

Module 8: Azure Backup and Site Recovery

Module Overview

Azure Vaults

Configuring backups

Data Protection Manager

Azure Site Recovery and Disaster Recovery

On Premise Migration using Recovery Services

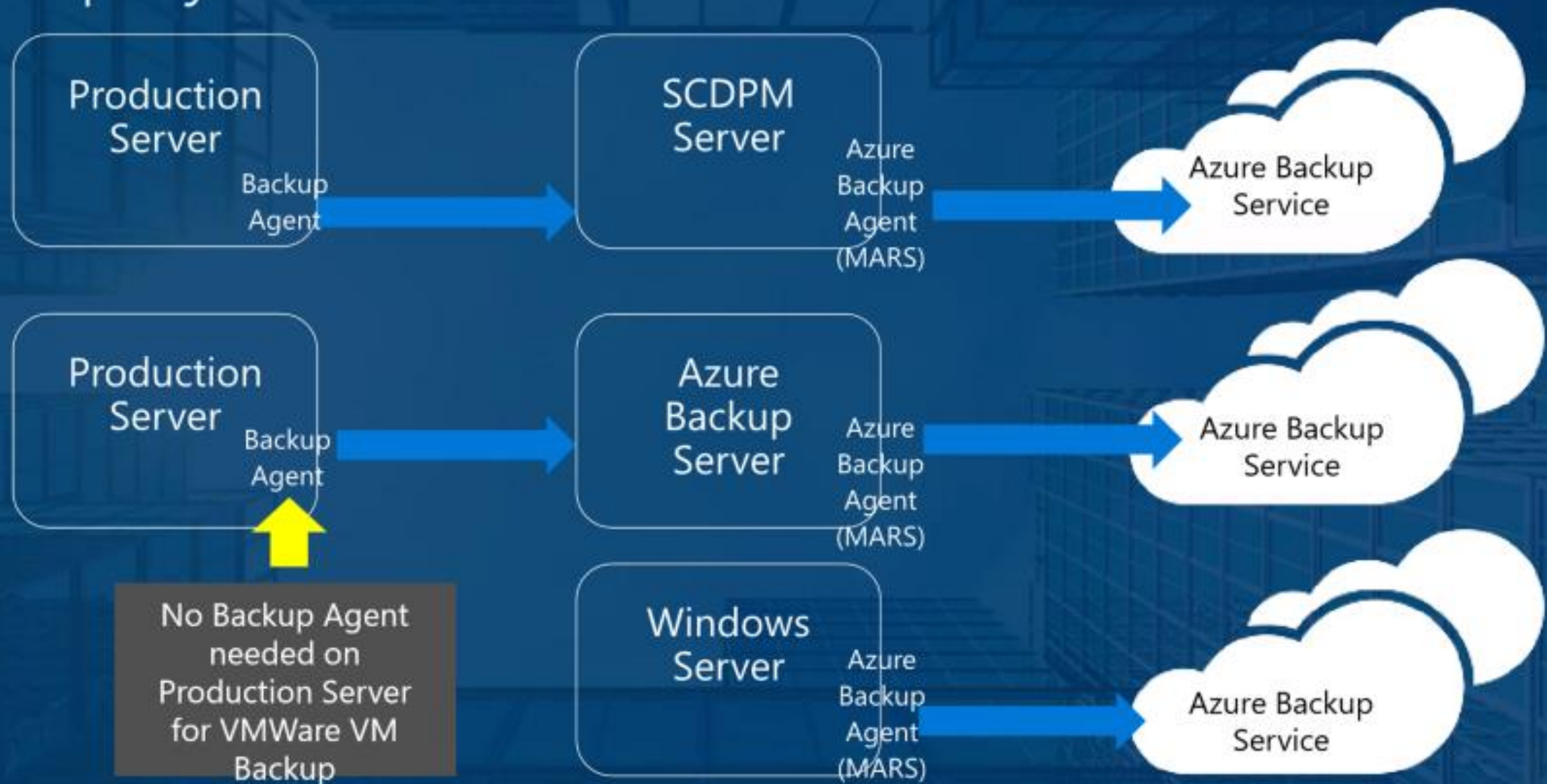
Azure Backup

Azure Backup is the Azure-based service we can use to back up (or protect) and restore our data in the Microsoft cloud. Azure Backup replaces our existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components that we can download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that we deploy depends on what we want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure.

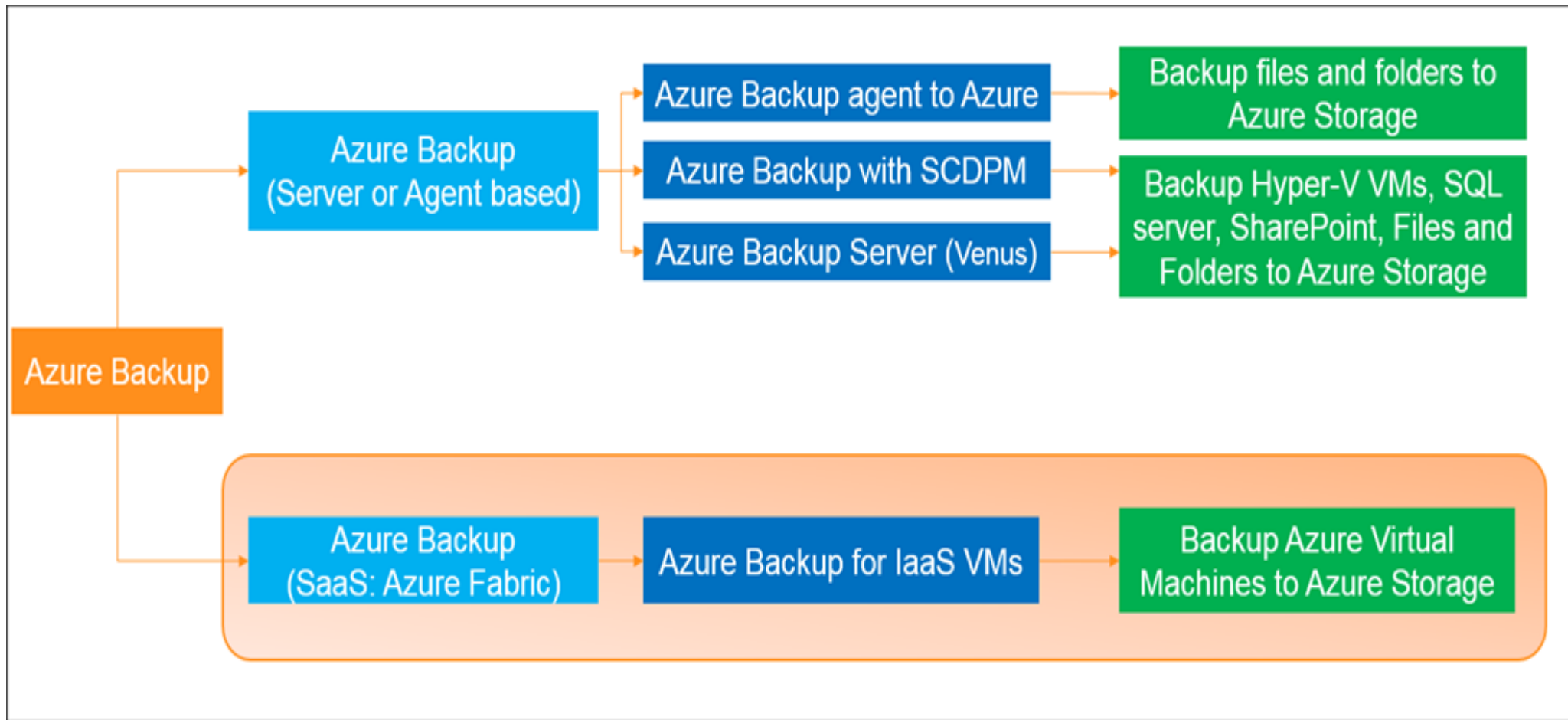
Azure Backup Components

- Azure Backup (MARS) agent
- System Center Data Protection Manager (DPM)
- Azure Backup Server
- Azure IaaS VM Backup

Deployment Models



Azure Backup under Recovery Services vaults support the 4 backup scenarios



Azure Backup (MARS) agent

Benefits

- Back up files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)
- No separate backup server required.

Limits

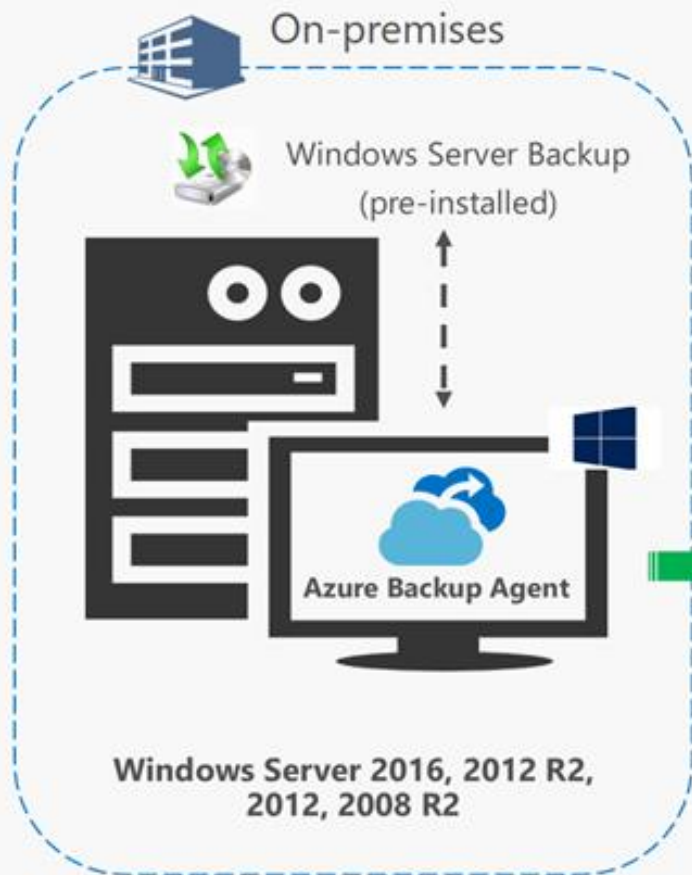
- Backup 3x per day
- Not application aware; file, folder, and volume-level restore only,
- No support for Linux.

What is protected?

- Files,
- Folders,
- System State

Where are backups stored?

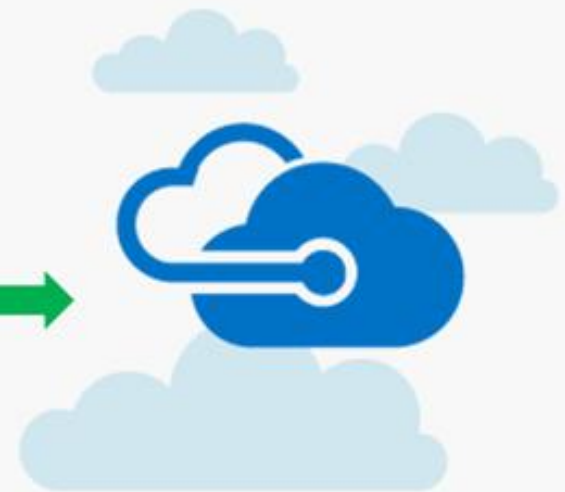
- Recovery Services vault



Windows Server System
State Backup

Directly to Azure!

Azure



Cost-Effective Offsite



Server Protection for File
Servers, AD & Web Servers



Secure Backups



Flexible restores



Single Management
pane in Azure

Azure



Azure Portal

Azure
subscription



contains

Recovery
Services Vault



Vault credential file
and Backup Agent



1

create

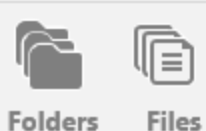
2

download



backup

4



Folders

Files

Azure Backup
Agent

install

register

3a

3b



Windows
Workstation or Server



On-Premises

System Center Data Protection Manager (DPM)

Every organization needs a business continuity and disaster recovery (BCDR) strategy to make sure resources are available during planned and unplanned outages, and that we're able to recover to normal working conditions when things go wrong. Your BCDR strategy requires keeping our data safe and recoverable, and keeping our business workloads, applications, and services continuously available. System Center Data Protection Manager (DPM) is a robust enterprise backup and recovery system that contributes to our BCDR strategy by facilitating the backup and recovery of enterprise data.

We can deploy System Center Data Protection Manager (DPM) for:

- **Application-aware backup:** Application-aware back up of Microsoft workloads, including SQL Server, Exchange, and SharePoint.
- **File backup:** Back up files, folders and volumes for computers running Windows server and Windows client operating systems.
- **System backup:** Back up system state or run full, bare-metal backups of physical computers running Windows server or Windows client operating systems.
- **Hyper-V backup:** Back up Hyper-V virtual machines (VM) running Windows or Linux. We can back up an entire VM, or run application-aware backups of Microsoft workloads on Hyper-V VMs running Windows.

System Center Data Protection Manager (DPM)

Benefits

- 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

Limits

- Cannot back up Oracle workload

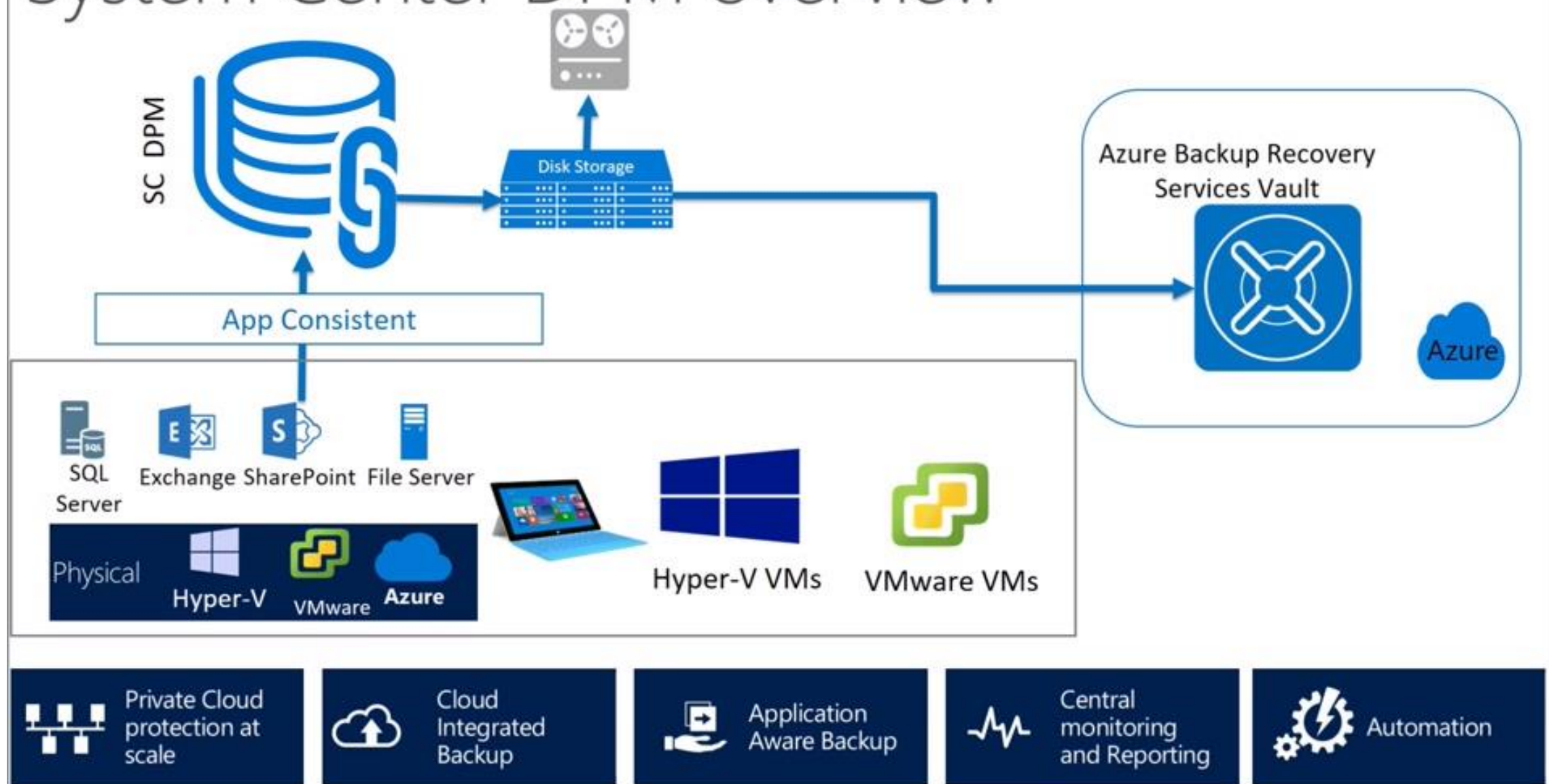
What is protected?

- Files,
- Folders,
- Volumes,
- VMs,
- Applications,
- Workloads
- System State

Where are backups stored?

- Recovery Services vault,
- Locally attached disk,
- Tape (on-premises only)

System Center DPM overview



Azure Backup Server

Azure Backup Server, we can protect application workloads such as Hyper-V VMs, Microsoft SQL Server, SharePoint Server, Microsoft Exchange, and Windows clients from a single console.

Azure Backup Server can now protect VMware VMs and provides improved security capabilities.

It inherits much of the workload backup functionality from Data Protection Manager (DPM) and shared some of the functionality.

Though Azure Backup Server shares much of the same functionality as DPM. It does not back up to tape, nor does it integrate with System Center.

Azure Backup Server is designed to run on a dedicated, single-purpose server. We cannot install Azure Backup Server on:

- A computer running as a domain controller
- A computer on which the Application Server role is installed
- A computer that is a System Center Operations Manager management server
- A computer on which Exchange Server is running
- A computer that is a node of a cluster

Always join Azure Backup Server to a domain. If we plan to move the server to a different domain, it is recommended that we join the server to the new domain before installing Azure Backup Server. Moving an existing Azure Backup Server machine to a new domain after deployment is not supported.

Azure Backup Server

Benefits:

- 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
- Does not require a System Center license

Limits:

- Cannot back up Oracle workload.
- Always requires live Azure subscription
- No support for tape backup

What is protected?

- Files,
- Folders,
- Volumes,
- VMs,
- Applications,
- Workloads
- System State

Where are backups stored?

- Recovery Services vault,
- Locally attached disk,

Azure IaaS VM Backup

Benefits:

- Application-aware snapshots (VSS)
- Native backups for Windows/Linux
- No specific agent installation required
- Fabric-level backup with no backup infrastructure needed

Limits:

- Back up VMs once-a-day
- Restore VMs only at disk level
- Cannot back up on-premises

What is protected?

- VMs,
- All disks (using PowerShell)

Where are backups stored?

- Recovery Services vault

Maximum backup frequency for each component

	Azure Backup agent	System Center DPM	Azure Backup Server	Azure IaaS VM Backup
Backup frequency (to Recovery Services vault)	Three backups per day	Two backups per day	Two backups per day	One backup per day
Backup frequency (to disk)	Not applicable	<ul style="list-style-type: none">• Every 15 minutes for SQL Server• Every hour for other workloads	<ul style="list-style-type: none">• Every 15 minutes for SQL Server• Every hour for other workloads	Not applicable
Retention options	Daily, weekly, monthly, yearly	Daily, weekly, monthly, yearly	Daily, weekly, monthly, yearly	Daily, weekly, monthly, yearly
Maximum recovery points per protected instance	9999	9999	9999	9999
Maximum retention period	Depends on backup frequency	Depends on backup frequency	Depends on backup frequency	Depends on backup frequency
Recovery points on local disk	Not applicable	<ul style="list-style-type: none">• 64 for File Servers,• 448 for Application Servers	<ul style="list-style-type: none">• 64 for File Servers,• 448 for Application Servers	Not applicable
Recovery points on tape	Not applicable	Unlimited	Not applicable	Not applicable

Azure Backup!

- Setup backup for your VMs in 3 steps
- Customized retention to be set at daily, weekly, monthly and yearly levels
- 9,999 recovery points
- 99 years of retention (not tested yet)

Backup policy

Choose backup policy ⓘ
Create New ▼

* Policy name ⓘ
DailyPolicy

Backup frequency
Daily ▼ 11:30 PM ▼ (UTC) Coordinated Universal Time ▼

Retention range

☒ Retention of daily backup point.

* At 11:30 PM ▼ 30 ▼ Day(s)

☒ Retention of weekly backup point.

* On Sunday ▼ * At 11:30 PM ▼ For 52 ▼ Week(s)

☒ Retention of monthly backup point.

Week Based Day Based

* On First ▼ * Day Sunday ▼ * At 11:30 PM ▼ For 60 Month(s)

☒ Retention of yearly backup point.

Week Based Day Based

* In January ▼ * On First ▼ * Day Sunday ▼ * At 11:30 PM ▼ For 10 Year(s)

Backup and Retention

Azure Backup has a limit of 9999 recovery points, also known as backup copies or snapshots, per protected instance. A protected instance is a computer, server (physical or virtual), or workload configured to back up data to Azure. An instance is protected once a backup copy of data has been saved. The backup copy of data is the protection. If the source data was lost or became corrupt, the backup copy could restore the source data. The above table shows the maximum backup frequency for each component. Our backup policy configuration determines how quickly we consume the recovery points. For example, if we create a recovery point each day, then we can retain recovery points for 27 years before we run out. If we take a monthly recovery point, we can retain recovery points for 833 years before we run out. The Backup service does not set an expiration time limit on a recovery point.

Protected Instance

A protected instance is a generic reference to a Windows computer, a server (physical or virtual), or SQL database that has been configured to back up to Azure. An instance is protected once we configure a backup policy for the computer, server, or database, and create a backup copy of the data. Subsequent copies of the backup data for that protected instance (which are called recovery points), increase the amount of storage consumed. We can create up to 9999 recovery points for a protected instance. If we delete a recovery point from storage, it does not count against the 9999 recovery point total.

Some common examples of protected instances are virtual machines, application servers, databases, and personal computers running the Windows operating system. For example:

- A virtual machine running the Hyper-V or Azure IaaS hypervisor fabric. The guest operating systems for the virtual machine can be Windows Server or Linux.
- An application server: The application server can be a physical or virtual machine running Windows Server and workloads with data that needs to be backed up. Common workloads are Microsoft SQL Server, Microsoft Exchange server, Microsoft SharePoint server, and the File Server role on Windows Server. To back up these workloads we need System Center Data Protection Manager (DPM) or Azure Backup Server.
- A personal computer, workstation, or laptop running the Windows operating system.

Recovery Services Vault

A Recovery Services vault is an online storage entity in Azure used to hold data such as backup copies, recovery points, and backup policies. We can use Recovery Services vaults to hold backup data for Azure services and on-premises servers and workstations. Recovery Services vaults make it easy to organize your backup data, while minimizing management overhead. Within each Azure subscription, we can create up to 25 Recovery Services vaults per Azure region. When considering where to store our data, not all regions are the same.

We can no longer create Backup vaults, and all existing Backup vaults have been upgraded to Recovery Services vaults. We can use the Azure portal to manage the vaults that were upgraded to Recovery Services vaults.

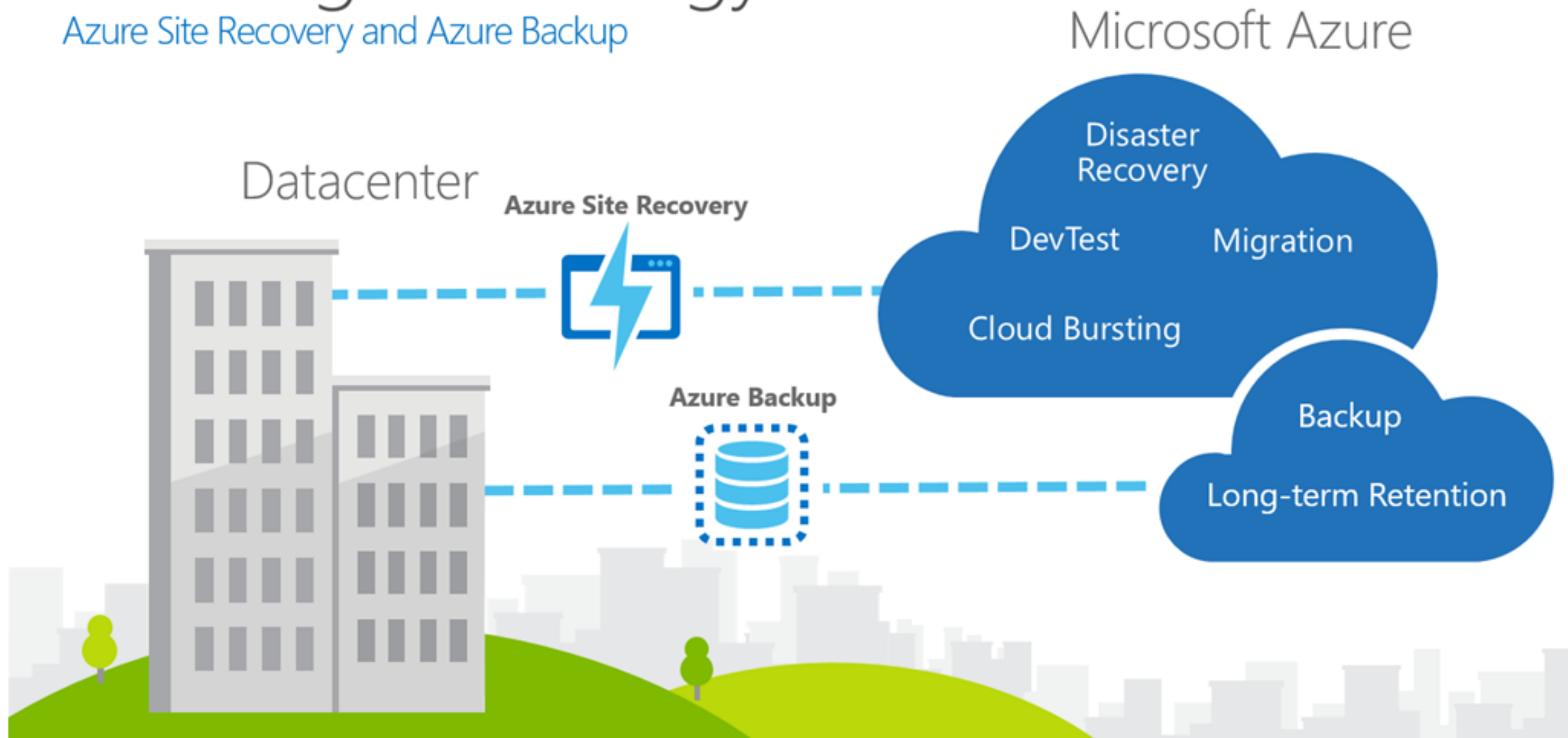
Azure Backup Vs Azure Site Recovery

Azure Backup and Azure Site Recovery are related in that both services back up data and can restore that data. However, these services serve different purposes in providing business continuity and disaster recovery in our business. We must use Azure Backup to protect and restore data at a more granular level. For example, if a presentation on a laptop became corrupted, we would use Azure Backup to restore the presentation. If we wanted to replicate the configuration and data on a VM across another datacenter, we will use Azure Site Recovery.

Azure Backup protects data on-premises and in the cloud. Azure Site Recovery coordinates virtual-machine and physical-server replication, failover, and failback. Both services are important because our disaster recovery solution needs to keep our data safe and recoverable (Backup) and keep our workloads available (Site Recovery) when outages occur.

Enabling technology

Azure Site Recovery and Azure Backup



Why We Selected Azure Site Recovery

Our customers' pain points:

Resource constraints for design, architecture and management

Recovery is complex, lack skills and knowledge

Responsible for data protection, but struggle to convince the business

Budgets are limited – especially for ensuring data protection

Virtualized environments are complex, manual failover is resource intensive

ASR is reliable, fast,
simple & cost-effective

- ✓ Don't pay for virtual machines in Azure until failover occurs
- ✓ Low-cost cloud storage for replicated data, reducing the need for dedicated infrastructure
- ✓ Encrypted replication across the Internet
- ✓ Non-disruptive failover testing with automated workflows

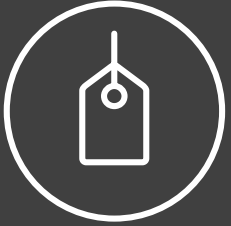
Below concepts can help us make important decisions around backup and disaster recovery.

Concept	Details	Backup	Disaster recovery (DR)
Recovery point objective (RPO)	The amount of acceptable data loss if a recovery needs to be done.	Backup solutions have wide variability in their acceptable RPO. Virtual machine backups usually have an RPO of one day, while database backups have RPOs as low as 15 minutes.	Disaster recovery solutions have low RPOs. The DR copy can be behind by a few seconds or a few minutes.
Recovery time objective (RTO)	The amount of time that it takes to complete a recovery or restore.	Because of the larger RPO, the amount of data that a backup solution needs to process is typically much higher, which leads to longer RTOs. For example, it can take days to restore data from tapes, depending on the time it takes to transport the tape from an off-site location.	Disaster recovery solutions have smaller RTOs because they are more in sync with the source. Fewer changes need to be processed.
Retention	How long data needs to be stored	For scenarios that require operational recovery (data corruption, inadvertent file deletion, OS failure), backup data is typically retained for 30 days or less. From a compliance standpoint, data might need to be stored for months or even years. Backup data is ideally suited for archiving in such cases.	Disaster recovery needs only operational recovery data, which typically takes a few hours or up to a day. Because of the fine-grained data capture used in DR solutions, using DR data for long-term retention is not recommended.

Why disaster recovery is needed

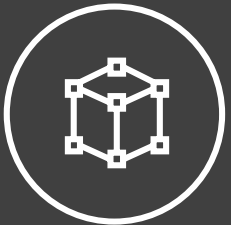
- Every company relies on IT systems to operate in this digital world
- Implementing disaster recovery across our enterprise can be daunting and therefore avoided.
- Yet, nearly every company is susceptible to some kind of disaster.
- Failure to provide service can lead to not only a service outage but long term brand damage.

Challenges implementing disaster recovery



Cost

- Data center cost
- Resource cost
- Hardware cost



Complexity

- Multiple data centers
- Replication technologies/restore hardware
- Managing management software

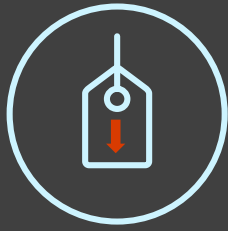


Reliability

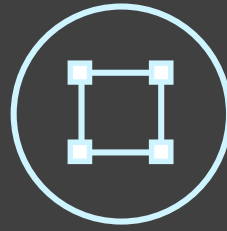
- Recovery of data
- Providing service

How Microsoft Azure can help

Accelerate your business continuity strategy



Reduced
cost



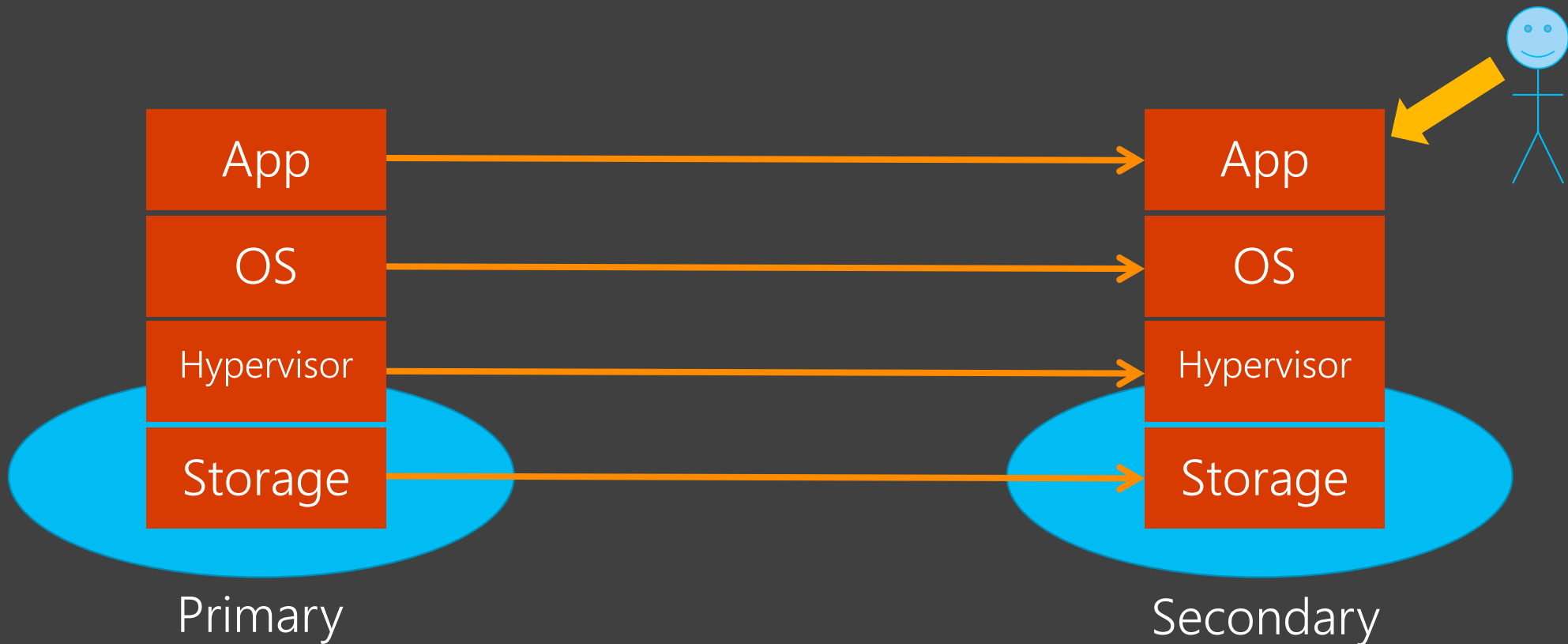
Reduced
complexity



Increased
reliability

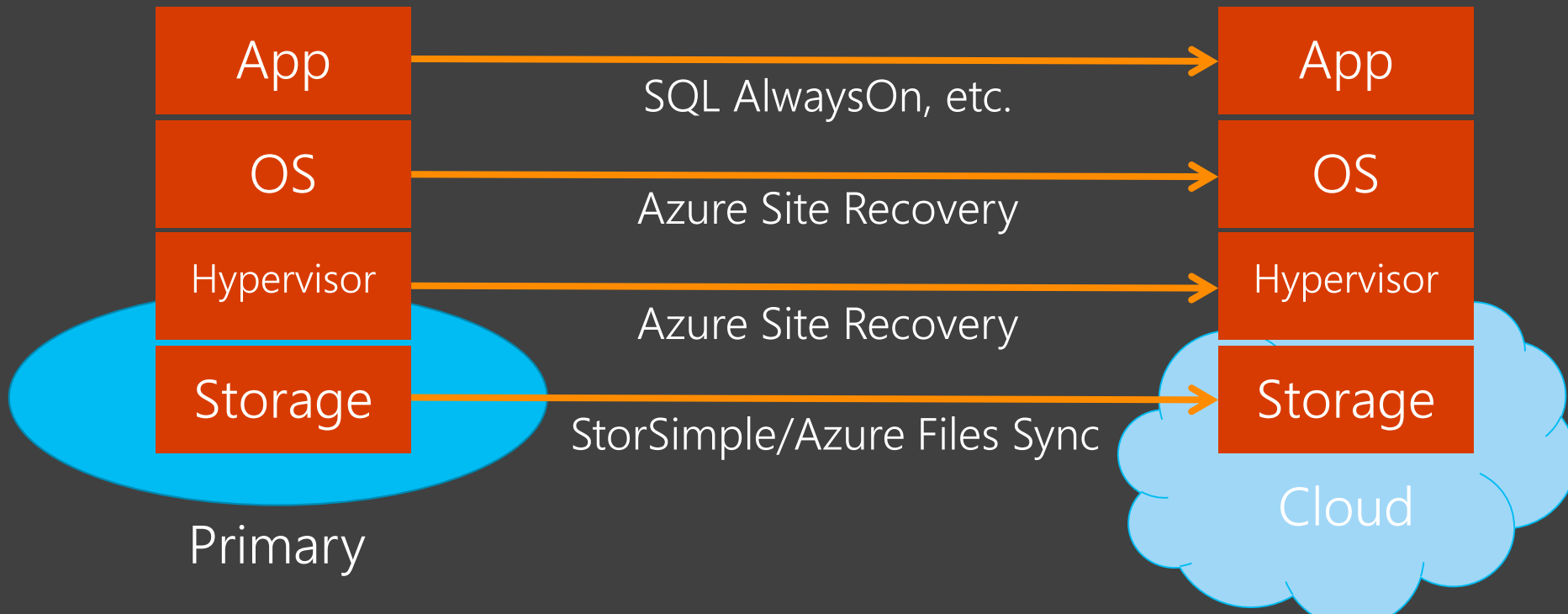
How is disaster recovery achieved on-premises?

- Alternative location
- Meet tight RPO and RTO objectives



Disaster recovery to Azure

The same process as on-premises, but with the benefits of Azure




Azure to Azure disaster recovery

- Same failover experience and features of on-premises to Azure replication
- Setup and test disaster recovery in 3 steps
- Quickly ensure your applications are compliant

Configure Site Recovery - PREVIEW

TestVM42

 **Site Recovery**
The virtual machine will be replicated to the selected target location with the specified settings so that you can recover the VM in the event of prolonged data center outages in source location. [Learn more.](#)

* Target region
North Central US



Target settings

	SOURCE	TARGET
VM resource group	RG_SCUS	(new) RG_SCUS-asr
Availability set	Not Applicable	Not Applicable
Virtual network	RG_SCUS-vnet	(new) RG_SCUS-vnet-asr

Storage settings

SOURCE STORAGE	TARGET STORAGE	CACHE STORAGE
savscuslrs [StandardLRS]	(new) savscuslrsasr [Standard_LRS]	(new) savscuslrsacheasr [Standard_LRS]

Replication settings

Recovery services vault	(new) Site-recovery-vault-northcentralus	
Recovery services vault resource group	(new) Site-recovery-vault-RG	
Replication policy	(new) 24-hour-retention-policy	