
## Module Overview

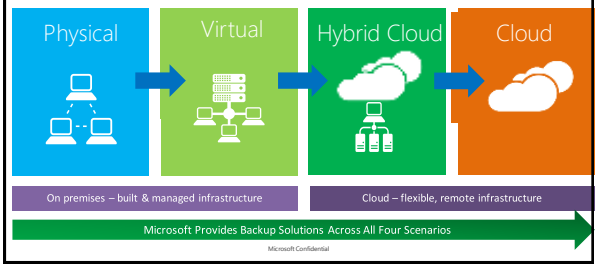
- This module discusses the following sections:
  - Section 1: Product Overview
  - Section 2: Deployment Models
  - Section 3: Preparing for Azure Backup
  - Section 4: Backup Azure IaaS VM Workloads
  - Section 5: Backup Workloads with SCDPM / Azure Backup Server
  - Section 6: Monitor Backup



## Module 1: Microsoft Azure Backup

### Section 1: Product Overview

## Organization's infrastructure evolution




Microsoft Confidential

## Data Protection Challenges

Rapid Data Growth

Data rates are growing at rapid growth per year

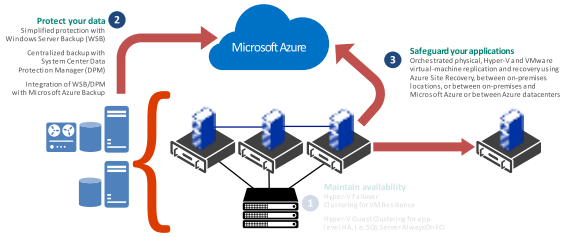
Important data may go without the protection it should have

Operation Challenges

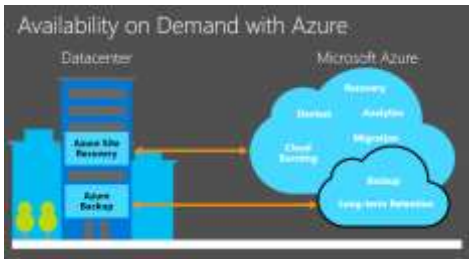
- Cost of storage growing
- Cost of backup solutions
- Complexity of managing all that storage

Microsoft Confidential 5

## Breadth and depth solutions for business continuity and DR



## Business continuity and Disaster recovery with Azure






## 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



## 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

## Azure Backup Key Features (continued)

- **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

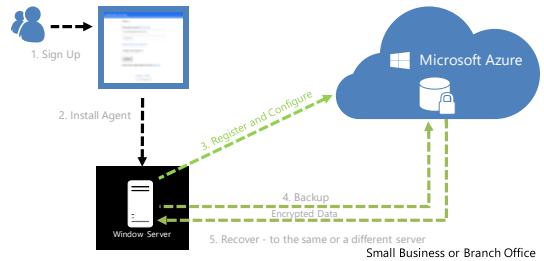


## Azure Backup Key Features (continued)

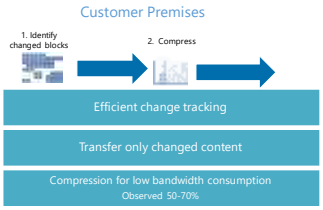
- **Data integrity verified in the cloud**
  - Backed up data is also automatically checked for integrity once the backup is complete. As a result, any corruptions due to data transfer are automatically identified and repair is attempted in the next backup
- **Configurable retention policies**
  - Retention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



## How Microsoft Azure Backup Works

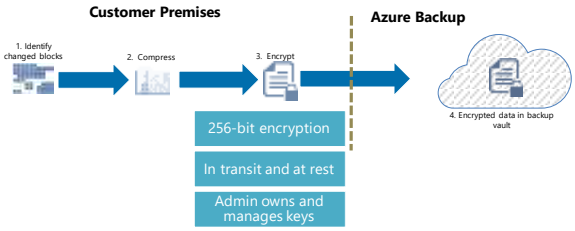


## Azure Backup Network Efficiency





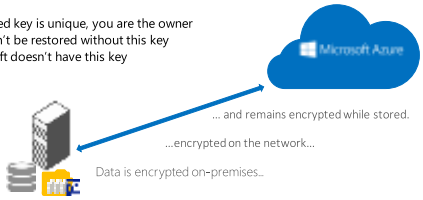

## Azure Backup Security






## Security

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

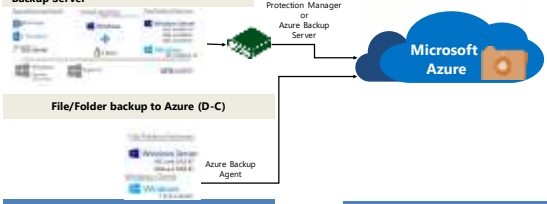


Module 1: Microsoft Azure Backup

Section 2: Deployment Models

## On-premises to Azure Deployment Models

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

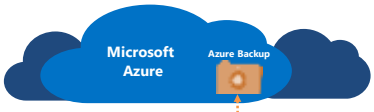



On-premises – built and managed infrastructure

Cloud – flexible, and remote infrastructure

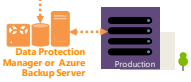


## Enterprise and Branch Office Backup

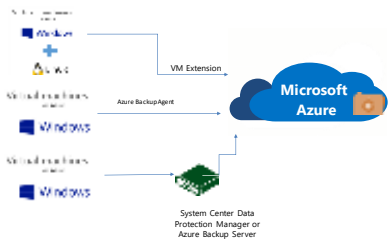



**Solutions:**

- Cloud as tape replacement
- Minimize local storage
- Workload backup to Azure
- Centralized management
- Restore data to alternate server



## Deployment Models within Cloud






## Azure Backup Components

| Component | Benefits | Limits | What is protected? | Where are backups stored? |
|---|---|---|---|---|
| **Azure Backup (MARS) agent (can be deployed to VMs on Azure and on-premises)** | · Back up files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)<br>· No separate backup server required. | · Backup 3x per day<br>· Not application aware; file, folder, and volume-level restore only.<br>· No support for Linux. | · Files,<br>· Folders | Azure Backup vault |
| **System Center DPM (can be deployed in Azure and on-premises)** | · Application-aware snapshots (VSS)<br>· Full flexibility for when to take backups<br>· Recovery granularity (all)<br>· Can use Azure Backup vault<br>· Linux support on Hyper-V and VMware VMs<br>· Back up and restore VMware VMs using DPM 2012 R2 | Cannot back up Oracle workload. | · Files,<br>· Folders,<br>· Volumes,<br>· VMs,<br>· Applications,<br>· Workloads | · Azure Backup vault,<br>· Locally attached disk,<br>· Tape (on-premises only) |



## Azure Backup Components (continued)

| Component | Benefits | Limits | What is protected? | Where are backups stored? |
|---|---|---|---|---|
| **Azure Backup Server (can be deployed in Azure and on-premises)** | • App aware snapshots (VSS)<br>• Full flexibility for when to take backups<br>• Recovery granularity (all)<br>• Can use Azure Backup vault<br>• Linux support on Hyper-V and VMware VMs<br>• Back up and restore VMware VMs<br>• Does not require a System Center license | • Cannot back up Oracle workload.<br>• Always requires live Azure subscription<br>• No support for tape backup | • Files,<br>• Folders,<br>• Volumes,<br>• VMs,<br>• Applications,<br>• Workloads | • Azure Backup vault,<br>• Locally attached disk |
| **Azure IaaS VM Backup** | • Native backups for Windows/Linux<br>• No specific agent installation required<br>• Fabric-level backup with no backup infrastructure needed | • Back up VMs once-a-day<br>• Restore VMs only at disk level<br>• Cannot back up on-premises | • VMs,<br>• All disks (using PowerShell) | Azure Backup vault |

## Which applications and workloads can be backed up?

| Workload | Source machine | Azure Backup solution |
|---|---|---|
| Files and folders | Windows Server | Azure Backup agent, System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent) |
| Files and folders | Windows client | Azure Backup agent, System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent) |
| Hyper-V virtual machine (Windows) | Windows Server | System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent) |
| Hyper-V virtual machine (Linux) | Windows Server | System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent) |
| Microsoft SQL Server | Windows Server | System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent) |
| Microsoft SharePoint | Windows Server | System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent) |
| Microsoft Exchange | Windows Server | System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent) |
| Azure IaaS VMs (Windows) | - | Azure Backup (VM extension) |
| Azure IaaS VMs (Linux) | - | Azure Backup (VM extension) |

22

## Azure Backup Agent - Supported Platforms

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



## Module 1: Microsoft Azure Backup

Section 3: Preparing for Azure Backup

## Backup Vault

- The Azure Backup service uses a vault called the Recovery Services vault.
- Your vault is the location that you use to store backup and configuration information about servers that you are protecting using Azure Backup.
- Each vault you create is in a specific region and can also be moved between resource groups and subscriptions
- For IaaS VM backups, the vault stores all the backups and recovery points that have been created over time.
- The vault also contains the backup policies that will be applied to the virtual machines being backed up



## Description (continued)



## Getting Started with Azure Backup

On Azure

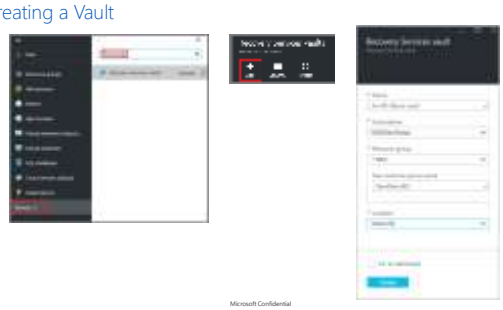
- To back up Virtual Machines hosted in Azure, you must first:
  - Create a Recovery Services vault
    - You must create a recovery services vault in the geographic region where you want to store the data
  - Select a Backup Policy and VM workloads in the 'Getting Started with Backup' wizard

On-Premise

- To back up files and data from your Windows Server to Azure, you must first:
  - Create a Recovery Services vault
    - 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
  - Install the Azure Backup Agent and register the server

## Creating a Vault





## Determine storage redundancy



## Storage redundancy

- Storage data in a 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 backup vault

## Storage redundancy (continued)

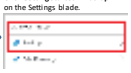
- If you are using Azure as a primary backup storage endpoint (for example, you are backing up to Azure from a Windows Server), you should consider picking (the default) geo-redundant storage option.
- If you are using Azure as a tertiary backup storage endpoint (for example, you are using SCDPM to have 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.



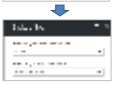
## Configuring Backup (Azure Workloads)

Click **Settings** on the Recovery Services vault dashboard.

Click **Getting Started > Backup** on the Settings blade.



Click **Backup goal** on the Backup blade.
Select **Backup Policy**.
Select **Items to Backup**.



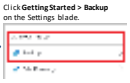
Under **Backup Goal**
Select **Azure** from the Where is your workload running? menu.
Select **Virtual Machine** from the What do you want to backup? menu, and click **OK**.



## Configuring Backup (On-premise Workloads)

Click **Settings** on the Recovery Services vault dashboard.

Click **Getting Started > Backup** on the Settings blade.



Click **Backup goal** on the Backup blade.
Click **Prepare Infrastructure**.

Under **Backup Goal**
Select **On-premises** from the Where is your workload running? menu.
Select **Files and folders** or **List of options** from the What do you want to backup? menu, and click **OK**.

Click **Download Agent for Windows Server or Windows Client** in the **Prepare infrastructure** blade.
Click **Download > Save** to download **Vault Credentials** on the Prepare infrastructure blade.

## Register Your Server to Azure Backup Service

1. Install Azure Backup Agent - 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



## Vault Credentials

- The on-premises machine (Windows Server or Windows client) needs to be authenticated with a backup 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.

## Azure Backup Unsupported Scenarios

- **Migration & recovery scenarios**
  - 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



Module 1: Microsoft Azure Backup

Section 4: Backup Azure IaaS VM workload

## Azure IaaS VM backup

**Features**

- Application Consistent
- No need to shutdown
- Incremental backup
- Long Term Retention
- Restore as VM or VHD

**Configurations**

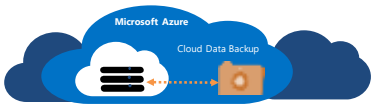
- Windows and Linux
- 16 disks
- Load balancer
- Multi NIC
- Reserved IP
- CloudLink Secure VM
- Premium Storage

**Management**

- Built-in policies
- PowerShell
- Job monitoring and report
- Alerts based on Oplogs



## Overview



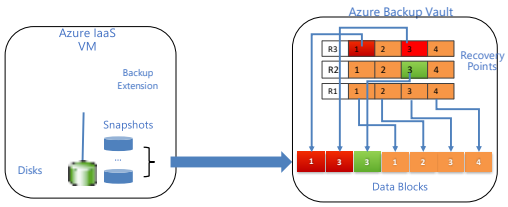

Enterprise ready solution

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



## How It Works ? (continued)

## How It Works? (continued)






## Data consistency

- Azure IaaS VM – Consistency Types

| Application consistency ensures | File-system consistency ensures | Crash consistency |
|---|---|---|
| • That the VM boots up<br>• There is no corruption<br>• There is no data loss<br>• The data is consistent to the application that uses the data, by involving the application at the time of backup - using VSS | • That the VM boots up<br>• There is no corruption<br>• There is no data loss | • No Guarantee<br>• All data is collected at once<br>• No memory contents or pending I/O transactions<br>• Same state as power loss or system failure |

**Note:** For Linux virtual machines, only file-consistent backups are possible, since Linux does not have an equivalent platform to VSS.



## Discover your IaaS VMs

**Tip** :

- Only VMs in the same region and within the same subscription than the backup vault are discoverable

## 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.
- Azure Backup has a limit of 9999 recovery points, also known as backup copies or snapshots. The Backup service does not set an expiration time limit on a recovery point.



## Define items to backup

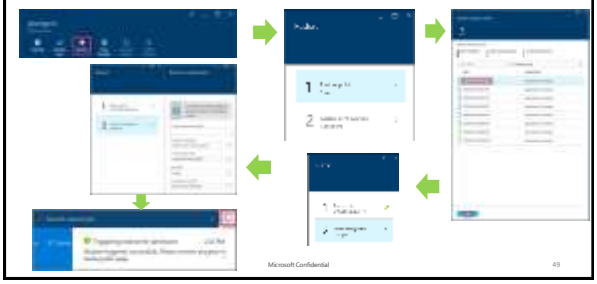
**Tip:**

- 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.



## Protect your IaaS VMs (continued)

## Restore your data





## Limitations

- Backing up virtual machines with more than 16 data disks is not supported.
- Backing up virtual machines with a reserved IP address and no defined endpoint is not supported.
- Backup of Linux virtual machines with Docker extension is not supported.
- Backup data doesn't include network mounted drives attached to VM.
- Replacing an existing virtual machine during restore is not supported. If you attempt to restore the VM when the VM exists, the restore operation fails.
- Cross-region backup and restore is not supported.
- Restoring a domain controller (DC) VM that is part of a multi-DC configuration is supported only through PowerShell. Read more about restoring a multi-DC domain controller.
- Restoring virtual machines that have the following special network configurations is supported only through PowerShell. VMs created using the restore workflow in the UI will not have these network configurations after the restore operation is complete. To learn more, see Restoring VMs with special network configurations.
  - Virtual machines under load balancer configuration (internal and external)
  - Virtual machines with multiple reserved IP addresses
  - Virtual machines with multiple network adapters

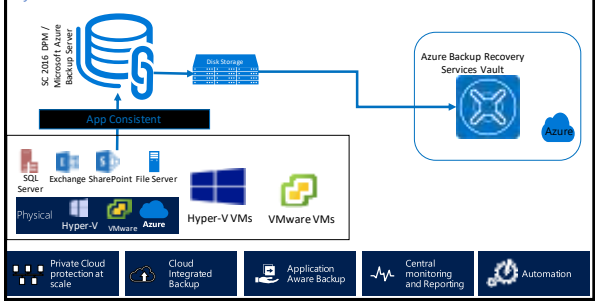


## Demo: Backup Azure VMs with Snapshots

# Module 1: Microsoft Azure Backup

## Section 5: Backup Workload with DPM or MABS

## System Center DPM overview

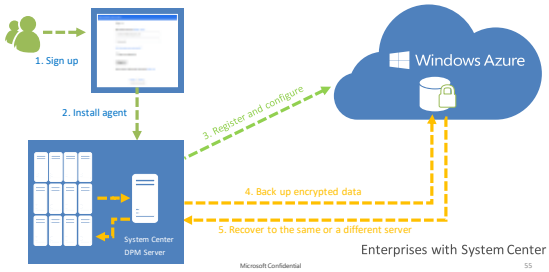



## DPM – Interaction with Azure

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 Backup 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 Backup vault.

## How Windows Azure Backup works




Enterprises with System Center



## DPM – Requirements

Prepare Azure Backup to back up DPM data as follows:

- **Create a Backup 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 Windows server and register the DPM server in the backup vault.



## DPM – Requirements (continued)

- 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

## DPM – Requirements (continued)

- 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 5 % 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 5 GB of free space in the scratch location.
- 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 Backup vault but the size of a data source (for example a virtual machine or database) shouldn't exceed 54400 GB.



## 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)

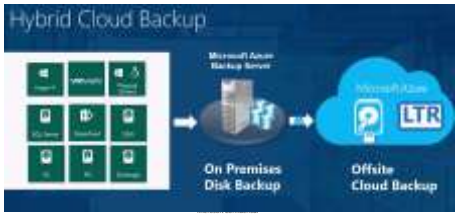
And these are unsupported:

- 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



## 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 (continued)

- When you install, you'll get:

**SQL Server Standard Edition**: A free license of MABS that you can only use for MABS.
**Microsoft Azure Backup Server**: 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 backup 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

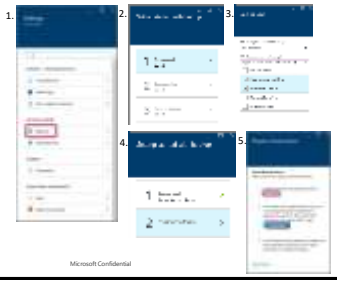
The server can be on a Hyper-V VM, a VMware VM, or a physical host. The recommended minimum requirements for the server hardware are 2 cores and 4 GB RAM. The supported operating systems are listed in the following table.

| Operating System | Platform | SKU |
|---|---|---|
| Windows Server 2012 R2 and latest SPs | 64 bit | Standard, Datacenter, Foundation |
| Windows Server 2012 and latest SPs | 64 bit | Datacenter, Foundation, Standard |
| Windows Storage Server 2012 R2 and latest SPs | 64 bit | Standard, Workgroup |
| Windows Storage Server 2012 and latest SPs | 64 bit | Standard, Workgroup |



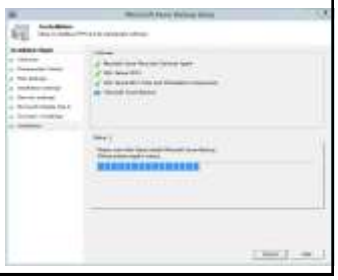
## MABS – Deployment

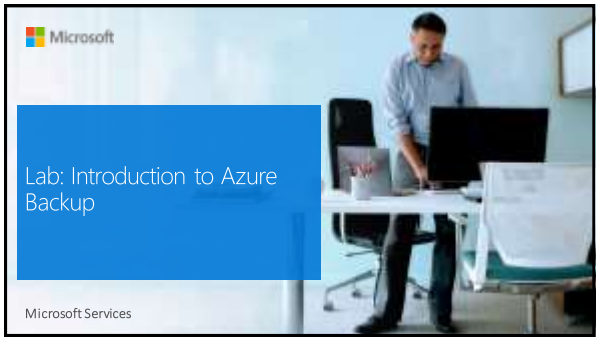
- Creation of a backup vault
- Download vault credentials file
- Download product from backup vault



## MABS – Deployment (continued)

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






Module 1: Microsoft Azure Backup

Section 6: Monitor Backup

## Which tools to monitor backup ?

- **Azure Vault Dashboard**
- **Azure Logs**
  - Operational logs
    - Follow the flow of operations and check for potential issues
  - PowerShell and Alerts
    - Custom alerts creation based on eventing from the audit logs
- **Azure Log Analytics ( aka Operational Insights)**
  - Solution dedicated to backup
  - Integration with the OMS suite




## 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 Log Analytics.



## Monitor (Continued)

## Audit

Event 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)
- Restore
- Stop protection
- Delete backup data
- Add policy
- Delete policy
- Update policy
- Cancel job



## Audit (continued)



## Alerts

The service can be configured to send email notifications for the alerts that occurred over the past hour, or when particular types of events occur.

### 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

Demo: Overview of the monitoring solutions

Microsoft