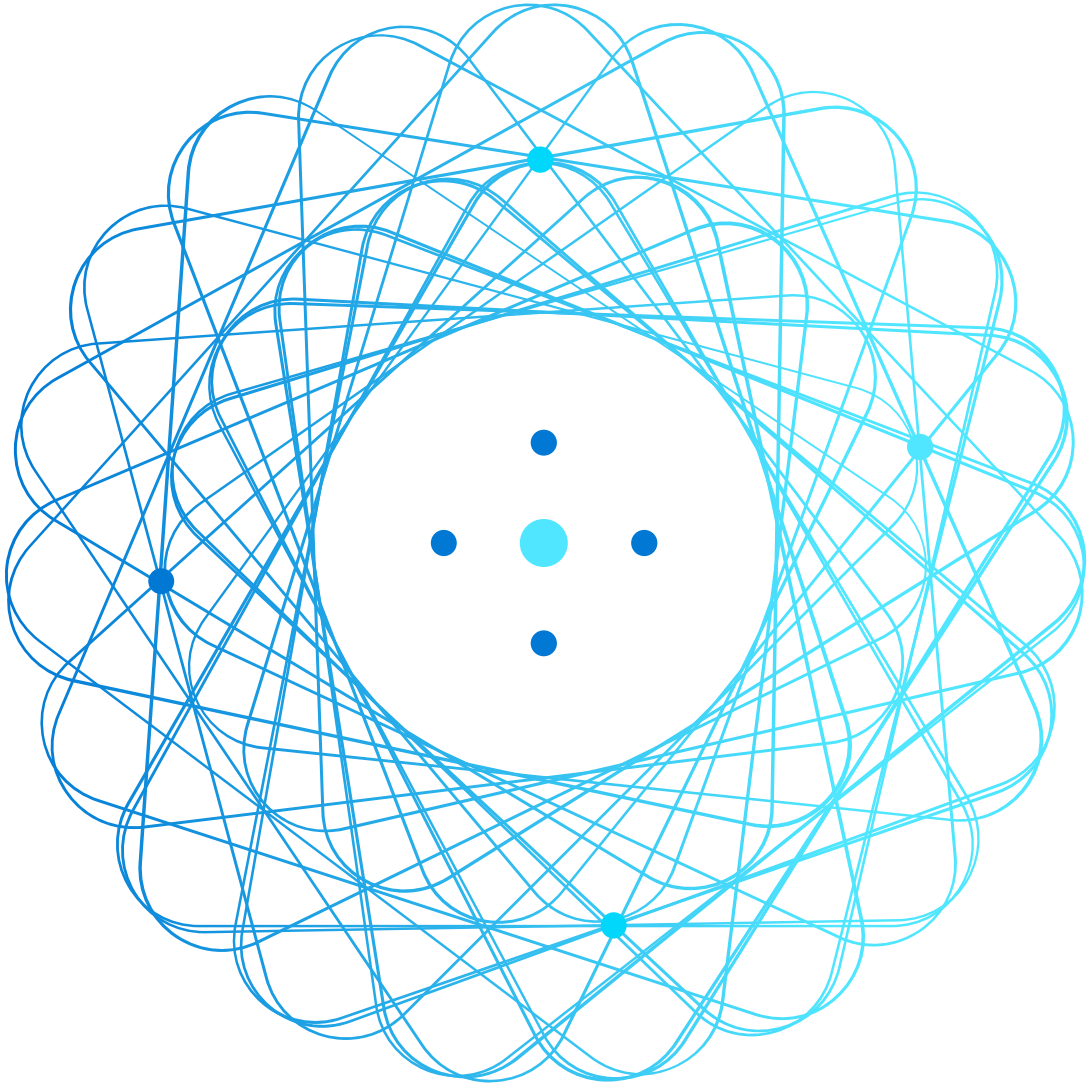
Microsoft Azure

AZ-801

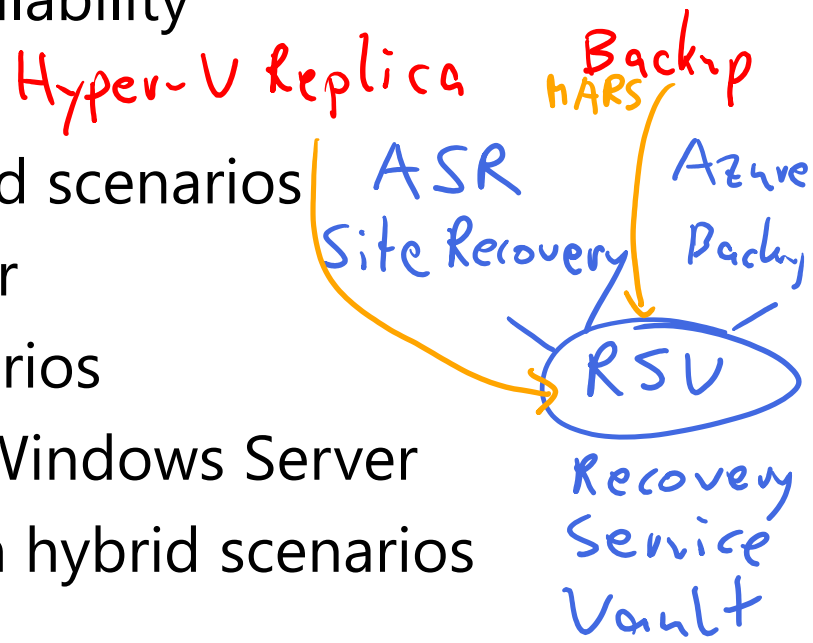
Configuring Windows Server Hybrid Advanced Services



AZ-801

Module 01: Windows Server security
Module 02: Implementing security solutions in hybrid scenarios
Module 03: Implementing Windows Server high availability
Module 04: Disaster recovery in Windows Server
Module 05: Implementing recovery services in hybrid scenarios
Module 06: Upgrade and migrate in Windows Server
Module 07: Implementing migration in hybrid scenarios
Module 08: Server and performance monitoring in Windows Server
Module 09: Implementing operational monitoring in hybrid scenarios

LP 3



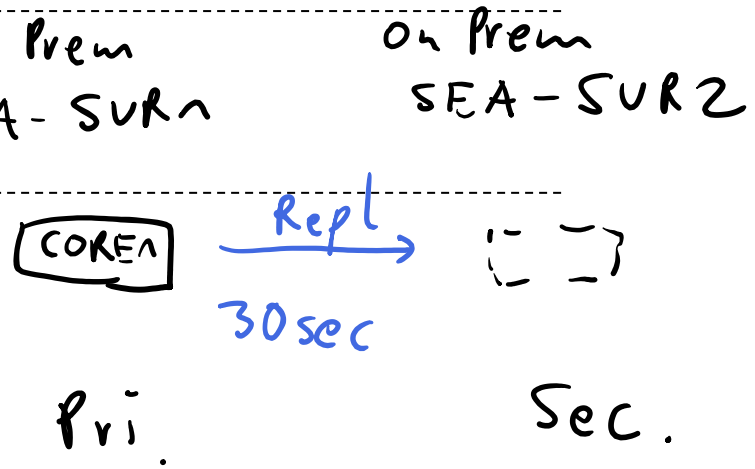
Learning Path 3: Implement disaster recovery in Windows Server on-premises and hybrid environments

(Disaster recovery in Windows Server)

Implement Hyper-V Replica

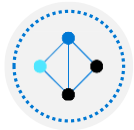
Protect your on-premises infrastructure from disasters with Azure Site Recovery

Lab 04



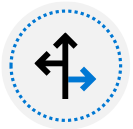
Module 1: Implement Hyper-V Replica

Implement Hyper-V Replica



Define Hyper-V Replica

Plan for Hyper-V Replica



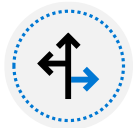
Configure and implement Hyper-V Replica

Demonstration – Configure and implement Hyper-V Replica

Define extended replication

Define Azure Site Recovery

Implement Site Recovery from on-premises site to Azure



Implement Site Recovery from on-premises site to on-premises site

Define Hyper-V Replica

Overview

- Hyper-V failover clusters are used to make VMs highly available
- Typically limited to a single location
- Multi-site clusters usually depend on specialized hardware and can be complicated and expensive to implement
- One possible solution is to periodically copy the VM manually

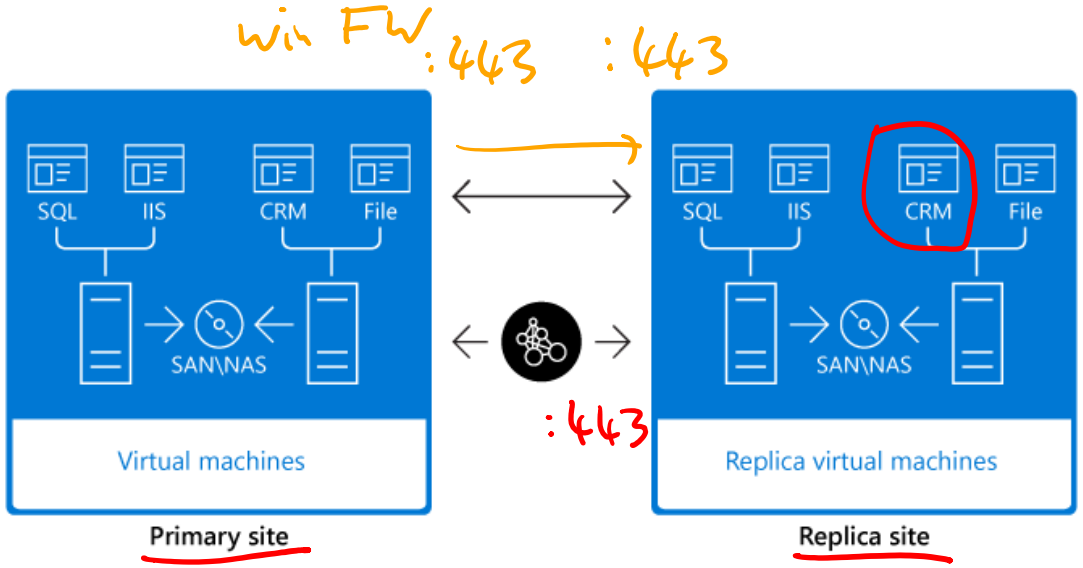
Usage scenarios:

- Hyper-V Replica can protect against data loss from site outage by copying a live VM as a replica VM from one location to another
- If necessary, you can use Hyper-V Replica to extend replication of the offline copy to a third location
- If your organization only has a single location available, you can still use Hyper-V Replica to replicate VMs to:
  - A partner organization in another location
  - To a hosting provider
  - To Microsoft Azure

Define Hyper-V Replica

Hyper-V Replica can have the following two instances of a single VM residing on different Hyper-V hosts:

- The main, actively running VM, which is called a primary VM
- An offline copy of the primary VM, which is called a replica VM



If failure occurs at the primary server site, you can use Hyper-V Replica to perform a failover of the VM(s) to the replica server at a secondary server site

Define Hyper-V Replica

Prerequisites for Hyper-V Replica implementation:

- A supported version of Windows Server with the Hyper-V role installed at both the primary and replica locations
- Sufficient storage on both the primary and replica Hyper-V hosts to store and run all VMs
- Sufficient storage for the log files that contain the changes at the primary location
- Network connectivity between the locations that are hosting the primary and the replica Hyper-V hosts
- Firewall rules to allow replication between the primary and replica sites
- Authentication certification or AD DS infrastructure requirements, depending on which type of authentication you plan to use

Define Hyper-V Replica

Hyper-V Replica consists of the following components:

- Replication engine
- Change tracking module
- Network module
- Hyper-V Replica Broker
- Management tools

Hyper-V replica can help protect all kinds of workloads, including:

- Microsoft SharePoint Server
- Microsoft Exchange Server
- Microsoft Dynamics CRM
- Microsoft SQL Server
- AD DS
- Internet Information Services
- Third-party applications

Plan for Hyper-V Replica

When planning for Hyper-V Replica deployment, you must define several parameters used in Hyper-V Replica configuration. Careful planning is important before setting up replication between Hyper-V hosts.

Hyper-V Replica host scenarios

Replication settings

Hyper-V Replica security considerations

Configure and implement Hyper-V Replica

To enable Hyper-V Replica, you must complete the following two high-level steps:

1. Enable a Hyper-V host to act as a replica server.
2. Enable replication on each VM that needs to be replicated on the primary Hyper-V host.

Manage Hyper-V Replica by using Windows PowerShell

You can also manage Hyper-V Replica by using Windows PowerShell

Failover TCP/IP

A feature that you can use to control the static IP address and other TCP/IP network settings that a VM uses when started as part of a failover

Replication health monitoring

When you enable replication for a VM, changes in the primary VM write to a log file that periodically transfers to the replica server

Failover options

- Test Failover
- Planned Failover
- Failover

Demonstration – Configure and implement Hyper-V Replica

Configure Hyper-V Replica on two host machines

Configure replication by using Windows PowerShell

Validate failover

Define extended replication

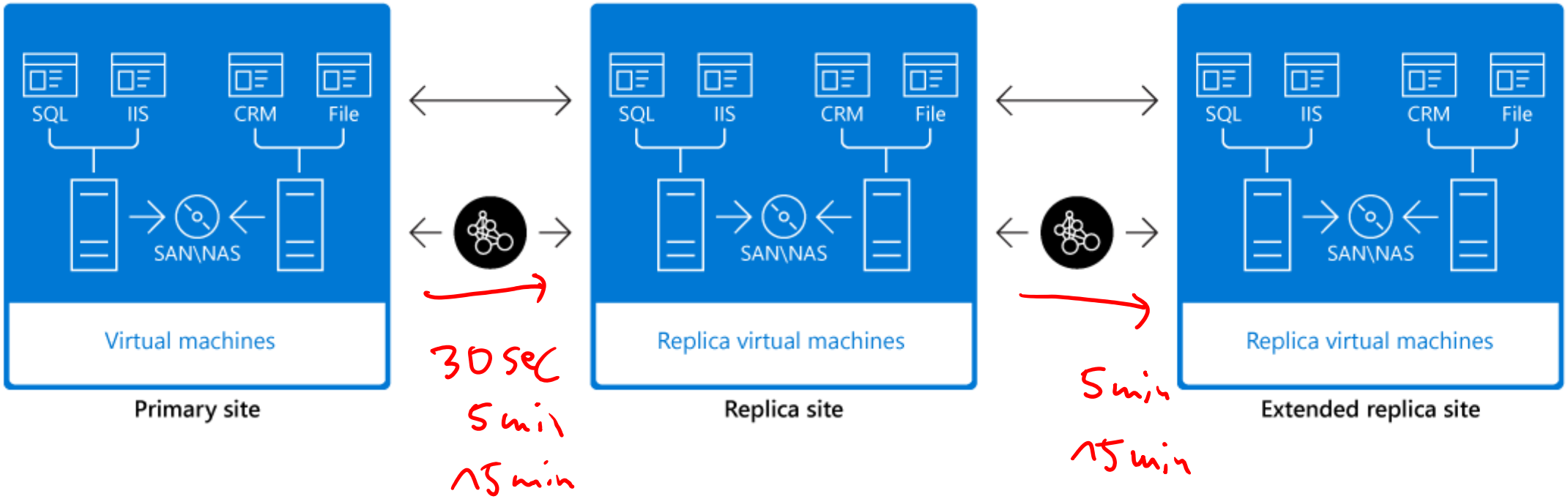
Extended replication:

- Supports replication to a third server to provide additional disaster recovery protection in case of failure of both primary and replica sites
- Enables you to replicate a running VM to two independent servers which could be in different geographic locations, providing additional options for recovering a failed VM

Limits of extended replication configuration:

- Replication frequency can be 5 minutes or 15 minutes only
- Replication frequency can't be lower than the initial replication
- You can't change the authentication type

Define extended replication



Define extended replication

To create an extended replica in Hyper-V Manager:

1. Select the replica VM
2. Select **Replication** > **Extend Replication**
3. In the **Extend replication for** <**VMName**> wizard, select the following:
   a. Select the replica server that will act as the extended replica server
   b. Select whether to compress the data that's transmitted over the network
   c. Select the frequency at which changes are sent to the extended replica server
   d. Select the option to maintain only the latest recovery points or create additional hourly recovery points
   e. Select an initial replication method and schedule

Define Azure Site Recovery

Azure Site Recovery (Site Recovery) is a BCDR solution that can replicate VMs (on-premises or cloud based) and physical servers to Microsoft Azure or to a second site.

- When an outage occurs at your primary site, workloads on a primary site can failover to secondary location and access apps from that site
- After the primary site is running again, you can failover back to the primary VM in the primary site, and resume accessing apps from the primary site

The secondary site can be:

On-premises in the same datacenter	In a geographically separate private datacenter	In Azure

Define Azure Site Recovery

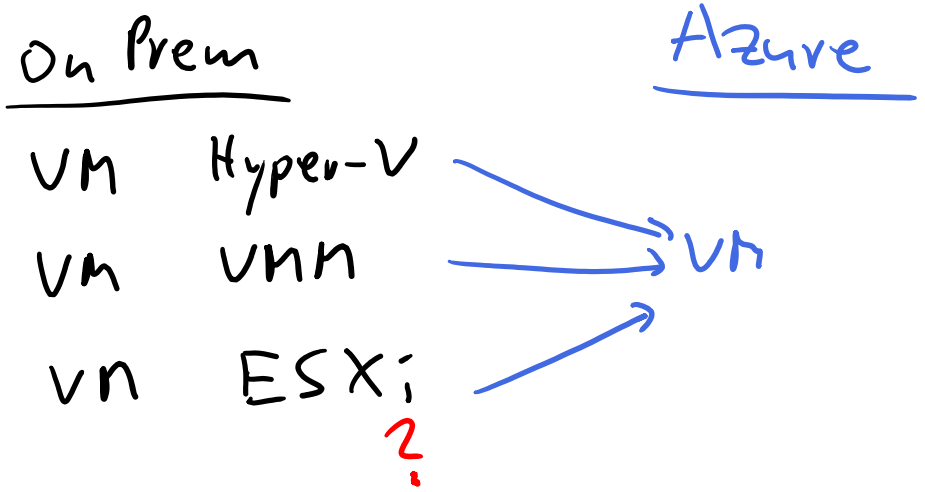
Benefits of using Site Recovery:

Site Recovery provides many benefits, including:

- It's workload and application agnostic
- It has near-synchronous replication
- It provides testing without disruption
- It has *Recovery plans* that enable you to customize and sequence the failover and recovery of apps running on multiple VMs
- It integrates and leverages other Azure services and other BCDR technologies

Site Recovery supports the following failover types:

- Test failover
- Planned failover
- Unplanned failover



Implement Site Recovery from on-premises site to Azure

Types of machines or servers with which Site Recovery can replicate:

- Physical Windows Server or Linux servers
- Hyper-V VM
- Azure VMs
- Azure Stack VMs
- VMWare VM
- Amazon Web Services (AWS) Windows VMs

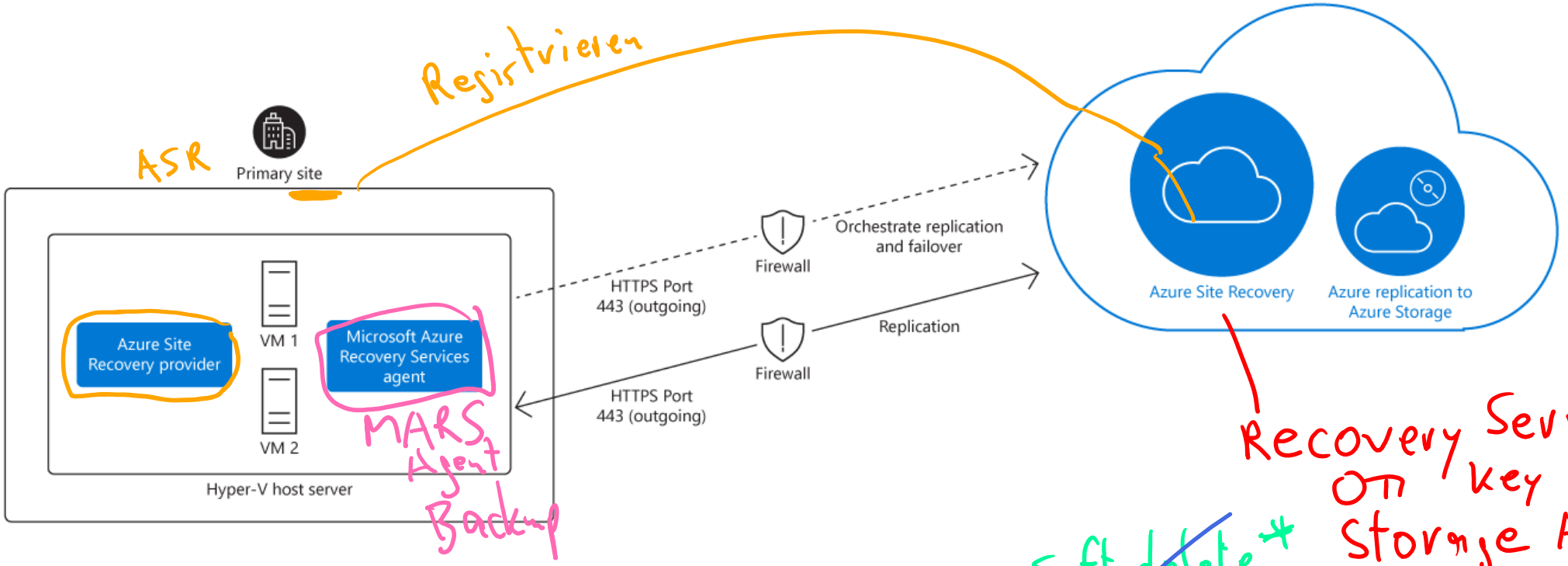
Deployment scenarios:

- On-premises Hyper-V Replication to Azure (without VMM)
- On-premises Hyper-V Replication to a secondary on-premises Hyper-V site (with VMM)

Implement Site Recovery from on-premises site to Azure

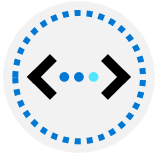
On-premises Hyper-V Replication to Azure (without VMM)

The on-premises site has a Hyper-V server host with the Site Recovery Provider and Microsoft Azure Recovery Services Agent installed. There is replication traffic over HTTPS port 443 to Site Recovery, which in turn has Azure Storage present for storing replicated VMs.



Implement Site Recovery from on-premises site to Azure

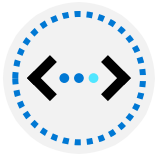
Task 1: Complete Deployment planning



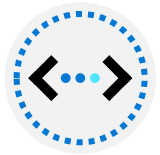
Task 2: Create Azure resources

Task 3: Configure Hyper-V hosts

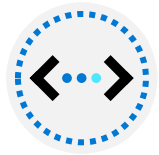
Task 4: Prepare infrastructure



Task 5: Enable replication



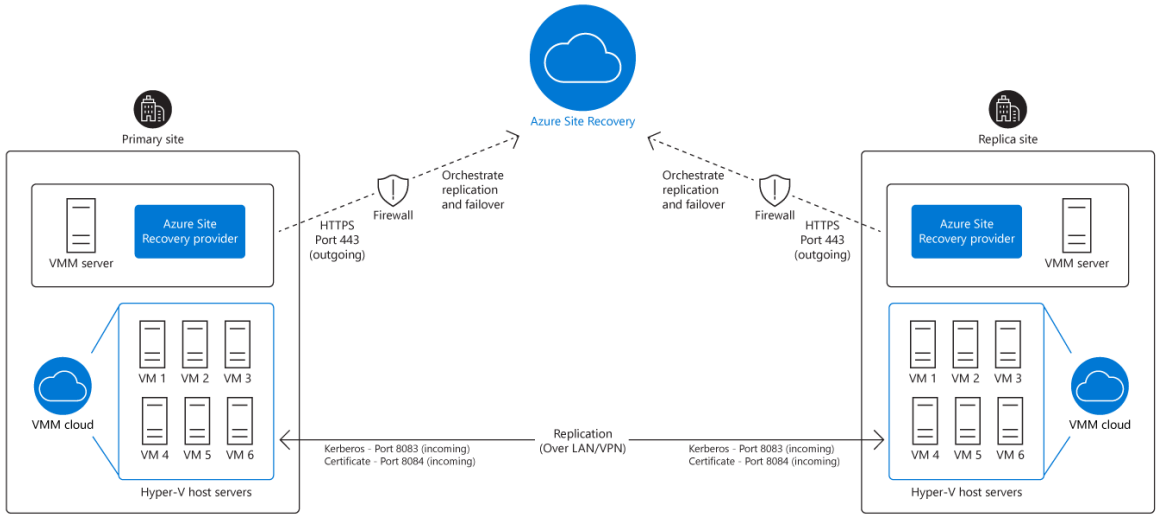
Task 6: Run a disaster recovery drill to Azure



Implement Site Recovery from on-premises site to on-premises site

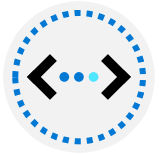
On-premises Hyper-V Replication to a secondary on-premises Hyper-V site (with VMM):

- The graphic illustrates two on-premises environments, a primary site and an identical replica site, both with VMM private cloud environments with Hyper-V host servers running six VMs
- Azure Site Recovery orchestrates the replication and failover between the two sites but not VM data replicates to Azure



On-premises Hyper-V Replication to a secondary on-premises Hyper-V site (with VMM)

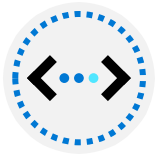
Task 1: Create Azure resources



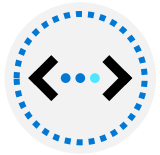
Task 2: Configure the Recovery Services vault

Task 3: Prepare infrastructure

Task 4: Enable replication



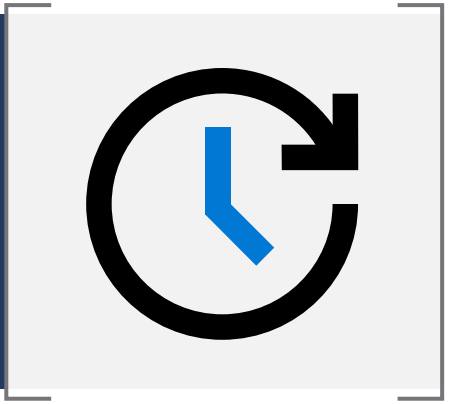
Task 5: Manage a recovery plan



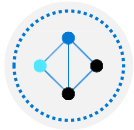
Knowledge check and resources – Implement Hyper-V Replica

Knowledge Check	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Implement Hyper-V Replica

Module 2: Protect Your On-premises Infrastructure from Disasters with Azure Site Recovery

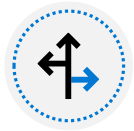


Protect Your On-premises Infrastructure from Disasters with Azure Site Recovery Introduction



Azure Site Recovery overview

Workloads supported for protection with Azure Site Recovery



Run a disaster recovery drill

Failover and failback

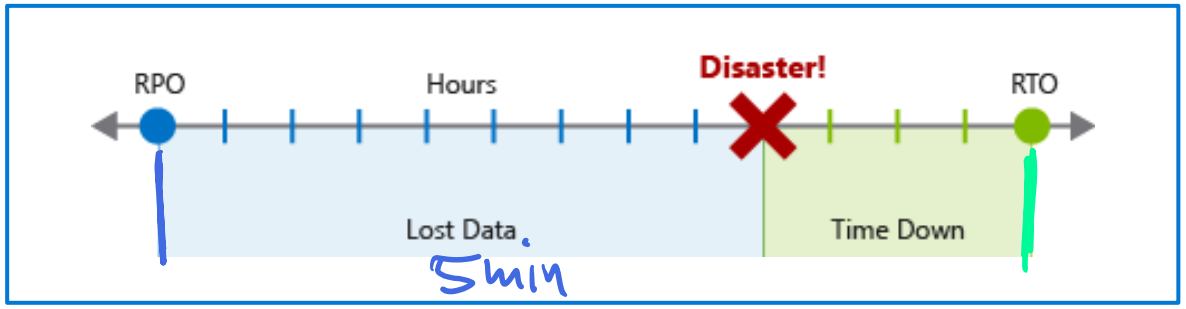
Knowledge check and resources

Azure Site Recovery overview

Business continuity and disaster recovery

As part of your BCDR plan, identify the following for your applications:

- Recovery time objective
- Recovery point objective



What is Azure Site Recovery?

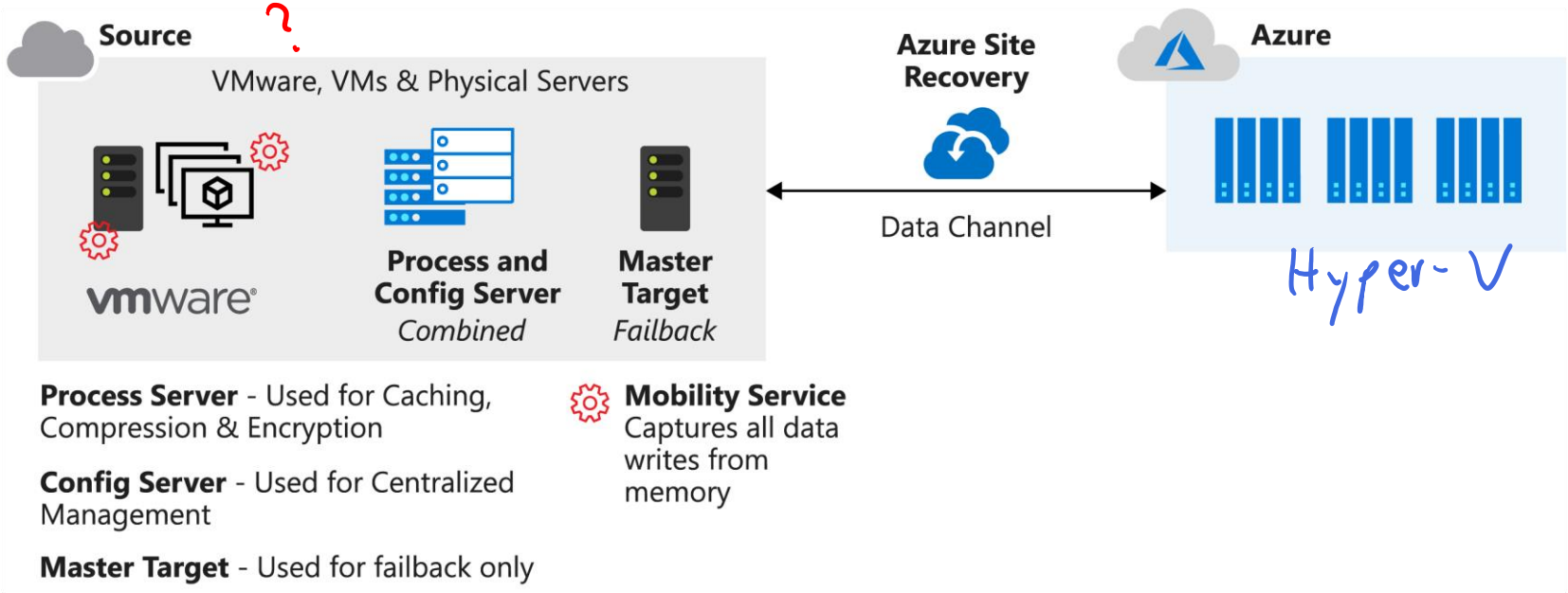
Azure Site Recovery has the following features:

- Central management
- On-premises virtual machine replication
- Azure virtual machine replication
- App consistency during failover
- Flexible failover
- Network integration

Azure Site Recovery overview

Several components must be set up to enable Azure Site Recovery:

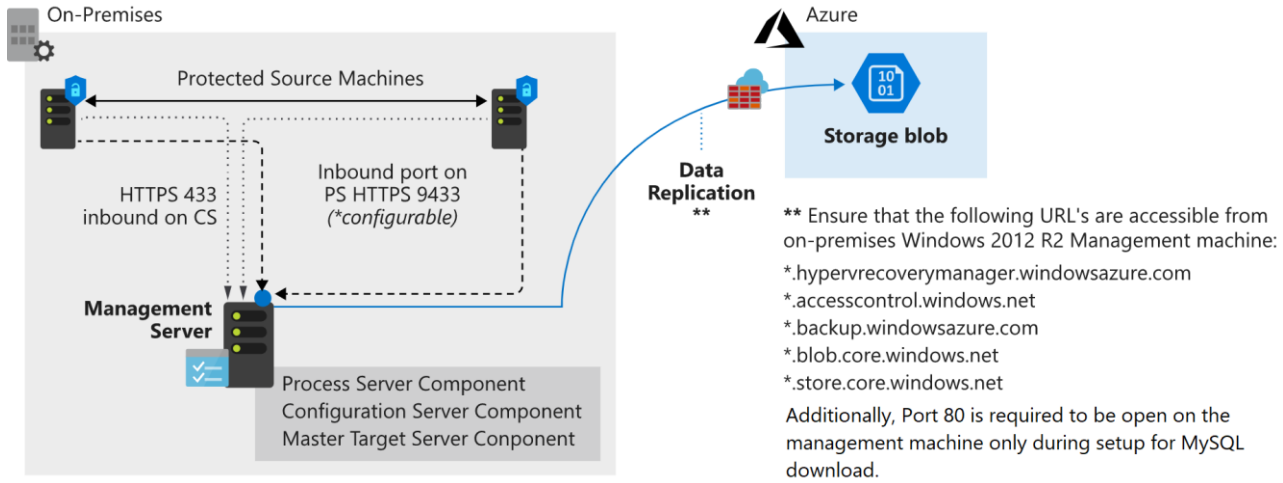
- Networking
- Recovery Services vault
- Credentials
- Configuration server
  - Process server
  - Master target server



Azure Site Recovery overview

Replication process

1. **First replication**: the server data is replicated to Azure Storage.
2. **Second replication**: The delta changes to the virtual machine are replicated to Azure.



Then test the configuration by doing a disaster recovery drill on an isolated VM

Workloads supported for protection with Azure Site Recovery

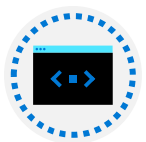
Azure Site Recovery supported workloads

Site Recovery can replicate any app that runs on a supported machine:

Azure VM: Replication is available for any workload that runs on a supported Azure virtual machine.

Hyper-V VM: Protection is available for any workload that runs on a Hyper-V virtual machine.

Physical servers: Protection is available for Windows and Linux operating systems.



VMware VM: Protection is available for any workload that runs in a VMware virtual machine.

Workloads supported for protection with Azure Site Recovery

Site Recovery provides application-aware replication for many types of workloads or applications that run on top of the server operating system.

Some of the features offered include:

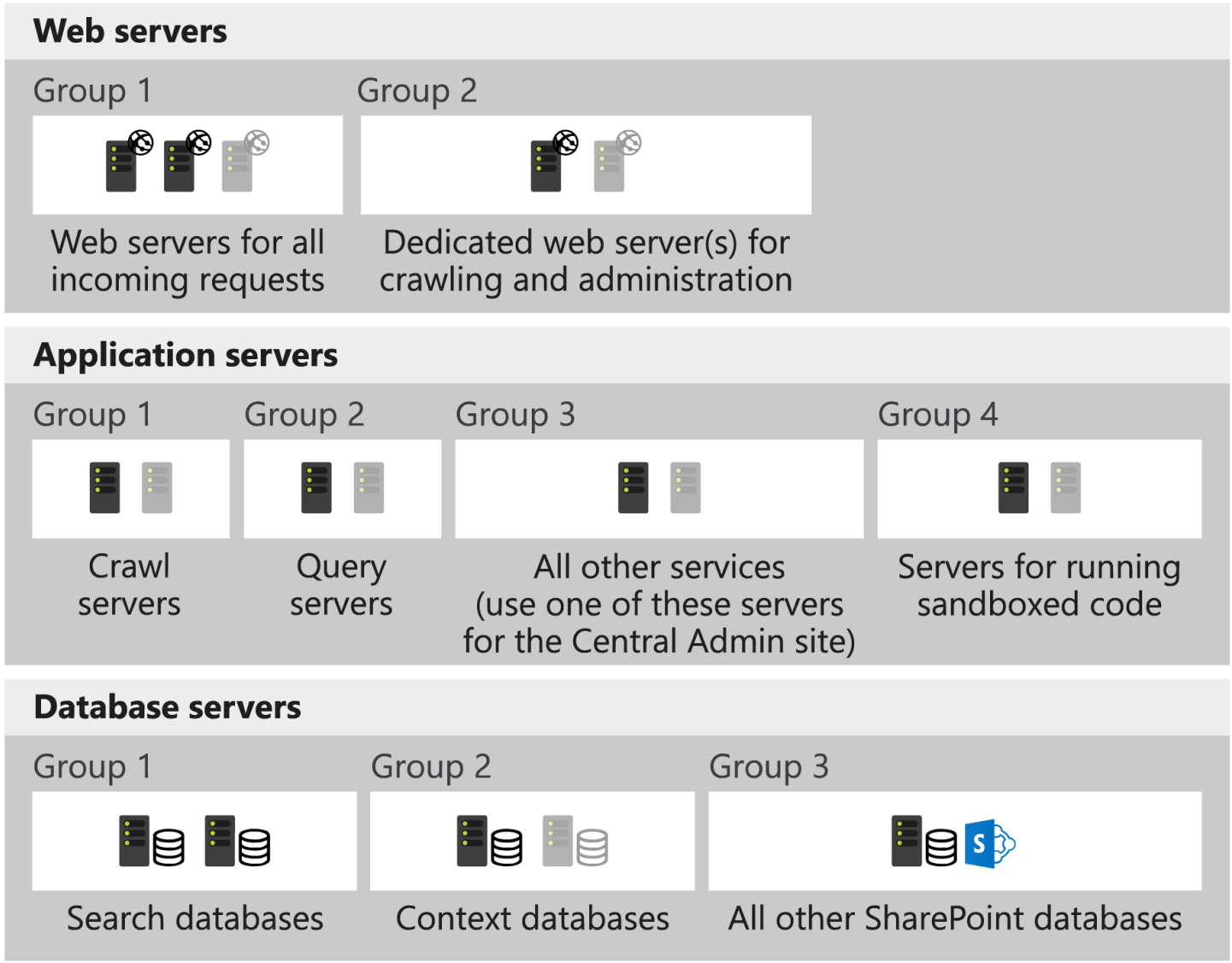
- Near synchronous replication
- App-consistent snapshots
- Integration with SQL Always On
- Flexible recovery plans:
  - Network management
  - Automation library

Workloads supported for protection with Azure Site Recovery

- Active Directory and DNS
- SQL Server
- SharePoint
- Dynamics AX

- Remote desktop services
- Exchange
- SAP
- IISCitrix XenApp and XenDesktop

Workloads supported for protection with Azure Site Recovery

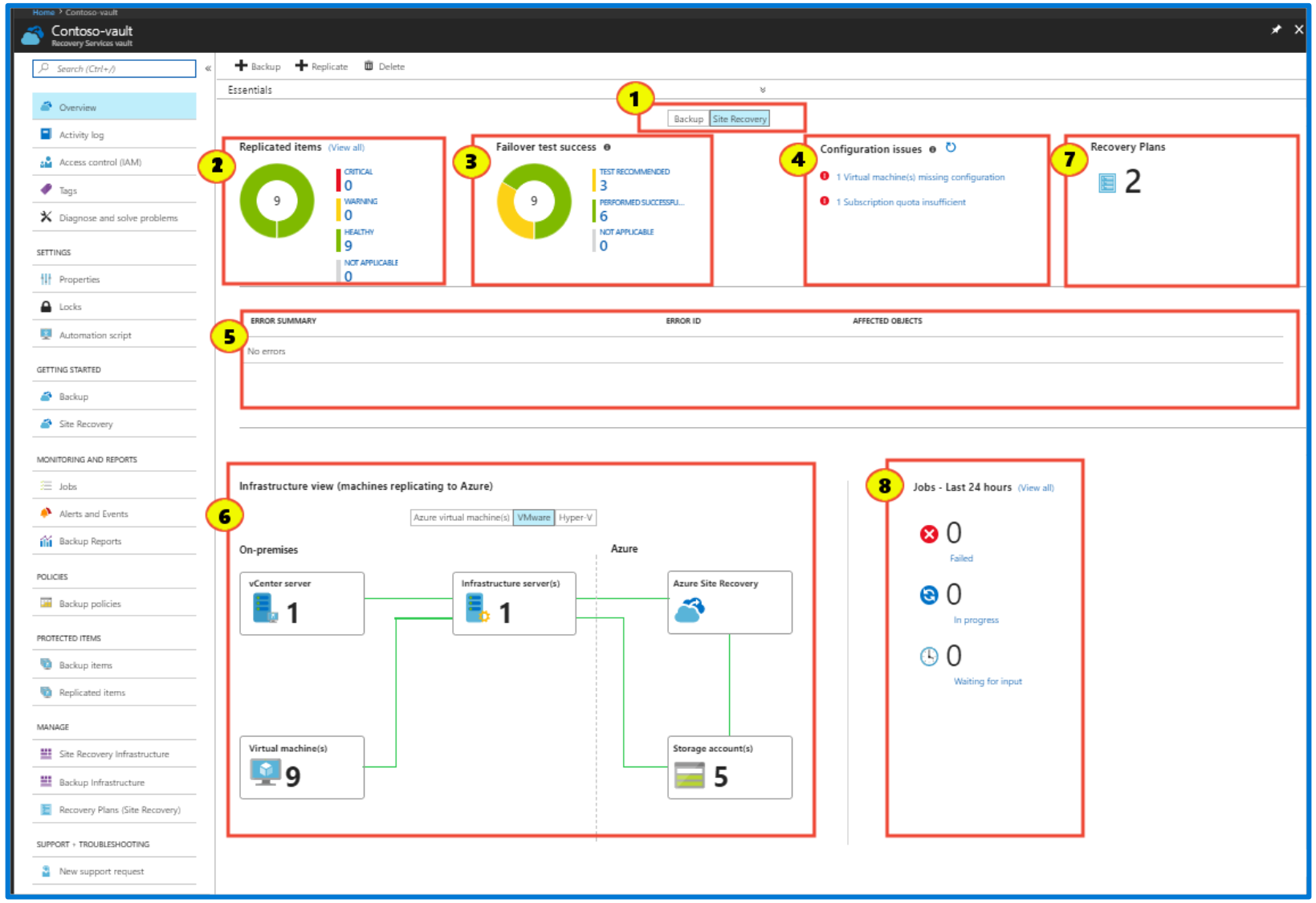


Run a disaster recovery drill

Disaster recovery drill

- With Site Recovery, you can do a full disaster recovery test without affecting your existing live environment.
- Recovery plans are created within Site Recovery to allow the automation of recovery tasks and model an app around its dependencies, such as the need for Active Directory or DNS to function.
- BCDR plans also allow you to test your disaster recovery.

Run a disaster recovery drill



Test Failover

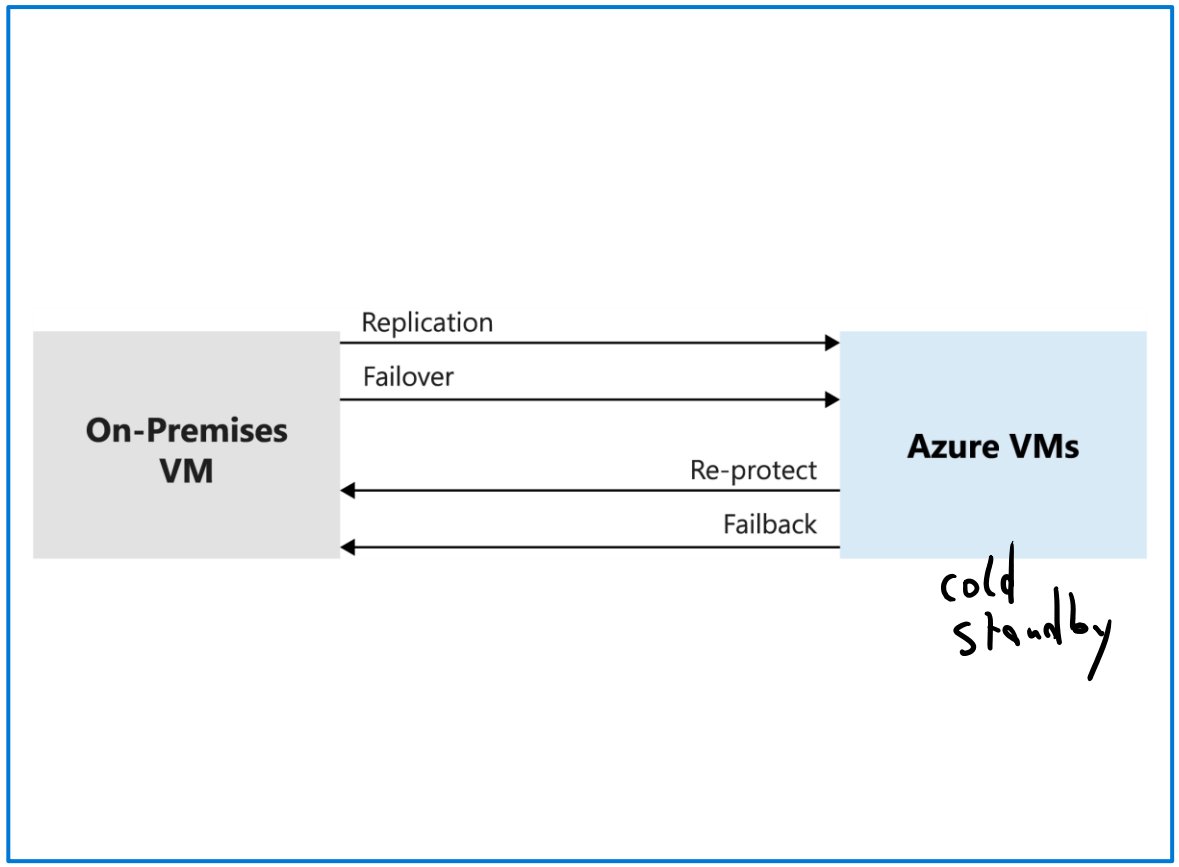
Failover and failback

Azure Site Recovery gives you the flexibility to fail over to Azure if a disaster occurs and fail back to on-premises machines after the event is over.

Failover and failback

The four stages of failover and failback actions are:

- Fail over to Azure
- Reprotect Azure virtual machines
- Fail back to on-premises
- Reprotect on-premises virtual machines



Failover and failback

Failback policies

When you create an on-premises replication policy to copy your on-premises machines to Azure, an associated failback policy is automatically created for you.

Business Continuity and Disaster Recovery plans

BCDR plans within Site Recovery allow for the customization and sequencing of failover and failback of virtual machines and the applications that run on them.

Flexible failovers

With the ability to be flexible with failovers, Site Recovery can run failovers on demand for test purposes.

Knowledge check and resources – Protect your on-premises infrastructure from disasters with Azure Site Recovery

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Protect your on-premises infrastructure from disasters with Azure Site Recovery

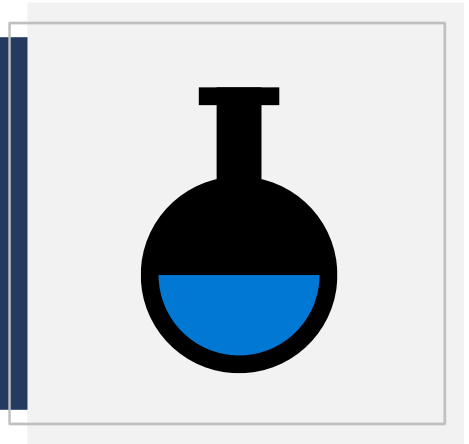
SEA-SVR1
Hyper-V

CORE 1

SEA-SVR2
Hyper-V

Repl.
30sec

Lab 04



SEA-SVR1

Backup Feature
Backup Policy

SEE-SVR2

DPM

Lab 04 – Implementing Hyper-V Replica and Windows Server Backup

Lab scenario

You're working as an administrator at Contoso, Ltd. Contoso wants to assess and configure new disaster recovery and backup features and technologies. As the system administrator, you have been tasked with performing that assessment and implementation. You decided to evaluate Hyper-V Replica and Windows Server Backup.

Objectives

- Configure and implement Hyper-V Replica
- Configure and implement backup with Windows Server Backup

End of presentation