Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powerd by simplilearn

Cloud
Computing

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Technologies: AZ:303

Powerd by simplilearn

Cloud

Manage Workloads in Azure

Powerd by simplilearn

Caltech | Center for Technology & Management Education

Learning Objectives

By the end of this lesson, you will be able to:

- Migrate workloads using Azure Migrate
- Implement Azure Backup for Azure Workloads
- Implement disaster recovery
- Implement Azure Automation Update Management

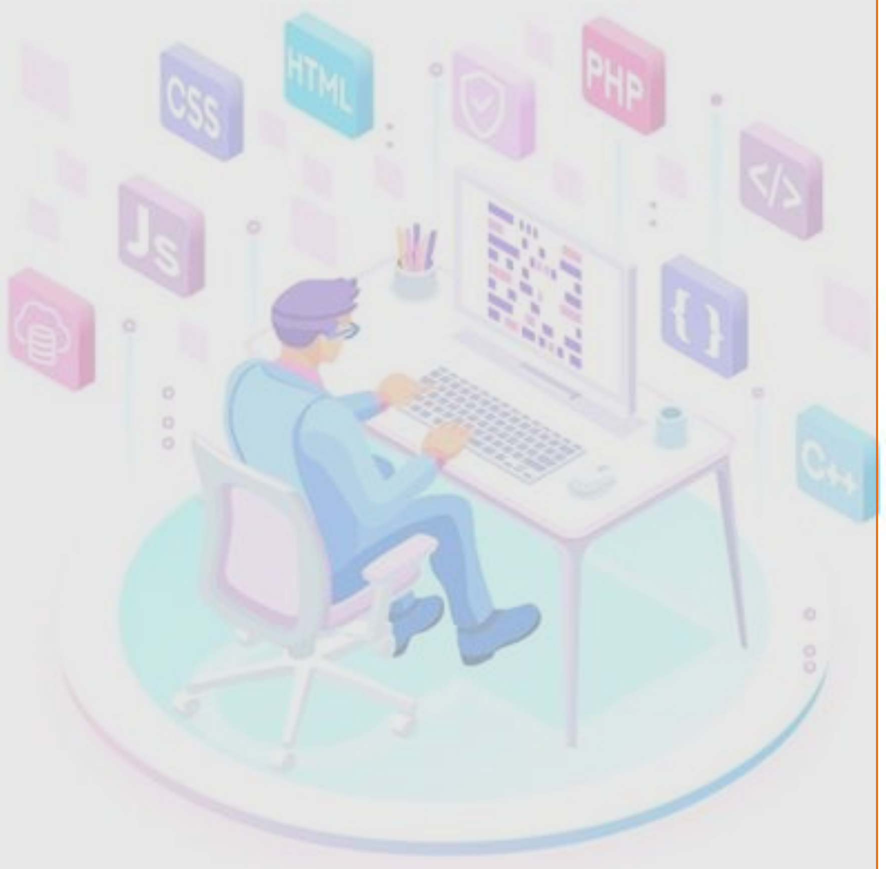
A Day in the Life of an Azure Architect

The company you are working for is planning to move to the cloud and hence looking for a solution that can help migrate on-premise VMware VMs, Hyper-V VMs, physical servers, other virtualized machines, and private or public cloud instances to Azure.

Additionally, to avoid any data loss you are asked to advise a solution that offers simple and reliable backup and protection for critical data in an easily recoverable way, from any location.

Also, you need to ensure business continuity and disaster recovery (BCDR) strategy that will keep the company data safe and the apps and workloads online, whenever planned and unplanned outages occur.

To achieve all the above along with some additional features, we will be learning a few concepts in this lesson that will help you find a solution for the given scenario.



Azure Migrate

Azure Migrate

Azure migrate helps the user to migrate on-premise VMware VMs, Hyper-V VMs, physical servers, other virtualized machines, and private or public cloud instances to Azure.

Azure Migrate

The key features of Azure Migrate are:

- Unified migration platform
- Wide range of migration tools:
  - Azure Migrate Server assessment
  - Azure Migrate Server migration
  - Database assessment or migration
  - Azure Migrate appliance

Assess

Migrate

Optimize

Secure & Manage

VMware Migration

VMware VMs can be migrated using Azure Migrate Server Migration with the following two options:

Agentless replication

Migrate VMs without installing an agent on the VMs

Agent-based replication

Install an agent on the VM for replication

VMware Migration

Agentless replication is easier to deploy in VMware, but has the following limitations:

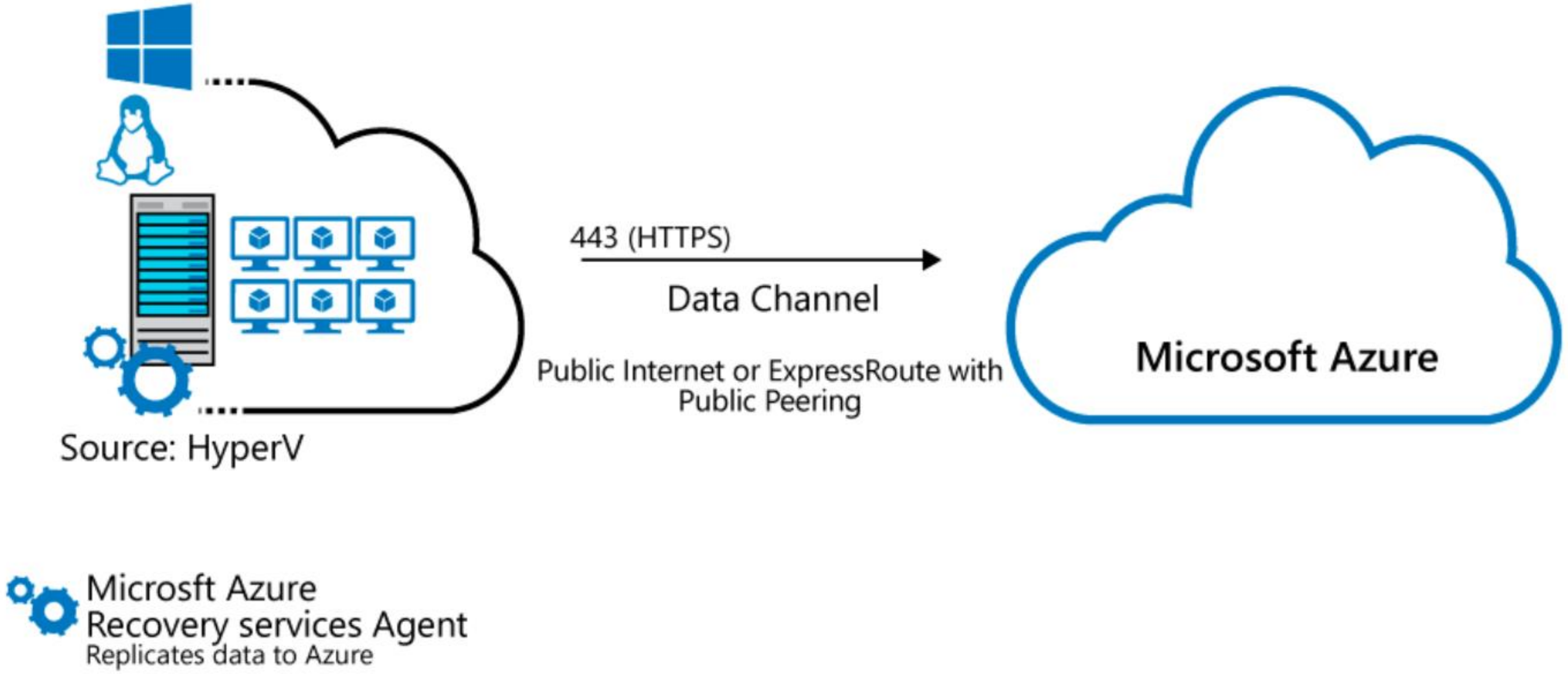
- Simultaneous replication: maximum of 300 VMs migrated at a time
- VM must have 60 or less disks
- VM operating systems may need manual configuration before migration
- Issues with Linux or EUFI boot, encrypted disks or volumes, NFS volumes, and target storage

Deployment Steps Comparison

Task	Details	Agentless	Agent-based
Prepare VMware servers and VMs for migration	Configure a number of settings on VMware servers and VMs	Required	Required
Add the Server Migration tool	Add the Azure Migrate Server Migration tool in the Azure Migrate project	Required	Required
Deploy the Azure Migrate appliance	Set up a lightweight appliance on a VMware VM for VM discovery and assessment	Required	Not required
Install the mobility service on VMs	Install the mobility service on each VM the user want to replicate	Not required	Required
Deploy the Azure Migrate Server Migration server Migration replication appliance	Set up an appliance on a VMware VM to discover VMs, and bridge between the mobility service running on VMs and Azure Migrate Server Migration	Not required	Required
Replicate VMs. Enable VM replication	Configure replication settings and select VMs to replicate	Required	Required
Run a test migration	Run a test migration to make sure everything's working as expected	Required	Required
Run a full migration	Migrate the VMs	Required	Required

Hyper-V Migration

The Azure Migrate Server Migration tool provides agentless replication for on-premise Hyper-V VMs, using a migration workflow that's optimized for Hyper-V.



Hyper-V Migration

Hyper-V VM installs services such as, Microsoft Azure Site Recovery provider and Microsoft Azure Recovery Service agent on Hyper-V Hosts or cluster nodes for migration.

Replication provider

It is installed on Hyper-V hosts, and registered with Azure Migration Server Migration. The provider orchestrates replication for Hyper-V VMs.

Recovery Services agent

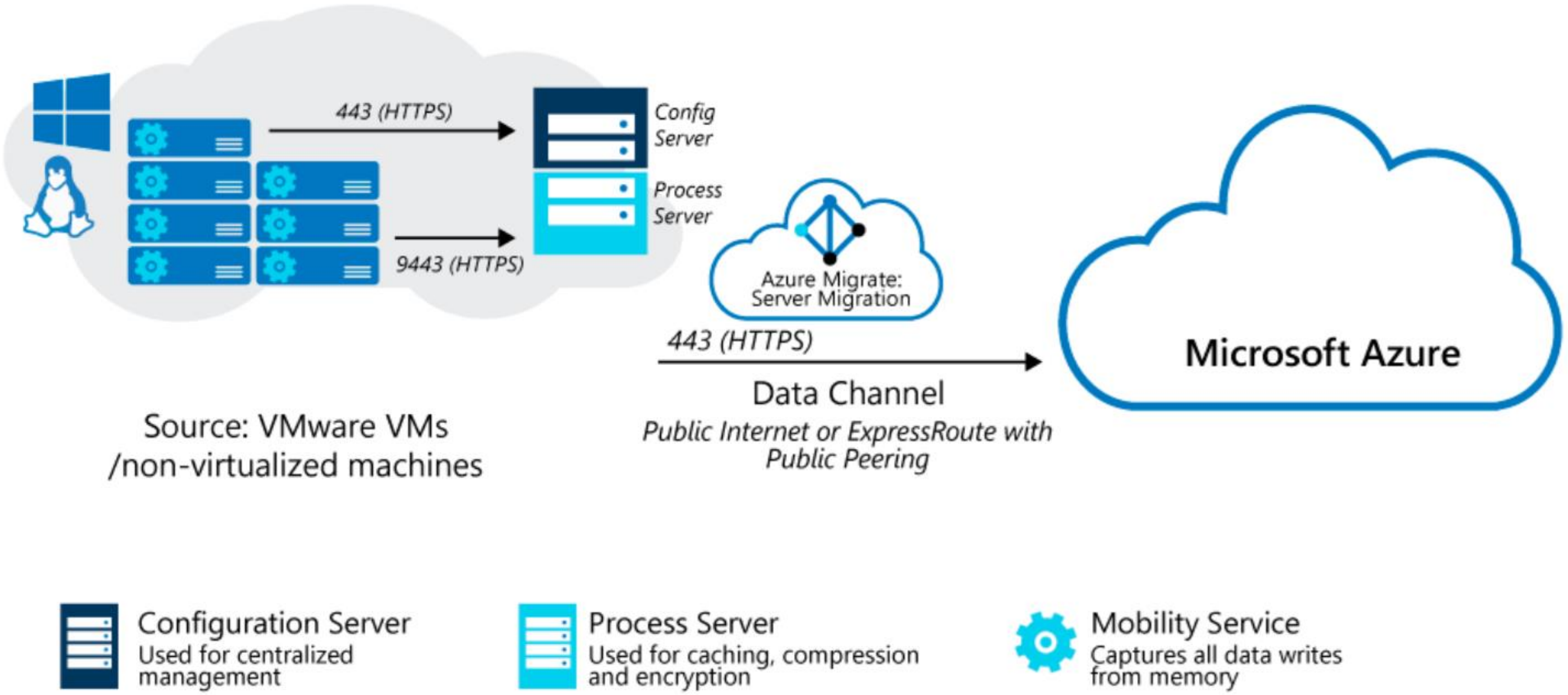
It handles data replication. It works with the provider to replicate data from Hyper-V VMs to Azure.

Agent-Based Migration Architecture

The following diagram shows the architecture of agent-based migration:

Core requirements

- Configuration VM
- ESXi hosts > v5.5
- Permissions
- VM Requirements
- Mobility Service
- Azure Storage



443 (HTTPS)
Config Server
Process Server
9443 (HTTPS)
Azure Migrate: Server Migration
443 (HTTPS)
Microsoft Azure
Data Channel
Public Internet or ExpressRoute with Public Peering
Source: VMware VMs /non-virtualized machines
Configuration Server
Used for centralized management
Process Server
Used for caching, compression and encryption
Mobility Service
Captures all data writes from memory

Azure Backup for Workloads

Overview of Microsoft Azure Backup

Microsoft Azure Backup service offers simple and reliable backup and protection for critical data in an easily recoverable way, from any location.

Reliable offsite data protectionz

- Convenient offsite protection
- Safe data
- Encrypted backups

A Simple and integrated solution

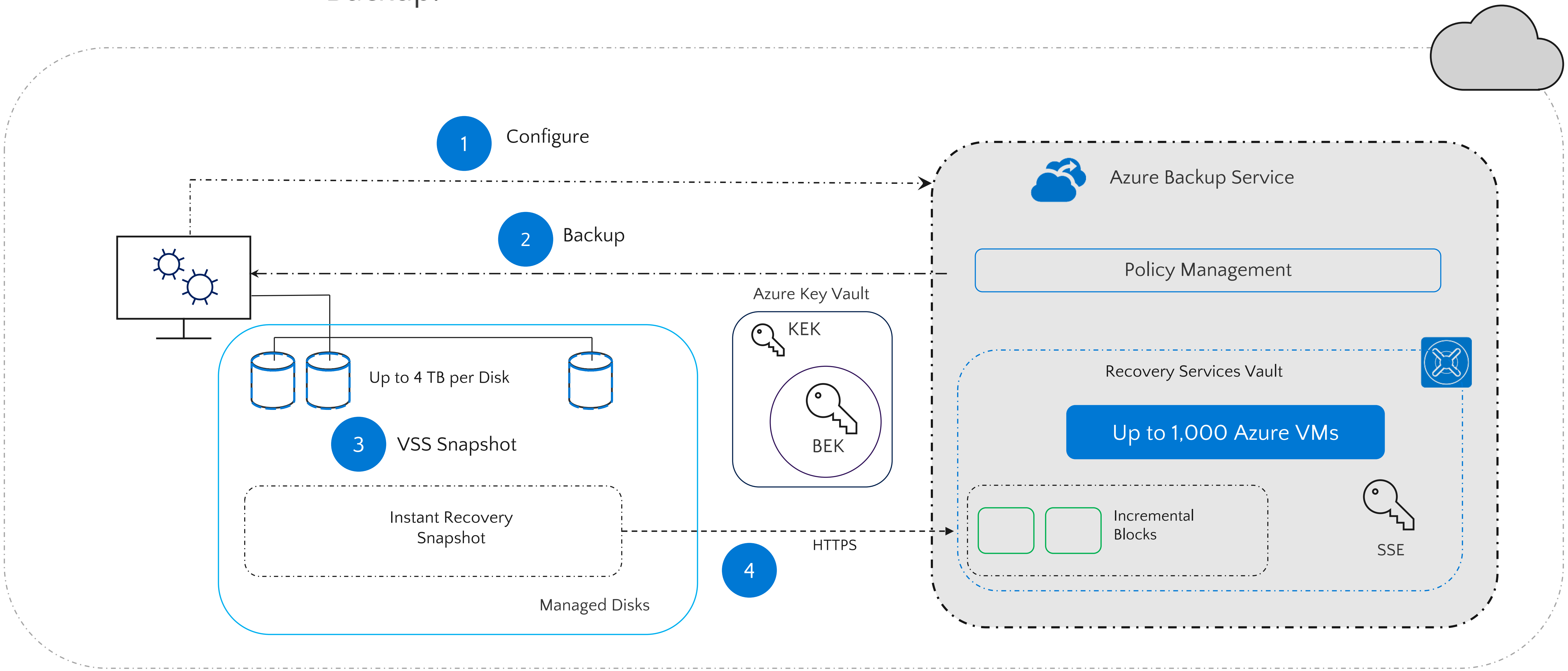
- Familiar interface
- Azure integration

Efficient backup and recovery

- Efficient use of bandwidth and storage
- Flexible configuration
- Flexibility in recovery
- Cost-effective and metered by usage

Azure VM Backup Architecture

The following diagram shows the architecture of Azure VM Backup:



Azure Backup

The features of Azure Backup are:

Simple configuration and management

Block-level incremental backups

Data integrity verified in the cloud

Configurable retention policies

- 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

Azure Backup

The following are the features of Azure Backup:

Simple configuration and management

Block-level incremental backups

Data integrity verified in the cloud

Configurable retention policies

- Automatic incremental backups to track file and block level changes
- Different point-in-time versions of backups use storage efficiently by only storing the changed blocks between these versions

Azure Backup

The following are the features of Azure Backup:

Simple configuration and management

Block level incremental backups

Data integrity verified in the cloud

Configurable retention policies

- Backed up data is automatically checked for integrity once the backup is complete.
- Any corruptions due to data transfer are automatically identified and repair is attempted in the next backup.

Azure Backup

The following are the features of Azure Backup:

Simple configuration and management

Block level incremental backups

Data integrity verified in the cloud

Configurable retention policies

- Retention policies are used to control how long a backup is saved in Azure.
- This helps to comply with business policies and manage backup costs.

Azure IaaS Backup Components

The backup components and details of Azure IaaS are as follows:

Component	Benefits	Limits	Protected	Backups stored
Azure Backup Server (can be deployed in Azure and on-premise)	• App-aware snapshots (VSS) • Full flexibility of backup schedule • Recovery granularity (all) • Can use Recovery Services vault • Linux support on Hyper-V and VMware VMs • Backup and restore VMware VMs • Doesn't require a System Center license	• Cannot back up Oracle workload • Always requires live Azure subscription • No support for tape backup	• Files • Folders • Volumes • VMs • Applications • Workloads • System State	• Recovery Services vault • Locally attached disk

Azure IaaS Backup Components

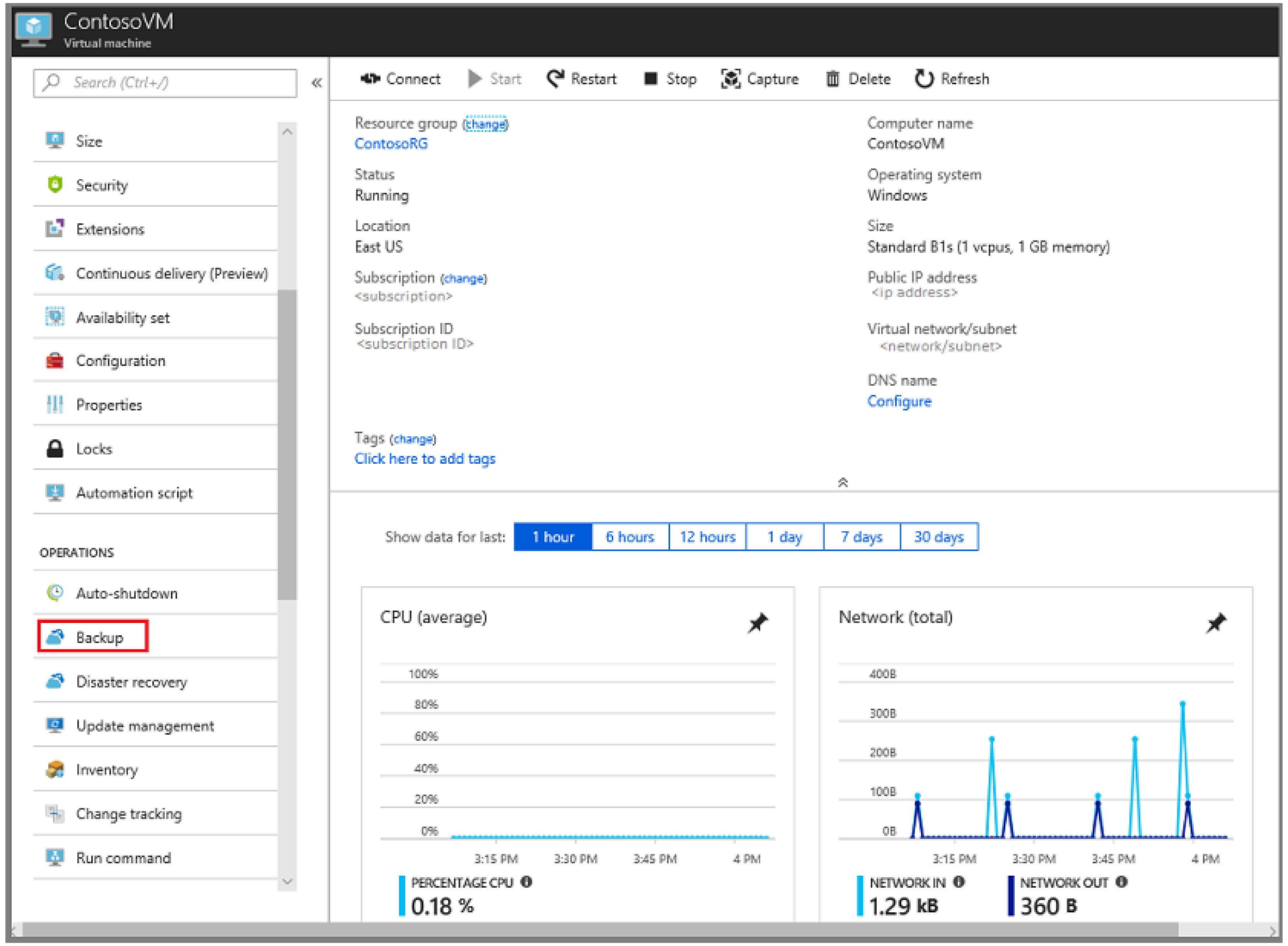
These are the backup components and its details of Azure IaaS:

Component	Benefits	Limits	Protected	Backups stored
Azure IaaS VM Backup	• Native backups for Windows/Linux • No specific agent installation required • Fabric-level backup with no backup infrastructure required	• Backup VMs once a day • Restore VMs only at disk level • Cannot back up on-premise	• VMs, • All disks (using PowerShell)	• Recovery Services vault

Overview of Recovery Services Vault

A Recovery Services vault is a storage entity in Azure that contains data.

- It Secures backed up data
- It Provides central monitoring
- Role Based Access Control restricts backup and restore access to the defined set of user roles



ContosoVM
Virtual machine

Resource group (change)
ContosoRG

Status
Running

Location
East US

Subscription (change)
<subscription>

Subscription ID
<subscription ID>

Tags (change)
Click here to add tags

Computer name
ContosoVM

Operating system
Windows

Size
Standard B1s (1 vcpus, 1 GB memory)

Public IP address
<ip address>

Virtual network/subnet
<network/subnet>

DNS name
Configure

Show data for last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

PERCENTAGE CPU
0.18 %

NETWORK IN
1.29 kB

NETWORK OUT
360 B

Powerd by simplilearn

Caltech Center for Technology & Management Education

Disaster Recovery

Azure to Azure Site Recovery

- Azure Site Recovery (ASR) is a disaster recovery as a service (DRaaS) solution that works in public and the hybrid cloud environments.

- It allows the user to use Azure as a disaster recovery platform on-demand, without having to purchase the disaster recovery equipment up front.

- ASR creates synchronized replicas of computer systems by using a near-real-time data replication technique.

- It creates application-consistent snapshots, ensuring that the data is accessible after a failover.

Azure to Azure Site Recovery

Azure Site Recovery provides the following features:

Features	Details
Azure VM replication	Restore Azure VMs from a primary region to a secondary region in the event of a disaster.
Workload replication	Replicate any workload that runs on Azure VMs, on-premise Hyper-V, VMware VMs and Windows/Linux physical servers.
Testing without disruption	Perform disaster recovery exercises without disrupting ongoing replication.
Azure Automation integration	Use Site Recovery with a rich Azure Automation library. Download and integrate application-specific scripts from the library.

Azure to Azure Architecture

The Azure to Azure Architecture is shown below:

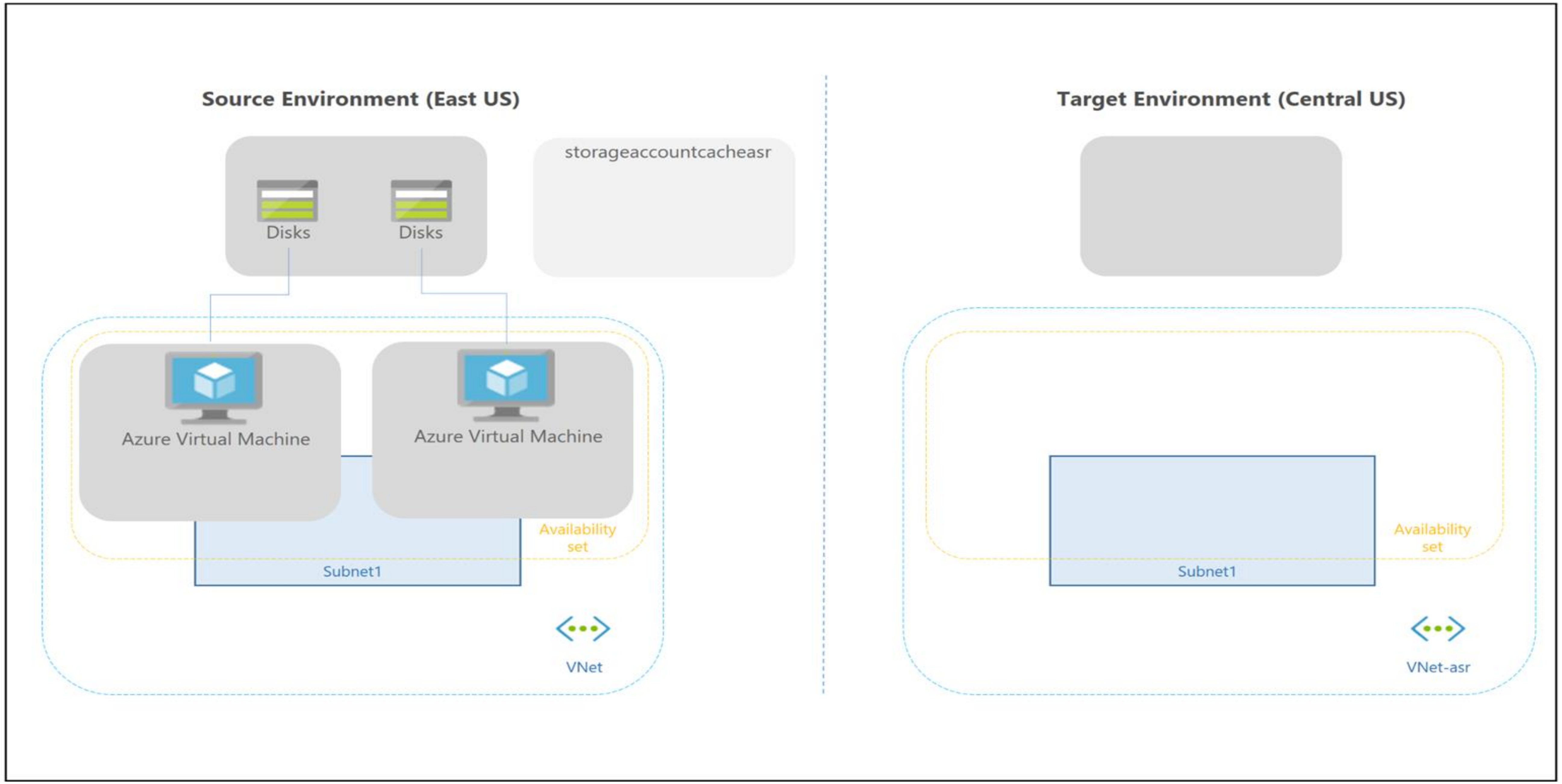


image source: https://docs.microsoft.com/en-in/

Azure to Azure Architecture

The architectural components and requirements of Azure to Azure are:

Components	Requirements
VMs in Source Region	One of more Azure VMs in a supported source region.
Source VM Storage	Non-managed disks can be distributed through storage accounts, whereas managed disks can be used in Azure VMs.
Source VM Networks	In the source field, VMs can be found in one or more subnets of a virtual network.
Cache Storage Account	Using a cache means that production applications running on a VM have minimal effects.
Target Resources	Target resources are used during replication and failover.

Azure to Azure Site Recovery: Network Traffic

- Azure to Azure Site Recovery network traffic is only outward-bound from protected VMs.
- Firewalls and network security groups (NSGs) are used to secure networks (NSGs).
- Service tags should be used to monitor network access.
- Service tags should be able to monitor outbound communication using NSGs.

Note

IP address based filtering shouldn’t be performed to control outbound connectivity.

Azure to Azure Site Recovery: Network Traffic

To control outbound connectivity by the user the following site recovery URLs must be allowed :

Features	Details
*.blob.core.widows.net	This is required so that data can be written to the cache storage account in the source region from the VM.
*.login.microsoftonline.com	This is required for authorization and authentication to the Site Recovery service URLs.
*.hypervrecoverymanager.windowsazure.com	This is required for the Site Recovery service to communicate with the VM.
*.servicebus.windows.net	This is required for the Site Recovery monitoring and diagnostics data to be written from the VM.

Azure to Azure Site Recovery: Network Traffic

To allow replication from the target region to the source region after a failover, you must:

- Create an outbound HTTPS (443) security rule for "Storage.Central US" on the NSG
- Create an outbound HTTPS (443) security rule for "Azure Active Directory" on the NSG
- Create outbound HTTPS (443) security rule for "EventHub.EastUS" on the NSG that corresponds to the source location
- Create an outbound HTTPS (443) security rule for "Azure Site Recovery" on the NSG which allows access to Site Recovery Service in any region

Azure Automation Update Management

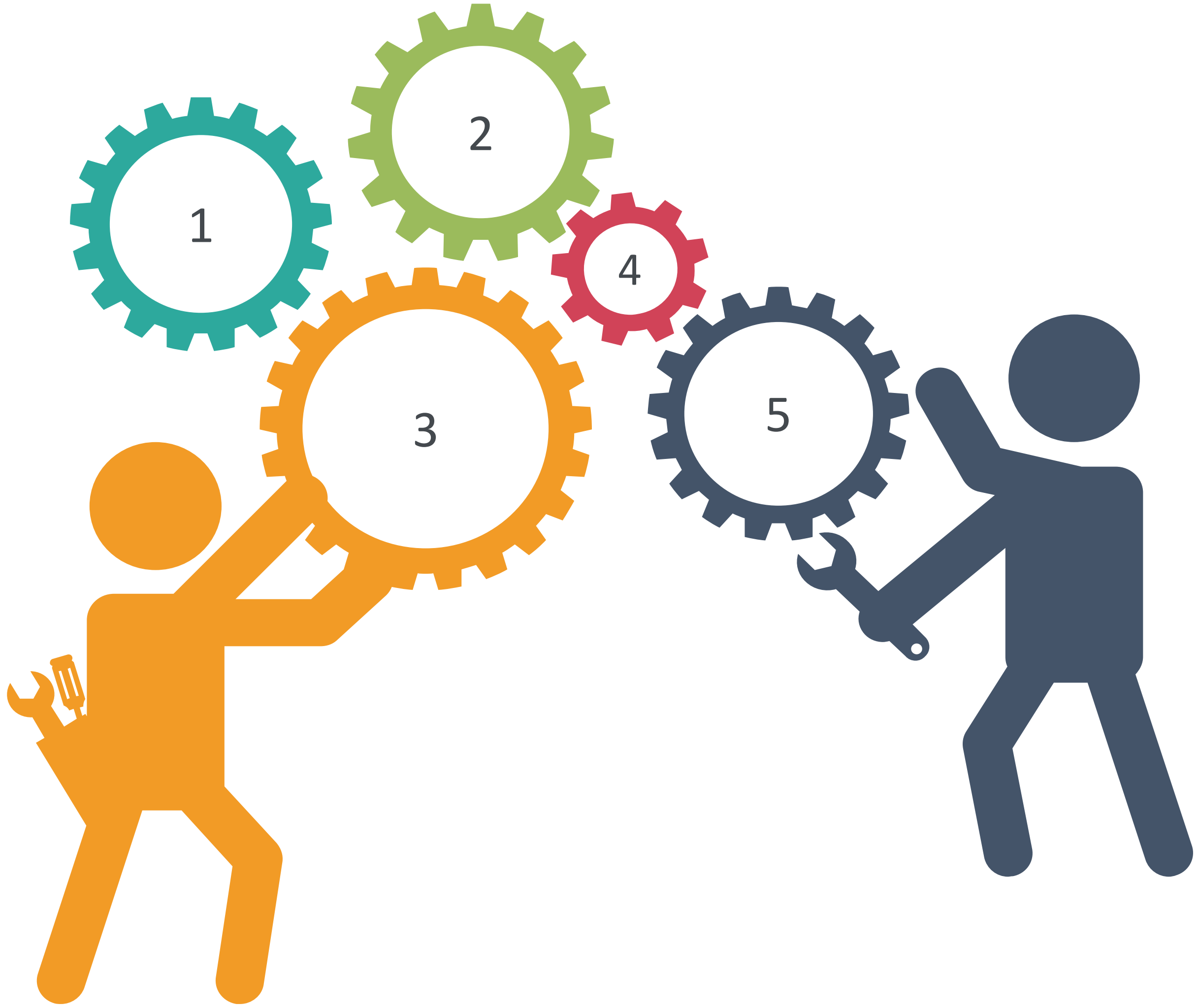
Update Management

These are the features of update management:

- It allows the user to determine the status of updates around his environment and monitor the Windows and the Linux servers both on-premise and in Azure.
- It is available at no additional cost.
- The user can easily onboard multiple machines into Update Management.

Implement Update Management: Workflow

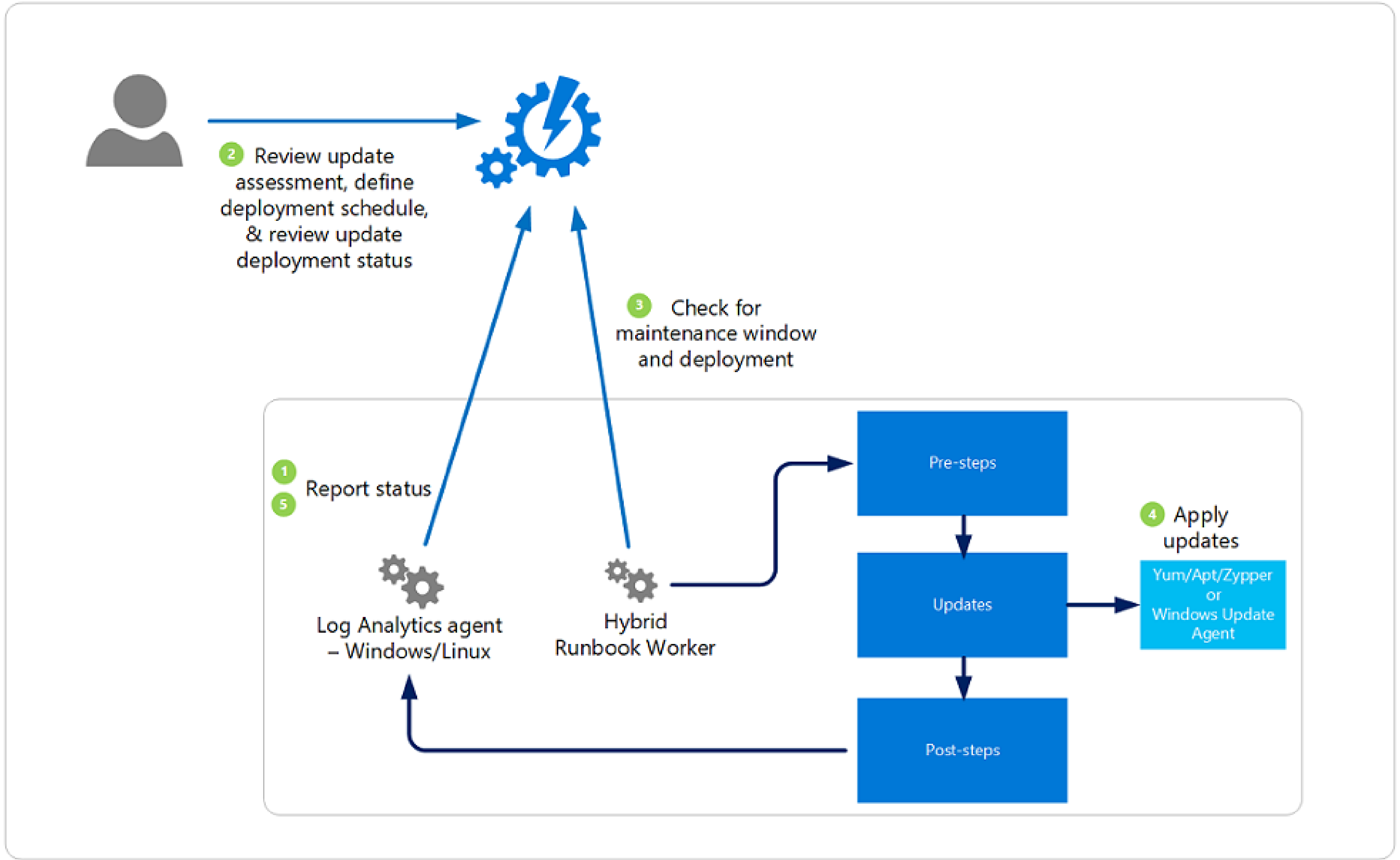
The workflow to implement Update Management is:



- Create a Log Analytics workspace
- Create an Automation account
- Link the Automation account with the Log Analytics workspace
- Enable Update Management for Azure VMs
- Enable Update Management for non-Azure VMs

Implement Update Management: Workflow

Update Management assesses and applies security updates to all related Windows Server and Linux servers in a workspace:



2 Review update assessment, define deployment schedule, & review update deployment status
3 Check for maintenance window and deployment
1
5 Report status
Log Analytics agent – Windows/Linux
Hybrid Runbook Worker
Pre-steps
Updates
Post-steps
4 Apply updates
Yum/Apt/Zypper or Windows Update Agent

image source: https://docs.microsoft.com/en-in/

Assisted Practice

Azure site recovery

Duration: 10 Min.

Problem Statement:

You are given a project to create Azure site recovery in order to implement a business continuity and disaster recovery (BCDR) strategy that keeps your data safe and your apps and workloads online, whenever planned and unplanned outages occur.

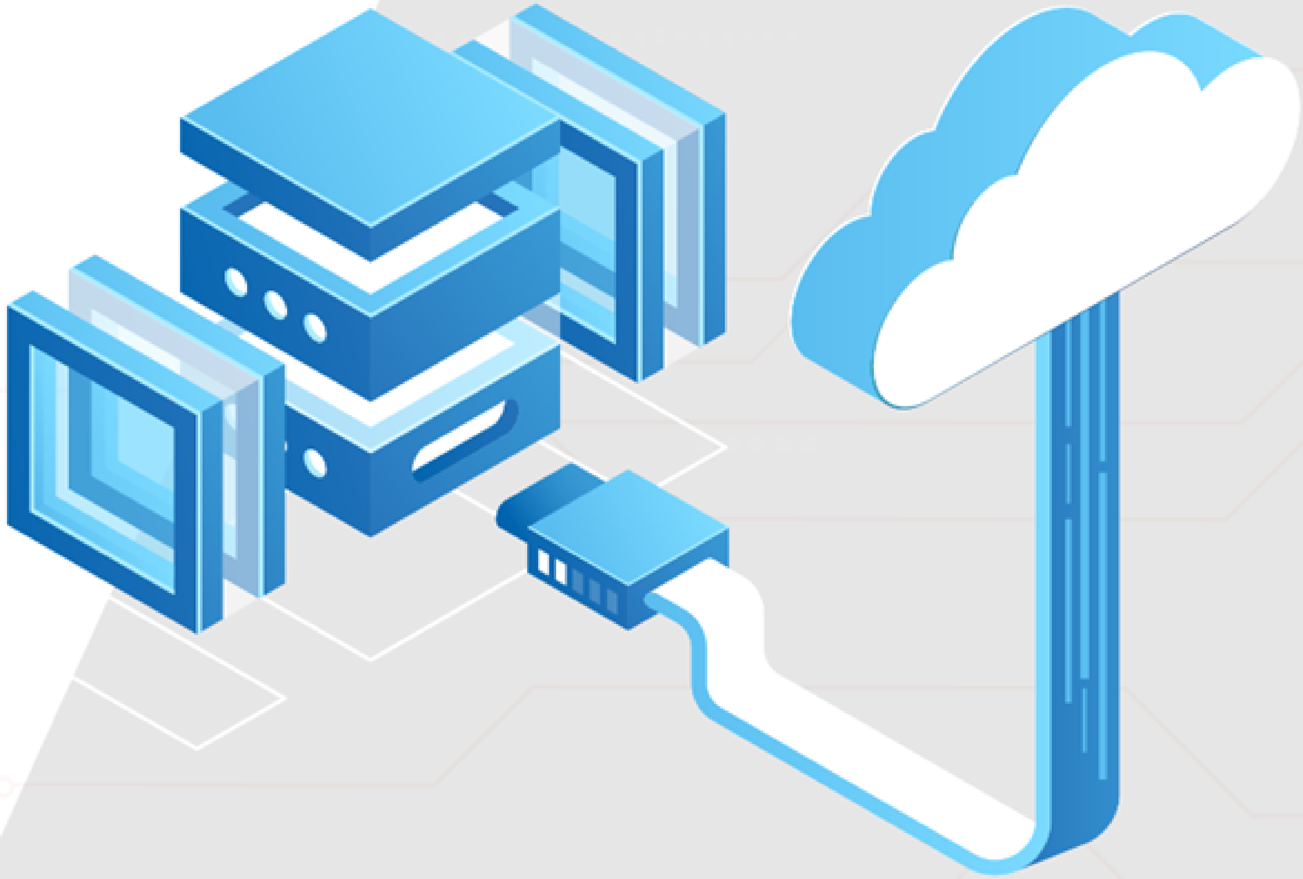
Assisted Practice: Guidelines

Steps to create Azure site recovery are:

1. Login to your Azure portal
2. Search and select recovery services vault
3. Enter details and create recovery service vault

Key Takeaways

- Azure Migrate enables planning of cloud migration.
- Microsoft Azure Backup service offers simple and reliable backup and protection for critical data.
- Azure Site Recovery is a disaster recovery as a service (DRaaS) solution that works in public and the hybrid cloud environments.
- Update Management allows the user to monitor the status updates of the environment.



Thank you