

# 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



Module 1: Azure backup

Module 2: ASR Overview

Module 3: Hyper-V

Module 4: VMware

Module 5: Azure to Azure

Module 6: Troubleshooting

# 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

# 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

# Module 1: Microsoft Azure Backup

## Section 1: Product Overview



# Section Objectives

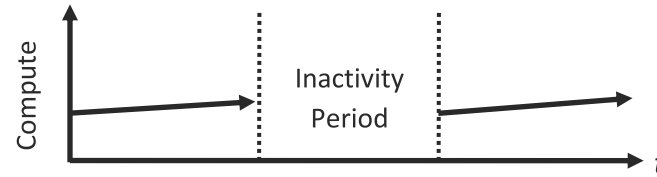
- After completing this section, you will be able to:
  - What is Cloud computing and Microsoft Azure
  - Articulate the challenges that Microsoft Azure Backup solves
  - Understand what Microsoft Azure Backup does
  - Identify Key Features in Microsoft Azure Backup
  - Be aware of Supported Platforms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

# What is the Cloud?

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

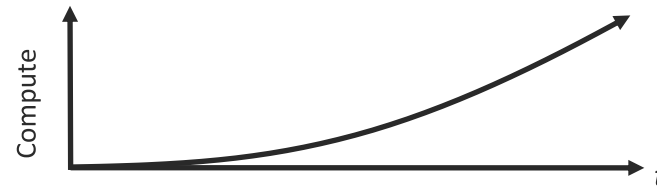


# Cloud Computing patterns



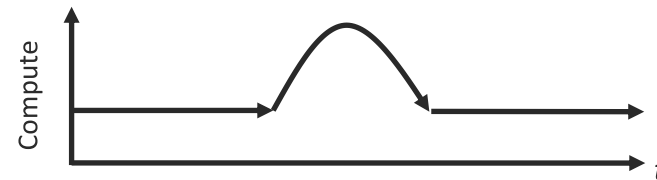
## On and Off

On and off workloads (e.g. batch job)  
Over provisioned capacity is wasted  
Time to market can be cumbersome



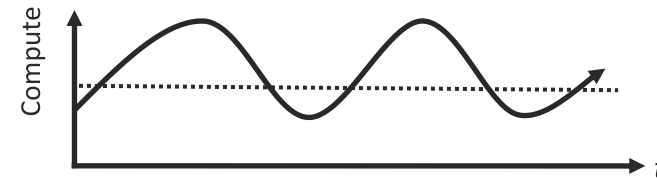
## Growing Fast

Successful services needs to grow/scale  
Keeping up with growth is a big IT challenge  
Cannot provision hardware fast enough



## Unpredictable Bursting

Unexpected/unplanned peak in demand  
Sudden spike impacts performance  
Cannot over provision for extreme cases



## Predictable Bursting

Services with micro seasonality trends  
Peaks due to periodic increased demand  
IT complexity and wasted capacity

# Cloud Computing terms



IaaS

Infrastructure as a Service

Host



PaaS

Platform as a Service

Build

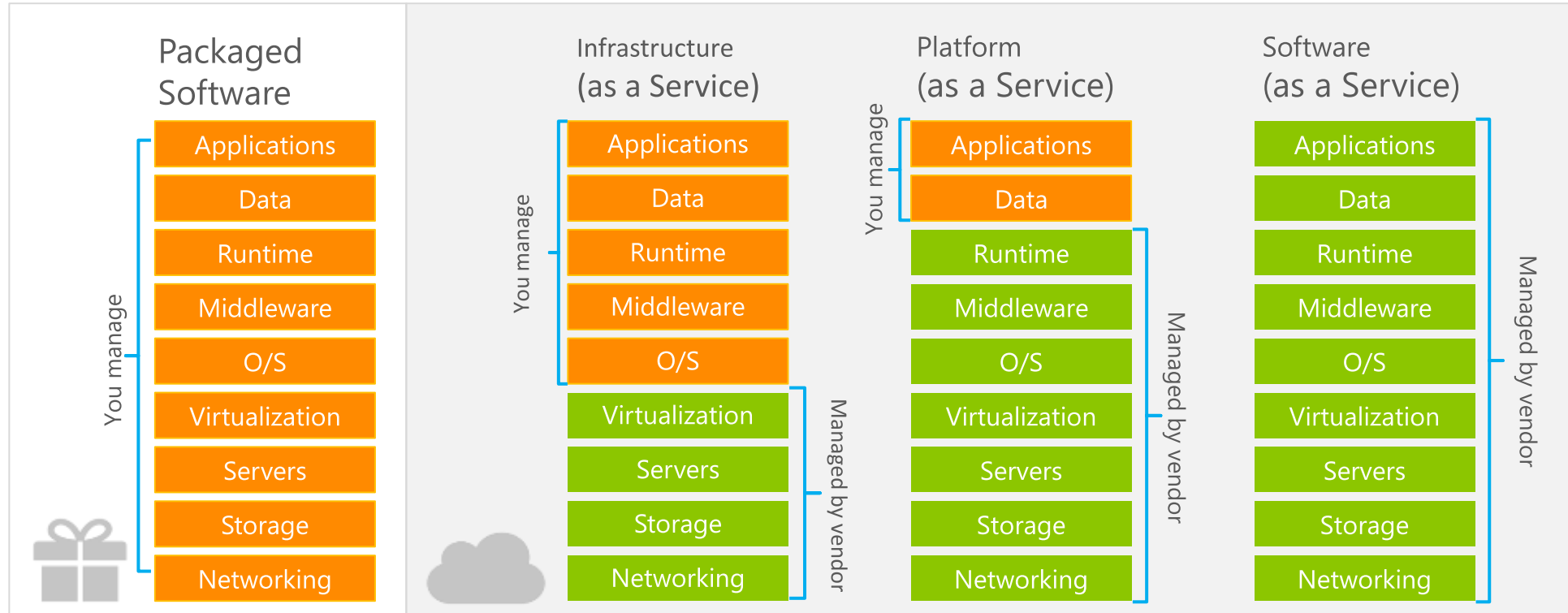


SaaS

Software as a Service

Consume

# Cloud Computing terms (continued)



# Microsoft Azure Compute



App Service



Cloud Services



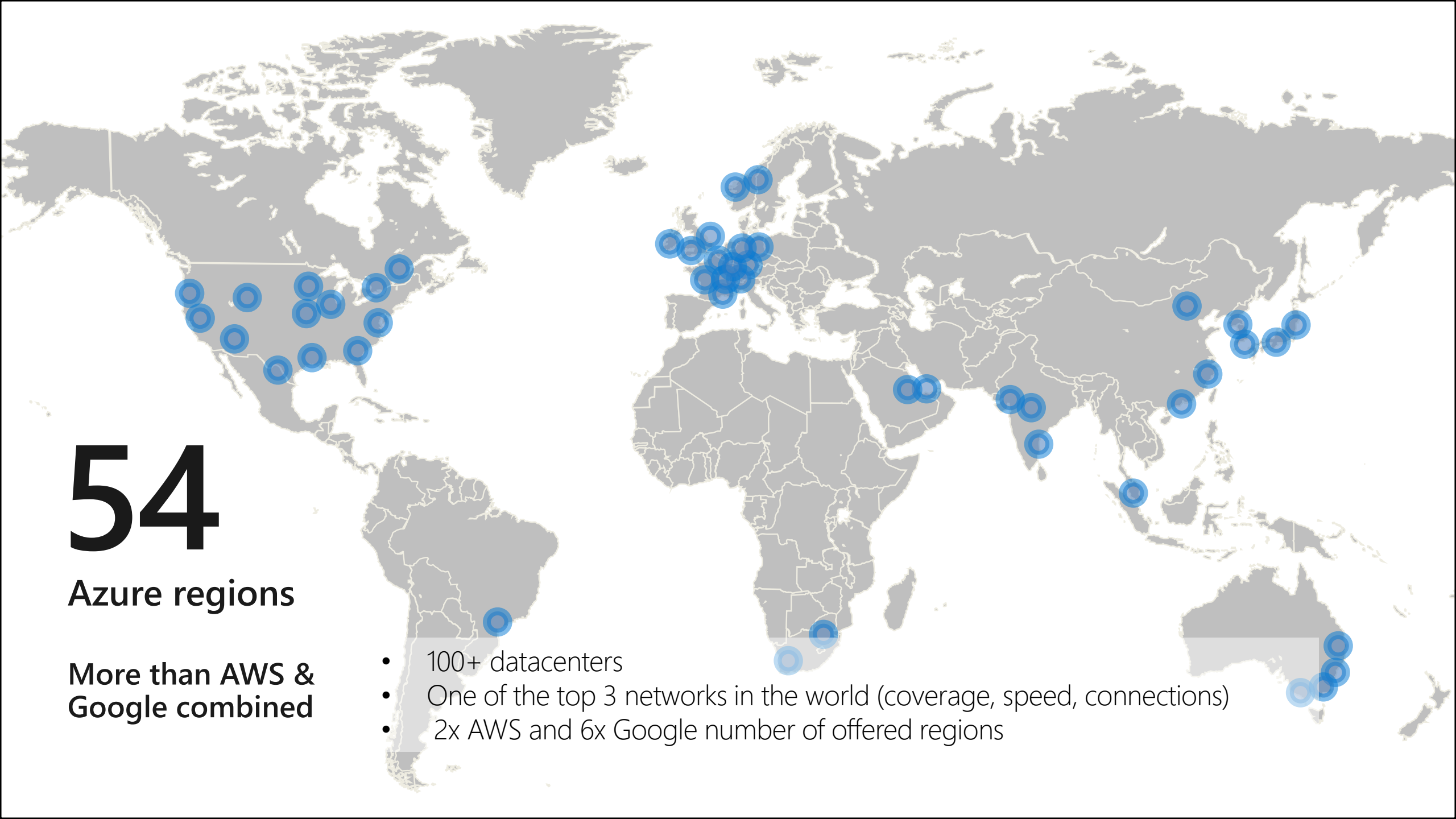
Virtual Machines (VMs -  
IaaS)

# 54

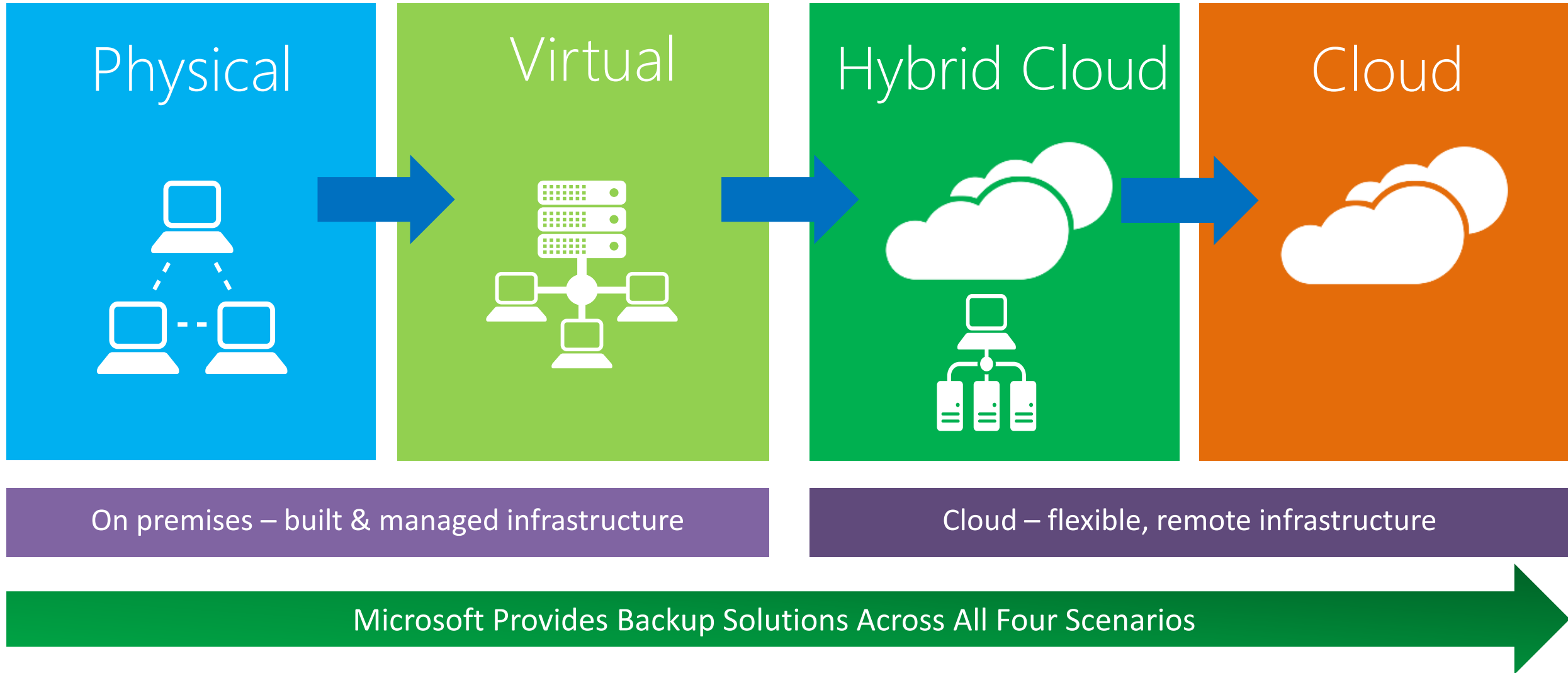
Azure regions

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





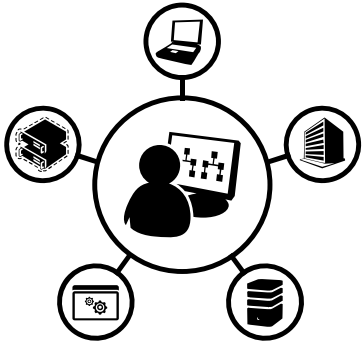
# Data Protection Challenges



Rapid Data Growth



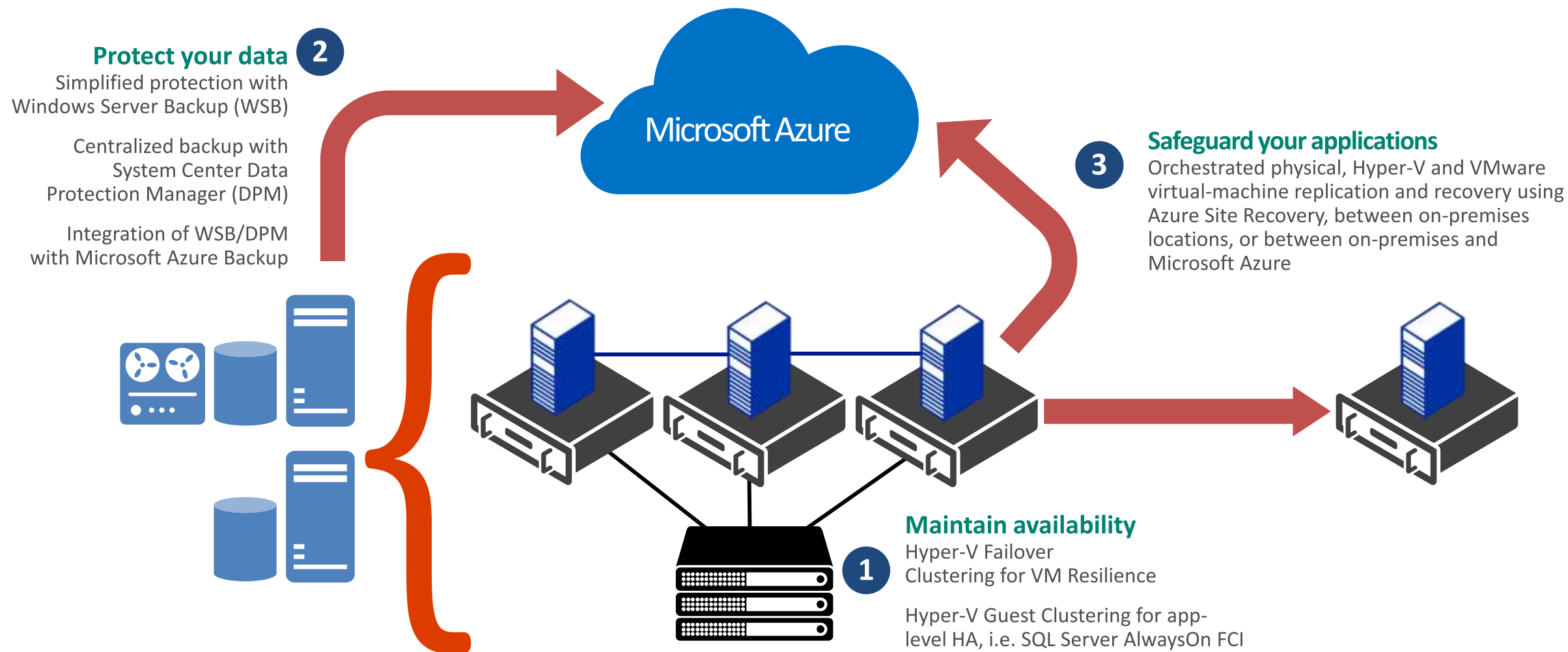
Important data may go without the protection it should have



Operation Challenges

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

# 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

# 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)

- **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

# 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

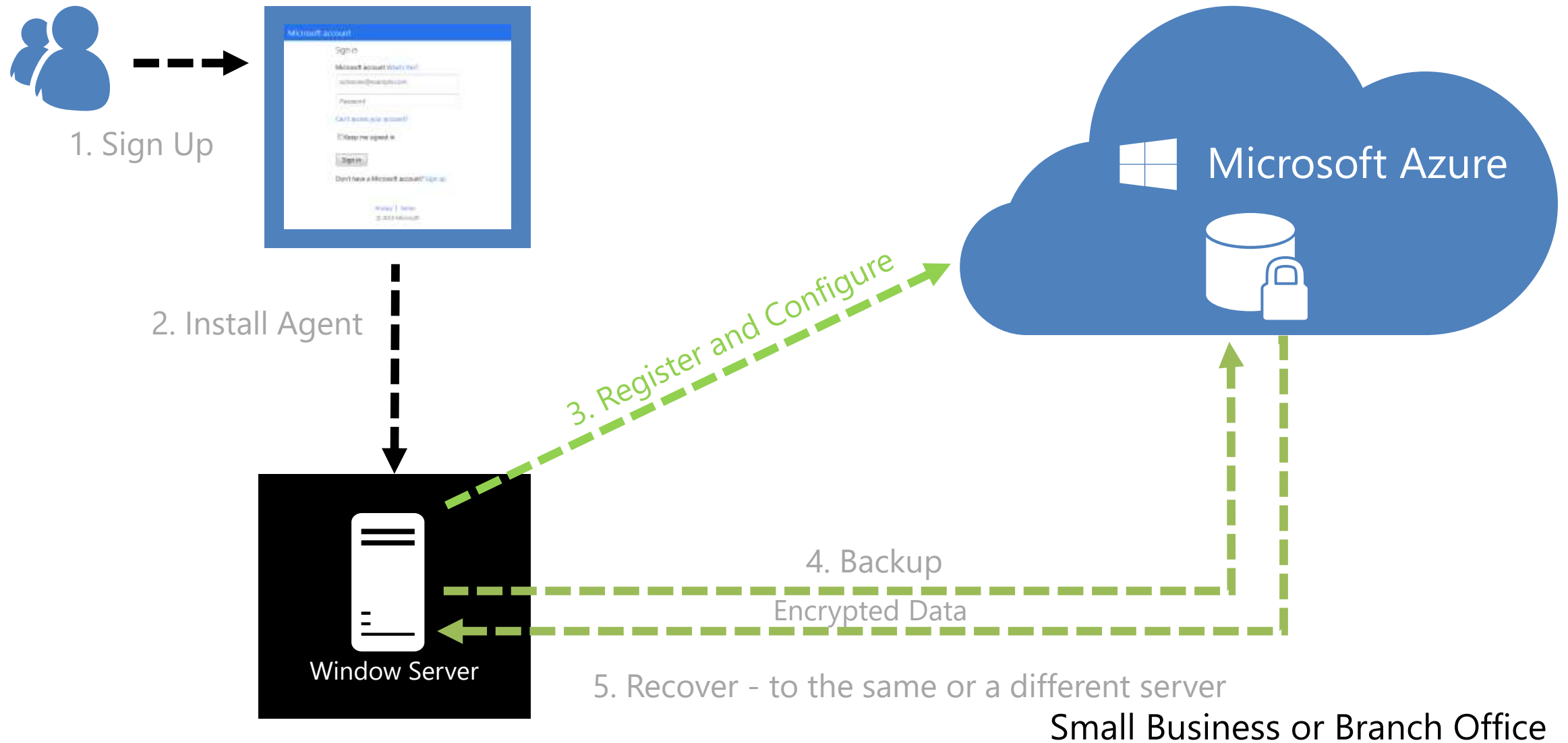
- **Multiple storage options**

- 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

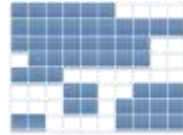
# How Microsoft Azure Backup Works



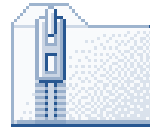
# Azure Backup Network Efficiency

## Customer Premises

1. Identify  
changed blocks



2. Compress



3. Send  
to Azure



Efficient change tracking

Transfer only changed content

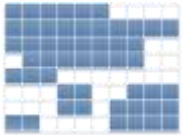
Compression for low bandwidth consumption  
Observed 50-70%



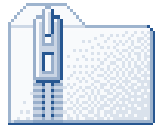
# Azure Backup Security

## Customer Premises

1. Identify  
changed blocks



2. Compress



3. Encrypt



## Azure Backup



4. Encrypted data in recovery  
vault

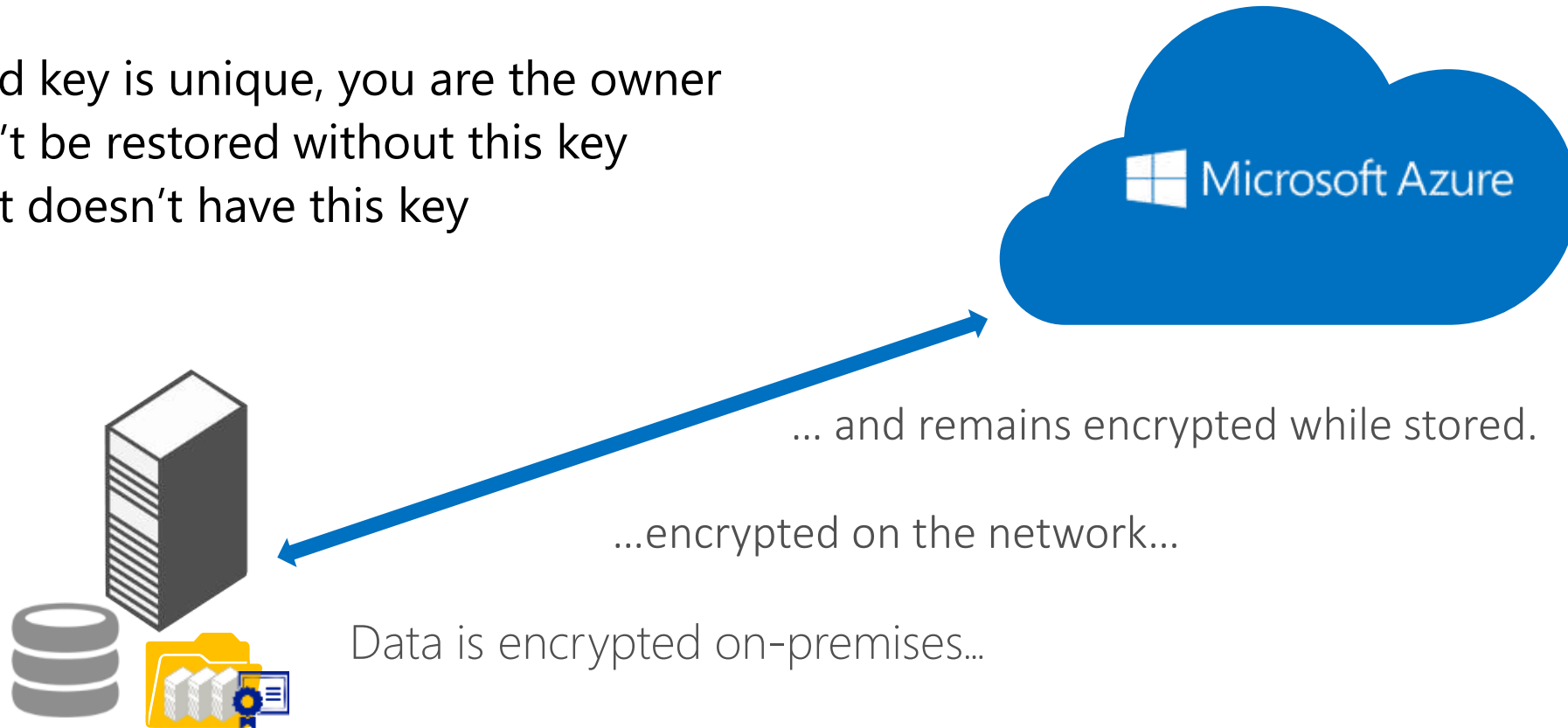
256-bit encryption

In transit and at rest

Admin owns and  
manages keys

# Security

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



# 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.

# 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 v2

### Specialized workloads:

- Exchange2010 and later
- SharePoint 2010 and later
- SQL Server 2008 and later

Exchange

SharePoint

Microsoft SQL Server

Microsoft Hyper-V

vmware

### Virtual machines

(on Azure, Hyper-V, VMware):  
Windows\* & Linux

Physical servers: Windows\* & Linux

\* Windows Server 2008 SP2 and later, on Azure Windows Server 2008 R2 SP1 and later

## File/Folder backup to Azure

Windows Server: Windows Server 2008 SP2 and later

Windows Clients: Windows 7, 8, 8.1, 10

System Center Data  
Protection Manager  
or  
Azure Backup  
Server

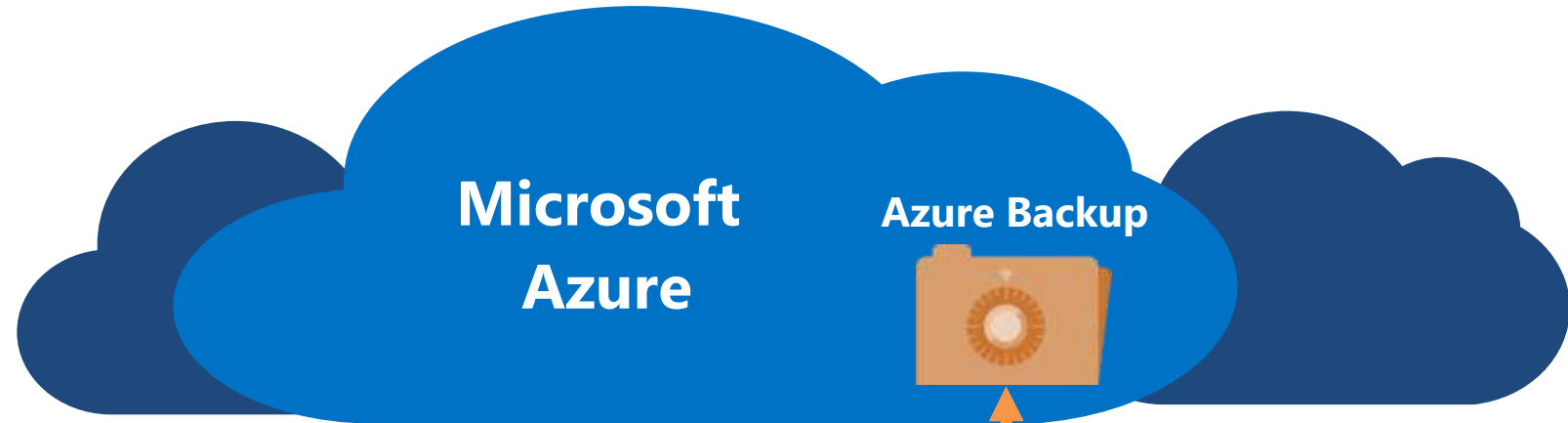
Microsoft  
Azure

Azure Backup  
Agent

On-premises – built and managed infrastructure

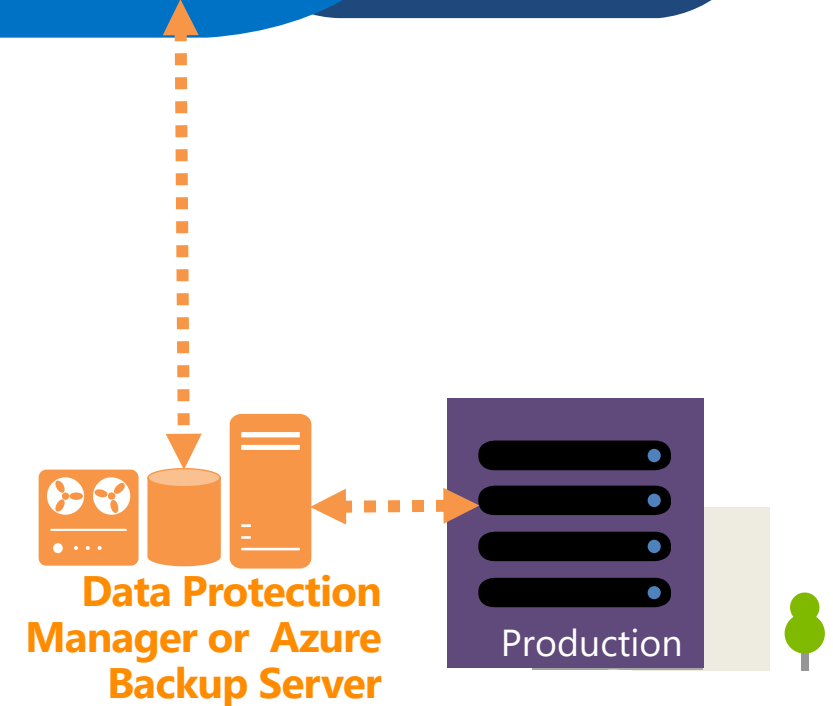
Cloud – flexible, and remote infrastructure

# Enterprise and Branch Office Backup

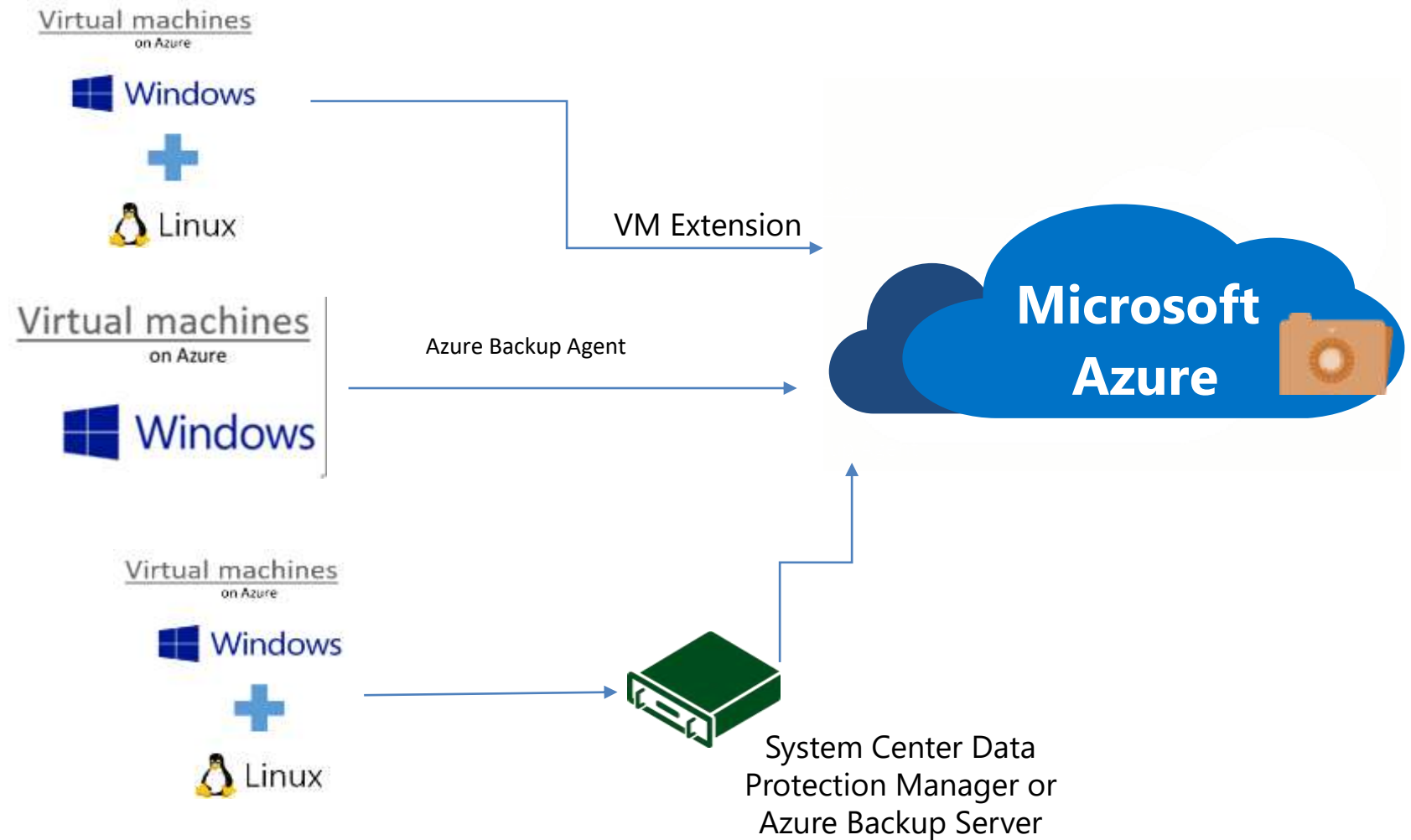


## Solutions:

- 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?
<b>Azure Backup (MARS) agent (can be deployed to VMs on Azure and on-premises)</b>	<ul style="list-style-type: none"><li>· Back up files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)</li><li>· No separate backup server required.</li></ul>	<ul style="list-style-type: none"><li>· Backup 3x per day</li><li>· Not application aware; file, folder, and volume-level restore only,</li><li>· No support for Linux.</li></ul>	<ul style="list-style-type: none"><li>· Files,</li><li>· Folders</li><li>· System State</li></ul>	Recovery Services vault
<b>System Center DPM (can be deployed in Azure and on-premises)</b>	<ul style="list-style-type: none"><li>· Application-aware snapshots (VSS)</li><li>· Full flexibility for when to take backups</li><li>· Recovery granularity (all)</li><li>· Can use Recovery Services vault</li><li>· Linux support on Hyper-V and VMware VMs</li><li>· Back up and restore VMware VMs using DPM 2012 R2</li></ul>	Cannot back up Oracle workload.	<ul style="list-style-type: none"><li>· Files,</li><li>· Folders,</li><li>· Volumes,</li><li>· VMs,</li><li>· Applications,</li><li>· Workloads</li><li>· System State</li></ul>	<ul style="list-style-type: none"><li>· Recovery Services vault,</li><li>· Locally attached disk,</li><li>· Tape (on-premises only)</li></ul>



# Azure Backup Components (continued)

Component	Benefits	Limits	What is protected?	Where are backups stored?
<b>Azure Backup Server</b> (can be deployed in Azure and on-premises)	<ul style="list-style-type: none"><li>• App aware snapshots (VSS)</li><li>• Full flexibility for when to take backups</li><li>• Recovery granularity (all)</li><li>• Can use Recovery Services vault</li><li>• Linux support on Hyper-V and VMware VMs</li><li>• Back up and restore VMware VMs</li><li>• Does not require a System Center license</li></ul>	<ul style="list-style-type: none"><li>• Cannot back up Oracle workload.</li><li>• Always requires live Azure subscription</li><li>• No support for tape backup</li></ul>	<ul style="list-style-type: none"><li>• Files,</li><li>• Folders,</li><li>• Volumes,</li><li>• VMs,</li><li>• Applications,</li><li>• Workloads,</li><li>• System State</li></ul>	<ul style="list-style-type: none"><li>• Recovery Services vault,</li><li>• Locally attached disk</li></ul>
<b>Azure IaaS VM Backup</b>	<ul style="list-style-type: none"><li>• Native backups for Windows/Linux</li><li>• No specific agent installation required</li><li>• Fabric-level backup with no backup infrastructure needed</li></ul>	<ul style="list-style-type: none"><li>• Back up VMs once-a-day</li><li>• Restore VMs only at disk level</li><li>• Cannot back up on-premises</li></ul>	<ul style="list-style-type: none"><li>• VMs,</li><li>• All disks (using PowerShell)</li></ul>	Recovery Services vault

# Which applications and workloads can be backed up?

Workload	Source machine	Azure Backup solution
Files and folders	Windows Server Windows Client	<a href="#">Azure Backup agent</a> , <a href="#">System Center DPM</a> (+ the Azure Backup agent), <a href="#">Azure Backup Server</a> (includes the Azure Backup agent)
Hyper-V virtual machine Windows & Linux	Windows Server	<a href="#">System Center DPM</a> (+ the Azure Backup agent), <a href="#">Azure Backup Server</a> (includes the Azure Backup agent)
VMware virtual machine	-	<a href="#">System Center DPM</a> (+ the Azure Backup agent), <a href="#">Azure Backup Server</a> (includes the Azure Backup agent)
Microsoft SQL Server	Windows Server	<a href="#">System Center DPM</a> (+ the Azure Backup agent), <a href="#">Azure Backup Server</a> (includes the Azure Backup agent)
Microsoft SharePoint	Windows Server	<a href="#">System Center DPM</a> (+ the Azure Backup agent), <a href="#">Azure Backup Server</a> (includes the Azure Backup agent)
Microsoft Exchange	Windows Server	<a href="#">System Center DPM</a> (+ the Azure Backup agent), <a href="#">Azure Backup Server</a> (includes the Azure Backup agent)
Azure IaaS VMs (Windows)	running in Azure	<a href="#">Azure Backup (VM extension)</a>
Azure IaaS VMs (Linux)	running in Azure	<a href="#">Azure Backup (VM extension)</a>

# 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

# 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

# Module 1: Microsoft Azure Backup

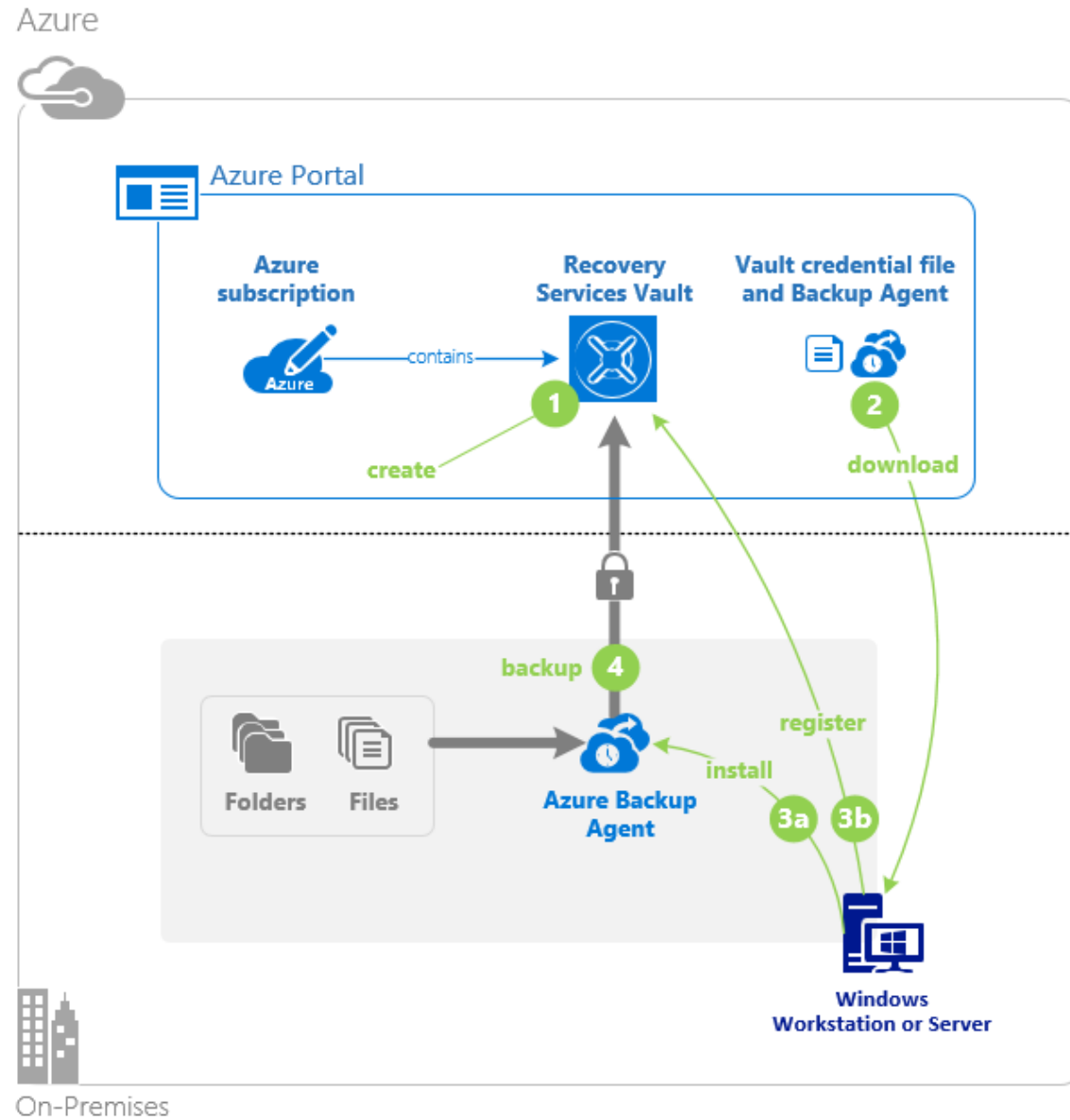
## Section 3: Preparing for Azure Backup

# 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

.

# Description (continued)



# Getting Started with Azure Backup

## On Azure

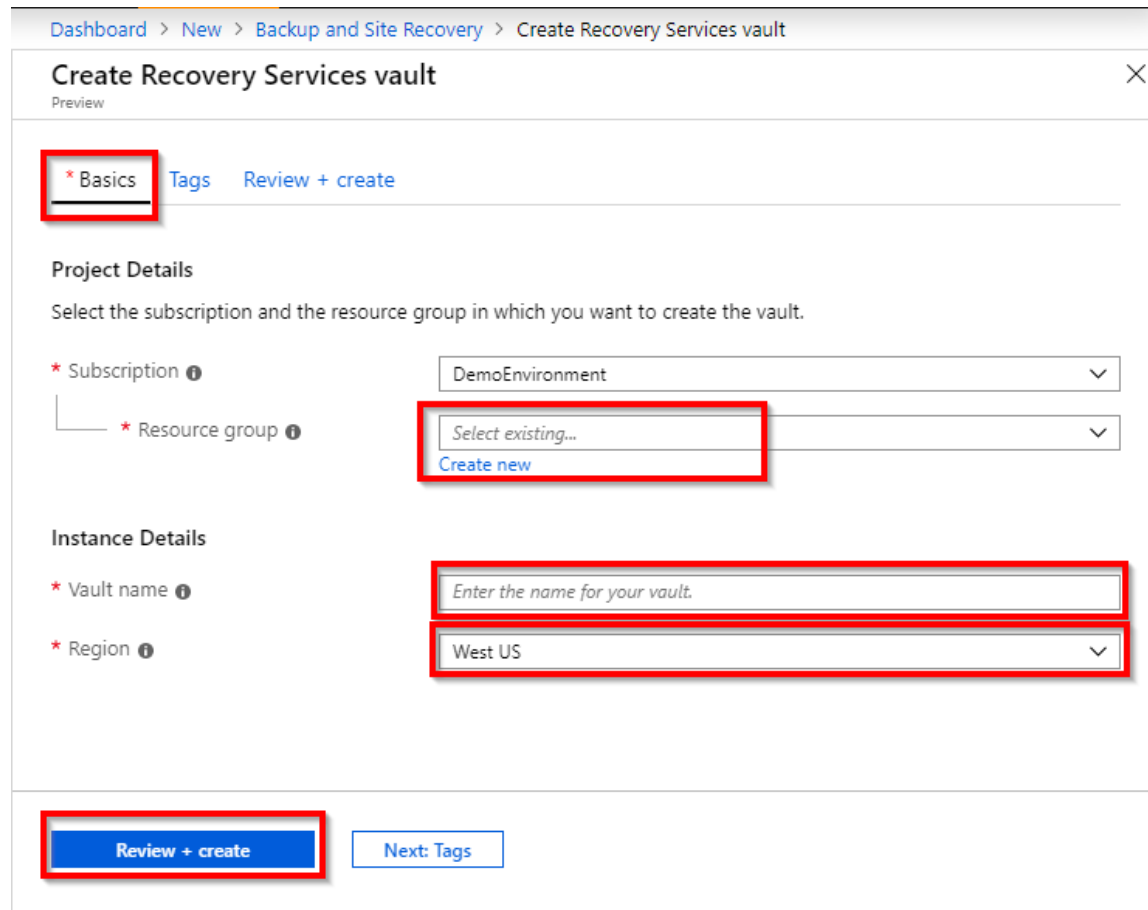
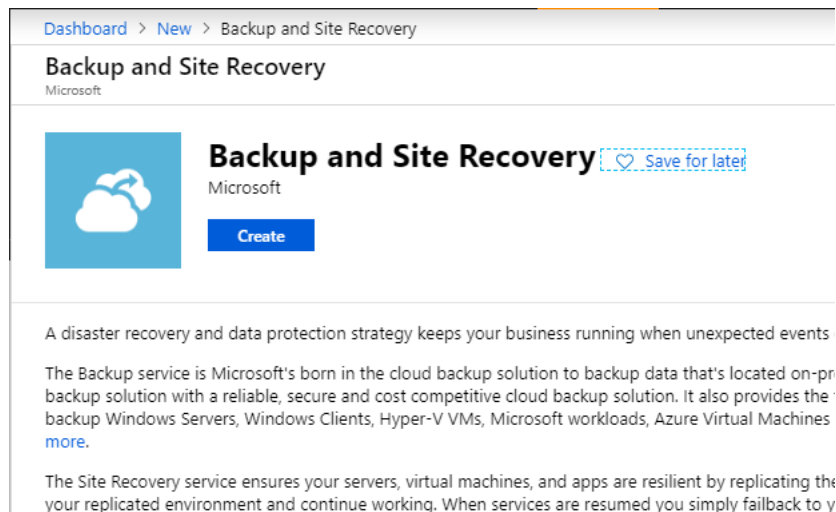
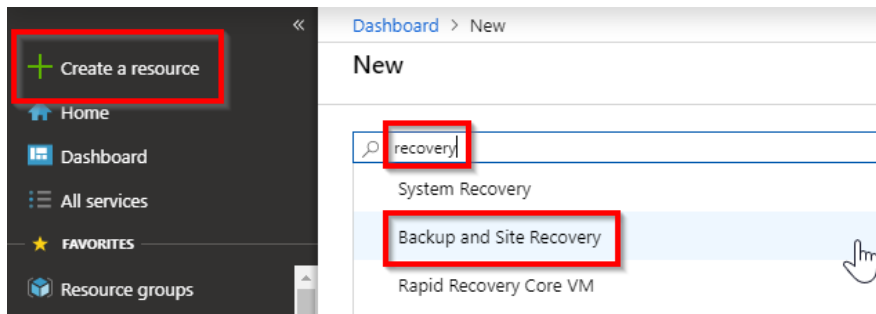
- To back up Virtual Machines hosted in Azure, you must first:
  - Create a Recovery Services vault
    - You must create a backup vault in the geographic region where you want to store the data
  - Define a backup Goal, Backup policy and select the VMs

## 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



# Creating a Vault



# Determine storage redundancy

Dashboard > Microsoft.RecoveryServicesV2 - Overview > Demo - Properties

### Demo - Properties

Recovery Services vault

Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings**
  - Properties**
  - Locks
  - Export template
- Getting started
  - Backup
  - Site Recovery
- Protected items
  - Backup items
  - Replicated items
- Manage
  - Backup policies

Status: Active

Location: West US

Subscription Name: DemoEnvironment

Subscription Id: 4ba1f230-3c4c-4c62-a732-c412cd86d55f

Resource group: DemoTestRG

Diagnostics Settings: [Update](#)

BACKUP

Backup Configuration: [Update](#)

Security Settings

### Backup Configuration

Demo

Save Discard Refresh

Storage replication type: [Locally-redundant](#) **[Geo-redundant](#)**

# Storage redundancy

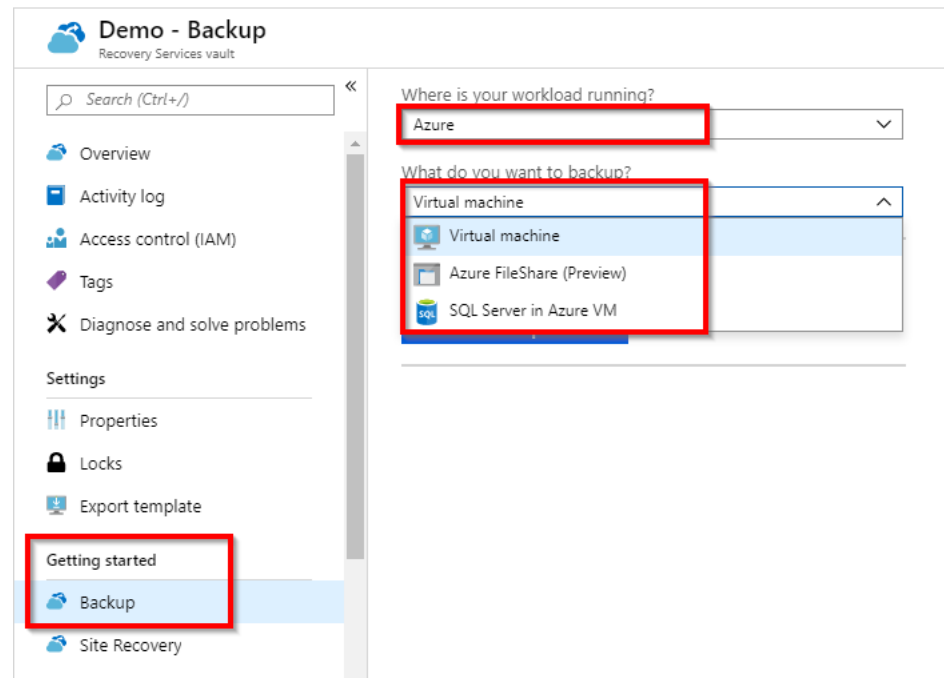
- Storage data in a vault are always redundant
- The best time to identify your storage redundancy option is right after vault creation and before any machines are registered to the vault. Once an item has been registered to the vault, the storage redundancy option is locked and cannot be modified.
- 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)

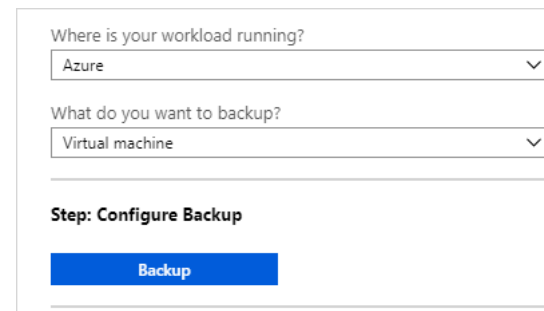
- If you are using Azure as a primary backup storage endpoint (for example, you are backing up to Azure from a Windows Server), you should consider picking (the default) geo-redundant storage option.
- If you are using Azure as a tertiary backup storage endpoint (for example, you are using SCDPM to have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

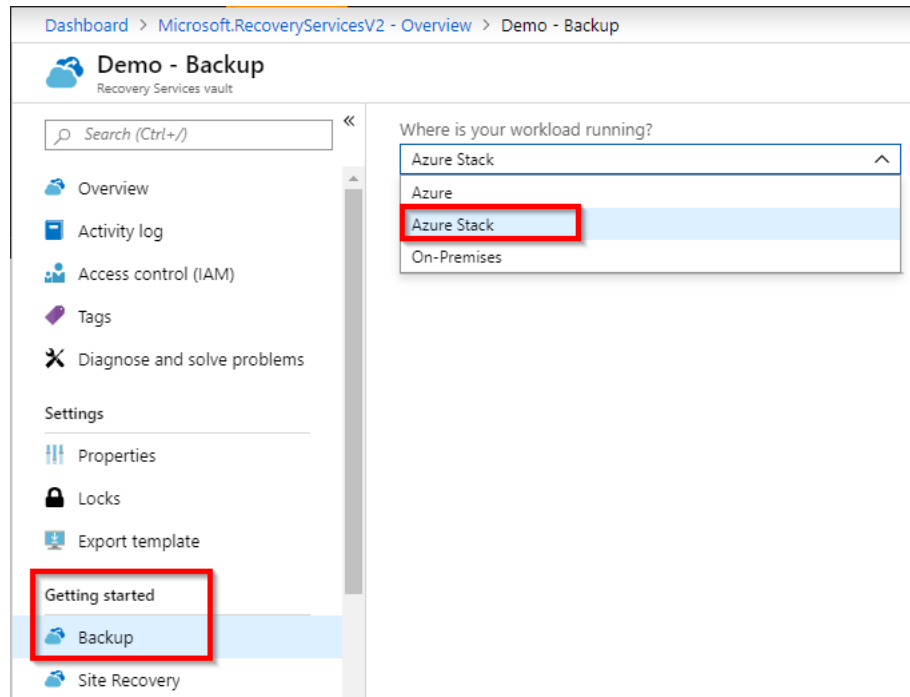


Under **Backup Goal**  
Select **Azure** from the Where  
is your workload running?  
menu.  
Select the item you want from  
the *What do you want to  
backup?* Menu  
Click the blue **Backup** button

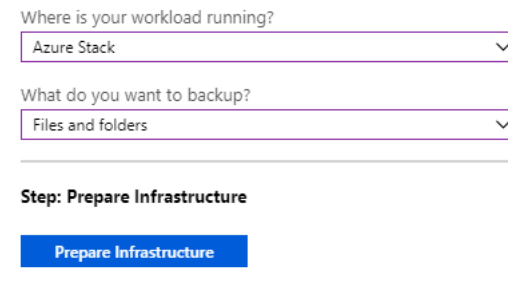


# Configuring Backup (Azure Stack Workloads)

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

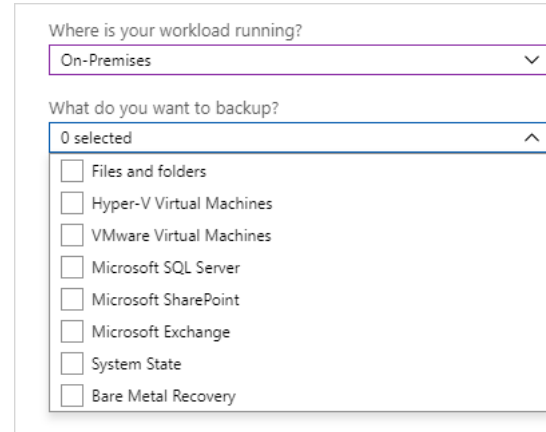
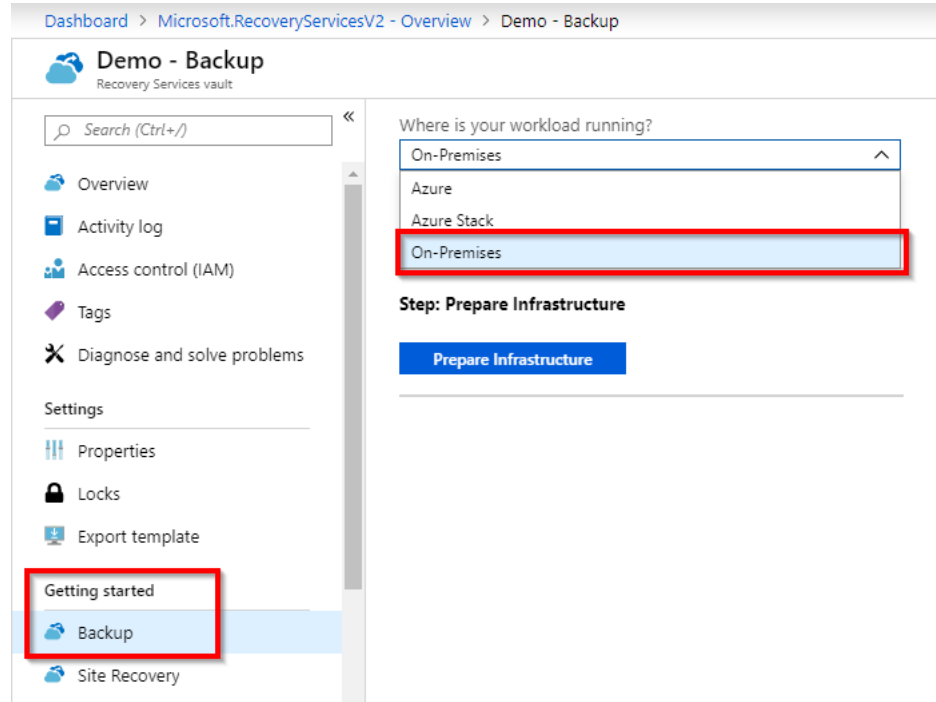


Under **Backup Goal**  
Select **Azure Stack** from the  
Where is your workload  
running? menu.  
Select the item you want from  
the *What do you want to  
backup?* Menu  
Click the blue **Prepare  
Infrastructure** button



# Configuring Backup (On-premises Workloads)

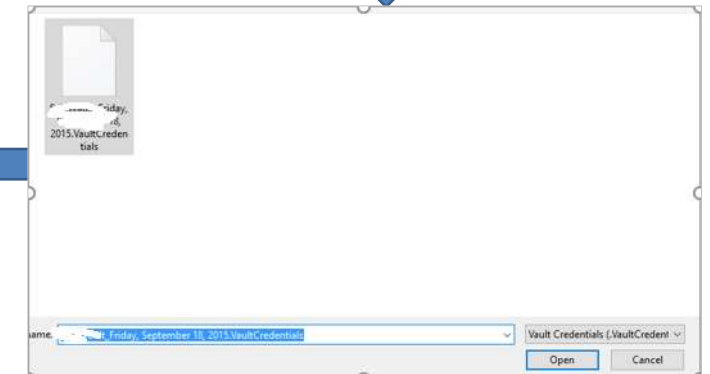
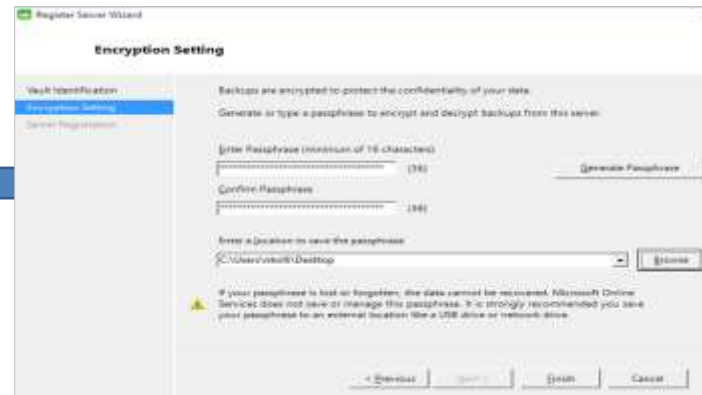
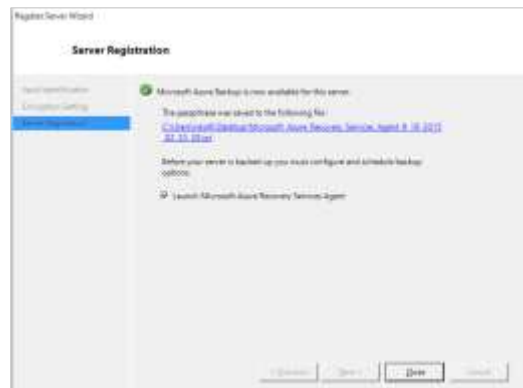
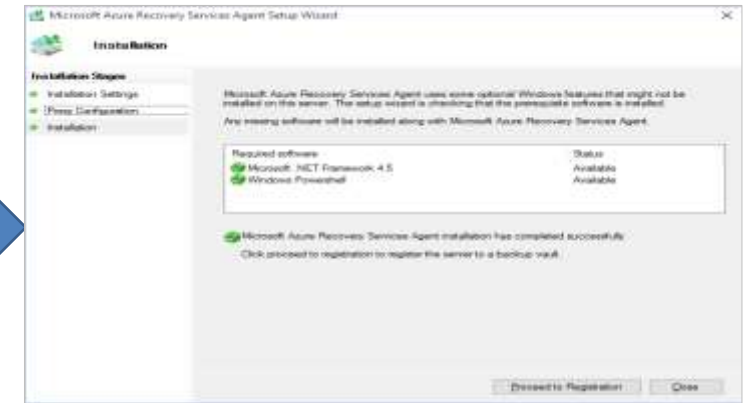
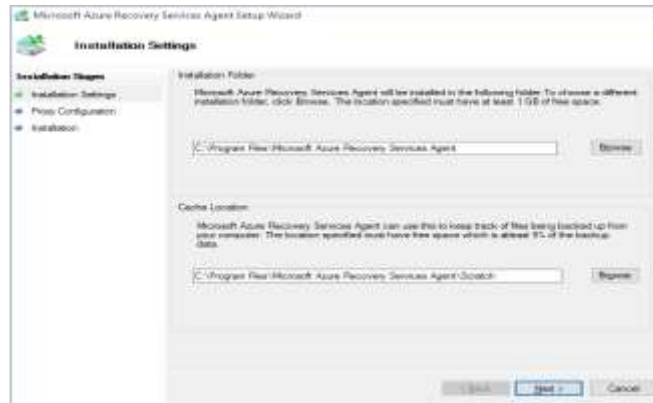
Click **Getting Started > Backup** on the Settings blade.



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

# Register Your Server to Azure Backup Service

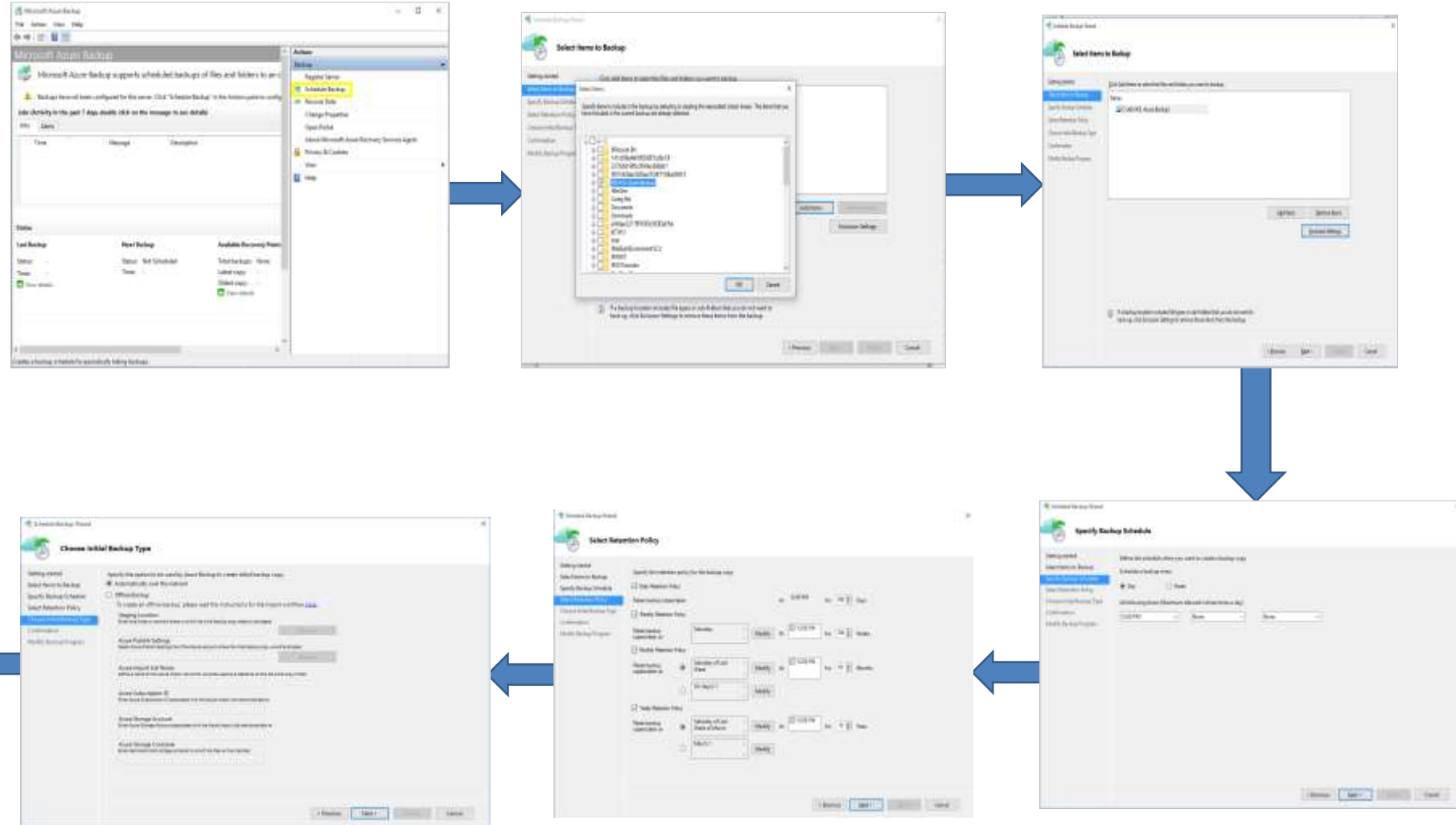
1. Install Azure Backup Agent - MARSAgentInstaller.exe
2. Register the server
3. Create the PassPhrase Key
4. Complete the registration





# 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

- **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

# 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

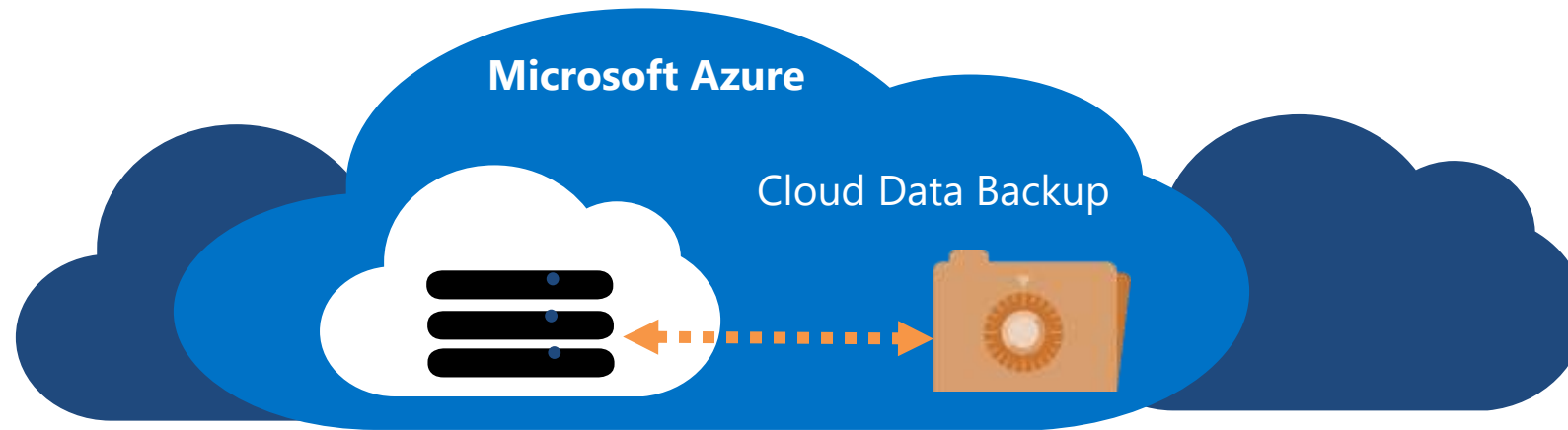
## Configurations

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

## Management

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

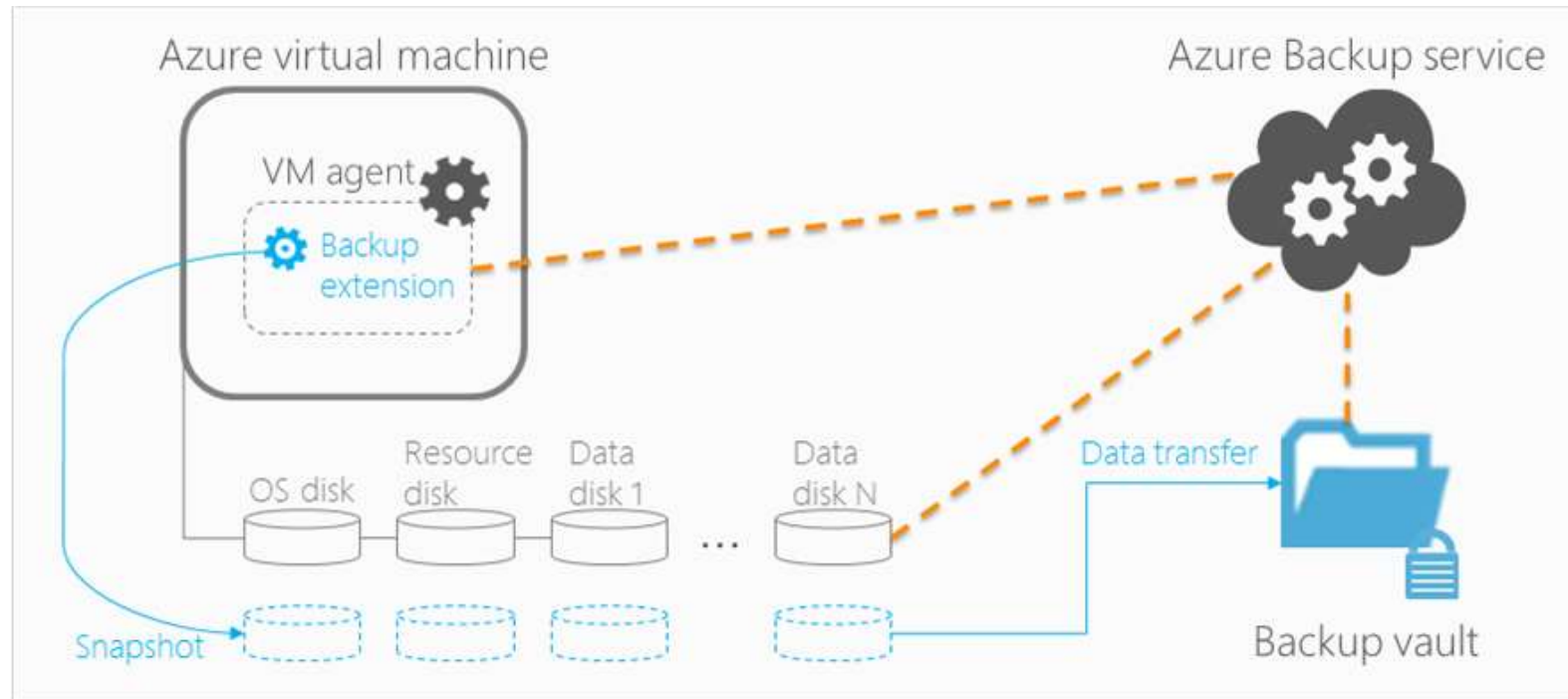
# Overview



## Enterprise ready solution

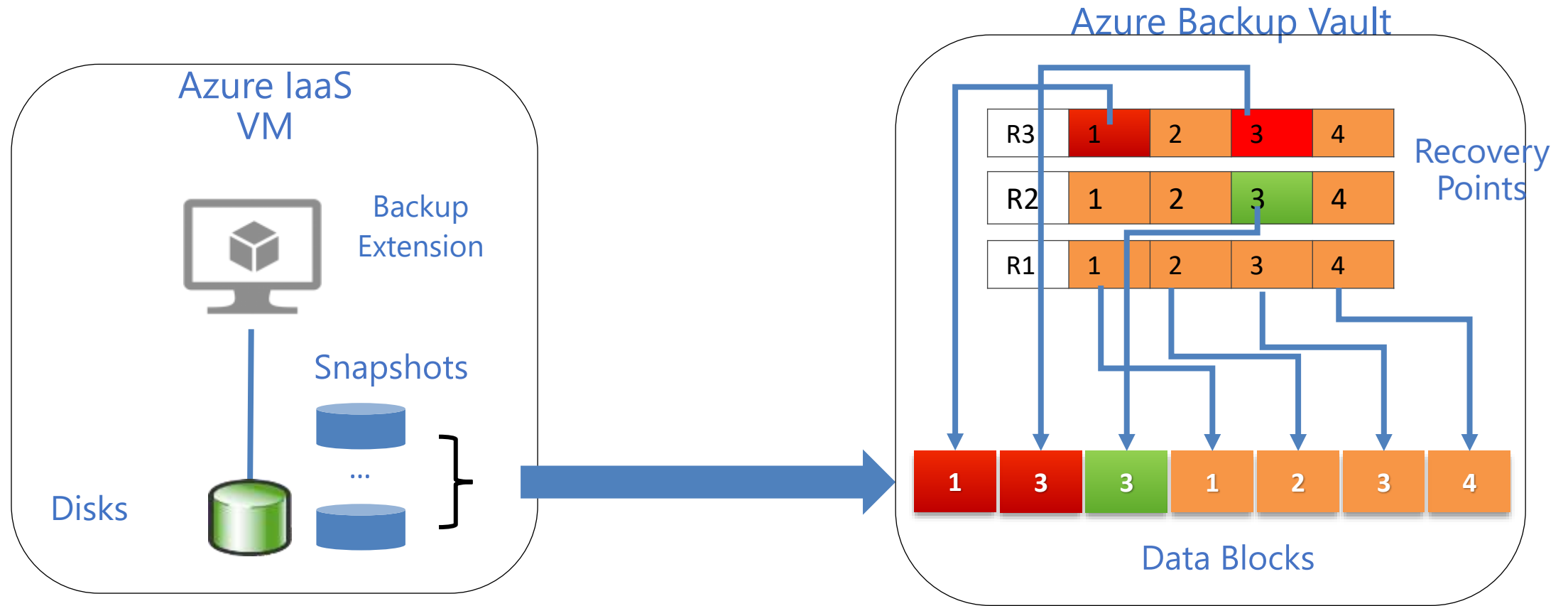
- Application consistent backup for Windows and for Linux workloads
- Fabric level protection for Azure IaaS VMs
- Azure Backup transfers snapshots taken on a VM to a secure, reliable Azure Backup vault and can restore the VM in a single click.
- Long-term protection using industry standard GFS based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

## How It Works ? (continued)



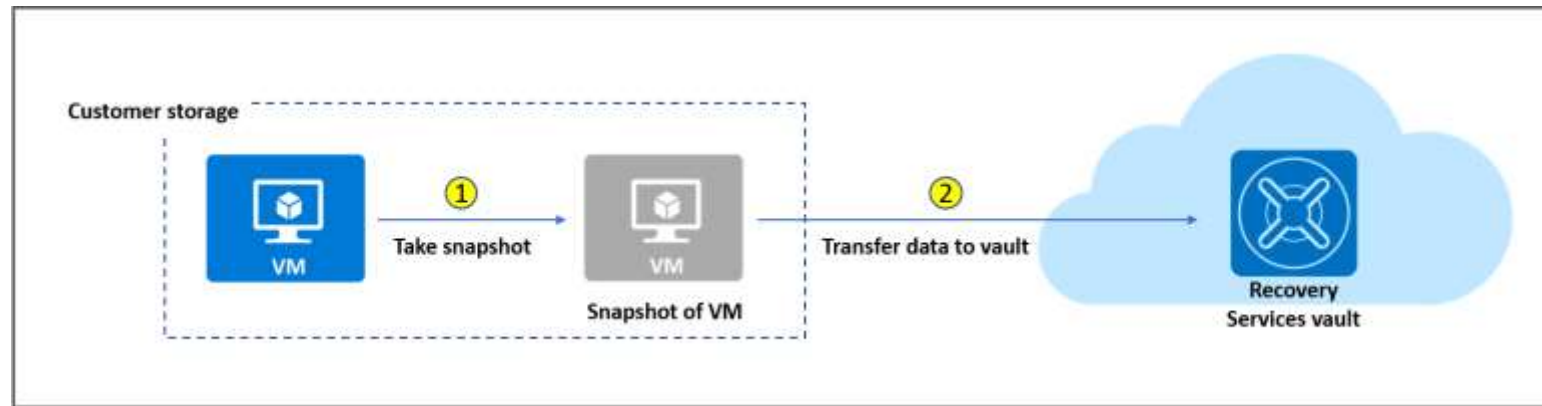


# How It Works? (continued)



# 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

- 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

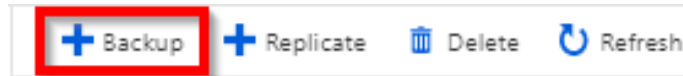
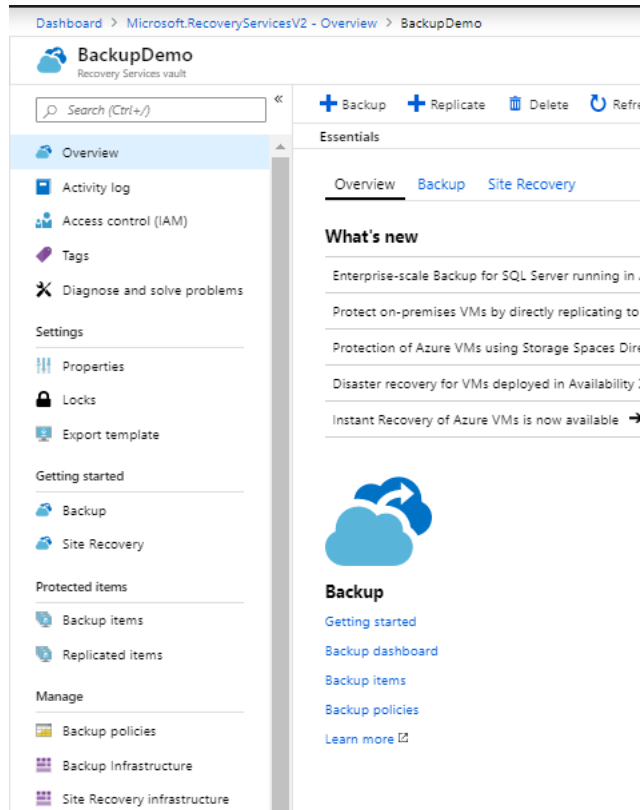
- That the VM boots up
- There is no corruption
- There is no data loss

## 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
- 

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

# Discover your IaaS VMs



**Backup Goal**

Where is your workload running?

What do you want to backup?

**Step: Configure Backup**

## Tip :

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

# Define a backup policy

Backup

×

1 Backup policy  
Select

2 Items to backup  
Select

Choose backup policy ⓘ  
DefaultPolicy ▼

**BACKUP FREQUENCY**  
Daily at 3:00 AM UTC

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

**RETENTION RANGE**  
**Retention of daily backup point**  
Retain backup taken every day at 3:00 AM for 30 Day(s)

## 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 a custom backup policy

Backup policy

Choose backup policy ⓘ

Create New

\* Policy name ⓘ



The changes will apply to all the existing and new recovery points. Existing recovery points will be affected and now retained as per the modified retention range.

Backup schedule

\* Frequency

Daily

\* Time

12:30 AM

\* Timezone

(UTC) Coordinated Universal Time

Instant Restore ⓘ

Retain instant recovery snapshot(s) for

2

Day(s) ⓘ

Retention range

☒ Retention of daily backup point.

\* At

12:30 AM

For

180

Day(s)

☐ Retention of weekly backup point.

Not Configured

☐ Retention of monthly backup point.

Not Configured

☐ Retention of yearly backup point.

Not Configured

# Define items to backup

Backup

×

1 Backup policy  
DefaultPolicy ✓

2 Items to backup  
Select >

Enable backup

Select virtual machines

✓ Virtual machines in the same region as vault and not protected by another vault are shown. Click to learn more on best practices to configure backup.

Filter items ...

	VIRTUAL MACHINE NAME	RESOURCE GROUP
<input type="checkbox"/>	ad-bdc	testlabRG
<input type="checkbox"/>	ad-pdc	testlabRG
<input checked="" type="checkbox"/>	sps-app-0	testlabRG
<input checked="" type="checkbox"/>	sps-app-1	testlabRG
<input checked="" type="checkbox"/>	sps-web-0	testlabRG
<input checked="" type="checkbox"/>	sps-web-1	testlabRG
<input type="checkbox"/>	sql-0	testlabRG
<input type="checkbox"/>	sql-1	testlabRG

Selected virtual machines  
4

OK

Backup

□ ×

1 Backup policy  
DefaultPolicy ✓

2 Items to backup  
Items selected : 4 ✓

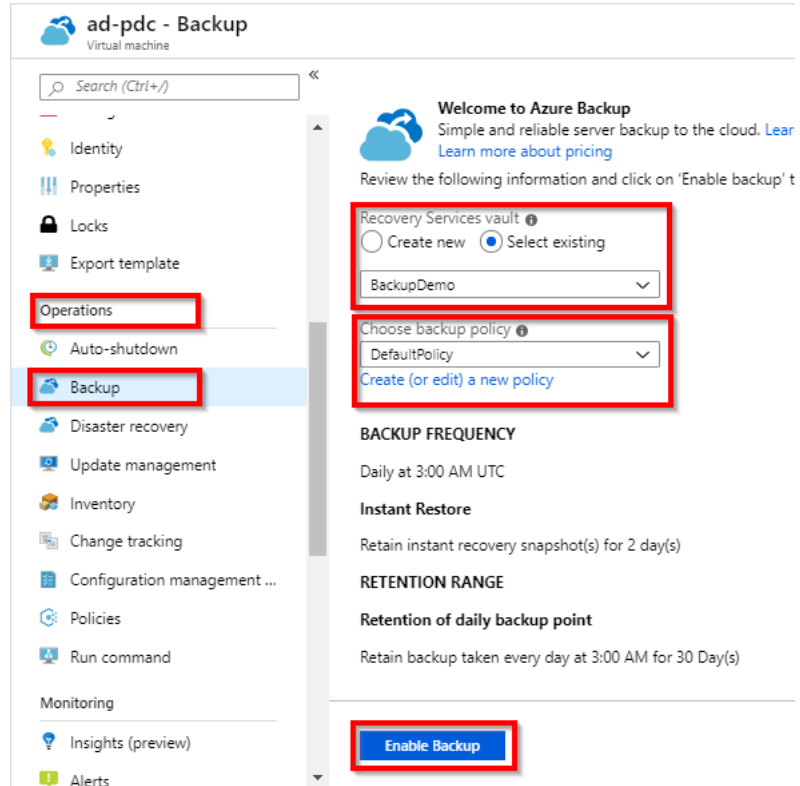
Enable backup

## 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

- Initiate Backup from the VM





# Protect your IaaS VMs

- The BEST way

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

**Azure Security Center**  
Azure Security Center provides unified security management and advanced threat protection actions. [Learn more](#)

✔ Your subscription is protected by Azure Security Center standard plan.

**Monitoring**

Boot diagnostics ☒ On ☐ Off

OS guest diagnostics ☐ On ☒ Off

\* Diagnostics storage account   
[Create new](#)

**Identity**

System assigned managed identity ☐ On ☒ Off

**Azure Active Directory**

Login with AAD credentials (Preview) ☐ On ☒ Off

**Auto-shutdown**

Enable auto-shutdown ☐ On ☒ Off

**Backup**

Enable backup ☐ On ☒ Off

[Review + create](#) [< Previous](#) [Next : Advanced >](#)

## Backup

Enable backup ⓘ

☒ On ☐ Off

\* Recovery Services vault ⓘ

☒ Create new ☐ Use existing

✔

\* Resource group

▼

[Create new](#)

\* Backup policy

▼

[Create new](#)

```

{
  "apiVersion": "2017-05-10",
  "name": "BackupVaultAndOrPolicy-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'))]"
          ]
        }
      ]
    }
  }
}

```

# Protect your IaaS VMs

+ Backup

+ Replicate

🗑 Delete

🔄 Refresh

📘

Enterprise-scale Backup for SQL Server running in Azure VM is Generally Available. [Learn more.](#)

Essentials

OverviewBackupSite Recovery

Monitoring

Backup Alerts (last 24 hours)

Critical	0
Warning	0

Backup Pre-Check Status (Azure VMs)

0

Critical0

Warning0

Backup Jobs

In progress	0
Failed	0

Usage

Backup items

7

Backup Storage


Cloud - LRS	0 B
Cloud - GRS	1,243 ...







🔄 Refresh

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	6
Azure Backup Agent	1
SQL in Azure VM	0
Azure Storage (Azure Files)	0
DPM	0
Azure Backup Server	0

Microsoft Confidential

# Restore your data

 **TestServer1**  
Backup Item

 Backup now  **Restore VM**  File Recovery  Stop backup  Resume backup  Delete backup data

**Restore**

1 Restore point  
8/4/2019, 6:05:28 PM

2 Restore configuration  
Configure

**Select restore point**

Filter

Filtered for last 30 days

CRASH CONSISTENT

APPLICATION CONSISTENT

FILE-SYSTEM CONSISTENT

Filter items...

All restore points

TIME	CONSISTENCY	RECOVERY TYPE
8/5/2019, 6:12:22 PM	Crash Consistent	Snapshot and Vault
8/4/2019, 6:05:28 PM	Crash Consistent	Snapshot and Vault
8/3/2019, 6:04:46 PM	Crash Consistent	Vault
8/2/2019, 6:07:18 PM	Crash Consistent	Vault
8/1/2019, 6:09:15 PM	Crash Consistent	Vault


**Restore**


1 Restore point  
8/4/2019, 6:05:28 PM


2 Restore configuration  
Configure


Create new


Replace existing


 To create an alternate configuration when restoring your VM (from the following menus), use PowerShell cmdlets.


Restore Type   
Create virtual machine

\* Virtual machine name 

\* Resource group   
Infrastructure

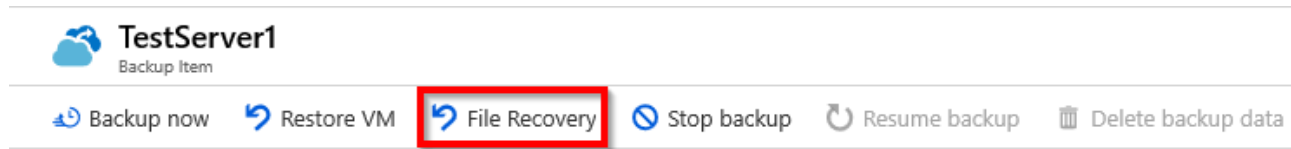
\* Virtual network   
TestNet (Infrastructure)

\* Subnet   
testnet1

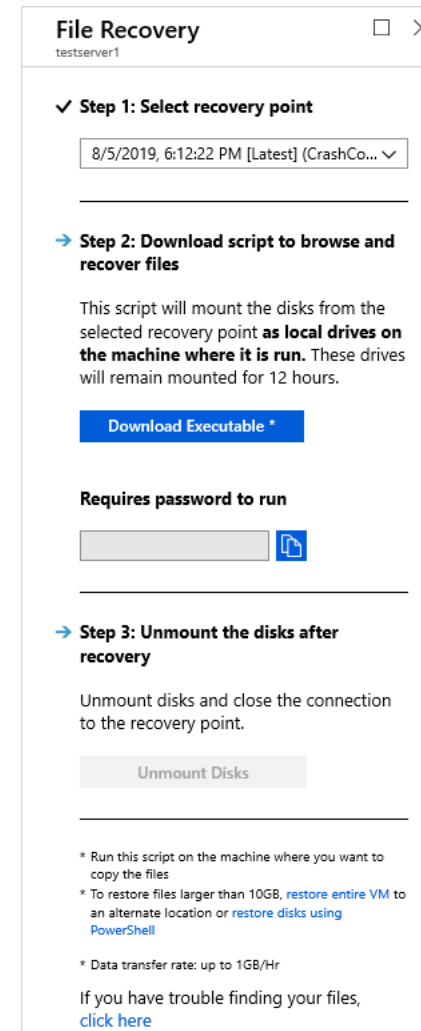
\* Staging Location   
Select an option

Can't find your storage account ?

# Restore your data



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



# 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

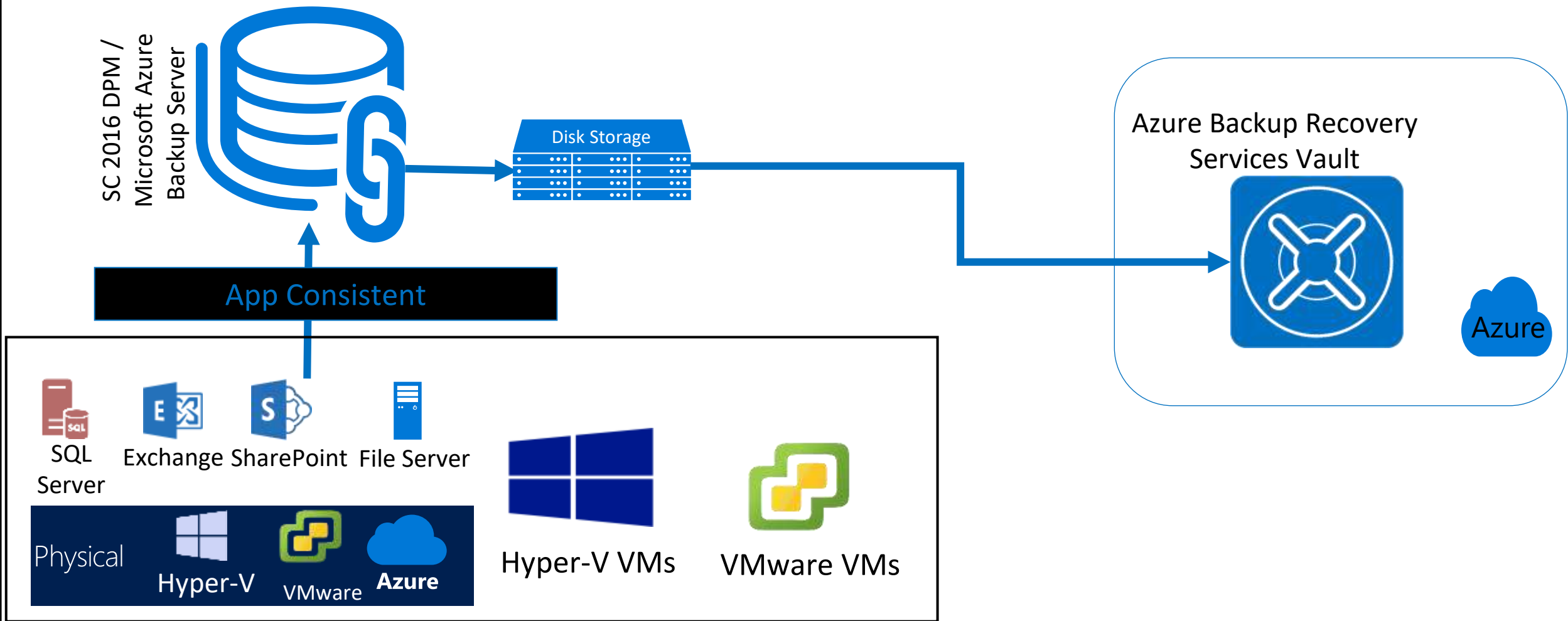
# Demo: Backup Azure VMs with snapshots

# Module 1: Microsoft Azure Backup

## Section 5: Backup Workload with DPM or MABS



# System Center DPM overview



 Private Cloud protection at scale

 Cloud Integrated Backup

 Application Aware Backup

 Central monitoring and Reporting

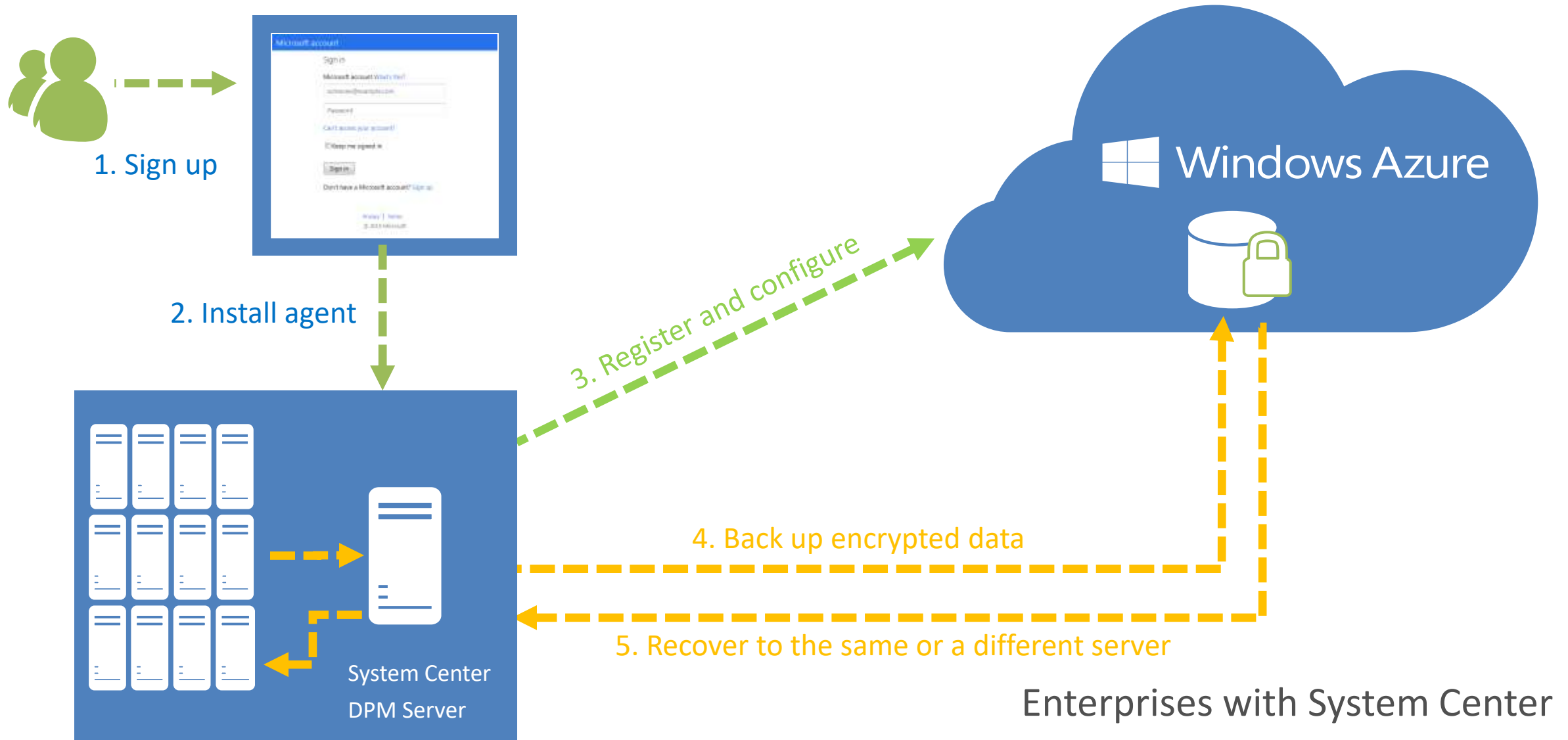
 Automation

# 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.

# How Windows Azure Backup works



# 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.



## 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

## 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:

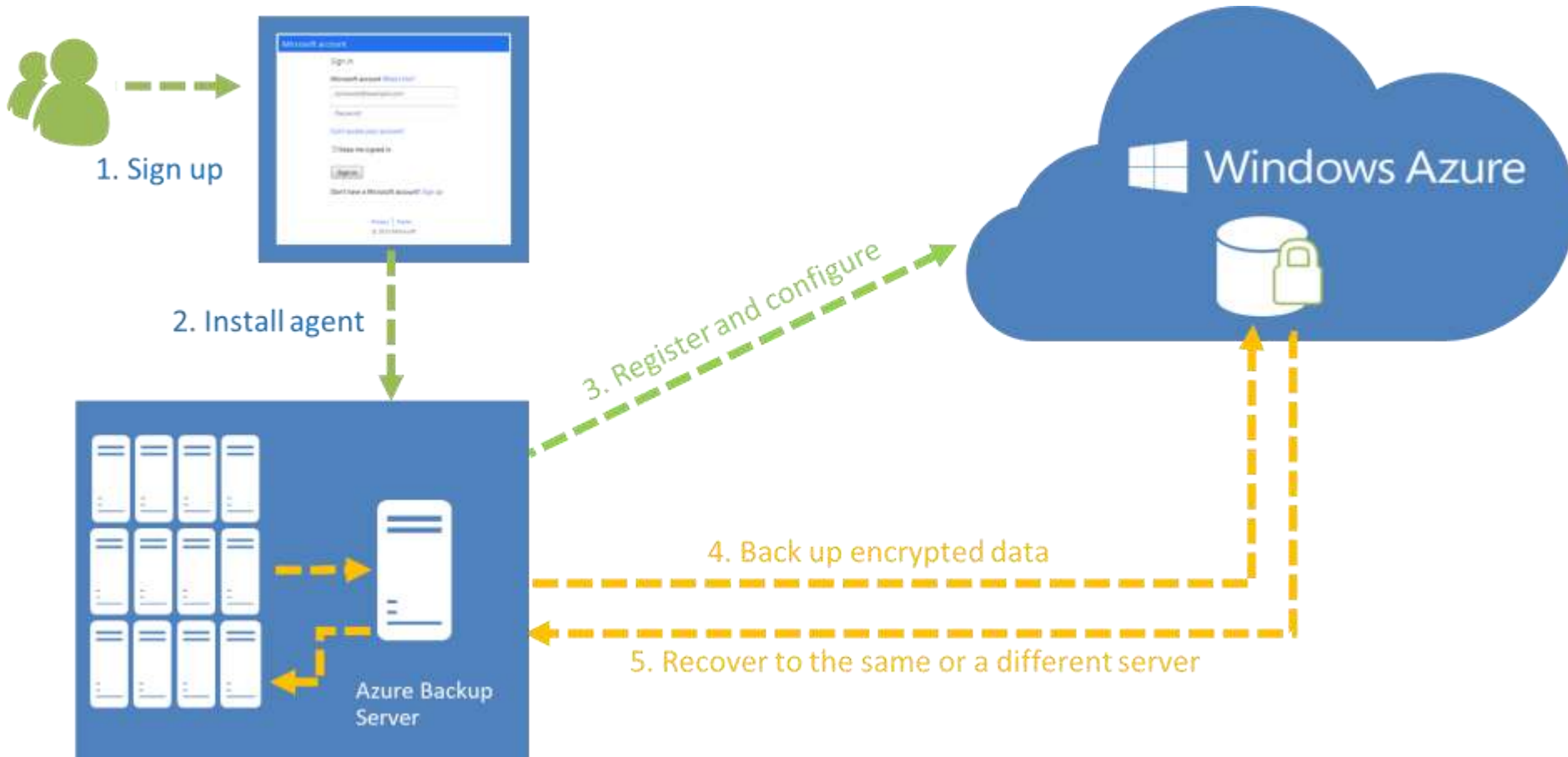
- Encrypted (Full backups only)
- Compressed (Incremental backups supported)
- Sparse (Incremental backups supported)
- Compressed and sparse (Treated as Sparse)

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.

- 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

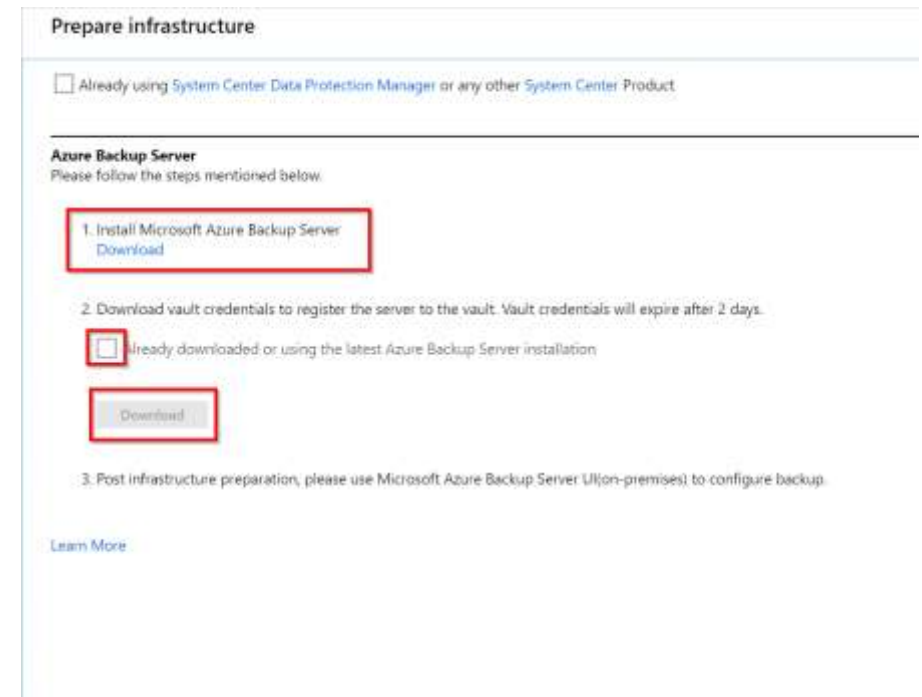
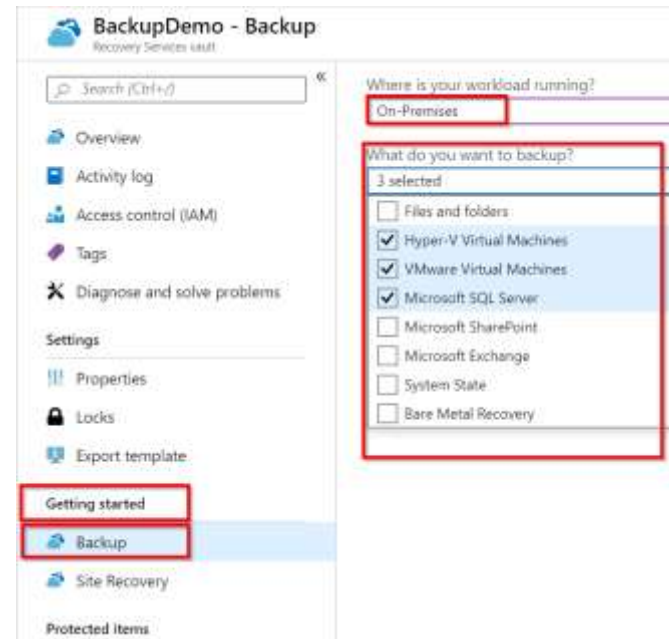
Scenario	DPM/MABS
MABS on an Azure VM	<p>Windows Server 2012 R2, 2106 and 2019 Datacenter edition</p> <p>We recommend that you start with an image from the marketplace. Minimum A2 Standard with two cores and 3.5 GB of RAM.</p>
DPM on an Azure VM	<p>System Center 2012 R2 with Update 3 or later. Windows operating system as <a href="#">required by System Center</a>.</p> <p>We recommend that you start with an image from the marketplace. Minimum A2 Standard with two cores and 3.5 GB of RAM.</p>
MABS on-premises	<p>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</p>
DPM on-premises	<p>Physical server/Hyper-V VM: System Center 2012 SP1 or later. VMware VM: System Center 2012 R2 with Update 5 or later.</p>

# 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.

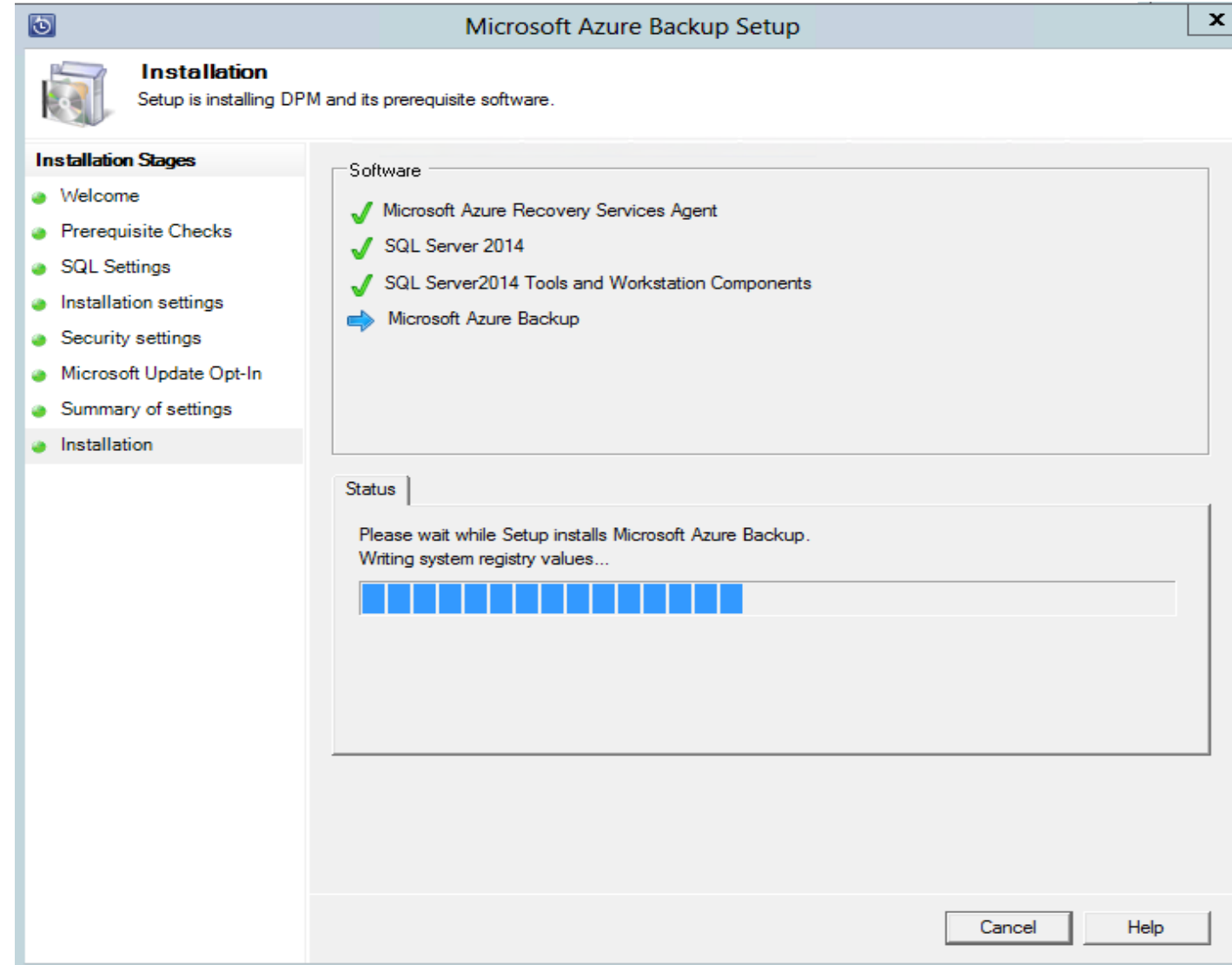
# MABS – Deployment

- 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

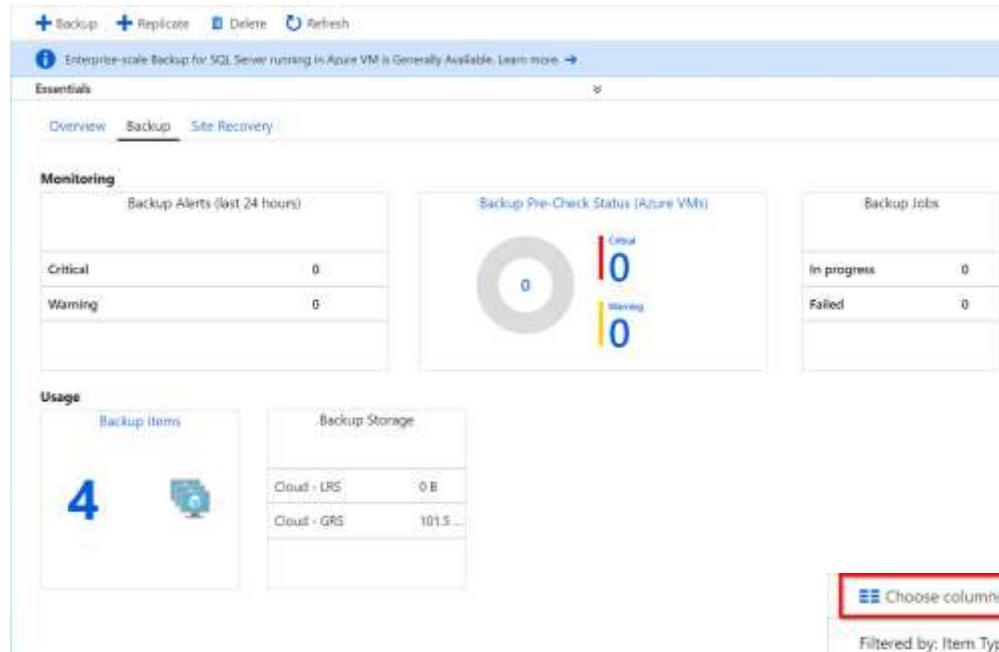
# Which tools to monitor backup ?

- 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

# Demo: Overview of the monitoring solutions



# Monitor



## Monitoring

- Alerts
- Diagnostic settings
- Backup Jobs
- Site Recovery jobs
- Backup Alerts
- Site Recovery events

## 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

Choose columns Filter Export jobs Refresh


Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 8/11/2019, 7:14:21 PM, End Time - 8/12/2019, 7:14:21 PM

Completed fetching data from the service.

Filter items...

WORKLOAD NAME	OPERATION	STATUS	TYPE	START TIME	DURATION
sps-web-1	Backup	Completed	Azure virtual machine	8/11/2019, 10:13:02 PM	01:11:18
sps-app-0	Backup	Completed	Azure virtual machine	8/11/2019, 10:08:45 PM	00:51:15
sps-web-0	Backup	Completed	Azure virtual machine	8/11/2019, 10:06:17 PM	00:51:18
sps-app-1	Backup	Completed	Azure virtual machine	8/11/2019, 10:05:04 PM	00:51:14

# Monitor

 **BackupDemo - Activity log**  
Recovery Services vault

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Properties

Locks

Export template

Edit columns Refresh Export to Event Hub Download as CSV Logs Pin current filters Reset filters						
Search Quick Insights						
Management Group : None Subscription : ASD-Azure-IPDev Timespan : Last week Event severity : All Resource group : RecoveryVault						
Resource : BackupDemo Add Filter						
26 items.						
OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY	
Backup Protected Item	Succeeded	20 h ago	Sun Aug 11 ...	ASD-Azure-IPDev	Microsoft.RecoveryServices	
Backup Protected Item	Succeeded	20 h ago	Sun Aug 11 ...	ASD-Azure-IPDev	Microsoft.RecoveryServices	
Backup Protected Item	Succeeded	20 h ago	Sun Aug 11 ...	ASD-Azure-IPDev	Microsoft.RecoveryServices	
Backup Protected Item	Succeeded	20 h ago	Sun Aug 11 ...	ASD-Azure-IPDev	Microsoft.RecoveryServices	
Backup Protected Item	Succeeded	2 d ago	Sat Aug 10 ...	ASD-Azure-IPDev	Microsoft.RecoveryServices	
Backup Protected Item	Succeeded	2 d ago	Sat Aug 10 ...	ASD-Azure-IPDev	Microsoft.RecoveryServices	

# 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

# Monitor

- Quick Insights
  - 24 synopsis

The screenshot displays the Azure Monitor 'Quick Insights' interface. At the top, there are links for 'Export to Event Hub', 'Download as CSV', and 'Logs'. Below these is a search bar and a 'Quick Insights' button, which is highlighted with a red box. The main area shows a table of activity logs with columns for 'STATUS', 'TIME', and 'TIME STAMP'. The table contains seven rows, all with a 'Succeeded' status. To the right of the table is a sidebar titled 'Quick Insights (last 24 hrs)' which contains five summary cards, each with a count of 0.

	STATUS	TIME	TIME STAMP
	Succeeded	20 h ago	Sun Aug 1
	Succeeded	20 h ago	Sun Aug 1
	Succeeded	20 h ago	Sun Aug 1
	Succeeded	20 h ago	Sun Aug 1
	Succeeded	2 d ago	Sat Aug 1
	Succeeded	2 d ago	Sat Aug 1
	Succeeded	2 d ago	Sat Aug 1

### Quick Insights (last 24 hrs)

- Errors**  
An entry in the activity log where the severity filed is set to "Error". 0
- Failed deployments**  
When you try to deploy one or more Azure resources and the system fails to deploy it. 0
- Alerts fired**  
An Azure alert that was activated by an alert activation event. 0
- Service Health**  
The Azure infrastructure is failing and might be affecting one or more of your subscriptions. 0
- Role assignments**  
Security objects created to grant or limit access to subscription administrators or users. 0

# Alerts

## Monitoring

- Alerts
- Diagnostic settings
- Backup Jobs
- Site Recovery jobs
- Backup Alerts**
- Site Recovery events

## BackupTest - Backup Alerts

Recovery Services vault

Search (Ctrl+V)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
  - Properties

Choose columns Filter **Configure notifications** Refresh

Filtered by: Status - Status - All, Severity - All Severities, Start Time - 1/1/2025, 7:07:45 PM, End Time - 3/31/2025, 7:07:45 PM

Completed fetching data from the service.

Filter items...

ALERT	BACKUP ITEM	PROTECTED SERVER	SEVERITY	DURATION
-------	-------------	------------------	----------	----------

No alerts found for the selected filter values.

### Configure notifications

BackupTest (preview)

Save Discard

Email notifications

On Off

\* Recipients (Email)

backupgroup@contoso.com

Privacy statement

Notify

Per Alert Hourly Digest

Severity

- ☒ Critical
- ☐ Warning
- ☐ Information

# Module Summary

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

