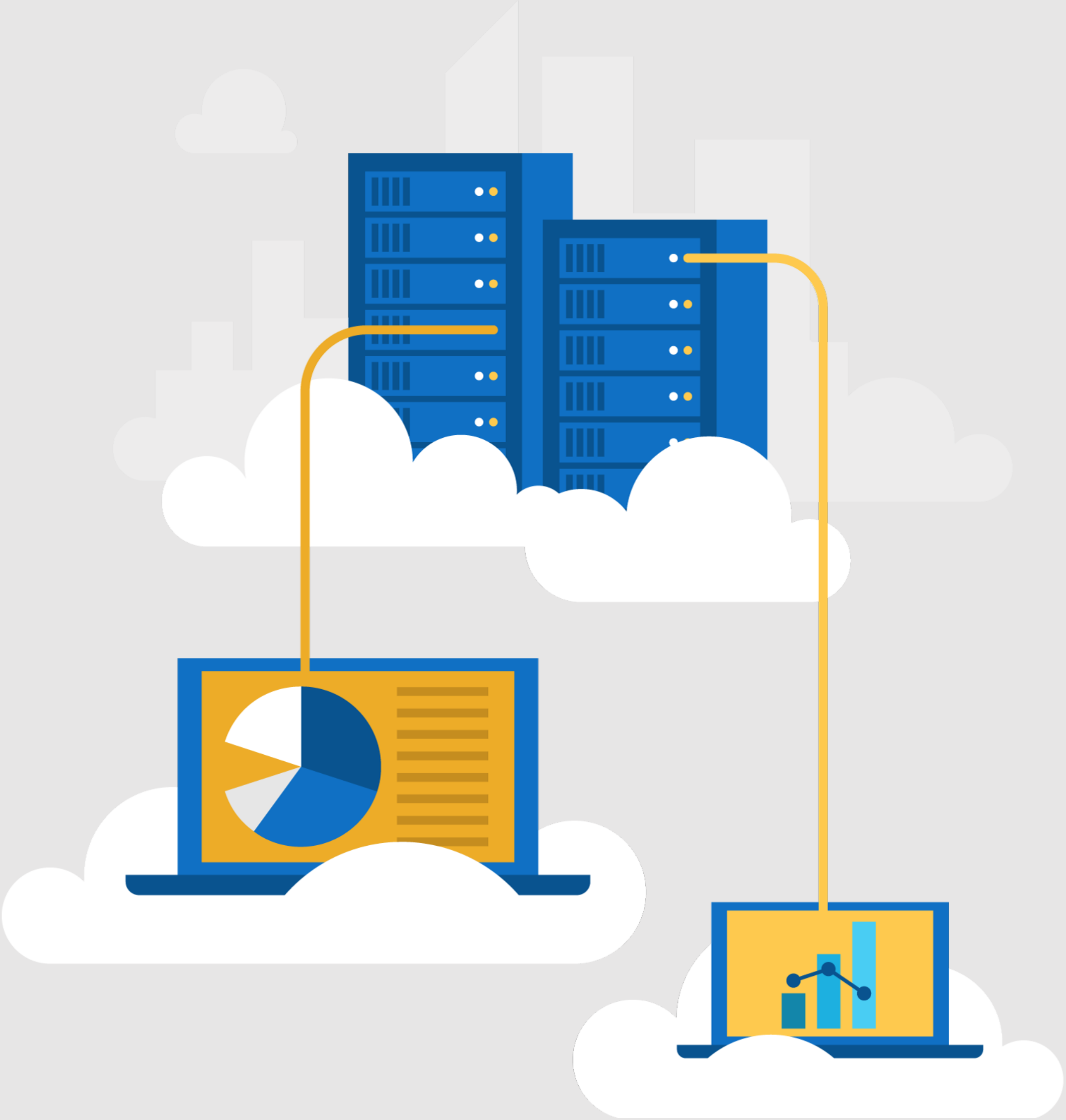
Microsoft

Azure Study Group

AZ-301 - Microsoft Azure Architect Design

Jeff Mitchell
Cloud Solution Architect



Microsoft Azure

Design a Business Continuity Strategy (15-20%)

Agenda

1. Agenda
2. Speaker Introduction
3. Feedback Loop
4. Objective Review
5. Open Mic

Series Agenda

1 Determine Workload Requirements (10-15%)

2 Design for Identity and Security (20-25%)

3 Design a Data Platform Solution (15-20%)

4 Design a Business Continuity Strategy (15-20%)

5 Design for Deployment, Migration, and Integration (10-15%)

6 Design an Infrastructure Strategy (15-20%)

https://aka.ms/azurecsg

Series Agenda

1. Determine Workload Requirements (10-15%)
2. Design for Identity and Security (20-25%)
3. Design a Data Platform Solution (15-20%)
4. Design a Business Continuity Strategy (15-20%)
5. Design for Deployment, Migration, and Integration (10-15%)
6. Design an Infrastructure Strategy (15-20%)

https://aka.ms/azurecsg

Speaker Introduction – Jeff Mitchell

- Cloud Solution Architect based in Destin, FL
- 2+ years with Microsoft, more in the industry
- This is hard. This is fun. – *Carol Dweck*
- Working on the same certifications that you are

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Feedback Loop

Objectives

Design a Site Recovery Strategy

May include but not limited to: Design a recovery solution; design a site recovery replication policy; design for site recovery capacity and for storage replication; design site failover and failback (planned/unplanned); design the site recovery network; recommend recovery objectives (e.g., Azure, on-prem, hybrid, Recovery Time Objective (RTO), Recovery Level Objective (RLO), Recovery Point Objective (RPO)); identify resources that require site recovery; identify supported and unsupported workloads; recommend a geographical distribution strategy

Design for High Availability

May include but not limited to: Design for application redundancy, autoscaling, data center and fault domain redundancy, and network redundancy; identify resources that require high availability; identify storage types for high availability

Objectives (cont.)

Design a disaster recovery strategy for individual workloads

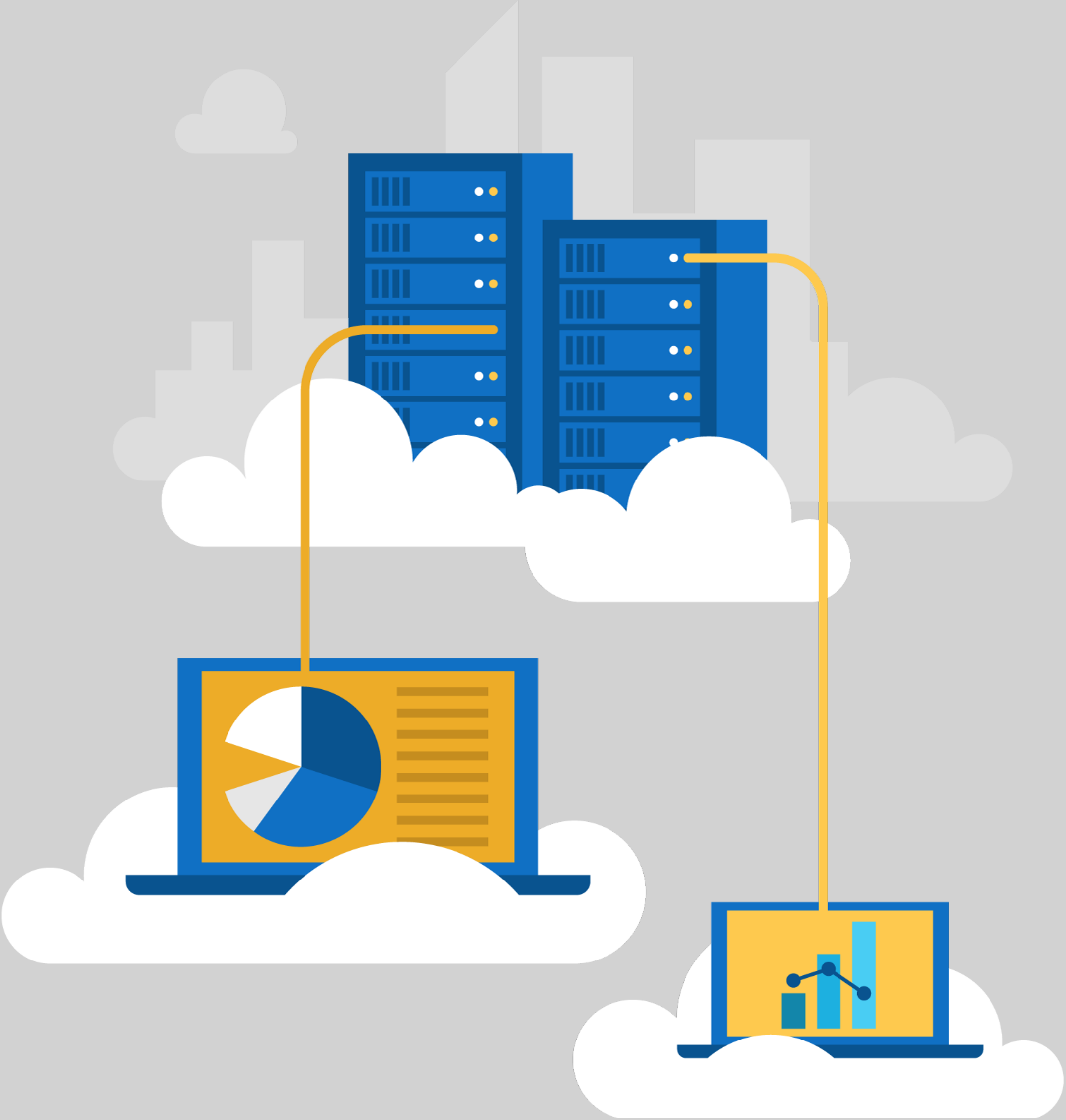
May include but not limited to: Design failover/failback scenario(s); document recovery requirements; identify resources that require backup; recommend a geographic availability strategy

Design a Data Archiving Strategy

May include but not limited to: Recommend storage types and methodology for data archiving; identify requirements for data archiving and business compliance requirements for data archiving; identify SLA(s) for data archiving

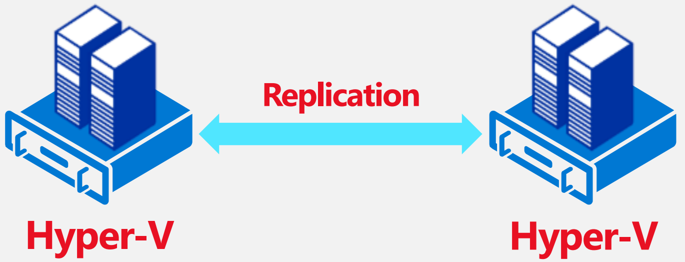
Microsoft

Design a Site Recovery Strategy

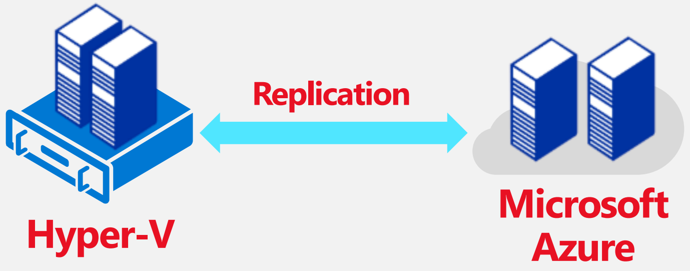


Azure Site Recovery

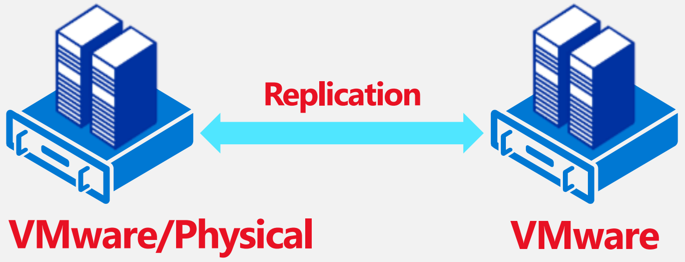
One solution for multiple infrastructures



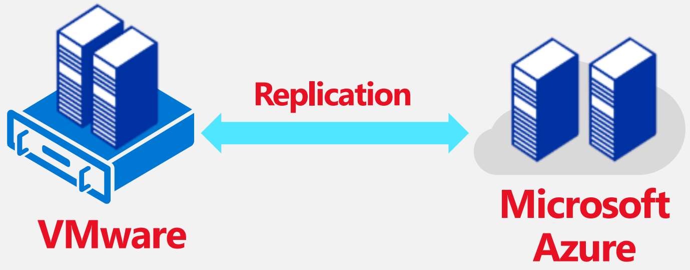
1 Hyper-V to Hyper-V (on-premises)



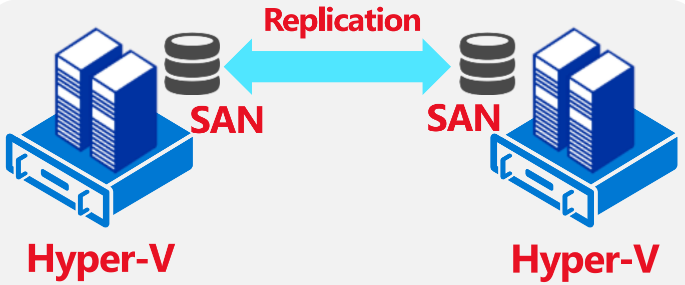
2 Hyper-V to Microsoft Azure



3 VMware or Physical to VMware (on-premises)



4 VMware or Physical to Microsoft Azure

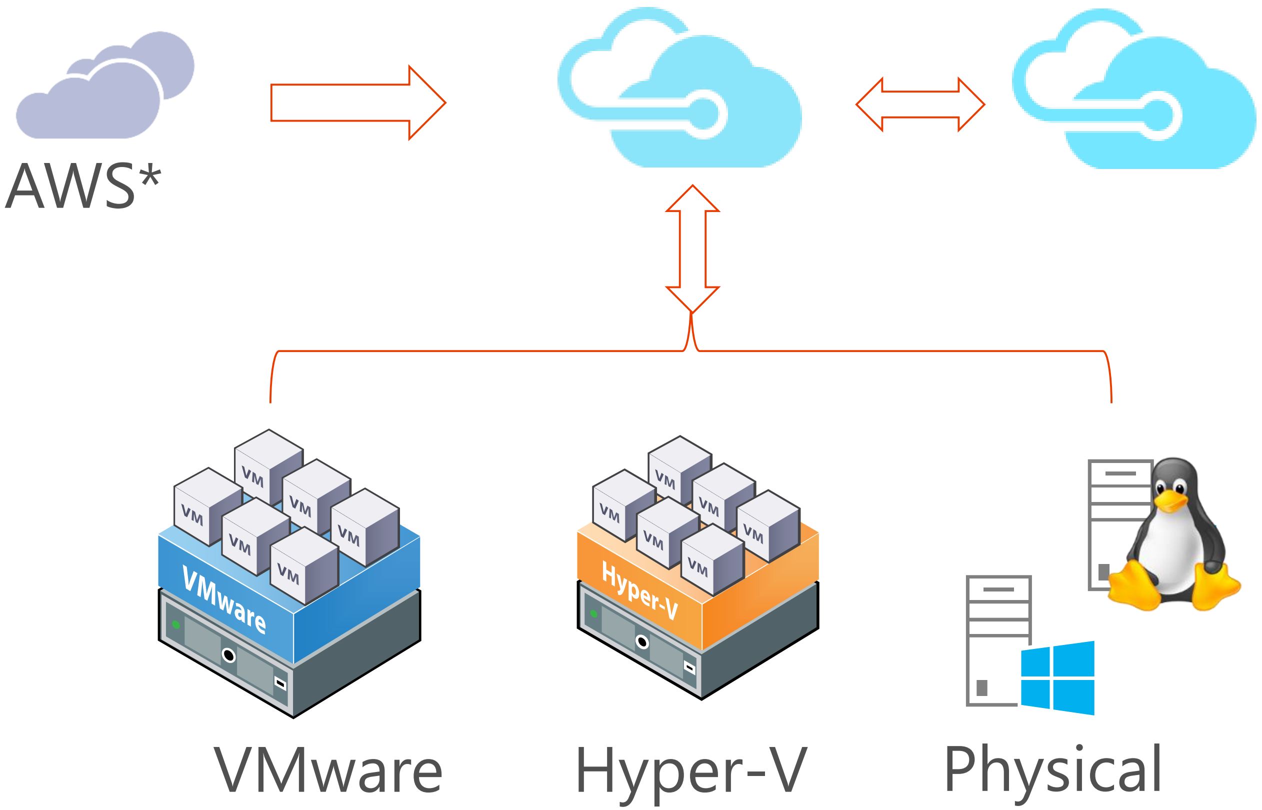


5 Hyper-V to Hyper-V (on-premises)

Protect important applications by coordinating the replication and recovery of private clouds across sites.
Protect your applications to your own second site, a hoster's site, or even use Microsoft Azure as your disaster recovery site

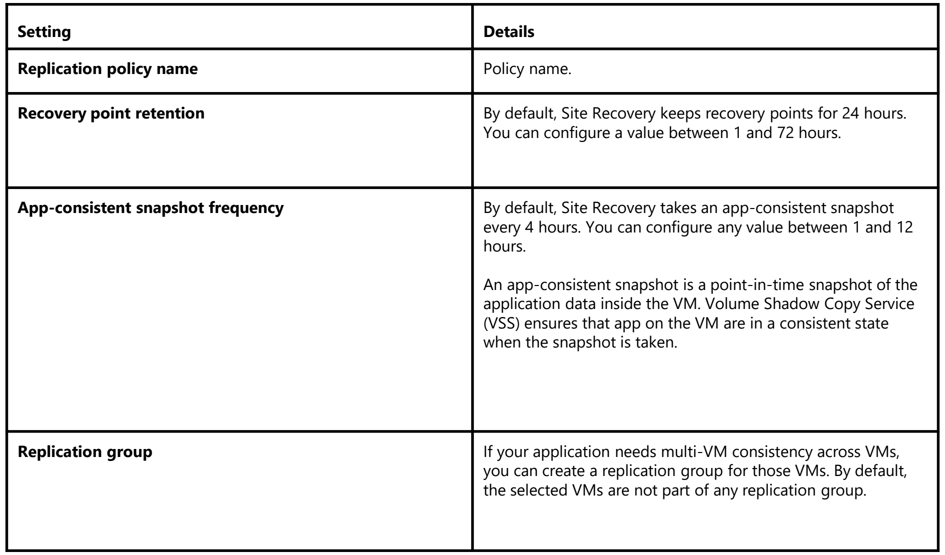
Azure Site Recovery: The Complete Disaster Recovery Solution

Site to Azure Any Cloud



What does Site Recovery Provide?

What can I replicate?



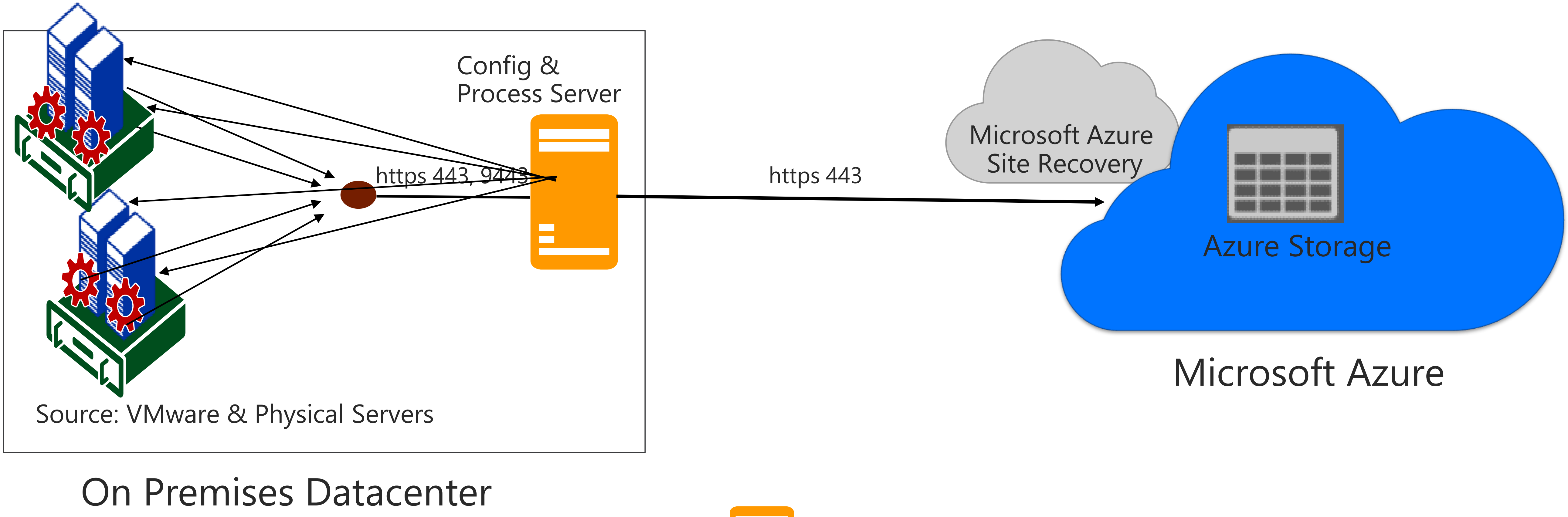
Setting	**Details**
Replication policy name	Policy name.
Recovery point retention	By default, Site Recovery keeps recovery points for 24 hours. You can configure a value between 1 and 72 hours.
App-consistent snapshot frequency	By default, Site Recovery takes an app-consistent snapshot every 4 hours. You can configure any value between 1 and 12 hours. An app-consistent snapshot is a point-in-time snapshot of the application data inside the VM. Volume Shadow Copy Service (VSS) ensures that app on the VM are in a consistent state when the snapshot is taken.
Replication group	If your application needs multi-VM consistency across VMs, you can create a replication group for those VMs. By default, the selected VMs are not part of any replication group.

Windows Any OS Linux

Migration Solutions Matrix

Source	Target	Availability	Supported Guest OS Types
Hyper-V 2012 R2	Azure	Available	All Guest OS types supported by Azure
Hyper-V 2008 R2 SP1 and 2012	Azure	Available	Windows* and Linux*
VMware vSphere 5.1, 5.5, 6.0 and Physical Servers	Azure	Available	Windows* and Linux*
Amazon Web Services (Windows AMIs)	Azure	Available	Windows Server 2008 R2 SP1+ (HVM only)
Amazon Web Services (Linux AMIs)	Azure	Available	RHEL 6.7 HVM
Hyper-V 2012	Hyper-V 2012R2	Available	All Guest OS types supported by Hyper-V
VMware vSphere 5.1, 5.5, 6.0	Hyper-V 2012R2	Available via Microsoft Services Global Delivery	Windows Server 2008 R2 SP1+

Migrate or Replicate VMware and Physical Servers to Azure



Config & Process Server – Used for Caching, Compression, Encryption & Management

Mobility Service – Captures all data writes from memory

Capacity Planning

Network bandwidth

- Initial replication
- Delta replication and peaks

Storage

- Replication
- Workload IOPS during failovers
- Test failover (Replication and Workload IOPS simultaneously)
- Standard or premium storage
- Storage account naming convention

Compute capacity

- Test failover to ensure necessary capacity

Capacity considerations

Component	Details
Replication	**Maximum daily change rate**: A protected machine can use only one process server. A single process server can handle a daily change rate up to 2 TB. So, 2 TB is the maximum daily data change rate that's supported for a protected machine. **Maximum throughput**: A replicated machine can belong to one storage account in Azure. A standard Azure Storage account can handle a maximum of 20,000 requests per second. We recommend that you limit the number of input/output operations per second (IOPS) across a source machine to 20,000. For example, if you have a source machine that has five disks and each disk generates 120 IOPS (8 K in size) on the source machine, the source machine is within the Azure per-disk IOPS limit of 500. (The number of storage accounts required is equal to the total source machine IOPS divided by 20,000.)
Configuration server	The configuration server must be able to handle the daily change rate capacity across all workloads running on protected machines. The configuration machine must have sufficient bandwidth to continuously replicate data to Azure Storage. A best practice is to place the configuration server on the same network and LAN segment as the machines that you want to protect. You can place the configuration server on a different network, but machines that you want to protect should have layer 3 network visibility. Size recommendations for the configuration server are summarized in the table in the following section.
Process server	The first process server is installed by default on the configuration server. You can deploy additional process servers to scale your environment. The process server receives replication data from protected machines. The process server optimizes data by using caching, compression, and encryption. Then, the process server sends the data to Azure. The process server machine must have sufficient resources to perform these tasks. The process server uses a disk-based cache. Use a separate cache disk of 600 GB or more to handle data changes that are stored if a network bottleneck or outage occurs.

Firewall Rules

- All ASR scenarios require access to following URLs
  - *.hypervrecoverymanager.windowsazure.com
  - *.accesscontrol.windows.net
  - *.backup.windowsazure.com
  - *.blob.core.windows.net
  - *.store.core.windows.net
- All communication happens on https (443)
- IP address based firewall rules can be created by opening up Azure Datacenter IP Ranges for the region of recovery services vault and for WUS
  - IP range can change therefore it is not recommended to use IP based firewall rules
- VMware Network Interfaces, and IP addressing Failover
- NSG Rules

Create and customize recovery plans

Recovery time objective (RTO) is the maximum acceptable time that an application can be unavailable after an incident. If your RTO is 90 minutes, you must be able to restore the application to a running state within 90 minutes from the start of a disaster. If you have a very low RTO, you might keep a second regional deployment continually running an active/passive configuration on standby, to protect against a regional outage.

In some cases you might deploy an active/active configuration to achieve even lower RTO.

Recovery point objective (RPO) is the maximum duration of data loss that is acceptable during a disaster.

For example, if you store data in a single database, with no replication to other databases, and perform hourly backups, you could lose up to an hour of data.

Mean time to recover (MTTR) is the average time that it takes to restore a component after a failure.

MTTR is an empirical fact about a component. Based on the MTTR of each component, you can estimate the MTTR of an entire application. Building applications from multiple components with low MTTR values results in an application with a low overall MTTR — one that recovers quickly from failures.

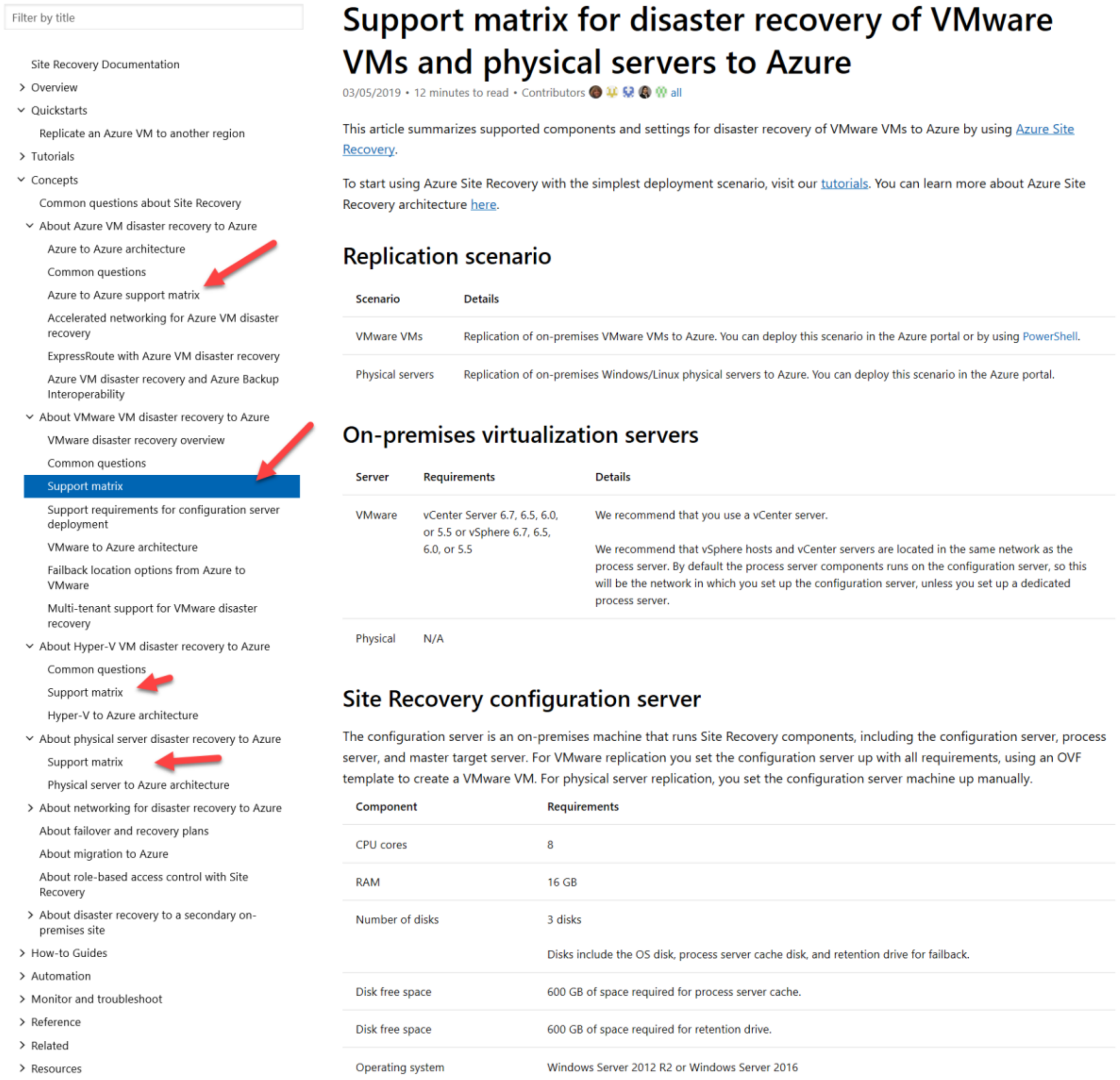
Mean time between failures (MTBF) is the runtime that a component can reasonably expect to last between outages. This metric can help you to calculate how frequently a service will become unavailable.

An unreliable component has a low MTBF, resulting in a low SLA number for that component.

However, a low MTBF can be mitigated by deploying multiple instances of the component and implementing failover between them.

Support matrix

Resource Support
Region Support
OS Support
Compute settings for replicated VM
Service Limits


Filter by title
Site Recovery Documentation
Overview
Quickstarts
Replicate an Azure VM to another region
Tutorials
Concepts
Common questions about Site Recovery
About Azure VM disaster recovery to Azure
Azure to Azure architecture
Common questions
Azure to Azure support matrix
Accelerated networking for Azure VM disaster recovery
ExpressRoute with Azure VM disaster recovery
Azure VM disaster recovery and Azure Backup Interoperability
About VMware VM disaster recovery to Azure
VMware disaster recovery overview
Common questions
Support matrix
Support requirements for configuration server deployment
VMware to Azure architecture
Failback location options from Azure to VMware
Multi-tenant support for VMware disaster recovery
About Hyper-V VM disaster recovery to Azure
Common questions
Support matrix
Hyper-V to Azure architecture
About physical server disaster recovery to Azure
Support matrix
Physical server to Azure architecture
About networking for disaster recovery to Azure
About failover and recovery plans
About migration to Azure
About role-based access control with Site Recovery
About disaster recovery to a secondary on-premises site
How-to Guides
Automation
Monitor and troubleshoot
Reference
Related
Resources

Support matrix for disaster recovery of VMware VMs and physical servers to Azure

03/05/2019 • 12 minutes to read • Contributors all

This article summarizes supported components and settings for disaster recovery of VMware VMs to Azure by using Azure Site Recovery.

To start using Azure Site Recovery with the simplest deployment scenario, visit our tutorials. You can learn more about Azure Site Recovery architecture here.

Replication scenario

Scenario	Details
VMware VMs	Replication of on-premises VMware VMs to Azure. You can deploy this scenario in the Azure portal or by using PowerShell.
Physical servers	Replication of on-premises Windows/Linux physical servers to Azure. You can deploy this scenario in the Azure portal.

On-premises virtualization servers

Server	Requirements	Details
VMware	vCenter Server 6.7, 6.5, 6.0, or 5.5 or vSphere 6.7, 6.5, 6.0, or 5.5	We recommend that you use a vCenter server. We recommend that vSphere hosts and vCenter servers are located in the same network as the process server. By default the process server components runs on the configuration server, so this will be the network in which you set up the configuration server, unless you set up a dedicated process server.
Physical	N/A	

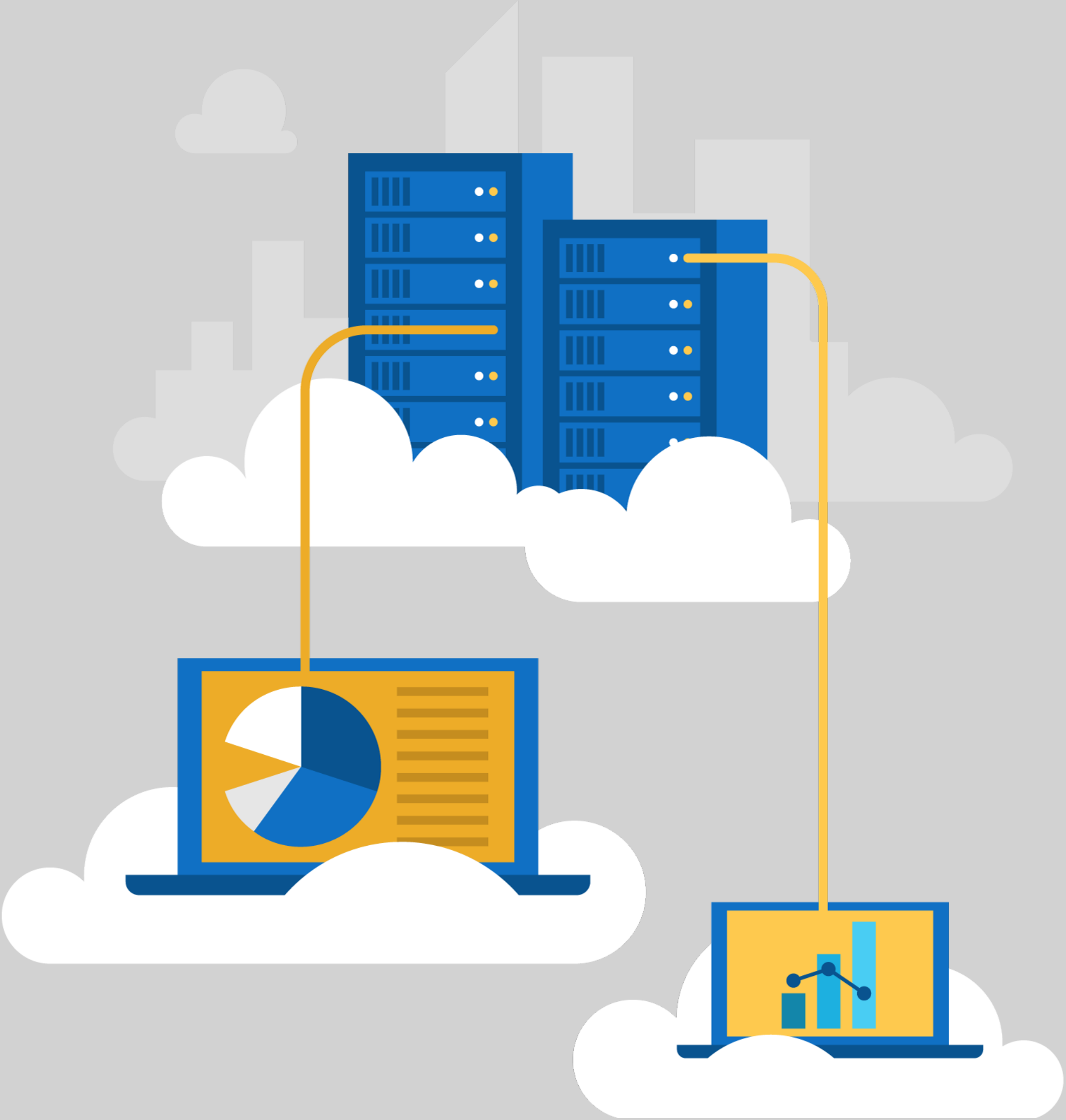
Site Recovery configuration server

The configuration server is an on-premises machine that runs Site Recovery components, including the configuration server, process server, and master target server. For VMware replication you set the configuration server up with all requirements, using an OVF template to create a VMware VM. For physical server replication, you set the configuration server machine up manually.

Component	Requirements
CPU cores	8
RAM	16 GB
Number of disks	3 disks Disks include the OS disk, process server cache disk, and retention drive for failback.
Disk free space	600 GB of space required for process server cache.
Disk free space	600 GB of space required for retention drive.
Operating system	Windows Server 2012 R2 or Windows Server 2016

Microsoft

Design for High Availability



Microsoft Azure

Azure Resiliency checklists-General, Azure Serices

Configure autoscaling for an Azure solution

Azure provides built-in autoscaling for most compute options.

- **Virtual Machines** support autoscaling through the use of VM Scale Sets, which are a way to manage a set of Azure virtual machines as a group. See How to use automatic scaling and Virtual Machine Scale Sets.
- **Service Fabric** also supports auto-scaling through VM Scale Sets. Every node type in a Service Fabric cluster is set up as a separate VM scale set. That way, each node type can be scaled in or out independently. See Scale a Service Fabric cluster in or out using auto-scale rules.
- **Azure App Service** has built-in autoscaling. Autoscale settings apply to all of the apps within an App Service. See Scale instance count manually or automatically.
- **Azure Cloud Services** has built-in autoscaling at the role level. See How to configure auto scaling for a Cloud Service in the portal.

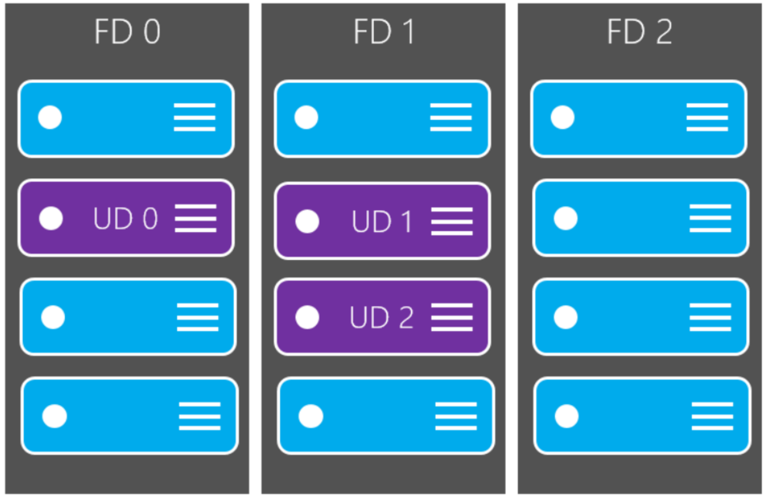
These compute options all use Azure Monitor autoscale to provide a common set of autoscaling functionality.

- **Azure Functions** differs from the previous compute options, because you don't need to configure any autoscale rules. Instead, Azure Functions automatically allocates compute power when your code is running, scaling out as necessary to handle load. For more information, see Choose the correct hosting plan for Azure Functions.

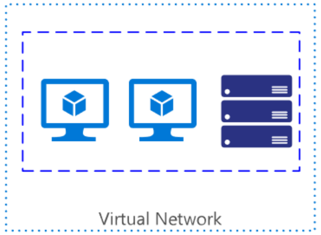
Finally, a custom autoscaling solution can sometimes be useful. For example, you could use Azure diagnostics and application-based metrics, along with custom code to monitor and export the application metrics. Then you could define custom rules based on these metrics, and use Resource Manager REST APIs to trigger autoscaling. However, a custom solution is not simple to implement, and should be considered only if none of the previous approaches can fulfill your requirements.

Use the built-in autoscaling features of the platform, if they meet your requirements. If not, carefully consider whether you really need more complex scaling features. Examples of additional requirements may include more granularity of control, different ways to detect trigger events for scaling, scaling across subscriptions, and scaling other types of resources.

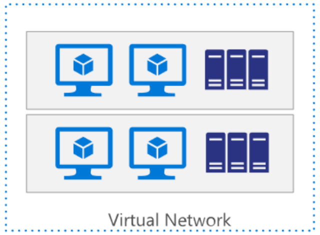
SLA	Downtime per week	Downtime per month	Downtime per year
99%	1.68 hours	7.2 hours	3.65 days
99.9%	10.1 minutes	43.2 minutes	8.76 hours
99.95%	5 minutes	21.6 minutes	4.38 hours
99.99%	1.01 minutes	4.32 minutes	52.56 minutes
99.999%	6 seconds	25.9 seconds	5.26 minutes



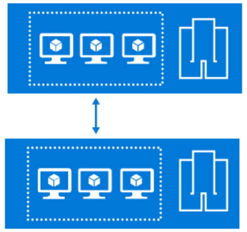
Availability Set



Availability Zones

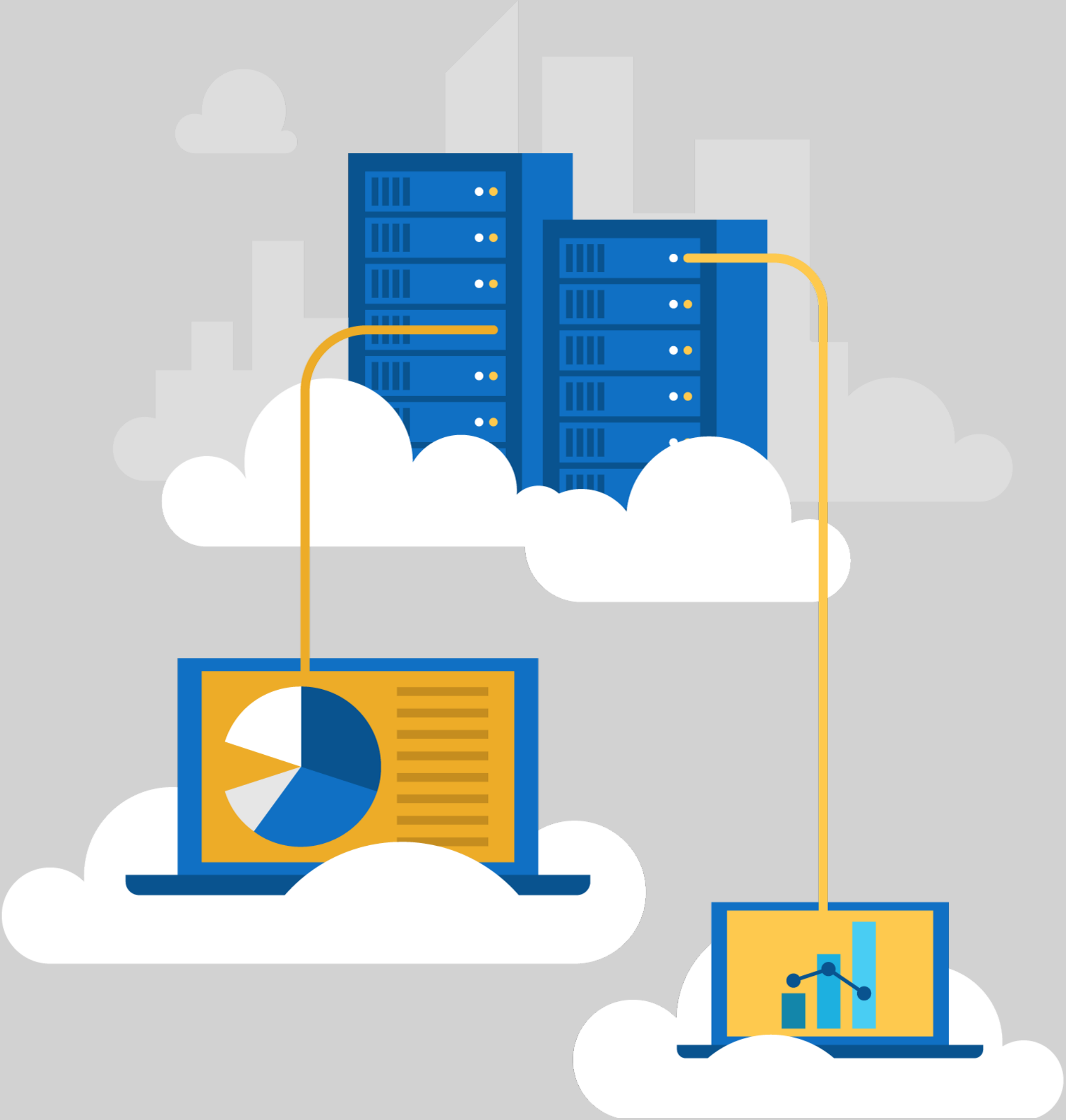


Paired Regions



Microsoft

Design a disaster recovery strategy for individual workloads

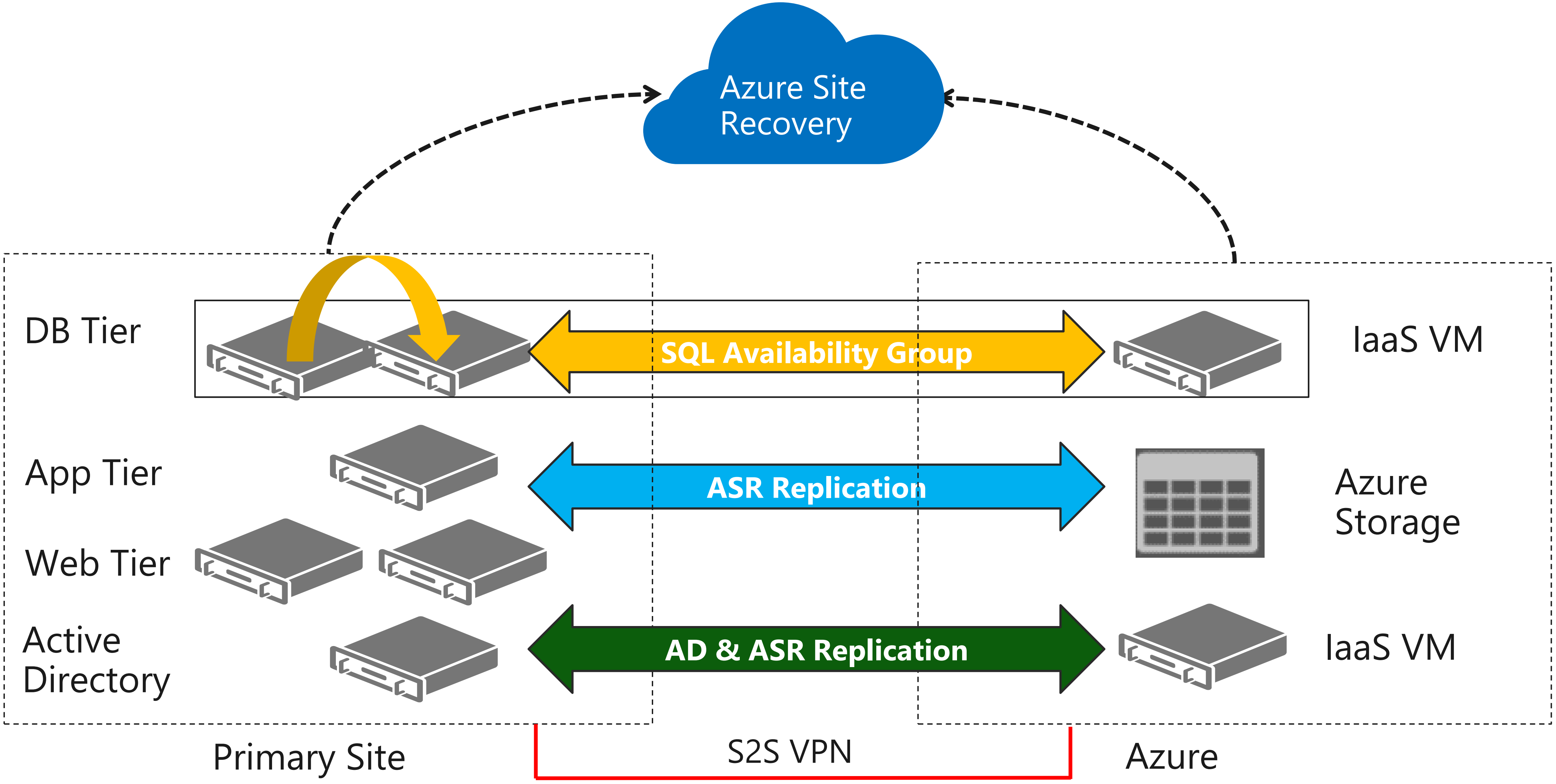


Workload summary

Site Recovery can replicate any app running on a supported machine. In addition, we've partnered with product teams to carry out additional app-specific testing.

Workload	Replicate Azure VMs to Azure	Replicate Hyper-V VMs to a secondary site	Replicate Hyper-V VMs to Azure	Replicate VMware VMs to a secondary site	Replicate VMware VMs to Azure
Active Directory, DNS	Y	Y	Y	Y	Y
Web apps (IIS, SQL)	Y	Y	Y	Y	Y
System Center Operations Manager	Y	Y	Y	Y	Y
SharePoint	Y	Y	Y	Y	Y
SAP Replicate SAP site to Azure for non-cluster	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Exchange (non-DAG)	Y	Y	Y	Y	Y
Remote Desktop/VDI	Y	Y	Y	Y	Y
Linux (operating system and apps)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Dynamics AX	Y	Y	Y	Y	Y
Windows File Server	Y	Y	Y	Y	Y
Citrix XenApp and XenDesktop	Y	N/A	Y	N/A	Y

Migrate Applications to Azure



Site Recovery Application Support

SharePoint

Exchange

Microsoft Dynamics AX

Microsoft SQL Server

Microsoft System Center Operations Manager

SAP

Active Directory | IIS | RDS/VDI | File Server

ORACLE

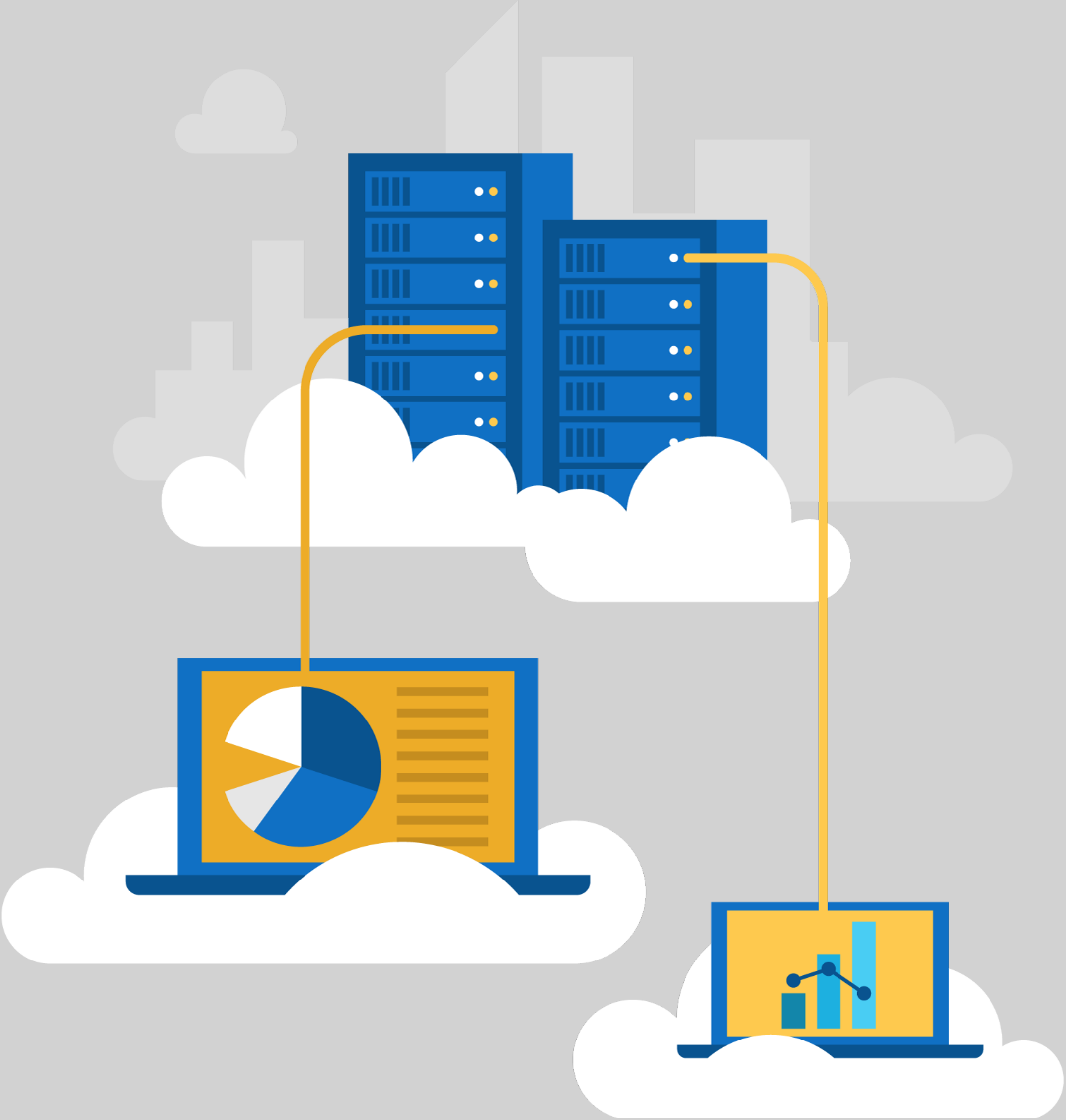
Disaster Recovery Solution backed by Microsoft Support for Microsoft Applications

For SA Customers: **Zero** additional license charge for DR of 1st party workloads

VSS integration, App consistent, Multi-VM consistent replication

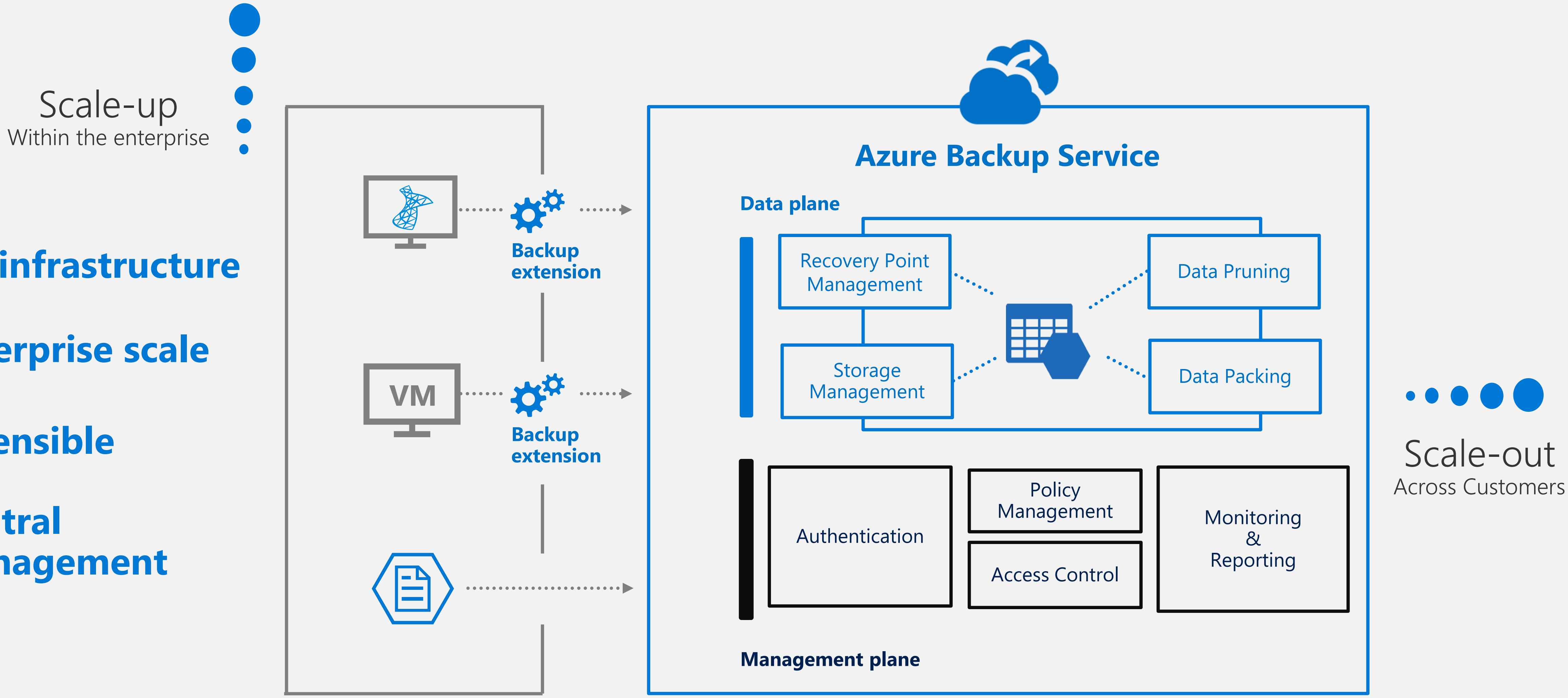
Microsoft

Design a Data Archiving Strategy

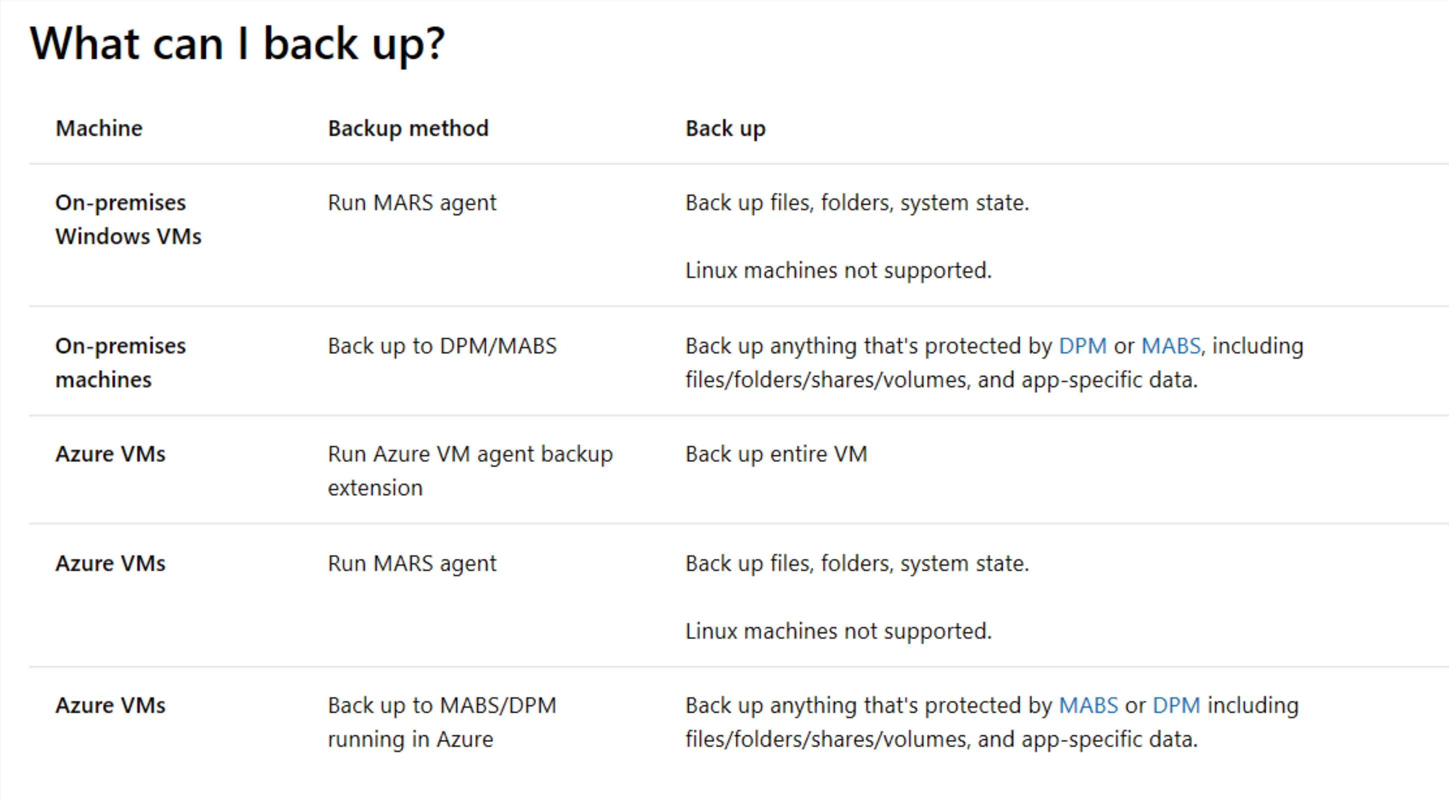


Architecture matters

- **No infrastructure**
- **Enterprise scale**
- **Extensible**
- **Central management**



Backup and Storage Tiers

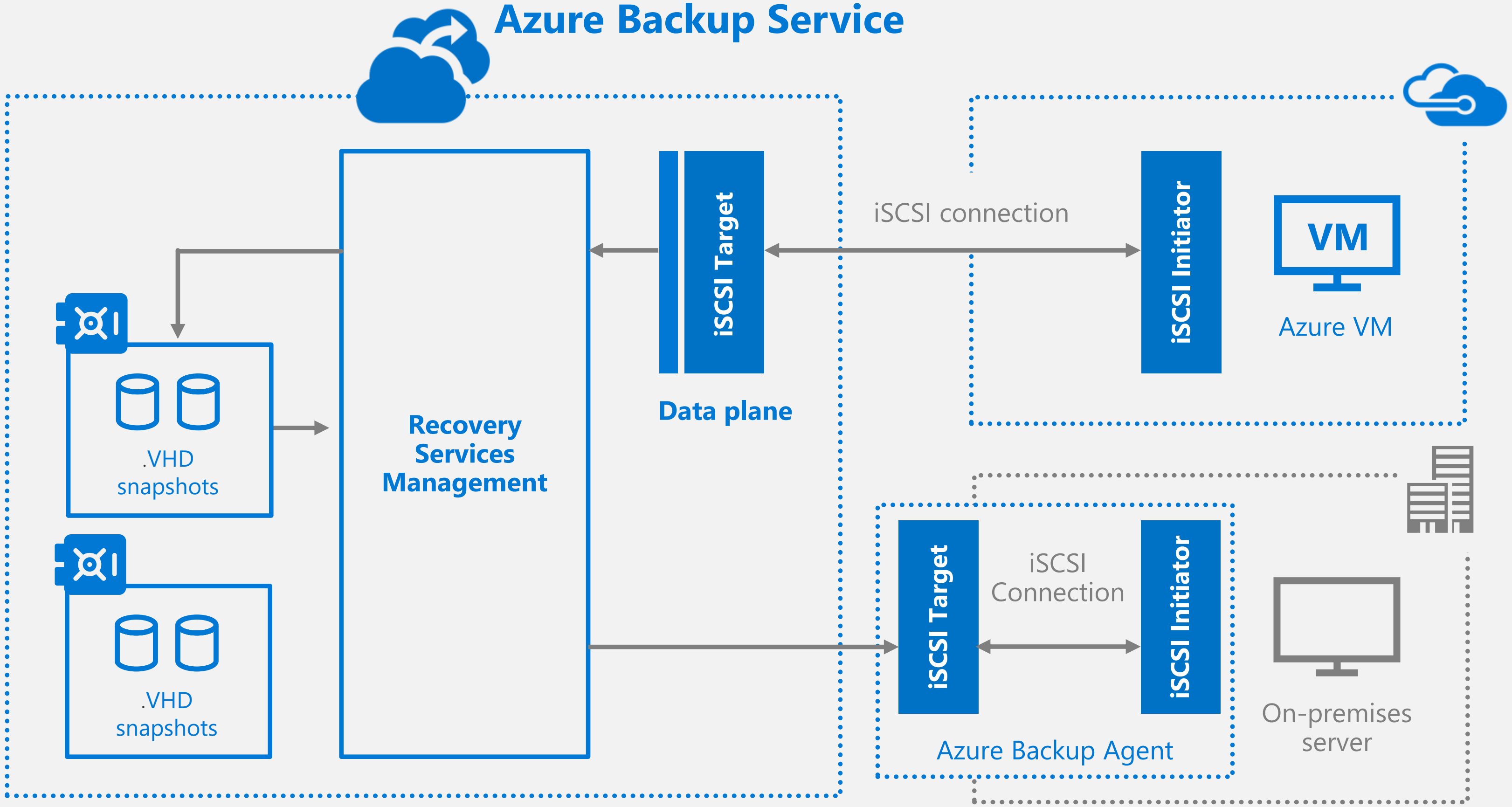


What can I back up?

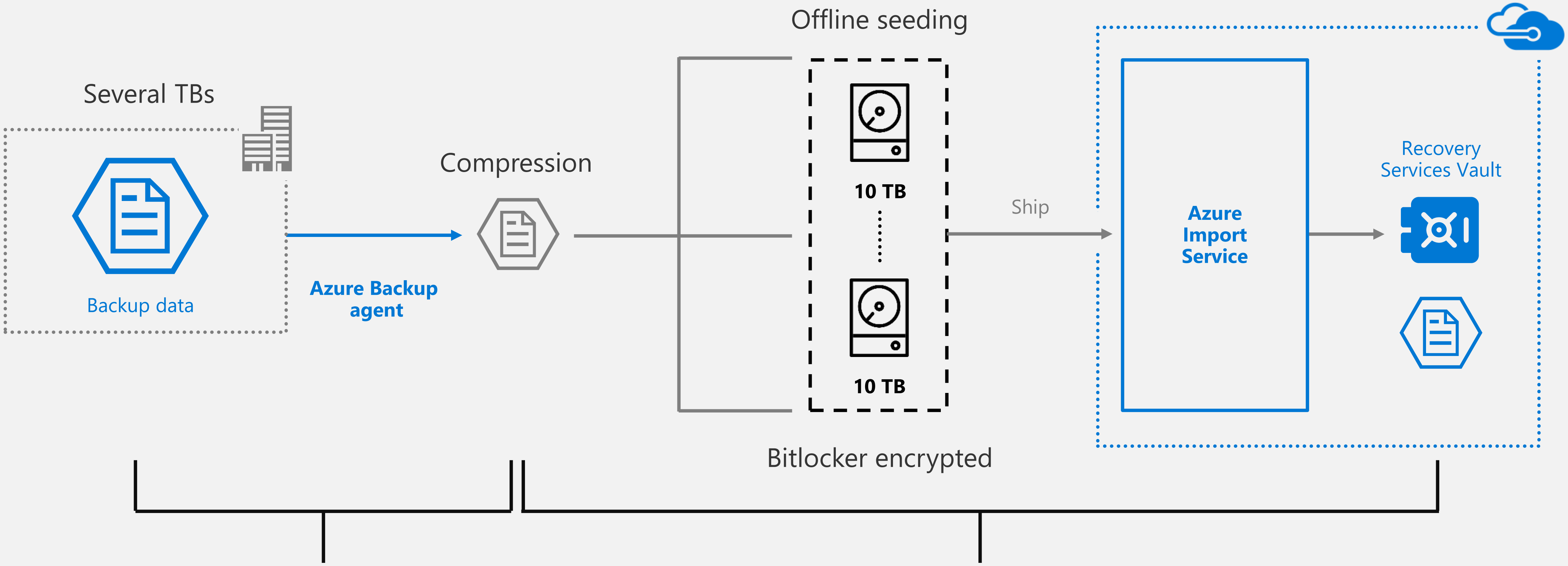
Machine	Backup method	Back up
On-premises Windows VMs	Run MARS agent	Back up files, folders, system state. Linux machines not supported.
On-premises machines	Back up to DPM/MABS	Back up anything that's protected by DPM or MABS, including files/folders/shares/volumes, and app-specific data.
Azure VMs	Run Azure VM agent backup extension	Back up entire VM
Azure VMs	Run MARS agent	Back up files, folders, system state. Linux machines not supported.
Azure VMs	Back up to MABS/DPM running in Azure	Back up anything that's protected by MABS or DPM including files/folders/shares/volumes, and app-specific data.

Restore-as-a-Service

- No infrastructure
- Inspect before restore
- Consistent



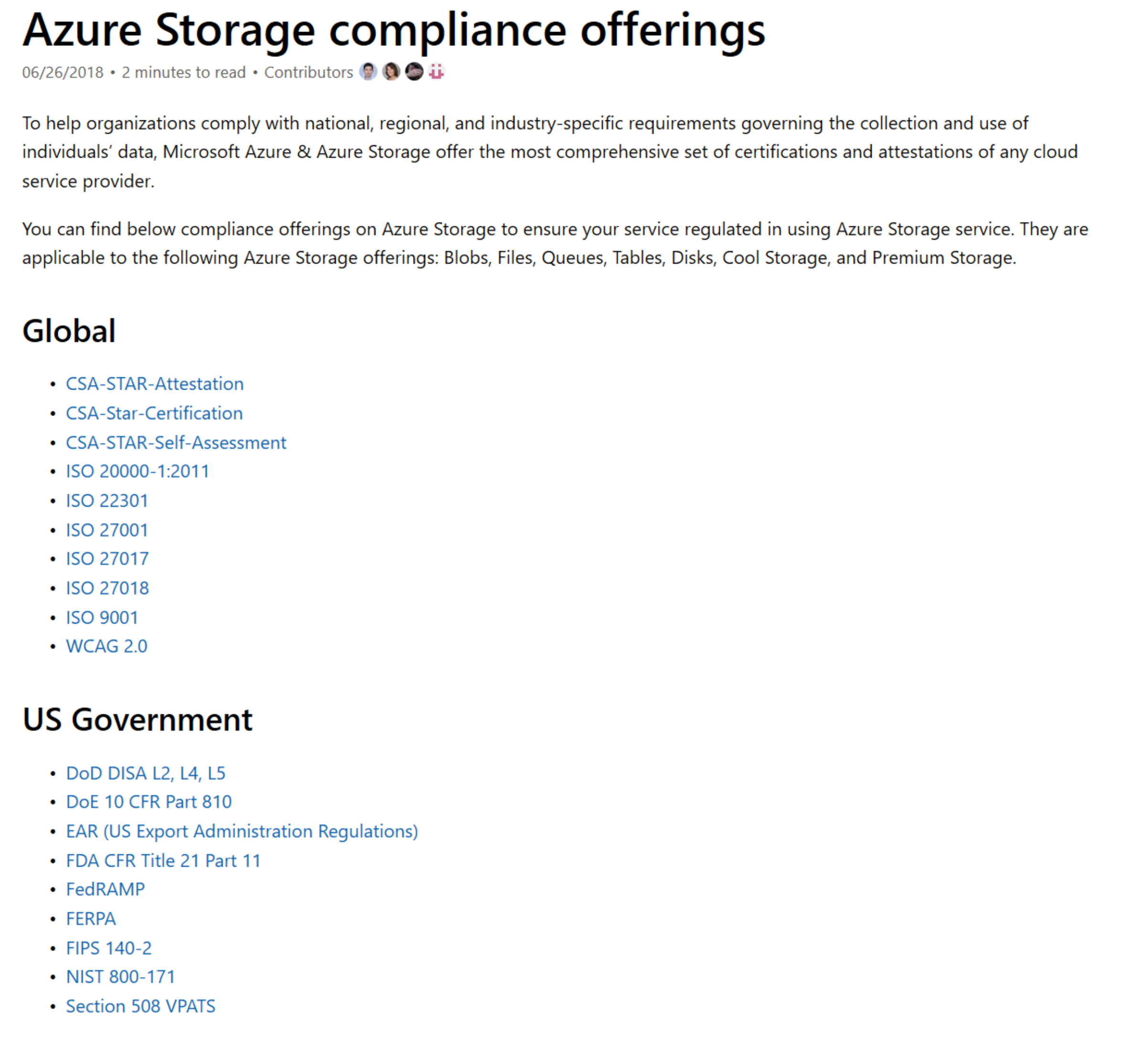
Sending (large) data efficiently



30 – 40% reduction in size

Save network bandwidth and time

Compliance



Azure Storage compliance offerings

06/26/2018 • 2 minutes to read • Contributors

To help organizations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft Azure & Azure Storage offer the most comprehensive set of certifications and attestations of any cloud service provider.

You can find below compliance offerings on Azure Storage to ensure your service regulated in using Azure Storage service. They are applicable to the following Azure Storage offerings: Blobs, Files, Queues, Tables, Disks, Cool Storage, and Premium Storage.

Global

- CSA-STAR-Attestation
- CSA-Star-Certification
- CSA-STAR-Self-Assessment
- ISO 20000-1:2011
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 9001
- WCAG 2.0

US Government

- DoD DISA L2, L4, L5
- DoE 10 CFR Part 810
- EAR (US Export Administration Regulations)
- FDA CFR Title 21 Part 11
- FedRAMP
- FERPA
- FIPS 140-2
- NIST 800-171
- Section 508 VPATS

Questions?

Homework Assignment

https://aka.ms/az301asg

Microsoft Azure

Open Mic