Microsoft Azure: Site Recovery Services Workshop*PLUS*

Conditions and Terms of Use

Microsoft Confidential

This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

© 2016 Microsoft Corporation. All rights reserved.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see Use of Microsoft Copyrighted Content at

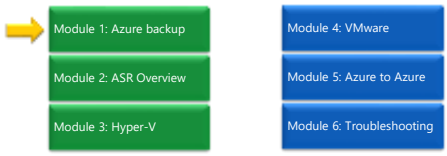
http://www.microsoft.com/en-us/legal/intellectualproperty/permissions/default.aspx

Active Directory, Azure, BitLocker, Hyper-V, Microsoft, Microsoft Corporate Logo, Outlook, PowerPoint, SharePoint, SQL Server, Windows, Windows Server, and Windows PowerShell are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

How to View This Presentation

- To switch to **Notes Page** view:
  - On the ribbon, click the **View** tab, and then click **Notes Page**
- To navigate through notes, use the Page Up and Page Down keys
  - Zoom in or zoom out, if required
- In the **Notes Page** view, you can:
  - Read any supporting text
    - Terminology List—a list of terms used in this course is provided in the Notes section.
  - Add notes to your copy of the presentation, if required
- Take the presentation files home with you

Workshop overview



Microsoft Confidential

Module 1: Introduction to Microsoft Azure Backup

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

Microsoft Confidential

Module Objective

- After completing this module, you will be able to:
  - Understand the power, simplicity and efficiency of Microsoft Azure Backup
  - Understand how to deploy, configure and manage Microsoft Azure Backup

Microsoft Confidential

Module 1: Microsoft Azure Backup

Section 1: Product Overview

Section Objectives

- After completing this section, you will be able to:
  - What is Cloud computing and Microsoft Azure
  - Articulate the challenges that Microsoft Azure Backup solves
  - Understand what Microsoft Azure Backup does
  - Identify Key Features in Microsoft Azure Backup
  - Be aware of Supported Platforms and Unsupported Scenarios

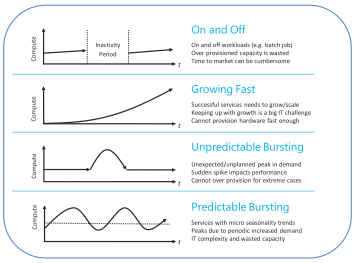
Microsoft Confidential

What is the Cloud?

- An approach to computing that is about Internet scaling and connecting to a variety of devices and endpoints

Microsoft Confidential

Cloud Computing patterns

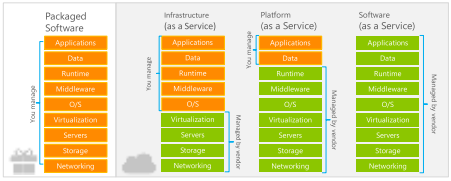


Microsoft Confidential

Cloud Computing terms

Microsoft Confidential

Cloud Computing terms (continued)



Microsoft Confidential

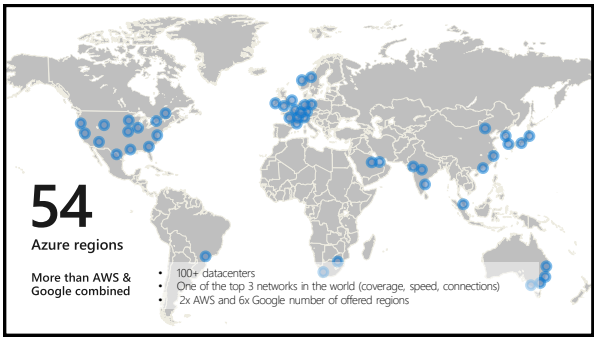
Microsoft Azure Compute

App Service

Cloud Services

Virtual Machines (VMs - IaaS)

Microsoft Confidential



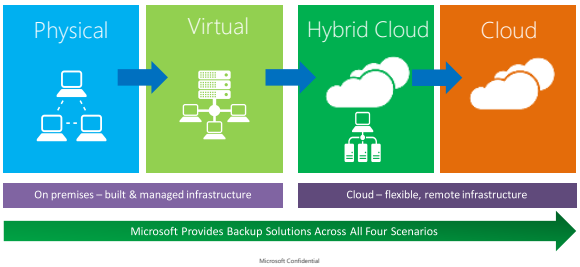
54

Azure regions

More than AWS & Google combined

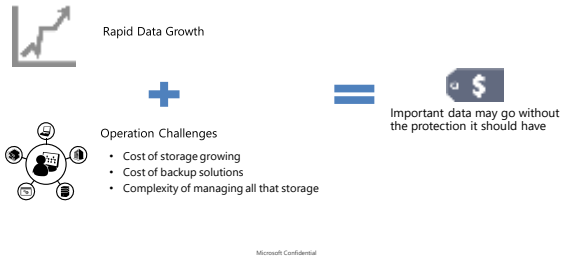
- 100+ datacenters
- One of the top 3 networks in the world (coverage, speed, connections)
- 2x AWS and 6x Google number of offered regions

Organization's infrastructure evolution



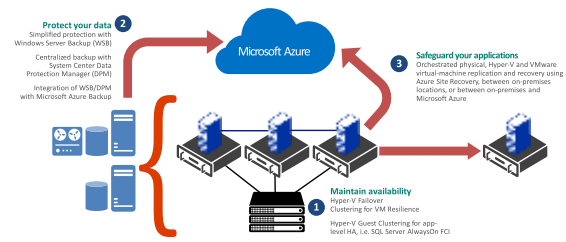
Microsoft Confidential

Data Protection Challenges



Microsoft Confidential

Breadth and depth solutions for business continuity and DR



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 (continued)

- **Application-consistent backup**
  - An application-consistent backup means a recovery point has all required data to restore the backup copy, which ensure additional fixes are not required to restore the data.
  - Restoring application-consistent data reduces the restoration time, allowing you to quickly return to a running state.
- **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

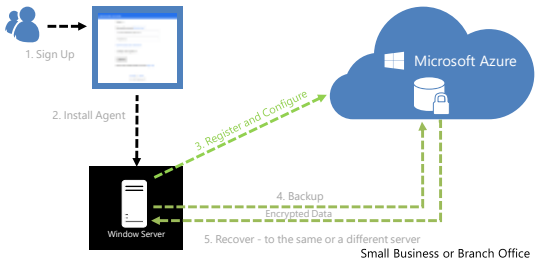
Microsoft Confidential

Azure Backup Key Features (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
- **Multiple storage options**
  - An aspect of high-availability is storage replication. Azure Backup offers two types of replication: locally redundant storage and geo-redundant storage.
- **Role-Based Access Control**
  - Azure Backup provides 3 built-in roles to control backup management operations: Backup Contributor, Backup Operator, Backup Reader

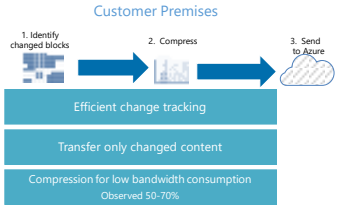
Microsoft Confidential

How Microsoft Azure Backup Works



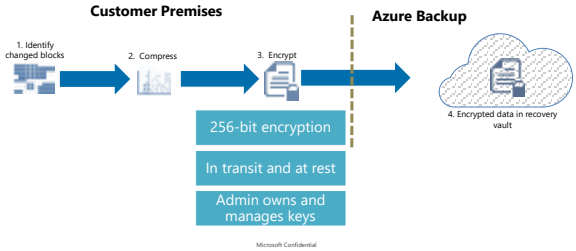
Microsoft Confidential

Azure Backup Network Efficiency



Microsoft Confidential

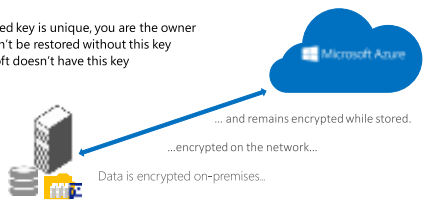
Azure Backup Security



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



Microsoft Confidential 27

How are Microsoft Azure Charges Incurred?

- The pricing model for Azure Backup has two components:
  - *Protected instances:* This is the primary billing unit for Azure Backup. Customers pay for the number of instances that are protected with the Azure backup service.
    - An instance is a physical or virtual computer, files and folders or database. The size of the backed-up data determines the pricing for Azure Backup in each protected instance before compression and encryption.
  - *Storage:* Customers can choose between Locally Redundant Storage (LRS) or Geo-Redundant Storage (GRS)* for their backup vault. The net price for Storage depends on the amount of data stored with the service.

    * When you write data into GRS accounts, that data will be replicated to another Azure region. The Geo-Replication Data Transfer charge is the bandwidth cost of replicating that data to another Azure region.

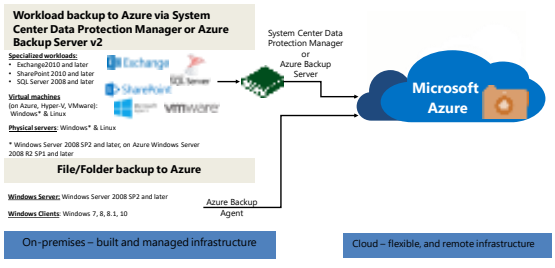
- Customers **will not be charged** for any restore operations or outbound network bandwidth (egress) that is associated with restore operations.

Microsoft Confidential 28

Module 1: Microsoft Azure Backup

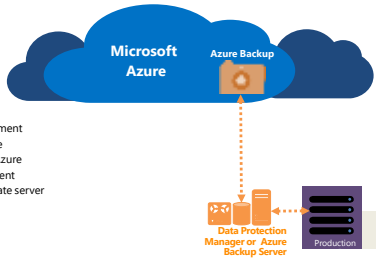
Section 2: Deployment Models

On-premises to Azure Deployment Models



Microsoft Confidential

Enterprise and Branch Office Backup

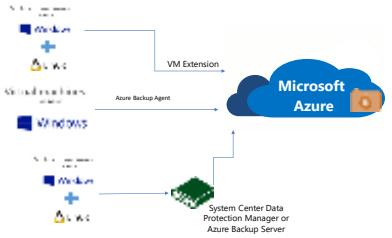


Solutions:

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

Microsoft Confidential

Deployment Models within Cloud



Microsoft Confidential

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) · No separate backup server required.	· Backup 3x per day · Not application aware; file, folder, and volume-level restore only, · No support for Linux.	· Files, · Folders · System State	Recovery Services vault
System Center DPM (can be deployed in Azure and on-premises)	· Application-aware snapshots (VSS) · Full flexibility for when to take backups · Recovery granularity (all) · Can use Recovery Services vault · Linux support on Hyper-V and VMware VMs · Back up and restore VMware VMs using DPM 2012 R2	Cannot back up Oracle workload.	· Files, · Folders, · Volumes, · VMs, · Applications, · Workloads · System State	· Recovery Services vault, · Locally attached disk, · Tape (on-premises only)

Microsoft Confidential

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) • Full flexibility for when to take backups • Recovery granularity (all) • Can use Recovery Services vault • Linux support on Hyper-V and VMware VMs • Back up and restore VMware VMs • Does not require a System Center license	• Cannot back up Oracle workload. • Always requires live Azure subscription • No support for tape backup	• Files, • Folders, • Volumes, • VMs, • Applications, • Workloads, • System State	• Recovery Services vault, • Locally attached disk
Azure IaaS VM Backup	• Native backups for Windows/Linux • No specific agent installation required • Fabric-level backup with no backup infrastructure needed	• Back up VMs once-a-day • Restore VMs only at disk level • Cannot back up on-premises	• VMs, • All disks (using PowerShell)	Recovery Services vault

Microsoft Confidential

Which applications and workloads can be backed up?

Workload	Source machine	Azure Backup solution
Files and folders	Windows Server 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 & Linux	Windows Server	System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)
VMware virtual machine	-	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)	running in Azure	Azure Backup (VM extension)
Azure IaaS VMs (Linux)	running in Azure	Azure Backup (VM extension)

Microsoft Confidential

Azure Backup Agent - Supported Platforms

Workstation	
Windows 10 64 bit	Enterprise, Pro, Home
Windows 8.1 64 bit	Enterprise, Pro
Windows 8 64 bit	Enterprise, Pro
Windows 7 64 bit	Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter

Microsoft Confidential

Azure Backup Agent - Supported Platforms

Server	
Windows Server 2019 64 bit	Standard, Datacenter, Essentials
Windows Server 2016 64 bit	Standard, Datacenter, Essentials
Windows Server 2012 R2 64 bit	Standard, Datacenter, Foundation
Windows Server 2012 64 bit	Datacenter, Foundation, Standard
Windows Storage Server 2016 64 bit	Standard, Workgroup
Windows Storage Server 2012 R2 64 bit	Standard, Workgroup, Essential
Windows Storage Server 2012 64 bit	Standard, Workgroup
Windows Server 2008 R2 SP1 64 bit	Standard, Enterprise, Datacenter, Foundation
Windows Server 2008 64 bit	Standard, Enterprise, Datacenter

Microsoft Confidential

Module 1: Microsoft Azure Backup

Section 3: Preparing for Azure Backup

Recovery Services Vault

- The Azure Backup service has one type of vault called the Recovery Services vault.
- Your vault is the location that you use to store backups from your servers that you are protecting using Azure Backup.
- Each vault you create can be in a specific region and is tied to your organization's subscription.
- For IaaS VM backups, 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

.

Microsoft Confidential

Description (continued)

Microsoft Confidential

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 backup vault in the geographic region where you want to store the data
  - Define a backup Goal, Backup policy and select the VMs

On-Premises

- 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 backup vault in the geographic region where you want to store the data
  - Download vault credentials
  - Install the Azure Backup Agent ***(MARS)*** and register the server

Microsoft Confidential

Creating a Vault

Microsoft Confidential

Determine storage redundancy

Microsoft Confidential

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

Microsoft Confidential

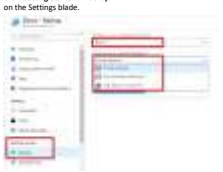
Storage redundancy (continued)

- 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.

Microsoft Confidential

Configuring Backup (Azure Workloads)

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



Under **Backup Goal**
Select **Azure** from the Where is your workload running? menu.
Select the item you want from the *What do you want to backup?* Menu
Click the blue **Backup** button

Microsoft Confidential

Configuring Backup (Azure Stack Workloads)

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

Under **Backup Goal**
Select **Azure Stack** from the Where is your workload running? menu.
Select the item you want from the *What do you want to backup?* Menu
Click the blue **Prepare Infrastructure** button

Microsoft Confidential

Configuring Backup (On-premises Workloads)

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

Under **Backup Goal**
Select **On-premises** from the Where is your workload running? menu.
Select the item you want from the *What do you want to backup?* Menu
Click the blue **Prepare Infrastructure** button

Microsoft Confidential

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

Microsoft Confidential

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

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.

Microsoft Confidential

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

Microsoft Confidential

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

Microsoft Confidential

Module 1: Microsoft Azure Backup

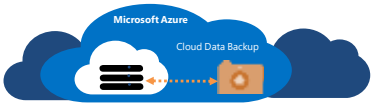
Section 4: Backup Azure IaaS VM workload

Azure IaaS VM backup

Features	Configurations	Management
• Application Consistent • No need to shutdown • Incremental backup • Long Term Retention • Restore as VM or VHD	• Windows and Linux • 16 disks maximum • Load balancer • Multi NIC • Reserved IP • CloudLink Secure VM • Premium Storage	• Built-in policies • PowerShell • Job monitoring and report • Alerts based on Oplogs

Microsoft Confidential

Overview



Enterprise ready solution

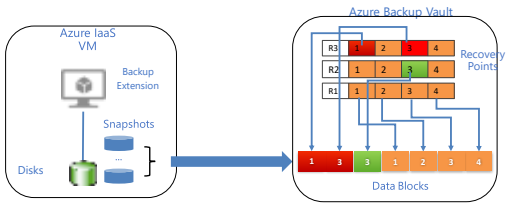
- Application consistent backup for Windows and for Linux workloads
- Fabric level protection for Azure IaaS VMs
- Azure Backup transfers snapshots taken on a VM to a secure, reliable Azure Backup vault and can restore the VM in a single click.
- Long-term protection using industry standard GFS based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

Microsoft Confidential

How It Works ? (continued)

Microsoft Confidential

How It Works? (continued)



Microsoft Confidential

Instant Restore

- Super fast restore from locally stored snapshot
- Default retention - 2 days – customizable

- Snapshots are incremental in storage and charged per GB

Data consistency

- Azure IaaS VM – Consistency Types

Application consistency ensures	File-system consistency ensures	Crash consistency
• 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	• That the VM boots up • There is no corruption • There is no data loss	• No Guarantee • All data is collected at once • No memory contents or pending I/O transactions • Same state as power loss or system failure

Note: For Linux virtual machines a pre-script and post-script framework can be installed on each VM to all for Application Consistent backups. https://docs.microsoft.com/en-us/azure/backup/backup-azure-linux-app-consistent

Discover your IaaS VMs

Tip :

- Only VMs in the same region and within the same subscription as 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.

Microsoft Confidential

Define a custom backup policy

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

- Initiate Backup from the VM

Microsoft Confidential

Protect your IaaS VMs

- The BEST way

Microsoft Confidential

```
{
"apiVersion": "2017-05-10",
"name": "BackupVaultAndPolicy-vaultNAME-DailyPolicy",
"type": "Microsoft.Resources/deployments",
"resourceGroup": "[parameters('backupVaultRGName')]",
"properties": {
    "mode": "Incremental",
    "template": {
        "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
        "contentVersion": "1.0.0.0",
        "resources": [
            {
                "name": "[parameters('backupVaultName')]",
                "type": "Microsoft.RecoveryServices/vaults",
                "apiVersion": "2016-06-01",
                "location": "[parameters('location')]",
                "sku": {
                    "name": "RS0",
                    "tier": "Standard"
                },
                "properties": {},
                "dependsOn": []
            },
            {
                "name": "[concat(parameters('backupVaultName'), '/', parameters('backupPolicyName'))]",
                "apiVersion": "2017-07-01",
                "type": "Microsoft.RecoveryServices/vaults/backupPolicies",
                "properties": {
                    "backupManagementType": "AzureIaasVM",
                    "schedulePolicy": "[parameters('backupPolicySchedule')]",
                    "retentionPolicy": "[parameters('backupPolicyRetention')]",
                    "timeZone": "[parameters('backupPolicyTimeZone')]"
                },
                    "dependsOn": [
                    "[resourceId(parameters('backupVaultRGName'), 'Microsoft.RecoveryServices/vaults', parameters('backupVaultName'))]"
                ]
            }
        ]
    }
}
```

Microsoft Confidential

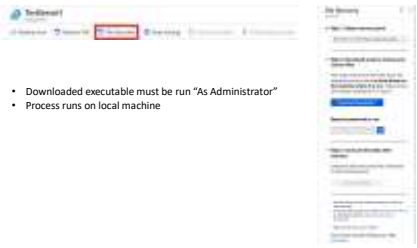
Protect your IaaS VMs

Microsoft Confidential

Restore your data

Microsoft Confidential

Restore your data



- Downloaded executable must be run "As Administrator"
- Process runs on local machine

Microsoft Confidential

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.
- Backing up Linux VMs encrypted through Linux Unified Key Setup (LUKS) encryption is not supported.
- Backup data doesn't include network mounted drives attached to VM.
- Cross-region backup and restore are not supported.
- Managing special

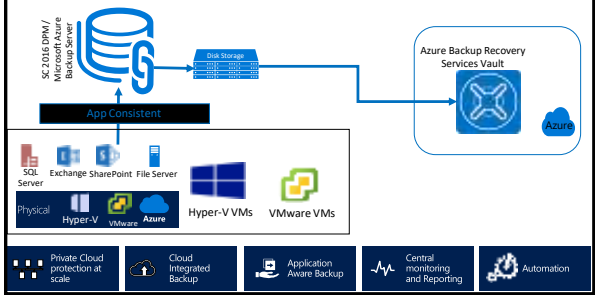
Microsoft Confidential

Demo: Backup Azure VMs with snapshots

Module 1: Microsoft Azure Backup

Section 5: Backup Workload with DPM or MABS

System Center DPM overview



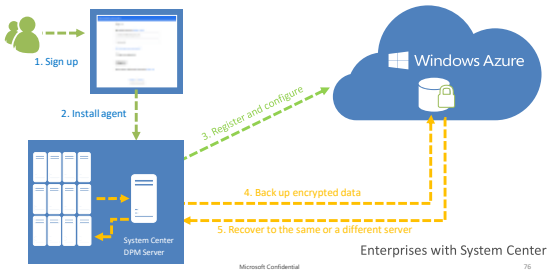
DPM – Interaction with Azure

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 and upwards, 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.

Microsoft Confidential

How Windows Azure Backup works



Enterprises with System Center

Microsoft Confidential

DPM – Requirements

Prepare Azure Backup to back up DPM data as follows:

- **Create a Recovery services vault** — Create a vault in the Azure portal
- **Download vault credentials** — Download the credentials you use to register the DPM server with the Recovery Services vault.
- **Install the Azure Backup Agent and register the server** — Install the agent on each DPM server and register the DPM server with the Recovery Services vault.

Microsoft Confidential

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 or higher. 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 or higher
- 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 (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.

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)

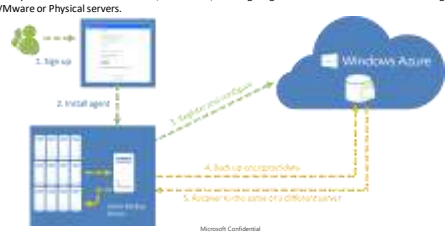
And these are unsupported:

- 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 – 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.



Microsoft Confidential

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.

- 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)

Microsoft Confidential

MABS – Requirements

Scenario	DPM/MABS
MABS on an Azure VM	Windows Server 2012 R2, 2106 and 2019 Datacenter edition We recommend that you start with an image from the marketplace. Minimum A2 Standard with two cores and 3.5 GB of RAM.
DPM on an Azure VM	System Center 2012 R2 with Update 3 or later. Windows operating system as required by System Center. We recommend that you start with an image from the marketplace. Minimum A2 Standard with two cores and 3.5 GB of RAM.
MABS on-premises	Supported 64-bit operating systems: MABS v3 and later: Windows Server 2019 (Standard, Datacenter, Essentials) MABS v2 and later: Windows Server 2016 (Standard, Datacenter, Essentials) All MABS versions: Windows Server 2012 R2 and Storage Server 2012 R2
DPM on-premises	Physical server/Hyper-V VM: System Center 2012 SP1 or later. VMware VM: System Center 2012 R2 with Update 5 or later.

Microsoft Confidential

MABS Deployment Options

Deployment	Support	Details
Deployed on-premises	Physical server Hyper-V VM VMware VM	If DPM/MABS is installed as a VMware VM, it only backs up VMware VMs and workloads that are running on those VMs.
Deployed as an Azure Stack VM	MABS only	DPM can't be used to back up Azure Stack VMs.
Deployed as an Azure VM	Protects Azure VMs and workloads that are running on those VMs	DPM/MABS running in Azure can't back up on-premises machines.

Microsoft Confidential

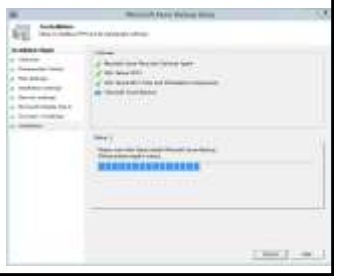
MABS – Deployment

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

Microsoft Confidential

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

Microsoft Confidential

Demo: Overview of the monitoring solutions

Monitor

Note :

- Dashboard page shows the number of successful, failed or in progress jobs from the last 24 hours
- On the Jobs page sort and filter to better see results

Microsoft Confidential

Monitor

Microsoft Confidential

Monitor

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

Microsoft Confidential

Monitor

- Quick Insights
  - 24 synopsis

Microsoft Confidential

Alerts

Microsoft Confidential

Module Summary

- In this lesson, you learned:
  - The simplicity and efficiency of Microsoft Azure Backup
  - How to deploy, configure and manage Microsoft Azure Backup