Agenda: Azure Storage Service

- About Storage Service and Account
- Creating a Storage Account
- Working with Blob Storage
    - Types of Blobs (Block, Append, Page)
    - Container and Metadata
    - Soft Copy
    - Azure Storage Explorer
    - Transfer Data using AzCopy
    - Programming Blob Storage
    - Async Blob Copy
    - Import and Export Service
    - Implement and Configure CDN
    - Configure Custom Domain
    - Scale Blob Storage
    - Storage Service Encryption
- Manage Access / Securing Storage
    - Create and Manage Shared Access Signature
    - Account SAS vs Service SAS
    - Using Stored Access Policies
    - Regenerating Keys
    - Encrypt Keys using Azure Key Vault integration
    - Programming in C#
- Working with Table Storage
    - Understanding NoSQL Database
    - Creating Table and Entities using Storage Explorer
    - Entities and Properties
    - Table storage vs COSMOS DB Table API
    - Programming Table Storage
- Azure Queues Storage
    - Understanding Async Communication using Queues
    - Comparing Azure Queues and Service Bus Queues

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

    - Programming Queues
- Azure SMB File Storage
    - Common usage of File Storage
    - Shares, Directory and File
    - Managing Using Azure Portal
    - Programming File Storage
- Azure File Sync
- Configure diagnostics, monitoring and analytics
    - Capturing Metrics Data
    - Analyzing Diagnostic Data
    - Capturing Logs
    - Retention Policies and Logging Levels
    - Analyze Logs
    - Enabling Monitoring
    - Enabling Alerts

About Azure Storage Service and Account

Cloud computing enables new scenarios for applications requiring **scalable, durable and highly available** storage for their data – which is exactly why Microsoft developed **Azure Storage Service.**

- Azure Storage is a **PaaS service** that you can use to store both **unstructured** and **partially structured** data.
- **Azure Storage is massively scalable and elastic:** It can store and process **hundreds of terabytes of data** to support the big data scenarios required by scientific, financial analysis, and media applications. Or you can store the **small amounts of data** required for a small business website.
- By default, you can create up to **100 storage accounts** in a single Azure subscription. Each standard storage account can contain up to **500 TB** of combined blob, queue, table and file data.
- As the demands on your storage application grow, Azure Storage **automatically allocates** the appropriate resources to meet them. **We are charged only for what we use**.

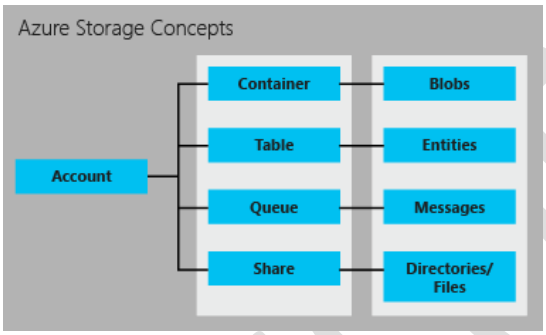
It offers **four types of storage services**, depending on the type of data that they are designed to store:

1. **Blob Storage** stores file data. A blob can be any type of **text or binary data**, such as a document, media file, or application installer. Blob Storage is sometimes referred to as **Object storage**.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

2. **Table Storage** stores partially structured datasets. Table storage is a **NoSQL** key-attribute data store, which allows for rapid development and fast access to large quantities of data.
3. **Queue Storage** provides **reliable messaging** for workflow processing and for communication between components of cloud services.
4. **File Storage** Similar to blobs, these provide storage for unstructured files, but they offer support for file sharing in the same manner as traditional on-premises Windows file shares.



Azure Storage Account

An Azure storage account is a **secure account** that gives you access to services in Azure Storage. Your storage account provides the unique namespace for your storage resources. There are two types of storage accounts:

1. A **standard storage** account includes Blob, Table, Queue, and File storage.

Standard storage accounts are backed by magnetic drives (HDD) and provide the lowest cost per GB. They are best for applications that require bulk storage or where data is accessed infrequently.

2. A **premium storage** account is ideally supposed to be used for Azure Virtual Machine disks.

Premium storage accounts are backed by solid state drives (SSD) and offer consistent low-latency performance. They can only be used with Azure virtual machine disks and are best for I/O-intensive applications, like databases. Additionally, virtual machines that use Premium storage for all disks qualify for a 99.9% SLA, even when running outside an availability set.

Creating Storage Account

1. Azure Portal → Browse Storage Accounts → **New** → **Data + Storage** → **Storage account**
2. Enter Name (must be all lowercase)
3. Deployment Model = Resource Manager
4. and select Subscription, Resource Group, Location
5. **Account Kind**: Storage (general purpose v1) / **StorageV2 (general purpose v2)** / Blob Storage

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- ~~**General-purpose v1** accounts: Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.~~
- ~~**Blob storage accounts**: Blob-only storage accounts. Supports Block blobs and append blobs only. Use general-purpose v2 accounts instead when possible.~~
- **General-purpose v2 accounts**: Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.
- **Block blob storage accounts**: Blob-only storage accounts with premium performance characteristics. Recommended for scenarios with high transactions rates, using smaller objects, or requiring consistently low storage latency.
- **FileStorage storage accounts**: Files-only storage accounts with premium performance characteristics. Recommended for enterprise or high performance scale applications.

Storage account type	Supported services	Supported performance tiers	Replication options
~~**BlobStorage**~~	~~Blob (block blobs and append blobs only)~~	~~Standard~~	~~LRS, GRS, RA-GRS~~
~~**General-purpose V1**~~	~~Blob, File, Queue, Table, and Disk~~	~~Standard, Premium~~	~~LRS, GRS, RA-GRS~~
General-purpose V2	Blob, File, Queue, Table, and Disk (VHD)	Standard	LRS, GRS, ~~RA-GRS~~, ZRS, ZGRS ~~RA-ZGRS~~
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS
FileStorage	Files only	Premium	LRS
Page Blobs	Disk (VHD)	Premium	LRS

6. Performance: **Standard / Premium**

   Standard use HDD Drives and Premiun use SSD Drives

   Premium is used for disks of VMs (Page Blobs)

   Note that it is not possible to convert a Standard storage account to Premium storage account or vice versa.

7. Access tier: Cool / **Hot**

   Account kind: **Blob storage,** Performance**: Standard**

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- Access tier: **Hot**, if objects will be **more** frequently accessed. This allows you to store data at a **lower access cost.**
- Access tier: **Cool**, if objects will be **less** frequently accessed. This allows you to store data at **a lower data storage cost.**
- Acces tier: **Archive.** The archive tier is optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days. The archive tier is the most cost-effective option for storing data, but accessing that data is more expensive than accessing data in the hot or cool tiers. It is available at level of an individual blob only, not at the storage account level. Only block blobs and append blobs can be archived.

Rehydrate an archived blob to an online tier:

- To read data in archive storage, you must first change the tier of the blob to hot or cool. This process is known as rehydration and can take hours to complete.
- There are currently two rehydrate priorities, High and Standard, which can be set via the optional **x-ms-rehydrate-priority** property on a **Set Blob Tier or Copy Blob** operation.
  - **Standard priority**: The rehydration request will be processed in the order it was received and may take up to 15 hours.
  - **High priority**: The rehydration request will be prioritized over Standard requests and may finish in under 1 hour.

8. Replication:

Locally redundant storage (LRS):

- **Replicates 3 times within a single data center in a single region where Storage Account is created.**
- Locally redundant storage (LRS) provides at least 99.999999999% (11 nines) durability of objects over a given year.
- The replicas are spread across UDs and FDs within one storage scale unit (A storage scale unit is a collection of racks of storage nodes.)
- A request returns successfully only once it has been written to all three replicas.
- This architecture ensures your data is available if a hardware failure affects a single rack or when nodes are upgraded during a service upgrade.
- LRS is less expensive than GRS and also offers higher throughput.
- For Premium Storage accounts - This is the only option available.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

Zone-redundant storage (ZRS)

- Replicates your data across three (3) storage clusters in a single region. Each storage cluster is physically separated from the others and resides in its own availability zone. Each availability zone, and the ZRS cluster within it, is autonomous, with separate utilities and networking capabilities.
- ZRS is not yet available in all regions.
- Once you have created your storage account and selected ZRS, you **cannot convert** it to use to any other type of replication, or vice versa.
- Consider ZRS for scenarios that require strong consistency, strong durability, and high availability even if an outage or natural disaster renders a zonal data center unavailable.
- **What happens when a zone becomes unavailable?** Your data is still accessible for both read and write operations even if a zone becomes unavailable. Microsoft recommends that you continue to follow practices for **transient fault handling**. These practices include implementing retry policies with exponential back-off.

Geo-redundant storage (GRS)

- GRS maintains **6 copies** of your data. 3 replicas in **primary region** and also replicates your data 3 additional times to a **secondary region** that is hundreds of miles away from the primary region.
- 99.99999999999999 (16 9s) Availablility is supported when calculated around a year.
- Data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable.
- If failure occurs in the primary region, Azure Storage **automatically failover** to the secondary region.
- An update is first committed to the primary region, where it is replicated three times. Then the update is replicated to the secondary region, where it is also replicated three times.
- Requests to write data are replicated **asynchronously** to the secondary region. It is important to note that opting for GRS does not impact latency of requests made against the primary region.
- The secondary region is **automatically determined** based on the primary region, and cannot be changed.

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

- As with GRS, your data replicates asynchronously across two regions and synchronously within each region, yielding six copies of a storage account.
- This is default option when we create a storage account.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- In the event that data becomes unavailable in the primary region, your application can **read data** from the secondary region.
- If your primary endpoint for the Blob service is **myaccount.blob.core.windows.net**, then your secondary endpoint is **myaccount-secondary.blob.core.windows.net**. The **access keys** for your storage account are the **same** for both the primary and secondary endpoints.

More Details: https://azure.microsoft.com/en-in/documentation/articles/storage-redundancy/

9. Secure transfer required = **Disabled** / Enabled

   If Enabled only HTTPS requests will be accepted.

   This option doesn't work with Custom Domain Names for Storage account.
10. Select Subscription, Resource Group, Location
11. Virtual network: Disabled
12. Click on "Create".

PowerShell Command to Create Storage Account

Login-AzureRmAccount

Create a storage account.

- **New-AzureRmStorageAccount** -ResourceGroupName "DemoRG" -Name "dssdemostorage" -SkuName Standard_LRS -Location 'South India'

Modify storage account properties, such as type.

- **Set-AzureRmStorageAccount** -ResourceGroupName "DemoRG" -AccountName "dssdemostorage" -Type "Standard_RAGRS"

Retrieve a specific storage account or all the storage accounts in a resource group or subscription.

- **Get-AzureRmStorageAccount** -ResourceGroupName "DemoRG" -AccountName "dssdemostorage"

Pricing and Billing

All storage accounts use a pricing model for blob storage based on the tier of each blob.

When using a storage account, the following billing considerations apply:

- **Storage costs**: In addition to, the amount of data stored, the cost of storing data varies depending on the storage tier. The per-gigabyte cost decreases as the tier gets cooler.
- **Data access costs**: Data access charges increase as the tier gets cooler. For data in the cool and archive storage tier, you are charged a per-gigabyte data access charge for reads.
- **Transaction costs**: There is a per-transaction charge for all tiers that increases as the tier gets cooler.

- **Geo-Replication data transfer costs**: This charge only applies to accounts with geo-replication configured, including GRS and RA-GRS. Geo-replication data transfer incurs a per-gigabyte charge.
- **Outbound data transfer costs**: Outbound data transfers (data that is transferred out of an Azure region) incur billing for bandwidth usage on a per-gigabyte basis, consistent with general-purpose storage accounts.
- **Changing the storage tier**: Changing the account storage tier from cool to hot incurs a charge equal to reading all the data existing in the storage account. However, changing the account storage tier from hot to cool incurs a charge equal to writing all the data into the cool tier (GPv2 accounts only).

Azure Storage encryption for data at rest

- Azure Storage automatically encrypts your data when persisting it to the cloud.
- Storage accounts are encrypted regardless of their performance tier (standard or premium)
- All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted.
- Encryption does not affect Azure Storage performance.
- You can rely on **Microsoft-managed keys** for the encryption of your storage account, or you can manage encryption with your own keys.
- If you choose to manage encryption with your own keys, you have two options:
    - You can specify a **customer-managed key**. It is used to encrypt all data in all services.
    - You can specify a **customer-provided key on Blob** storage operations. A client making a read or write request against Blob storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.

	Microsoft-managed keys	Customer-managed keys	Customer-provided keys
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	Azure Key Vault or any other key store
Key rotation responsi-bility	Microsoft	Customer	Customer
Key usage	Microsoft	Azure portal, Storage Resource Provider REST API, Azure Storage management libraries, PowerShell, CLI	Azure Storage REST API (Blob storage), Azure Storage client libraries
Key access	Microsoft only	Microsoft, Customer	Customer only

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

Working with Blob Storage

- **Blobs** are binary large objects. The Blob service stores text and binary data.
- Blob storage is also referred to as **object storage**.
- You can use Blob storage to store content such as:
    - Documents
    - Social data such as photos, videos, music, and blogs
    - Backups of files, computers, databases, and devices
    - Images and text for web applications
    - Configuration data for cloud applications
    - Big data, such as logs and other large datasets
- Every blob is organized into a **container**. Containers also provide a useful way to assign security policies to groups of objects. A storage account can contain any number of containers, and a container can contain any number of blobs, up to the **500 TB capacity** limit of the storage account.
- **Creating BLOB Hierarchies:** The blob service in Azure Storage is based on a **flat storage scheme**. This means that creating a container one level below the **root is the only true level of container**. However, you can specify a delimiter as part of the blob name to create your own **virtual hierarchy**. For example, you could create a blob named **/January/Reports.txt** and **/February/Reports.txt**, and filter based on **/January or /February** in most tools that support Azure Storage. Most third-party storage tools allow you to create folders within a container, but they are actually being clever with the name of the blob itself.

Blobs are addressable using the following URL format:

http(s)://<storage account name>.**blob**.core.windows.net/<container>/<blob name>

Types of blobs:

1. **Block blobs** are optimized for streaming (**sequential access**) and for uploads and downloads, and are a good choice for storing documents, media files, backups etc. Azure divides data into smaller blocks of up to 100 megabytes (MB) in size, which subsequently **upload or download in parallel**. Individual block blobs (file) can be up to 100 GB in size. One blob can have max of 50,000 blocks.
2. **Append blobs:** Append blobs are similar to block blobs, but are optimized for append operations. This works best with **logging and auditing** activities. Updating or deleting of existing blocks is not supported. Max block size can be 4 MB only.

3. **Page blobs** are optimized for **random read/write** operations and provide the ability to write to a range of bytes in a blob. Blobs are accessed as **pages**, each of which is up to **512 bytes** in size. Each Page blob can be up to **8TB** each. Is best suited for **virtual machine disks (VHD)**.

Additional Topics

- Snapshot
- Versions
- What is Lease
- Metadata
- Soft Delete

Azure Storage Explorer

Microsoft Azure Storage Explorer is a standalone app from Microsoft that allows you to easily work with Azure Storage data.

Some of the benefits of Azure Storage Explorer are:

a) Access multiple accounts and subscriptions across Azure

b) Create, delete, view, and edit storage resources.

c) View and edit Blob, Queue, Table, File, Cosmos DB storage and Data Lake Storage.

d) Obtain shared access signature (SAS) keys.

e) Available for Windows, Mac, and Linux

Azure Storage Explorer has many uses when it comes to managing your storage. See the following articles to learn more. Also, check out the videos that follow this topic.

- **Connect to an Azure subscription:** Manage storage resources that belong to your Azure subscription.
- **Work with local development storage:** Manage local storage by using the Azure Storage Emulator.
- **Attach to external storage:** Manage storage resources that belong to another Azure subscription or that are under national Azure clouds by using the storage account's name, key, and endpoints.
- **Attach a storage account by using an SAS:** Manage storage resources that belong to another Azure subscription by using a shared access signature (SAS).
- **Attach a service by using an SAS:** Manage a specific storage service (blob container, queue, or table) that belongs to another Azure subscription by using an SAS.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- **Connect to an Azure Cosmos DB account by using a connection string:** Manage Cosmos DB account by using a connection string.

Transfer data with the AzCopy

AzCopy is a command-line utility designed for copying data to/from Microsoft Azure Blob, File, and Table storage, using simple commands designed for optimal performance. You can copy data between a file system and a storage account, or between storage accounts.

The basic syntax for AzCopy commands is:

```
azcopy source destination [options]
```

Login to Azure Storage:

- Login: **azcopy login**
- Login to specific tenant: azcopy login --tenant-id=sandeepsonideccansoft.onmicrosoft.com

Note: The login user should have **Storage Blob Account Reader/Owner/Contributor** Role

To copy from Local to Azure storage

- Copy file: **azcopy copy** "d:\demo.txt" "https://dssdemostorage.blob.core.windows.net/con1/demo.txt"
- Copy Directory: **azcopy copy** "D:\Temp\Demo\" "https://dssdemostorage.blob.core.windows.net/demo" --recursive=true

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

What's new

- Synchronize a file system to Azure Blob or vice versa. Ideal for incremental copy scenarios.
- Supports Azure Data Lake Storage Gen2 APIs.
- Supports copying an entire account (Blob service only) to another account.
- Account to account copy is now using the new Put from URL APIs. No data transfer to the client is needed which makes the transfer faster.
- List/Remove files and blobs in a given path.
- Supports wildcard patterns in a path as well as –include and –exclude flags.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- Improved resiliency: every AzCopy instance will create a job order and a related log file. You can view and restart previous jobs and resume failed jobs. AzCopy will also automatically retry a transfer after a failure.
- General performance improvements.
- Can copy from and to to AWS S3 stoage.

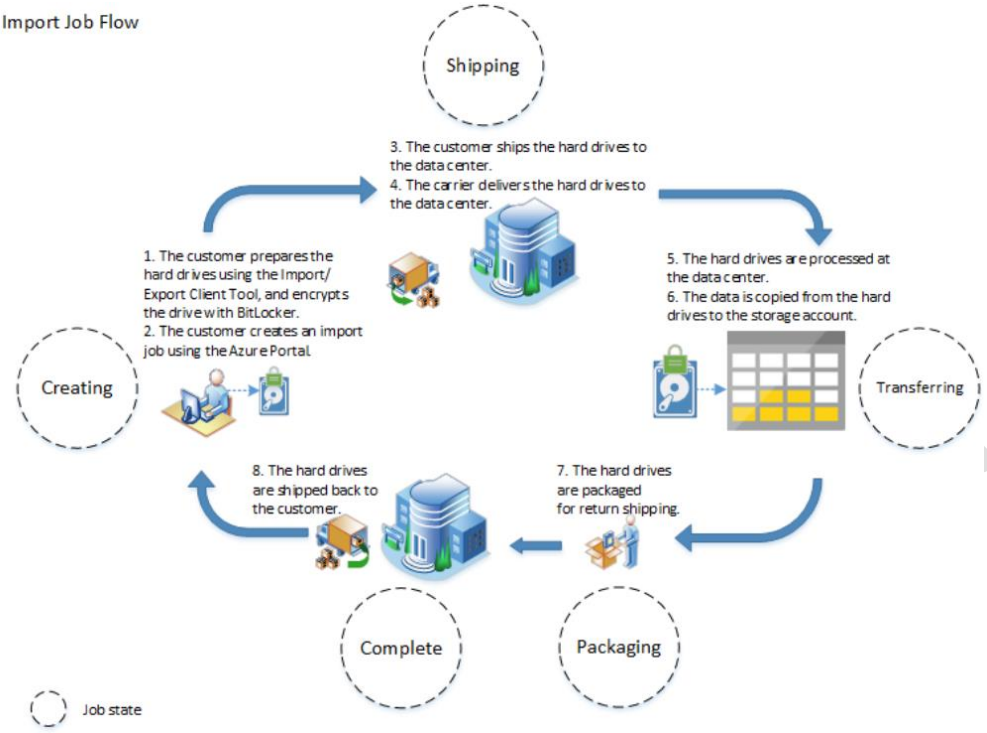
Import and Export Service

When it comes to transferring very large amounts of data to or from the cloud you will want to consider using the Azure Import/Export service. The Azure Import/Export Service allows you to:

- **Import to Azure Storage**. Securely transfer large amounts of data to Azure Blob storage (block and page blobs) and Azure Files by **shipping disk drives** to an Azure data center. In this case, you will be shipping hard drives containing your data.
- **Export from Azure Storage**. Transfer data from Azure storage to hard disk drives and ship to your on-premise sites. Currently, you can only export **Block** blobs, **Page** blobs or **Append** blobs from Azure storage using this service. Exporting Azure Files is not currently supported. In this case, you will be shipping empty hard drives.

✔ **Only 2.5" SSD or 2.5" or 3.5" SATA II or III internal HDD are supported for use with the Import/Export service.**

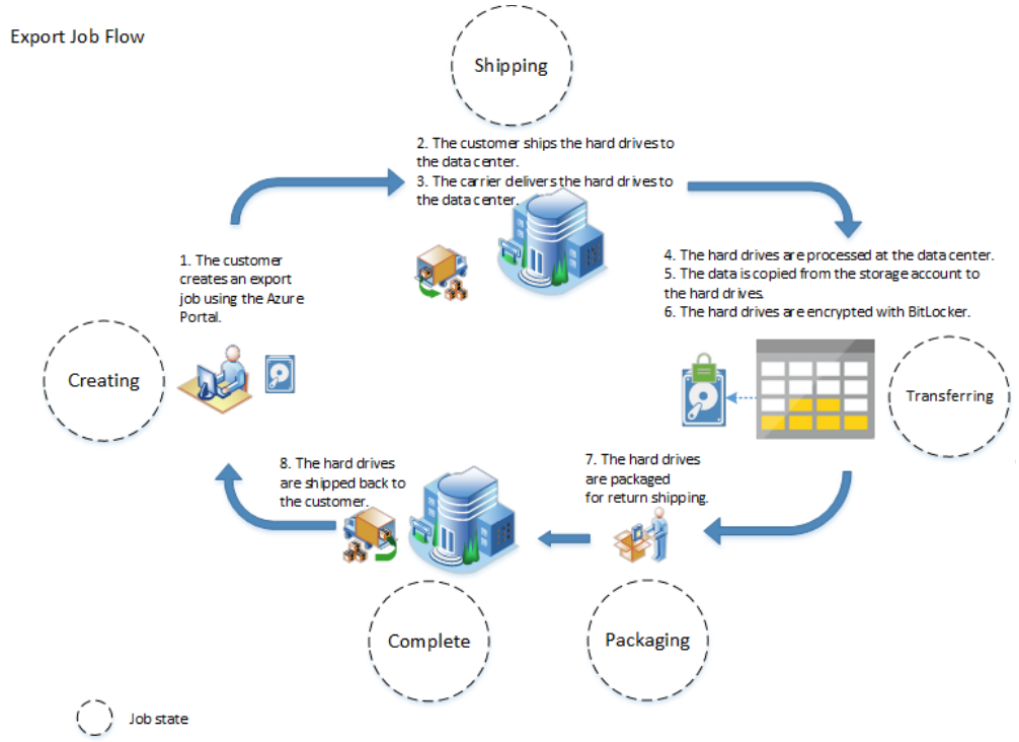
Import Job



At a high level, an import job involves the following steps:

1. Create an Azure Storage account.
2. Determine data to be imported, number of drives you need, destination blob location for your data in Azure storage.
3. Use the **WAImportExport.EXE tool** to copy data to disk drives. **Encrypt** the disk drives with **BitLocker**. **This creates a .jrn file**.
4. Create an import job in your target storage account in Azure portal. Upload the drive **journal files**.
5. Provide the **return address** and carrier account number for shipping the drives back to you.
6. Ship the disk drives to the shipping address provided during job creation.
7. Update the delivery tracking number in the import job details and submit the import job.
8. The drives are received and processed at the Azure data center.
9. The drives are shipped using your carrier account to the return address provided in the import job.

Export Job



At a high level, an export job involves the following steps:

1. Determine the data to be exported, number of drives you need, source blobs or container paths of your data in Blob storage.
2. Create an export job in your source storage account in Azure portal.
3. Specify source blobs or container paths for the data to be exported.
4. Provide the return address and carrier account number for shipping the drives back to you.
5. Ship the disk drives to the shipping address provided during job creation.
6. Update the delivery tracking number in the export job details and submit the export job.
7. The drives are received and processed at the Azure data center.
8. The drives are encrypted with BitLocker and the keys are available via the Azure portal.
9. The drives are shipped using your carrier account to the return address provided in the import job.

Note:

Block blobs, Page blobs, and Append blobs will be exported. Export of Azure Files is not supported.

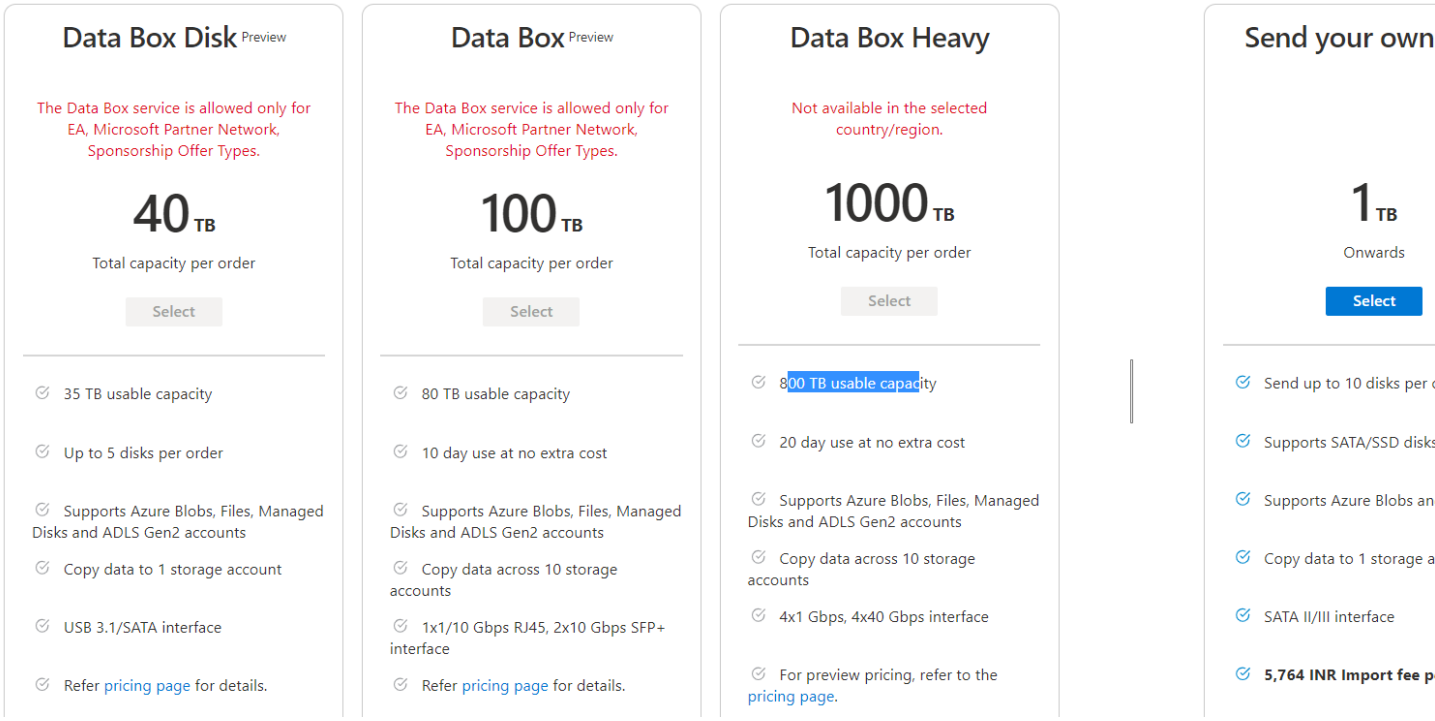
Azure Import/Export Tool

The Microsoft Azure Import/Export Tool (**WAImportExport.exe**) is the drive preparation and repair tool that you can use with the Microsoft Azure Import/Export service. You can use the tool for the following functions:

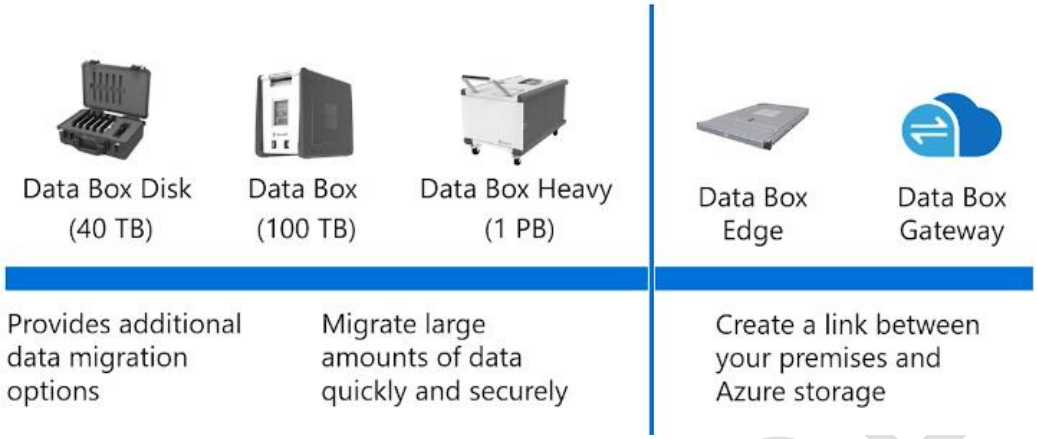
- Before creating an import job, you can use this tool to copy data to the hard drives you are going to ship to an Azure data center.
- After an import job has completed, you can use this tool to repair any blobs that were corrupted, were missing, or conflicted with other blobs.
- After you receive the drives from a completed export job, you can use this tool to repair any files that were corrupted or missing on the drives.

Import/Export service requires the use of internal SATA II/III HDDs or SSDs. Each disk contains a single NTFS volume that you encrypt with BitLocker when preparing the drive. To prepare a drive, you must connect it to a computer running a **64-bit version of the Windows client or server operating system** and run the WAImportExport tool from that computer. **The WAImportExport tool handles data copy, volume encryption, and creation of journal files**. Journal files are necessary to create an import/export job and help ensure the integrity of the data transfer.

Azure Portal → Storage Account → **Data transfer**



Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)



Programming BLOB Storage using Powershell

Step 1: Copy Keys: Storage accounts → <Account Name> → Settings → Access Keys → Copy Keys for future use.

To Create a Container:

```
Login-AzureRmAccount
Set-AzureRmContext -SubscriptionName "Visual Studio Enterprise - SS"
```

$ctx = (Get-AzureRmStorageAccount -ResourceGroupName TestRG -StorageAccountName dssdemostorage).Context

New-AzureStorageContainer -Name "democontainer" -Context $ctx -Permission Off

You can optionally enable anonymous access at the container level for blob storage. The available options for this security policy are described as below:

Access Type	Resulting access
Off	No anonymous access (default)
Blob	Access blobs via anonymous requests
Container	List and access blobs via anonymous requests

To Upload a local file to Container:

Set-AzureStorageBlobContent -Container democontainer -File D:\happy.gif -Blob happy.gif **-Context $ctx**

OR

Set-AzureRmCurrentStorageAccount -StorageAccountName **dssdemostorage** -ResourceGroupName DemoRG

Set-AzureStorageBlobContent -Container democontainer -File D:\happy.gif -Blob happy.gif

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

To download BLOB

$blob = **Get-AzureStorageBlobContent** -Blob happy.gif -Container democontainer

Upload file and set Metadata:

$meta = @{"key" = "value"; "name" = "test"}

Set-AzureStorageBlobContent -File D:\demo.txt -Container democontainer **-Metadata $meta -Context $ctx**

To get Metadata of BLOB

$CloudBlockBlob = [Microsoft.WindowsAzure.Storage.Blob.**CloudBlockBlob**] $blob.ICloudBlob

$CloudBlockBlob.**FetchAttributes**()

$meta = $CloudBlockBlob.**Metadata**

$meta["name"]

Using the Async blob copy service:

The async blob copy service is a server side based service that can copy files you specify from a source location to a destination in an Azure Storage account. The source blob can be located in another Azure Storage account, or it can even be outside of Azure as long as the storage service can access the blob directly for it to copy.

```
$vhdName = "[file name]"
$srcContainer = "[source container]"
$destContainer = "[destination container]"
$srcStorageAccount = "[source storage]"
$destStorageAccount = "[dest storage]"

Login-AzureRmAccount
$srcStorageKey = (Get-AzureStorageKey -StorageAccountName $srcStorageAccount).Primary
$destStorageKey = (Get-AzureStorageKey -StorageAccountName $destStorageAccount).Primary

$srcContext = New-AzureStorageContext –StorageAccountName $srcStorageAccount -StorageAccountKey
$srcStorageKey
$destContext = New-AzureStorageContext –StorageAccountName $destStorageAccount -StorageAccountKey
$destStorageKey

New-AzureStorageContainer -Name $destContainer -Context $destContext
```

```
$copiedBlob = Start-AzureStorageBlobCopy -SrcBlob $vhdName -SrcContainer $srcContainer -Context $srcContext
-DestContainer $destContainer -DestBlob $vhdName -DestContext $destContext
```

Copy SPECIFIC BLOB from one container to another:

Get-AzureStorageContainer -Name $srcContainer | **Start-AzureStorageBlobCopy** -SrcBlob $vhdName -DestContainer $destContext

Copy ALL BLOBS from one container to another

Get-AzureStorageBlob -Container $srcContainer | **Start-AzureStorageBlobCopy** -DestContainer $destContext

Copy a blob from a URI:

Start-AzureStorageBlobCopy -AbsoluteUri "http://www.contosointernal.com/planning" -DestContainer $destContext -DestBlob $vhdName -DestContext $Context

Shared Access Policy and Shared Access Signature (SAS) Token

There are two techniques for controlling access to objects within an Azure Storage account.

1. Using the **access/authentication key and storage account name** is one technique – Gives FULL ACCESS
2. Granting access using a **shared access signature (SAS Token)** (with or without **shared access policy)** to allow granular access with expiration is another technique.

A shared access signature (SAS) is a URI that grants **restricted access rights** to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified **period of time**.

- A shared access signature (SAS) is a **token** that can be appended to a URL that enables delegated access to a storage resource.
- Anyone who possesses the token can access the resource it points to with the permissions it specifies, for the period of time that it is valid.

Azure Storage supports two kinds of shared access signatures:

1. An **Account SAS** delegates access to resources in **one or more** of the storage services. You can also delegate access to read, write, and delete operations on blob containers, tables, queues, and file shares that are not permitted with a service SAS.
2. The **Service SAS** delegates access to a resource in **just one** of the storage services: Blob, Queue, Table, or File service.

Note that **Stored Access Policies** are currently not supported for an **Account-Level SAS**.

Creating an **Account SAS** (for many operations)

1. Azure Portal → Storage Accounts → Select Account
2. Settings → **Shared access signature**
3. Provide the options as required → Generate SAS
4. Copy the SAS token and share it with the client.

https://dssdemostorage.blob.core.windows.net/container1/Azure%20Storage%20Service.pdf?sv=2017-11-09&ss=b&srt=co&sp=r&se=2018-08-13T10:05:57Z&st=2018-08-11T02:05:57Z&spr=https&sig=hFYQeZ2fvj52%2BQl0kg%2BbPmErr8J%2F5hKrGkAnF7Q7u%2F4%3D

Stored Access Policies

A Shared Access Signature can take one of two forms:

- **An ad hoc SAS**. When you create an ad hoc SAS, the start time, expiration time, and permissions for the SAS are all specified on the SAS URI (or implied in the case where the start time is omitted). This type of SAS can be created on a container, blob, table, or queue.
- **An SAS with a Stored Access Policy**. A stored access policy is defined on a resource container—a blob container, table, or queue—and can be used to manage constraints for one or more Shared Access Signatures. When you associate an SAS with a stored access policy, the SAS inherits the constraints—the start time, expiration time, and permissions—defined for the stored access policy.

Note: Stored access policies give you the option to revoke permissions without having to regenerate the storage account keys. Set the expiration on these to be a very long time (or infinite), and make sure that it is regularly updated to move it further into the future.

Create Ad-hoc Service SAS using Portal

1. Azure Portal → Storage Accounts → Select Account
2. BLOB → Container → <Select Blob Item> → **Click on Generate SAS Tab**
3. Provide the details → … → Generate SAS

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

4. Copy the Token and use with Blob URL.

Create Stored Access Policy using Portal

1. Azure Portal → Storage Accounts → Select Account
2. BLOB → Container → Select the container → right click → Access Policy → + Add Policy

Create SAS using Stored Access Policy using Portal

1. Azure Portal → Storage Accounts → Storage Explorer
2. BLOB → Container → Select the container / Blob → Right Click → Get Shared Access Signature
3. Select the Stored Access Policy and create the SAS.

Stored Access Policy and SAS Token if Deployment Model = Resource Manager

```
$storageAccountName = 'dssdemostorage'
$rgName = 'DemoRG'
$containerName = 'container1'

$accountKeys = Get-AzureRmStorageAccountKey -ResourceGroupName $rgName -Name $storageAccountName
$storageContext = New-AzureStorageContext -StorageAccountName $storageAccountName -StorageAccountKey
$accountKeys[0].Value
$expiryTime = (get-date).AddYears(1)
$startTime = (get-date).AddHours(-1)
$permission = "rwl"

//Creates a STORED ACCESS POLICY for an Azure storage container.
New-AzureStorageContainerStoredAccessPolicy -Context $storageContext -Container $containerName -Policy
"testPolicy" -ExpiryTime $expiryTime -Permission $permission

//Creates a SAS Token using a STORED ACCESS POLICY
$sasToken = New-AzureStorageContainerSASToken  -Name $containerName -Policy "testPolicy" -Context
$storageContext
Write-Host "SAS token (ref shared access policy): $sasToken"

//Creates a SAS Token with Adhoc Access Policy
```

```
$sasContainerToken2 = New-AzureStorageContainerSASToken -Name $containerName -Context $storageContext
-Permission rwl -StartTime $startTime -ExpiryTime $expiryTime
Write-Host 'SAS token: ' $($sasToken2)

//Create a SAS Token for a specific BLOB Item
$sasBlobToken3 = New-AzureStorageBlobSASToken -Container "container1" -Blob "SmileyNormal.png" -Context
$storageContext  -Permission "rwd" -StartTime $startTime -ExpiryTime $endTime
```

It's in query string format. This is a query string that can be appended to the full URI of the blob or container the SAS URI was created with, and passed to a client.

Example: http://dssdemostorage.blob.core.windows.net/secure/reports1.xlsx***?sv=2014-02-14&sr=b&sig=8qLv51D3ahgw9Zoyf9vhVfSvOuVdak%2Fdh1gIHmb6pII%3D&st=2014-11-29T12%3A17%3A50Z&se=2014-11-29T16%3A17%3A50Z&sp=rwd***

Note: SAS Token without policy cannot be revoked.

Similarly we have:

- New-AzureStorageQueueSASToken
- New-AzureStorageTableSASToken
- New-AzureStorageFileSASToken

Summary:

SAS Token

Account SAS

Always Ad-hoc

Same SAS token can be used for **all** services.

Service SAS

Ad-hoc / Policy based

Specific to **only one** service at a time.

Container SAS token works for all blobs in that container

Blob SAS token is only for the blob for which it is generated

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

Overview of Azure AD for Blobs and Queues

- When a security principal attempts to access a blob or queue resource, the request must be authorized
- The authentication step requires that an application request an OAuth 2.0 access token at runtime
- The authorization step requires that one or more RBAC roles be assigned to the security principal

Built-in RBAC roles for blobs and queues

- Storage Blob Data Owner
- Storage Blob Data Contributor
- Storage Blob Data Reader
- Storage Queue Data Contributor
- Storage Queue Data Reader
- Storage Queue Data Message Processor
- Storage Queue Data Message Sender

Resource Scope

The levels at which you can scope access to Azure blob and queue resources:

- An individual container
- An individual queue
- The storage account
- The resource group
- The subscription

Azure Storage Firewalls and Virtual Networks

Azure Storage Firewall and Virtual Networks protect storage at the network level.

Considerations:

- Configure a rule to deny access from all networks and then grant access to traffic from specific virtual network subnets only.
- If needed, configure rules to grant access to allow connections from specific internet or on-premises clients.
- Network rules are enforced on all network protocols to Azure storage, including REST and SMB.
- Once network rules are applied, they're enforced for all requests, including those based on SAS.
- Virtual machine disk traffic is not affected by network rules.
- Classic storage accounts do not support firewalls and virtual networks.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

Azure Blob storage lifecycle

The lifecycle management policy lets you:

- Transition blobs to a cooler storage tier (hot to cool, hot to archive, or cool to archive) to optimize for performance and cost
- Delete blobs at the end of their lifecycles
- Define rules to be run once per day at the storage account level
- Apply rules to containers or a subset of blobs (using prefixes as filters)

Azure Portal → Select Storage Account → Blob Service → Lifecycle Management

Code View:

```
{
 "rules": [
  {
   "name": "ruleFoo",
   "enabled": true,
   "type": "Lifecycle",
   "definition": {
    "filters": {
     "blobTypes": [ "blockBlob" ],
     "prefixMatch": [ "container1/foo" ]
    },
    "actions": {
     "baseBlob": {
      "tierToCool": { "daysAfterModificationGreaterThan": 30 },
      "tierToArchive": { "daysAfterModificationGreaterThan": 90 },
      "delete": { "daysAfterModificationGreaterThan": 2555 }
     },
     "snapshot": {
      "delete": { "daysAfterCreationGreaterThan": 90 }
     }
    }
   }
  }
```


Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

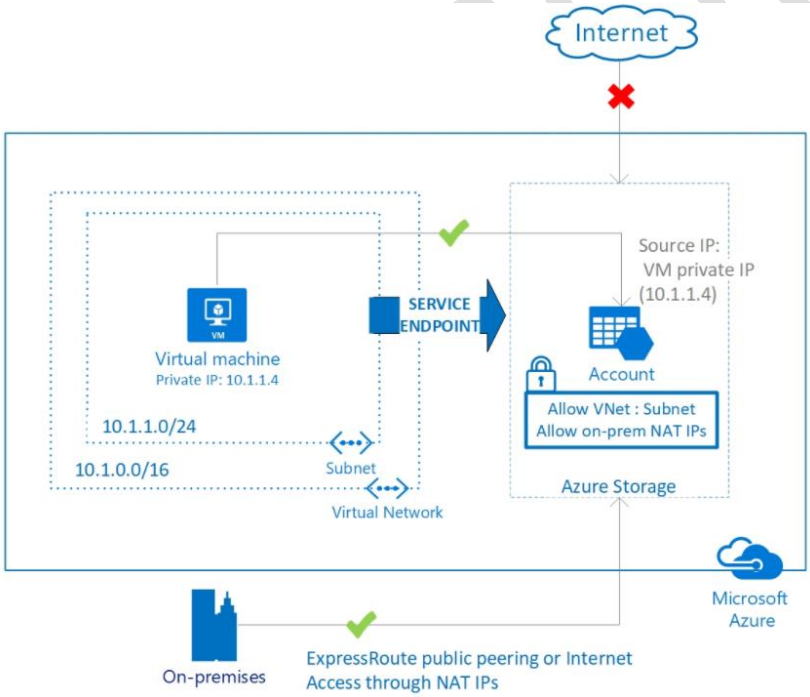
```
 ]
}
```

Service Endpoints

- By default, storage accounts accept connections from clients on any network
- Virtual network service endpoints enable you to limit network access to Azure service resources. Access is limited to just the virtual network subnets and IP addresses you specify.

Currently, Azure supports service endpoints to these services: Cosmos DB, Event Hub, Key Vault, SQL, and Storage and few more…

Endpoints allow you to secure your critical Azure service resources to your virtual networks.



Walkthrough: To restrict access to Storage Account BLOB only from a VM in a given Subnet.

1. Create a virtual network
    a. One subnet with **disabled Service EndPoint**
    b. Another subnet with **enabled service endpoint**. Eg: Storage Service
2. Create a Storage Account
    a. Create a Container (Name = demo, Access Level = Blob)
    b. Upload a file to the container.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

c. Copy the URL of the uploaded file (eg: https://dsdemostorage.blob.core.windows.net/demo/Demo.txt)

3. Note that the URL is currently accessible from everywhere (from VM inside vNET and from my local machine outside vNET)
4. Restrict access to Azure PaaS service (Storage Account) only from **second** subnet.
   a. **Storage Account → Networking → Firewalls and virtual networks Tab**
   b. Select Selected networks
   c. Select VNet and Second Subnet
   d. Save.
5. Confirm access is denied to a resource from another subnet of vNET and also from the internet (my machine)

   Your Local Machine → Browser → URL of BLOB uploaded to Storage Account
   a. Note that you **are not able** to view the blob/file content
6. Confirm access to a resource from an allowed subnet.

   VM created in second subnet → Browser → URL of BLOB uploaded to Storage Account
   a. Note that you are **able** to view the blob/file content.

Note: You can add your machine IP Address under filewall and access the Storage Account from your local machine.

Problems:

a) The Storage Account PaaS is always used using it's Public IP and that may not be allowed in many corporate networks as it would require explicit whitelisting of the Public IP in corporate Firewall.

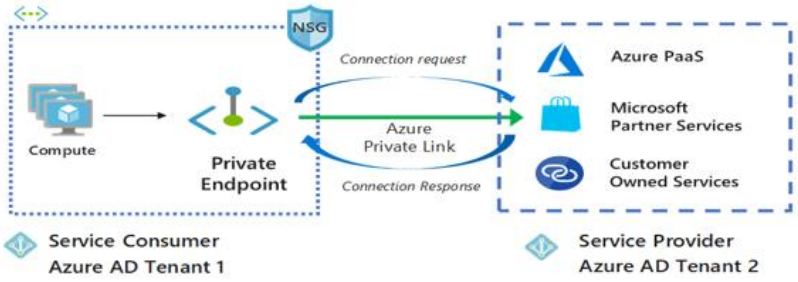
b) Explicit need for adding every subnet (of vNET)

Note: Azure Storage File Service can be used for this demo.

Azure Private Link

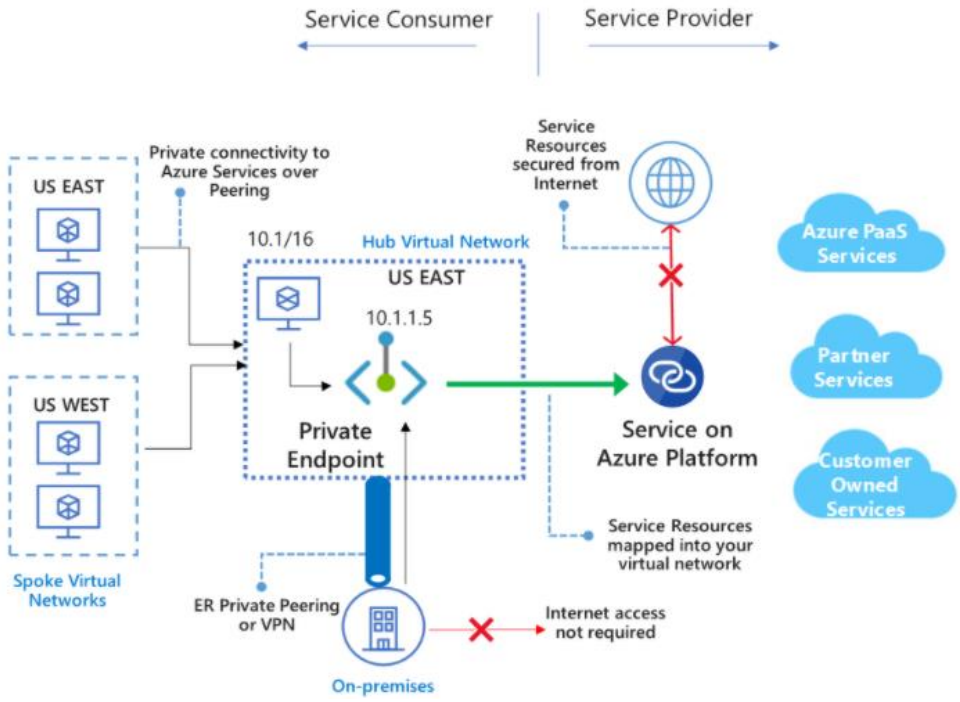
Azure Private Link enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)



Azure Private Link works on an approval call flow model wherein the Private Link service consumer can request a connection to the service provider for consuming the service. The service provider can then decide whether to allow the consumer to connect or not. Azure Private Link enables the service providers to manage the private endpoint connection on their resources.

Traffic between your virtual network and the service travels the Microsoft backbone network. Exposing your service to the public internet is no longer necessary.



KeyPoints

- Block public access with the firewall.
- Internal DNS resolves to private IP
- NSG's are not applied to the private endpoint.

Azure Private Link provides the following benefits:

- **Privately access services on the Azure platform**: Connect your virtual network to services in Azure without a public IP address at the source or destination. Service providers can render their services in their own virtual network and consumers can access those services in their local virtual network. The Private Link platform will handle the connectivity between the consumer and services over the Azure backbone network.
- **On-premises and peered networks**: Access services running in Azure from on-premises over ExpressRoute private peering, VPN tunnels, and peered virtual networks using private endpoints. There's no need to configure ExpressRoute Microsoft peering or traverse the internet to reach the service. Private Link provides a secure way to migrate workloads to Azure.
- **Protection against data leakage**: A private endpoint is mapped to an instance of a PaaS resource instead of the entire service. Consumers can only connect to the specific resource. Access to any other resource in the service is blocked. This mechanism provides protection against data leakage risks.
- **Global reach**: Connect privately to services running in other regions. The consumer's virtual network could be in region A and it can connect to services behind Private Link in region B.
- **Extend to your own services**: Enable the same experience and functionality to render your service privately to consumers in Azure. By placing your service behind a standard Azure Load Balancer, you can enable it for Private Link. The consumer can then connect directly to your service using a private endpoint in their own virtual network. You can manage the connection requests using an approval call flow. Azure Private Link works for consumers and services belonging to different Azure Active Directory tenants.

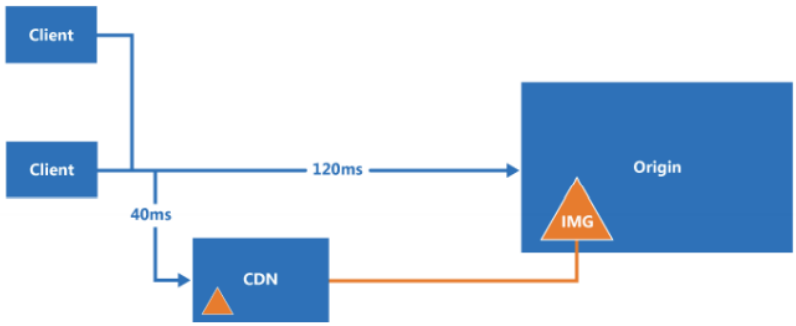
Walkthrough: To Ensure that Azure PaaS service uses Private IP, if requested from vNET and public IP, if requested from outside the vNET.

1. Create a Virtual Machine to test the private endpoint is working from it.
2. Create a Storage Account, Add Public Container and upoad a file.
3. Create a **Private Endpoint**: **Search Private Link → Create private endpoint → Enter Basic details**
    1. **Resource type = Microsoft.Storage/storageAccounts**
    2. **Resource = <Storage Account>**
    3. **Target sub-resource = blob**
    4. Select Virtual Network and Subnet in which it Private IP will be created.
    5. Integrate with Private DNS zone = Yes and Either create or select DNS zone
    6. Review + Create
    7. This creates a Private DNS (<storageaccount>.blob.core.windows.net) name and NIC with Private IP addres (10.0.1.4).

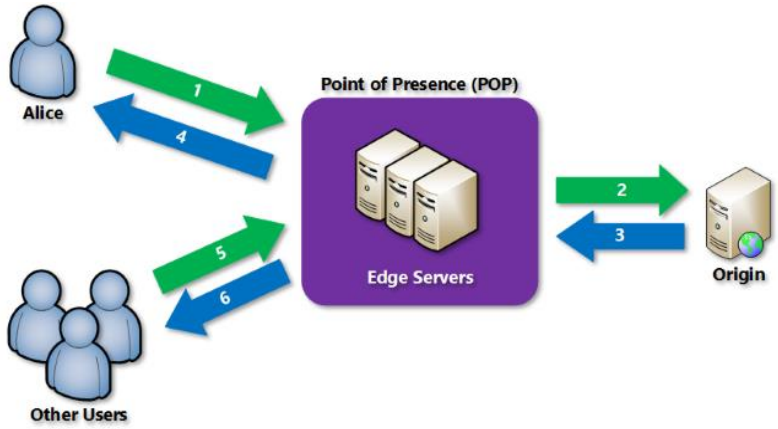
4. Test connectivity to private endpoint from **outside** the VNet (your local machine)
    1. nslookup <storageaccount>.blob.core.windows.net
    2. Note that the IP address listed is **public IP**
    3. Try Access to Blob storage file from local machine and note that is accessible*.
5. *To restrict public access to storage account
    1. Go to Storage Account → Firewalls and virtual networks → Select **Selected Networks** and don't select any network.
    2. Try Access to Blob storage file from local machine and note that it is not accessible*.
6. Test connectivity to private endpoint from **inside** the VNet
    1. RDP to VM
    2. **nslookup** <storageaccount>.blob.core.windows.net
    3. Note that the IP address listed is **private IP (It's the IP Address of the NIC created for Private endpoint)**
    4. Try Acceess to Blob storage file from VM and **it succeeds to connect**.

Implement and Configure Content Delivery Network

- Azure provides Content Delivery Network (CDN) functionality, which **decreases the time** it takes to download web content by first distributing it across **multiple locations around the world** and then delivering it from the location that is closest to the consumer of that content.
- CDNs are typically used to deliver **static content** such as images, style sheets, documents, client-side scripts, and HTML pages.



Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)



1. A user (Alice) requests a file (also called an asset) using a URL with a special domain name, such as <endpointname>.azureedge.net. DNS routes the request to the best performing Point-of-Presence (POP) location, which is usually the POP that is geographically closest to the user.
2. If the edge servers in the POP do not have the file in their cache, the edge server requests the file from the origin.
3. The origin returns the file to the edge server, including optional HTTP headers describing the file's Time-to-Live (TTL).
4. The edge server caches the file and returns the file to the original requestor (Alice). The file remains cached on the edge server until the TTL expires. Azure CDN automatically applies a default **TTL of seven days** unless you've set up caching rules in the Azure portal.
5. Additional users may then request the same file using that same URL and may also be directed to that same POP.
6. If the TTL for the file hasn't expired, the edge server returns the file from the cache.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

Typical uses for a CDN include:

- Delivering static resources for client applications, often from a website.
- Delivering public **static and shared** content to devices such as cell phones and tablet computers.
- Serving entire websites that consist of only public static content to clients, without requiring any dedicated compute resources.
- Streaming video files to the client on demand.
- Generally improving the experience for users, especially those located far from the datacenter hosting the application.
- Supporting IoT (Internet of Things) solutions, such as distributing firmware updates.
- Coping with peaks and surges in demand without requiring the application to scale, avoiding the consequent increased running costs.

Azure content delivery networks cache content from

1. Azure Storage blobs
2. Web Apps
3. PaaS cloud services
4. Custom origin (any public web location that you can access by using HTTP or HTTPS)

Important points to be noted:

- If you modify an object that's currently cached in the CDN, the updated content **will not be** available via CDN until CDN refreshes its content after the **time-to-live period** for the cached content expires.

- CDNs are intended for **static content**. Dynamic content needs to be refreshed constantly from the content provider, minimizing and potentially eliminating any associated CDN benefits.
- The CDN service is **global** and **not bound to a location**, however you must specify a resource group location where the metadata associated with the CDN profile will reside. This location will not have any impact on the runtime availability of your profile.

CDNs offer a number of advantages:

1. **Improved user-experience**, especially if users reside in areas distant from the original content location.
2. **Improved scalability** by eliminating performance bottlenecks that are associated with hosting content in a single location.
3. **Increased resiliency** (capacity to recover) by eliminating a single point of failure. In particular, if one CDN node becomes unavailable, content transparently retrieves from the next nearest node.

Creating CDN profiles and endpoints

- A CDN profile is a collection of CDN endpoints with the same pricing tier and provider (origin).
- The profile constitutes an administrative and billing unit according to its pricing tier.
- The profile also provides additional features, such as country filtering, which includes blocking or allowing access to cached content from designated countries and analytics reporting.
- A CDN profile can contain up to **four endpoints**, and there is a limit of **eight CDN profiles** per Azure subscription.

Walkthrough:

1. All Services → CDN Profiles → + Add
2. Name = DemoProfile
3. In the **CDN profile** blade, click **+ Endpoint**.
4. In the **Add an endpoint** blade, specify the following:
    - Name. This is a unique name in the **azureedge.net** Domain Name System (DNS) namespace.
    - **Origin type.** This is **Storage**, Cloud service, Web app, or Custom origin.
    - **Origin hostname**. This is the name of the host that represents the origin type that you selected. This can be a name that displays automatically for Azure resources, an FQDN, or its corresponding IP address for custom origins.
    - **Origin path**. This allows you to specify a directory path to retrieve from the origin..

- **Origin host header**. This is designates the host header value that should be sent to the origin with each request. This is useful if you host multiple virtual domains on a single target server.
- **Protocol and origin port:** HTTP with the default port 80 and HTTPS with the default port 443.

5. Click **Add**.

The **metadata** to control the **TTL**, and also the **content type**, is set on each blob as it is **uploaded**. The max-age attribute is measured in seconds. In the following example, the TTL is set to 86400 seconds, or 1 day.

$blobProperties = @{**ContentType**="img/png"; **CacheControl="**public, max-age=86400**"** }

Set-AzureStorageBlobContent -File $_.FullName -Container $container -Context $context **-Properties $blobProperties**

For every endpoint, you can configure a number of settings, such as:

CDN Profiles → Select Profile → Click on Endpoints → Select Endpoint

- **Compression**: Compress x` CDN to reduce size and improve performance. All listed MIME types will be compressed when enabling the feature. Note that files are only compressed on the fly by the CDN if it is served from CDN cache. Compressed by the origin can still be delivered compressed to the client without being cached..
- **Cache rules: Query string caching behavior**. This setting controls caching behavior, depending on whether the request to the endpoint includes a query string or ignore query strings or ignore caching altogether.

Azure CDN caching rules are available only for **Azure CDN Standard from Verizon** and **Azure CDN Standard from Akamai**.

Custom Caching Rules

The **path** can **match** a single file (e.g. '/pictures/city.png') or a folder (e.g. '/pictures/' or '/pictures/cities/'). When a folder is specified (i.e. with a trailing slash), the filter applies to all files and sub-folders under it

- **Geo-filtering**: Create geo-filtering rules on specific paths on your endpoint to block or allow content in the selected countries.

Caching content from Azure blobs

- For a CDN to cache blobs, users must be able to access the **blobs anonymously**.
- After a CDN is implemented, all publicly available blobs in storage account will be cached.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- A blob stays in the CDN cache for a period known as the Time to Live (TTL), which by default **is seven days**. Therefore, if users access this content frequently in a seven-day period, the CDN will offer a significant performance gain. If users access this content every 10 days, CDN would provide no performance gains.

Caching content from cloud services and web apps

- The content to cache should be static and must be accessible via HTTP on port 80 or HTTPS an 443.
- The cloud service must be in the **production** deployment slot
- The content to cache must be in **/cdn** folder of cloud service.
- Similar to blob-based endpoints, cached content from cloud services has a **seven-day TTL** by default. You can modify this by specifying the **clientCache** setting in the **web.config** file in the **/cdn** folder.

Using custom domains to access CDNs

CDN Profiles → Select Profile → Click on Endpoints → Select Endpoint → **Custom domains**

In several scenarios, you might want to point to CDN-cached content by using names in your own custom DNS namespace. If that is the case, keep in mind that the target names must include a prefix, such as www.adatum.com," and they cannot take the form of a root domain, such as "adatum.com."

Register a custom domain for an Azure CDN endpoint using the intermediary cdnverify subdomain:

1. Navigate to your domain registrar's web site, Create a new CNAME record, and provide a subdomain alias that includes the **cdnverify** subdomain.
   For example, the subdomain that you specify will be in the format **cdnverify.www** or **cdnverify.cdn**. Then provide the host name, which is your CDN endpoint, in the format **cdnverify.<EndpointName>.azureedge.net**. Your DNS mapping should look like: **cdnverify**.www.consoto.com CNAME **cdnverify**.consoto.azureedge.net
2. Add custom domain name for CDN EndPoint. Azure will verify that the CNAME record exists for the cdnverify domain name you have entered.
3. At this point, your custom domain has been verified by Azure, but traffic to your domain is not yet being routed to your CDN endpoint. After waiting long enough to allow the custom domain settings to propagate to the CDN edge nodes (90 minutes for **Azure CDN from Verizon**, 1-2 minutes for **Azure CDN from Akamai**), return to your DNS registrar's web site and create another CNAME record that maps your subdomain to your CDN endpoint. For example, specify the subdomain as **www** or **cdn**, and the hostname as **<EndpointName>.azureedge.net**. With this step, the registration of your custom domain is complete.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

4. Finally, you can delete the CNAME record you created using **cdnverify**, as it was necessary only as an intermediary step.

Current Status: cdn.deccansoft.com => demostroge1.azureedge.net

New Requirement is to Map **cdn.deccansoft.com** => **demostorage2.azureedge.net**

WRONG APPROACH to switch custom domain from demostorage1.azureedge.net to demostorage2.azureedge.net

0. Current DNS Status: cdn.deccansoft.com => demostorage1.azureedge.net

Traffic is sent to demostorage1

1**. DNS Server: cdn.deccansoft.com => demostorage2.azureedge.net**

Traffic is sent to demostorage2 Storage Server but REJECTED as Domain is not VERIFIED

(So here is the downtime for the app using CDN Server)

2. Add a custom domain cdn.deccansoft.com => demostorage2.azureedge.net

Traffic is sent to NEW edge server…

Note: Mapping a domain to an Azure Storage account in DNS with the asverify intermediary domain

CORRECT APPROACH to switch custom domain from demostorage1.azureedge.net to demostorage2.azureedge.net

0. Current DNS Status: cdn.deccansoft.com => demostorage1.azureedge.net

Traffic is sent to demostorage1

1. **DNS Server: cdnverify.cdn.deccansoft.com => cdnverify.demostorage2.azureedge.net**

Traffic is sent to demostorage1

2. CDN Profile Custom Domain Verification: Add a custom domain cdn.deccansoft.com => demostorage2.azureedge.net

Traffic is sent to demostorage1

3. DNS Server: cdn.deccansoft.com => demostorage2.azureedge.net

Traffic is sent to demostorage2

CNAME RECORD	TARGET
asverify.blobs.contoso.com	asverify.contosoblobs.blob.core.windows.net
blobs.contoso.com	contosoblobs.blob.core.windows.net

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

Azure Table Storage

Category(PKCategoryId, CategoryName, ...) - SQL Table

1, Furniture

2, Pets

3, Electronics

4, Plants

…more…

Product(PKProductId, FKCategoryId, ProductName, Price, Quantity) - SQL Table

1, 2, Dog01, 100, 3

2, 2, Cat01, 150, 2

3, 1, Chair01, 100, 100

4, 1, Table01, 50, 20

ProductAttributes (NoSQL Table) – NO FIXED SCHEMA

PartitionKey: 2 (Pets), RowKey:1 (Dog01), Age:3, Breed:Pomerian, Color:White

PartitionKey: 2 (Pets), RowKey:2 (Cat01), Age:1, Breed:Indian, Color:Black

PartitionKey: 1 (Furniture), RowKey:3 (Chair01), Weight: 10KG, Color: Brown, Type: Chair

PartitionKey: 1 (Furniture), RowKey:4 (Table01), Weight: 30KG, Color: Black, Type: Table

- The Azure Table storage service stores large amounts of **partially structured** data offering high availability and massively scalable storage.
- The service is a **NoSQL datastore** which accepts **authenticated calls** from inside and outside the Azure cloud.
- For today's Internet-based applications, NoSQL databases like Table storage offer a popular alternative to traditional relational databases.

Common uses of the Table service include:

- You can use Table storage to store flexible datasets, such as user data for web applications, address books, device information, and any other type of metadata that your service requires.
- Storing datasets that **don't** require complex joins, foreign keys, or stored procedures and can be de-normalized for fast access.

- Quickly querying data using a clustered index (Combination of PartitionKey and RowKey).
- Accessing data using the **OData protocol** and **LINQ queries** with WCF Data Service .NET Libraries.

You can use the Table service to store and query huge sets of structured, non-relational data, and your tables will scale as demand increases.

- **Table**: A table is a collection of entities. Tables don't enforce a schema on entities, which means a single table can contain entities that have different sets of properties. The number of tables that a storage account can contain is limited only by the storage account capacity limit.
- **Entity**: An entity is a set of properties, similar to a database row. An entity can be up to **1MB in size**.
- **Properties**: A property is a name-value pair. Each entity can include up to **252 custom properties** to store up to **1 MB** of data. Each entity also has **3 system** properties that specify a **partition key** (string upto 1KB in size)**, a row key** (string upto 1KB in size) **and a timestamp**. **Entities with the same partition key can be queried more quickly**, and inserted/updated in atomic operations. One batch operation cannot have two entities with different partition key. An entity's row key is its unique identifier within a partition.

The URI for a specific table access is structured as follows:

http://<account>.**table**.core.windows.net/<TableName>

Note about Batch Operations

- A **batch operation** is a collection of table operations which are executed by the Storage Service REST API as **a single atomic** operation.
- A batch operation may contain up to **100 individual table operations**, with the requirement that each operation entity must have **same partition key.**
- The total payload of a batch operation is limited to 4MB.
- A batch with a retrieve operation cannot contain any other operations.

Using Visual Studio Server Explorer

1. Server Explorer → … →Select Windows Azure Storage → Select and Expand Storage Account.
2. Expand to Tables → Create Table…, Enter Name of Table
3. Select Table → Right click → View Table
4. Use the Editor to manage Table.

Choosing Table storage or Cosmos DB Table API

Azure Cosmos DB Table API and Azure Table storage share the same table data model and expose the same create, delete, update, and query operations through their SDKs.

If you currently use Azure Table Storage, you gain the following benefits by moving to the Azure Cosmos DB Table API:

	Azure Table storage	**Azure Cosmos DB Table API**
Latency	Fast, but no upper bounds on latency.	Single-digit millisecond latency for reads and writes, backed with <10-ms latency reads and <15-ms latency writes at the 99th percentile, at any scale, anywhere in the world.
Throughput	Variable throughput model. Tables have a scalability limit of 20,000 operations/s.	Highly scalable with dedicated reserved throughput per table that's backed by SLAs. Accounts have no upper limit on throughput and support >10 million operations/s per table.
Global distribution	Single region with one optional readable secondary read region for high availability. You can't initiate failover.	Turnkey global distribution from one to 30+ regions. Support for automatic and manual failovers at any time, anywhere in the world.
Indexing	Only primary index on PartitionKey and RowKey. No secondary indexes.	Automatic and complete indexing on all properties, no index management.
Query	Query execution uses index for primary key, and scans otherwise.	Queries can take advantage of automatic indexing on properties for fast query times.
Consistency	Strong within primary region. Eventual within secondary region.	Five well-defined consistency levels to trade off availability, latency, throughput, and consistency based on your application needs.
Pricing	Storage-optimized.	Throughput-optimized.
SLAs	99.99% availability.	99.99% availability SLA for all single region accounts and all multi-region accounts with relaxed consistency, and 99.999% read availability on all multi-region database accounts Industry-leading comprehensive SLAs on general availability.

Azure Queues Storage

Azure Queue storage is a service for storing large numbers of messages that can be accessed from anywhere in the world via authenticated calls using HTTP or HTTPS.

A single queue message can be up to 64 KB in size, and a queue can contain millions of messages, up to the total capacity limit of a storage account (i.e. 500TB)

Queues can have metadata associated with them. Metadata is in the form of <name, value> pairs.

Common uses of Queue storage include:

1. Creating a backlog of work to process asynchronously
2. Passing messages from an Azure App Service to an Azure Function.

- **Queue:** A queue contains a set of messages. All messages must be in a queue.
- **Message:** A message, **in any format**, of up to 64KB.

Difference between Storage Queues and Service Bus Queue

1. Azure storage queue does not provide publish/subscribe mechanism.
2. Azure storage queue can store data maximum for 7 days.
3. Azure storage queue does not provide a guaranteed FIFO delivery.
4. Azure storage queue does not provide transactional behavior.

Important Notes about Storage Queues:

- When a message is retrieved from the queue, the response includes the message and a pop receipt value, which is required to delete the message.
- The message is **not automatically deleted** from the queue, but after it has been retrieved, it is **not visible to other clients** for the time interval specified by the ***visibilitytimeout*** parameter. Hence every message is delivered **at-least once**.
- Every time it's received and not deleted, its **Dequeuecount is incremented**.

Azure File Storage

- Azure File storage is a service that offers file shares in the cloud using the standard Server Message Block (SMB) Protocol.

- With Azure File storage, you can migrate **legacy applications** that rely on file shares to Azure quickly and without costly rewrites.
- Microsoft Azure virtual machines can share file data across application components via mounted shares, and on-premises applications can access file data in a share via the File storage API.

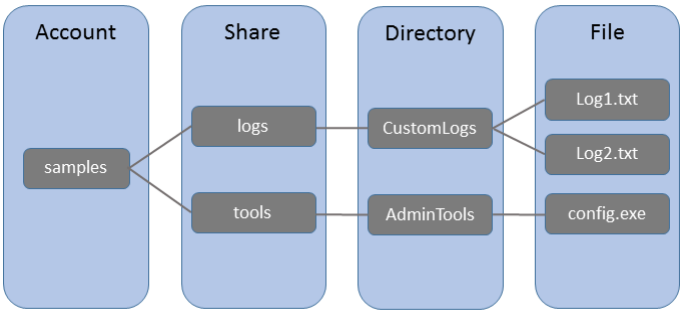
Why Azure File is useful

- Replace or supplement on-premises file servers.
- "Lift and shift" of Legacy applications.
- Simplify cloud development
    - Shared application settings
    - Diagnostic share
    - Dev/Test/Debug

Common uses of File storage include:

- Migrating on-premises applications that rely on file shares to run on Azure virtual machines or cloud services, without expensive rewrites.
- Storing shared application settings, for example in configuration files.
- Storing diagnostic data such as logs, metrics, and crash dumps in a shared location.
- Storing tools and utilities needed for developing or administering Azure virtual machines or cloud services.

File storage concepts



- **Storage Account:** All access to Azure Storage is done through a storage account.
- **Share:** A File storage share is an SMB file share in Azure. All directories and files must be created in a parent share. An account can contain an unlimited number of shares, and a share can store an unlimited number of files, up to the 5 TB total capacity of the file share.

- **Directory:** An optional hierarchy of directories.
- **File:** A file in the share. A file may be up to 1 TB in size.
- **Max size of a File Share = 5TB**

URL format: https**://<storage account>**.file.core.windows.net/**<share>/<directory/directory>/<file>**

The following example URL could be used to address one of the files in the diagram above:

http://samples.file.core.windows.net/logs/CustomLogs/Log1.txt

Managing Using Azure Portal:

1. Azure Portal → **Storage accounts** → Create and Choose the Storage Account
   Note: File storage is replicated only via LRS or GRS right now…
2. Choose "Files" service → Click "+ File share" → New file share = Images, Quota=100GB
3. Optionally add directory and in the directory and upload the file[s].

Mapping the file share in Windows

4. Go to File Share Blade and click on **Connect** → Copy the net command edit the values
5. Open Command Prompt in Administrator Mode → Execute the net command
6. You can manage the File Share using the local drive.

Note: Ensure port 445 is open: Azure Files uses SMB protocol. SMB communicates over TCP port 445

Creating File Share using Powershell

Retrieve storage account and storage account key

$storageContext = **New-AzureStorageContext** <storage-account-name> <storage-account-key>

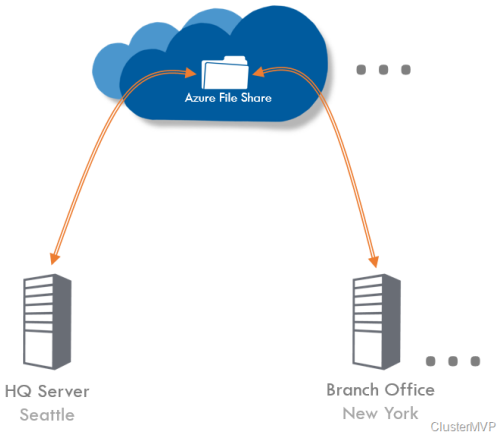
Create the file share, in this case "logs"

$share = **New-AzureStorageShare** logs -Context $storageContext

Azure File Sync

- Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server.
- Azure File Sync transforms Windows Server into a quick cache of your Azure file share.
- You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS.
- You can have as many caches as you need across the world.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

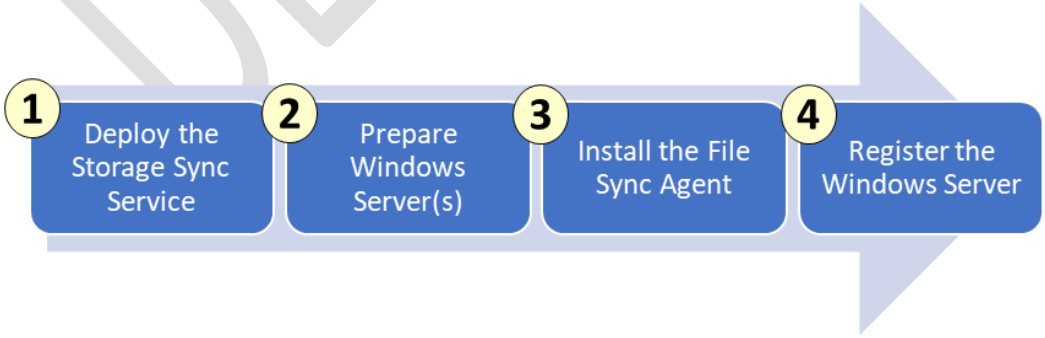


There are many uses and advantages to file sync.

- **Lift and shift.** The ability to move applications that require access between Azure and on-premises systems. Provide write access to the same data across Windows Servers and Azure Files. This lets companies with multiple offices have a need to share files with all offices.
- **Branch Offices**. Branch offices need to backup files, or you need to setup a new server that will connect to Azure storage.
- **Backup and Disaster Recovery**. Once File Sync is implemented, Azure Backup will back up your on-premises data. Also, you can restore file metadata immediately and recall data as needed for rapid disaster recovery.
- **File Archiving**. Only recently accessed data is located on local servers. Non-used data moves to Azure in what is called Cloud Tiering. Cloud Tiering files will have greyed icons with an offline 'O' file attribute to let the user know the file is only in Azure.

File Sync Service Deployment

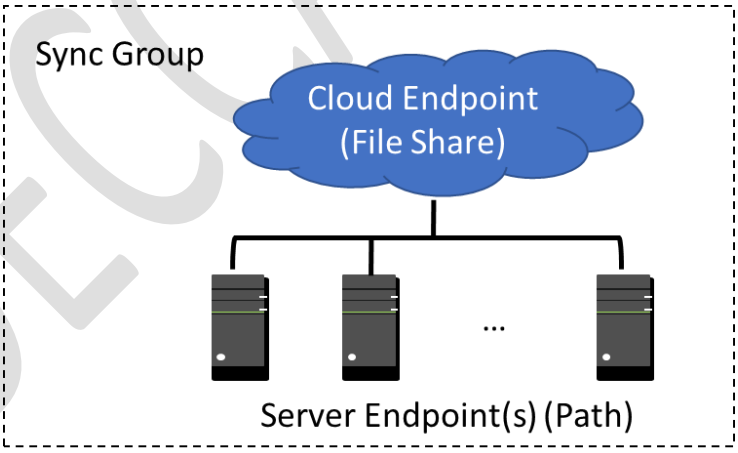
There are a few things that need to be configured before you synchronize your files.



Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

1. **Deploy the Storage Sync Service**. The Storage Sync Service is the top-level Azure resource for Azure File Sync. A distinct top-level resource from the storage account resource is required because the Storage Sync Service can create sync relationships with multiple storage accounts via multiple sync groups. A subscription can have multiple Storage Sync Service resources deployed.
2. **Prepare Windows Server to use with Azure File Sync**. For each server that you intend to use with Azure File Sync, including server nodes in a Failover Cluster, you will need to configure the server. Preparation steps include temporarily disabling Internet Explorer Enhanced Security and ensuring you have latest PowerShell version.
3. **Install the Azure File Sync Agent**. The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share. The Azure File Sync agent installation package should install relatively quickly. We recommend that you keep the default installation path and that you enable Microsoft Update to keep Azure File Sync up to date.
4. **Register Windows Server with Storage Sync Service**. When the Azure File Sync agent installation is finished, the Server Registration UI automatically opens. Registering Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service. Registration requires your Subscription ID, Resource Group, and Storage Sync Service (created in step one). A server (or cluster) can be registered with only one Storage Sync Service at a time.

File Sync Service Deployment (Synchronization)

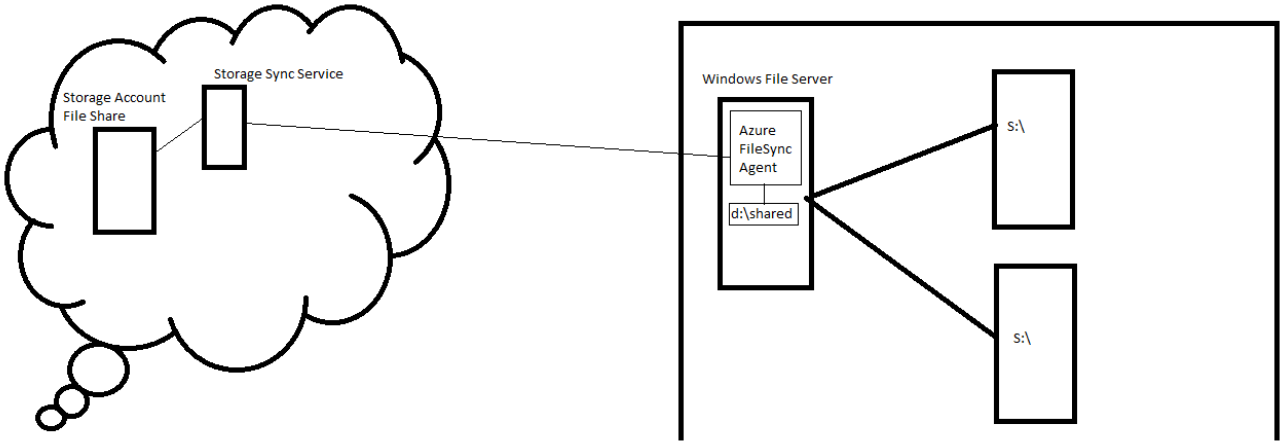


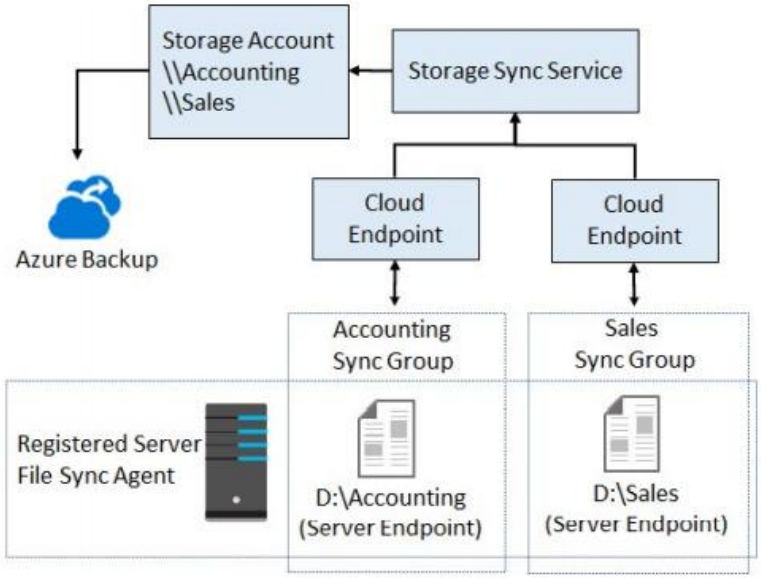
A **Sync Group** defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain at least one cloud endpoint, which represents an Azure file share created in your storage account, and at least one server endpoint, which represents a path on a Windows Server.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

✔ As Azure File Sync is available in only few Regions: Eg: West US, remember that your storage account must be located in one of the regions in which Azure File Sync is supported.





Walkthrough

1. Create Storage Account
    a. Create **File Share** in Storage Account.
2. Create **Azure File Sync** Service
    a. Azure Portal → Create a Resource → **Azure File Sync**

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

b. In File Sync Service → Create Sync Group

i. Select Storage Account and File Share created in Step1

3. Register our **On-Premise Server** or local server

a. Create a **Windows** VM 2019 Server

b. RDP to VM, Ensure that Azure PowerShell Cmdlets are installed.

```
Install-Module AzureRM
Import-Module AzureRM
```

c. Go to Server Manager → Local Server → **Turn Off IE Enanhanced Security**

d. Open Browser → Search **Azure File Sync Agent Download** → Download and Install File Sync Agent

e. Complete the **Registration** process: **SignIn to Azure Account** → Select the File Sync Service → Register

4. Azure Portal → File Sync Group → Sync Group → Add server endpoint → Path = **C:\AzureFiles.**

- **Registered server**. The name of the server or cluster where you want to create the server endpoint.
- **Path**. The Windows Server path to be synced as part of the sync group. The path should not be the root volume.
- **Cloud Tiering**. A switch to enable or disable cloud tiering.
- **Volume Free Space**. The amount of free space to reserve on the volume on which the server endpoint is located. For example, if volume free space is set to 50% on a volume that has a single server endpoint, roughly half the amount of data is tiered to Azure Files.

5. RDP to VM and Note that the folder is created in that VM.
6. Dump some files in that folder and note in Portal that files are now present in Azure file share.

Implement Azure storage account failover

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

https://docs.microsoft.com/en-us/azure/storage/common/last-sync-time-get