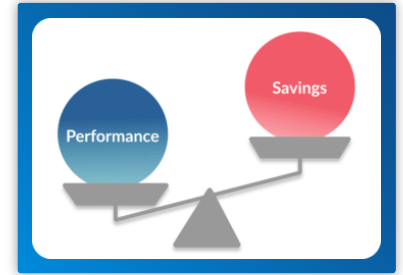


# CloudBolt Industry Insights Report: The DevOps Guide to Azure Costs

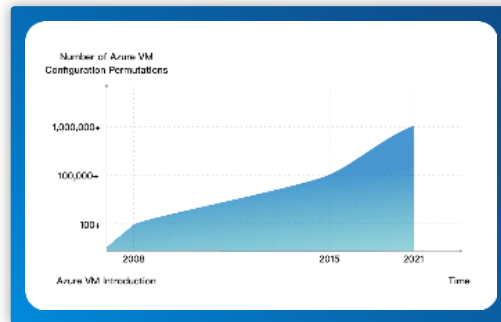


# Introduction

At CloudBolt, we get questions every day from advanced DevOps engineers and technical managers about how to best optimize Microsoft Azure cloud spending. As Azure administration experts, their questions aren't about the service functionalities but instead about the ever-expanding pricing models and the industry best practices to safely reduce their monthly bill without compromising service performance.

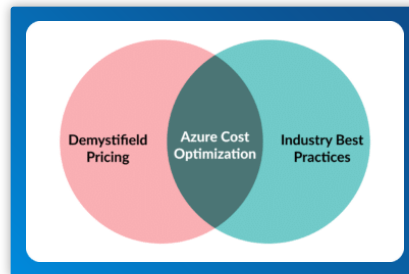


Public clouds gained popularity over the last decade mainly because of their simplicity and convenience; however, the basic Azure virtual machine gradually evolved to support multiple instance families, types, and versions, translating into hundreds of thousands of configuration permutations and purchasing plans. The resulting complexity confuses even the most experienced cloud administrators.



**There were over 1 million permutations as of the writing of this article**

In this guide, we clarify the pricing options, summarize the concepts into tables and diagrams, and share industry best practices for safely reducing your spending.



We have created this guide to publicly share our responses to the most common questions involving popular Azure concepts such as migration, storage, spot, reservations, and SQL pricing.



# Chapters

## Chapter 1: Azure Storage Pricing

Compare Azure storage types, storage accounts, and storage redundancy options to determine which combination works best for your organization.

## Chapter 2: Azure Reservations

Learn the difference between Azure's reserved instances and reserved capacity offerings, VMs vs dedicated hosts, and commitment discount ranges based on one and three year terms.

## Chapter 3: Azure Spot

Determine if your use cases are a good fit for Azure's Spot offering, its configuration options, and important VM limitations to consider.

## Chapter 4: Azure Migrate

Understand Azure Migrate Service's top four use cases and how your data gets replicated from VmWare, Physical Servers, and Hyper-V.

## Chapter 5: Azure SQL Pricing

Discover which of the many Azure SQL permutations is a best fit for both your budget and your workload needs.

## Chapter 6: Azure Backup Pricing

Understand how Azure backup is priced, how you can optimize your spending while using its services, and read about its best practices and limitations.

## Chapter 7: Azure Advisor

Find out how Azure Advisor implements Azure's well-architected framework concepts, learn its best practices, and understand its shortcomings.

## Chapter 8: Azure NSG

Learn about Azure Network Security Groups (NSG) capabilities, rule settings and enforcements, flow log best practices, and NSG's limitations and shortcomings.

# Chapter 1: Azure Storage Pricing

Microsoft Azure provides a variety of storage solutions for scaling your applications, service performance, and budget. Selecting which combination of solutions works best for you depends on your use case. In this article, we'll examine the major account and storage types offered by Azure along with high-level pricing information, so that you can begin planning with your storage needs in mind.

## Azure Storage Types

The following table lists the available Azure storage types that we will go over individually in the next several sections.

Storage Type	Description	Pricing
Azure Block Blobs	Scalable object storage for documents, videos, images, and unstructured text or binary data. There are 3 tiers to choose from Hot, Cool or Archive.	Prices for LRS Archive Block Blob with 3 years of reserved capacity start at \$0.00081 / GB per month.
Azure Data Lake Storage Gen2	Combines the power of a Hadoop-compatible file system (which uses an integrated hierarchical namespace) with the massive scale and economy of Azure Blob Storage.	Prices for LRS archive storage with 3 years of reserved capacity start at \$0.00081 / GB per month.
Azure Managed Disks	Persistent, secure disks that support easy and scalable virtual machine deployment; designed to achieve 99.999% availability.	Prices for standard managed disks start at \$1.54 per month.
Azure Files	Fully managed file shares in the cloud (accessible via standard Server Message Block (SMB) protocol) for applications using Windows APIs or REST API.	Prices for LRS file storage start at \$0.058 / GB per month.
Azure Page Blobs	Optimized for random read / write options that are ideal for overwriting small segments at a known address. Page blobs can be accessed via the REST protocol or attached to a VM to support disk traffic as unmanaged disks.	Prices for LRS file storage start at \$0.14 / GB per month.
Azure Table Storage	Offers NoSQL storage for unstructured and semi-structured data which is ideal for web applications, address books and other user data.	Prices for LRS file storage start at \$0.045 / GB per month.
Azure Queues Storage	Provides a reliable messaging solution for your apps and is generally used to store messages that are processed asynchronously; messages can be up to 64 KB in size.	Prices for LRS file storage start at \$0.045 / GB per month.

## Azure Block Blobs

Azure Block Blobs are efficient at uploading large amounts of data into blocks, identified using a Block ID. Block blobs may contain up to 50,000 blocks. Blocks can vary in size, however their size limit can be defined for the service version used to create or modify the blob. You can write a set of blocks via `put block`, commit blocks via `put block list`, and upload blobs less than the size specified by the service version via `put blob`.

## Azure Data Lake Storage Gen2

Azure Data Lake Storage Gen2 (DLSg2) is a set of big-data analytics functionalities that utilize Azure Blob storage functionality. Designed for servicing petabytes of information, DLSg2 provides file-system semantics and file-level security at scale. DLSg2 is foundational for building enterprise data lakes on Azure.

## Azure Managed Disks

Azure Managed Disks are essentially virtualized physical disks in the cloud, managed by azure, and used with Azure Virtual Machines. After you specify your disk size, type, and finally provision your disk, Azure handles the rest.

The types of disks available are:

- Ultra-disks
- Premium solid-state drives (SSD)
- Standard SSDs
- Standard hard disk drives (HDD)

## Azure Files

Azure Files are managed file shares that are accessible through either Server Message Block (SMB) protocol or Network File System (NFS) protocol.

Access Method	Supported Clients
SMB	Windows, Linux, macOS
NFS	Linux, macOS

With Azure Files, you can:

- Mount Azure Files concurrently by cloud or on-premise deployments
- Cache Azure Files on Windows Servers with Azure File Sync for fast access

## Azure Page Blobs

Azure Page Blobs are a section of 512-byte pages. These sections allow you to read/write random ranges of bytes, making them ideal for index-based storage and sparse data structures (e.g., OS, data disks for VMs, databases). Azure SQL DB uses Azure Page Blobs for persistent database storage.

## Azure Table Storage

Azure Table Storage houses non-relational structured NoSQL data using a schema-less design that relies on key/attribute storage. Because it's schema-less, adapting data to the needs of your application is easier. Table Storage is ideal for flexible datasets, like user data and metadata. A Table Storage account may contain any number of tables, and a table may contain any number of entities, up to the capacity limit of the storage account.

Generally, Azure Table Storage is fast and cost-effective, making it ideal for many types of applications in comparison to using traditional SQL for similar volumes of data.

## Azure Queues Storage

Azure Queue Storage bundles large numbers of messages (up to millions) into queues, which are accessible from anywhere in the world via authenticated HTTP/HTTPS calls. Messages can be up to 64KB in size; queues can take up to the maximum capacity limit of a storage account.

# Azure Storage Account

## What is Azure Storage Account?

Your [Azure Storage Account](#) will contain all of your blobs, files, queues, tables, and disks. Your Azure Storage assets are accessible via the unique namespace created for your account and contains all your Azure Storage data objects such as Blobs, Files, Queues, Tables and Disks. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. Data in your Azure Storage Account is durable, highly available, secure, and massively scalable.

## Types of Azure Storage Accounts

Azure offers different storage accounts, each with their own list of features and pricing models. It's important to understand the differences between these accounts before getting started with using Azure Storage for your own applications.

- **General-purpose v2 accounts:** A basic storage account type that supports blobs, files, queues, and tables. This account type is adequate for most use cases.
- **General-purpose v1 accounts:** A legacy account type that supports blobs, files, queues, and tables.
- **BlockBlobStorage accounts:** A premium performance account that enhances block blobs and append blobs. This account type is recommended for high-transaction-rate scenarios, smaller objects, and other scenarios requiring consistently low latency.
- **FileStorage accounts:** A storage account that supports files only, but with enhanced performance for enterprise-scale applications.
- **BlobStorage accounts:** A legacy account type that supports only blobs.

Storage account type	Supported services	Redundancy options	Deployment model
General-purpose V2	Blob, File, Queue, Table, Disk, and Data Lake Gen2	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Resource Manager
General-purpose V1	Blob, File, Queue, Table, and Disk	LRS, GRS, RA-GRS	Resource Manager, Classic
BlockBlobStorage	Blob (block blobs and append blobs only)	LRS, ZRS	Resource Manager
FileStorage	File only	LRS, ZRS	Resource Manager
BlobStorage	Blob (block blobs and append blobs only)	LRS, GRS, RA-GRS	Resource Manager

## Azure Storage Accounts Encryption

### What is Azure Storage Accounts Encryption?

Azure Storage Account Encryption is similar to BitLocker encryption on Windows and it is enabled for all storage accounts. This encryption uses 256-bit AES encryption, a FIPS 140-2 compliant block cipher. Encryption cannot be disabled; it is active by default without the need for modifying code or applications.

# Key Management Options for Azure Storage Encryption

Key management parameter	Microsoft-managed keys	Customer-managed keys	Europe (Frankfurt) Pricing
Encryption/decryption operations	Azure	Azure	Azure
Azure Storage services supported	All	Blob storage, Azure Files	Blob storage
Key storage	Microsoft key store	Azure Key Vault or Key Vault HSM	Customer's own key store
Key rotation responsibility	Microsoft	Customer	Customer
Key control	Microsoft	Customer	Customer

## Azure Storage Data Redundancy Options

There are several Azure Storage Data Redundancy options available.

- **Locally redundant storage (LRS):** Helps replicate data synchronously within the same datacenter for the lowest cost; is the least durable option.
- **Zone-redundant storage (ZRS):** Helps performance and enables synchronous data replication across up to three physically separate storage clusters in a single region.
- **Geo-redundant storage (GRS):** Helps replicate data to a far-off region.
- **Read-access geo-redundant storage (RA-GRS):** Helps replicate data to a far-off region, but allows read access to the secondary region (without a failover event).

Parameter	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
Object Durability per Year (%)	at least 99.999999999% (11 9's)	at least 99.999999999% (12 9's)	at least 99.9999999999999% (16 9's)	at least 99.9999999999999% (16 9's)
Read Availability	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)
Write Availability	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)
Total Data Copies	Three copies within a single region	3 copies across separate availability zones within a single region	6 copies total, including 3 in the primary region and 3 in the secondary region	6 copies total, including 3 across separate availability zones in the primary region and 3 locally redundant copies in the secondary region

## Redundancy Options vs Azure Storage Accounts

LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
General-purpose v2 General-purpose v1	General-purpose v2 Block blob storage	General-purpose v2 General-purpose v1	General-purpose v2
Block blob storage	File storage	Blob storage	
Blob storage			
File storage			

# Azure Storage Billing

Azure Storage space is charged based on storage capacity, storage transaction numbers, and the amount of data transferred. [Azure Storage fees](#) consist of below 3 key elements:

- 1. Bandwidth:** The transfer rate of data at the storage account's location. Managed services and their corresponding storage can be placed at the same location, providing free bandwidth between compute services and storage services. Pay only for access bandwidth usage when accessing the storage service outside of its location.
- 2. Transactions:** The number of requests executed on your storage account. RESTs requests are generated for every storage service (blob, table, and queue) and are considered billable.
- 3. Total capacity:** The sum of data in persistent storage. Azure totals the capacity of stored blobs, entities, messages, apps, and metadata to determine total capacity.

## Azure Storage Account Billing

Azure Storage is billed based on usage. Objects in an account are billed together; storage costs are calculated using these factors:

- **Region:** Your account's geographical region
- **Account type:** Your account's type
- **Access tier:** Your specified data-usage pattern (GPv2, Blob)
- **Capacity:** Your active total of stored data
- **Replication:** Your number of data copies
- **Transactions:** Your log of read and write operations
- **Data egress:** Your total outbound data transfer amount

## Azure Storage Best Practices to Optimize Costs & Security

There are a number of best practices for administering Azure storage systems. We have summarized the most important ones in the table below, and organized them by their main use case in three categories: Security, high availability, or cost savings.

Azure Storage Configuration Best Practices	Payment Option
Restrict shared access signature tokens to just HTTPS	Security
Check for lax stored access policies	Security
Check for public web containers	Security
Enable logging for Azure Storage Queue service	Security
Enable secure transfer in Azure storage	Security
Enable trusted Microsoft services for Storage Account access	Security
Limit Storage Account access by IP address	Security
Regenerate Storage Account Access keys periodically	Security
Restrict default network access for Storage Accounts	Security



Configure shared access signature tokens to expire	Security
Disable anonymous access to blob containers	Security
Use BYOK for Storage Account encryption	Security
Define content-type of each element	Security
Regularly review Storage Accounts that host static websites for security compliance	Security
Upload contents to Blob Storage in parallel	High Availability
Enable the Content Delivery Network for better availability	High Availability
Take snapshots to improve availability and caching	High Availability
Serve static contents directly from Blob Storage	High Availability
Enable blob storage lifecycle management	Cost Optimization
Enable immutable blob storage	Cost Optimization
Customize your soft deleted data retention period	Cost Optimization
Define the Cache-Control header for each element	Cost Optimization

## Conclusion

To recap, Microsoft Azure offers three main account types: general purpose, blockblob, and file storage accounts. Each type of account supports a variety of data redundancy options; all account types bill for storage space based on bandwidth, transactions (REST requests), and total used capacity. Billing groups similar objects and calculates fees based on factors like account type, region, and data egress.

# Chapter 2: Azure Reservations

For Microsoft, the concept of cost optimization is foundational to success in the cloud. As one of the five pillars of their [Microsoft Azure Well-Architected Framework](#), cost optimization as a practice encourages cloud administrators to adopt the process of build, measure, and learn.

That process would look something like this:

1. Review your cost principles.
2. Develop (or update) cost models, budgets, and spending alerts.
3. Measure and analyze your real-world resource consumption with the right set of KPIs.
4. Update your resource portfolio, consumption, and commitments.

These steps appear simple enough, however getting cost optimization right can be challenging for many reasons. One common challenge in particular is not fully understanding how Azure Reservations work. In this article, we'll explain all there is to know about Azure Reservations.

Let's get started.

## What are Azure Reservations?

Azure Reservations are pre-purchase commitments that reduce cloud consumption costs by reserving resources in advance. However, this pricing option does not apply to every resource on Azure. You can only leverage Azure Reservation discounts on a subset of virtual machines, app services, storage platforms, databases, or analytics services.

Microsoft splits Azure Reservations into two broad categories: Reserved Instances and Reserved Capacity.

- **Reserved Instances:** a pricing option for virtual machines
- **Reserved Capacity:** a set of discounts for Azure app, storage, and data services

## Reserved Instances

Azure Reserved Instances is a pricing option that allows you to reserve capacity on a subset of virtual machines for a period of one or three years. By committing and prepaying for the Azure virtual machine and compute component, you can reduce the cost by up to 72 percent. However, this discount only applies to your virtual machine cost—it does not apply to any pre-installed software, networking, or storage costs.

The table below details the inclusions and exclusions:

Resource Type	Included	Excluded
Reserved Virtual Machine Instance	Virtual machine and cloud services compute costs	Additional software, Windows, networking, or storage charges.
Azure Dedicated Host	Compute costs	Virtual machine, cloud services compute costs, additional software, Windows, networking, or storage charges.

## Reserved Instances Minimum Requirements

You can apply Reserved Instance pricing to both Windows and Linux virtual machines running on Azure. However, not every configuration is eligible for this discount. This pricing plan excludes virtual machines that form part of the A-series, Av2-series, and G-series. Any promotional virtual machines or images in preview are also ineligible.

## Reserved Instance Options

Reserved Instance Type	Savings vs Pay-as-You-Go
Windows VMs	Up to 80%
Linux VMs	Up to 72%

## Reserved Capacity

Reserved Capacity, like Reserved Instances, offers pricing discounts for pre-committing to services. The difference between the two offerings is the selected resources. Reserved Instances refers to a pricing plan that applies to virtual machines. Reserved Capacity covers everything else eligible for an Azure Reservation. Depending on the service and length of commitment, Reserved Capacity savings can range up to 65 percent. Azure also excludes individual components. Depending on the consumed service, you may still pay the full price for software, networking, and storage.

The table below details the inclusions and exclusions:

Resource Type	Redundancy options	Redundancy options
Azure Disk Storage reservations	Premium SSDs of P30 size or greater.	Other disk types or sizes smaller than P30.
Azure Storage reserved capacity	Standard storage accounts for Blob storage or Azure Data Lake Gen2 storage.	Bandwidth and transaction rates.
Azure Cosmos DB reserved capacity	Throughput.	Storage and networking.
SQL Database reserved vCore	SQL Managed Instance and SQL Database Elastic Pool/single database.	SQL license billed separately.
Azure Synapse Analytics	DWU usage.	Storage and networking.
Azure Databricks	DBU usage.	Compute, storage, and networking.
App Service stamp fee	Stamp usage.	Workers or any other resources associated with the stamp.
Azure Database for MySQL	Compute costs	Software, networking, and storage.
Azure Database for PostgreSQL	Compute costs.	Software, networking, and storage.
Azure Database for MariaDB	Compute costs.	Software, networking, and storage.
Azure Data Explorer	Markup charges.	Compute, networking, and storage.
Azure Cache for Redis	Compute costs.	Networking and storage.

## Reserved Capacity Minimum Requirements

Like Reserved Instances, Reserved Capacity is not a universal discount for all data services running on Azure. Microsoft applies Reserved Capacity pricing to data solutions running on a minimum of 8 vCores for SQL Databases or 20,000 Request Units (RUs) for Azure Cosmos DB. Reservation discounts on App Services are only available on the Premium V3 and Isolated tiers.

## Reserved Capacity Options

Reserved Instance Type	Savings vs Pay-as-You-Go
Azure SQL Database	Up to 80%
Azure Cosmos DB	Up to 65%
Azure Synapse Analytics	Up to 65%
App Service	Up to 55%
Azure Storage Reserved Capacity	Up to 38%

## Recommendations

### How recommendations are calculated

Azure's recommendation engine evaluates your hourly usage over the past 7, 30, and 60 days. Azure typically recommends selecting the quantity of reservations that maximizes your savings. Estimated costs are simulated both with and without reservations for comparison, and this calculation includes any special discounts you may have applied to your on-demand usage rates.

Recommendation quantity and savings are calculated for a 3-year reservation when available. If a 3-year reservation isn't purchasable, the recommendation is calculated using the 1-year reservation price. Recommendations available in Advisor consider your past 30-day usage trend.

### Other Considerations

- Recommendations are not provided for resources that are shut down regularly.
- Advisor has only single-subscription scope recommendations. If you want to see recommendations for the entire billing scope (which is billing account or billing profile), you can use Azure portal.
- Advisor recommendations for shared-scope reservations can take up to 5 days to disappear.
- You cannot save unused reserved hours for later, so if you do not have any qualifying resources in a given hour, then you lose the reservation quantity for that hour.

## Scope

Once you purchase an Azure Reservation, Microsoft automatically applies the discount to resources matching the reservation's options and quantity. It implements the discounted pricing to the scope you set during the purchase process; this could be a subscription, resource group, or single resource.

For example, reserving an instance and applying it to a resource group will use the Reserved Instance discount for any compute elements in that collection. Similarly, purchasing Reserved Capacity and setting the scope to the subscription will apply the discount to eligible Azure data services at that level.

Determining the scope and reservation to purchase requires analysis. Microsoft recommends you only buy a reservation after examining the consistent base usage of the identified resource. For virtual machines, MeterCategory, ServiceType, and ResourceLocation are metrics that provide the usage insight you need. Similarly, MeterCategory, MeterName, and MeterSubCategory help determine usage statistics for the Azure Synapse Analytics service.

In addition to analyzing usage data, Microsoft also provides resources that offer recommendations based on consumption patterns. The Azure Portal provides recommendations during the reservation purchase process. The VM BI Coverage report that forms part of the [Cost Management Power BI app](#) is another valuable resource that Enterprise customers can use. Azure Advisor, a built-in Azure service that analyzes configurations and usage telemetry, also offers reservation recommendations.

## Pricing

Depending on the service, Microsoft applies reservation pricing as detailed in the table below:

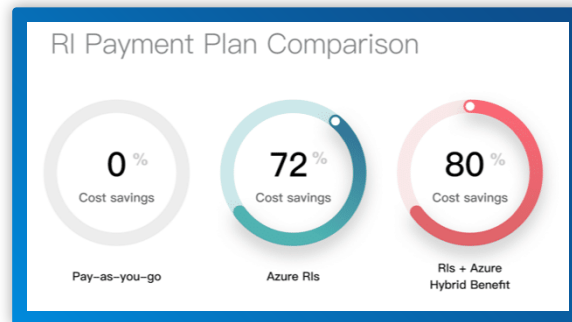
Resource Type	One Year Commitment	Three Year Commitment
Reserved Virtual Machine Instance	Up to 32% discount	Up to 72% discount
Azure Disk Storage reservations	Up to 5% discount	Not on offer
SQL Database reserved vCore	Up to 21% discount	Up to 33% discount
Azure Synapse Analytics	Up to 37% discount	Up to 65% discount
Azure Databricks	Up to 39% discount	Up to 61% discount
Azure Database for MySQL	Up to 42% discount	Up to 61% discount
Azure Database for PostgreSQL	Up to 39% discount	Up to 59% discount
Azure Database for MariaDB	Up to 42% discount	Up to 61% discount
Azure Cache for Redis	Up to 33% discount	Up to 65% discount
Azure App Service Premium V3	Up to 25% discount	Up to 40% discount
Azure App Service Isolated	Not on offer	Up to 40% discount

It is important to note reservation discounts work on a "use-it-or-lose-it" basis. Since the costing is measured per hour, if you do not have matching resources for that period, you forfeit the reservation quantity. Reserved hours cannot be carried forward or accumulated.

Leveraging Azure Reservations optimizes your cloud consumption cost. In addition to this primary benefit, there are other advantages in subscribing to this service. These include higher cost savings with the Azure Hybrid Use Benefit, payment flexibility, operational agility, and predictable budgeting and forecasting.

# Higher Cost Savings for Azure Hybrid Use Benefit

If you are an existing Microsoft Enterprise Agreement customer with Software Assurance, you can also get a further discount by leveraging the [Azure Hybrid Use Benefit \(HUB\)](#). Combining the reserve pricing discount with HUB can increase savings by up to 80 percent for virtual machines.



RI Payment Plan Comparison

## Pay Monthly or Annually

When signing up for Azure Reservations, the terms offer either a one or three year option. Even though it is a yearly contractual commitment, Microsoft gives you a choice to pay for your services monthly or annually. The cost per hour for either payment plan does not differ.

## Operational Agility

Even though reservation pricing refers to a particular resource, you set it to a specified scope. This configuration increases operational flexibility. For example, should you have two virtual machines in a scoped resource group, you can split the instance saving across identical resources. In this way, should you shut down the one virtual machine, you do not lose the reserved pricing benefit as Azure applies it to the other resource in the scope.

## Predictable Budgeting and Forecasting

One of the challenges many organizations face when migrating to Azure is estimating their forecasted expenditure. As Azure Reservations provide a fixed monthly or annual charge, it minimizes the potential unpredictability of Azure costing.

## Cancellations and Exchanges

Even though Azure Reservations commit you to a one or five-year term, Microsoft does give you the flexibility to cancel or exchange your prepayment engagement. However, depending on your commitment's remaining length and usage, the refund or credit differs. There is also a refund cap of \$50,000 and a termination fee of 12 percent in most instances.

The table below provided by Microsoft details the various scenarios.

Cancellation date (days)	Usage	Credit	Early termination fee	Refund cap
5 or fewer	No	100%	No	\$50,000 USD
5 or fewer	Yes	Prorated	No	\$50,000 USD
More than 5	No	Prorated	12%	\$50,000 USD
More than 5	Yes	Prorated	12%	\$50,000 USD

## Charges Covered by Azure Reservations

Azure Reservation	Charge Covered	Not Covered
Reserved Virtual Machine Instance	Covers virtual machine and cloud services compute costs.	Does not cover additional software, Windows licenses, networking, or storage charges.
Azure Storage reserved capacity	Covers storage capacity for standard storage accounts (Blob storage) or Azure Data Lake Gen2 storage.	Does not cover bandwidth or transaction rates.
Azure Cosmos DB reserved capacity	Covers your resources' provisioned throughput.	Does not cover the storage and networking charges.
SQL Database reserved vCore	Covers both SQL Managed Instance and SQL Database Elastic Pool/single database. Only compute costs are included.	Does not cover the SQL License (billed separately).
Azure Synapse Analytics	Covers cDWU usage.	Does not cover storage or networking charges associated with the Azure Synapse Analytics usage.
Azure Databricks	Covers only the DBU usage.	Does not cover compute, storage, and networking.
App Service stamp fee	Covers stamp usage.	Does not cover workers; all other resources associated with the stamp are charged separately.
Azure Database for MySQL	Covers the compute costs.	Does not cover software, networking, or storage charges associated with the MySQL Database server.
Azure Database for PostgreSQL	Covers the compute costs.	Does not cover software, networking, or storage charges associated with the PostgreSQL Database servers.
Azure Database for MariaDB	Covers the compute costs.	Does not cover software, networking, or storage charges associated with the MariaDB Database server.
Azure Data Explorer	Covers the markup charges.	Does not apply to compute, networking, or storage charges associated with the clusters.
Azure Cache for Redis	Covers the compute costs.	Does not cover networking or storage charges associated with the Redis cache instances.
Azure Dedicated Host	Covers the compute costs with the Dedicated host.	
Azure Disk Storage reservations	Covers premium SSDs of P30 size or greater.	Does not cover any other disk types or sizes smaller than P30.
SUSE Linux	Covers the software plan costs. The discounts apply only to SUSE meters.	Does not include VM usage.
Red Hat Plans	Covers the software plan costs. The discounts apply only to RedHat meters..	Does not include VM usage.
Azure VMware Solution by CloudSimple	Covers the VMware CloudSimple Nodes.	
Azure Red Hat OpenShift	Covers the OpenShift costs.	Does not cover Azure infrastructure costs.

# AWS Disaster Recovery Methods

Azure Reservations work well when you have a predictable usage pattern. If you know that you will be using a particular resource for an extended period, then an Azure Reservation is a perfect use case. Conversely, intermittent, scalable, or scheduled workloads are not suitable for reservations. For example, if you reserve a virtual machine instance but find that you need to shut it down regularly, then a Reserved Instance may not be the best option. This pricing model works well for servers that need to remain online such as domain controllers.

## Optimizing Your Reservation

If you find that your reservations are underutilized, there are several steps you could take to ensure you leverage the full benefit of your commitment.

### 1. Use Instance Flexibility

Reserved virtual machine instances give you the option to optimize instance size flexibility. This configuration allows you to apply the reservation to virtual machines in the same instance size flexibility group. For example, if you purchase a reservation for a Standard\_D5S\_v2 virtual machine, you could apply it to other virtual machines in the same tier, such as a Standard\_D1S\_v2.

### 2. Change the scope to shared

Changing the reservation from single scope to shared increases flexibility and use of the Azure Reservation as it will apply the discount to more resources.

### 3. Exchanges

If you cannot utilize the full benefit of your reservation, you could exchange it and use the credit to purchase a reservation for a better-suited resource.

## Conclusion

You can save up to 80% on your Azure purchases by committing to, or paying in advance for reserved instances and reserved capacity. You can save on your purchases of virtual machines, storage, database, analytics, and caching services, however the discounts won't apply to ancillary services associated with a reserved resource such as networking and bandwidth. If your plans change, Microsoft offers help in the form of instance flexibility, scope changes, and the option to exchange your reservations, however they are subject to refund caps and exchange fees. All things considered, at least a portion of your environment can always benefit from discounts offered by reservations without any considerable risk.



# Chapter 3: Azure Spot

## Azure Spot Virtual Machines

Cloud service providers need customers to consume as much compute capacity as possible to enhance their platform's efficiency. With price being a major contributing factor, they need an innovative costing model. One that drives high utilization and offers the vendor some flexibility. Azure Spot VMs is an Azure feature that provides this benefit. Its pricing delivers significant discounts to customers while giving Microsoft the agility it needs to rapidly reassign or reclaim resources on its public cloud platform.

### What is Azure Spot?

Azure Spot VMs is an Azure feature that allows you to take advantage of the platform's unused capacity. Using this option helps Microsoft drive efficiencies and realize the returns needed on their economies of scale. Subscribers get Azure Spot VMs at a significantly discounted rate for selecting this feature, making it a win-win for both parties. This option can help Azure customers lower their cloud computing costs up to 90 percent discount in some cases.

Pricing and eviction are the only differences between Azure Spot VMs and regular virtual machines. You will learn about evictions in this article. As far as performance, vCPU, memory, and network, the services are identical. Azure Spot VMs also offer the same security, scalability, and flexibility. You commission them on the same virtual network, protect them with Network Security Groups, and you can load balance and scale them using Virtual Machine Scale Sets. The core difference between Azure Spot VMs and regular virtual machines is uninterrupted availability. As you are getting a significant discount for consuming Azure's unused capacity, when Microsoft needs it back, they re-allocate the spot resources to customers paying full price. This is what is defined as Eviction.



Comparing Savings with Stability

### Use Cases for Azure Spot VMs

Although high-availability is not a core feature of Azure Spot VMs, other workload types pair very well with this consumption pricing model. The ideal use case for a Spot VM is a service or application where an interruption is acceptable. However, the workload selected must also not need to complete within a given timeframe.

### High-Performance Computing Scenarios

Suppose you have a workload that uses multiple CPU or GPU-based computers to solve complex mathematical algorithms. In that case, the Azure Spot VM pricing model is the perfect balance between performance and price. As these tasks typically involve long periods where users wait for calculations to complete, any interruption will not diminish the user experience. It may take a while longer, but as the user is not interacting with the service, the break will not impact production.

## Batch Processing Jobs

Like high-performance computing scenarios, batch processing jobs also fit the use case for Azure Spot VMs. These workloads follow the same approach where a workflow submits a task to a computing resource for execution. If these batch processing jobs take some time to complete, assigning them to an Azure Spot VM instance will lower the cost. As there is no interaction while the batch runs the process, an interruption will not impact your user's experience. As mentioned previously, if the batch run timing is mission-critical, commissioning a standard VM would be a better option.

## Dev/Test Environments

Another ideal use case for Azure Spot VMs is a development or test scenario. Typically, these environments do not require high-availability. They are also usually at the bottom of the critical list when it comes to IT budgets. Often organizations do not spin up development or test environments in the cloud to save cost. Legacy on-premise hardware is the usual location for these non-critical services. However, having these environments on-prem and your production on Azure is not ideal. Not only does it counter the best practice recommendation that all settings should be identical. It also creates unnecessary complexity in your DevOps environment when you need to deploy fixes or releases. By leveraging Azure Spot VM pricing, you can align development, test, and production while achieving a significant discount.

## Other Azure Spot VM Use Cases

In addition to the examples listed above, a few other workloads may make ideal candidates for Azure Spot VMs. However, depending on the service they host or process, you need to consider the impact should an interruption occur.

**Stateless:** Single-use, stateless applications like web servers that host static content are also candidates for Azure Spot VMs. However, depending on the hosted content, this use case may not be ideal. For example, if your public website consumes static content, you would not want visitors to experience your site without any CSS, images, or JavaScript. A more suitable use case would be a scenario where your development team needs to host these data types for a test environment.

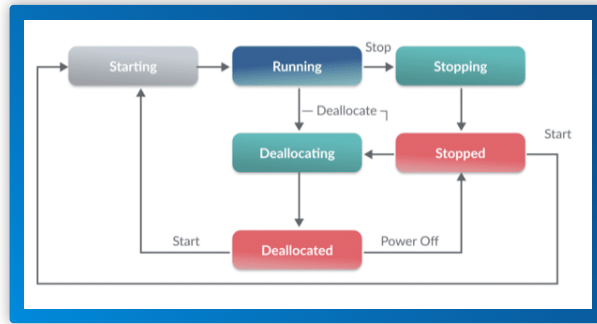
**Temporary Services:** In some instances, you may need to spin up a virtual machine for a short amount of time. If you are comfortable running the risk, a Spot VM may be a suitable candidate. Unfortunately, there is no way to predict if or when Azure may need its unused capacity back. For this usage scenario, the level of risk equals the amount of time you need the service online.

## Instance Configuration Options and Cost Optimizations

Azure Spot VMs can help you reduce your Azure compute spend by offering significant discounts for consuming unused capacity. However, in addition to this feature, they also help you save costs by setting a maximum price.

### Instance Configuration Options

A spot VM may be running, stopped, deallocated, or transitioning between two states. The diagram below summarizes the states that a spot VM may be in:



The transitions from state to state are managed by the configuration options. The table below provided by Microsoft details the various configuration options and the outcomes of each.

Option	Not Covered
Max price is set to $\geq$ the current price	VM deployed if capacity and quota are available.
Max price set to $<$ the current price	VM not deployed. You will get an error message that the max price needs to be $\geq$ current price.
Restarting a stop/ deallocate VM if the max price is $\geq$ the current price	If capacity and quota are available, then the VM is deployed.
The price for the VM has gone up and is now $>$ the max price	The VM gets evicted. You get a 30-second notification before actual eviction.
After the eviction, the price for the VM goes back to being $<$ the max price	Azure will not automatically restart the VM. You can restart the VM yourself, and Azure will charge it at the current price.
If the max price is set to -1	Azure will not evict the VM for pricing reasons. The maximum would be the price for standard VMs. Azure will never charge you above the standard price.
Changing the max price	You need to deallocate the VM to change the max price. Deallocate the VM, set a new max price, then update the VM.

## Eviction Options

When Azure evicts your Spot VM, the service will not notify you unless you opt-in to receive in-VM notifications via [Azure Scheduled Events](#). Should Microsoft need capacity, or the spot price exceeds the maximum price, the eviction process only gives you 30 seconds' notice. This minimal timeframe endorses the previous recommendations that you need to select the workloads you deploy on Azure Spot VM instances carefully.

When you configure an Azure Spot VM instance, you select the eviction type and policy during the virtual machine creation process. There are two eviction types.

## Eviction Types

**Capacity Only:** If you select this eviction type, Azure will only evict your VM when it needs capacity. In this instance, the Spot VM's maximum price is the regular price for a standard virtual machine on your subscription. As the price you pay for your VM may vary, this option is not ideal when you are working with a strict budget. However, the probability of Azure evicting your Spot VM is lower.

**Price or Capacity:** If you choose Price or Capacity as your eviction type, Azure will evict your VM when the spot price exceeds the threshold you set during the configuration phase. It will also evict it if it needs capacity. This eviction type is best suited for workloads that have a set budget. Consequently, it also has a higher eviction probability.

## Eviction Policies

The Azure Spot VM eviction policy dictates Azure's actions when your Spot VM exceeds the capacity or maximum price threshold. Currently, there are two configurable eviction policies: Stop/Deallocate and Delete. If you opt for the Stop/Deallocate option, you must bear in mind that Azure will still charge you for the disk storage. Azure Spot VM pricing only applies to the compute cost of the VM.

## Azure Spot VM Limitations

### VM Series Restrictions

The Azure Spot VM pricing model does not support every Azure virtual machine size. It excludes VMs configured to use the B-Series. Spot instance pricing is also not available for promotional VMs of any size, such as the Dv2, NV, NC, and H promo offers.

### Subscription Restrictions

All regular subscriptions offer Azure Spot VM pricing. However, this offer excludes any benefit or free subscriptions. These include Azure subscriptions linked to an MSDN or Partner agreement. Azure Spot VM pricing also excludes Microsoft's free Azure credit when you sign up as a new Pay-As-You-Go customer. Supported subscriptions include Enterprise Agreements, Pay-As-You-Go (after the credit has expired), and Cloud Service Provider.

### Technology Restrictions

Azure Spot VMs do not support ephemeral disks, which Azure creates on the local virtual machine storage. If you want to qualify for Spot VM pricing, you would need to configure your VM to use the standard Azure remote storage. The other technology restriction that applies to Azure Spot VMs is conversion. You cannot convert a Spot VM to a regular VM. Similarly, you cannot convert a regular VM to a Spot VM either. If you want to migrate your compute resources from spot to regular, or vice versa, you need to create a new VM and attach the existing disk.

### Auto Start Caveat

There is also an operational limitation when using an Azure Spot VM. When Azure stops and deallocates your virtual machine, it does not start up automatically when capacity returns. Even though you can opt-in to receive a notification using Azure Scheduled Events as mentioned earlier, you would still need to restart it manually. However, you could automate this manual process with PowerShell and utilize Azure Automation, a Function App, or a Logic App.

## Pricing Comparisons

Spot VM pricing differs for each region and SKU. If you opt for the Price or Capacity eviction type, the savings could be even lower, assuming that Microsoft accepts the price at the time and has the capacity.

VM Size	Resources	Regular Cost	Spot Cost	Savings
D2v3	2vCPUs 8GB	0.209 per hour	0.012 per hour	95%
D8sv3	8vCPUs 32GB	0.836 per hour	0.108 per hour	87%
D2v4	2vCPUs 8GB	0.204 per hour	0.012 per hour	95%
D8sv4	8vCPUs 32GB	0.816 per hour	0.488 per hour	60%
E4sv4	4vCPUs 32GB	0.464 per hour	0.032 per hour	94%
E8sv4	8vCPUs 64GB	0.928 per hour	0.064 per hour	94%
F4sv2	4vCPUs 8GB	0.396 per hour	0.068 per hour	83%
F8v2	8vCPUs 16GB	0.792 per hour	0.137 per hour	83%

The table above clearly illustrates the significant cost savings achievable with Azure Spot VM instances. However, the discount does vary between region and SKU, so you must perform the necessary due diligence before committing.

## Cost Saving Versus Increased Risk

Azure Spot VM cost optimization and configuration selection is a trade-off between cost and risk. Considering these scenarios, optimizing cost using Azure Spot VMs requires careful consideration of three factors: the type of workload, budget restrictions, and the acceptable level of risk.

As the potential cost of a Spot VM changes continuously, setting a budget before configuring is important. If you opt for the capacity eviction type, you need to monitor the total spend as costs fluctuate. With the maximum cost option, you fix your budget upfront. However, the total cost depends on the Azure Spot VM price when you commission your virtual machine. Both eviction types also carry a varying level of risk. Depending on the workload, you will need to take the eviction probability and its impact on your organization into account.

# Chapter 4: Azure Migrate

## The Azure Migrate Service, Explained

Initially, the Azure Migrate Service offering focused on enabling users to discover and migrate to VMware virtual machines, Hyper-V virtual machines, and on-premise servers. Today, the Azure Migrate Service has evolved to accommodate more than just "lift-and-shift migration" projects. For example, the service now allows you to migrate workloads to the Azure Platform as a Service in what is known as a "replatforming migration."

### Azure Migrate's Top 4 Use Cases

- **Server Assessment:** Discover and assess on-premises VMware VMs, Hyper-V VMs, and physical servers in preparation for migration to Azure.
- **Server Migration:** Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized machines, and public cloud VMs to Azure.
- **Azure Database Migration Service:** Can help you replatform your MSSQL, Postgres, and MySQL databases to Azure PaaS databases.
- **Web app migration assistant:** Can help you replatform your website that resided on IIS to [Azure App Service](#).

Although it is becoming less common to use tools that are not integrated with the Azure Migrate offering, some worth noting are: [Movere](#), which was acquired by Microsoft for server migrations, and [Azure Data Box](#), which helps move massive amounts of data to Azure.

### How Azure Migrate Service Helps

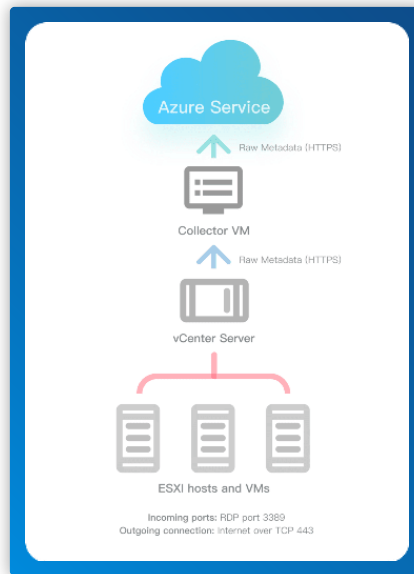
The Azure Migrate Service helps you with your migration projects using the following steps:

1. Azure first acquires your data and begins testing
2. Azure then identifies any blockers for migrations (both via lift-and-shift and replatforming)
3. Azure finally performs the final migration on your behalf

In some scenarios, Azure Migrate can do a performance-based sizing, which provides cost estimations for running your on-premises machines in Azure. After the assessment, you can use services such as [Azure Site Recovery \(ASR\)](#) and [Azure Database Migration Service](#), to migrate the machines to Azure.

### The Architecture of Azure Migrate Service

When choosing the replatforming method for a migration project, you must install a VM "collector appliance" to help Microsoft discover information about your on-premises machines. This appliance collects VM metadata using various methods (e.g., VMware PowerCLI cmdlets) and discovery is agentless. Collected metadata includes information from resource cores, memory, disks, disk sizes, and network adapters.



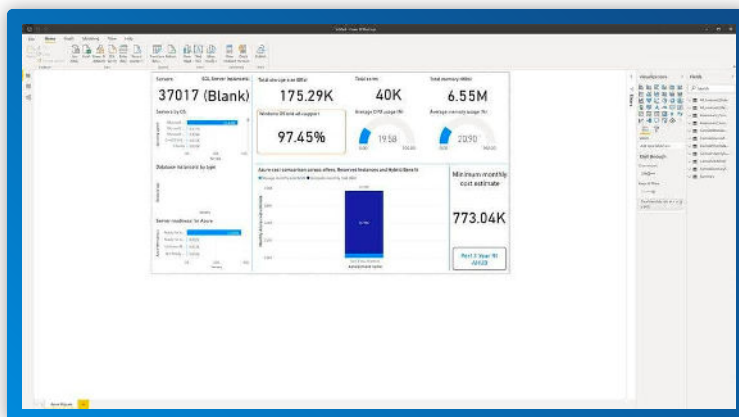
**Azure Migrate Service Flow**

After performing an inventory check for all of your websites and databases, if any blockers are identified, it is then up to you and your team to resolve those issues. A replatforming migration cannot occur without those blockers being resolved. Alternatively, you can proceed via the lift-and-shift migration option, which is much more complicated but enables you to migrate all datacenters to Azure in replication stages.

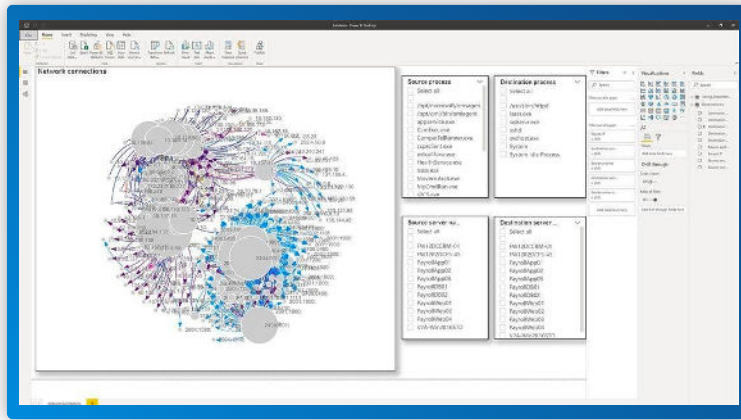
## Grouping and Visualization in Azure Portal

All of the data transferred into your Azure Migrate project can be viewed from the Azure Portal. From there, you can organize the discovered VMs into groups. Groups provide visualizations of the dependencies for any one machine or for all machines within the group. Once a group is formed, you create an assessment for the group.

After the assessment finishes, you can view it in the portal, download it in Excel format, or use [PowerBI](#) dashboards, like the one shown below:



**Dashboard Visualization From PowerBI**



**Network Connections Visualization From PowerBI**

## Detailed Reports

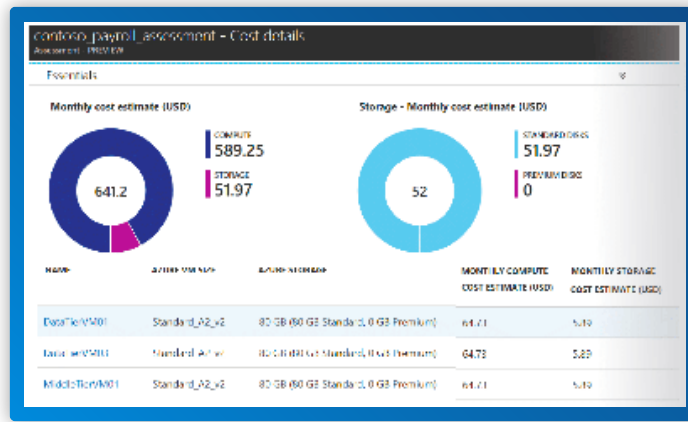
Azure Migrate sends detailed reports on the state of the migration, including potential blockers and any relevant recommendations for what to do next.

The following is an example of a reported configuration error:

```
HRESULT=800700B7,
  Action=reading_config_section,
  SectionSchemaName=system.codedom,
  AttributeName=,
  Message=Filename: \\\?
  \\\C:\\\\inetpub\\vhosts\\app.example.com\\web.config\r\n
  Line number: 122\r\nError: Cannot add duplicate collection entry of type 'compiler' with
  combined key attributes 'language, extension' respectively set to '#;cs;csharp, .cs\r\n\r\n';
  HRESULT=8007000D,
  Action=reading_config_section,
  SectionSchemaName=system.net/mailSettings/smtp,
  AttributeName=,
  Message=Filename: \\\?
  \\\C:\\\\inetpub\\vhosts\\app.example.com\\web.config\r\nLine number: 108\r\nError:
  Unrecognized attribute 'enableSsl'\r\n\r\n
```

For massive scale data center migration, you can also review consolidated reports, like the one shown below:



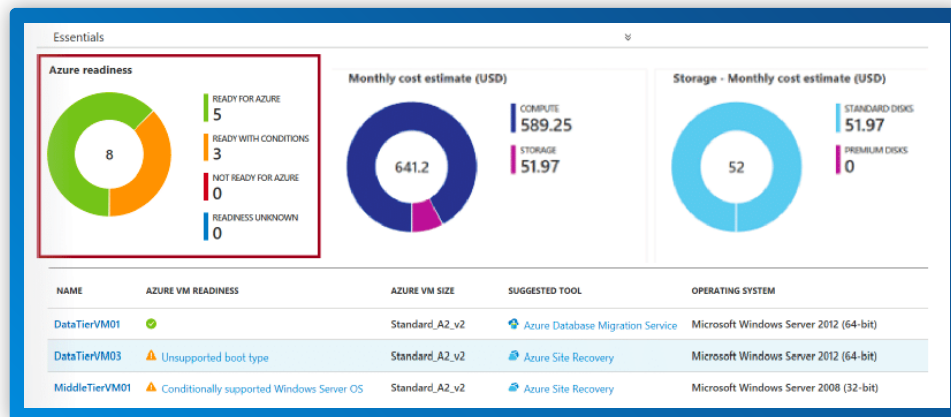


**Consolidated Report Example**

## Grouping and Visualization in Azure Portal

You can review the readiness of your resources for migration by checking the Azure Readiness view. The most important statuses to pay attention to are: "Ready with conditions" and "Not ready for Azure." For these VMs, Azure Migrate explains what the issues are and provides remediation steps.

Azure Migrate considers several data points when making this determination, such as: boot type, cores, memory, storage disks, networking components, and operating system.



**Azure Readiness Visualization**

## Azure Site Recovery

After the assessment comes the migration. In the case of PaaS Services, this simply means taking the next step of the setup wizard. VMs and physical servers get migrated to Azure Site Recovery, by replicating your VMs.

Let's first take a look at the service architecture of Azure Site Recovery which help perform the replication, before we examine any replication steps.

# Site Recovery Service Architecture

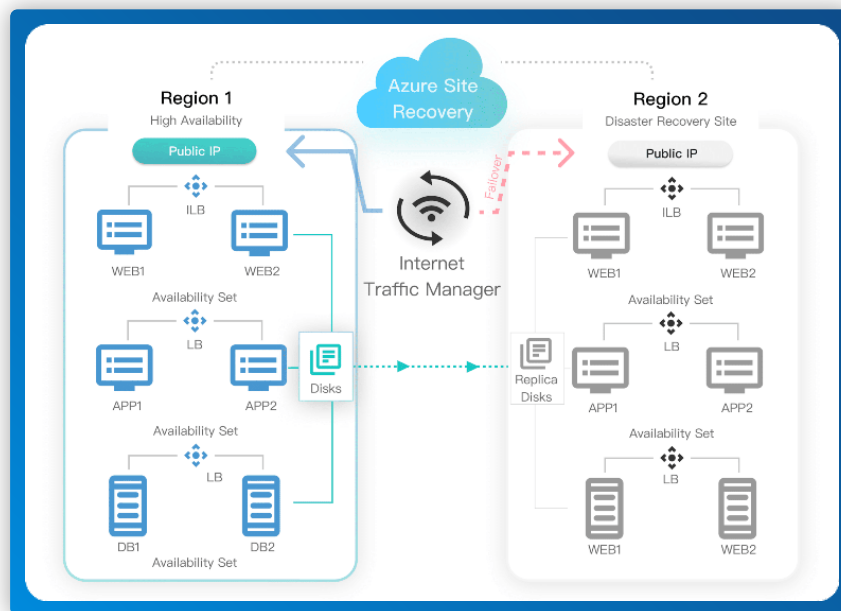
The following components make up the Azure Site Recovery Service:

- **Configuration server:** Coordinates communications between on-premises servers and Azure; also manages data replication.
- **Process server:** Receives and optimizes replication data with caching, compression, encryption, and sends it to Azure storage; acts as a replication gateway.
- **Master target server:** Handles replication data during failback from Azure (not necessary in Migration Scenario).
- **Mobility Service:** Captures and forwards data-writes on a given machine to the process server.

Mobility Service can only be installed on 64-bit systems and supported Linux Systems (e.g., Debian, CentOS, Ubuntu). The Mobility Service does not support Dynamic Raid 1 disks in Windows; Secure Boot is also not fully supported. For more information, refer to this [Azure guide](#).

## Replication

The final step in your Azure Migrate journey is replication, which occurs when source machines are working properly. Replication can be controlled from the Azure Portal, PowerShell Scripts, or via the Azure API.



Replication Flow

The replication process differs based on what is being replicated.

## Replicating VMware & Physical Machines

Dedicated machines (process servers) are required for VMware and physical machines to receive information about VMs (e.g., disk sector changes) and push that information to Azure. A Mobility Agent must be installed on every source VM; for mass scaling, the agent can be provisioned automatically.

## High-level Site Recovery Steps

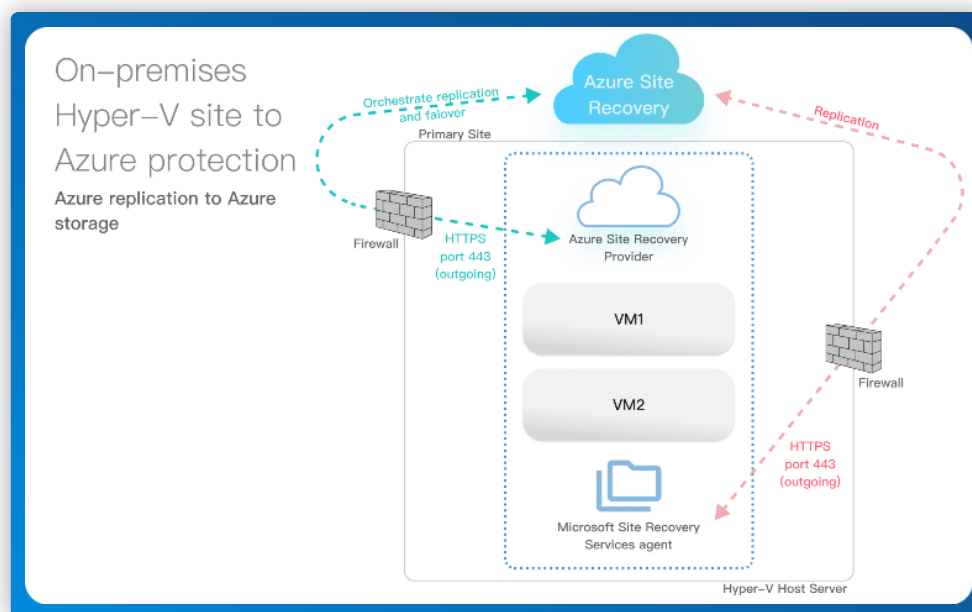
1. Download the Vault Registration Key
2. Install Process Server
3. Write Passphrase
4. Add Account to VM, Physical Servers, vCenter, or ESXi
5. Install Mobility Service on Every VM and/or physical server

## Replicating Hyper-V

Microsoft Azure Site Recovery Provider is needed for Hyper-V recovery preparation. Replication is based on the Hyper-V Replica subsystem and also works on Hyper-V Free servers and/or Core Servers. Hyper-V does not require a Mobility Agent, making it less complex to scale.

## High-level Site Recovery Steps

1. Download the Vault Registration Key
2. Install Azure Site Recovery Provider



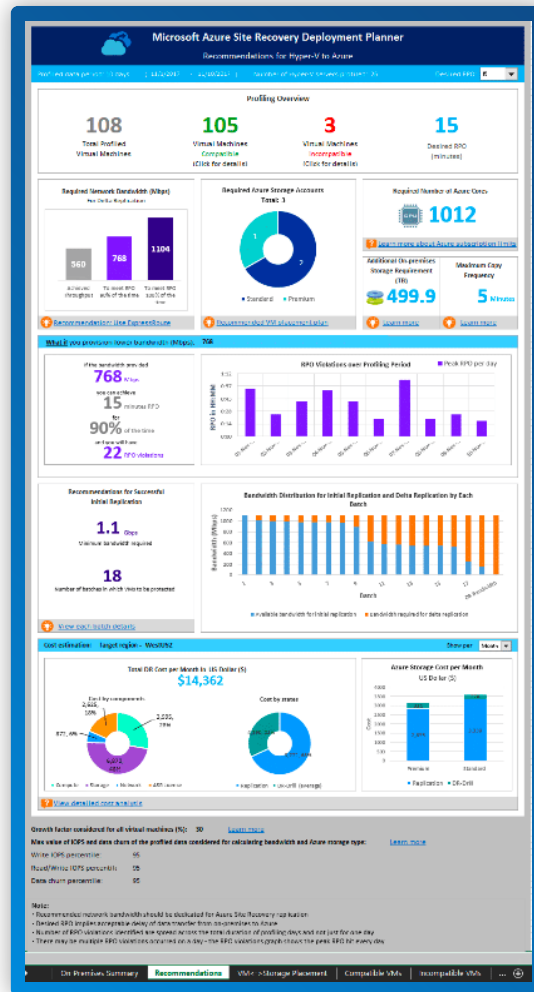
Hyper-V Replication Flow

## Site Recovery Deployment Planner

The Azure Site Recovery Deployment Planner is a dedicated command-line tool for gathering planning information that is compatible with Hyper-V and VMware servers. This deployment planner generates an Excel report containing the following information:

- On-premises summary
- Recommendations
- VM storage placement
- Compatible VMs

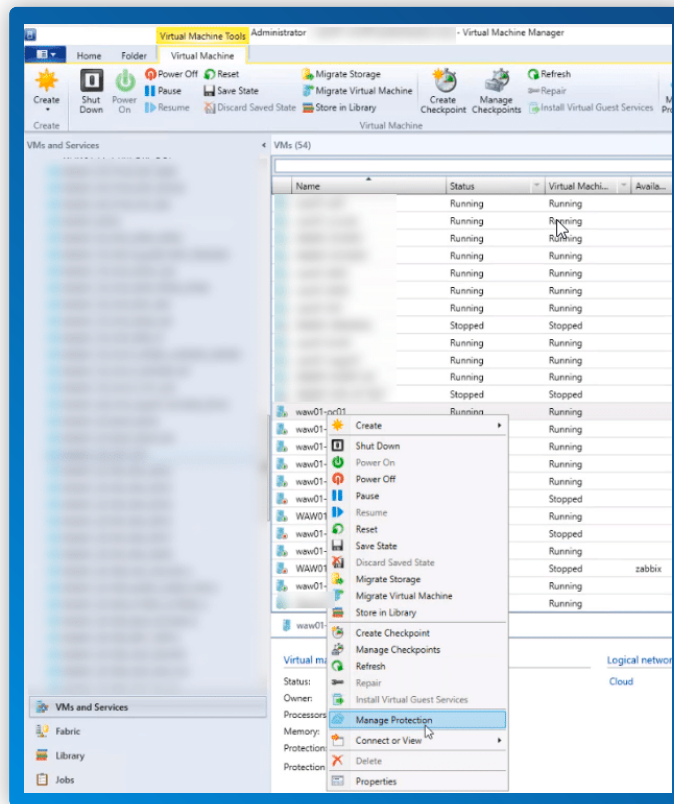
- Incompatible VMs
- On-premises storage requirement
- Initial Replication batching
- Cost estimation



Deployment Planner Visualization

## Site Recovery with Virtual Machine Manager

Virtual Machine Manager (SCVMM) is designed for the management of large numbers of Virtual Servers based on Microsoft Virtual Server and Hyper-V. SCVMM helps utilize Azure Site Recovery on a massive scale, even from GUI.



**Virtual Machine Manager**

## Conclusion

Azure Migrate is certainly worth checking out, especially considering that the service is free. Moreover, we recommend doing the Assessment, especially for your databases (even if you do not plan any migration). Why? Because not only is Azure Migrate a great inventory tool, it's also useful for generating database reports to detect orphaned resources (e.g., stored procedures that no longer work due to missing query tables).

Even when your architecture is not eligible for a replatforming migration, lift-and-shift migration remains an option. This can be a sensible approach for the smallest systems or a temporary solution if there is a strong business reason forcing you to leave the data center. However, it should be understood that this approach will not take advantage of any of the benefits of the cloud and will likely cost more. Lift-and-shift migrations are essentially lateral moves where the systems move from a data center, as is, to the cloud. While your architecture remains unchanged. If you would like to take advantage of auto-scaling and fault tolerance in the cloud, then replatform or even re-architecting would be recommended.

# Chapter 5: Azure SQL Pricing

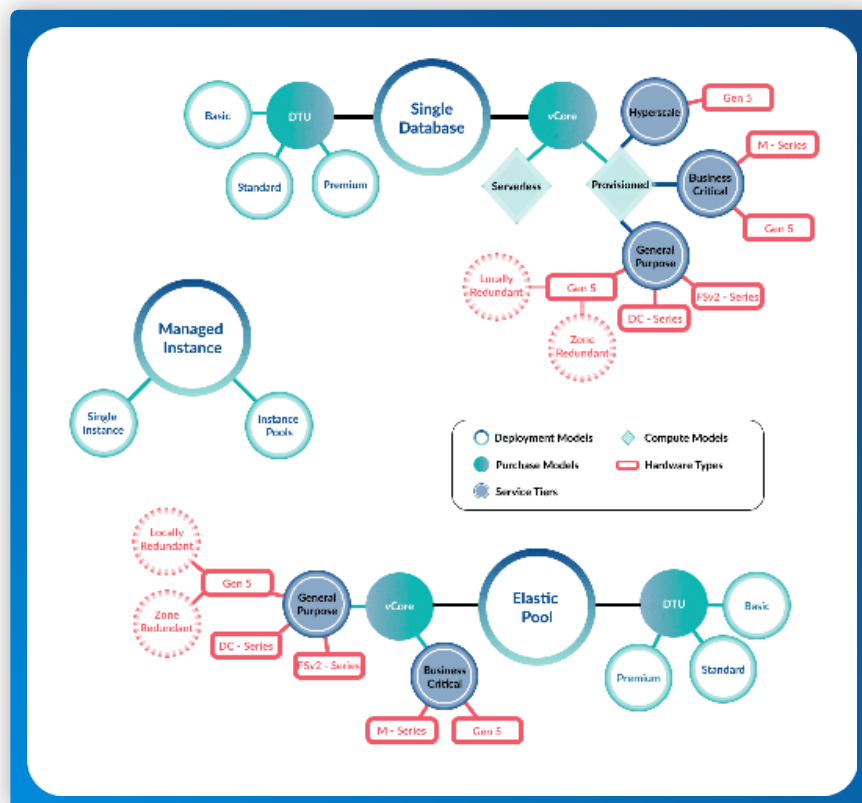
In the first half of this article, we'll present complete Microsoft Azure SQL Database pricing options in a tabular format – and we'll explain the concepts behind the pricing along with administrative best practices in the second half.

Microsoft Azure SQL Database is offered as part of Microsoft Azure's public cloud platform, and allows developers to utilize an intelligent and scalable relational database service. It conforms to all the characteristics of a genuine cloud service, one being that you only have to pay for what you use.

## Azure SQL Pricing

Estimating Microsoft Azure SQL Database pricing can be challenging due to the multiple configurations available. For illustration, consider the following options to get an idea of how many permutations there are:

- **2 purchase models:** DTU (Database Transaction Unit), vCore (Virtual Core)
- **3 deployment models:** Single Database, Elastic Pool, Managed Instance
- **3 service tiers:** General Purpose, Business Critical, Hyperscale
- **2 compute models:** Provisioned, Serverless
- **4 hardware types:** Gen 5, DC-Series, Fsv2-series, M-Series



Map of Available Options for Azure SQL

The number of choices available can be overwhelming at first. We recommend starting your cost optimization exercise by first starting with what your requirements are. Once you have a clear understanding of what you need, you can use the [Azure SQL Database pricing page](#) filter shown in the following image to narrow down the various options.

Single database Elastic pool

Single database offers provisioned compute and serverless compute tier choices.

Purchase Model: vCore  
 Compute Tier: All  
 Service Tier: All  
 Hardware Type: All

Region: West US 2  
 Currency: US Dollar (\$)   
 Display pricing by: Hour

### Hyper-V Replication Flow

## Azure SQL Database Single Database Pricing

### DTU Pricing

Service Tier	Name	DTUs	Included Storage	Max Storage	Price per Hour
Basic	B	5	2 GB	2 GB	\$0.0068/hour
Standard	S0	10	250 GB	250 GB	\$0.0202/hour
Standard	S1	20	250 GB	250 GB	\$0.0404/hour
Standard	S2	50	250 GB	250 GB	\$0.1009/hour
Standard	S3	100	250 GB	1 TB	\$0.2017/hour
Standard	S4	200	250 GB	1 TB	\$0.4033/hour
Standard	S6	400	250 GB	1 TB	\$0.8066/hour
Standard	S7	800	250 GB	1 TB	\$1.6130/hour
Standard	S9	1,600	250 GB	1 TB	\$3.2260/hour
Standard	S12	3,000	250 GB	1 TB	\$6.0488/hour
Premium	P1	125	500 GB	1 TB	\$0.6251/hour
Premium	P2	250	500 GB	1 TB	\$1.2500/hour
Premium	P4	500	500 GB	1 TB	\$2.5000/hour
Premium	P6	1,000	500 GB	1 TB	\$5.0000/hour
Premium	P11	1,750	4 TB	4 TB	\$9.4088/hour
Premium	P15	4,000	4 TB	4 TB	\$21.5054/hour

# vCore Provisioned Compute Pricing

## Gen 5 Hardware Type

vCore	Memory	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour	Hyperscale Cost per Hour
2	10.2 GB	\$0.5044/hour	\$0.6871/hour	\$1.3589/hour	\$0.5653/hour
4	20.4 GB	\$1.0088/hour	\$1.3741/hour	\$2.7178/hour	\$1.1306/hour
6	30.6 GB	\$1.5131/hour	\$2.0611/hour	\$4.0767/hour	\$1.6958/hour
8	40.8 GB	\$2.0175/hour	\$2.7482/hour	\$5.4355/hour	\$2.2611/hour
10	51.0 GB	\$2.5219/hour	\$3.4352/hour	\$6.7944/hour	\$2.8263/hour
12	61.2 GB	\$3.0262/hour	\$4.1222/hour	\$8.1533/hour	\$3.3916/hour
14	71.4 GB	\$3.5306/hour	\$4.8092/hour	\$9.5121/hour	\$3.9568/hour
16	81.6 GB	\$4.0350/hour	\$5.4963/hour	\$10.8710/hour	\$4.5221/hour
18	91.8 GB	\$4.5393/hour	\$6.1833/hour	\$12.2299/hour	\$5.0873/hour
20	102.0 GB	\$5.0437/hour	\$6.8703/hour	\$13.5887/hour	\$5.6526/hour
24	122.4 GB	\$6.0524/hour	\$8.2444/hour	\$16.3065/hour	\$6.7831/hour
32	163.2 GB	\$8.0699/hour	\$7.7936/hour	\$21.7420/hour	\$9.0441/hour
40	204.0 GB	\$10.0874/hour	\$13.7406/hour	\$27.1774/hour	\$11.3051/hour
80	396.0 GB	\$20.1747/hour	\$27.4811/hour	\$54.3548/hour	\$22.6101/hour

## DC-series Hardware Type

vCore	Memory	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour	Hyperscale Cost per Hour
2	9 GB	\$0.8830/hour	Not Available	\$2.116/hour	\$1.8400/hour
4	18 GB	\$1.7659/hour	Not Available	\$4.233/hour	\$6.9599/hour
6	27 GB	\$2.6498/hour	Not Available	\$6.349/hour	\$15.3598/hour
8	36 GB	\$3.5328/hour	Not Available	\$8.466/hour	\$27.0318/hour

## Fsv2-series Hardware Type

vCore	Memory	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour	Hyperscale Cost per Hour
8	15.1 GB	\$1.8684/hour	Not Available	Not Available	Not Available
10	18.9 GB	\$2.3355/hour	Not Available	Not Available	Not Available
12	22.7 GB	\$2.8026/hour	Not Available	Not Available	Not Available
14	26.5 GB	\$3.2697/hour	Not Available	Not Available	Not Available
16	30.2 GB	\$3.7368/hour	Not Available	Not Available	Not Available
18	34.0 GB	\$4.2039/hour	Not Available	Not Available	Not Available
20	37.8 GB	\$4.6710/hour	Not Available	Not Available	Not Available



24	45.4 GB	\$5.6052/hour	Not Available	Not Available	Not Available
32	60.5 GB	\$7.4735/hour	Not Available	Not Available	Not Available
36	68.0 GB	\$8.4077/hour	Not Available	Not Available	Not Available
72	136 GB	\$16.8154/hour	Not Available	Not Available	Not Available

## M-series Hardware Type

vCore	Memory	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour	Hyperscale Cost per Hour
8	235.4 GB	Not Available	Not Available	\$16.4303/hour	Not Available
10	294.3 GB	Not Available	Not Available	\$20.5379/hour	Not Available
12	353.2	Not Available	Not Available	\$24.6454/hour	Not Available
14	412.0 GB	Not Available	Not Available	\$28.7530/hour	Not Available
16	470.9 GB	Not Available	Not Available	\$32.8605/hour	Not Available
18	529.7 GB	Not Available	Not Available	\$36.9681/hour	Not Available
20	588.6 GB	Not Available	Not Available	\$41.0757/hour	Not Available
24	706.3 GB	Not Available	Not Available	\$49.2908/hour	Not Available
32	941.8 GB	Not Available	Not Available	\$65.7210/hour	Not Available
64	1.839 TB	Not Available	Not Available	\$131.4420/hour	Not Available
128	3.678 TB	Not Available	Not Available	\$262.884/hour	Not Available

## vCore Serverless Compute Pricing

Minimum vCores	Maximum vCores	Minimum Memory	Maximum Memory	Price
0.5	40	2.02 GB	120 GB	\$0.0001450/vCore-second (\$0.5218/vCore-hour)

## Azure SQL Database Elastic Pool Pricing

### DTU Pricing

Service Tier	eDTUs per Pool	Included Storage per Pool	Max Storage per Pool	Max eDTUs per Database	Price per Hour
Basic	50	5 GB	5 GB	100	\$0.1009/hour
Basic	100	10 GB	10 GB	200	\$0.2017/hour
Basic	200	20 GB	20 GB	500	\$0.4034/hour
Basic	300	29 GB	29 GB	500	\$0.6051/hour
Basic	400	39 GB	39 GB	500	\$0.8067/hour
Basic	800	78 GB	78 GB	500	\$1.6134/hour
Basic	1,200	117 GB	117 GB	500	\$2.4200/hour
Basic	1,600	156 GB	156 GB	500	\$3.2267/hour

Standard	50	50 GB	500 GB	100	\$0.1511/hour
Standard	100	100 GB	750 GB	200	\$0.3021/hour
Standard	200	200 GB	1 TB	500	\$0.6042/hour
Standard	300	300 GB	1.25 TB	500	\$0.9063/hour
Standard	400	400 GB	1.5 TB	500	\$1.2084/hour
Standard	800	800 GB	2 TB	500	\$2.4167/hour
Standard	1,200	1.17 TB	2.5 TB	500	\$3.6250/hour
Standard	1,600	1.56 TB	3 TB	500	\$4.8334/hour
Standard	2,000	1.95 TB	3.5 TB	500	\$6.0417/hour
Standard	2,500	2.44 TB	4 TB	500	\$7.5521/hour
Standard	3,000	2.93 TB	4 TB	500	\$9.0626/hour
Premium	125	250 GB	1 TB	50	\$0.9376/hour
Premium	250	500 GB	1 TB	100	\$1.8750/hour
Premium	500	750 GB	1 TB	100	\$3.7500/hour
Premium	1,000	1 TB	1 TB	100	\$7.5001/hour
Premium	1,500	1.5 TB	1.5 TB	100	\$11.2500/hour
Premium	2,000	2 TB	2 TB	100	\$15.0000/hour
Premium	2,500	2.5 TB	2.5 TB	100	\$18.7500/hour
Premium	3,000	3 TB	3 TB	100	\$22.5000/hour
Premium	3,500	3.5 TB	3.5 TB	100	\$26.2500/hour
Premium	4,000	4 TB	4 TB	100	\$30.0000/hour

## vCore Provisioned Compute Pricing

### Gen 5 Hardware Type

vCore	Memory	General Purpose Max no. of Databases per Pool	Business Critical Max no. of Databases per Pool	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour
2	10.2 GB	100	Not Available	\$0.5044/hour	\$0.6871/hour	Not Available
4	20.4 GB	200	50	\$1.0088/hour	\$1.3741/hour	\$2.7178/hour
6	30.6 GB	500	100	\$1.5131/hour	\$2.0611/hour	\$4.0767/hour
8	40.8 GB	500	100	\$2.0175/hour	\$2.7482/hour	\$5.4355/hour
10	51.0 GB	500	100	\$2.5219/hour	\$3.4352/hour	\$6.7944/hour
12	61.2 GB	500	100	\$3.0262/hour	\$4.1222/hour	\$8.1533/hour
14	71.4 GB	500	100	\$3.5306/hour	\$4.8092/hour	\$9.5121/hour
16	81.6 GB	500	100	\$4.0350/hour	\$5.4963/hour	\$10.8710/hour
18	91.8 GB	500	100	\$4.5393/hour	\$6.1833/hour	\$12.2299/hour
20	102.0 GB	500	100	\$5.0437/hour	\$6.8703/hour	\$13.5887/hour
24	122.4 GB	500	100	\$6.0524/hour	\$8.2444/hour	\$16.3065/hour
32	163.2 GB	500	100	\$8.0699/hour	\$10.9925/hour	\$21.7420/hour
40	204.0 GB	500	100	\$10.0874/hour	\$13.7406/hour	\$27.1774/hour
80	396.0 GB	500	100	\$20.1747/hour	\$27.4811/hour	\$54.3548/hour

## DC-series Hardware Type

vCore	Memory	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour
2	9 GB	\$0.8830/hour	Not Available	\$2.116/hour
4	18 GB	\$1.7659/hour	Not Available	\$4.233/hour
6	27 GB	\$3.3328/hour	Not Available	\$6.349/hour
8	36 GB	\$2.8498/hour	Not Available	\$8.466/hour

## Fsv2-series Hardware Type

vCore	Memory	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour
8	15.1 GB	\$1.8684/hour	Not Available	Not Available
10	18.9 GB	\$2.3355/hour	Not Available	Not Available
12	22.7 GB	\$2.8026/hour	Not Available	Not Available
14	26.5 GB	\$3.2697/hour	Not Available	Not Available
16	30.2 GB	\$3.7368/hour	Not Available	Not Available
18	34.0 GB	\$4.2039/hour	Not Available	Not Available
20	37.8 GB	\$4.6710/hour	Not Available	Not Available
24	45.4 GB	\$5.6052/hour	Not Available	Not Available
32	60.5 GB	\$7.4735/hour	Not Available	Not Available
36	68.0 GB	\$8.4077/hour	Not Available	Not Available
72	136 GB	\$16.8154/hour	Not Available	Not Available

## M-series Hardware Type

vCore	Memory	Business Critical Max no. of Databases per Pool	General Purpose Locally Redundant Cost per Hour	General Purpose Zone Redundant Cost per Hour	Business Critical Cost per Hour
8	235.4 GB	100	Not Available	Not Available	\$16.4303/hour
10	294.3 GB	100	Not Available	Not Available	\$20.5379/hour
12	353.2	100	Not Available	Not Available	\$24.6454/hour
14	412.0 GB	100	Not Available	Not Available	\$28.7530/hour
16	470.9 GB	100	Not Available	Not Available	\$32.8605/hour
18	529.7 GB	100	Not Available	Not Available	\$36.9681/hour
20	588.6 GB	100	Not Available	Not Available	\$41.0757/hour
24	706.3 GB	100	Not Available	Not Available	\$49.2908/hour
32	941.8 GB	100	Not Available	Not Available	\$65.7210/hour
64	1.839 TB	100	Not Available	Not Available	\$131.4420/hour
128	3.678 TB	100	Not Available	Not Available	\$262.884/hour

## Azure SQL Database Managed Instance Pricing

### vCore Pricing – Single Instance

#### Gen 5 Hardware Type

vCore	Memory	Included Storage	Price per Hour
4	20.4 GB	First 32 GB per month	\$1.01/hour
8	40.8 GB	First 32 GB per month	\$2.02/hour
16	81.6 GB	First 32 GB per month	\$4.04/hour
24	122.4 GB	First 32 GB per month	\$6.06/hour
32	163.2 GB	First 32 GB per month	\$8.07/hour
40	204.0 GB	First 32 GB per month	\$10.09/hour
64	326.4 GB	First 32 GB per month	\$16.14/hour
80	396.0 GB	First 32 GB per month	\$20.18/hour

### vCore Pricing – Instance Pools

#### Gen 5 Hardware Type

vCore	Memory	Included Storage	Price per Hour
8	40.8 GB	First 32 GB per instance per month	\$2.02/hour
16	81.6 GB	First 32 GB per instance per month	\$4.04/hour
24	122.4 GB	First 32 GB per instance per month	\$6.06/hour
32	163.2 GB	First 32 GB per instance per month	\$8.07/hour
40	204.0 GB	First 32 GB per instance per month	\$10.09/hour
64	326.4 GB	First 32 GB per instance per month	\$16.14/hour
80	396.0 GB	First 32 GB per instance per month	\$20.18/hour

## Microsoft Azure SQL Database Pricing Concepts

Selecting the correct Microsoft Azure SQL Database pricing model for your solution can be challenging. With so many options and variations available, choosing the right combination of deployment model, purchase model, compute tier, service tier, and hardware type is complicated. However, understanding what each of these components offers can help you determine your solution's best configuration.

## Azure SQL Deployment Models

If you want to leverage Microsoft Azure SQL Database as your database solution, you can choose between three deployment models.

- **Single Database:** The single database resource type creates a database with its own set of resources that you manage via a server.
- **Elastic Pool:** The elastic pool deployment model offers auto-scaling of database resources (either vCore or DTU) that are shared among multiple databases. Administrators set a minimum and maximum for the entire pool according to their budget, and also set a minimum and maximum for resource usage for each database, and then simply pay by the hour of total usage.
- **Managed Instance:** The Azure SQL Managed Instance deployment model offers the best compatibility benefits and licensing flexibility designed to incentivize migration from on-premise environments. A fully-featured SQL solution running on an Azure VM is compatible with the latest on-prem SQL Server Enterprise Edition, and offers automatic patching, backups, and high availability.

## Azure SQL Purchase Models

Azure SQL Database offers two purchase models for the Single Database and Elastic Pool deployment options: Database Transaction Unit (DTU) and vCore. The Managed Instance deployment model does not have DTU as an option and only offers vCore.

The difference between the two models are the resources provisioned.

- **DTU:** bundles compute and storage resources. A DTU represents a composite measure of CPU, memory, reads, and writes.
- **vCore:** allows you to provide an exact amount of computing resources via the provisioned compute model.

## Azure SQL Compute Tiers

If you choose to leverage the vCore purchase model for the Single Database deployment option, you can opt for Provisioned or [Serverless](#). Note that these compute tiers are only available for this deployment model. The Elastic Pool and Managed Instance deployment models only offer a provisioned solution. The table below outlines the recommended usage, scaling, and billing scenarios for each tier.

	Provisioned	Serverless
Usage Scenario	Regular usage patterns with higher compute utilization over time.	Irregular, unpredictable usage patterns with lower average compute utilization over time.
Scaling	Manual (Managed by Customer)	Automatic (Managed by Azure)
Billing	Per hour	Per second

## Azure SQL Service Tiers

### vCore Service Tiers

Microsoft Azure SQL Database offers three service tiers under its vCore purchase model: General Purpose, Business Critical, and Hyperscale. However, depending on the deployment you select, not every option is available. The table below correlates the availability of each service tier with the relevant deployment model.

	Single Database	Elastic Pool	Managed Instance
General Purpose	Available	Available	Available
Business Critical	Available	Available	Available
Hyperscale	Available	Not Available	Not Available

Each tier offers various performance and SLA guarantees. The option you choose depends on your business requirements. As with every other Azure service, the higher the performance and SLA, the higher the cost.

- **General Purpose:** This tier is the default selection for Single Database and Managed Instance. It offers a fully managed database engine with a 99.99% SLA and storage latency between 5 ms and 10 ms.
- **Business Critical:** This tier offers better performance than the General Purpose option. It has an SLA of 99.995% and storage latency of between 1ms and 2ms.
- **Hyperscale:** The Hyperscale tier leverages highly scalable storage and compute performance. It offers support for databases of 100TB in size, much faster backups and restores, faster log throughput and transaction commit times, and rapid scale-up and scale-out.

## DTU Service Tiers

The Single Instance and Elastic Pool deployment models offer a DTU purchase model in addition to vCore. As with the vCore option, the DTU alternative offers three service tiers: Basic, Standard, and Premium. As mentioned previously, a DTU is a blended measure of CPU, memory, reads, and writes. The following [table from Microsoft](#) details the features of each DTU service tier.

	Basic	Standard	Premium
Target workload	Development and Production	Development and Production	Development and Production
Uptime SLA	99.99%	99.99%	99.99%
CPU	Low	Low, Medium, High	Medium, High
Maximum Backup Retention	7 days	35 days	35 days
IOPS (approximate)	1 to 4 IOPS per DTU	1 to 4 IOPS per DTU	25 IOPS per DTU
IO latency (approximate)	5 ms read, 10 ms write	5 ms read, 10 ms write	2 ms read and write
Columnstore indexing	Not Available	S3 and above	Supported
In-memory OLTP	Not Available	Not Available	Supported

## Azure SQL Hardware Types

All three Azure SQL deployment options offer a vCore purchase model. As with the service tiers, you can also select the hardware that will host your Azure SQL database solution. There are four hardware types. However, the options available depend on the service tier and deployment model selected.

- **Gen 5:** The Gen 5 hardware type provides a balance between compute and memory resources. It is suitable for most data workloads that do not require higher memory or CPU.
- **Fsv2-series:** The Fsv2-series is compute-optimized. It delivers lower CPU latency and higher clock speeds. This hardware type is ideal for compute-intensive data workloads.
- **M-series:** The M-series is memory-optimized. It offers 29 GB per vCore, increasing the memory limit relative to a Gen 5 by a factor of eight.
- **DC-series:** The DC-series is ideal for secure workloads. It uses Intel processors with Software Guard Extension technology. Like Gen 5, it offers a balance between compute and memory.

## Azure SQL Cost Optimization

As with all Azure services, optimizing your Microsoft Azure SQL Database can help you increase efficiency while reducing cost. Azure offers several pricing and configuration options that ensure you get the most resources for every dollar spent.

### Pricing Options

When configuring your Azure SQL Database solution, Microsoft offers various pricing options. These include Reserved Capacity and the Azure Hybrid Benefit.

### Reserved Capacity

Azure Reserved Capacity can reduce the compute cost of your Azure SQL significantly. However, this cost-saving feature is only available for the vCore Gen 5 options. Savings can range from 16% to 33%, depending on the service tier and Reserved Capacity commitment length. For example, on a vCore Gen 5 General Purpose configuration, a one-year commitment can save you 21% and a three-year commitment 33%. If you upgrade your service tier to Business Critical, the savings are 16% for one-year and 25% for a three-year commitment.

### Azure Hybrid Benefit

The Azure Hybrid Benefit is another cost-saving option that can reduce your Azure SQL costs. By leveraging the licensing from an Enterprise Agreement's Software Assurance, you can realize savings of up to 55% depending on the hardware type and service tier. Azure Hybrid Benefit discounts are available for all vCore hardware types. However, this discount is not an option if you select the DTU purchasing model.

### Configuration Options

Besides the various direct cost-saving options, you can also optimize your Azure SQL solution by configuring it efficiently. Using the correct combination of deployment model, purchase model, compute tier, service tier, and hardware type can provide you with the performance you need and deliver it at the lowest possible cost.

### Deployment Options

If your solution does not need a dedicated Azure SQL server, then opting for the Elastic Pool deployment model is a better cost option. As you are only paying for the resources you use, this option is highly cost-effective for intermittent or ad hoc data workloads.

## Service Tier Options

Both the DTU and vCore purchase models offer various service tiers. Each tier offers different performance and cost features, with the premium or business-critical ones being the most expensive. Selecting the tier that best matches your business requirements is vital. For example, choosing the business-critical or premium tier for a dev/test environment is far from the ideal SQL optimization scenario.

## Compute Tier Options

The vCore purchase model allows you to select either a provisioned or serverless compute tier. If your Azure SQL Database workload has irregular, unpredictable usage patterns with lower average compute utilization over time, then this option can also deliver significant cost savings. As you only pay for the resources you use, and billing is per second instead of per hour, selecting the serverless compute option increases the efficiency of your Azure SQL spend.

## Hardware Types

The vCore purchase model offers four different hardware types. Depending on the option you choose, prices can vary significantly. For example, the Fsv2-series and M-series are not as cost-effective as the Gen 5.

In addition to selecting the correct hardware type, choosing the vCore option that best matches your requirement can also reduce your Azure spend. For example, opting for an 8 vCore solution when your needs do not exceed 6 cores and 30 GB is an inefficient use of resources.

## Storage

Storage is often one of the more significant portions of a subscription's Azure spend. As this component makes up a considerable part of any Azure SQL solution, optimizing the storage you utilize is vital in containing costs. Good database hygiene, such as archiving off older data and storing it on more cost-effective alternatives, should form part of any Azure SQL optimization exercise.

## Best Practices for Administering Azure SQL

Ongoing operational management and maintenance of your Azure SQL environment are vital in ensuring its efficiency and security. Unlike traditional SQL Server deployments that require maintenance tasks that include regular log shrinking, Azure SQL is a Platform as a Service (PaaS), which means Microsoft takes care of the traditional infrastructure tasks for you. However, you should apply a few configuration settings to secure and monitor your Azure SQL solution.

## Security

Azure SQL security controls have two major functions: protecting data and controlling access.

## Protecting Data with Encryption

Microsoft [recommends](#) that you encrypt data on Azure while it is in transit and at rest. You should leverage Transport Layer Security (TLS) while data is moving across networks. If you are using a client to connect to your Azure SQL instance, [Tabular Data Stream over TLS](#) is another requirement.



While data is at rest, leveraging [Transparent Data Encryption](#) secures it from malicious offline activity. This technology is enabled by default. However, existing Azure SQL databases created before May 2017 and SQL databases created through restore, geo-replication, and database copy are not. Databases residing on a Managed Instance deployment model are also encrypted by default. However, this encryption only applies to databases created after February 2019.

## Control Access

Leveraging the [principle of least privilege](#), you should limit direct access to Azure SQL data. Only services and individuals that need to query the information directly should be given the relevant authorization. Microsoft recommends implementing Multi-Factor Authentication where possible and limiting the use of password-based authentication for applications.

## Monitoring

Azure offers several monitoring tools you can use to monitor your Microsoft Azure SQL Database's efficiency and performance. The option to utilize depends on the metric you need to track. The list below highlights the features of each one.

- **Azure Portal:** Navigating to the Resources tab on the Overview Blade can give you insight into CPU, memory, and network performance.
- **Azure SQL Analytics:** This tool that runs with [Azure Monitor](#) helps you track all your Azure SQL databases' performance across multiple subscriptions. It provides you with a single view collecting and visualizing key performance metrics.
- **Activity Logs:** This feature also runs on Azure Monitor and provides insight into subscription-level events such as adding, creating, or deleting a database.
- **Azure Security Center:** This Azure resource provides a centralized security view of all your Azure resources. It assesses your environment and its configuration and provides recommended actions to remediate any security vulnerabilities. It also raises security-related alerts when it detects an anomaly or when certain activities exceed a particular threshold.

# Chapter 6: Azure Backup Pricing

Azure Backup provides a centralized interface for managing backups for a wide range of enterprise services, including:

- Azure Managed disks
- Azure File Shares
- SQL Server Databases
- SAP HANA databases
- SharePoint, Exchange, Hyper-V workloads
- VMWare and bare metal machines

Azure Backup ensures application consistency through its Volume Shadow Copy Service (VSS) and pre/post processing scripts. Storage options include Locally Redundant Storage (LRS), Geo-Redundant storage (GRS), Zone Redundant Storage (ZRS), and Read-Access Geo-Redundant Storage (RA-GRS).

## Azure Backup Pricing

There are three main components that drive the cost of Azure Backup pricing:

- 1. Fixed service cost:** This cost is incurred regardless of the amount of data or bandwidth consumed.
- 2. Storage:** This cost is based on how much data you store and depends on backup sizes, retention periods, the frequency of your backup schedule, and storage types.
- 3. Average daily data churn:** This cost is based on how often your data changes.

The Azure Pricing Calculator allows you to configure the various cost elements to determine your approximate Azure Backup costs. However, as multiple variables contribute to the total cost, using the Azure Backup pricing estimator offers greater accuracy. This Excel-based worksheet tool also provides accurate Azure Backup cost estimates for the various workloads protected by this service.

## Calculating Azure Backup Costs

Because so many elements are factored into the total cost of backing up a particular workload, calculating your Azure Backup costs requires specifying the key details for each service. Use the following sections to get an idea of how to accomplish this.

### Azure Virtual Machines (VMs) or On-Premise Servers

Key Details:

- The “used size” (vs. provisioned size) of disks that require backing up
- The total number of servers multiplied by their amount of “used disk space”
- The expected amount of data churn (high, moderate, or low)
- Backup policy retention time lengths (daily, weekly, monthly, yearly)
- Backup storage redundancy (Locally Redundant Storage (LRS), Geo-Redundant Storage (GRS), or Read-Access Geo-Redundant Storage (RA-GRS))

The table below provides an indicative cost for various Azure VM or on-premise server backup scenarios.

Service	Protected Instances	Backup Policy Retention	Backup Storage Data Characteristics	Average Monthly Backup Data	Monthly Data Cost	Fixed Cost	Total Cost
Azure VM	1 x 40 GB	30 Days 5 Weeks 12 Months 5 Years	Moderate Churn GRS	136 GB	\$6.10	\$5.00	\$11.10
Azure VM	1 x 500 GB	30 Days 5 Weeks 12 Months 5 Years	High Churn GRS	2,502 GB	\$112.10	\$10.00	\$122.10
Azure VM	1 x 1000 GB	30 Days 5 Weeks 12 Months 5 Years	Low Churn LRS	2,601 GB	\$58.28	\$20.00	\$78.28
On-Prem Server	1 x 40 GB	30 Days 5 Weeks 12 Months 5 Years	Moderate Churn LRS	136 GB	\$3.05	\$5.00	\$8.05
On-Prem Server	1 x 500 GB	30 Days 5 Weeks 12 Months 5 Years	High Churn GRS	2,502 GB	\$112.10	\$10.00	\$122.10
On-Prem Server	1 x 2000 GB	30 Days 5 Weeks 12 Months 5 Years	High Churn GRS	10,0008 GB	\$448.40	\$40.00	\$488.40

## SQL Server on Azure VMs

Key Details:

- The data size of the SQL servers that require backing up
- Number of SQL servers with that size
- Expected compression
- Expected log size as a percentage of the SQL server size
- The expected amount of data churn (high, moderate, or low)
- Backup type; daily differentials with weekly, monthly, yearly full backups, or daily, weekly, monthly, yearly full backups
- Backup policy retention time lengths (daily, weekly, monthly, yearly)
- Backup storage redundancy (Locally Redundant Storage (LRS) or Geo-Redundant Storage (GRS))

The table below provides an indicative cost for various SQL in Azure VM backup scenarios.

Service	Protected Instances	Backup Policy Retention	Backup Storage Data Characteristics	Average Monthly Backup Data	Monthly Data Cost	Fixed Cost	Total Cost
SQL Server on Azure VM	1 x 40 GB	30 Days 5 Weeks 12 Months 5 Years 15 Day Log Rotation	High Churn GRS	222 GB	\$9.95	\$25.00	\$34.95
SQL Server on Azure VM	1 x 500 GB	30 Days 5 Weeks 12 Months 5 Years 15 Day Log Rotation	Moderate Churn LRS	2,404 GB	\$107.70	\$25.00	\$132.70
SQL Server on Azure VM	1 x 1000 GB	30 Days 5 Weeks 12 Months 5 Years 15 Day Log Rotation	High Churn GRS	5,555 GB	\$248.86	\$50.00	\$298.86
SQL Server on Azure VM	1 x 2000 GB	30 Days 5 Weeks 12 Months 5 Years 15 Day Log Rotation	High Churn GRS	9,510 GB	\$426.05	\$426.05	\$526.05

## SAP HANA in Azure VMs

- The sum of the full backup size of each of the databases, as reported by SAP HANA
- Number of SQL servers with that size
- Expected log size as a percentage of the SAP HANA database size
- The expected amount of data churn (high, moderate, or low)
- Backup type; daily differentials with weekly, monthly, yearly full backups, or daily, weekly, monthly, yearly full backups
- Backup policy retention time lengths (daily, weekly, monthly, yearly)
- Backup storage redundancy (Locally Redundant Storage (LRS) or Geo-Redundant Storage (GRS))
- The option to check your estimates for a different region or discounted rates

The table below provides an indicative cost for various SAP HANA in Azure VM backup scenarios.

Service	Protected Instances	Backup Policy Retention	Backup Storage Data Characteristics	Average Monthly Backup Data	Monthly Data Cost	Fixed Cost	Total Cost
SAP HANA on Azure VM	1 x 40 GB	30 Days 5 Weeks 12 Months 5 Years 7 Day Log Rotation	Moderate Churn LRS	512 GB	\$11.47	\$80.00	\$91.47
SAP HANA on Azure VM	1 x 500 GB	30 Days 5 Weeks 12 Months 5 Years 7 Day Log Rotation	Moderate Churn LRS	6,400 GB	\$286.76	\$80.00	\$366.76

SAP HANA on Azure VM	1 x 1000 GB	30 Days 5 Weeks 12 Months 5 Years 7 Day Log Rotation	High Churn GRS	15,016 GB	\$672.75	\$160.00	\$832.75
SAP HANA on Azure VM	1 x 2000 GB	30 Days 5 Weeks 12 Months 5 Years 7 Day Log Rotation	High Churn GRS	30,033 GB	\$1,345.89	\$320.00	\$1,665.49

## Azure files shares

- Size (in GB) of the file shares
- The number of storage accounts hosting the file shares with the quoted size
- The expected amount of data churn (high, moderate, or low)
- Type of storage account (standard or premium)
- Backup policy retention time lengths (daily, weekly, monthly, yearly)
- Backup storage redundancy (Locally Redundant Storage (LRS), Geo-Redundant Storage (GRS), or Zone Redundant Storage (ZRS))
- Performance tier (Transaction Optimized, Premium, Hot, Cool)
- The option to check your estimates for a different region or discounted rates

The table below provides an indicative cost for various Azure file share scenarios.

Service	Protected Instances	Backup Policy Retention	Backup Storage Data Characteristics	Average Monthly Backup Data	Monthly Data Cost	Fixed Cost	Total Cost
Azure Files	1 x 40 GB	30 Days 5 Weeks 12 Months 10 Years	Low Churn LRS Transaction Optimized Tier	64 GB	\$3.84	\$3.00	\$6.84
Azure Files	1 x 500 GB	30 Days 5 Weeks 12 Months 10 Years	High Churn GRS Hot Tier	2,002 GB	\$126.54	\$5.00	\$131.54
Azure Files	1 x 1000 GB	30 Days 5 Weeks 12 Months 10 Years	High Churn GRS Transaction Optimized Tier	4,004 GB	\$400.45	\$5.00	\$405.45
Azure Files	1 x 2000 GB	30 Days 5 Weeks 12 Months 5 Years 15 Day Log Rotation	Moderate Churn GRS Cool Tier	4,805 GB	\$240.75	\$5.00	\$245.75

# Azure Backup Architecture

Azure Backup leverages four different technologies: Azure virtual machine extensions, Microsoft Azure Backup Server (MABS), System Center Data Protection Manager (DPM), and Microsoft Azure Recovery Services (MARS).

- **VM Extensions:** Uses small applications in post-deployment to backup VMs.
- **MABS:** Deployable using an on-premise server or an Azure virtual machine. As you run it on a server you manage, it uses the Infrastructure as a Service (IaaS) cloud computing service model.
- **DPM:** The same as MABS except for licensing; if you have System Center in your on-premise environment, then DPM falls under that model.
- **MARS:** Deployable using a lightweight agent on selected workloads; does not need any infrastructure to operate and uses the Platform as a Service (PaaS) cloud computing service model.

Azure's setup wizard specifies which architecture should be used based on the type of workload you want to back up. The following screenshots walk through the setup wizard.

**Backup Goal** ...

⚠ The storage replication is set to Geo-redundant. This option cannot be changed later. Before proceeding further, click here. →

Where is your workload running?  
On-Premises

What do you want to backup?  
8 selected

- Files and folders
- Hyper-V Virtual Machines
- VMware Virtual Machines
- Microsoft SQL Server
- Microsoft SharePoint
- Microsoft Exchange
- System State
- Bare Metal Recovery

**Prepare infrastructure** ...

already using System Center Data Protection Manager or any other System Center Product

---

**Azure Backup Server**  
Please follow the steps mentioned below.

1. Install Microsoft Azure Backup Server  
[Download](#)
2. Download vault credentials to register the server to the vault. Vault credentials will expire after 10 days.  
 Already downloaded or using the latest Azure Backup Server installation  
[Download](#)
3. Post infrastructure preparation, please use Microsoft Azure Backup Server U(on-premises) to configure backup.

In the second example, when we choose Azure as the workload's location and select a virtual machine, it uses the Azure VM extension to protect the workload.

### Backup Goal

**⚠** The storage replication is set to Geo-redundant. This option cannot be changed later. Before proceeding further, click here. →

Where is your workload running?

What do you want to backup?

**Step: Configure Backup**

### Configure Backup

Backup policy \*   
[Create a new policy](#)

**Policy Details**

Full Backup

**Backup Frequency**  
Daily at 12:00 AM UTC

**Instant Restore**  
Retain instant recovery snapshot(s) for 2 day(s)

**Retention of daily backup point**  
Retain backup taken every day at 12:00 AM for 30 Day(s)

**Virtual machines**

Name	Resource Group	OS Disk Only
No Virtual machines selected.		

**i OS Disk only backup** option allows you to backup Azure Virtual Machine with only OS disk and exclude all the data disks. You can use Selective Disk Backup feature through Powershell or CLI to include or exclude specific data disks. Know more about Selective Disk Backup feature, its limitation and pricing: [Learn more](#).

The solution selected by Azure depends on a combination of workload and location. The table below details the limits and benefits of each Azure Backup solution.

Azure Backup Solution	Features	Limitations
Azure VM Extensions	<ul style="list-style-type: none"> <li>• Full VM backup for Windows or Linux with no additional agent needed</li> <li>• Application-aware snapshots using Volume Shadow Copy Services (VSS) on Windows and pre- and post-processing scripts on Linux</li> <li>• Platform as a Service; no additional backup infrastructure needed</li> </ul>	<ul style="list-style-type: none"> <li>• One scheduled backup per day, however, you can also execute three on-demand backups per day</li> <li>• No monthly or yearly backup support</li> <li>• Limited granularity as you can only restore at the disk level</li> <li>• No on-premise backup support</li> </ul>
Azure MARS Agent	<ul style="list-style-type: none"> <li>• Supports backup for on-premise and Azure virtual machines</li> <li>• Platform as a Service; no additional backup infrastructure needed</li> </ul>	<ul style="list-style-type: none"> <li>• No application awareness; backups are limited to files, folders, and volumes</li> <li>• No Linux support</li> <li>• Limited to 3 scheduled backups per day</li> </ul>

<p>Azure MABS</p>	<ul style="list-style-type: none"> <li>• Supports Windows and Linux</li> <li>• Application-aware with agents for SQL, Exchange, etc.</li> <li>• Granular backups and restores</li> <li>• VMware and Hyper-V support</li> <li>• No additional licensing cost</li> <li>• SQL backups every 15 minutes; other workloads are backed up hourly</li> </ul>	<ul style="list-style-type: none"> <li>• Can only backup Azure VMs if MABS is deployed in Azure</li> <li>• Infrastructure as a Service requiring additional monitoring and maintenance</li> </ul>
<p>System Center DPM</p>	<ul style="list-style-type: none"> <li>• Supports Windows and Linux</li> <li>• Application-aware with agents for SQL, Exchange, etc.</li> <li>• Granular backups and restores</li> <li>• VMware and Hyper-V support</li> </ul>	<ul style="list-style-type: none"> <li>• Licensing cost</li> <li>• Infrastructure as a Service requiring additional monitoring and maintenance</li> </ul>

## Azure Backup Cost Optimization

You can optimize your Azure Backup costs in the following ways.

### 1. Optimize Backup Policies

Microsoft Azure Backup offers three backup policies: full backups, differential backups, and incremental backups. Each policy type has its advantages and disadvantages regarding cost, recovery point objectives, and recovery time objectives. The key to optimizing Azure Backups is to apply the appropriate policies to the relevant workloads. Configuring a blanket policy for every server, database, or file storage location is inefficient.

### Recovery Point and Recovery Time Objectives

Recovery points and the recovery time form the core components of any backup strategy.

- **Recovery Point Objective (RPO):** Relates to the point in time the backup takes place. For example, if you run backups once daily, your RPO is 24 hours. In this instance, should you need to restore your data, the maximum amount of information you may lose is 24 hours.
- **Recovery Time Objective (RTO):** Represents the amount of time it would take to restore the data from backup. For example, if you keep data on a local disk, your recovery time will be far shorter than restoring data from a data center in another part of the world.

Your backup policy's RPO and RTO determine the type of backup you need for each workload. It also dictates your backup schedule. If your backup strategy requires a very high RPO, you need to ensure your backups run more frequently. Regarding the RTO, full backups offer the fastest recovery times as you only need to recover one backup.

Differential backups offer the second-fastest RTO as you need to perform two restore operations: the last full backup and the latest differential. Incrementals are potentially the slowest backup type to recover. As you need to restore the last full backup and every incremental since that point, you may need to perform several operations to recover data.

### Optimizing Recovery Point and Recovery Time Objectives

If your workloads do not need a very high RPO, setting your backups to run less frequently will lower your Azure Backup storage costs. The same approach can also save you money when it comes to your RTO. For example, running a full backup every day stores more data than a full backup once a week and an incremental every other day. Reviewing the Optimize tab in your Azure Backup reports is a quick and efficient way to determine which workloads have daily full backups configured. You can click on the backup policy from this screen and amend it for workloads that need a lower RPO.



## 2. Reviewing Backups for Deleted Resources

The Azure Backup service stores backups until an administrator deletes them. Although the retention policies determine the number of successful backups it retains, the data remains perpetually if a workload no longer exists. There may be instances where an organization may need to keep this information. For example, some regulatory frameworks obligate companies to store records for several years. However, in many instances, administrators neglect to delete the backups when they decommission a particular service.

Regularly reviewing your Azure Backup reports can help you determine if you have any backups taking up storage that you no longer need. You can also configure these reports to provide [details on inactive resources](#). This report configuration also helps you identify any protected resources that have not reported a successful backup for an extended time. You can find this information by navigating to the Optimize tab and selecting the Inactive Resources tile.

## 3. Reduce Retention Periods

The retention periods you specify when configuring your Azure Backup policies affect the cost you need to pay for the service. In some instances, you may meet your compliance requirements and RTO and RPO objectives by reducing the duration of your retention periods.

For example, web servers may need backing up but do not need long retention periods; databases may need longer retention periods with backups that run more frequently. You can set retention periods when configuring your Azure backups.

## 4. Backup selectively

In many cases, you only need to protect some of the data in a particular workload. For example, a virtual machine may have a second drive to store non-production data, or a database server may contain a combination of test and production information. In these instances, configuring a full backup of the entire virtual machine or database is inefficient and costly, especially if you are backing up a large quantity of data.

The Azure Backup service gives you the option to include or exclude particular objects from your backup policy. For example, if you need to backup an Azure VM, you can select to include or exclude certain disks. It also has an OS disk-only option ideal for servers that host vital services but no data, such as web servers.

## Azure Backup Limitations

Although Azure Backup offers many features that make it an enterprise-grade data protection solution, the service does have some limitations. Before deploying Azure Backup, administrators must ensure these limitations do not contravene any compliance obligations or business requirements.

The list below details some of the service's limitations.

- **Maximum backup frequency:** The maximum backup frequency for SQL Server is every 15 minutes, and other workloads are once per hour using MABS/DPM. The MARS agent only allows a maximum of three backups per day. If you are backing up using the VM extension, then that backup frequency drops even further to once a day.

- **Disks:** Azure Backup does not support Ultra SSD, temporary, and NVME/ephemeral disks.
- **Static IP addresses:** VMs configured with a static IP address lose the association should you restore the VM.
- **Linux Support:** The MARS agent does not support Linux. If you need to protect an Azure Linux VM, you will need to use the Azure VM extension. MABS/DPM Linux support is limited to on-prem Hyper-V and VMware platforms.

# Chapter 7: Azure Advisor

## What to Expect When Using Azure Advisor

Azure Advisor is a Microsoft Azure service that provides recommendations based on your deployed Azure services configuration. By analyzing data from various telemetries, it helps you optimize your Azure configuration using the five pillars of the [Microsoft Azure Well-Architected Framework](#) as a baseline. By leveraging Azure Advisor's recommendations, you can enhance and refine your Azure services' cost, security, reliability, operational excellence, and performance.



**Illustration of Microsoft Azure's Well-Architected Framework**

The Microsoft Azure Well-Architected Framework provides a logical methodology for optimizing cloud-based workloads using a 5-pillar approach. Let's take a look at each pillar and how they work together.

Pillar	Description	Examples
Cost Optimization	Recommendations that accelerate time-to-market while keeping costs to a minimum.	Workload sizing recommendations.
Operational Excellence	Recommendations that improve workload- and application-supporting operations.	Automation, continuous monitoring, and diagnostic recommendations.
Performance Efficiency	Recommendations that enable resource scaling both horizontally and vertically.	Database configuration, storage configuration, and service availability recommendations.
Reliability	Recommendations that improve resiliency, availability, and fault-tolerance.	Virtual Machine protection and VPN resiliency recommendations.
Security	Recommendations that improve security without causing workflow bottlenecks.	Identity management, access control, application security, and encryption recommendations.

## Azure Advisor Recommended Best Practices

### Cost Optimization

Azure Advisor's cost optimization recommendations aim to reduce your Azure spend by identifying idle or underutilized resources.

General	Cleanup	Examples
Right-size your database servers (MariaDB, MySQL, and PostgreSQL).	Shut down or downsize underutilized VMs.	Reserve general purpose VM instances.
Use standard snapshots for managed disks.	Right-size your database servers (MariaDB, MySQL, and PostgreSQL).	Reserve resource-optimized instances.
Use lifecycle management.	Eliminate unprovisioned ExpressRoute circuits.	Reserve Azure Cosmos DB capacity.
Create an Ephemeral OS Disk recommendation	Delete or reconfigure idle virtual network gateways.	Reserve SQL Database and SQL Managed Instance capacity.
	Delete unassociated public IP addresses.	Reserve App Service Stamp Fee capacity.
	Delete failing Azure Data Factory pipelines.	Reserve Blob storage capacity.
	Use standard snapshots for managed disks.	Reserve MariaDB, MySQL, and PostgreSQL capacity.
	Create an Ephemeral OS Disk recommendation.	Reserve Azure Synapse Analytics capacity.

## Operational Excellence

Operational Excellence recommendations provide guidance that enables process and workflow efficiency, resource manageability, and deployment best practices.

General	Alerting & Compliance	Resource Management
Ensure you have access to Azure cloud experts when you need it.	Create Azure Service Health alerts.	Delete and re-create your pool to remove a deprecated internal component.
	Repair invalid log alert rules.	Enable a non-validation environment for production.
	Use Azure Policy recommendations.	Enable Traffic Analytics to view insights across Azure resources.
		Configure your storage accounts to prevent reaching the maximum subscription limit.

## Performance

Azure Advisor's performance recommendations provide guidance on improving the speed and responsiveness of configured and supported workloads.

General	Database	Query
Reduce DNS time-to-live on your Traffic Manager profile to failover to healthy endpoints faster.	Use an Azure Database for MySQL or Azure Database for PostgreSQL read replica to scale out reads for read-intensive workloads.	Remove data skew on your Azure Synapse Analytics tables.
Upgrade your Storage client library to the latest version.	Improve MySQL connection management.	Create or update outdated table statistics in your Azure Synapse Analytics tables.
Use managed disks to prevent disk I/O throttling.	Fix the CPU pressure of your Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Database for MariaDB servers with CPU bottlenecks.	Scale up to optimize cache utilization on your Azure Synapse Analytics tables.
Use Premium storage for VM disks when possible.	Set your Azure Cosmos DB query page size (MaxItemCount) to -1.	Convert Azure Synapse Analytics tables to replicated tables.
Migrate your storage account to Azure Resource Manager.	Optimize MySQL temporary-table sizing.	Increase batch size when loading to maximize load throughput, data compression, and query performance.

Increase the size of your VPN Gateway SKU to address high P2S and/or CPU use.	Reduce memory constraints or move to a Memory-Optimized SKU.	Scale your cache to a different size or SKU.
Upgrade to the latest Immersive Reader SDK.	Scale your Azure Database to a higher SKU to prevent connection constraints.	Co-locate storage accounts in the same region to minimize latency.
Improve user experience and connectivity by deploying VMs closer to Windows Virtual Desktop deployment location.	Add regions with traffic to your Azure Cosmos DB account.	
Use Accelerated Writes in your HBase cluster.	Configure your Azure Cosmos DB indexing policy by using custom included or excluded paths.	
Change the maximum session limit to improve VM performance.		

## Reliability

The reliability recommendations Azure Advisor provides aim to increase the availability and resiliency of supported Azure workloads.

General	Resilience	Upgrades
Protect your virtual machine data from accidental deletion.	Configure Consistent indexing mode on your Azure Cosmos DB collection.	Update version of your CheckPoint network virtual appliance image.
Use soft delete on your Azure storage account to save and recover data after accidental overwrite or deletion.	Use production VPN gateway for production workloads.	Upgrade your Azure Cosmos DB .NET SDK to the latest version from NuGet.
Ensure application gateway fault tolerance.	Configure Traffic Manager endpoints	Upgrade your Azure Cosmos DB Java SDK to the latest version from Maven
Enable virtual machine replication.	Configure your VPN gateway to active-active.	Upgrade your Azure Cosmos DB Spark connector to the latest version from Maven.
Do not override hostname to ensure website integrity.	Configure your Azure Cosmos DB containers with a partition key.	Upgrade to Kafka 2.1 on HDInsight 4.0.
		Upgrade older Spark versions in HDInsight Spark clusters.

## Security

Azure Advisor leverages the Azure Security Center platform to provide recommendations that help protect Azure resources.

App Services	Compute	Containers
Enable Azure Defender for App Service.	Enable adaptive application controls for defining safe applications.	Enable Azure Defender for Kubernetes and container registries.
Require HTTPS in your API app, function app, and web app.	Update allowlist rules in your adaptive application control policy.	Deploy from trusted registries only.
Use the latest version of TLS in your function app and web app.	Encrypt automation account variables.	Avoid running containers as a root user.
	Enable Azure Defender and file integrity monitoring for servers.	Use Role-Based Access Control (RBAC) for all Kubernetes services.
	Use disk encryption on virtual machines.	Install Azure Policy Addon-on for Kubernetes on your clusters.
	Use endpoint protection on your machines and VM scale sets.	Ensure clusters are only accessible over HTTPS.
	Install the Log Analytics agent on your Azure Arc machines, virtual machines, and machine scale sets.	Avoid overriding or disabling container AppArmor profiles.
	Protect management ports for VMs with just-in-time network access control.	

Data	Cleanup	Examples
Provision Azure Active Directory for SQL servers.	Have at least 2 but no more than 3 owners per subscription.	Apply adaptive network hardening recommendations on internet-facing VMs.
Install the Azure Defender extension on Azure Arc clusters.	Enable Azure Defender for Key Vault.	Restrict network ports with network security groups.
Use customer-managed keys to encrypt data at rest for Azure Cosmos DB accounts.	Remove deprecated and external accounts with owner permissions, read permissions, and write permissions.	Enable secure transfer to storage accounts.
Enable Azure Defender for SQL Database servers, DNS, Resource Manager, and storage.	Use expirations for keys and secrets in your Key Vault.	Protect VM management ports with just-in-time network access control.
	Enable MFA across all accounts with owner, read, and write permissions.	

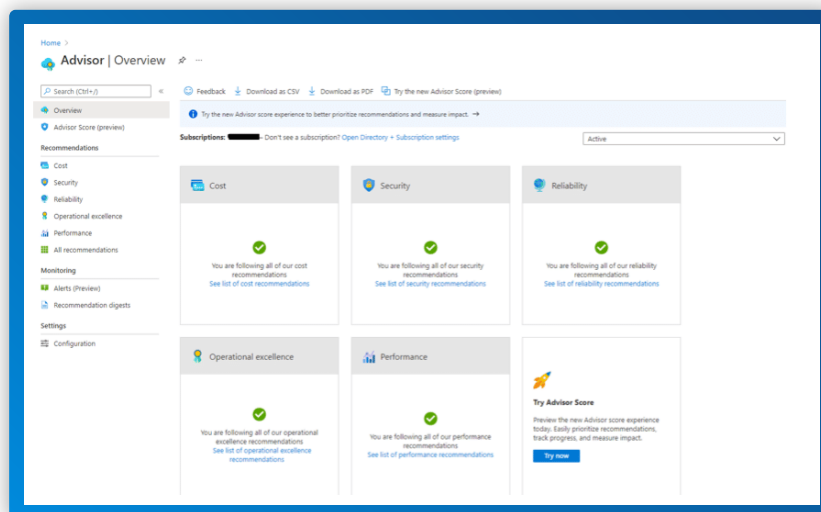
For the complete list of security best practices, visit: [Reference table for all Azure Security Center recommendations | Microsoft Docs](#).

## Managing Azure Advisor

Azure Advisor offers recommendations after it analyzes the deployed resources on a particular subscription. Depending on the service, the relevant data may take some time to materialize. Recommendations appear in the Azure Advisor dashboard, but as with most Azure services, you can also manage Azure Advisor using the Azure Portal, the Azure CLI, or Azure PowerShell.

## Managing Azure Advisor with Azure Portal

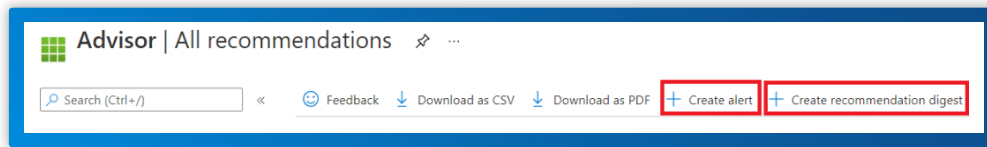
You can manage your Azure Advisor recommendations through Azure Portal's dashboard. In the following screenshot, there are no recommendations available. However, to ensure you stay informed of any new recommendations, you must set up alerts and a recommendation digest.



A Screenshot of the Azure Advisor Overview Page

# Creating an Azure Advisor Recommendation Digest

An Azure Advisor recommendation digest provides you with a customized synopsis of any active recommendations. You can create an Azure Advisor recommendation digest via the Azure Portal by navigating to "All Recommendations."



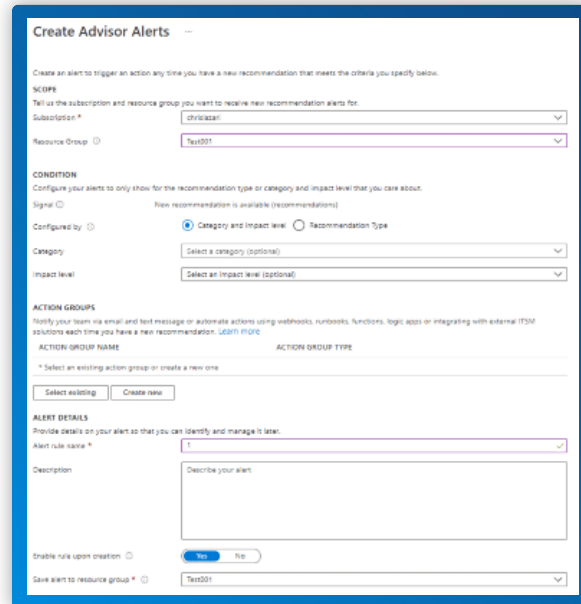
A Screenshot of Azure Advisor's All Recommendations Page

Recommendation digests have the following settings:

- **Frequency:** Defines the frequency of the digest (Weekly, Bi-Weekly, or Monthly).
- **Recommendation category:** Defines which recommendation categories to include.
- **Action Groups:** Specifies an [Action Group](#) to receive these digest recommendations.
- **Recommendation digest name:** Defines the name of the digest for segmentation and reporting.

## Creating an Azure Advisor Alert

Creating an alert on Azure Advisor enables you to receive proactive communication when the service makes a particular recommendation. You can select to receive alerts for a category or a specific recommendation type as well as choose the alert mechanism. The screenshot below shows the form that you need to complete on the Azure Portal.

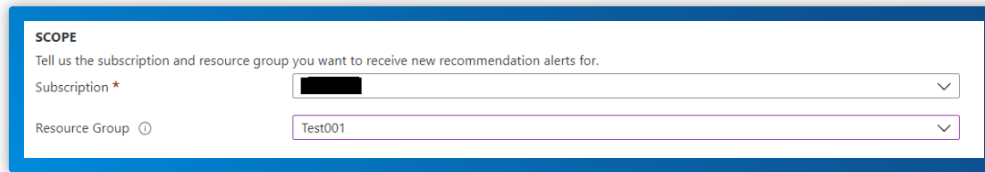


A Screenshot of the Advisor Alerts Creation Page

### 1. Setting the Scope

Azure Advisor uses the Azure Resource Manager model to segment services for analysis. To ensure you and your teams receive the right messages, it's important to organize workloads by roles and service aids so that they can be aligned with a resource group.

For example, suppose you assign all your security services to the same resource group. In that case, you can provide your security team with proper access controls and ensure they receive any security-related alerts or recommendations.



**SCOPE**  
Tell us the subscription and resource group you want to receive new recommendation alerts for.

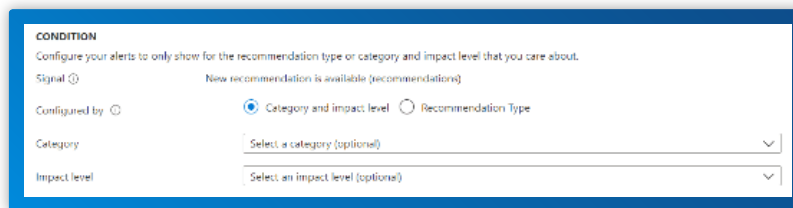
Subscription \* [Redacted]

Resource Group ⓘ Test001

**Set the Scope of your Azure Advisor Alert**

## 2. Setting the Condition

Azure Advisor gives you the option to receive alerts by category and impact level or recommendation type.



**CONDITION**  
Configure your alerts to only show for the recommendation type or category and impact level that you care about.

Signal ⓘ New recommendation is available (recommendations)

Configured by ⓘ  Category and impact level  Recommendation Type

Category Select a category (optional) [v]

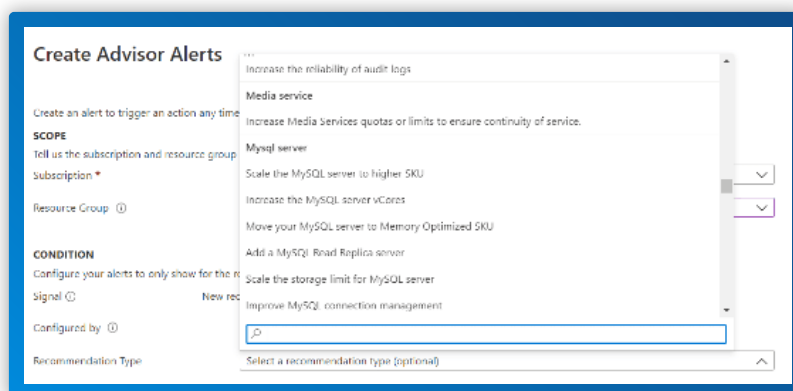
Impact level Select an impact level (optional) [v]

**Set the Condition of your Azure Advisor Alert**

Category alerts notify the relevant parties when Azure Advisor creates a recommendation for a particular category. For example, if you configure an Azure Advisor alert for the security resource group, you can select the security category. In this way, Azure Advisor will alert the security team when it creates a security-related recommendation.

Category alerts also allow you to select the impact level. By leveraging this feature, you can send different alert levels to various groups. For example, you may want your NOC to receive every alert recommendation and only notify your senior leadership team when the impact level is high.

As previously mentioned, you can also configure Azure Advisor alerts per recommendation type. By selecting this option, you can offer your team alerts with better granularity. For example, you may want to send database-related alerts and recommendations to your DBAs.



**Create Advisor Alerts**

Create an alert to trigger an action any time

**SCOPE**  
Tell us the subscription and resource group

Subscription \* [Redacted]

Resource Group ⓘ [Redacted]

**CONDITION**  
Configure your alerts to only show for the

Signal ⓘ New rec

Configured by ⓘ  Category and impact level  Recommendation Type

Recommendation Type Select a recommendation type (optional) [v]

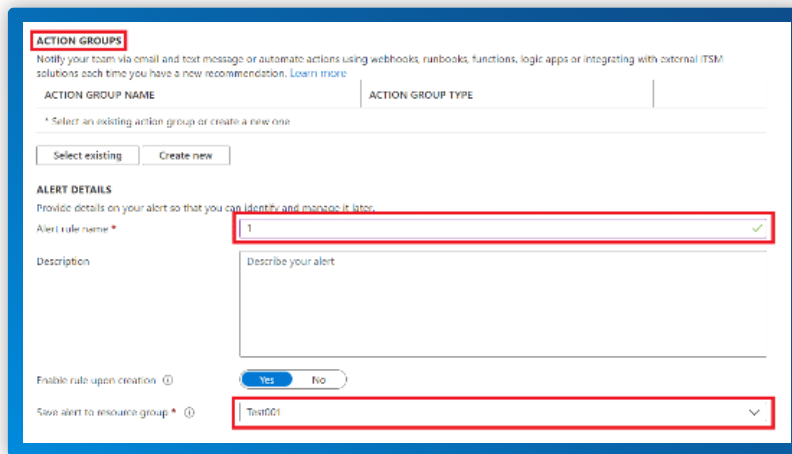
- Increase the reliability of audit logs
- Media service
  - Increase Media Services quotas or limits to ensure continuity of service.
- MySQL server
  - Scale the MySQL server to higher SKU
  - Increase the MySQL server vCores
  - Move your MySQL server to Memory Optimized SKU
  - Add a MySQL Read Replica server
  - Scale the storage limit for MySQL server
  - Improve MySQL connection management

**Set a Recommendation Type Alert For More Granularity**



### 3. Configuring the Action Group and Alert Details

Once you have configured the scope and condition, you need to assign the action group, provide the alert with a name, and save it to a resource group.



Finalizing Your Azure Advisor Alert

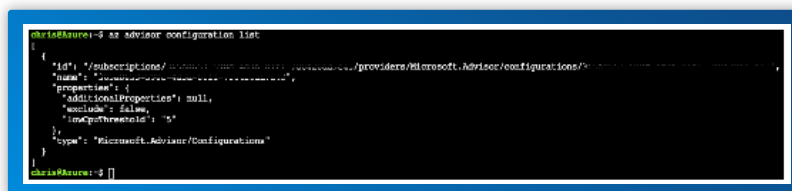
### Managing Azure Advisor with Azure CLI

In addition to the Azure Portal, you can also manage Azure Advisor by using the Azure CLI. However, the Azure Portal has far more features and settings. For example, you can only list, enable, and disable particular recommendations using the Azure CLI.

In the following screenshot, running the command

```
az advisor configuration list
```

displays the complete list of user-configured Azure Advisor configurations.



A Screenshot of the Azure CLI

As an example, if you wanted to disable the recommendation for one day, you could run the following Azure CLI command:

```
az advisor recommendation disable --days 1 --ids <ResourceID>
```

For a complete list of Azure CLI Azure Advisor commands, see [az advisor | Microsoft Docs](#).

## Managing Azure Advisor with Azure PowerShell

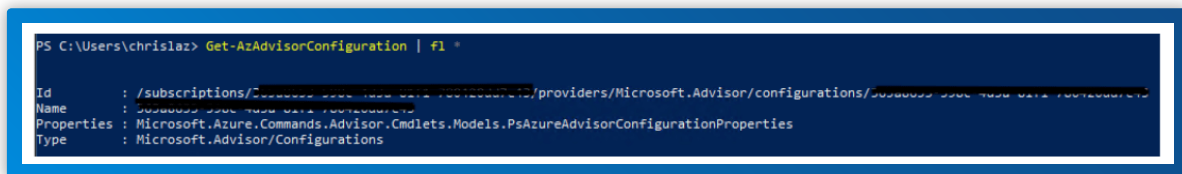
Azure PowerShell offers users and administrators another option for managing Azure Advisor. However, like the Azure CLI, its management options are limited. You can obtain, enable, and disable recommendations, and you can also get and set the Azure Advisor configuration.

For example, running the PowerShell command

```
Get-AzAdvisorConfiguration | fl *
```

returns the same result as the Azure CLI command

```
az advisor configuration list
```



**A Screenshot of Azure Powershell**

If you wanted to disable the recommendation for one day as with the Azure CLI example, you could run the following PowerShell command:

```
Disable-AzAdvisorRecommendation -Days 1 -ResourceID <ResourceID>
```

For a complete list of Azure PowerShell Azure Advisor commands, see [Az.Advisor Module | Microsoft Docs](#).

## Automating Azure Advisor

You can set up automation for Azure Advisor using either a runbook and automation account or custom code powered by a Logic or Function App. However, since Azure automation leverages PowerShell, you are limited to obtaining, enabling, and disabling recommendations (in addition to defining the Azure Advisor configurations).

One workaround is to receive Azure Advisor recommendations as an input for an automation process and, based on a defined threshold, execute against that input. For example, you could check for recommendations and consolidate that data with information from log analytics. Based on the resource's criticality, you could then leverage Azure automation to right-size it.

## Shortcomings and Limitations

Although Azure Advisor has some valuable features, it also has its limitations:

- **No Multi-Cloud Support:** Azure Advisor only offers recommendations for Azure-based services. It does not provide guidance for any other private or public cloud platforms. If the organization has a multi-cloud or hybrid-cloud strategy, this limitation means either managing multiple solutions or implementing a third-party platform.
- **Limited Scope:** Azure Advisor only analyzes and provides recommendations for a subset of Azure services. These include Application Gateway, App Services, availability sets, Azure Cache, Azure Data Factory, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Database for MariaDB, Azure ExpressRoute, Azure Cosmos DB, Azure public IP addresses, Azure Synapse Analytics, SQL servers, storage accounts, Traffic Manager profiles, and virtual machines.
- **No SLA:** Azure Advisor is a free service, so it does not have an SLA.
- **Limited Automation:** Automating interventions based on Azure Advisor recommendations requires effort and technical expertise. You either need to write code that calls the Azure Advisor API or leverages an Azure Automation runbook.
- **Recommendation Limitations:** Although Azure Advisor provides a long list of recommendations for the services it does support, it does not cover every possibility.

## Are Azure Advisor's Recommendations Enough?

Azure Advisor has a lot to offer; its alignment with the Azure Well-Architected Framework helps organizations monitor, analyze, and implement recommendations for their Azure services. However, the service does have its limitations. Since it does not cover every Azure service and offers no multi-cloud support, organizations that want to optimize their workloads using this native solution must also manage additional solutions or implement a third-party platform.

# Chapter 8: Azure Network Security Groups

## The Guide to Azure NSG

An *Azure Network Security Group* (NSG) is a core component of Azure's security fabric. Leveraging an NSG, you can filter traffic to and from Azure resources that you have commissioned on an Azure Virtual Network (VNet).

At its core, an NSG is effectively a set of access control rules you assign to an Azure resource. It inspects inbound and outbound traffic and uses these rules to determine whether it should grant or deny access to a particular network packet. At a high level, Azure groups NSG rules into inbound and outbound. The management and configuration of these rules are similar to those you find on a traditional firewall. Using the Azure Portal, Azure PowerShell, or Azure CLI, you can manage an Azure NSG and specify the source and destination IPs, port, and protocol.

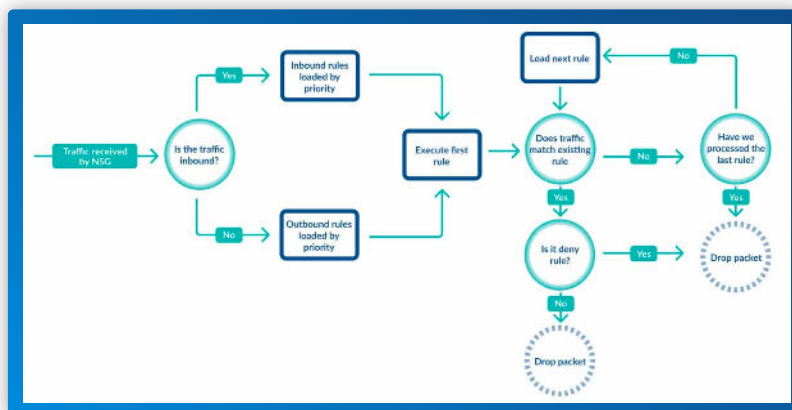
## Azure NSG Capabilities

Azure NSGs control access and manage communication between:

- Individual workloads hosted on one or more Azure VNets.
- Connectivity between on-prem environments and Azure via an Application Gateway, VPN Gateway, Azure Firewall, Azure Bastion service, and Virtual Network Appliances.
- Connections to and from the Internet.

The diagram below details the flow of network traffic and the rule enforcement protocol an Azure NSG follows.

A standard Azure subscription can have up to 5,000 NSGs, and each NSG can have a maximum of 1,000 rules. The table below specifies the rule setting and its associated properties.



A standard Azure subscription can have up to 5,000 NSGs, and each NSG can have a maximum of 1,000 rules. The table below specifies the rule setting and its associated properties.

Storage Type	Description
Name	The name of the rule. This setting is a free text field but must be unique within the NSG.
Priority	This setting needs to be a number between 100 and 4096. The Azure NSG processes its rules in order of priority, with lower numbers processed before higher ones. It is important to note that the Azure NSG will stop processing a network packet when it finds a matching rule. Therefore, should you have another rule with the same attributes lower in the priority list, the NSG will not process it.
Source or Destination	This setting defines the source or destination of the network traffic. It can be set to "Any" for traffic from anywhere, or you could lock it down to a single IP address or an IP range that you need to specify in CIDR notation, e.g., 10.0.0.0/16.
Protocol	This NSG setting describes the network protocol of your rule. You can set it to look for "Any" protocol or specify one of TCP, UDP, ICMP, ESP, or AH.
Direction	This setting defines the direction of the network traffic, and you can set it to either Inbound or Outbound.
Port Range	The port range setting describes the port or ports of the rule. You can specify a single port, e.g., 80, or a range of ports, e.g., 1000-2000.
Action	This setting defines the action the rule will execute. You can set it to either "Allow" or "Deny."

## Azure NSG Rule Enforcement

When you create an Azure NSG, Azure populates it with six default security rules, as illustrated in the image below.

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

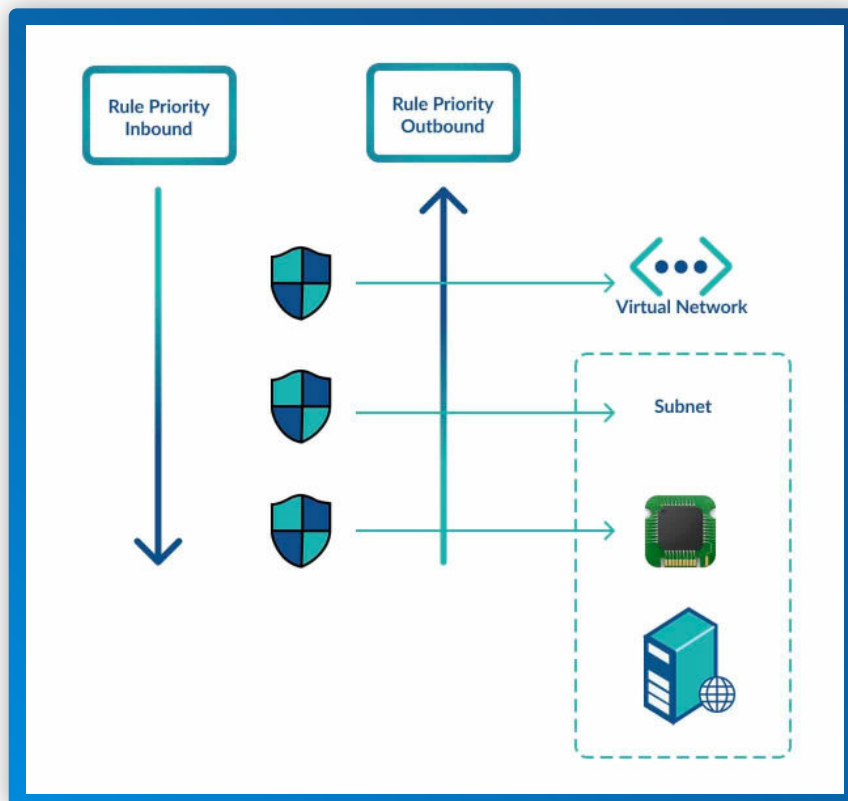
The table below provides details on each rule and its purpose.

Rule Name	Description
AllowVnetInbound	This default rule allows all inbound traffic inside the virtual network. It permits all hosts within the same Vnet and connected subnets to communicate with each other. Note that this rule allows all inbound traffic between all hosts. If your security strategy requires locking some services, you will need to configure additional deny rules to enforce it.

AllowAzureLoadBalancerInBound	This rule allows communication between an Azure Load Balancer and your Azure resources, i.e., VNet or Virtual Machine (VM). Typically, Azure uses this rule to send and receive heartbeats between your VM and the Load Balancer.
DenyAllInbound	This default rule, as the name implies, blocks all inbound traffic. Azure only enforces it after processing every other rule in the list as it has the lowest priority.
AllowVnetOutbound	This default rule allows all outbound traffic inside the virtual network. It permits all hosts within the same Vnet and connected subnets to communicate with each other. Note that this rule allows all outbound traffic between all hosts. If your security strategy requires locking some services, you will need to configure additional deny rules to enforce it.
AllowInternetOutBound	This default rule allows all outbound traffic to the Internet. If your security configuration states that only specific ports and services should be allowed to access the Internet, you will need to configure additional rules.
DenyAllOutbound	This default rule, as the name implies, blocks all outbound traffic. Azure only enforces it after processing every other rule in the list as it has the lowest priority.

## Rule Priorities

As mentioned, Azure NSGs execute rules in order of priority, with the lower numbered priorities processed before high numbers. However, you can also nest NSGs for a particular resource, as shown in the image below. In the diagram, there is a VM running a web server connected to a subnet. That subnet forms part of a more extensive virtual network. The Azure administrator has configured three NSGs and attached one to the virtual network, subnet, and VM's network card.



As there are three active Azure NSGs, configuring rules for the VM requires setting the correct configuration on all three NSGs. For example, if you want to allow access from the Internet to Port 80 (the default HTTP port) on the VM, you will need to create an inbound rule on all three NSGs. Since inbound traffic first traverses the virtual network, then routes to the subnet, and finally the VM's network card, every NSG needs an allow rule. These explicit allow rules are required because each NSG has the default DenyAllInbound rule.

For outbound traffic, NSG rules are enforced in reverse. For example, let's assume the webserver also provides an SMTP service to other VMs hosted on the same VNet and your security policies dictate that you cannot send any SMTP traffic to the Internet. In that case, you would need to configure an allow SMTP rule on the VM network card's NSG and the subnet's NSG to allow SMTP traffic to flow between the VMs within the VNet. The DenyAllOutbound rule on the virtual network's NSG will prevent any Internet-bound SMTP traffic from leaving the VNet.

## Azure NSG Flow Logs

The primary purpose of an Azure NSG is to protect resources commissioned on an Azure virtual network. However, security best practices state that continuous monitoring of your environment is vital. As incoming alerts can help you identify any security incidents, putting measures in place that monitor your environment is crucial.

[Azure NSG Flow Logs](#) is a feature provided by [Azure Network Watcher](#). This service allows you to log IP traffic information for data flowing through your configured NSGs. Azure sends this flow log data to an Azure storage account where you can access it or export it for analysis by a SIEM or IDS.

## Azure NSG Flow Log Use Cases

Azure NSG Flow Logs give you the insight you need to monitor your environment for security, compliance, and performance. By analyzing data on the current state of your Azure virtual network, they provide vital information such as which services have connections, where those connections are coming from, and which ports are open to the Internet. You can leverage Azure Flow Logs in several different use cases, as illustrated in the table below.

Use Case	Features
Network Monitoring	<ul style="list-style-type: none"> <li>Identify unknown or suspicious network traffic.</li> <li>Monitor bandwidth consumption and traffic levels.</li> <li>Leverage filtering by IP and port to baseline application behavior.</li> <li>Export log data for reporting or live monitoring dashboard feeds.</li> </ul>
Usage Monitoring and Optimization	<ul style="list-style-type: none"> <li>Identify the top talkers in your network.</li> <li>Leverage Geo-IP and identify cross-region traffic.</li> <li>Utilize flow log data for capacity forecasting.</li> <li>Identify and resolve unoptimized traffic rules.</li> </ul>
Compliance	<ul style="list-style-type: none"> <li>Verify your traffic rules adhere to network isolation and compliance obligations.</li> </ul>
Network Forensics and Security Analysis	<ul style="list-style-type: none"> <li>Export flow log data to any IDS or SIEM.</li> <li>Analyze network flow from suspicious IPs or network interfaces.</li> </ul>

## How Azure NSG Flow Logs Work

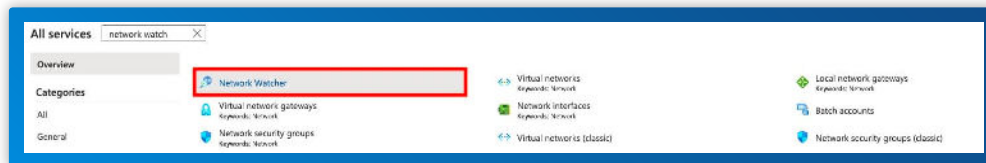
Azure NSG Flow Logs record all IP flows in and out of an NSG, and Azure collects this data at one-minute intervals. The service stores the logged information in JSON format with a default retention period of one year for all logs. It is vital to note that Azure sets NSG Flow Logs to be disabled by default. However, you can activate and manage this service using several Azure management capabilities, including the Azure Portal, Azure CLI, and Azure PowerShell.

## Enabling Azure NSG Flow Logs using the Azure Portal

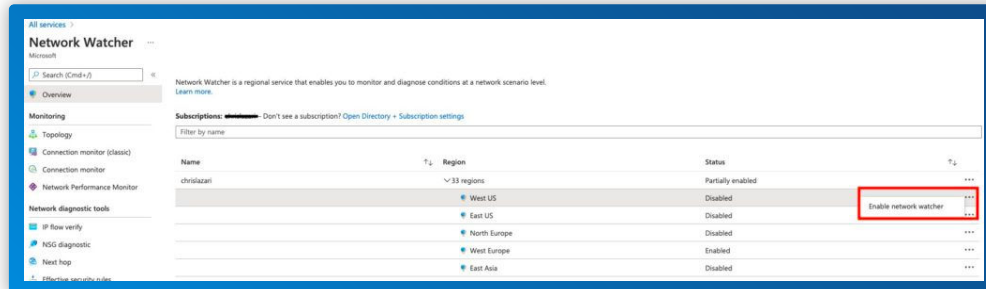
Before activating the Azure NSG Flow Logs using the Azure Portal, you need to enable the Network Watcher and register the Insights provider.

Enabling the Network Watcher via the Azure Portal is a quick, three-step process.

Search for Network Watcher after selecting All Services in the Azure Portal.

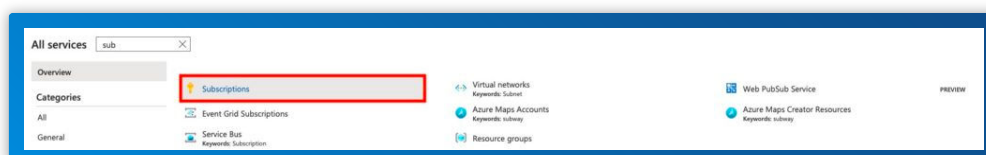


Then, select the region associated with your virtual network and NSG, and enable the Network Watcher as illustrated in the image below.



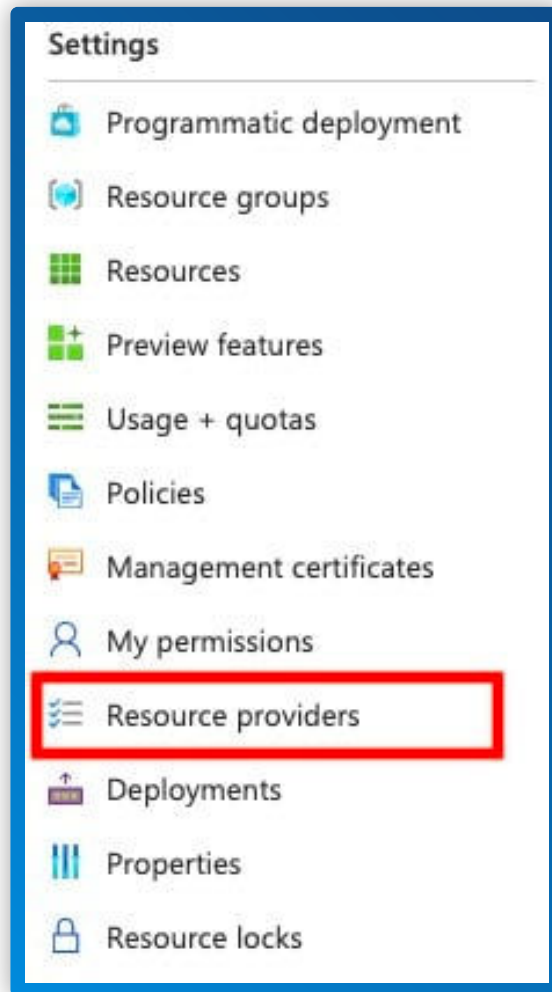
The Microsoft Insights provider is a prerequisite for Azure NSG flow logging. You can follow the steps below to enable it using the Azure Portal.

Search for Subscriptions after selecting All Services in the Azure Portal.

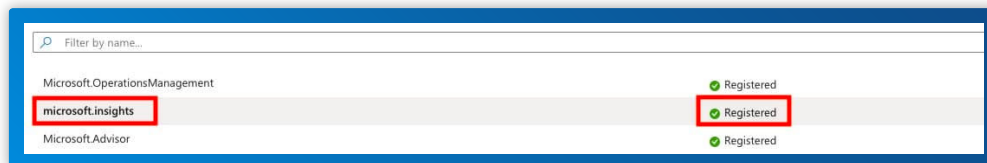


Open the relevant subscription, and on the blade menu, select Resource Providers under the Settings section.





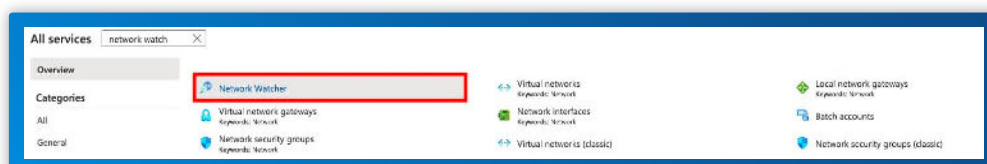
Confirm microsoft.insights displays as registered as shown in the image below.



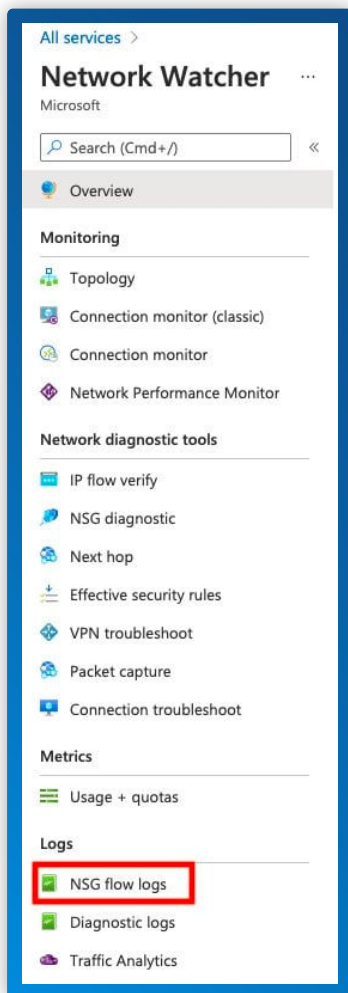
As mentioned, NSG Flow logs require a storage account to store data. If you do not have a storage account, you will need to create one before enabling NSG flow logging.

Once you have confirmed that the Network Watcher is enabled, the Microsoft Insights Provider is registered, and you have a storage account available, you can enable Azure NSG flow logging by following these steps.


Search for Network Watcher after selecting All Services in the Azure Portal.



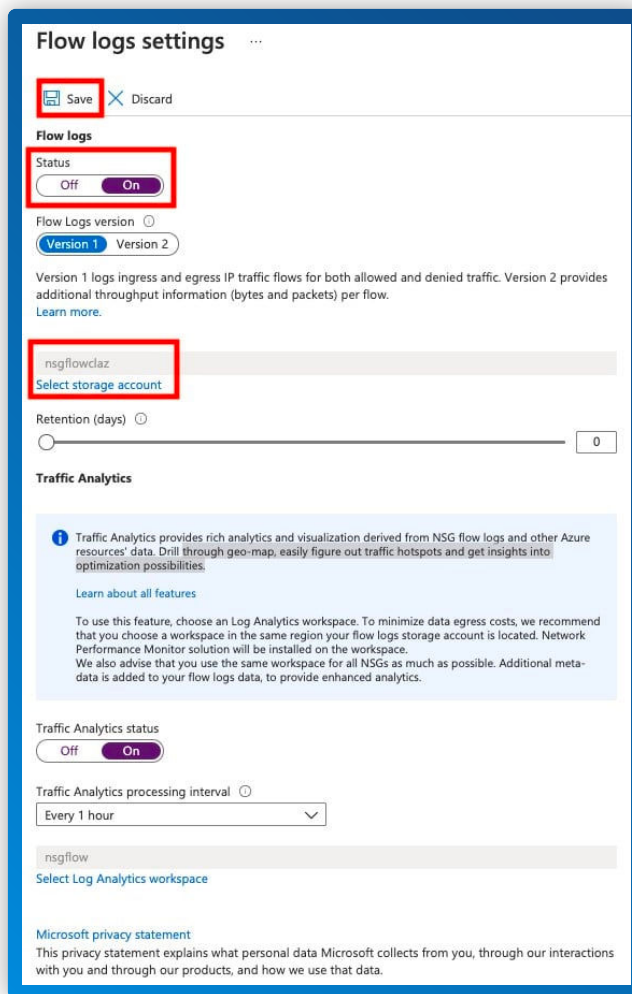
On the left-hand vertical navigation, select NSG flow logs.



Click on the NSG you want to monitor with Azure NSG Flow Logs.

Name	Resource type	Resource group	Status
 NSG1	Network security group	Temp	⊖ Disabled

Set the Flow log status to On, select your storage account, and click Save. You can also set other options for NSG flow logs on this form. For example, version 1 only logs ingress and egress IP traffic flow for both allowed and denied traffic, whereas version 2 provides additional throughput information (bytes and packets) per flow. You can also enable Traffic Analysis if you have a Log Analytics Workspace configured. This feature offers other rich analytics and visualizations, such as the ability to drill through geo-map, quickly figure out traffic hotspots, and get insights into optimization possibilities.



## Enabling Azure NSG Flow Logs using the Azure CLI

You can also enable Azure NSG Flow Logs using the Azure CLI. As with the Azure Portal, you first need to register the Insights Provider. The Azure CLI command for actioning this step is:

```
az provider register --namespace Microsoft.Insights
```

Once you have confirmed registration of the Insights Provider, you can run this command to enable NSG Flow logging:

```
az network watcher flow-log create --resource-group resourceGroupName --enabled true --nsg nsgName --storage-account storageAccountName --location location
```

Azure also allows you to configure additional settings for Azure NSG flow logging via the Azure CLI. For example, if you want to enable logging with version 2, you can run this command:

```
az network watcher flow-log create --resource-group resourceGroupName --enabled true --nsg nsgName --storage-account storageAccountName --location location --format JSON --log-version 2
```

# Enabling Azure NSG Flow Logs using Azure PowerShell

You can also manage Azure NSG Flow Logs with Azure PowerShell.

First, you need to set your variables, as shown in the script example below.

```
$NW = Get-AzNetworkWatcher -ResourceGroupName NetworkWatcherRg -Name NetworkWatcher_  
$nsg = Get-AzNetworkSecurityGroup -ResourceGroupName nsgRG -Name nsgName  
$storageAccount = Get-AzStorageAccount -ResourceGroupName StorageRG -Name contosostorage123  
Get-AzNetworkWatcherFlowLogStatus -NetworkWatcher $NW -TargetResourceId $nsg.Id
```

If you want to enable Traffic Analysis, you will also need to set these parameters.

```
$workspaceResourceId =  
"/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourcegroups/trafficanalyticserg/providers/microsoft.operationalinsights/workspaces/taworkspace"  
$workspaceGUID = "cccccccc-cccc-cccc-cccc-cccccccccccc" $workspaceLocation = " e.g.  
westcentralus"
```

The following Azure PowerShell commands provide examples of enabling NSG flow logging with various options.

## Configure Version 1 Flow Logs

```
Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher $NW -TargetResourceId $nsg.Id  
-StorageAccountId $storageAccount.Id -EnableFlowLog $true -FormatType Json -FormatVersion 1
```

## Configure Version 2 Flow Logs and configure Traffic Analytics

```
Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher $NW -TargetResourceId $nsg.Id  
-StorageAccountId $storageAccount.Id -EnableFlowLog $true -FormatType Json -FormatVersion 1
```

## Configure Version 2 Flow Logs with Traffic Analytics Configured

```
Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher $NW -TargetResourceId $nsg.Id  
-StorageAccountId $storageAccount.Id -EnableFlowLog $true -FormatType Json -FormatVersion 2  
-EnableTrafficAnalytics -WorkspaceResourceId $workspaceResourceId -WorkspaceGUID  
$workspaceGUID -WorkspaceLocation $workspaceLocation
```

## Query Flow Log Status

```
Get-AzNetworkWatcherFlowLogStatus -NetworkWatcher $NW -TargetResourceId $nsg.Id
```

# Azure NSG Best Practices

Working with multiple NSGs can be challenging, especially if you need to understand the effective rules when two or more NSGs control your network traffic. However, following a few best practices can help you manage Azure NSGs more effectively.

## Align NSGs to Resource Groups and Services

You do not need to configure an NSG for every Azure resource hosted on a virtual network. Depending on your use case, you could easily manage all your rules at the VNet or subnet level. However, it is important to keep maintainability in mind.

For example, managing all your access rules in a single NSG may seem more straightforward because you do not need to factor in any other NSG rules. However, an NSG can have up to 1,000 rules, and maintaining hundreds of allow and deny settings can become complex as you scale. In turn, this complexity can lead to oversights and misconfigurations. As with any other technology implementation, the structure needs to align with the strategy. As you develop your Azure security strategy, make sure to keep the maintainability of your NSG rules in mind.

For instance, instead of having a single NSG for an entire VNet, consider aligning your NSGs with a particular resource group or service. Using this approach allows you to manage and maintain a smaller set of rules that is easier and more efficient. It also offers additional security when you decommission services. You can delete the NSG with its resource group, mitigating the risk of open rules you no longer need.

## Use Logical Naming Conventions

Azure gives you a lot of flexibility when it comes to naming resources. If you label your Azure NSGs with a naming convention that provides the reader with enough information, it will reduce the amount of effort needed to support your Azure environment. For example, if you need to commission an NSG for a VM named SRV-WEB-01, naming it NSG-SRV-WEB-01 is far easier for support to identify than a generic name such as NSG01.

## Leverage IP Ranges to Streamline Rule Creation

Azure NSGs allow you to either specify a single IP address and port or enter a range. Where possible, use ranges instead of individual addresses, as it will limit the number of rules you need to create and manage. However, if you need to restrict access to a single resource, then a single IP Address and port are advisable.

## Leave Spaces Between Rule Priority Numbers

As mentioned, Azure NSGs process rules in order of priority, with the lower numbers processed first. Therefore, when creating rules, leave enough space between your priorities in case you need to create a rule that requires processing before a preceding rule. For example, start your first rule with a priority of 110 instead of 100. Using this approach will give you the flexibility in the event you need to create another rule that needs to precede it.

## Use Tags to Improve Readability

When you need to manage multiple objects, you can leverage [virtual network service tags](#). These Azure resources represent a group of IP address prefixes that relate to a particular Azure service. For example, "VirtualNetwork" represents the entire VNet address range, and "Internet" indicates all external IP addresses that are publicly routable. Therefore, using the tags in your source and destination fields enhances the readability of your NSG rules.

## Azure NSG Shortcomings and Limitations

Although Azure NSGs offer adequate security, they do have some limitations. Microsoft offers [Azure Firewall](#), a highly available, managed service providing additional security features relevant to some use cases. The table below details the functionality available for both security products.

Feature	Azure NSG	Azure Firewall
OSI Layers	Filters traffic on Layer 3 (network) and Layer 4 (session).	Filters traffic on Layer 3 (network), Layer 4 (session), and Layer 7 (application).
Protocol-based traffic filtering	Yes	Yes
Service Tag support	Yes	Yes
Fully Qualified Domain Name (FQDN) Tag support	No	Yes – With Azure Firewall, you can tag a group of fully qualified domain names, like Windows Updates or Microsoft 365 services.
Source Network Address Translation (SNAT)	No	Yes – Azure Firewall allows you to configure a public IP to mask an internal IP.
Destination Network Address Translation (DNAT)	No	Yes – Azure Firewall supports DNAT, which you can use to translate incoming traffic to the private IP address of your virtual network.
Integrated with Azure Monitor	Yes – However, Flow Logs with Traffic Analysis is not enabled by default.	Yes – However, diagnostic logging is not enabled by default.
Threat Intelligence	No	Yes – Azure Firewall gives you the ability to block traffic based on Microsoft threat analytics data.