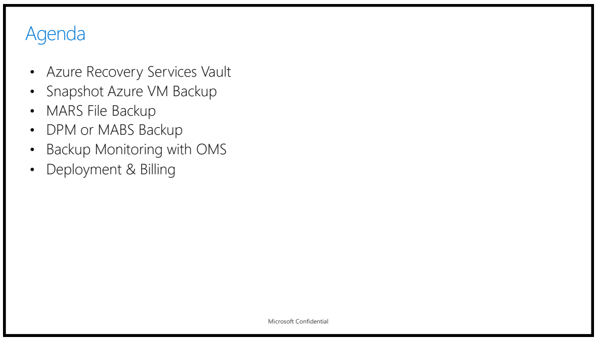
Microsoft

# Azure Backup

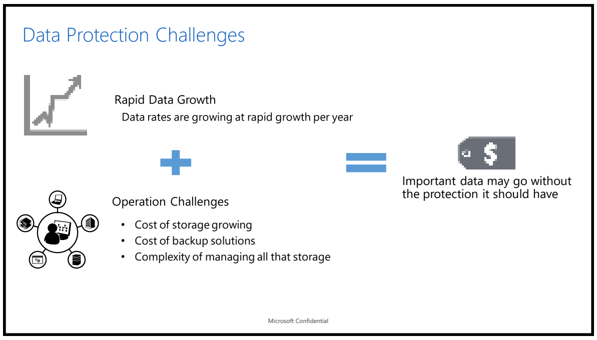
Microsoft Services



## Agenda

- Azure Recovery Services Vault
- Snapshot Azure VM Backup
- MARS File Backup
- DPM or MABS Backup
- Backup Monitoring with OMS
- Deployment & Billing

Microsoft Confidential



## Data Protection Challenges

Rapid Data Growth

Data rates are growing at rapid growth per year

+

Operation Challenges

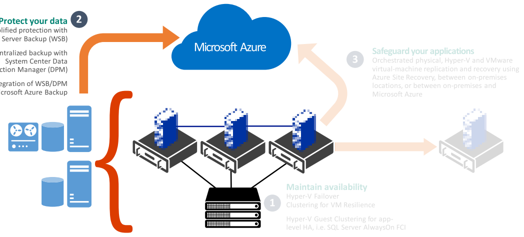
- Cost of storage growing
- Cost of backup solutions
- Complexity of managing all that storage

=

Important data may go without the protection it should have

Microsoft Confidential

## Breadth and depth solutions for business continuity and DR

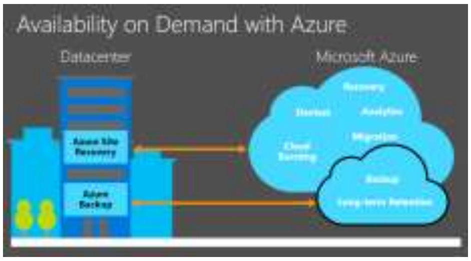


**Protect your data**
Simplified protection with Windows Server Backup (WSB)
Centralized backup with System Center Data Protection Manager (DPM)
Integration of WSB/DPM with Microsoft Azure Backup

**Safeguard your applications**
Orchestrated physical, Hyper-V and VMware virtual-machine replication and recovery using Azure Site Recovery, between on-premises locations, or between on-premises and Microsoft Azure

**Maintain availability**
Hyper-V Failover Clustering for VM Resilience
Hyper-V Guest Clustering for app-level HA, i.e. SQL Server AlwaysOn FCI

## Business continuity and Disaster recovery with Azure



Microsoft Confidential

## Microsoft Azure Backup Overview

- Simple and reliable server backup to the cloud

**Reliable offsite data protection**

- Convenient offsite protection
- Safe data
- Encrypted backups

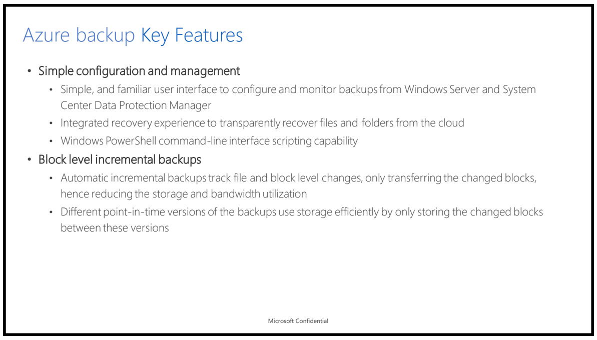
**A simple and integrated solution**

- Familiar interface
- Azure integration

**Efficient backup and recovery**

- Efficient use of bandwidth and storage
- Flexible configuration
- Flexibility in recovery
- Cost-effective and metered by usage

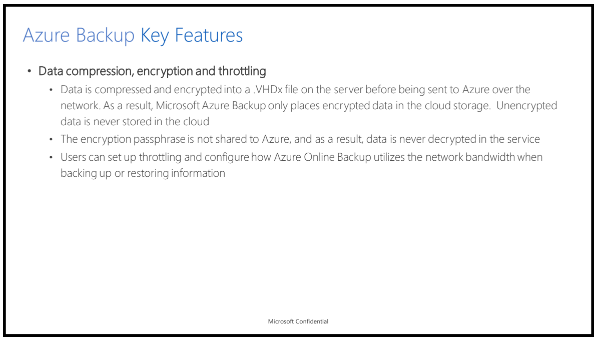
Microsoft Confidential



## Azure backup Key Features

- Simple configuration and management
  - Simple, and familiar user interface to configure and monitor backups from Windows Server and System Center Data Protection Manager
  - Integrated recovery experience to transparently recover files and folders from the cloud
  - Windows PowerShell command-line interface scripting capability
- Block level incremental backups
  - Automatic incremental backups track file and block level changes, only transferring the changed blocks, hence reducing the storage and bandwidth utilization
  - Different point-in-time versions of the backups use storage efficiently by only storing the changed blocks between these versions

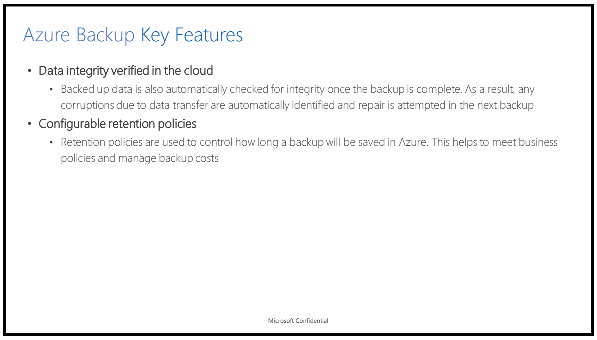
Microsoft Confidential



## Azure Backup Key Features

- Data compression, encryption and throttling
  - Data is compressed and encrypted into a .VHDx file on the server before being sent to Azure over the network. As a result, Microsoft Azure Backup only places encrypted data in the cloud storage. Unencrypted data is never stored in the cloud
  - The encryption passphrase is not shared to Azure, and as a result, data is never decrypted in the service
  - Users can set up throttling and configure how Azure Online Backup utilizes the network bandwidth when backing up or restoring information

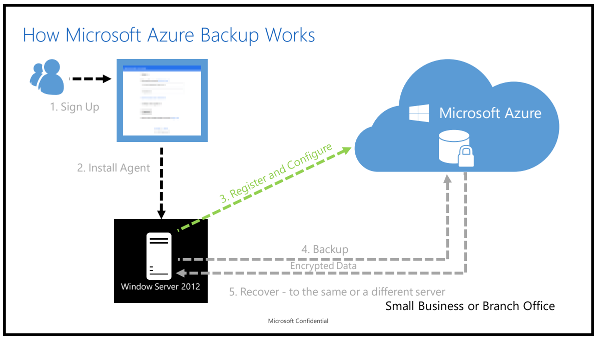
Microsoft Confidential



## Azure Backup Key Features

- Data integrity verified in the cloud
  - Backed up data is also automatically checked for integrity once the backup is complete. As a result, any corruptions due to data transfer are automatically identified and repair is attempted in the next backup
- Configurable retention policies
  - Retention policies are used to control how long a backup will be saved in Azure. This helps to meet business policies and manage backup costs

Microsoft Confidential



## How Microsoft Azure Backup Works

1. Sign Up

2. Install Agent

3. Register and Configure

Microsoft Azure

Window Server 2012

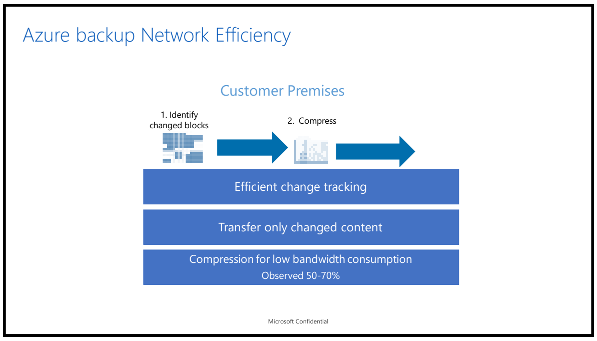
4. Backup

Encrypted Data

5. Recover - to the same or a different server

Small Business or Branch Office

Microsoft Confidential



## Azure backup Network Efficiency

Customer Premises

1. Identify changed blocks

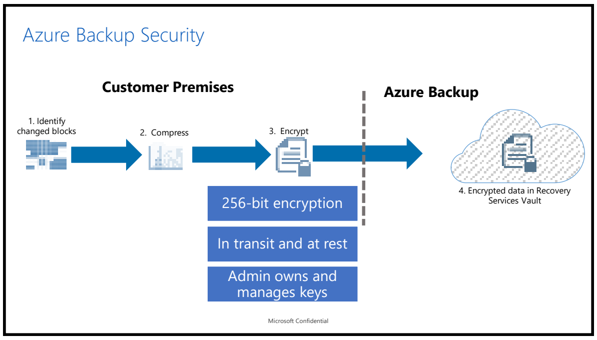
2. Compress

Efficient change tracking

Transfer only changed content

Compression for low bandwidth consumption
Observed 50-70%

Microsoft Confidential



## Azure Backup Security

**Customer Premises**

**Azure Backup**

1. Identify changed blocks

2. Compress

3. Encrypt

4. Encrypted data in Recovery Services Vault

256-bit encryption

In transit and at rest

Admin owns and manages keys

Microsoft Confidential

## Azure Backup Agent - Supported Platforms

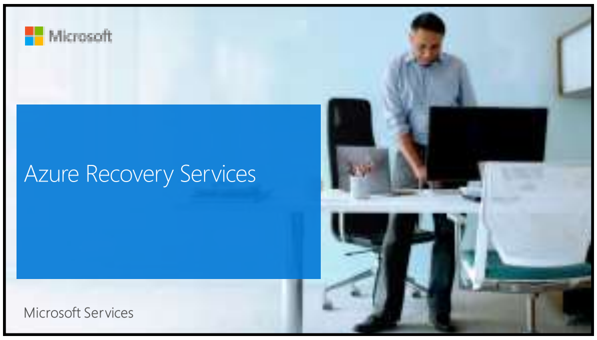
https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq/#installation-amp-configuration

## Azure Backup Unsupported Scenarios

- Vault to Vault migration not supported
  - Subscription to Subscription data migration not supported
  - Locally Redundant Storage (LRS) to Geo-redundant Storage (GRS) or vice versa migration not supported – configure vault before protection
  - Data cannot be recovered if encryption key is lost
- The following set of drives/volumes cannot be backed up:
  - Removable Media: The drive must report as a fixed to be used as a backup item source
  - Read-only Volumes: The volume must be writable for the volume shadow copy service (VSS) to function
  - Offline Volumes: The volume must be online for VSS to function
  - Network share: The volume must be local to the server to be backed up using online backup
  - BitLocker protected volumes: The volume must be unlocked before the backup can occur
  - File System Identification: NTFS is the only file system supported for this version of the online backup service

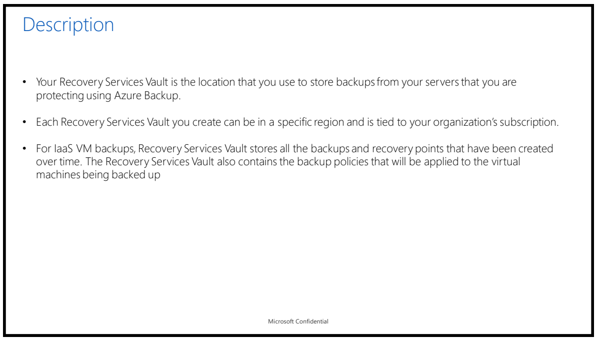
## Azure Backup Unsupported Scenarios

- The following types are not supported:
  - Hard Links: Not supported, skipped
  - Reparse Point: Not supported, skipped
  - Encrypted and Compressed: Not supported, skipped
  - Encrypted and Sparse: Not supported, skipped
  - Compressed Stream: Not supported, skipped
  - Sparse Stream: Not supported, skipped



# Azure Recovery Services

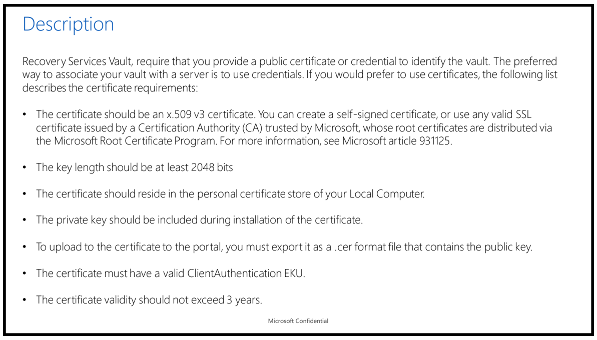
Microsoft Services



## Description

- Your Recovery Services Vault is the location that you use to store backups from your servers that you are protecting using Azure Backup.
- Each Recovery Services Vault you create can be in a specific region and is tied to your organization's subscription.
- For IaaS VM backups, Recovery Services Vault stores all the backups and recovery points that have been created over time. The Recovery Services Vault also contains the backup policies that will be applied to the virtual machines being backed up

Microsoft Confidential



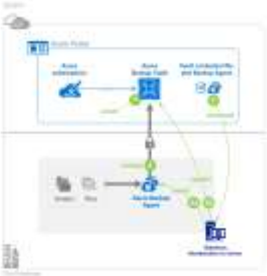
## Description

Recovery Services Vault, require that you provide a public certificate or credential to identify the vault. The preferred way to associate your vault with a server is to use credentials. If you would prefer to use certificates, the following list describes the certificate requirements:

- The certificate should be an x.509 v3 certificate. You can create a self-signed certificate, or use any valid SSL certificate issued by a Certification Authority (CA) trusted by Microsoft, whose root certificates are distributed via the Microsoft Root Certificate Program. For more information, see Microsoft article 931125.
- The key length should be at least 2048 bits
- The certificate should reside in the personal certificate store of your Local Computer.
- The private key should be included during installation of the certificate.
- To upload to the certificate to the portal, you must export it as a .cer format file that contains the public key.
- The certificate must have a valid ClientAuthentication EKU.
- The certificate validity should not exceed 3 years.

Microsoft Confidential

## Description



## Create a Recovery Services Vault

## Vault Credentials

## Vault Credentials

- The on-premises machine (Windows Server or Windows client) needs to be authenticated with a Recovery Services Vault before it can back up data to Azure.
- The authentication is achieved using vault credentials. The vault credential file is downloaded through a secure channel from the Azure portal.
- The Azure Backup service is unaware of the certificate private key, which does not persist in the portal or the service.
- The vault credentials file is only valid for 48 hours (after it's downloaded from the portal).
- The vault credentials file is used only during the registration workflow
- Ensure that the vault credentials is saved in a location which can be accessed from your machine. If it is stored in a file share/SMB, check for the access permissions.

Microsoft Confidential

## Storage redundancy

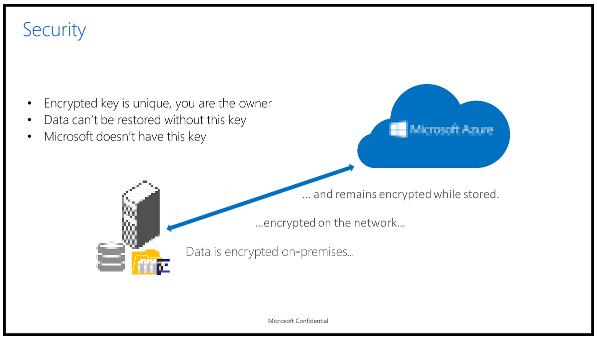
- Storage data in a Recovery Services Vault are always redundant
- The best time to identify your storage redundancy option is right after vault creation and before any machines are registered to the vault. Once an item has been registered to the vault, the storage redundancy option is locked and cannot be modified.
- When you create a storage account, you should select one of these options :
  - Locally redundant storage (LRS) (3 copies in the Datacenter)
  - Geo-redundant storage (GRS) – default (3 local copies + 3 copies on a second datacenter)
- You can't modify this option after configuring it and registering machines into the Recovery Services Vault

Microsoft Confidential

## Storage redundancy

- If you are using Azure as a primary backup storage endpoint (for example, you are backing up to Azure from a Windows Server), you should consider picking (the default) geo-redundant storage option.
- If you are using Azure as a tertiary backup storage endpoint (for example, you are using SCDPM to have a local backup copy on-premises & using Azure for your long term retention needs), you should consider choosing locally redundant storage. This brings down the cost of storing data in Azure, while providing a lower level of durability for your data that might be acceptable for tertiary copies.

Microsoft Confidential



## Security

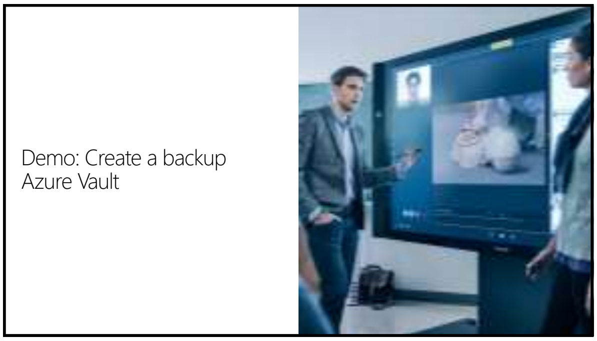
- Encrypted key is unique, you are the owner
- Data can't be restored without this key
- Microsoft doesn't have this key

... and remains encrypted while stored.

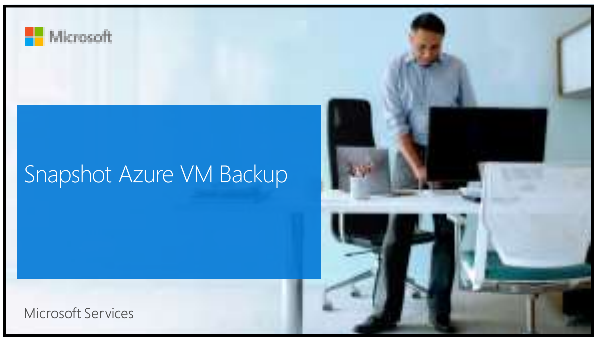
...encrypted on the network...

Data is encrypted on-premises...

Microsoft Confidential

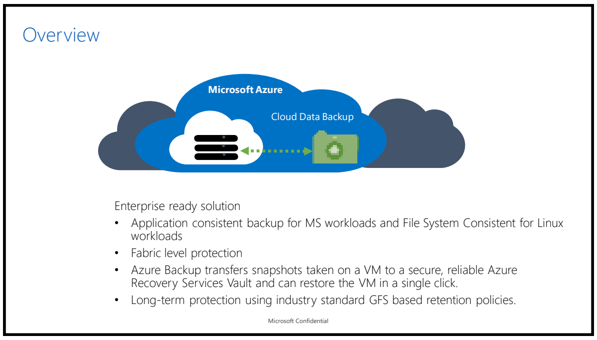


## Demo: Create a backup Azure Vault



## Snapshot Azure VM Backup

Microsoft Services

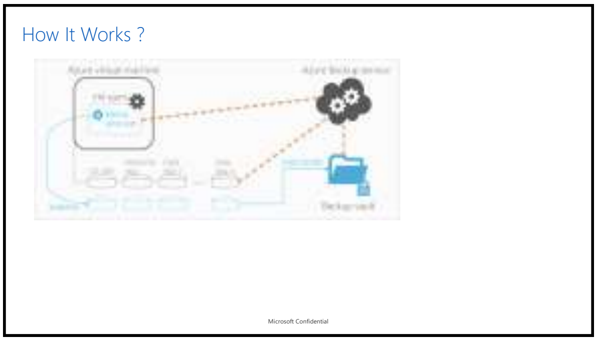


## Overview

Enterprise ready solution

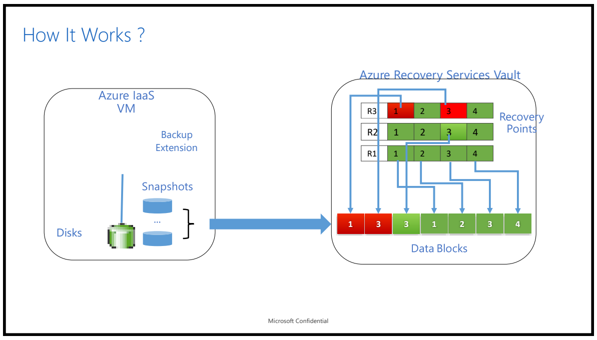
- Application consistent backup for MS workloads and File System Consistent for Linux workloads
- Fabric level protection
- Azure Backup transfers snapshots taken on a VM to a secure, reliable Azure Recovery Services Vault and can restore the VM in a single click.
- Long-term protection using industry standard GFS based retention policies.

Microsoft Confidential



## How It Works ?

Microsoft Confidential



## How It Works ?

Microsoft Confidential

## Discover your IaaS VMs

Tip :

- Only VMs in the same region and within the same souscription than the Recovery Services Vault are discoverable

Microsoft Confidential

## Define a backup policy

Tip:

- A backup policy includes a retention scheme for the scheduled backups. If you select an existing backup policy, you cannot modify the retention options in the next step.
- Virtual machine backups can be retained for up to 99 years.

Microsoft Confidential

## Define items to backup

Tip:

- Multiple virtual machines can be registered at one time.
- During the backup operation, the Azure Backup service issues a command to the backup extension in each virtual machine to flush all write jobs and take a consistent snapshot.

Microsoft Confidential

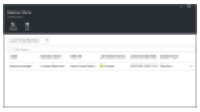
## Protect your IaaS VMs

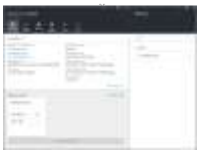
Note :

- During the backup operation, the Azure Backup service issues a command to the backup extension in each virtual machine to flush all write jobs and take a consistent snapshot.

Microsoft Confidential

## Monitor





Note :

- Dashboard page shows the number of successful, failed or in progress jobs from the last 24 hours
- On the Jobs page, use the Status, Operation, or From and To menus to filter the jobs.
- Monitoring of IaaS VM Backup is coming to Logs Analytics.

Microsoft Confidential

## Monitor

Microsoft Confidential

## Audit

Operations logs enable great post-mortem and audit support for the backup operations.

The following operations are logged in Azure Logs:

- Register
- Unregister
- Configure protection
- Backup ( Both scheduled as well as on-demand backup through BackupNow)
- Restore
- Stop protection
- Delete backup data
- Add policy
- Delete policy
- Update policy
- Cancel job

## Audit

## Alerts

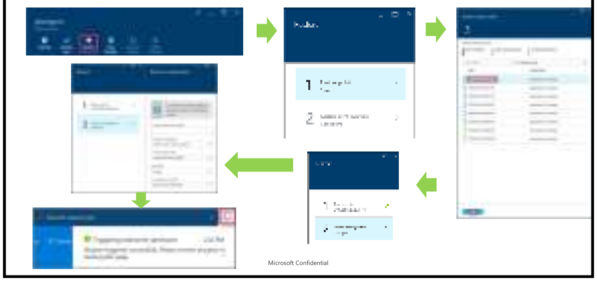
### Via PowerShell

```
$actionEmail = New-AzureRmAlertRuleEmail -CustomEmail
contoso@microsoft.com

Add-AzureRmLogAlertRule -Name backupFailedAlert -
Location "East US" -ResourceGroup R<RGName>
-OperationName
Microsoft.Backup/RecoveryServicesVault/Backup -Status
Failed -TargetResourceId /subscriptions/86eeac34-eth9a-
4de3-84db-
7a27d121967e/resourceGroups/RRGName/providers/micro
soft.backupbvtd2/RecoveryServicesVault/trinadhVault
-Actions $actionEmail
```

### Via the portal

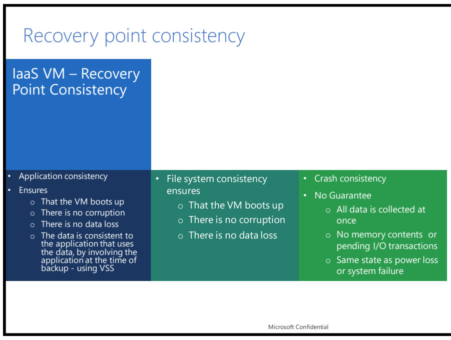
## Restore your data



## Restore considerations

- For Domain Controller VMs in a multi-DC environment, do not use the Azure portal for restore! Only PowerShell based restore is supported
- Azure Backup supports backup for following special network configurations of virtual machines.
  - VMs under load balancer ( internal and external)
  - VMs with multiple reserved IPs
  - VMs with multiple NICs
- PowerShell has the ability to just restore the VM disks from backup and not create the virtual machine. This is helpful when restoring virtual machines which require special network configurations mentioned above.
- Select a cloud service for the VM: This is mandatory for creating a VM. You can choose to either use an existing cloud service or create a new cloud service.
- You can select from existing storage accounts in the same region as the Azure Recovery Services Vault. We don't support storage accounts that are Zone redundant or of Premium storage type.

## Recovery point consistency

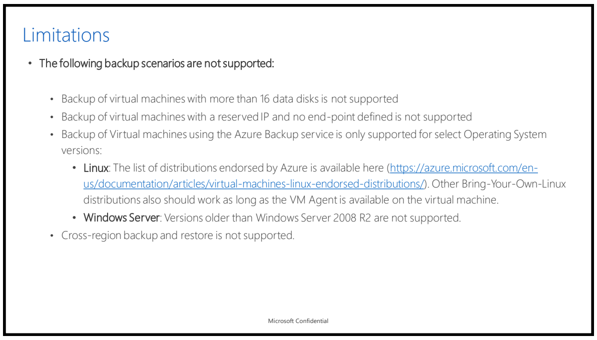


IaaS VM – Recovery Point Consistency

- Application consistency
- Ensures
  - That the VM boots up
  - There is no corruption
  - There is no data loss
  - The data is consistent to the application that uses the data, by involving the application at the time of backup - using VSS

- File system consistency ensures
  - That the VM boots up
  - There is no corruption
  - There is no data loss

- Crash consistency
- No Guarantee
  - All data is collected at once
  - No memory contents or pending I/O transactions
  - Same state as power loss or system failure



## Limitations

- The following backup scenarios are not supported:
  - Backup of virtual machines with more than 16 data disks is not supported
  - Backup of virtual machines with a reserved IP and no end-point defined is not supported
  - Backup of Virtual machines using the Azure Backup service is only supported for select Operating System versions:
    - **Linux**: The list of distributions endorsed by Azure is available here (https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-linux-endorsed-distributions/). Other Bring-Your-Own-Linux distributions also should work as long as the VM Agent is available on the virtual machine.
    - **Windows Server**: Versions older than Windows Server 2008 R2 are not supported.
  - Cross-region backup and restore is not supported.

Microsoft Confidential

Demo: Backup Azure VMs with snapshots

Microsoft

MARS File Backup

Microsoft Services

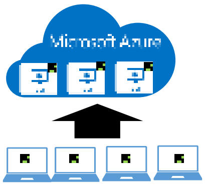
## Description

Ideal for Laptops and remote sites backup

Protect offline Files &Folders on client & servers

Long term retention :

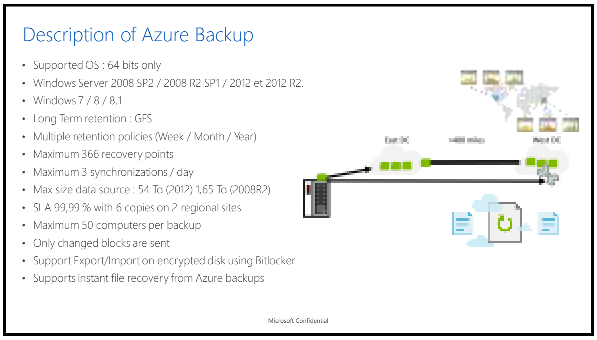
99+ days



## Azure backup Scenarios

## How does it works ?

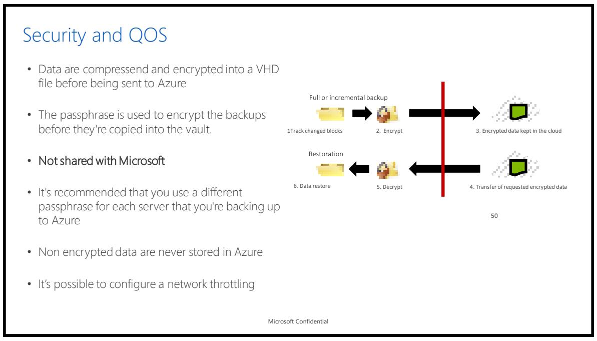
- With Windows Azure Backup, VSS doesn't use any writers.
- Without a writer, data sets that need to be prepped for the freeze can't be prepped. The downside to all of this is that any data that requires a special VSS writer can't be backed up using Windows Azure Backup.



## Description of Azure Backup

- Supported OS : 64 bits only
- Windows Server 2008 SP2 / 2008 R2 SP1 / 2012 et 2012 R2.
- Windows 7 / 8 / 8.1
- Long Term retention : GFS
- Multiple retention policies (Week / Month / Year)
- Maximum 366 recovery points
- Maximum 3 synchronizations / day
- Max size data source : 54 To (2012) 1,65 To (2008R2)
- SLA 99,99 % with 6 copies on 2 regional sites
- Maximum 50 computers per backup
- Only changed blocks are sent
- Support Export/Import on encrypted disk using Bitlocker
- Supports instant file recovery from Azure backups

Microsoft Confidential

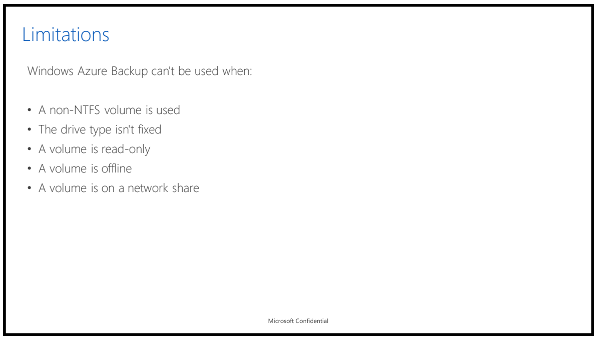


## Security and QOS

- Data are compressend and encrypted into a VHD file before being sent to Azure
- The passphrase is used to encrypt the backups before they're copied into the vault.
- Not shared with Microsoft
- It's recommended that you use a different passphrase for each server that you're backing up to Azure
- Non encrypted data are never stored in Azure
- It's possible to configure a network throttling

Full or incremental backup
1Track changed blocks
2. Encrypt
3. Encrypted data kept in the cloud
Restoration
6. Data restore
5. Decrypt
4. Transfer of requested encrypted data
50

Microsoft Confidential



## Limitations

Windows Azure Backup can't be used when:

- A non-NTFS volume is used
- The drive type isn't fixed
- A volume is read-only
- A volume is offline
- A volume is on a network share

Microsoft Confidential

## Requirements

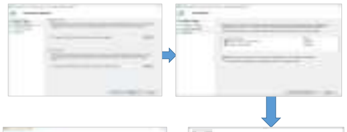
- To back up files and data from your Windows Server to Azure, you must first:
  - Create a Recovery Services Vault — Create a vault in the Azure Backup console
    - To back up files and data from your Windows Server or System Center Data Protection Manager to Azure or when backing up Infrastructure as a Service (IaaS) VMs to Azure, you must create a Recovery Services Vault in the geographic region where you want to store the data
  - Download vault credentials — In Azure Backup, upload the management certificate that you created to the vault
  - Install the Azure Backup Agent and register the server — From Azure Backup, install the agent and register the server in the Recovery Services Vault

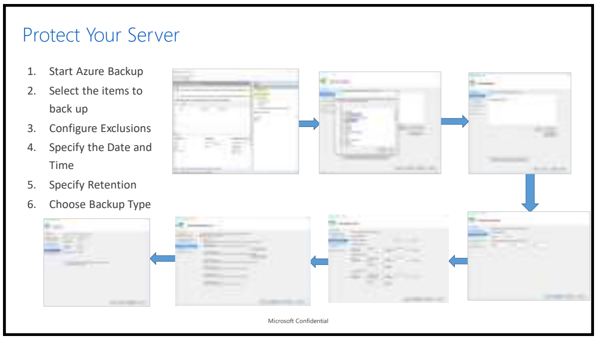
## Network Connectivity

- Backup Extension connectivity to Azure Public IPs
- Network Security Groups
- HTTP Proxy

## Register Your Server to Azure Backup Service

1. Install MARSAgent - MARSAgentInstaller.exe
2. Register the server
3. Create the PassPhrase Key
4. Complete the registration

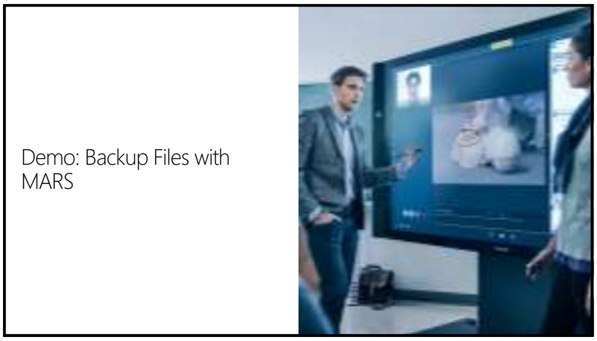




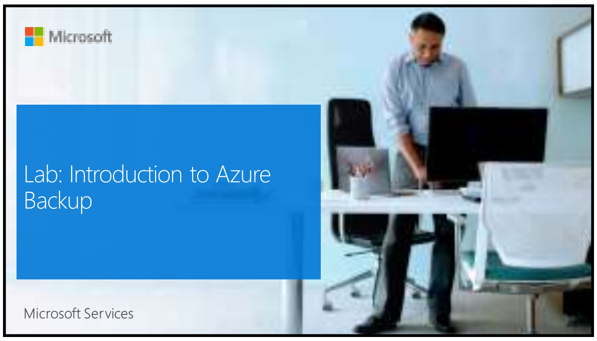
## Protect Your Server

1. Start Azure Backup
2. Select the items to back up
3. Configure Exclusions
4. Specify the Date and Time
5. Specify Retention
6. Choose Backup Type

Microsoft Confidential



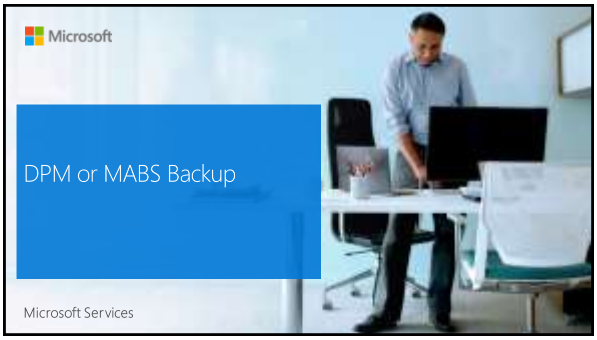
## Demo: Backup Files with MARS



Microsoft

## Lab: Introduction to Azure Backup

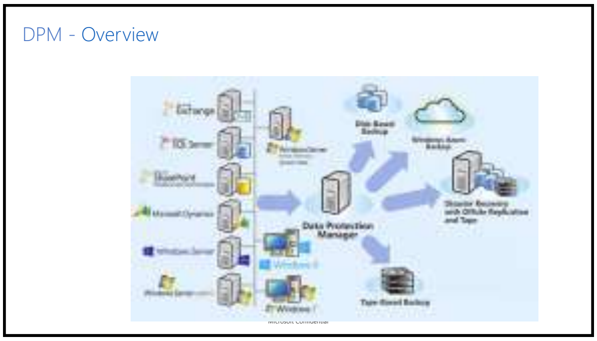
Microsoft Services



Microsoft

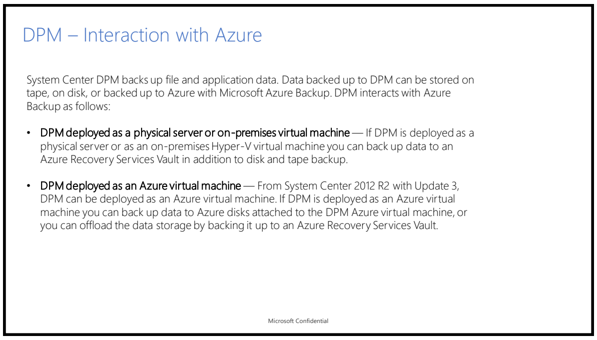
# DPM or MABS Backup

Microsoft Services



## DPM - Overview

Microsoft Confidential



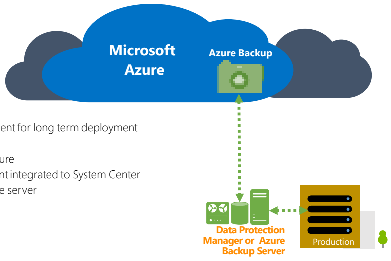
## DPM – Interaction with Azure

System Center DPM backs up file and application data. Data backed up to DPM can be stored on tape, on disk, or backed up to Azure with Microsoft Azure Backup. DPM interacts with Azure Backup as follows:

- DPM deployed as a physical server or on-premises virtual machine — If DPM is deployed as a physical server or as an on-premises Hyper-V virtual machine you can back up data to an Azure Recovery Services Vault in addition to disk and tape backup.
- DPM deployed as an Azure virtual machine — From System Center 2012 R2 with Update 3, DPM can be deployed as an Azure virtual machine. If DPM is deployed as an Azure virtual machine you can back up data to Azure disks attached to the DPM Azure virtual machine, or you can offload the data storage by backing it up to an Azure Recovery Services Vault.

Microsoft Confidential

## DPM – Solutions for enterprise and branch office backup



Solutions :

- Cloud as tape replacement for long term deployment
- Minimize local storage
- Workload backup to Azure
- Centralized management integrated to System Center
- Restore data to alternate server

Microsoft Confidential

## DPM - Features

**Workload integration**

DPM provides agents to protect enterprise workloads :

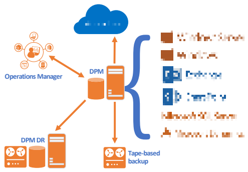
- Windows Server & Windows Client
- Exchange
- SQL Server
- SharePoint
- Dynamics
- Hyper-V VMs
- Linux (file consistent only)

**Several storage options**

Data storage on disks, tapes and cloud with Microsoft Azure Backup

**DRP Low Cost**

Possibility to chain DPM servers for a secondary protection



Microsoft Confidential

## DPM – Integration with System Center Operation Manager

- Centralized console of several DPM servers to monitor protected data, backup state, resource usage and analyze performances

Microsoft Confidential

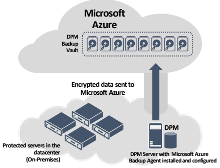
## DPM – DPM in the cloud

**Protected data offsite – Reliability and security**
Backup are encrypted in Microsoft Azure.
Backup are offsite, protected in a redundant Azure storage

**Solution simple and integrated**
Direct integration within the Data Protection Manager console

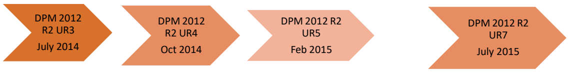
**Backup and restore efficient and flexible :**

- Supported workoads in the cloud : File servers / VM Hyper-V / SQL Server / Clients / Exchange / SharePoint (*DPM 2012 R2 UR 5*) / Linux
- Retention duration GFS
- Support Export/Import (Offline Sending)
- Easy Restore assistant to retrieve data from Azure


Microsoft Azure
DPM Backup Vault
Encrypted data sent to Microsoft Azure
DPM
Protected servers in the datacenter (On-Premises)
DPM Server with Microsoft Azure Backup Agent installed and configured

Microsoft Confidential

## DPM – Evolution



- Hyper-V protection at scale
- Backup & CC Window
- Tapes using Synthetic Fiber Channel

- Deduplication support
- Protect SQL 2014
- Simplified steps for Online backup registration
- Long Term retention for 9 years

- Protect SharePoint, Exchange and Client workloads to Azure
- Protect SharePoint with SQL Always On
- Long term retention (with GFS) on Azure
- Offline Initial Seeding for DPM to Azure
- Protect Microsoft workloads on VMWare
- Enterprise Reporting
- Inquiry Performance Improvements

- 9999 recovery points / 99 years
- All backup data on Azure can be restored from any DPM server in the enterprise

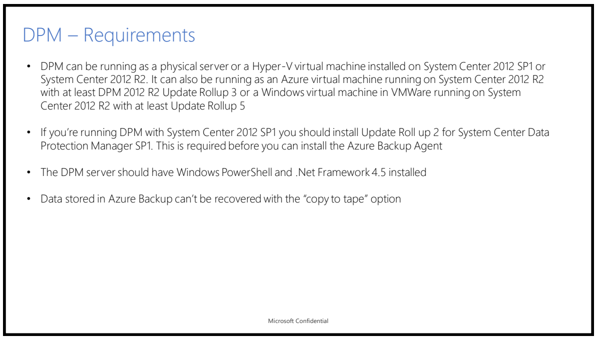
Impact: 50% jump in DPM server install numbers; 32% lesser call volume due to Console reliability

## DPM – Requirements

Prepare Azure Backup to back up DPM data as follows:

- **Create a Recovery Services Vault** — Create a vault in the Azure Backup console
- **Download vault credentials** — In Azure Backup, upload the management certificate you created to the vault
- **Install the Azure Backup Agent and register the server** — From Azure Backup, install the agent on each DPM server and register the DPM server in the Recovery Services Vault.

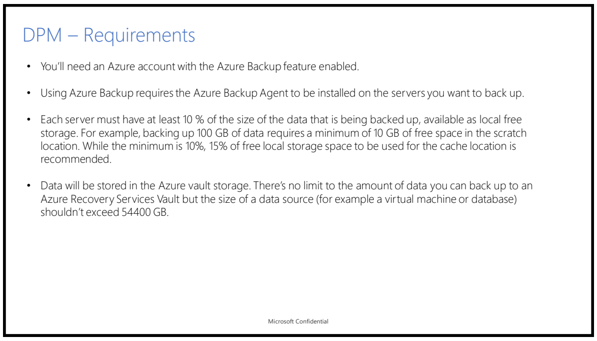
Microsoft Confidential



## DPM – Requirements

- DPM can be running as a physical server or a Hyper-V virtual machine installed on System Center 2012 SP1 or System Center 2012 R2. It can also be running as an Azure virtual machine running on System Center 2012 R2 with at least DPM 2012 R2 Update Rollup 3 or a Windows virtual machine in VMWare running on System Center 2012 R2 with at least Update Rollup 5
- If you're running DPM with System Center 2012 SP1 you should install Update Roll up 2 for System Center Data Protection Manager SP1. This is required before you can install the Azure Backup Agent
- The DPM server should have Windows PowerShell and .Net Framework 4.5 installed
- Data stored in Azure Backup can't be recovered with the "copy to tape" option

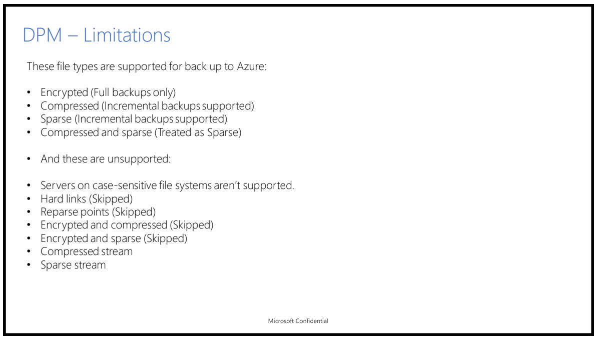
Microsoft Confidential



## DPM – Requirements

- You'll need an Azure account with the Azure Backup feature enabled.
- Using Azure Backup requires the Azure Backup Agent to be installed on the servers you want to back up.
- Each server must have at least 10 % of the size of the data that is being backed up, available as local free storage. For example, backing up 100 GB of data requires a minimum of 10 GB of free space in the scratch location. While the minimum is 10%, 15% of free local storage space to be used for the cache location is recommended.
- Data will be stored in the Azure vault storage. There's no limit to the amount of data you can back up to an Azure Recovery Services Vault but the size of a data source (for example a virtual machine or database) shouldn't exceed 54400 GB.

Microsoft Confidential



## DPM – Limitations

These file types are supported for back up to Azure:

- Encrypted (Full backups only)
- Compressed (Incremental backups supported)
- Sparse (Incremental backups supported)
- Compressed and sparse (Treated as Sparse)

- And these are unsupported:

- Servers on case-sensitive file systems aren't supported.
- Hard links (Skipped)
- Reparse points (Skipped)
- Encrypted and compressed (Skipped)
- Encrypted and sparse (Skipped)
- Compressed stream
- Sparse stream

Microsoft Confidential

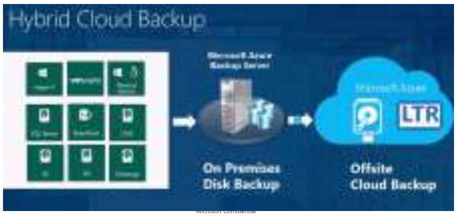
## MABS – What is missing from Azure backup ?

What has been missing from Azure Backup up to now?

- **Support for SME**: The focus of Azure Backup hybrid backup services for on-premises solutions was on customers with System Center Data Protection Manager (DPM). Unfortunately, DPM is licensed via the System Center Server Management License (SML), which is unaffordable for SMEs, as the sales of System Center to SMEs flat-lined in early 2012.
- **Service Support**: Azure Backup without DPM can only backup files and folders; the MARS agent is very limited at this time.
- **There is no cloud portal**: Hybrid backup is managed on each machine that the agent is installed in if you do not have DPM.

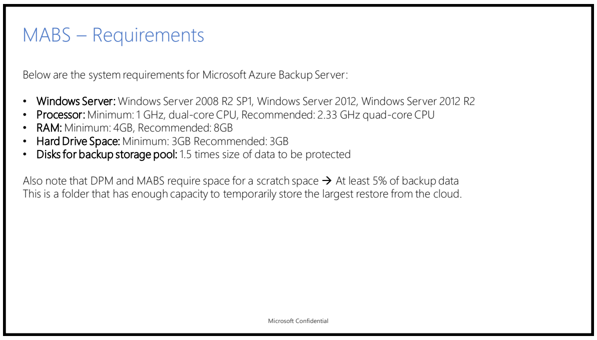
## MABS – Overview

- Microsoft Azure Backup Server is included as a **free download** with [Azure Backup]() that enables cloud backups and disk backups for key Microsoft workloads like SQL, SharePoint, Exchange regardless if these workloads are running on Hyper-V, VMware or Physical servers.



## MABS – Overview

- When you install, you'll get:
- **SQL Server 2014**: A free license of MABS that you can only use for MABS.
- **The MABS**: A customized version of System Center Data Protection Manager 2012 R2.
- Microsoft Azure Backup Server can only be used by Azure customers, and the setup requires you to provide Recovery Services Vault credentials.
- Although the Microsoft Azure Backup Server licensing is free, you'll need a Windows Server license to run it on.
- Disk→ Disk →Cloud backup with centralized local management and economic cloud-based off-site storage with long term retention (until 2 times per day)



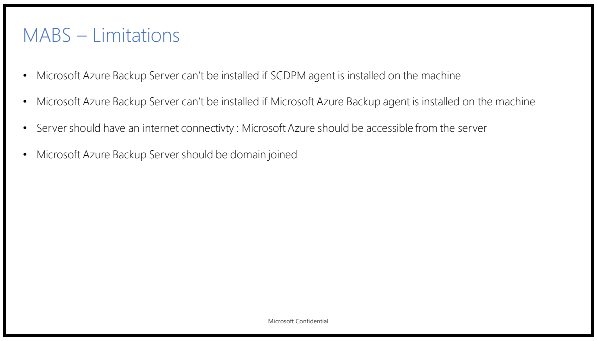
## MABS – Requirements

Below are the system requirements for Microsoft Azure Backup Server:

- **Windows Server:** Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2
- **Processor:** Minimum: 1 GHz, dual-core CPU, Recommended: 2.33 GHz quad-core CPU
- **RAM:** Minimum: 4GB, Recommended: 8GB
- **Hard Drive Space:** Minimum: 3GB Recommended: 3GB
- **Disks for backup storage pool:** 1.5 times size of data to be protected

Also note that DPM and MABS require space for a scratch space → At least 5% of backup data
This is a folder that has enough capacity to temporarily store the largest restore from the cloud.

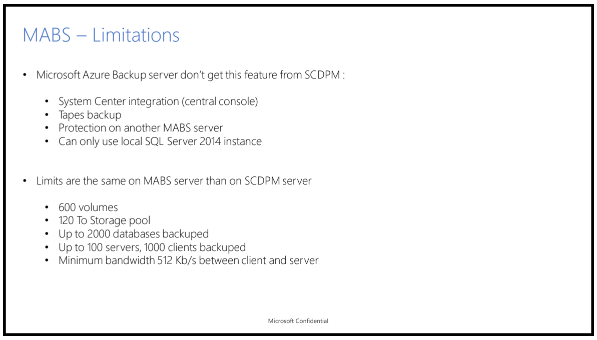
Microsoft Confidential



## MABS – Limitations

- Microsoft Azure Backup Server can't be installed if SCDPM agent is installed on the machine
- Microsoft Azure Backup Server can't be installed if Microsoft Azure Backup agent is installed on the machine
- Server should have an internet connectivty : Microsoft Azure should be accessible from the server
- Microsoft Azure Backup Server should be domain joined

Microsoft Confidential



## MABS – Limitations

- Microsoft Azure Backup server don't get this feature from SCDPM :
  - System Center integration (central console)
  - Tapes backup
  - Protection on another MABS server
  - Can only use local SQL Server 2014 instance
- Limits are the same on MABS server than on SCDPM server
  - 600 volumes
  - 120 To Storage pool
  - Up to 2000 databases backuped
  - Up to 100 servers, 1000 clients backuped
  - Minimum bandwidth 512 Kb/s between client and server

Microsoft Confidential

## MABS – Deployment

Microsoft Azure Backup Server can be installed as :

- Standalone physical server
- Virtual Machine Hyper-V
- Virtual Machine VMware
- Virtual Machine Azure : To protect Azure VMs

- Download directly or from the Recovery Services Vault

[http://www.microsoft.com/en-us/download/details.aspx?id=49170](http://www.microsoft.com/en-us/download/details.aspx?id=49170)

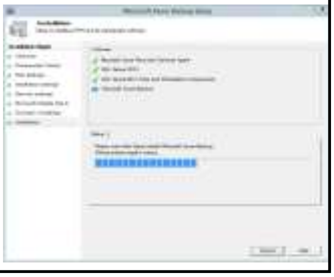
Microsoft Confidential

## MABS – Deployment

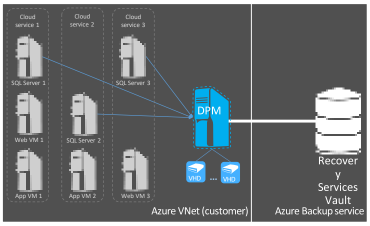
- Creation of a Recovery Services Vault
- Download vault credentials file
- Download product from Recovery Services Vault

## MABS – Deployment

- Install MARS agent
- Register Server from vault credentials
- Check of the internet connectivity
- Installation MABS & SQL Server



## MABS/DPM – Azure IaaS VM Backup



**Deploy an Azure IaaS VM with System Center DPM or MABS**

Microsoft Confidential

## MABS/DPM – Azure IaaS VM Backup

- MABS/DPM are supported in an Azure VM A2 or more
- A MABS/DPM server in Azure protect Azure VMs into the same Virtual Network and winthin the same souscription.
- Storage pool is limited to 16 disks with 1 To maximum (VM A4)
- VM is recommended is standard mode with a dedicated storage account
- There is a tool to calculate the necessary disk space for your VM MABS/DPM

Virtual machine size calculator for DPM IaaS VM in Azure
https://gallery.technet.microsoft.com/Virtual-machine-size-98673200

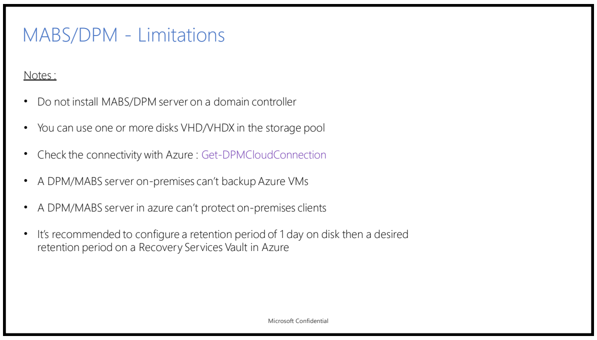
- Scale as needed

| DPM VM size | Backup scale |
|---|---|
| Standard tier - A2 | Up to 20 workloads (or) 2TB |
| Standard tier - A3 | Up to 40 workloads (or) 6TB |
| Standard tier - A4 | Up to 60 workloads (or) 12TB |

Microsoft Confidential

## MABS/DPM – Supported workloads in a VM Azure

Microsoft Confidential

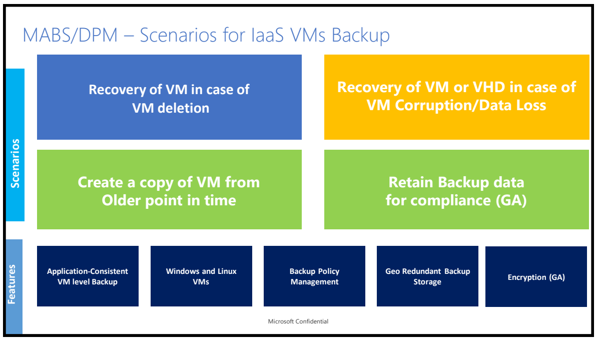


## MABS/DPM - Limitations

Notes :

- Do not install MABS/DPM server on a domain controller
- You can use one or more disks VHD/VHDX in the storage pool
- Check the connectivity with Azure : Get-DPMCloudConnection
- A DPM/MABS server on-premises can't backup Azure VMs
- A DPM/MABS server in azure can't protect on-premises clients
- It's recommended to configure a retention period of 1 day on disk then a desired retention period on a Recovery Services Vault in Azure

Microsoft Confidential



## MABS/DPM – Scenarios for IaaS VMs Backup

Scenarios

Recovery of VM in case of VM deletion

Recovery of VM or VHD in case of VM Corruption/Data Loss

Create a copy of VM from Older point in time

Retain Backup data for compliance (GA)

Features

Application-Consistent VM level Backup

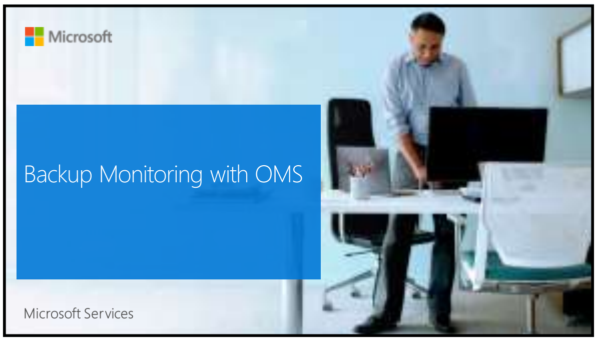
Windows and Linux VMs

Backup Policy Management

Geo Redundant Backup Storage

Encryption (GA)

Microsoft Confidential



Microsoft

## Backup Monitoring with OMS

Microsoft Services

## Which tools to monitor backup ?

- Azure Vault Dashboard
  - Classic portal for V1 vaults
  - ARM portal for V2 vaults
- Azure Audit Logs
  - Operational logs
    - Follow the flow of operations and check for portential issues
  - PowerShell and Alerts
    - Custom alerts creation based on eventing from the audit logs
- Azure Log Analytics ( aka Operationnal Insights)
  - Solution dedicated to backup
  - Integration with the OMS suite

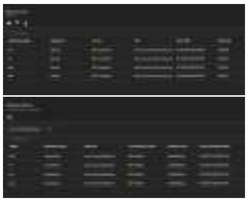
## Azure Vault Dashboard (Classic)

Remarks :

- Data is updated every 24h
- Azure backup monitoring is also integrated to Logs Analytics portal (Operational Insight)

## Audit Logs (Classic)

## Azure Vault Dashboard (ARM)



Remarks :

- Data is organized by « blade »

Microsoft Confidential

## Monitor

Note :

- Dashboard page shows the number of successful, failed or in progress jobs from the last 24 hours
- On the Jobs page, use the Status, Operation, or From and To menus to filter the jobs.
- Monitoring of IaaS VM Backup is coming to Logs Analytics.

Microsoft Confidential

## Monitor

Microsoft Confidential

## Audit

Operations logs enable great post-mortem and audit support for the backup operations.

The following operations are logged in Azure Logs:

- Register
- Unregister
- Configure protection
- Backup ( Both scheduled as well as on-demand backup through BackupNow)
- Restore
- Stop protection
- Delete backup data
- Add policy
- Delete policy
- Update policy
- Cancel job

## Audit

## Alerts

### Via PowerShell

```
$actionEmail = New-AzureRmAlertRuleEmail -CustomEmail
contoso@microsoft.com

Add-AzureRmLogAlertRule -Name backupFailedAlert -
Location "East US" -ResourceGroup R<RGName>
-OperationName
Microsoft.Backup/RecoveryServicesVault/Backup -Status
Failed -TargetResourceId /subscriptions/86eeac34-eth9a-
4de3-84db-
7a27d121967e/resourceGroups/RRGName/providers/micr
osoft.backupbvtd2/RecoveryServicesVault/trinadhVault
-Actions $actionEmail
```

### Via the portal

## Monitor backups through the OMS portal

Remark:

- Dashboard is still evolving
- Main interest is querying the data in the query section, since the dashboard is still limited
- Can ony monitor v1 recovery vaults

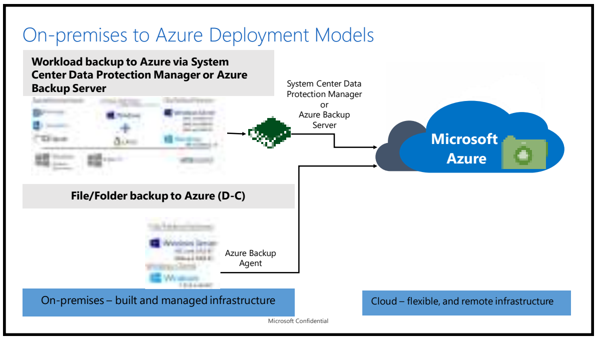
Microsoft Confidential

Demo: Overview of the monitoring solutions

Microsoft

## Deployment & Billing

Microsoft Services



## On-premises to Azure Deployment Models

**Workload backup to Azure via System Center Data Protection Manager or Azure Backup Server**

System Center Data Protection Manager or Azure Backup Server

Microsoft Azure

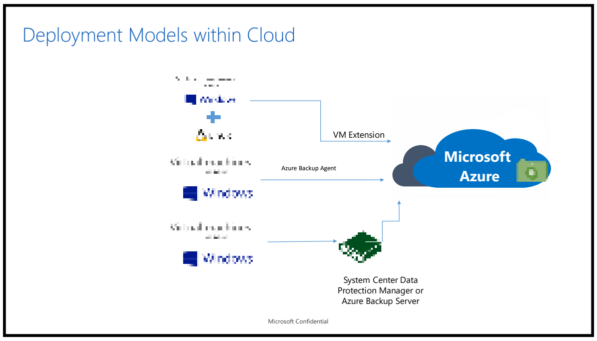
**File/Folder backup to Azure (D-C)**

Azure Backup Agent

On-premises – built and managed infrastructure

Cloud – flexible, and remote infrastructure

Microsoft Confidential



## Deployment Models within Cloud

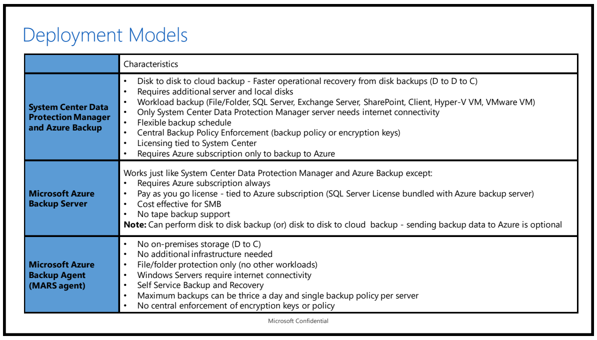
VM Extension

Azure Backup Agent

Microsoft Azure

System Center Data Protection Manager or Azure Backup Server

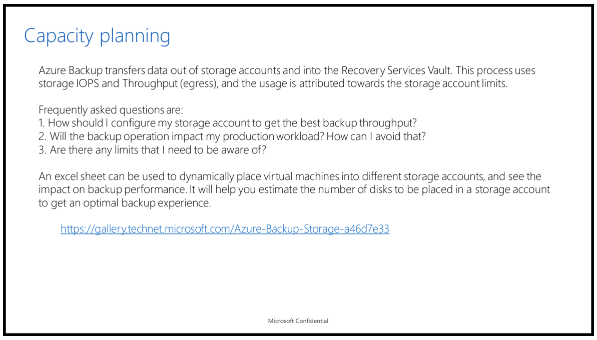
Microsoft Confidential



## Deployment Models

| | Characteristics |
|---|---|
| **System Center Data Protection Manager and Azure Backup** | • Disk to disk to cloud backup - Faster operational recovery from disk backups (D to D to C)<br>• Requires additional server and local disks<br>• Workload backup (File/Folder, SQL Server, Exchange Server, SharePoint, Client, Hyper-V VM, VMware VM)<br>• Only System Center Data Protection Manager server needs internet connectivity<br>• Flexible backup schedule<br>• Central Backup Policy Enforcement (backup policy or encryption keys)<br>• Licensing tied to System Center<br>• Requires Azure subscription only to backup to Azure |
| **Microsoft Azure Backup Server** | Works just like System Center Data Protection Manager and Azure Backup except:<br>• Requires Azure subscription always<br>• Pay as you go license - tied to Azure subscription (SQL Server License bundled with Azure backup server)<br>• Cost effective for SMB<br>• No tape backup support<br>**Note:** Can perform disk to disk backup (or) disk to disk to cloud backup - sending backup data to Azure is optional |
| **Microsoft Azure Backup Agent (MARS agent)** | • No on-premises storage (D to C)<br>• No additional infrastructure needed<br>• File/folder protection only (no other workloads)<br>• Windows Servers require internet connectivity<br>• Self Service Backup and Recovery<br>• Maximum backups can be thrice a day and single backup policy per server<br>• No central enforcement of encryption keys or policy |

Microsoft Confidential



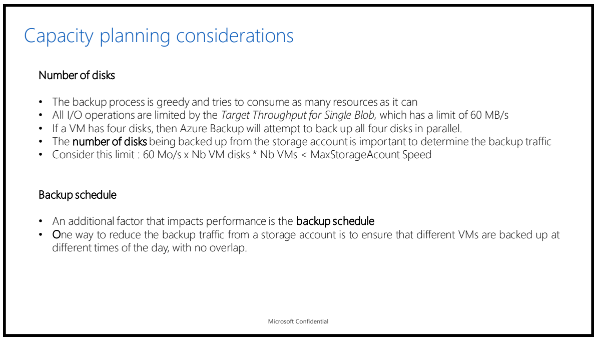
## Capacity planning

Azure Backup transfers data out of storage accounts and into the Recovery Services Vault. This process uses storage IOPS and Throughput (egress), and the usage is attributed towards the storage account limits.

Frequently asked questions are:
1. How should I configure my storage account to get the best backup throughput?
2. Will the backup operation impact my production workload? How can I avoid that?
3. Are there any limits that I need to be aware of?

An excel sheet can be used to dynamically place virtual machines into different storage accounts, and see the impact on backup performance. It will help you estimate the number of disks to be placed in a storage account to get an optimal backup experience.

https://gallery.technet.microsoft.com/Azure-Backup-Storage-a46d7e33



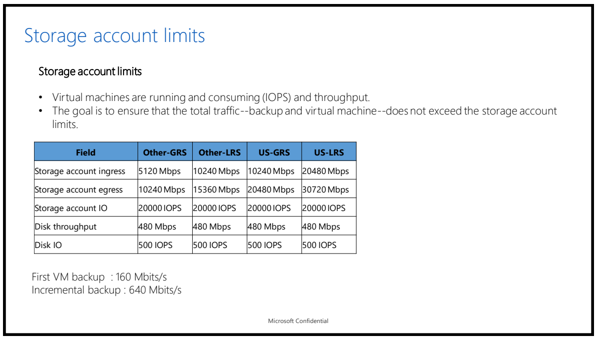
## Capacity planning considerations

Number of disks

- The backup process is greedy and tries to consume as many resources as it can
- All I/O operations are limited by the *Target Throughput for Single Blob*, which has a limit of 60 MB/s
- If a VM has four disks, then Azure Backup will attempt to back up all four disks in parallel.
- The number of disks being backed up from the storage account is important to determine the backup traffic
- Consider this limit : 60 Mo/s x Nb VM disks * Nb VMs < MaxStorageAcount Speed

Backup schedule

- An additional factor that impacts performance is the backup schedule
- One way to reduce the backup traffic from a storage account is to ensure that different VMs are backed up at different times of the day, with no overlap.



## Storage account limits

Storage account limits

- Virtual machines are running and consuming (IOPS) and throughput.
- The goal is to ensure that the total traffic--backup and virtual machine--does not exceed the storage account limits.

| Field | Other-GRS | Other-LRS | US-GRS | US-LRS |
|---|---|---|---|---|
| Storage account ingress | 5120 Mbps | 10240 Mbps | 10240 Mbps | 20480 Mbps |
| Storage account egress | 10240 Mbps | 15360 Mbps | 20480 Mbps | 30720 Mbps |
| Storage account IO | 20000 IOPS | 20000 IOPS | 20000 IOPS | 20000 IOPS |
| Disk throughput | 480 Mbps | 480 Mbps | 480 Mbps | 480 Mbps |
| Disk IO | 500 IOPS | 500 IOPS | 500 IOPS | 500 IOPS |

First VM backup : 160 Mbits/s
Incremental backup : 640 Mbits/s

## Billing

| [illegible] | [illegible] | [illegible] | Azure Backup ($) |
|---|---|---|---|
| [illegible] | [illegible] | [illegible] | 0 |
| [illegible] | [illegible] | [illegible] | 500 |
| [illegible] | [illegible] | [illegible] | 0 |
| [illegible] | [illegible] | [illegible] | 0 |
| [illegible] | [illegible] | [illegible] | 0 |
| [illegible] | [illegible] | [illegible] | 240 (1 hour/month) |
| [illegible] | [illegible] | [illegible] | 1843.20 |
| Total | [illegible] | [illegible] | 2583.20 |
| [illegible] | | | |
| [illegible] | [illegible] | [illegible] | Varies |
| [illegible] | [illegible] | [illegible] | Smaller |
| [illegible] | [illegible] | [illegible] | 0 |
| [illegible] | | | |

## Licensing – Model

- No cost on restore trafic (Outbound)
- Impact LRS/GRS (0,024$ par Go /Mo)
- Pricing Calculator :

https://azure.microsoft.com/en-us/pricing/calculator/

Microsoft

© 2015 Microsoft Corporation. All rights reserved.