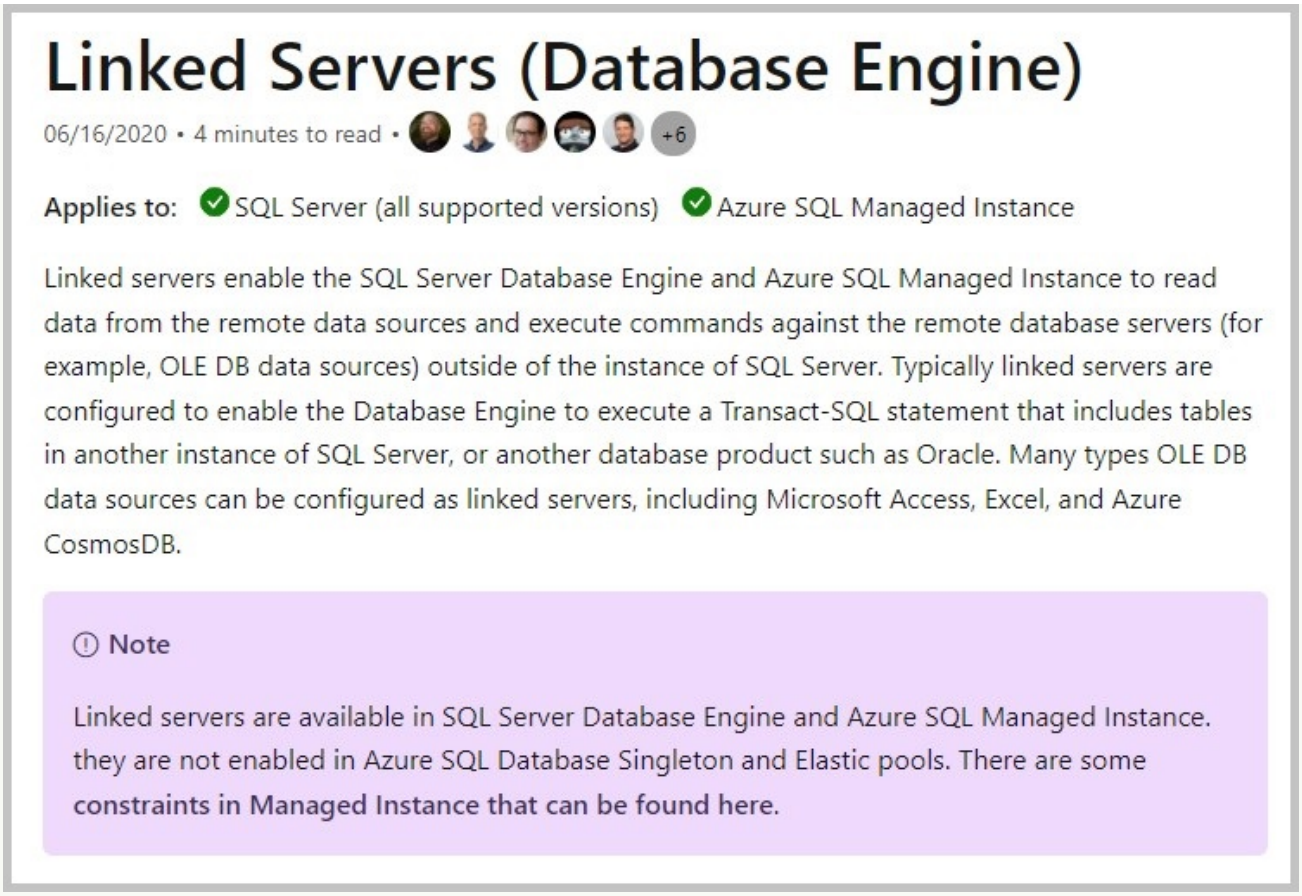
APPLIES TO: Azure SQL Managed Instance

Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

> **Important**
>
> For a list of regions where SQL Managed Instance is currently available, see **Supported regions**.

The following diagram outlines key features of SQL Managed Instance:





Linked Servers (Database Engine)

06/16/2020 • 4 minutes to read • +6

Applies to: SQL Server (all supported versions) Azure SQL Managed Instance

Linked servers enable the SQL Server Database Engine and Azure SQL Managed Instance to read data from the remote data sources and execute commands against the remote database servers (for example, OLE DB data sources) outside of the instance of SQL Server. Typically linked servers are configured to enable the Database Engine to execute a Transact-SQL statement that includes tables in another instance of SQL Server, or another database product such as Oracle. Many types OLE DB data sources can be configured as linked servers, including Microsoft Access, Excel, and Azure CosmosDB.

Note

Linked servers are available in SQL Server Database Engine and Azure SQL Managed Instance. they are not enabled in Azure SQL Database Singleton and Elastic pools. There are some **constraints in Managed Instance that can be found here.**

28. Question

You manage an on-premises network and Azure virtual networks.

You need to create a secure connection over a private network between the on-premises network and the Azure virtual networks. The connection must offer a redundant pair of cross connections to provide high availability.

What should you recommend?

- A. Azure Load Balancer
- B. VPN Gateway
- C. ExpressRoute
- D. virtual network peering

Incorrect

Each ExpressRoute circuit consists of two connections to two Microsoft Enterprise edge routers (MSEEs) at an ExpressRoute Location from the connectivity provider/your network edge. Microsoft requires dual BGP connection from the connectivity provider/your network edge one to each MSEE. You may choose not to deploy redundant devices/Ethernet circuits at your end. However, connectivity providers use redundant devices to ensure that your connections are handed off to Microsoft in a redundant manner.

Incorrect Answers:

A. Azure Load Balancer

This is a load balancing solution.

B. VPN Gateway

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.

D. virtual network peering

It establishes connectivity between two virtual networks.

Reference:

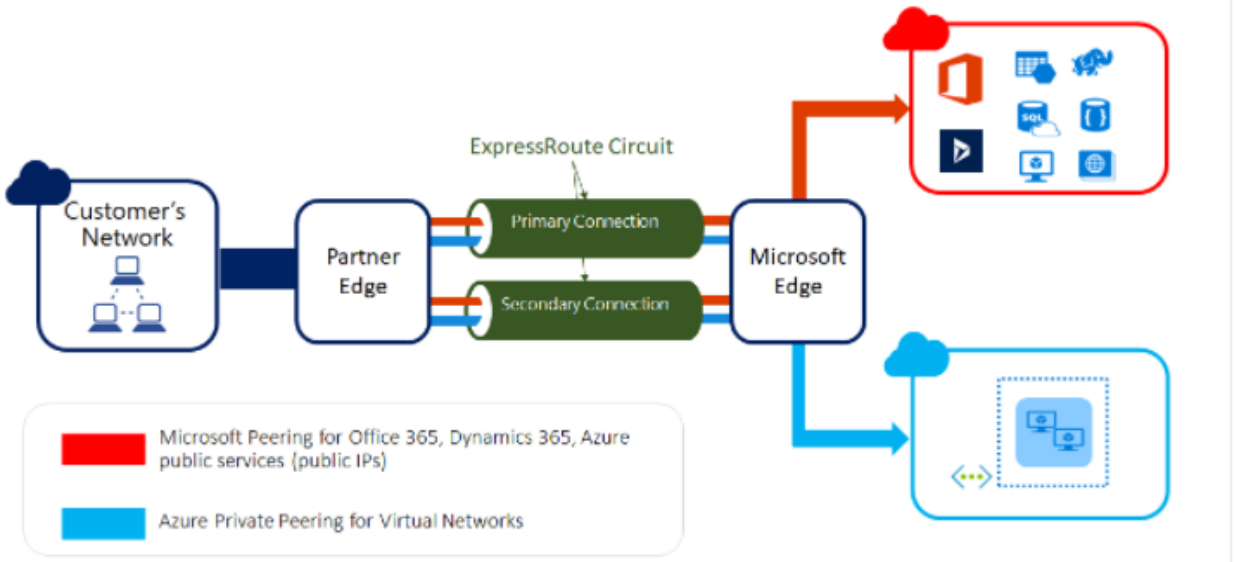
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction#redundancy

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.

29. 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 are evaluating the components of the migration to Azure that require you to provision an Azure Storage account.

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

You must provision an Azure Storage account for the SQL Server database migration

- A. Yes
- B. No

Correct

You can use the Database Migration service to carry out an online migration. Here you don t need to have a storage account.

Reference:

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

https://azure.microsoft.com/en-au/services/sql-server-stretch-database/

30. 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 are evaluating the components of the migration to Azure that require you to provision an Azure Storage account.

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

You must provision an Azure Storage account for the Web site content storage

- A. Yes
- B. No

Correct

You can migrate the web site content as it, and you don t need a separate storage account for this.

Reference:

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

31. 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 are evaluating the components of the migration to Azure that require you to provision an Azure Storage account.

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

You must provision an Azure Storage account for the Database metric monitoring

- A. Yes
- B. No

Correct

Yes, for enabling diagnostic setting which stores the database metrics, you can choose the data store as a storage account.

Reference:

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

32. 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 the web tier of WebApp1. The solution must minimize costs.

What should you recommend?

- A. Configure the Scale Up settings for a web app
- B. Deploy a virtual machine scale set that scales out on a 75 percent CPU threshold
- C. Create a runbook that resizes virtual machines automatically to a smaller size outside of business hours
- **D. Configure the Scale Out settings for a web app**

Correct

Scenario: Fabrikam, Inc plans to migrate the production and test instances of WebApp1 to Azure and to use the S1 plan.

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

Scaling out number of instances based on load will suffice the requirements.

Incorrect Answers:

A. Configure the Scale Up settings for a web app

Wrong. Scale up would cause disruption since you resizing a live webapp, scale out makes more sense

B. Deploy a virtual machine scale set that scales out on a 75 percent CPU threshold

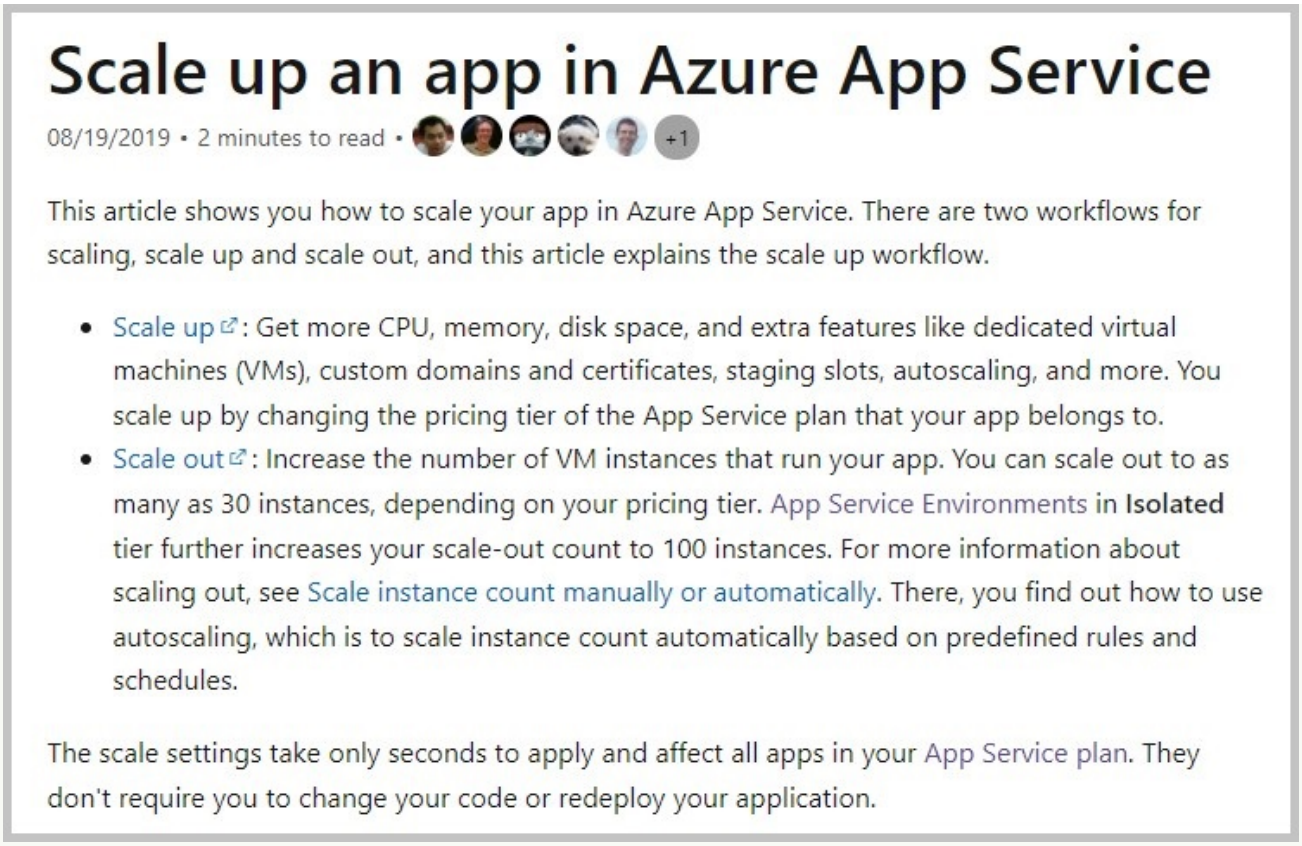
Wrong. Why use a VM scale set for a web app, solution must minimise costs therefore a web app is more cost effective.

C. Create a runbook that resizes virtual machines automatically to a smaller size outside of business hours

Wrong. Un-necessary disruption for not much benefit. True autoscaling would be more cost effective since it can run 24/7

Reference:

https://docs.microsoft.com/en-us/azure/app-service/manage-scale-up



Scale up an app in Azure App Service

08/19/2019 • 2 minutes to read • +1

This article shows you how to scale your app in Azure App Service. There are two workflows for scaling, scale up and scale out, and this article explains the scale up workflow.

- Scale up: Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more. You scale up by changing the pricing tier of the App Service plan that your app belongs to.
- Scale out: Increase the number of VM instances that run your app. You can scale out to as many as 30 instances, depending on your pricing tier. App Service Environments in **Isolated** tier further increases your scale-out count to 100 instances. For more information about scaling out, see Scale instance count manually or automatically. There, you find out how to use autoscaling, which is to scale instance count automatically based on predefined rules and schedules.

The scale settings take only seconds to apply and affect all apps in your App Service plan. They don't require you to change your code or redeploy your application.

33. Question

You have an on-premises database that you plan to migrate to Azure.

You need to design the database architecture to meet the following requirements:

? Support scaling up and down.

? Support geo-redundant backups.

? Support a database of up to 75 TB.

? Be optimized for online transaction processing (OLTP).

What should you include in Service in the design?

- A. Azure SQL Database
- B. Azure SQL Managed Instance
- C. Azure Synapse Analytics
- D. SQL Server on Azure Virtual Machines

Incorrect

Azure SQL Database:

Database size always depends on the underlying service tiers (e.g. Basic, Business Critical, Hyperscale).

It supports databases of up to 100 TB with Hyperscale service tier model.

Active geo-replication is a feature that lets you to create a continuously synchronized readable secondary database for a primary database. The readable secondary database may be in the same Azure region as the primary, or, more commonly, in a different region. This kind of readable secondary databases are also

known as geo-secondaries, or geo-replicas.

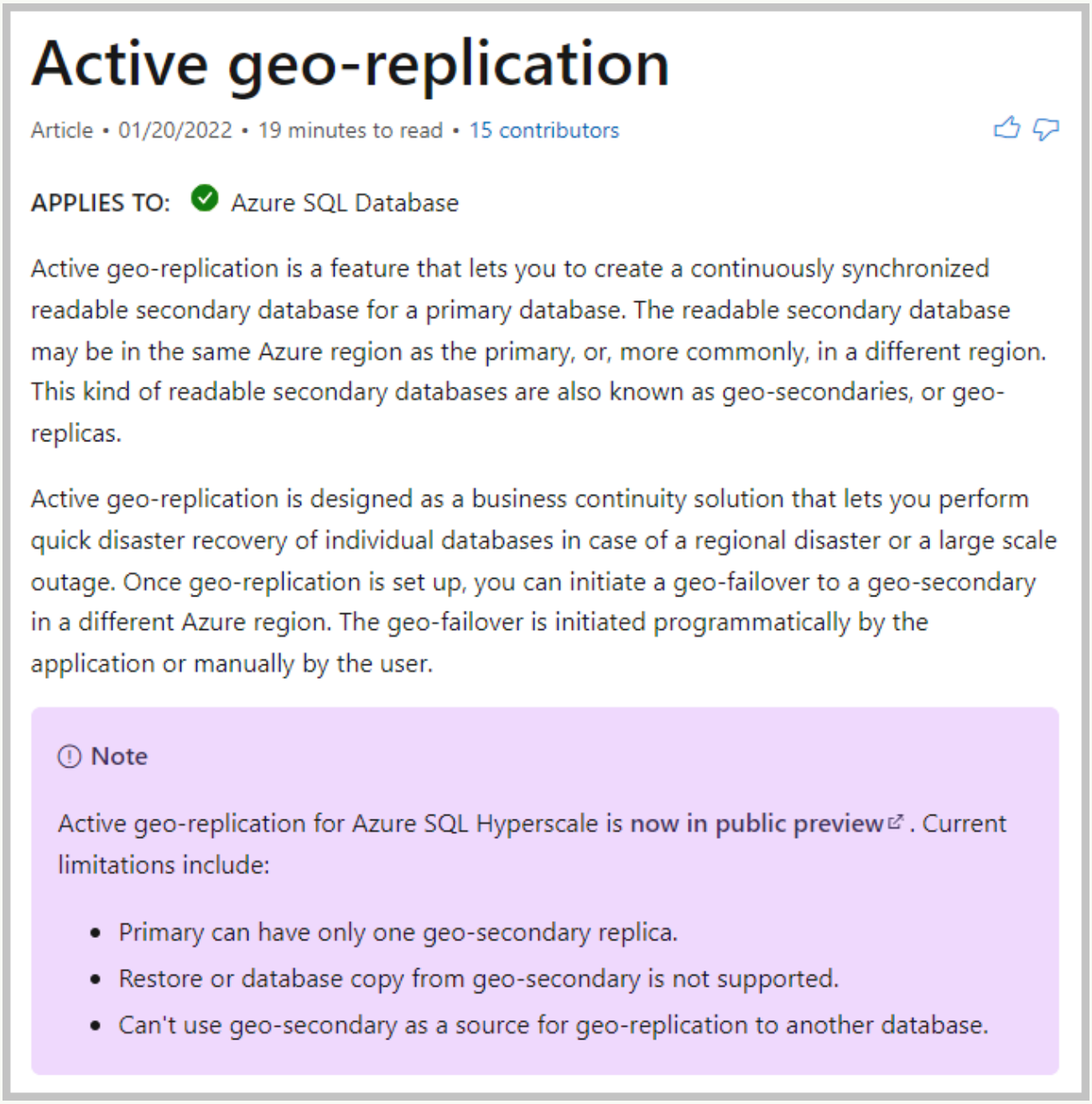
Azure SQL Database and SQL Managed Instance enable you to dynamically add more resources to your database with minimal downtime.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tier-hyperscale

https://medium.com/awesome-azure/azure-difference-between-azure-sql-database-and-sql-server-on-vm-comparison-azure-sql-vs-sql-server-vm-cf02578a1188

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



Active geo-replication

Article • 01/20/2022 • 19 minutes to read • 15 contributors

APPLIES TO: Azure SQL Database

Active geo-replication is a feature that lets you to create a continuously synchronized readable secondary database for a primary database. The readable secondary database may be in the same Azure region as the primary, or, more commonly, in a different region. This kind of readable secondary databases are also known as geo-secondaries, or geo-replicas.

Active geo-replication is designed as a business continuity solution that lets you perform quick disaster recovery of individual databases in case of a regional disaster or a large scale outage. Once geo-replication is set up, you can initiate a geo-failover to a geo-secondary in a different Azure region. The geo-failover is initiated programmatically by the application or manually by the user.

Note

Active geo-replication for Azure SQL Hyperscale is **now in public preview**. Current limitations include:

- Primary can have only one geo-secondary replica.
- Restore or database copy from geo-secondary is not supported.
- Can't use geo-secondary as a source for geo-replication to another database.

34. Question

You have an on-premises database that you plan to migrate to Azure.

You need to design the database architecture to meet the following requirements:

? Support scaling up and down.

? Support geo-redundant backups.

? Support a database of up to 75 TB.

? Be optimized for online transaction processing (OLTP).

What should you include in Service tier in the design?

- A. Basic
- B. Business Critical
- C. General Purpose
- D. Hyperscale
- E. Premium
- F. Standard

Incorrect

Azure SQL Database is based on SQL Server Database Engine architecture that is adjusted for the cloud environment in order to ensure 99.99% availability even in the cases of infrastructure failures. There are three architectural models that are used in Azure SQL Database:

? General Purpose/Standard

? Hyperscale

? Business Critical/Premium

A Hyperscale database is created with a starting size of 10 GB and it starts growing by 10 GB every 10 minutes, until it reaches the size of 40 GB.

For more information about Hyperscale pricing, see Azure SQL Database Pricing

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tier-hyperscale

https://medium.com/awesome-azure/azure-difference-between-azure-sql-database-and-sql-server-on-vm-comparison-azure-sql-vs-sql-server-vm-cf02578a1188

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

Hyperscale service tier

Article • 03/02/2022 • 15 minutes to read • 22 contributors

APPLIES TO: Azure SQL Database

Azure SQL Database is based on SQL Server Database Engine architecture that is adjusted for the cloud environment in order to ensure 99.99% availability even in the cases of infrastructure failures. There are three architectural models that are used in Azure SQL Database:

- General Purpose/Standard
- Hyperscale
- Business Critical/Premium

The Hyperscale service tier in Azure SQL Database is the newest service tier in the vCore-based purchasing model. This service tier is a highly scalable storage and compute performance tier that leverages the Azure architecture to scale out the storage and compute resources for an Azure SQL Database substantially beyond the limits available for the General Purpose and Business Critical service tiers.

Note

- For details on the General Purpose and Business Critical service tiers in the vCore-based purchasing model, see **General Purpose** and **Business Critical** service tiers. For a comparison of the vCore-based purchasing model with the DTU-based purchasing model, see **Azure SQL Database purchasing models and resources.**
- The Hyperscale service tier is currently only available for Azure SQL Database, and not Azure SQL Managed Instance.

35. Question

You are planning an Azure IoT Hub solution that will include 50,000 IoT devices.

Each device will stream data, including temperature, device ID, and time data. Approximately 50,000 records will be written every second. The data will be visualized in near real time.

You need to recommend a service to store and query the data.

Which two services can you recommend?

- [ ] A. Azure Table Storage

B. Azure Event Grid

C. Azure Cosmos DB SQL API

D. Azure Time Series Insights

Incorrect

C: The processed data is stored in an analytical data store, such as Azure Data Explorer, HBase, Azure Cosmos DB, Azure Data Lake, or Blob Storage.

D: Time Series Insights is a fully managed service for time series data. In this architecture, Time Series Insights performs the roles of stream processing, data store, and analytics and reporting. It accepts streaming data from either IoT Hub or Event Hubs and stores, processes, analyzes, and displays the data in near real time.

Note: IoT use cases commonly share some patterns in how they ingest, process, and store data. First, these systems need to ingest bursts of data from device sensors of various locales. Next, these systems process and analyze streaming data to derive real-time insights. The data is then archived to cold storage for batch analytics. Microsoft Azure offers rich services that can be applied for IoT use cases including Azure Cosmos DB, Azure Event Hubs, Azure Stream Analytics, Azure Notification Hub, Azure Machine Learning, Azure HDInsight, and Power BI.

Reference:

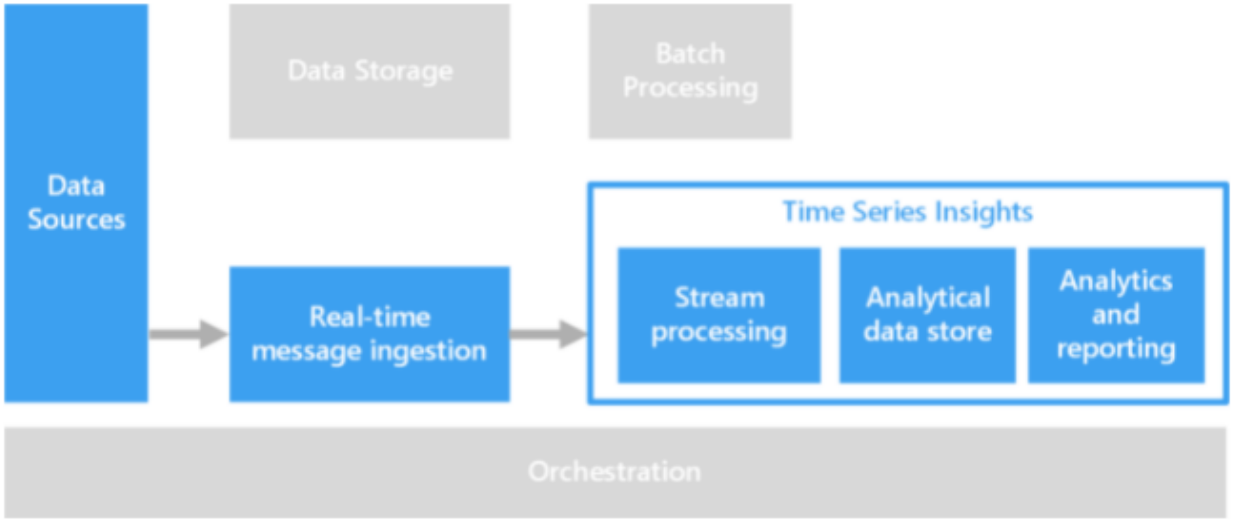
https://docs.microsoft.com/en-us/azure/architecture/data-guide/scenarios/time-series

https://docs.microsoft.com/en-gb/azure/cosmos-db/use-cases#iot-and-telematics

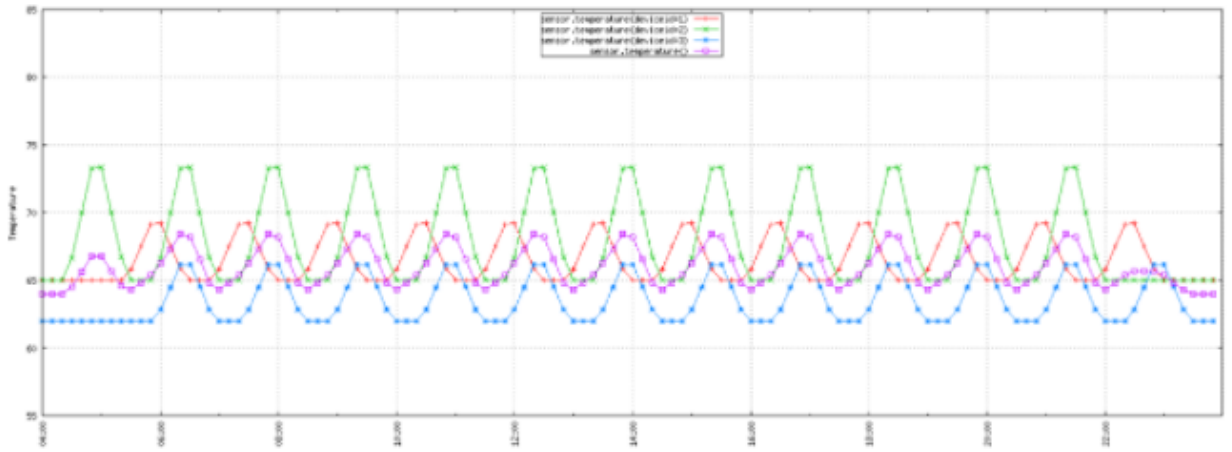
Time series data

IoT Hub | HDInsight | Data Explorer

Time series data is a set of values organized by time. Examples of time series data include sensor data, stock prices, click stream data, and application telemetry. Time series data can be analyzed for historical trends, real-time alerts, or predictive modeling.

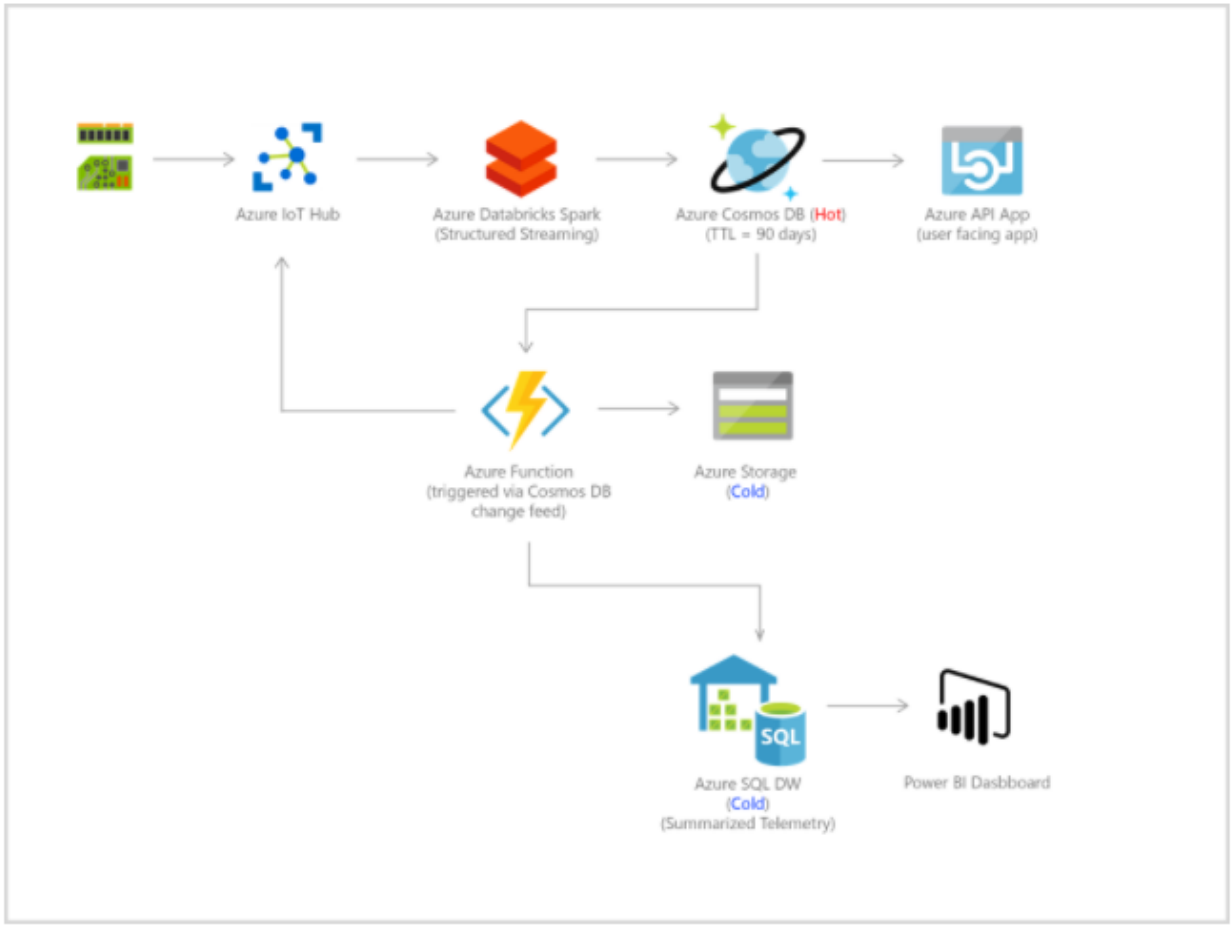


Time series data represents how an asset or process changes over time. The data has a timestamp, but more importantly, time is the most meaningful axis for viewing or analyzing the data. Time series data typically arrives in order of time and is usually treated as an insert rather than an update to your database. Because of this, change is measured over time, enabling you to look backward and to predict future change. As such, time series data is best visualized with scatter or line charts.



IoT and telematics

IoT use cases commonly share some patterns in how they ingest, process, and store data. First, these systems need to ingest bursts of data from device sensors of various locales. Next, these systems process and analyze streaming data to derive real-time insights. The data is then archived to cold storage for batch analytics. Microsoft Azure offers rich services that can be applied for IoT use cases including Azure Cosmos DB, Azure Event Hubs, Azure Stream Analytics, Azure Notification Hub, Azure Machine Learning, Azure HDInsight, and Power BI.

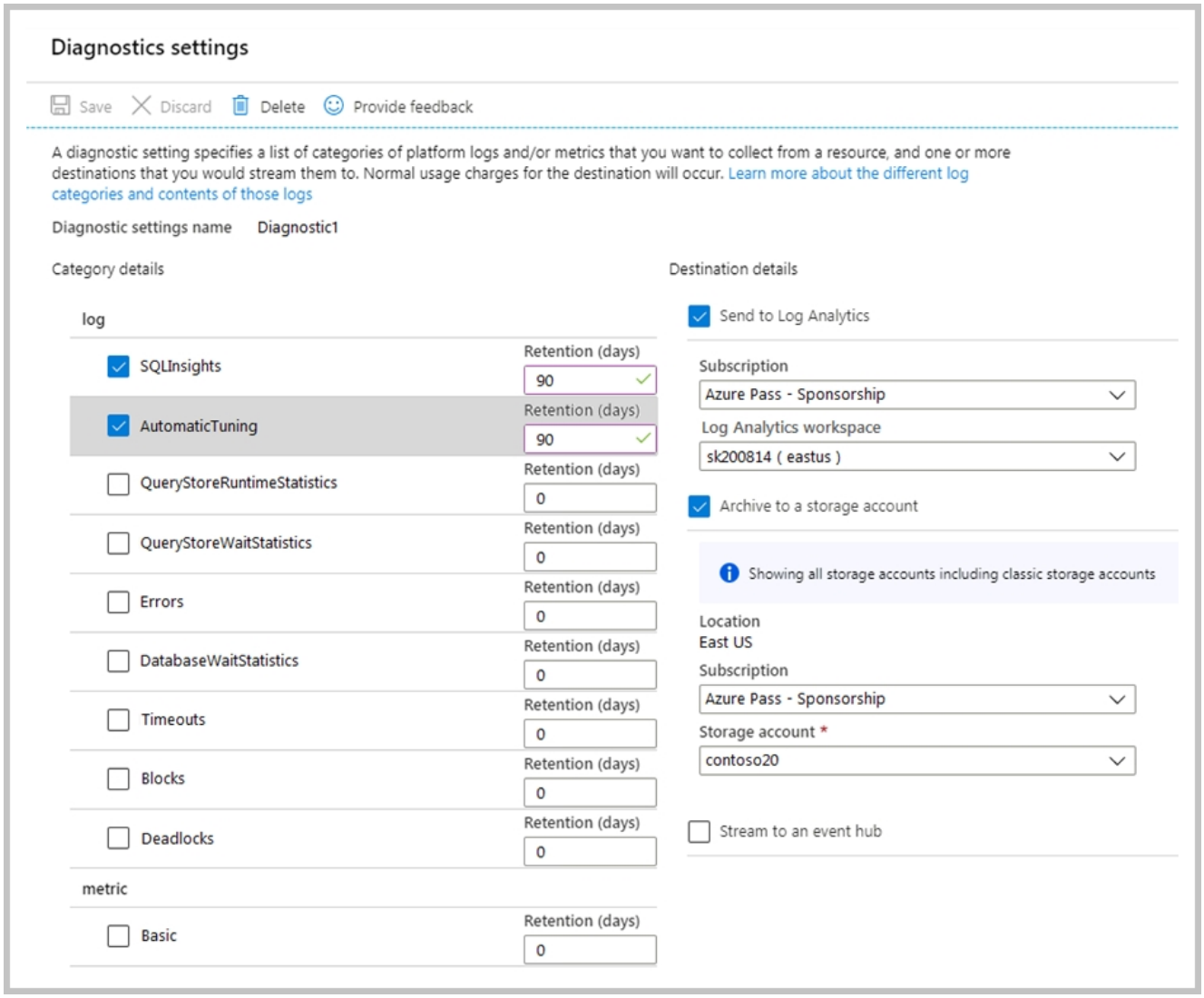


Bursts of data can be ingested by Azure Event Hubs as it offers high throughput data ingestion with low latency. Data ingested that needs to be processed for real-time insight can be funneled to Azure Stream Analytics for real-time analytics. Data can be loaded into Azure Cosmos DB for adhoc querying. Once the data is loaded into Azure Cosmos DB, the data is ready to be queried. In addition, new data and changes to existing data can be read on change feed. Change feed is a persistent, append only log that stores changes to Cosmos containers in sequential order. Then all data or just changes to data in Azure Cosmos DB can be used as reference data as part of real-time analytics. In addition, data can further be refined and processed by connecting Azure Cosmos DB data to HDInsight for Pig, Hive, or Map/Reduce jobs. Refined data is then loaded back to Azure Cosmos DB for reporting.

36. Question

You deploy several Azure SQL Database instances.

You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.



The amount of time that SQLInsights data will be stored in blob storage is .....?

- A. 30 days
- B. 90 days
- C. 730 days
- D. Indefinite

Correct

The amount of time SQL Insight data will be stored in Blob Storage should be 90 days as selected in retention period.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings?WT.mc_id=Portal-Microsoft_Azure_Monitoring

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

06/09/2021 • 11 minutes to read •

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

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

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

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

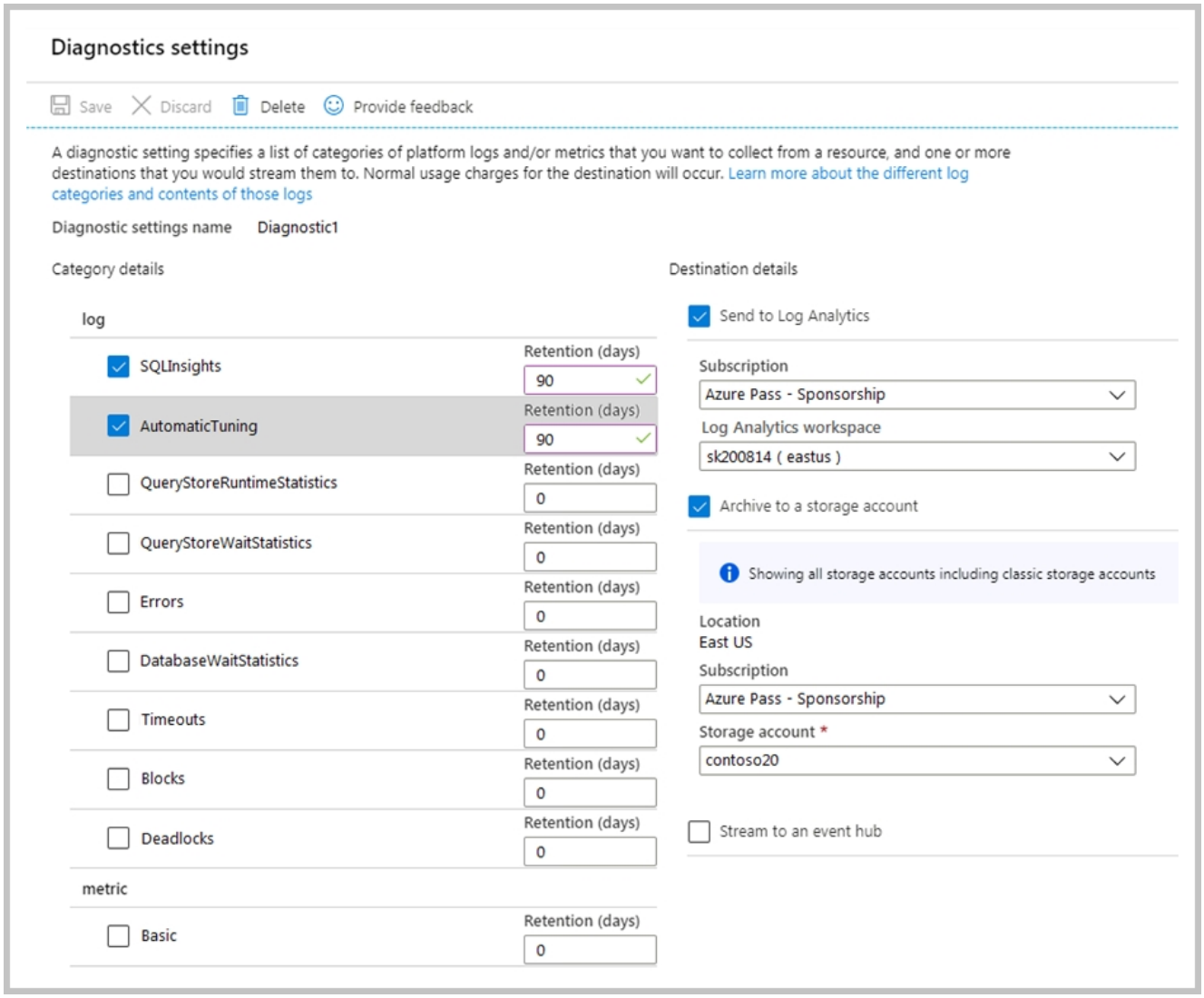
A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings.

> **Tip**
>
> Consider setting the retention policy to 0 and manually deleting your data from storage using a scheduled job to avoid possible confusion in the future.
>
> First, if you are using storage for archiving, you generally want your data around for more than 365 days. Second, if you choose a retention policy that is greater than 0, the expiration date is attached to the logs at the time of storage. You can't change the date for those logs once stored.
>
> For example, if you set the retention policy for *WorkflowRuntime* to 180 days and then 24 hours later set it to 365 days, the logs stored during those first 24 hours will be automatically deleted after 180 days, while all subsequent logs of that type will be automatically deleted after 365 days. Changing the retention policy later doesn't make the first 24 hours of logs stay around for 365 days.

37. Question

You deploy several Azure SQL Database instances.

You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.



The maximum amount of time that SQLInsights data will be stored in Azure Log Analytics is _____?

- A. 30 days
- B. 90 days
- C. 730 days
- D. Indefinite

Incorrect

In the exhibit, the SQLInsights data is configured to be stored in Azure Log Analytics for 90 days.

However, the question is asking for the “maximum“ amount of time that the data can be stored which is 730 days.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/service-limits

Log Analytics workspaces

Data collection volume and retention

Tier	Limit per day	Data retention	Comment
Current Per GB pricing tier (introduced April 2018)	No limit	30 - 730 days	Data retention beyond 31 days is available for additional charges. Learn more about Azure Monitor pricing.
Legacy Free tiers (introduced April 2016)	500 MB	7 days	When your workspace reaches the 500 MB per day limit, data ingestion stops and resumes at the start of the next day. A day is based on UTC. Note that data collected by Azure Security Center is not included in this 500 MB per day limit and will continue to be collected above this limit.
Legacy Standalone Per GB tier (introduced April 2016)	No limit	30 to 730 days	Data retention beyond 31 days is available for additional charges. Learn more about Azure Monitor pricing.
Legacy Per Node (OMS) (introduced April 2016)	No limit	30 to 730 days	Data retention beyond 31 days is available for additional charges. Learn more about Azure Monitor pricing.
Legacy Standard tier	No limit	30 days	Retention can't be adjusted
Legacy Premium tier	No limit	365 days	Retention can't be adjusted

38. Question

Your company uses Microsoft System Center Service Manager on its on-premises network.

You plan to deploy several services to Azure.

You need to recommend a solution to push Azure service health alerts to Service Manager.

What should you include in the recommendation?

- A. IT Service Management Connector (ITSM)
- B. Azure Event Hubs
- C. Azure Notification Hubs
- D. Application Insights Connector

Correct

IT Service Management Connector (ITSMC) allows you to connect Azure to a supported IT Service Management (ITSM) product or service.

ITSMC supports connections with the following ITSM tools:

? ServiceNow

? System Center Service Manager

? Provance

? Cherwell

Incorrect Answers:

B. Azure Event Hubs

Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second.

C. Azure Notification Hubs

Azure Notification Hubs provide an easy-to-use and scaled-out push engine that enables you to send notifications to any platform (iOS, Android, Windows, etc.) from any back-end (cloud or on-premises).

D. Application Insights Connector

Azure Application Insights is an extensible analytics service that helps you understand the performance and usage of your live web application. Application Insights Connector to connect from Logic Apps, Power Apps etc.

Reference:

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

IT Service Management Connector Overview

12/16/2020 • 2 minutes to read •

IT Service Management Connector (ITSMC) allows you to connect Azure to a supported IT Service Management (ITSM) product or service.

Azure services like Azure Log Analytics and Azure Monitor provide tools to detect, analyze, and troubleshoot problems with your Azure and non-Azure resources. But the work items related to an issue typically reside in an ITSM product or service. ITSMC provides a bi-directional connection between Azure and ITSM tools to help you resolve issues faster.

Configuration steps

ITSMC supports connections with the following ITSM tools:

- ServiceNow
- System Center Service Manager
- Provance
- Cherwell

> ⓘ Note
>
> As of 1-Oct-2020 Cherwell and Provance ITSM integrations with Azure Alert will no longer be enabled for new customers. New ITSM Connections will not be supported. Existing ITSM connections will be supported.

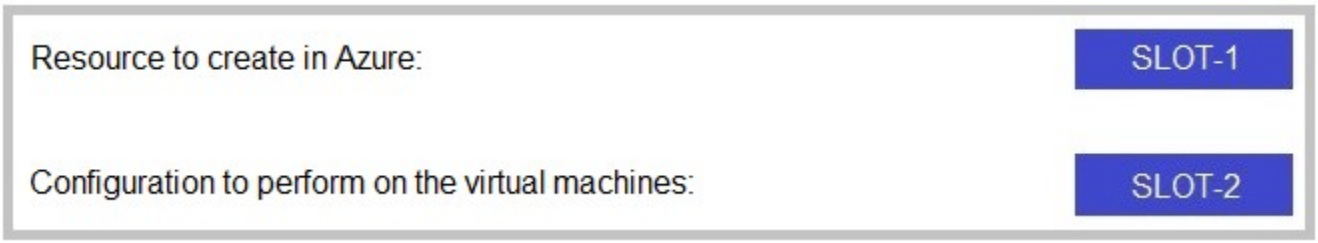
With ITSMC, you can:

- Create work items in your ITSM tool, based on your Azure alerts (Metric Alerts, Activity Log Alerts, and Log Analytics alerts).
- Optionally, you can sync your incident and change request data from your ITSM tool to an Azure Log Analytics workspace.

39. Question

You have an Azure subscription that contains 300 Azure virtual machines that run Windows Server 2016.

You need to centrally monitor all warning events in the System logs of the virtual machines.



Which of the following would go into Slot1?

- A. An event hub
- **B. A Log Analytics workspace**
- C. A search service
- D. A storage account

Correct

In order to monitor and manage virtual machines or physical computers in your local datacenter or other cloud environment with Azure Monitor, you need to deploy the Log Analytics agent (also referred to as the Microsoft Monitoring Agent (MMA)) and configure it to report to one or more Log Analytics workspaces. The agent also supports the Hybrid Runbook Worker role for Azure Automation.

Incorrect Answers:

A. An event hub

Azure Event Hubs is a big data streaming platform and event ingestion service.

C. A search service

Azure Cognitive Search is the only cloud search service with built-in AI capabilities that enrich all types of information to help you identify and explore relevant content at scale.

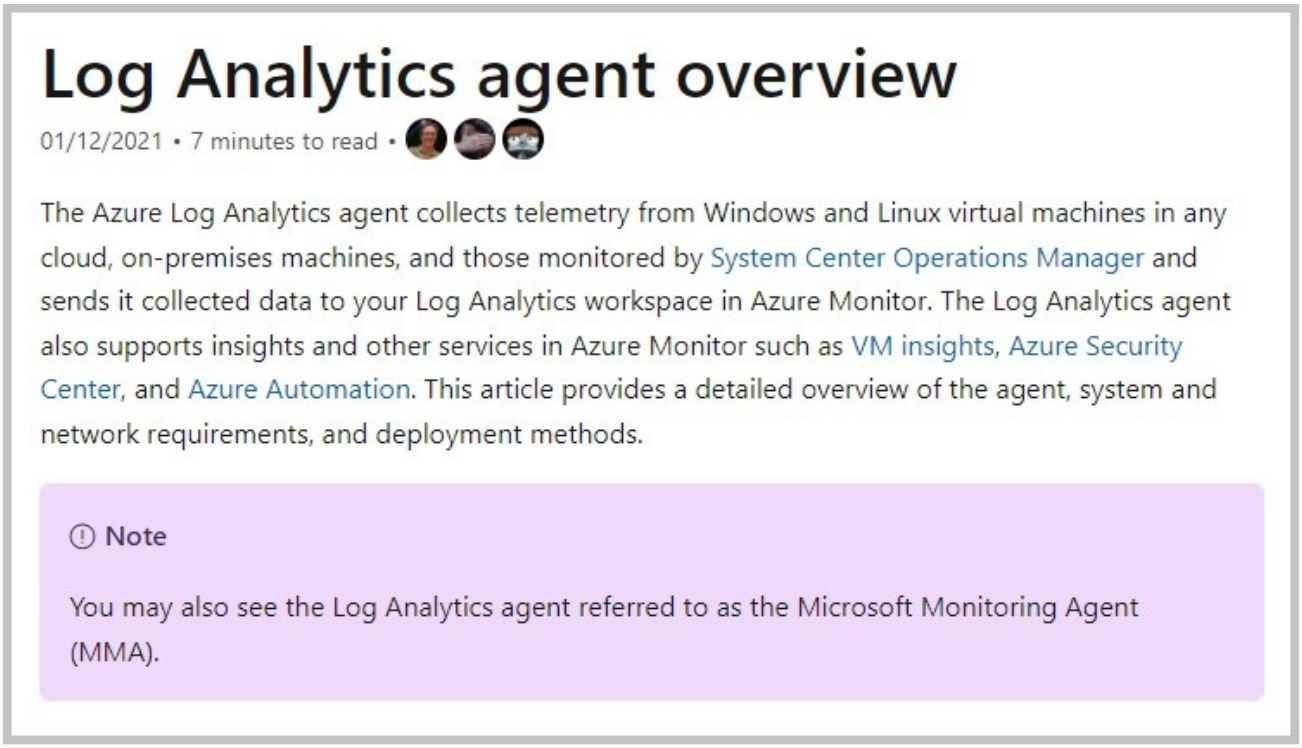
D. A storage account

An Azure storage account contains all of your Azure Storage data objects: blobs, file shares, queues, tables, and disks.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

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



Log Analytics agent overview

01/12/2021 • 7 minutes to read •

The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System Center Operations Manager and sends it collected data to your Log Analytics workspace in Azure Monitor. The Log Analytics agent also supports insights and other services in Azure Monitor such as VM insights, Azure Security Center, and Azure Automation. This article provides a detailed overview of the agent, system and network requirements, and deployment methods.

Note

You may also see the Log Analytics agent referred to as the Microsoft Monitoring Agent (MMA).

Overview of Azure Monitor agents

07/22/2021 • 9 minutes to read • +4

Virtual machines and other compute resources require an agent to collect monitoring data required to measure the performance and availability of their guest operating system and workloads. This article describes the agents used by Azure Monitor and helps you determine which you need to meet the requirements for your particular environment.

Note

Azure Monitor recently launched a new agent, the Azure Monitor agent, that provides all capabilities necessary to collect guest operating system monitoring data. While there are multiple legacy agents that exist due to the consolidation of Azure Monitor and Log Analytics, each with their unique capabilities with some overlap, we recommend that you use the new agent that aims to consolidate features from all existing agents, and provide additional benefits. **Learn More**

40. Question

You have an Azure subscription that contains 300 Azure virtual machines that run Windows Server 2016.

You need to centrally monitor all warning events in the System logs of the virtual machines.

Resource to create in Azure:	SLOT-1
Configuration to perform on the virtual machines:	SLOT-2

Which of the following would go into Slot2?

- Create event subscriptions
- Configure Continuous delivery
- **Install the Microsoft Monitoring Agent**
- Modify the membership of the Event Log Readers group

Correct

In order to monitor and manage virtual machines or physical computers in your local datacenter or other cloud environment with Azure Monitor, you need to deploy the Log Analytics agent (also referred to as the Microsoft Monitoring Agent (MMA)) and configure it to report to one or more Log Analytics workspaces. The agent also supports the Hybrid Runbook Worker role for Azure Automation.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

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

Log Analytics agent overview

01/12/2021 • 7 minutes to read •

The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System Center Operations Manager and sends it collected data to your Log Analytics workspace in Azure Monitor. The Log Analytics agent also supports insights and other services in Azure Monitor such as VM insights, Azure Security Center, and Azure Automation. This article provides a detailed overview of the agent, system and network requirements, and deployment methods.

Note

You may also see the Log Analytics agent referred to as the Microsoft Monitoring Agent (MMA).

Overview of Azure Monitor agents

07/22/2021 • 9 minutes to read • +4

Virtual machines and other compute resources require an agent to collect monitoring data required to measure the performance and availability of their guest operating system and workloads. This article describes the agents used by Azure Monitor and helps you determine which you need to meet the requirements for your particular environment.

Note

Azure Monitor recently launched a new agent, the Azure Monitor agent, that provides all capabilities necessary to collect guest operating system monitoring data. While there are multiple legacy agents that exist due to the consolidation of Azure Monitor and Log Analytics, each with their unique capabilities with some overlap, we recommend that you use the new agent that aims to consolidate features from all existing agents, and provide additional benefits. **Learn More**

41. Question

A company plans to implement an HTTP-based API to support a web app. The web app allows customers to check the status of their orders.

The API must meet the following requirements:

? Implement Azure Functions.

? Provide public read-only operations.

? Do not allow write operations.

You need to recommend configuration options.

What should you recommend for authentication level?

- A. Function
- **B. Anonymous**
- C. Admin

Correct

The option is Allow Anonymous requests. This option turns on authentication and authorization in App Service, but defers authorization decisions to your application code. For authenticated requests, App Service also passes along authentication information in the HTTP headers.

This option provides more flexibility in handling anonymous requests.

Incorrect Answers:

A. Function

Not a valid authentication level for public read-only operations.

C. Admin

Not a valid authentication level for public read-only operations.

Reference:

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

42. Question

A company plans to implement an HTTP-based API to support a web app. The web app allows customers to check the status of their orders.

The API must meet the following requirements:

? Implement Azure Functions.

? Provide public read-only operations.

? Do not allow write operations.

You need to recommend configuration options.

What should you recommend for allowed authentication methods?

- A. API methods
- B. GET only
- C. GET and POST only
- D. GET, POST, and OPTIONS only

Correct

Need to provide read only operations and should not allow write operations. So GET only.

Reference:

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

43. Question

A company has an existing web application that runs on virtual machines (VMs) in Azure.

You need to ensure that the application is protected from SQL injection attempts and uses a layer-7 load balancer. The solution must minimize disruption to the code for the existing web application.

Which azure service would go into Slot1?

- A. Web Application Firewall (WAF)
- B. Azure Application Gateway
- C. Azure Load Balancer
- D. Azure Traffic Manager
- E. SSL offloading
- F. URL-based content routing

Correct

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

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So if

/images is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos.

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

Reference:

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

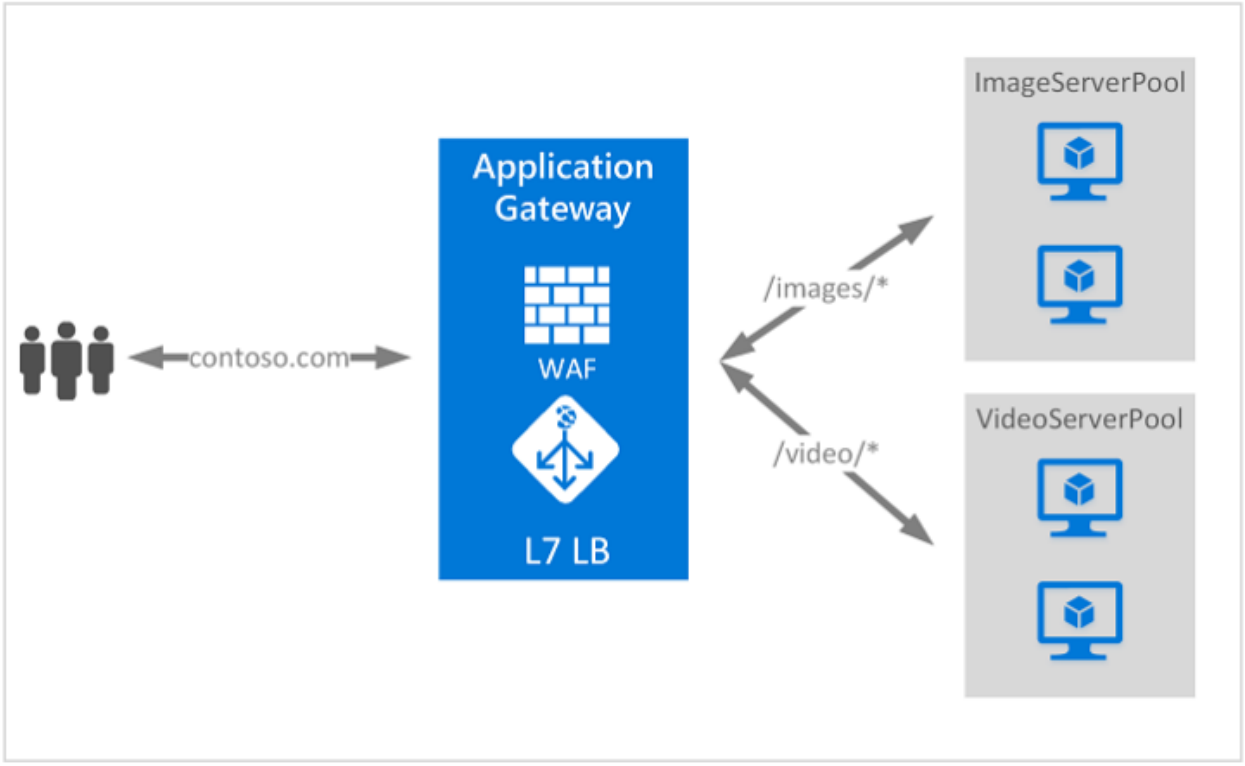
https://docs.microsoft.com/en-us/azure/application-gateway/overview

What is Azure Application Gateway?

08/26/2020 • 2 minutes to read • +5

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

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



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

44. Question

A company has an existing web application that runs on virtual machines (VMs) in Azure.

You need to ensure that the application is protected from SQL injection attempts and uses a layer-7 load balancer. The solution must minimize disruption to the code for the existing web application.

Which feature would go into Slot2?

- A. Web Application Firewall (WAF)
- B. Azure Application Gateway
- C. Azure Load Balancer
- D. Azure Traffic Manager
- E. SSL offloading
- F. URL-based content routing

Correct

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

Reference:

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

https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

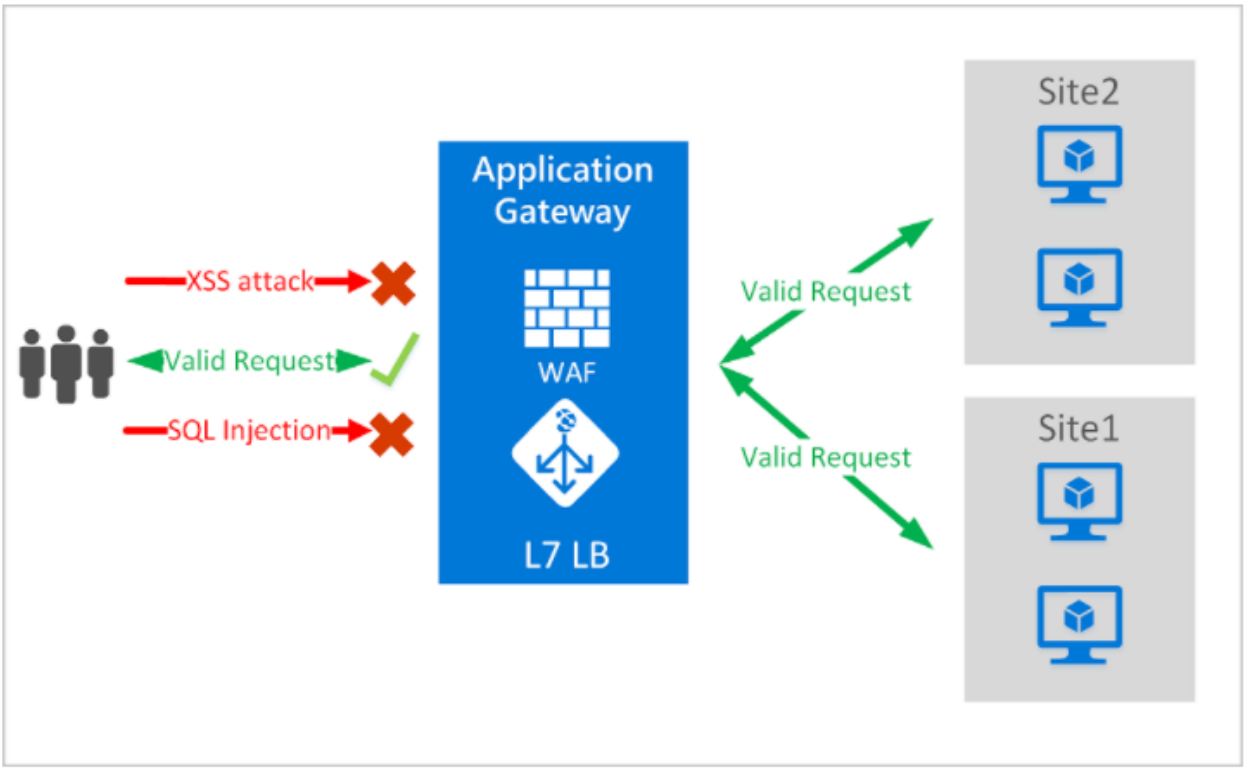
What is Azure Web Application Firewall on Azure Application Gateway?

09/02/2021 • 9 minutes to read •

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

WAF on Application Gateway is based on Core Rule Set (CRS) 3.1, 3.0, or 2.2.9 from the Open Web Application Security Project (OWASP).

All of the WAF features listed below exist inside of a WAF Policy. You can create multiple policies, and they can be associated with an Application Gateway, to individual listeners, or to path-based routing rules on an Application Gateway. This way, you can have separate policies for each site behind your Application Gateway if needed. For more information on WAF Policies, see Create a WAF Policy.



Application Gateway operates as an application delivery controller (ADC). It offers Transport Layer Security (TLS), previously known as Secure Sockets Layer (SSL), termination, cookie-based session affinity, round-robin load distribution, content-based routing, ability to host multiple websites, and security enhancements.

Application Gateway security enhancements include TLS policy management and end-to-end TLS support. Application security is strengthened by WAF integration into Application Gateway. The combination protects your web applications against common vulnerabilities. And it provides an easy-to-configure central location to manage.

45. Question

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

The users can connect to App1 without being prompted for authentication:	SLOT-1
The users can access App1 only from company-owned computers:	SLOT-2

Which of the following would go into Slot1?

- A. An Azure AD app registration
- B. An Azure AD managed identity
- C. Azure AD Application Proxy

Incorrect

Azure active directory (AD) provides cloud based directory and identity management services.You can use azure AD to manage users of your application and authenticate access to your applications using azure active directory.

You register your application with Azure active directory tenant.

Incorrect Answers:

B. An Azure AD 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.

C. Azure AD Application Proxy

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications

Reference:

https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application/

https://docs.microsoft.com/en-us/graph/auth-register-app-v2

46. Question

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

The users can connect to App1 without being prompted for authentication:	SLOT-1
The users can access App1 only from company-owned computers:	SLOT-2

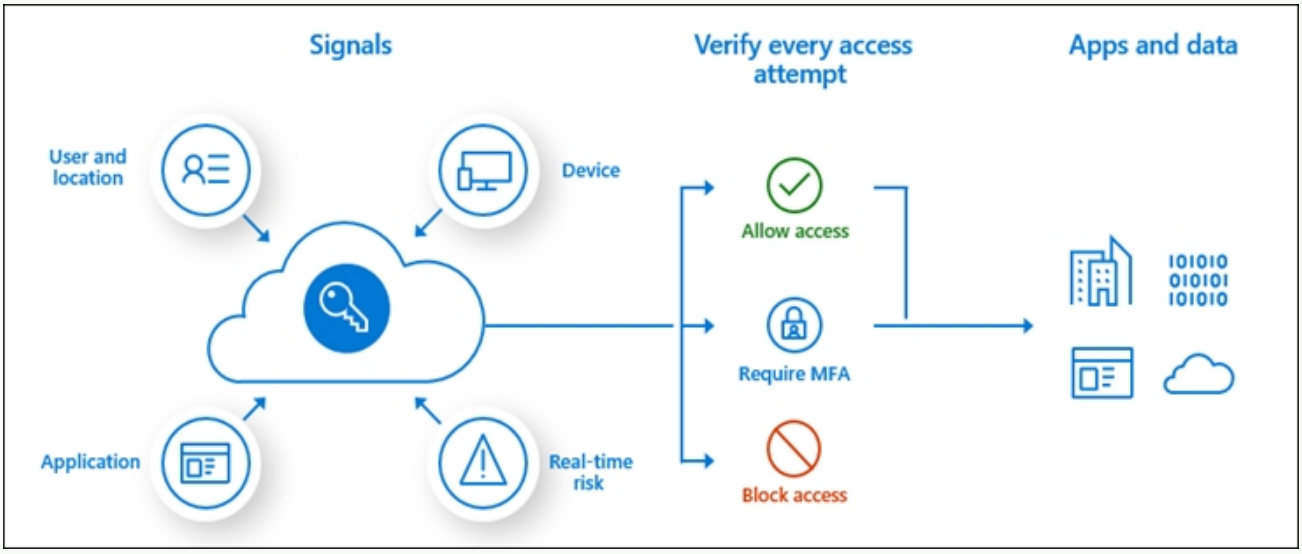
Which of the following would go into Slot2?

- A. A conditional access policy
- B. An Azure AD administrative unit
- C. Azure application gateway
- D. Azure Blueprints
- E. Azure Policy

Correct

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Incorrect Answers:

B. An Azure AD administrative unit

Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.

C. Azure application gateway

Application gateway is a load balancing solution.

D. Azure Blueprints

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.

E. Azure Policy

Azure policies are used to enforce organizational standards.

Reference:

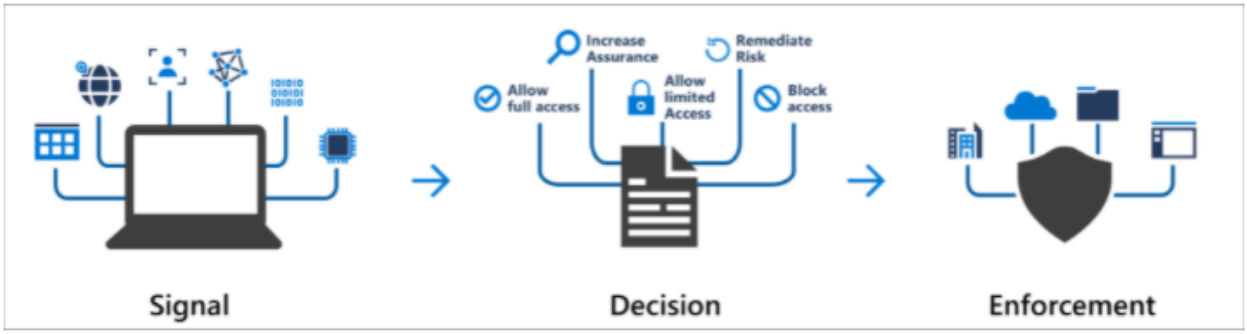
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

What is Conditional Access?

01/27/2021 • 2 minutes to read • +9

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can utilize these identity signals as part of their access control decisions.

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

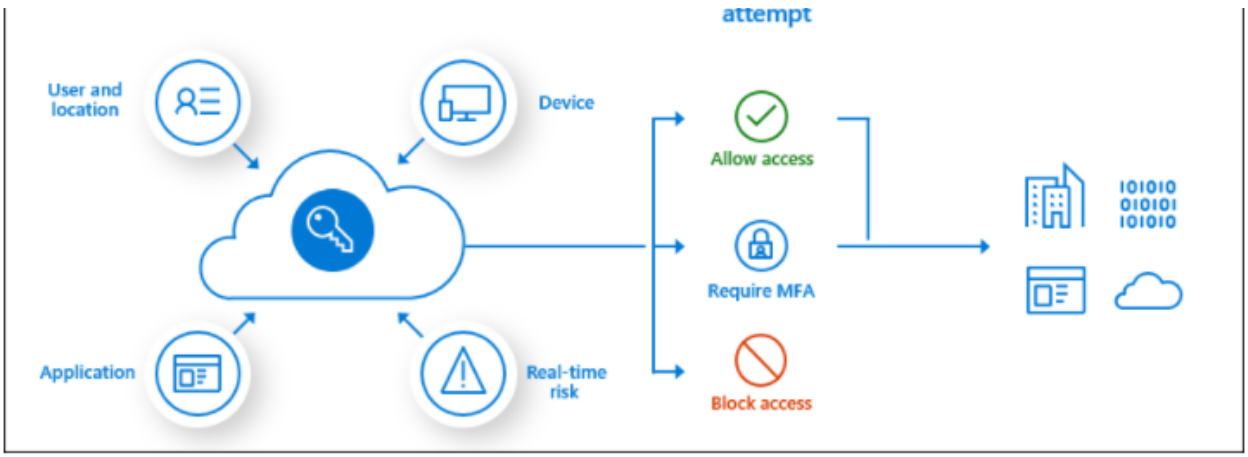


Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Important

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

47. Question

Your company has the offices shown in the following table.

Location	IP Address Space	Public NAT Segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24

The network contains an Active Directory domain named contoso.com that is synced to Azure Active Directory (Azure AD). All users connect to an Exchange Online.

You need to recommend a solution to ensure that all the users use Azure Multi-Factor Authentication (MFA) to connect to Exchange Online from one of the offices.

What should you include in the recommendation?

- A. a virtual network and two Microsoft Cloud App Security policies
- B. a named location and two Microsoft Cloud App Security policies
- C. a conditional access policy and two virtual networks
- D. a conditional access policy and two named locations

Correct

Conditional Access policies are at their most basic an if-then statement combining signals, to make decisions, and enforce organization policies. One of those signals that can be incorporated into the decision-making process is network location.

Locations are designated in the Azure portal under Azure Active Directory > Security > Conditional

Access > Named locations. These named network locations may include locations like an organization's headquarters network ranges, VPN network ranges, or ranges that you wish to block.

Incorrect Answers:

A. a virtual network and two Microsoft Cloud App Security policies

Virtual network is not required to define MFA.

B. a named location and two Microsoft Cloud App Security policies

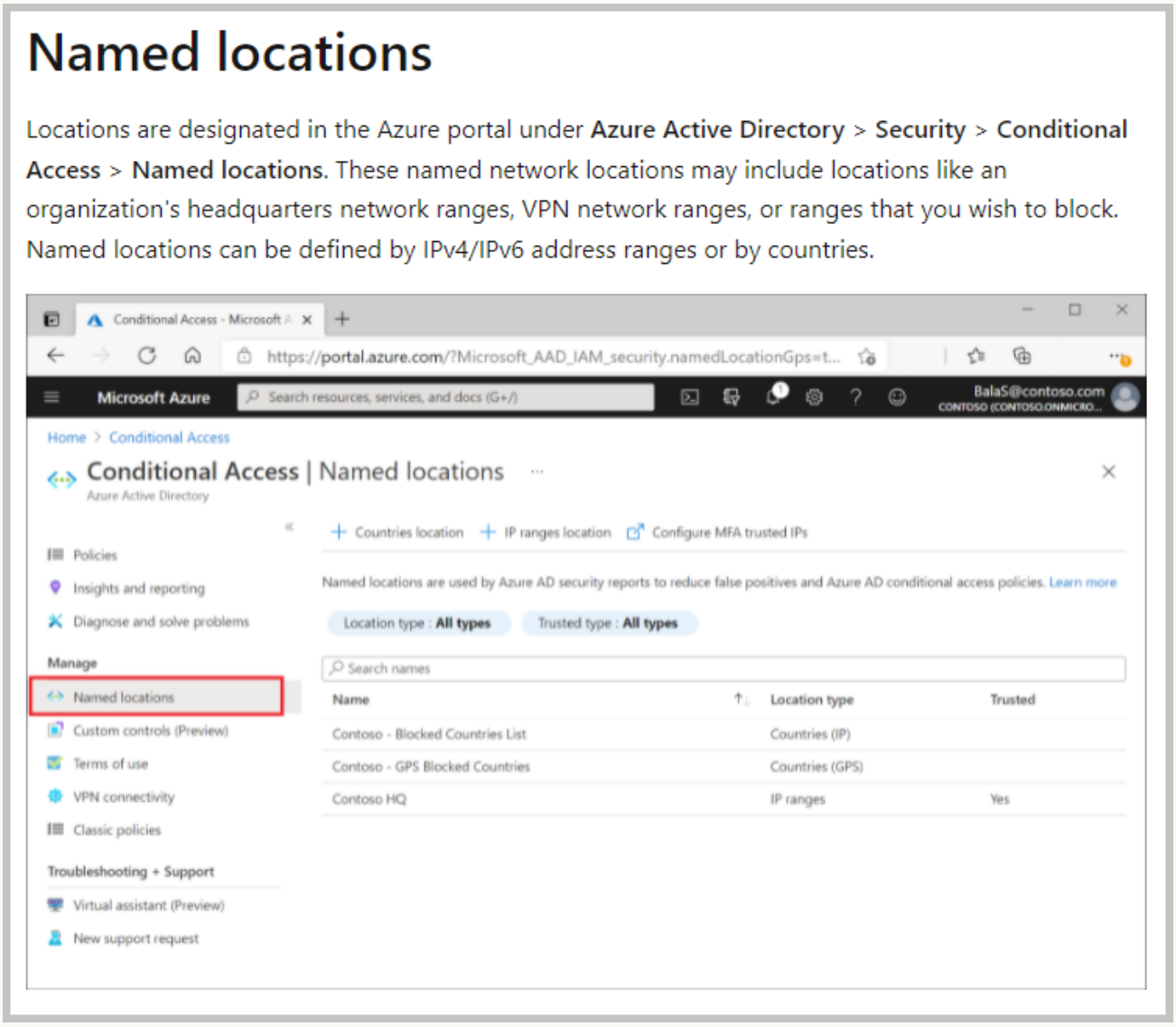
Microsoft Cloud App Security access policies enable real-time monitoring and control over access to cloud apps based on user, location, device, and app.

C. a conditional access policy and two virtual networks

Virtual network is not required to define MFA.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#named-locations



48. Question

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

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

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

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use password hash synchronization and select the “Enable single sign-on“ option.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don‘t need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

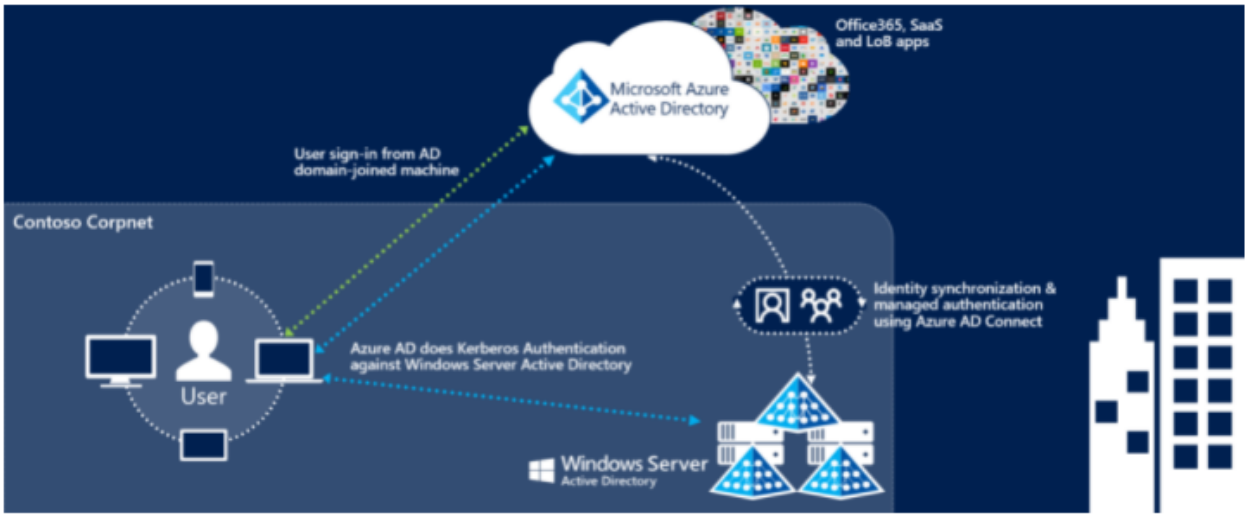
Azure Active Directory Seamless Single Sign-On

08/13/2019 • 3 minutes to read • +12

What is Azure Active Directory Seamless Single Sign-On?

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods. Seamless SSO is *not* applicable to Active Directory Federation Services (ADFS).



49. Question

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

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

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use pass-through authentication and select

the “Enable single sign-on“ option.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don‘t need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

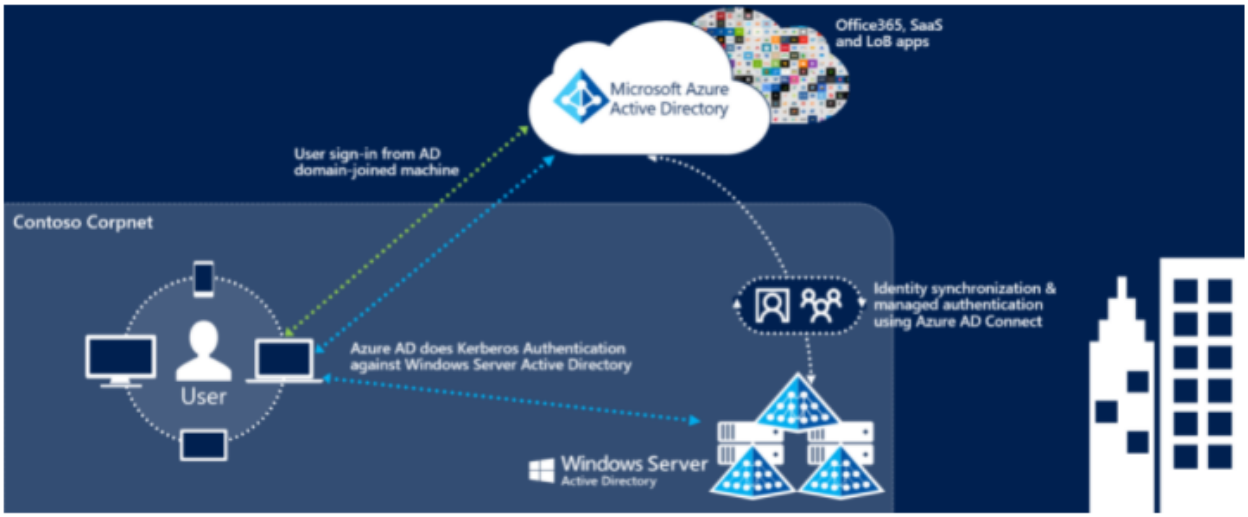
Azure Active Directory Seamless Single Sign-On

08/13/2019 • 3 minutes to read • +12

What is Azure Active Directory Seamless Single Sign-On?

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods. Seamless SSO is *not* applicable to Active Directory Federation Services (ADFS).



50. Question

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

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

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Configure an AD DS server in an Azure virtual machine (VM). Configure bidirectional replication.

Does the solution meet the goal?

- A. Yes
- B. No

Correct

Instead install and configure an Azure AD Connect server.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

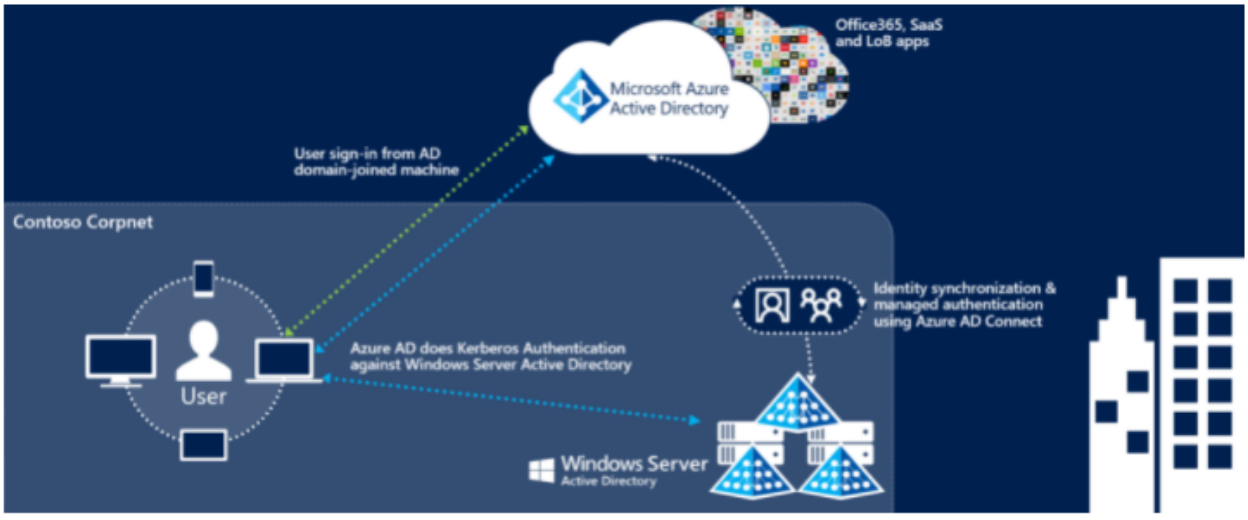
Azure Active Directory Seamless Single Sign-On

08/13/2019 • 3 minutes to read • +12

What is Azure Active Directory Seamless Single Sign-On?

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods. Seamless SSO is *not* applicable to Active Directory Federation Services (ADFS).



51. Question

You are designing an Azure web app that will use Azure Active Directory (Azure AD) for authentication.

You need to recommend a solution to provide users from multiple Azure AD tenants with access to App1.

The solution must ensure that the users use Azure Multi-Factor Authentication (MFA) when they connect to App1.

Which two types of objects should you include in the recommendation?

- [x] A. Azure AD conditional access policies
- [x] B. Azure AD managed identities
- [ ] C. an Identity Experience Framework policy
- [ ] D. an Azure application security group
- [ ] E. an Endpoint Manager app protection policy
- [ ] F. Azure AD guest accounts

Incorrect

The Conditional Access feature in Azure Active Directory (Azure AD) offers one of several ways that you can use to secure your app and protect a service.

Conditional Access enables developers and enterprise customers to protect services in a multitude of ways including:

? Multi-factor authentication

? Allowing only Intune enrolled devices to access specific services

? Restricting user locations and IP ranges

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policy:

? Service accounts and service principals.

If your organization has these accounts in use in scripts or code, consider replacing them with managed identities.

You can use either guest accounts or multi-tenant app registrations to allow users from other tenants to access your application.

Incorrect Answers:

B. Azure AD managed identities

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.

D. an Azure application security group

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

E. an Endpoint Manager app protection policy

Application security groups enable you to configure network security as a natural extension of an application? s structure, allowing you to group virtual machines and define network security policies based on those groups.

Note: The correct options should be application registration with Azure, this will allow the authentication of users on the AD to access the application. A default application registration validates that the user has valid login credentials. This can be your Active Directory or in case of a multi-tenant application the directory where the user is originated from.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-conditional-access-dev-guide

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management

https://www.re-mark-able.net/understanding-azure-active-directory-application-registrations/

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant

Developer guidance for Azure Active Directory Conditional Access

05/18/2020 • 9 minutes to read • +3

The Conditional Access feature in Azure Active Directory (Azure AD) offers one of several ways that you can use to secure your app and protect a service. Conditional Access enables developers and enterprise customers to protect services in a multitude of ways including:

- Multi-factor authentication
- Allowing only Intune enrolled devices to access specific services
- Restricting user locations and IP ranges

For more information on the full capabilities of Conditional Access, see the article What is Conditional Access.

For developers building apps for Azure AD, this article shows how you can use Conditional Access and you'll also learn about the impact of accessing resources that you don't have control over that may have Conditional Access policies applied. The article also explores the implications of Conditional Access in the on-behalf-of flow, web apps, accessing Microsoft Graph, and calling APIs.

Knowledge of single and multi-tenant apps and common authentication patterns is assumed.

Note

Using this feature requires an Azure AD Premium P1 license. To find the right license for your requirements, see **Comparing generally available features of the Free, Basic, and Premium editions**. Customers with **Microsoft 365 Business licenses** also have access to Conditional Access features.

52. Question

You need to create an Azure Storage account that uses a custom encryption key.

What do you need to implement the encryption?

- A. a certificate issued by an integrated certification authority (CA) and stored in Azure Key Vault
- B. a managed identity that is configured to access the storage account
- C. an Azure Active Directory Premium subscription
- D. an Azure key vault in the same Azure region as the storage account

Correct

Azure Storage encrypts all data in a storage account at rest. You can manage your own keys. Customer-managed keys must be stored in Azure Key Vault or Key Vault Managed Hardware Security Model (HSM).

You can use a new or existing key vault to store customer-managed keys. The storage account and the key vault must be in the same region, but they can be in different subscriptions.

Note: You must use either Azure Key Vault or Azure Key Vault Managed Hardware Security Module (HSM) (preview) to store your customer-managed keys. You can either create your own keys and store them in the key vault or managed HSM, or you can use the Azure Key Vault APIs to generate keys. The storage account and the key vault or managed HSM must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.

Incorrect Answers:

A. a certificate issued by an integrated certification authority (CA) and stored in Azure Key Vault

Azure Storage encryption supports RSA and RSA-HSM keys of sizes 2048, 3072 and 4096. Certificate is not required.

B. a managed identity that is configured to access the storage account

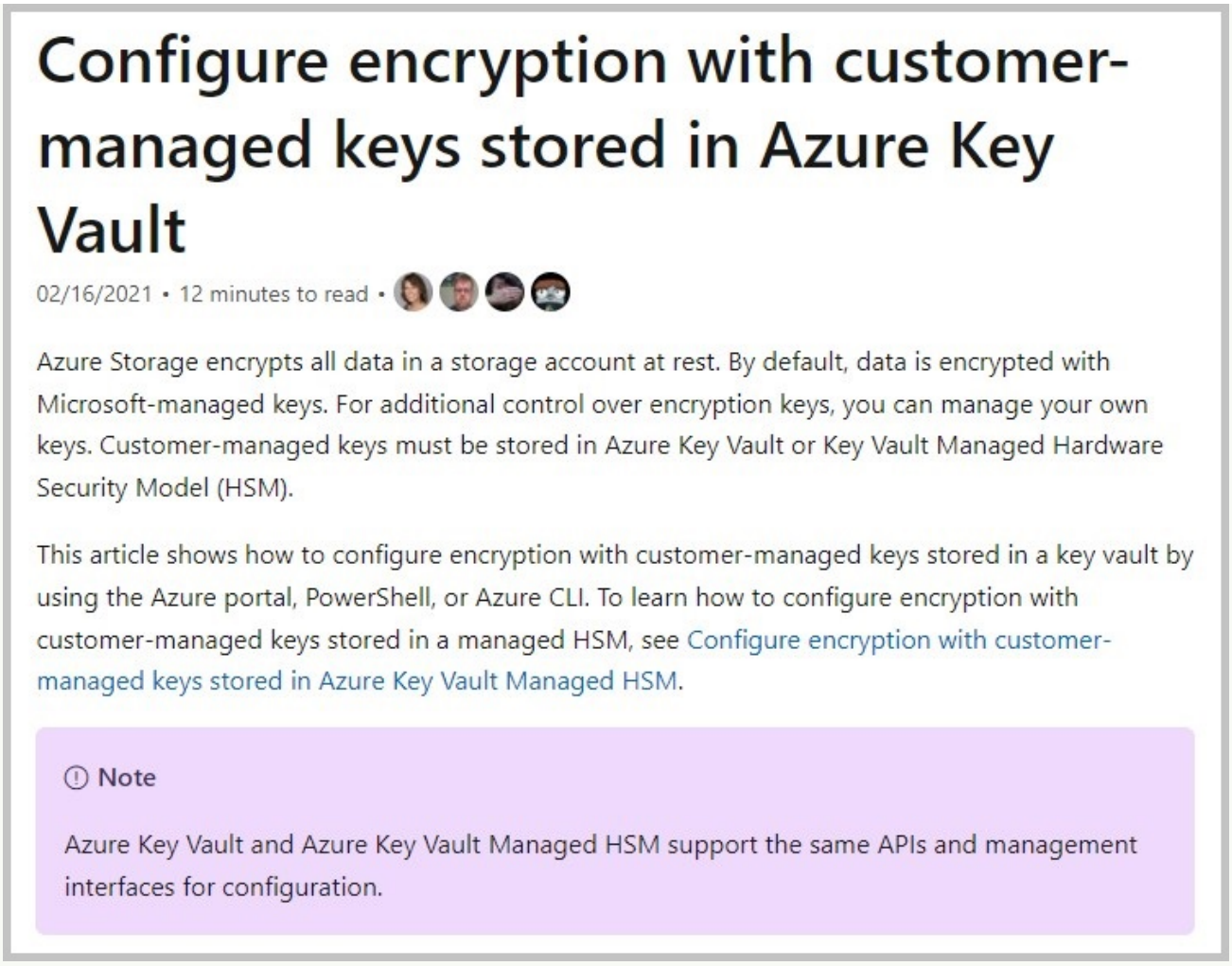
No need to create a managed identity. You select the custom encryption key from “Encryption“ in Settings window.

C. an Azure Active Directory Premium subscription

Not a valid option in this context.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=portal



Configure encryption with customer-managed keys stored in Azure Key Vault

02/16/2021 • 12 minutes to read •

Azure Storage encrypts all data in a storage account at rest. By default, data is encrypted with Microsoft-managed keys. For additional control over encryption keys, you can manage your own keys. Customer-managed keys must be stored in Azure Key Vault or Key Vault Managed Hardware Security Model (HSM).

This article shows how to configure encryption with customer-managed keys stored in a key vault by using the Azure portal, PowerShell, or Azure CLI. To learn how to configure encryption with customer-managed keys stored in a managed HSM, see Configure encryption with customer-managed keys stored in Azure Key Vault Managed HSM.

Note

Azure Key Vault and Azure Key Vault Managed HSM support the same APIs and management interfaces for configuration.

53. Question

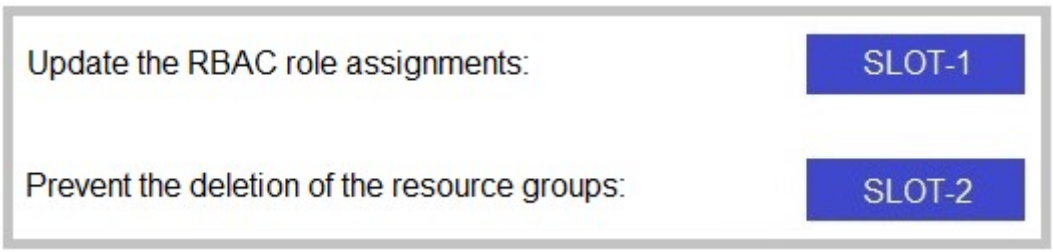
You plan to create an Azure environment that will have a root management group and five child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription.

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

? Prevent users who are assigned the Owner role for the subscriptions from deleting the resource groups from their respective subscription.

? Ensure that you can update RBAC role assignments across all the subscriptions and resource groups.

? Minimize administrative effort.



Which of the following would go into Slot1?

A. Azure Blueprints

B. Azure Policy

C. Azure Security Center

Incorrect

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

Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.

Incorrect Answers:

B. Azure Policy

A policy is a default allow and explicit deny system focused on resource properties during deployment and for already existing resources.

C. Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.

Reference:

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

54. Question

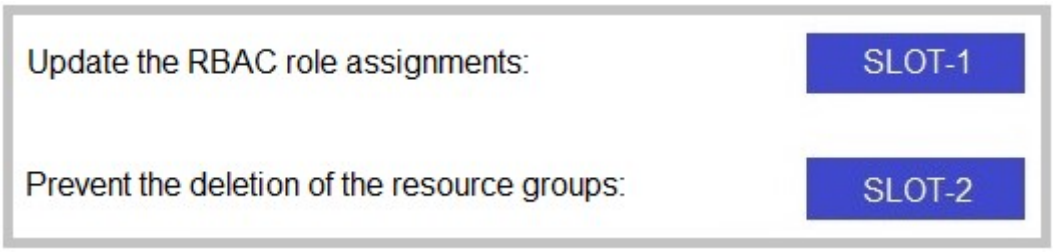
You plan to create an Azure environment that will have a root management group and five child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription.

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

? Prevent users who are assigned the Owner role for the subscriptions from deleting the resource groups from their respective subscription.

? Ensure that you can update RBAC role assignments across all the subscriptions and resource groups.

? Minimize administrative effort.



Which of the following would go into Slot2?

- A. Azure blueprints assignments that set locking mode at the subscription level
- B. Resource locks at the resource group level
- C. Resource locks at the subscription level

Incorrect

It's typically possible for someone with appropriate Azure role-based access control (Azure RBAC) on the subscription, such as the 'Owner' role, to be allowed to alter or delete any resource. This access isn't the case when Azure Blueprints applies locking as part of a deployed assignment. If the assignment was set with the Read Only or Do Not Delete option, not even the subscription owner can perform the blocked action on the protected resource.

This security measure protects the consistency of the defined blueprint and the environment it was designed to create from accidental or programmatic deletion or alteration.

Incorrect Answers:

B. Resource locks at the resource group level

Owners can remove the locks and delete the resources.

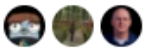
C. Resource locks at the subscription level

Owners can remove the locks and delete the resources. Moreover, a read-only lock on a subscription prevents Azure Advisor from working correctly.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

Understand resource locking in Azure Blueprints

08/17/2021 • 5 minutes to read • 

The creation of consistent environments at scale is only truly valuable if there's a mechanism to maintain that consistency. This article explains how resource locking works in Azure Blueprints. To see an example of resource locking and application of *deny assignments*, see the protecting new resources tutorial.

> ⓘ **Note**
>
> Resource locks deployed by Azure Blueprints are only applied to **non-extension resources** deployed by the blueprint assignment. Existing resources, such as those in resource groups that already exist, don't have locks added to them.

Locking modes and states

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

Resources created by artifacts in a blueprint assignment have four states: **Not Locked**, **Read Only**, **Cannot Edit / Delete**, or **Cannot Delete**. Each artifact type can be in the **Not Locked** state. The following table can be used to determine the state of a resource:

Mode	Artifact Resource Type	State	Description
Don't Lock	*	Not Locked	Resources aren't protected by Azure Blueprints. This state is also used for resources added to a **Read Only** or **Do Not Delete** resource group artifact from outside a blueprint assignment.
Read Only	Resource group	Cannot Edit / Delete	The resource group is read only and tags on the resource group can't be modified. **Not Locked** resources can be added, moved, changed, or deleted from this resource group.
Read Only	Non-resource group	Read Only	The resource can't be altered in any way. No changes and it can't be deleted.
Do Not Delete	*	Cannot Delete	The resources can be altered, but can't be deleted. **Not Locked** resources can be added, moved, changed, or deleted from this resource group.

55. Question

Your company has the divisions shown in the following table.

Division	Azure Subscription	Azure Active Directory (Azure AD) Tenant
East	Sub1	East.techzen-az304.com
West	Sub2	West.techzen-az304.com

Sub1 contains an Azure web app that runs an ASP.NET application named App1. App1 uses the Microsoft identity platform (v2.0) to handle user authentication.

Users from east.techzen-az304.com can authenticate to App1.

You need to recommend a solution to allow users from west.techzen-az304.com to authenticate to App1.

What should you recommend for the west.techzen-az304.com Azure AD tenant?

- A. a conditional access policy
- B. pass-through authentication
- C. guest accounts
- D. an app registration

Incorrect

You need to do app registration which supports Multi-tenant apps that are available to users in both their home tenant and other tenants.

Incorrect Answers:

A. a conditional access policy

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

B. pass-through authentication

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.

C. guest accounts

Managing guest users for every new user joined/moved in west.preparationlabs.com is a tedious task.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant

Sign in any Azure Active Directory user using the multi-tenant application pattern

10/27/2020 • 13 minutes to read • +13

If you offer a Software as a Service (SaaS) application to many organizations, you can configure your application to accept sign-ins from any Azure Active Directory (Azure AD) tenant. This configuration is called *making your application multi-tenant*. Users in any Azure AD tenant will be able to sign in to your application after consenting to use their account with your application.

If you have an existing application that has its own account system, or supports other kinds of sign-ins from other cloud providers, adding Azure AD sign-in from any tenant is simple. Just register your app, add sign-in code via OAuth2, OpenID Connect, or SAML, and put a "Sign in with Microsoft" button in your application.

Note

This article assumes you're already familiar with building a single-tenant application for Azure AD. If you're not, start with one of the quickstarts on the **developer guide homepage**.

56. Question

Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1.

You have a hybrid deployment of Azure Active Directory (Azure AD).

You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet.

Which three Azure services should you recommend be deployed and configured in sequence?

1. an internal Azure Load Balancer
2. an Azure AD conditional access policy
3. Azure AD Application Proxy
4. an Azure AD managed identity
5. a public Azure Load Balancer
6. an Azure AD enterprise application
7. an App Service plan

- 3 -> 6 -> 2
- 6 -> 2 -> 4
- 7 -> 4 -> 2

2 -> 4 -> 6

Incorrect

Step 1: Azure AD Application proxy

Azure AD Application Proxy is a prerequisite for a scenario with an on-premises legacy applications published for cloud access,

Note: 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.

Step 2: an Azure AD Enterprise Application

The Enterprise Applications blade might be confused with App Registrations because the Enterprise Application blade contains the list of your service principals. However, the term Enterprise App generally refers to applications published by other companies in the AAD gallery that can be used within your organization. For example, if you want to integrate Facebook and manage SSO within your organization, you can integrate it from the Enterprise Applications dropdown in the applications blade. Your own applications will also be represented in the Enterprise Applications blade as Service Principals, which are instantiations of your applications in the tenant.

Step 3: an Azure AD conditional access policy

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

With hybrid identity to Azure AD and hybrid identity management these scenarios become possible.

Reference:

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

https://thesleepyadmins.com/2019/02/

57. Question

A company named Techzen, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft 365 and an Azure subscription.

Techzen has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS), Active Directory

Federation Services (AD FS), Azure AD Connect, and Microsoft Identity Manager (MIM).

Techzen has a partnership with a company named Netizen, Inc. Netizen has an Active Directory forest and a Microsoft 365 tenant. Netizen has the same on- premises identity infrastructure components as Techzen.

A team of 10 developers from Netizen will work on an Azure solution that will be hosted in the Azure subscription of Techzen. The developers must be added to the Contributor role for a resource group in the Techzen subscription.

You need to recommend a solution to ensure that Techzen can assign the role to the 10 Netizen developers. The solution must ensure that the Netizen developers use their existing credentials to access

resources.

What should you recommend?

- A. In the Azure AD tenant of Techzen, enable Azure Active Directory Domain Services (Azure AD DS). Create a one-way forest trust that uses selective authentication between the Active Directory forests of Techzen and Netizen
- B. In the Azure AD tenant of Techzen, create cloud-only user accounts for the Netizen developers
- C. Configure a forest trust between the on-premises Active Directory forests of Techzen and Netizen
- **D. In the Azure AD tenant of Techzen, use MIM to create guest accounts for the Netizen developers**

Correct

You can use the capabilities in Azure Active Directory B2B to collaborate with external guest users and you can use Azure RBAC to grant just the permissions that guest users need in your environment

MIM enables the organization to have the right users and access rights for Active Directory for on-premises apps, and Azure AD Connect can then make available in Azure AD for Microsoft 365 and cloud-hosted apps.

Incorrect Answers:

A – a lot of work on prem (Fabricam) and mainly to give all users access to Azure. Not suitable

B – No access to on prem resources in Techzen

C – All Fabricam users would get access

Reference:

https://docs.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016

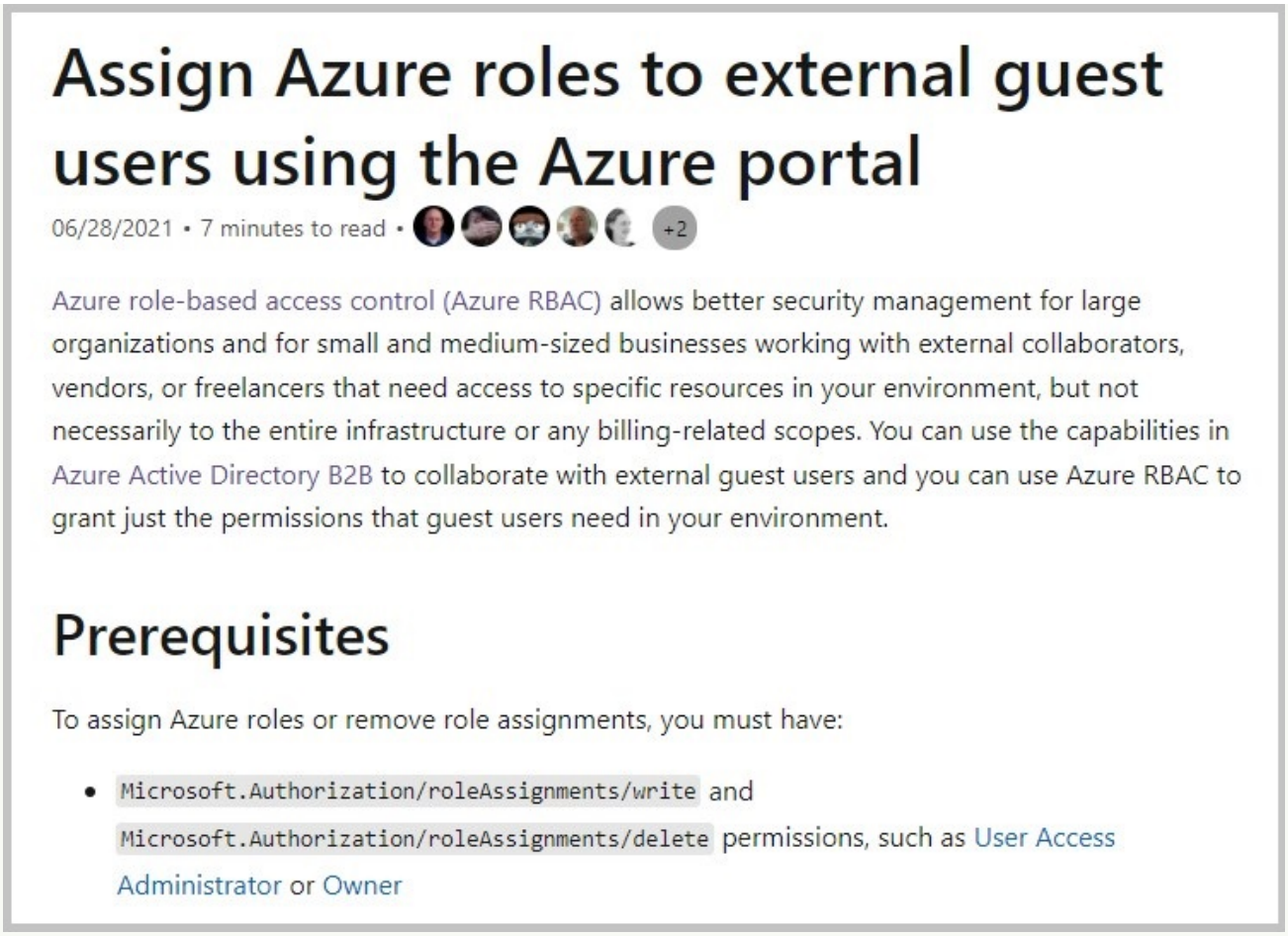
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

What is guest user access in Azure Active Directory B2B?

07/13/2021 • 3 minutes to read •

Azure Active Directory (Azure AD) business-to-business (B2B) collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization. With B2B collaboration, you can securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources. Developers can use Azure AD business-to-business APIs to customize the invitation process or write applications like self-service sign-up portals. For licensing and pricing information related to guest users, refer to Azure Active Directory External Identities pricing.



Assign Azure roles to external guest users using the Azure portal

06/28/2021 • 7 minutes to read • +2

Azure role-based access control (Azure RBAC) allows better security management for large organizations and for small and medium-sized businesses working with external collaborators, vendors, or freelancers that need access to specific resources in your environment, but not necessarily to the entire infrastructure or any billing-related scopes. You can use the capabilities in Azure Active Directory B2B to collaborate with external guest users and you can use Azure RBAC to grant just the permissions that guest users need in your environment.

Prerequisites

To assign Azure roles or remove role assignments, you must have:

- `Microsoft.Authorization/roleAssignments/write` and `Microsoft.Authorization/roleAssignments/delete` permissions, such as User Access Administrator or Owner

58. Question

You are designing an Azure governance solution.

All Azure resources must be easily identifiable based on the following operational information: environment, owner, department, and cost center.

You need to ensure that you can use the operational information when you generate reports for the Azure resources.

What should you include in the solution?

- A. an Azure data catalog that uses the Azure REST API as a data source
- B. Azure Active Directory (Azure AD) administrative units
- C. an Azure management group that uses parent groups to create a hierarchy
- D. an Azure policy that enforces tagging rules

Correct

You use Azure Policy to enforce tagging rules and conventions. By creating a policy, you avoid the scenario of resources being deployed to your subscription that don‘t have the expected tags for your organization. Instead of manually applying tags or searching for resources that aren‘t compliant, you create a policy that automatically applies the needed tags during deployment.

Note: Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments.

Use naming and tagging standards to organize your resources for these reasons:

Resource management: Your IT teams will need to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information. Organizing resources is critical to assigning organizational roles and access permissions for resource management.

Incorrect Answers:

A. an Azure data catalog that uses the Azure REST API as a data source

Azure Data Catalog is a fully managed cloud service. It lets users discover the data sources they need and understand the data sources they find.

B. Azure Active Directory (Azure AD) administrative units

An administrative unit is an Azure AD resource that can be a container for other Azure AD resources. An administrative unit can contain only users and groups. Administrative units restrict permissions in a role to any portion of your organization that you define.

C. an Azure management group that uses parent groups to create a hierarchy

Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called “management groups“ and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group.

Reference:

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

Assign policy definitions for tag compliance

07/21/2021 • 4 minutes to read •

You use Azure Policy to enforce tagging rules and conventions. By creating a policy, you avoid the scenario of resources being deployed to your subscription that don't have the expected tags for your organization. Instead of manually applying tags or searching for resources that aren't compliant, you create a policy that automatically applies the needed tags during deployment. Tags can also now be applied to existing resources with the new Modify effect and a remediation task. The following section shows example policy definitions for tags.

Resource naming and tagging decision guide

09/16/2021 • 5 minutes to read • +3

Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments. Naming and tagging standards help associate cloud usage costs with business teams via chargeback and show back accounting mechanisms. These conventions can be used as part of security orchestration, automation, and response (SOAR). Use naming and tagging standards to organize your resources for these reasons:

- **Resource management:** Your IT teams will need to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information. Organizing resources is critical to assigning organizational roles and access permissions for resource management.

59. Question

You have an on-premises file server that stores 2 TB of data files.

You plan to move the data files to Azure Blob storage in the Central Europe region.

You need to recommend a storage account type to store the data files and a replication solution for the storage account. The solution must meet the following requirements:

? Be available if a single Azure datacenter fails.

? Support storage tiers.

? Minimize cost.

Which of the following would go into Slot1?

- A. Blob storage
- B. Storage (general purpose v1)
- C. StorageV2 (general purpose v2)

Correct

Data must be available if a single Azure datacenter fails. It means the storage account must support ZRS replication.

Also, solution should support storage tiers.

Only General-purpose V2 supports ZRS and storage tiers.

Incorrect Answers:

A. Blob storage

ZRS is supported only in General-purpose V2 accounts.

B. Storage (general purpose v1)

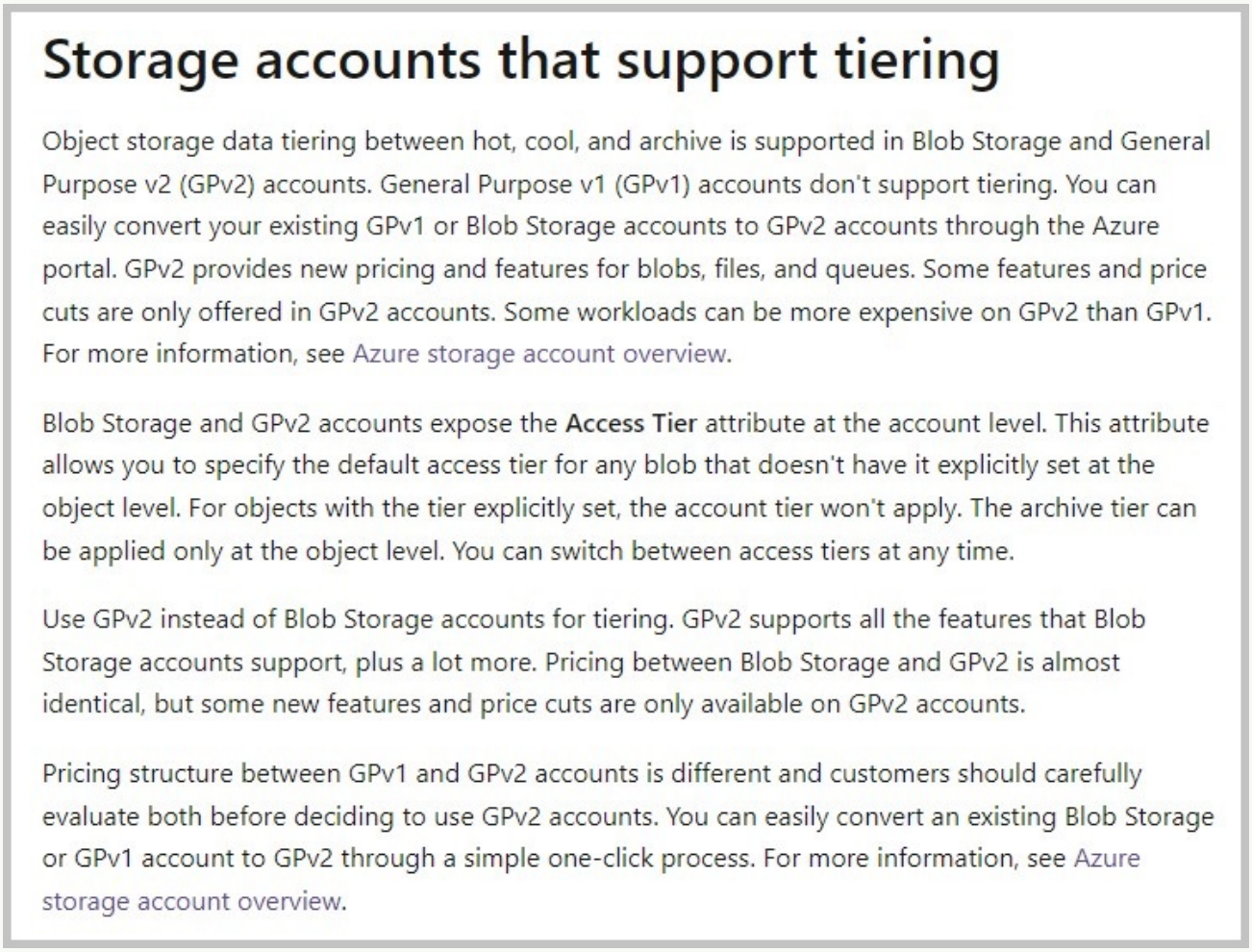
General Purpose v1 (GPv1) accounts don't support tiering

Reference:

https://en.wikipedia.org/wiki/Central_Europe

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#storage-accounts-that-support-tiering

https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview#types-of-storage-accounts



Storage accounts that support tiering

Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering. You can easily convert your existing GPv1 or Blob Storage accounts to GPv2 accounts through the Azure portal. GPv2 provides new pricing and features for blobs, files, and queues. Some features and price cuts are only offered in GPv2 accounts. Some workloads can be more expensive on GPv2 than GPv1. For more information, see Azure storage account overview.

Blob Storage and GPv2 accounts expose the **Access Tier** attribute at the account level. This attribute allows you to specify the default access tier for any blob that doesn't have it explicitly set at the object level. For objects with the tier explicitly set, the account tier won't apply. The archive tier can be applied only at the object level. You can switch between access tiers at any time.

Use GPv2 instead of Blob Storage accounts for tiering. GPv2 supports all the features that Blob Storage accounts support, plus a lot more. Pricing between Blob Storage and GPv2 is almost identical, but some new features and price cuts are only available on GPv2 accounts.

Pricing structure between GPv1 and GPv2 accounts is different and customers should carefully evaluate both before deciding to use GPv2 accounts. You can easily convert an existing Blob Storage or GPv1 account to GPv2 through a simple one-click process. For more information, see Azure storage account overview.

Types of storage accounts

Azure Storage offers several types of storage accounts. Each type supports different features and has its own pricing model. Consider these differences before you create a storage account to determine the type of account that's best for your applications.

The following table describes the types of storage accounts recommended by Microsoft for most scenarios. All of these use the Azure Resource Manager deployment model.

Type of storage account	Supported storage services	Redundancy options	Usage
Standard general-purpose v2	Blob (including Data Lake Storage[1]), Queue, and Table storage, Azure Files	LRS/GRS/RA-GRS ZRS/GZRS/RA-GZRS[2]	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. Note that if you want support for NFS file shares in Azure Files, use the premium file shares account type.
Premium block blobs[3]	Blob storage (including Data Lake Storage[1])	LRS ZRS[2]	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency. Learn more about example workloads.
Premium file shares[3]	Azure Files	LRS ZRS[2]	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both SMB and NFS file shares.
Premium page blobs[3]	Page blobs only	LRS	Premium storage account type for page blobs only. Learn more about page blobs and sample use cases.

60. Question

You have an on-premises file server that stores 2 TB of data files.

You plan to move the data files to Azure Blob storage in the Central Europe region.

You need to recommend a storage account type to store the data files and a replication solution for the storage account. The solution must meet the following requirements:

? Be available if a single Azure datacenter fails.

? Support storage tiers.

? Minimize cost.

Which of the following would go into Slot2?

- A. Geo-redundant storage (GRS)
- **B. Zone-redundant storage (ZRS)**
- C. Locally-redundant storage (LRS)
- D. Read-access geo-redundant storage (RA-GRS)

Correct

Zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region. Each availability zone is a separate physical location with independent power, cooling, and networking. ZRS offers durability for Azure Storage data objects of at least 99.9999999999% (12 9's) over a given year.

With ZRS, your data is still accessible for both read and write operations even if a zone becomes unavailable. If a zone becomes unavailable, Azure undertakes networking updates, such as DNS re-pointing.

Incorrect Answers:

A. Geo-redundant storage (GRS)

We can achieve the requirements with ZRS, that is cheaper as compared with GRS.

C. Locally-redundant storage (LRS)

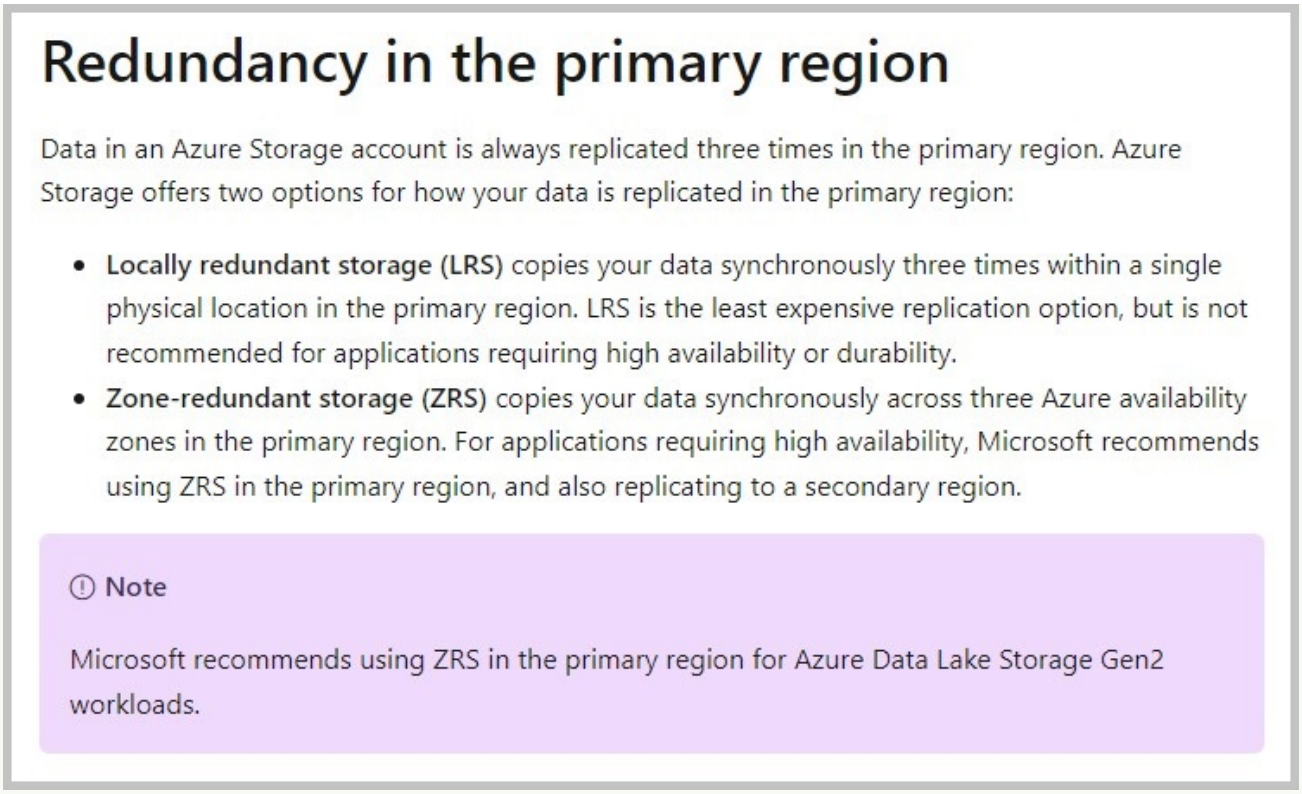
Locally redundant storage (LRS) replicates your data three times within a single data center in the primary region.

D. Read-access geo-redundant storage (RA-GRS)

We can achieve the requirements with ZRS, that is cheaper as compared with RA-GRS.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#redundancy-in-the-primary-region



61. Question

You plan to develop a new app that will store business critical data. The app must meet the following requirements:

? Prevent new data from being modified for one year.

? Minimize read latency.

? Maximize data resiliency.

You need to recommend a storage solution for the app.

Which of the following would go into Slot1?

- A. StorageV2
- B. Blob Storage
- C. BlockBlobStorage

Correct

Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. Immutable storage is available for general-purpose v1, general-purpose v2,

premium block blob, and legacy blob accounts in all Azure regions.

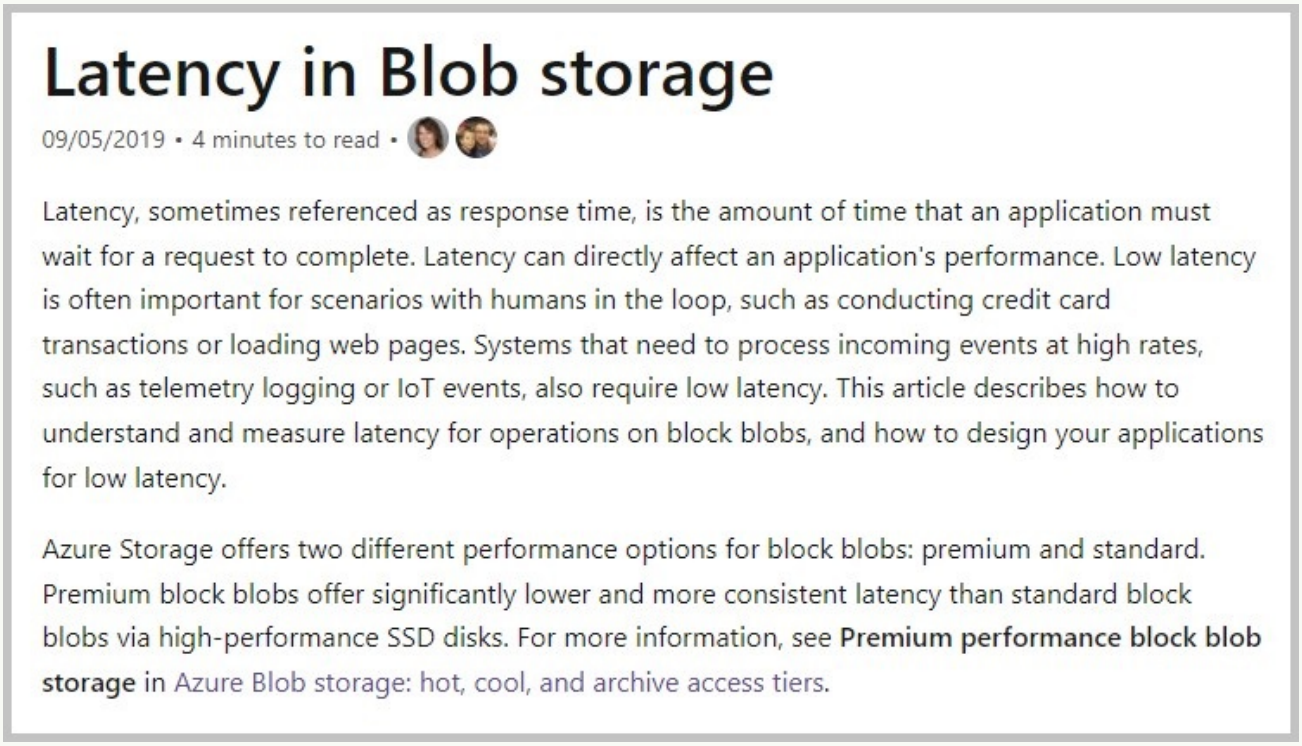
Only Premium block blobs offer significantly lower and more consistent latency.

Reference:

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

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

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



Latency in Blob storage

09/05/2019 • 4 minutes to read •

Latency, sometimes referenced as response time, is the amount of time that an application must wait for a request to complete. Latency can directly affect an application's performance. Low latency is often important for scenarios with humans in the loop, such as conducting credit card transactions or loading web pages. Systems that need to process incoming events at high rates, such as telemetry logging or IoT events, also require low latency. This article describes how to understand and measure latency for operations on block blobs, and how to design your applications for low latency.

Azure Storage offers two different performance options for block blobs: premium and standard. Premium block blobs offer significantly lower and more consistent latency than standard block blobs via high-performance SSD disks. For more information, see **Premium performance block blob storage** in Azure Blob storage: hot, cool, and archive access tiers.

62. Question

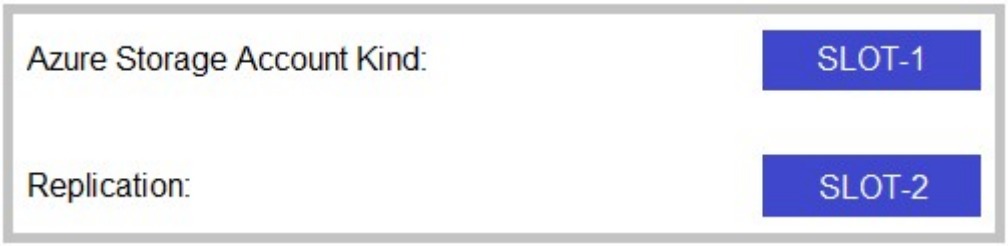
You plan to develop a new app that will store business critical data. The app must meet the following requirements:

? Prevent new data from being modified for one year.

? Minimize read latency.

? Maximize data resiliency.

You need to recommend a storage solution for the app.



Which of the following would go into Slot2?

- A. Zone-redundant storage (ZRS)
- B. Locally-redundant storage (LRS)

C. Read-access geo-redundant storage (RA-GRS)

Incorrect

Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. Immutable storage is available for general-purpose v1, general-purpose v2, premium block blob, and legacy blob accounts in all Azure regions.

Only Premium block blobs offer significantly lower and more consistent latency.

Only LRS & ZRS redundancy levels are available for premium performance blobs.

ZRS provides maximum data resiliency.

Reference:

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

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

Storage account overview

05/14/2021 • 6 minutes to read • +12

An Azure storage account contains all of your Azure Storage data objects: blobs, file shares, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. Data in your storage account is durable and highly available, secure, and massively scalable.

To learn how to create an Azure storage account, see Create a storage account.

Types of storage accounts

Azure Storage offers several types of storage accounts. Each type supports different features and has its own pricing model. Consider these differences before you create a storage account to determine the type of account that's best for your applications.

The following table describes the types of storage accounts recommended by Microsoft for most scenarios. All of these use the Azure Resource Manager deployment model.

Type of storage account	Supported storage services	Redundancy options	Usage
Standard general-purpose v2	Blob (including Data Lake Storage[1]), Queue, and Table storage, Azure Files	LRS/GRS/RA-GRS ZRS/GZRS/RA-GZRS[2]	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. Note that if you want support for NFS file shares in Azure Files, use the premium file shares account type.
Premium block blobs[3]	Blob storage (including Data Lake Storage[1])	LRS ZRS[2]	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency. Learn more about example workloads.
Premium file shares[3]	Azure Files	LRS ZRS[2]	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both SMB and NFS file shares.
Premium page blobs[3]	Page blobs only	LRS	Premium storage account type for page blobs only. Learn more about page blobs and sample use cases.

63. Question

You have an Azure subscription.

Your on-premises network contains a file server named Server1. Server1 stores 5 TB of company files that are accessed rarely.

You plan to copy the files to Azure Storage.

You need to implement a storage solution for the files that meets the following requirements:

? The files must be available within 24 hours of being requested.

? Storage costs must be minimized.

Which two possible storage solutions achieve this goal?

- [x] A. Create a general-purpose v2 storage account that is set to the Cool access tier. Create a file share in the storage account and copy the files to the file share
- [ ] **B. Create a general-purpose v2 storage account that is set to the Hot access tier. Create a blob container, copy the files to the blob container, and set each file to the Archive access tier**
- [ ] C. Create a general-purpose v1 storage account. Create a file share in the storage account and copy the files to the file share
- [x] **D. Create an Azure Blob storage account that is set to the Cool access tier. Create a blob container, copy the files to the blob container, and set each file to the Archive access tier**
- [ ] E. Create a general-purpose v1 storage account. Create a blob container and copy the files to the blob container

Incorrect

Question clearly asks for long term storage, retrieval in 24 hours and cheapest Other options wont satisfy. v1 cant be used so C&E options are gone. A is using Cool and File share which would be more expensive then Archive using Blob container.

Object storage data tiering between hot, cool, and archive is only supported in Blob storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don‘t support tiering. Blob storage and GPv2 accounts expose the Access Tier attribute at the account level. This attribute allows you to specify the default access tier for any blob that doesn‘t have it explicit set at the object level. For objects with the tier set at the object level, the account tier won‘t apply. The archive tier can be applied only at the object level. You can switch between these access tiers at any time.

Incorrect Answers:

A. Cool is cheaper then Hot, files are avail. for access within 24 hours. However archive tier would be even cheaper.

C. Doesn‘t mention anything about the access tier. I‘d rule it out.

E. Doesn‘t mention anything about the access tier. I‘d rule it out.

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs

https://docs.microsoft.com/en-us/azure/storage/blobs/archive-rehydrate-overview?tabs=azure-portal

Access tiers for Azure Blob Storage - hot, cool, and archive

03/18/2021 • 13 minutes to read • +17

Azure storage offers different access tiers, allowing you to store blob object data in the most cost-effective manner. Available access tiers include:

- **Hot** - Optimized for storing data that is accessed frequently.
- **Cool** - Optimized for storing data that is infrequently accessed and stored for at least 30 days.
- **Archive** - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.

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.

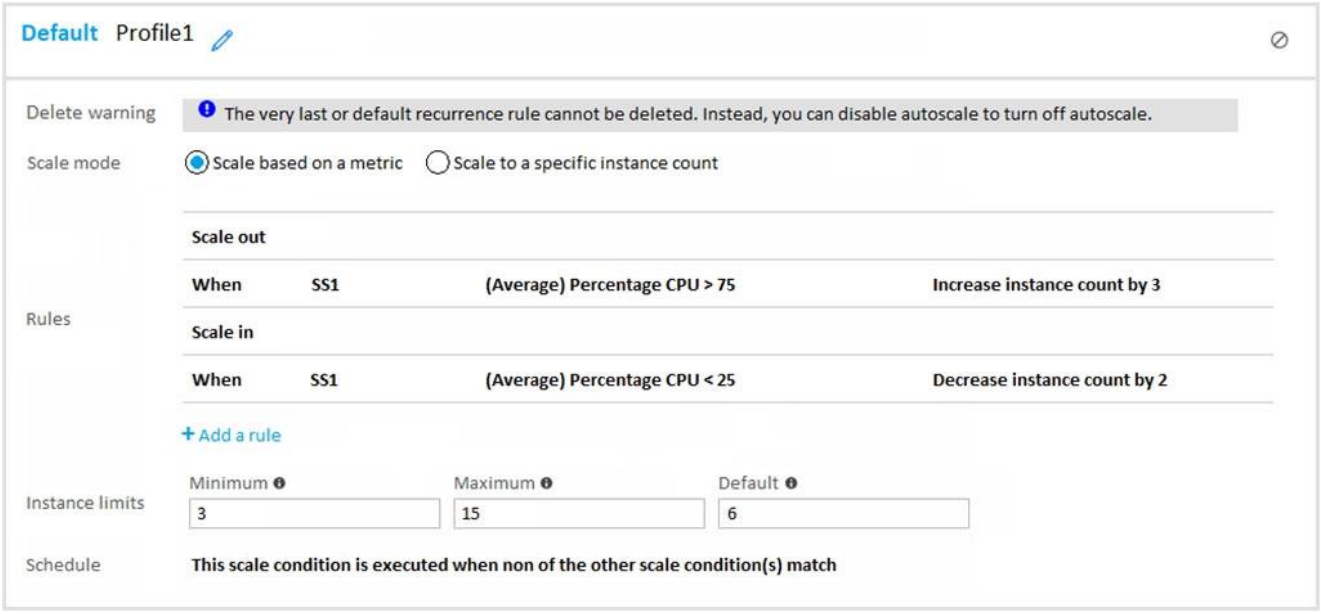
Rehydrating a blob from the archive tier can take several hours to complete. Microsoft recommends rehydrating larger blobs for optimal performance. Rehydrating several small blobs concurrently may require additional time.

You can configure Azure Event Grid to raise an event when you rehydrate a blob from the archive tier to an online tier and to send the event to an event handler. For more information, see Handle an event on blob rehydration.

64. Question

You have a virtual machine scale set named SS1.

You configure autoscaling as shown in the following exhibit.



You configure the scale out and scale in rules to have a duration of 10 minutes and a cool down time of 10 minutes.

If SS1 scales to nine virtual machines, what is the minimum amount of time before SS1 will scale out?

- A. 10 minutes
- B. 20 minutes
- C. 30 minutes
- D. 60 minutes

Incorrect

Duration does not wait for the cooldown to end. You can have multiple rules applied to the same autoscale rule with various cooldown times. You wouldn't want a rule to get skipped randomly because some other rule got triggered.

anirudhcavale commented on Oct 19, 2018 Contributor

@wgv-srsedate the way cool down works is as follows:
Let's say there are two rules in an autoscale setting

- Rule 1: Scale Up by 3 instances when CPU > 90%. Cool down = 10min
- Rule 2: Scale down by 1 instance when CPU < 30%. Cool down = 30min

Now let's play the scenario out:
12:00 - Autoscale runs and determines that CPU is 25% so it the scale down rule is triggered.
12:01 - Autoscale runs, CPU is 40%. No action
12:02 - Autoscale runs, CPU is 40%. No action
12:03-12:09 - Autoscale keeps running and determining that CPU is 25%. Rule 2 is satisfied, but its cool down says that it should not run within 30 min of the last scale operation. Last scale operation was not more than 30min ago. So no action taken.
12:10 - Autoscale runs CPU is 80%. No action.
12:11 - Autoscale runs CPU is now 93%. Rule 1 applies, and its cool down says that it should run within the 10min of the last scale operation. Last scale operation was more than 10min ago. So rule 1 can be executed. Scale up operation is initiated.

For Preview

Duration – The amount of time monitored before the metric and threshold values are compared. Does

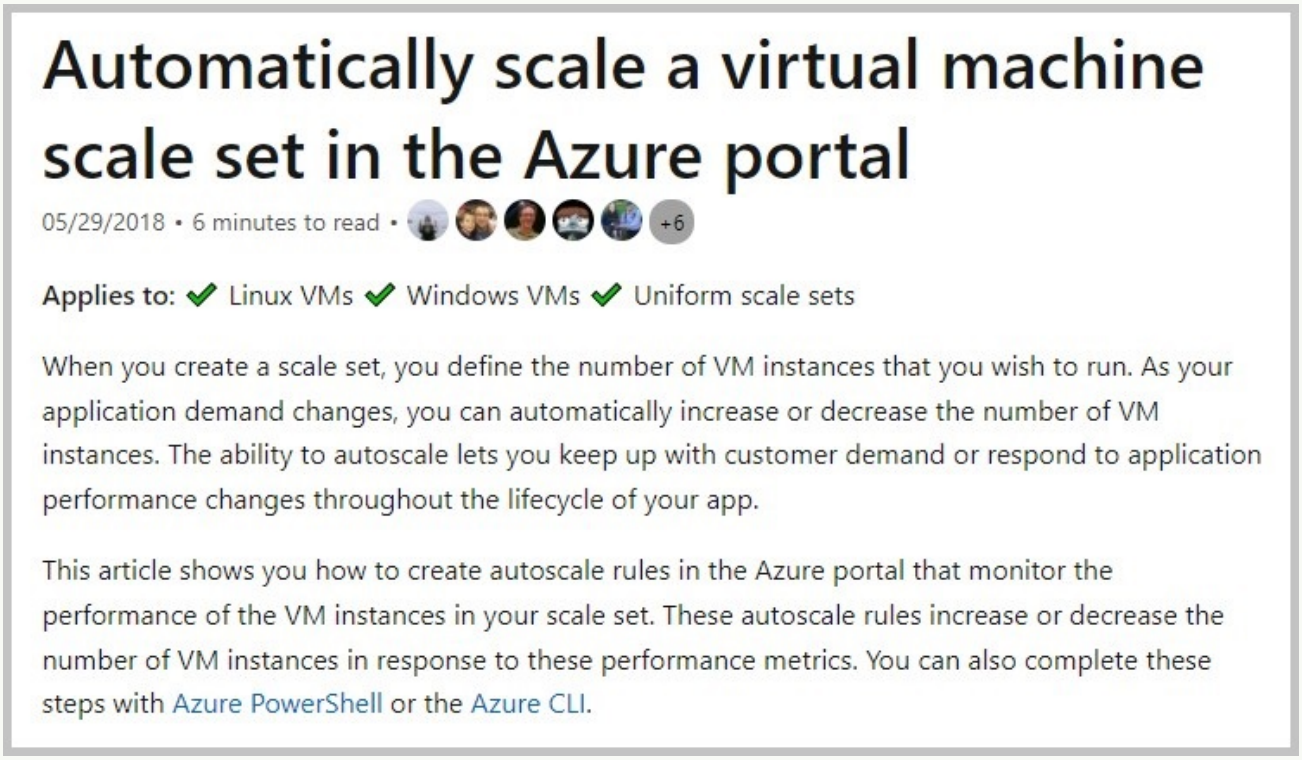
not include cool down period.

Cool down (minutes) – The amount of time to wait before the rule is applied again so that the autoscale actions have time to take effect.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-portal

https://github.com/MicrosoftDocs/azure-docs/issues/17169



Automatically scale a virtual machine scale set in the Azure portal

05/29/2018 • 6 minutes to read • +6

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

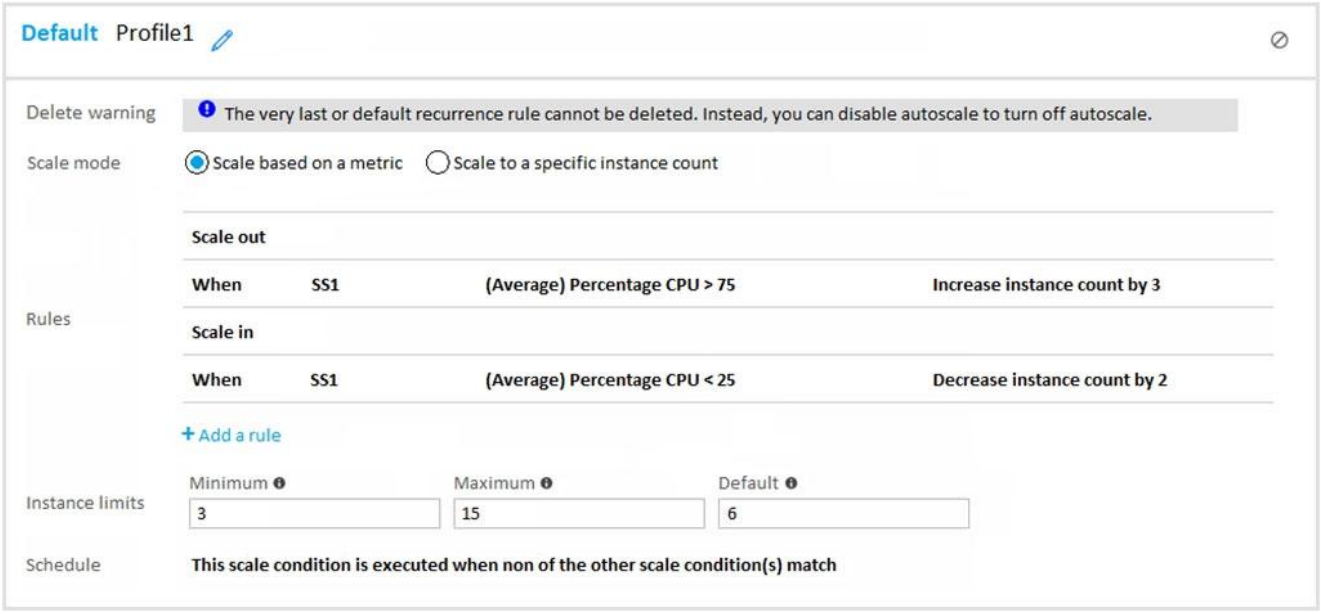
When you create a scale set, you define the number of VM instances that you wish to run. As your application demand changes, you can automatically increase or decrease the number of VM instances. The ability to autoscale lets you keep up with customer demand or respond to application performance changes throughout the lifecycle of your app.

This article shows you how to create autoscale rules in the Azure portal that monitor the performance of the VM instances in your scale set. These autoscale rules increase or decrease the number of VM instances in response to these performance metrics. You can also complete these steps with Azure PowerShell or the Azure CLI.

65. Question

You have a virtual machine scale set named SS1.

You configure autoscaling as shown in the following exhibit.



You configure the scale out and scale in rules to have a duration of 10 minutes and a cool down time of 10 minutes.

If SS1 scales to nine virtual machines, and then the average processor utilization is 30 percent for one hour, how many virtual machines will be in SS1?

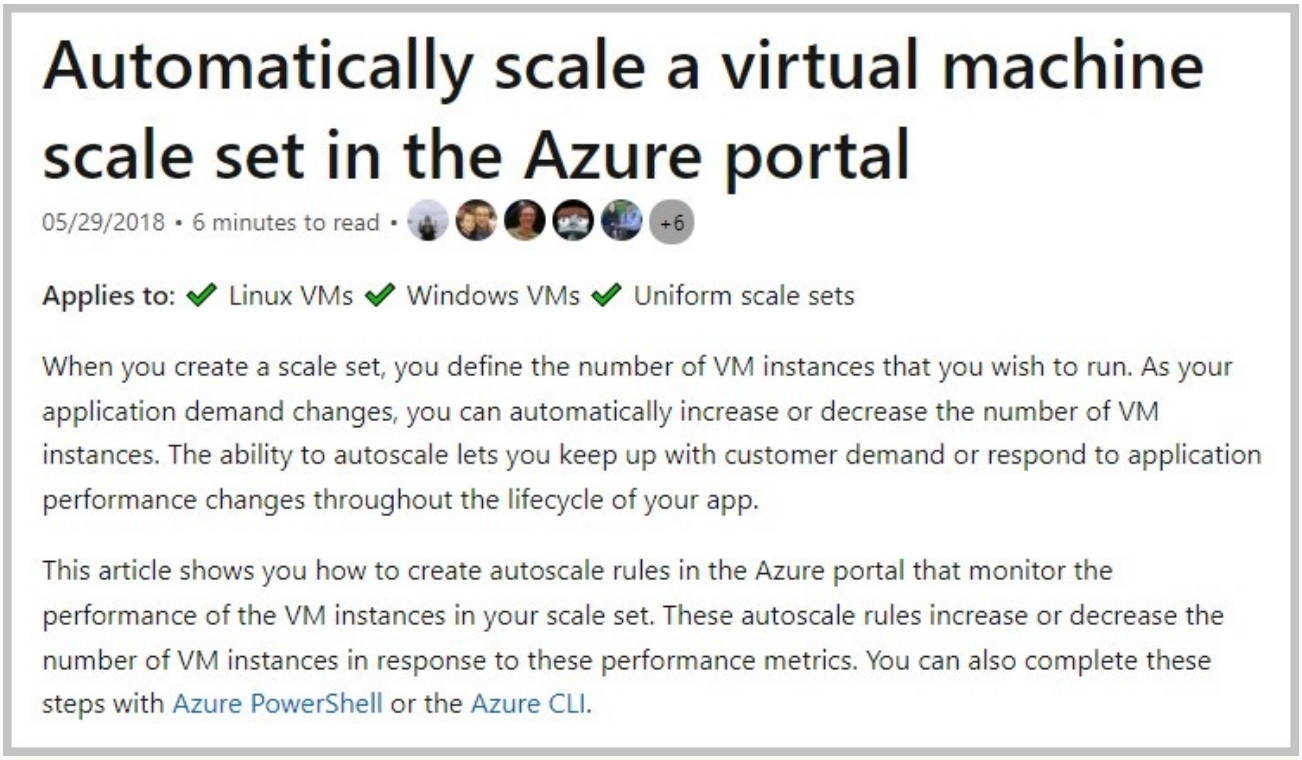
- 1
- 3
- 6
- 9
- 12
- 15

Correct

30% does not match the scale in requirement of less than 25% so the number of virtual machines will not change.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-portal



Automatically scale a virtual machine scale set in the Azure portal

05/29/2018 • 6 minutes to read • +6

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

When you create a scale set, you define the number of VM instances that you wish to run. As your application demand changes, you can automatically increase or decrease the number of VM instances. The ability to autoscale lets you keep up with customer demand or respond to application performance changes throughout the lifecycle of your app.

This article shows you how to create autoscale rules in the Azure portal that monitor the performance of the VM instances in your scale set. These autoscale rules increase or decrease the number of VM instances in response to these performance metrics. You can also complete these steps with Azure PowerShell or the Azure CLI.

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 →

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY