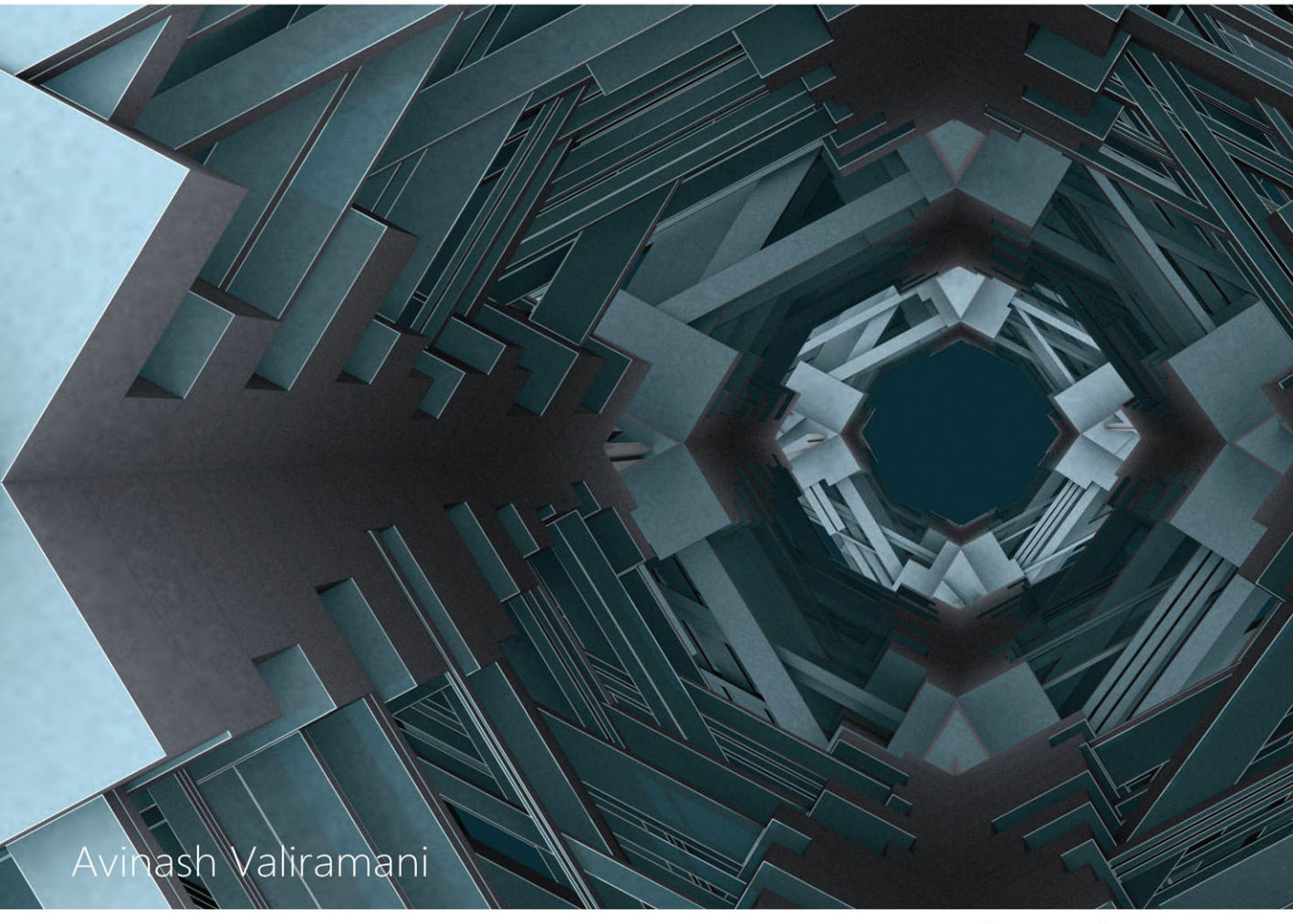
Microsoft

Microsoft Azure
Monitoring & Management

The Definitive Guide



Avinash Valiramani

FREE SAMPLE CHAPTER |

Microsoft

Microsoft Azure Monitoring & Management: The Definitive Guide

Avinash Valiramani

Microsoft Azure Monitoring & Management: The Definitive Guide

Published with the authorization of Microsoft Corporation by: Pearson Education, Inc.

ISBN-13: 978-0-13-757102-4
ISBN-10: 0-13-757102-X

Library of Congress Control Number: 2022947667

ScoutAutomatedPrintCode

CREDITS

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

SPONSORING EDITOR
Charvi Arora

DEVELOPMENT EDITOR
Kate Shoup

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Sarah Kearns

INDEXER
Tim Wright

PROOFREADER
Jen Hinchliffe

TECHNICAL EDITOR
Thomas Palathra

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
codeMantra

GRAPHICS
codeMantra

COVER ILLUSTRATION
NesaCera/Shutterstock

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Contents at a Glance

Contents

About the author

Avinash Valiramani is an IT Infrastructure and Cloud Architect with more than 16 years of expertise in areas of Microsoft Technologies such as Microsoft Azure, Microsoft 365, Windows Server, Active Directory, Microsoft Exchange, SCCM, Intune, and Hyper-V. He is a certified Architect on Azure Infrastructure, Azure Artificial Intelligence, Azure Security, and Microsoft365. He has been working primarily with large to mid-size enterprises globally in designing their Cloud Architecture, planning migration strategies and executing complex implementations. Avinash is publishing four books as part of the Microsoft Azure Best Practices series, including this current one, collating real-world experiences to deliver a comprehensive and concise experience for new and budding technologists. Avinash also holds certifications in Amazon AWS, Barracuda, Citrix, VMware, and many other IT/Security industry certifications to complement his Microsoft expertise. He has authored a course on Azure Virtual Desktop for O'Reilly Media and is planning many others in the coming months. You can follow Avinash on Twitter at @avaliramani and he will soon be posting frequent blogs on www.avinashvaliramani.com and www.cloudconsulting.services.

Acknowledgements

At the outset, my biggest thanks and gratitude to Loretta Yates for trusting me with this huge responsibility. The books in this series would not have been possible without your confidence in me and I will be forever grateful for that.

I would like to acknowledge Celine for all her support to me throughout the journey of these last two books. Celine, sincerely a Big Thank You for pushing and guiding me, whenever I needed it. These books would not have been possible without your constant support.

To my family, I am forever grateful for all your love and support.

To my extended family, thank you for tolerating my absence for over a year and a half while I closed myself off to focus on these books.

A special thank you to Kate Shoup for editing and reviewing this third book in this series. Your guidance and attention to detail throughout these series of books has been immensely valuable. Kate, it has been a wonderful experience working on these books with you and I could not have hoped for a better editor for this collaboration.

Thanks to Thomas Palathra, Sarah Kearns, and Tracey Croom for adding the final touches to bring this across the finish line. This book is the fruit of all our labour, I am extremely happy, and grateful we worked together on it.

Lastly, thanks to Charvi Arora and the entire Microsoft Press/Pearson team for their constant support and guidance on this project.

Three down, one more to go!

Introduction to Azure monitoring and management services

Welcome to *Azure Monitoring and Management: The Definitive Guide*. This is the third book in the series on Azure Infrastructure, and provides in-depth information about the various Azure services that support monitoring and management capabilities and shares best practices based on real-life experiences with the product in different environments.

This book focuses primarily on those Azure monitoring and management services generally available during 2021 and early 2022, encompassing developmental work done on these services over the years. A few monitoring and management features and functionalities were under preview at the time of this writing and could change before they are generally available; hence, we have decided to cover the most notable ones in subsequent iterations of this book as they go live globally.

Overview

Over the years, Microsoft has introduced various services related to the Azure monitoring and management stack to simplify, automate, and optimize workload deployments; make management easier; and improve monitoring of Azure compute, networking, and storage services. Microsoft has released regular updates to these services, introducing additional features and functionality, enhancing the service's support matrix, and making it easier to deploy and manage with each iteration.

Following is a brief timeline of the announcement of each of these services in public preview or general availability.

- **Azure Backup** Oct 2014
- **Azure Site Recovery** Oct 2014
- **Azure Migrate** July 2019
- **Azure Monitor** Mar 2017
- **Azure Network Monitor** Jan 2018
- **Azure Portal** Dec 2015
- **Azure Cloud Shell (Bash)** Nov 2017
- **Azure Cost Management** Sept 2017

Each service provides customers with various options to address their infrastructure management, redundancy, resiliency, and recovery requirements.

This book dives into each of these services to highlight important considerations in deploying and managing them and to share associated best practices. You will initially focus on the features provided by each service and on service requirements; thereafter, you will explore in-depth concepts of each service and the components that make up that service. This will allow you to better understand how each service can deliver value in your Azure deployment. After this, you will focus on deployment considerations and strategies, with step-by-step walkthroughs that illustrate deployment and management methods followed by best practices.

Cloud service categories

As in earlier books in this series, let us start by first discussing the different types of cloud service categories. Currently, cloud services are broken down into four main categories: infrastructure as a service (IaaS), platform as a service (PaaS), function as a service (FaaS), and software as a service (SaaS). SaaS is not relevant to the content covered in this Microsoft Azure book series; hence we will focus on better understanding the first three categories:

- **Infrastructure as a service (IaaS)** Using virtual machines (VMs) with storage and networking is generally referred to as infrastructure as a service (IaaS). This is a traditional approach to using cloud services in line with on-premises workloads. Most on-premises environments use virtualization technologies such as Hyper-V to virtualize Windows and Linux workloads. Migrating to IaaS from such an environment is much easier than migrating to PaaS or FaaS. Over time, as an organization's understanding of various other types of cloud services grows, it can migrate to PaaS or FaaS.
- **Platform as a service (PaaS)** One of the biggest benefits of using a cloud service is the capability to offload the management of back-end infrastructure to a service provider. This model is called platform as a service (PaaS). Examples of back-end infrastructure include different layers of the application, such as the compute layer, storage layer, networking layer, security layer, and monitoring layer. Organizations can use PaaS to free up their IT staff to focus on higher-level tasks and core organizational needs instead of on routine infrastructure monitoring, upgrade, and maintenance activities. Azure App Service and Azure Container Service are examples of Azure PaaS offerings.

- **Function as a service (FaaS)** Function as a service (FaaS) offerings go one step beyond PaaS to enable organizations to focus only on their application code, leaving the entire back-end infrastructure deployment and management to the cloud service provider. This provides developers with a great way to deploy their code without worrying about the back-end infrastructure deployment, scaling, and management. It also enables the use of microservices architectures for applications. An example of an Azure FaaS offering is Azure Functions.

From the Azure monitoring and management stack, the services largely fall under the PaaS category. For example:

- Azure Backup is a PaaS service that allows you to configure and manage backups in Azure and on-premises environments to protect both IaaS and PaaS workloads.
- Azure Site Recovery is a PaaS service that allows you to configure and manage disaster recovery for your workloads hosted in on-premises environments, such as Hyper-V and VMWare VMs, physical servers, and VMs hosted in Azure.

Each of these cloud-service categories has various features and limitations. Limitations might relate to the application, technological know-how, costs for redevelopment, among others. As a result, most organizations use some combination of different types of these cloud services to maximize their cloud investments.

Each service provides a different level of control and ease of management. For example:

- IaaS provides maximum control and flexibility in migration and use.
- FaaS provides maximum automation for workload deployment, management, and use.
- PaaS provides a mix of both at varying levels, depending on the PaaS service used.

Each service also offers varying levels of scalability. For example:

- IaaS requires the use of additional services to achieve true scalability and load balancing—for example, using Azure Load Balancer, a PaaS service, to balance requests across multiple Azure IaaS VMs.
- PaaS and FaaS services are generally designed with built-in scalability and load-balancing features.

Cost-wise, each service provides varying levels of efficiency. For example:

- FaaS offerings charge for compute services based only on the usage hours for compute services, making it extremely cost-effective.
- IaaS products charge for compute services regardless of usage once the compute service (for example, a VM) is online.
- PaaS offerings are a mixed bag depending on how the services are configured. Some PaaS products charge for compute resources regardless of usage, while others, if configured correctly, charge based on usage alone. For example, Azure Site Recovery is charged based on different factors:
  - There is a monthly site recovery license fee per protected physical or virtual server, based on average monthly usage.
  - The back-end storage used to store the replica data is billed based on storage usage per month and for any disk costs incurred during disaster recovery drills. In addition, storage transactions are billed based on monthly usage.
  - Bandwidth is charged for when replicating Azure VMs to another Azure region.
  - Recovery points created based on the replication policy will result in snapshots of the replica storage; these are charged for as well.
  - If you perform disaster recovery drills, there are additional charges for compute, networking, and storage resources based on actual consumption during each drill.

Service selection factors and strategies

There are certain factors to consider when selecting the Azure monitoring and management service for a given environment, based on application architecture, connectivity requirements, application security requirements, application delivery requirements, and other business needs. Let us start by understanding some of these key factors and the Azure monitoring and management services that best address them:

- **Securely manage Azure environment** The management stack provides multiple services that you can leverage to securely manage your Azure environment. These include the Azure Portal and Azure Cloud Shell services. While most admins heavily use the Azure Portal for most deployment, monitoring, and management activities, it is highly recommended that you

develop Azure Cloud Shell skills, as it will allow you to perform repetitive actions in a much faster and more automated manner.

- **Build redundancy for recovery of infrastructure** The Azure Backup and Azure Site Recovery services provide features to help you build redundancy for your environment. Based on your organizational requirements, you might deploy either one or both of these services. For example, Azure Backup is useful for long-term recovery point storage to allow you to restore data that might be days, weeks, months, or years old, whereas Azure Site Recovery is more suitable for short-term recovery points that can help you quickly recover Azure workloads in another Azure region with minimal downtime, but only if you restore from recovery points that are 48 to 72 hours old. Azure Backup can be considerably slower to use for data restoration compared to Azure Site Recovery, as you may need to deploy some infrastructure before you are able to recover the required data.
- **Migrate on-premises resources** The Azure Migrate service is best suited to migrate on-premises hosted physical or virtual servers or other cloud-hosted IaaS VMs. Azure Site Recovery service allows you to synchronize your on-premises servers to Azure and migrate them over, but the Azure Migrate service is built to better assess and manage such migration activities.
- **Optimizing Azure spends** The Azure Cost Management service can help you better understand your Azure spends and areas for optimization and cost reduction. The service provides you with automated recommendations based on analysis of data collected by the service on the usage and sizing of each service. In addition, you can use the data provided by the service to perform manual assessments and optimizations based on your experience and understanding of your environment and hosted workloads.
- **Monitoring Azure services** The Azure Monitor, Azure Network Monitor, and Azure Service Health services can help you to monitor the health of the overall Azure environment, Azure region, and services provided in a particular region or specific Azure networking components such as VPN. As we dive deeper into each service throughout this book, you will have more clarity on when each service can be leveraged in your environment.

As you can see, different factors can help you determine the monitoring or management service to use. As your understanding of these services improves during the course of reading this book, as you start to deploy and manage your Azure environment, and as your business needs evolve over time, you will be able to make better and wiser decisions on which service to leverage to meet those business demands.

Who is this book for?

Microsoft Azure Monitoring & Management: The Definitive Guide is for anyone interested in Azure infrastructure solutions—IT and cloud administrators, network professionals, security professionals, developers, and engineers. It is designed to be useful for the entire spectrum of Azure users. Whether you have basic experience using Azure or other on-premises or cloud virtualization technologies or you are an expert, you will still derive value from this book. This book provides introductory, intermediate, and advanced coverage of each monitoring and management service.

The book especially targets those who are working in medium-to-large enterprise organizations and have at least basic experience in administering, deploying, and managing Azure infrastructure or other virtualization technologies such as Microsoft Hyper-V, and are looking to enhance their understanding of how to build resiliency and redundancy in their on-premises and cloud environments and leverage the wide range of infrastructure services provided by Microsoft Azure.

How is this book organized?

This book is organized into nine chapters:

- Chapter 1: Azure Backup
- Chapter 2: Azure Site Recovery
- Chapter 3: Azure Migrate
- Chapter 4: Azure Monitor
- Chapter 5: Azure Network Watcher
- Chapter 6: Azure Portal
- Chapter 7: Azure Cloud Shell
- Chapter 8: Azure Service Health
- Chapter 9: Azure Cost Management

Each chapter focuses on a specific Azure monitoring and management service, covering its inner workings in depth, with walkthroughs to guide you in building and testing the service and real-world best practices to help you maximize your Azure investments.

The approach adopted for the book is a unique mix of didactic, narrative, and experiential instruction.

- The didactic component covers the core introductions to the services.
- The narrative leverages what you already understand and acts as a bridge to introduce concepts.
- The experiential instruction takes into account real-world experiences and challenges in small and large environments and the factors to consider while designing and implementing workloads. Step-by-step walkthroughs on how to configure each Azure monitoring and management service and its related features and options enable you to take advantage of all the benefits each service has to offer.

System requirements

To get the most out of this book, you must meet the following system requirements:

- **An Azure subscription** Microsoft provides a 30-day USD200 trial subscription that can be used to explore most services covered in this book. Some services, such as dedicated hosts, cannot be created using the trial subscription, however. To test and validate these services, you will need a paid subscription. If you plan to deploy any of these restricted services, you will need to procure a paid subscription.
- **Windows 10/11** This should include the latest updates from Microsoft Update Service.
- **Azure PowerShell** For more information, see *docs.microsoft.com/en-us/powershell/azure/install-az-ps*.
- **Azure CLI** For more information, see *docs.microsoft.com/en-us/cli/azure/install-azure-cli*.
- **Display monitor** This must be capable of 1024 x 768 resolution.
- **Pointing device** You need a Microsoft mouse or compatible pointing device.

About the companion content

The companion content for this book can be downloaded from the following pages:

MicrosoftPressStore.com/AzureMonitoringTDG/downloads or *github.com/avinashvaliramani/AzureMonitoringMgmtTDG*

The companion content includes PowerShell and CLI code for each walkthrough in the book (where applicable).

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/AzureMonitoringTDG/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit *MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *support.microsoft.com*.

Stay in touch

Let's keep the conversation going! We're on Twitter: *twitter.com/MicrosoftPress*.

Chapter 2

Azure Site Recovery

Overview

Microsoft introduced the Azure Site Recovery (ASR) service in public preview in June 2014. ASR initially focused on Hyper-V–to–Hyper-V and on-premises Hyper-V–to–Azure recovery scenarios. Over time, the service evolved to include additional capabilities, such as support for various operating systems, Azure IaaS VMs, and complex workloads that you could replicate in coordination with each other so you could bring them online in Azure with a similar recovery point. The simplicity, stability, and cost effectiveness provided by ASR has made it a very popular service used by organizations for their business continuity and disaster recovery (BCDR) strategy.

The key features of this service include the following:

- **Simplified interface to set up, monitor, and manage BCDR** ASR provides an intuitive interface that makes it possible to easily set up, monitor, and manage the service.
- **Support for most commonly used operating systems** ASR supports the replication of most operating systems, and the support list is expanding on a regular basis. This makes it possible to use ACR as a one-stop BCDR solution for most organizations.
- **Support to define replication schedules to meet the RTO and RPO objectives for most organizations** ASR supports replication as low as 30 seconds for Hyper-V VMs and continuous replication for Azure VMs. VMware support is currently under preview but is expected to allow continuous replication.
- **Support for any workload** ASR supports the replication of any workload as long as it is hosted on a supported operating system. This makes it a viable solution to address most organizations' needs.
- **On-premises Hyper-V–to–Hyper-V replication, monitoring, and recovery orchestration across multiple DR sites** ASR supports replication monitoring and failover coordination for on-premises Hyper-V–to–Hyper-V servers across multiple interconnected sites. Hyper-V replication is used for data replication, but ASR helps automate all the recovery steps from the cloud.

- **Azure–to–Azure IaaS VM replication, monitoring, and recovery orchestration across Azure regions** ASR added support for Azure VM replication and failover across Azure regions in 2017. This allowed organizations to set up a BCDR strategy for their critical cloud workloads across multiple Azure regions.
- **On-premises Hyper-V–and physical servers–to–Azure replication, monitoring, and recovery orchestration** ASR supports the entire recovery management for workloads hosted in on-premises Hyper-V and physical servers to Azure VMs. Azure Storage hosts the replicated data. VMs are created only after a failover is initiated, reducing the costs associated with a secondary datacenter.
- **App-consistent snapshots to recover applications more efficiently** ASR supports using app-consistent snapshots for replication to ensure that applications are replicated using disk data, all data in memory, and all transactions in process.
- **Simplified and cost-effective pricing** ASR charges a fixed fee per server for the replication software; Azure Storage costs for replicated data are charged only after the VMs are failed over in Azure. This makes it extremely cost-effective when the DR site in Azure is not actively used to host VMs, as the majority of costs are related to running the VM. All this makes it possible for most organizations to afford a BCDR solution for their environment.
- **Testing DR without interruption to production** ASR supports the activation of the replicated data in isolated networks in Azure. This enables you to test VMs to make sure your application, database, and other workloads are working as needed before you need to actually use them in a DR scenario. This also enables scenarios in which application upgrades can be tested in the Azure cloud before implementing them in your on-premises environment.
- **Integration with SQL Server AlwaysOn** ASR supports integration with SQL Server AlwaysOn to allow for seamless recovery of both interconnected application and database workloads.
- **Integration with Azure Automation** Azure Automation enables you to set up scripts and automated actions to provision other Azure services or run pre- and post-failover scripts as part of your automated recovery procedure.
- **Multi-VM consistency using replication groups** ASR supports setting up multi-VM replication groups so that multiple VMs are replicated together, and app-consistent and crash-consistent recovery points are created to facilitate failover. This enables you to address scenarios that require multiple VMs to be maintained at the same consistency.

ASR supports various recovery scenarios that can be used by organizations in different ways, depending on their individual needs. The following sections cover the two most important scenarios that ASR supports: Azure–to–Azure disaster recovery and on-premises Hyper-V–to–Azure disaster recovery. Read these sections to obtain a better understanding of how both these scenarios can be set up, managed, and monitored using ASR.

Azure–to–Azure disaster recovery

ASR enables you to set up the replication of an Azure IaaS VM to another Azure region. After you enable replication, ASR installs the Site Recovery agent extension on the Azure VM that is used to register the VM to the ASR service. Once this is done, existing disk data and changes to the disk are transferred to the target storage account or managed disk based on your selection. Data is transferred using Microsoft's private network rather than the public internet, regardless of the Azure region selected, ensuring your data is transferred in a secure manner. Replication is continuous and crash-consistent, and app-consistent recovery points are created based on the replication policy that you set up for a VM.

Replication policy

The replication policy created and associated by default during the DR setup process defines the following:

- **Recovery-point retention** This defines how far back in time ASR allows for recovery. The service retains recovery points based on retention timelines you define. At this time, the maximum supported recovery-point retention duration is 15 days for managed disks and 3 days for unmanaged disks; the default is 24 hours.

> ***NOTE*** **The higher the recovery-point retention period, the more data that is retained for that VM, and therefore the more you are charged for the storage used by the service.**

- **Crash-consistent recovery points** These are snapshots of the state of the VM disk taken and sent to the target region. These recovery points do not capture the data in memory and can therefore result in applications being brought online in an inconsistent state when recovered. Although most applications these days support crash-consistent recovery points, it is best to use app-consistent recovery points for recovery, if possible. By default, these are created every 5 minutes.
- **App-consistent recovery points** These are snapshots of the on-disk data along with all processes, data, and transactions running in memory. These are captured using the Volume Shadow Copy Service on Windows Servers. App-consistent snapshots take longer than crash-consistent snapshots and can add load to the server depending on the available resources and frequency defined. You should test to make sure these snapshots are not causing significant overhead or resize your VM workload to accommodate the additional load. The minimum frequency supported for this snapshot is 1 hour; the default setting is 4 hours.

You can define a replication policy based on your application, workload, or recovery point objective (RPO) requirements and set up your replication configuration to use that policy when setting up replication.

Data security

ASR does not intercept, scan, or analyze data transferred between source and target regions. This makes the entire process transparent to the service and eliminates the risk of the replicated data being used for malicious purposes. Data is encrypted in transit as well as encrypted while at rest when stored in the target region.

Multi-VM consistency

Multiple interdependent VMs can be set up in a replication group during replication setup so they are replicated to the target region with shared crash-consistent and app-consistent recovery points. This might be necessary when multiple application, interface, and database servers require that level of data consistency across each to ensure a supported failover. All VMs in a replication group must be failed over at the same time and cannot be failed over individually.

A replication group can contain a maximum of 16 VMs. VMs can be added to a replication group only when they are being set up for replication. To add a VM that is already replicating to a replication group, you must re-create the replication for that VM. Multi-VM consistency is quite resource intensive. It is therefore recommended that you enable it only in scenarios in which it is important for VMs to have such shared snapshots.

> ***NOTE*** **All VMs that are part of a multi-VM consistency replication group must communicate with each other over port 20004. Make sure any firewalls or network security groups set up between the VMs are configured to allow this traffic.**

Target environment configuration

You can define different configuration items for the target environment, even after setting up replication. However, there are a few configuration items that can be defined only during the initial setup. Following is a brief list of some of the key items that are supported at this time:

- **Target VM SKU** You can define this during replication setup, leave it set to automatic, or modify it after replication setup. When set to automatic, ASR will select a VM SKU that is the same or similar based on resource availability in the target region.
- **Target resource group** You can define the target resource group during replication setup or leave it set to automatic, in which case the service will create a new resource group or modify an existing one after replication setup.
- **Target virtual network** You can define the target virtual network during replication setup or leave it set to automatic, in which case the service will create a new one or modify an existing one after replication setup.

- **Target subnet** The service automatically assigns the VM to a subnet based on the source VM subnet setup. You can modify the target subnet after replication setup.
- **Target name** The service automatically assigns a target name based on the source VM name. You can modify the target name after replication setup.
- **Target disk type** You can define the target disk type during replication setup. The service automatically selects the disk type based on the source disk setup, but you can change it if required during replication setup.
- **Target subscription** The service automatically selects the subscription based on the source VM subscription, but if there is another subscription associated with the same Azure AD tenant, you can select it instead during replication setup.
- **Target proximity group** The service automatically sets the target proximity group to None, but you can change this during replication setup.
- **Target VM availability configuration** The service automatically sets the target VM availability configuration based on the source VM, but you can change this at replication setup.

Failover and failback

In the event of a disaster in the primary region, you can failover the Azure VM to the target region using the ASR service. You will be asked to select the recovery point to use for the restoration. The target VM will then be created based on the settings you've defined and the replicated data.

The target VM is created in an unprotected state. Once the primary region is back online, you can set up failback replication for the VM. At this time, the site recovery service checks whether the source disk is still available. If one exists, it will check it for consistency and determine the missing changes to replicate over. If no disk exists, it will start the replication of the entire disk.

You can perform a failback in the same manner as the failover and perform it whenever you have the appropriate downtime.

Test and planned failovers

ASR supports test and planned failover options. Each option is useful in different scenarios.

In a test failover, ASR creates a VM in a test network defined by you, with the replicated data. It is recommended that you set up an isolated test network without connectivity to the primary network to avoid accidental writes from test applications to the primary database or other unexpected issues. The test VM does not commit write operations to the replication data. This enables you to make changes to the test VM—for example, application or database

upgrades—without affecting the primary server or the replication in any way. You can perform test failovers to validate your VM and its workload failover as needed in the secondary region to perform application or database upgrade testing or for compliance auditory reasons. When you are finished testing, you can simply clean up the test environment; the test VM and associated disks will be deleted from the secondary Azure region, while the original replication continues unimpeded.

During a planned failover, ASR brings the VM online in the secondary region and allows changes to the VM to be committed to disk. While the changes are not replicated to the primary region, replication from the primary site is stopped. Use this option in scenarios where your primary VM is down or you are migrating to the secondary region.

Network security

You can control outbound replication traffic using network security groups (NSGs) in the source Azure region. ASR requires that any NSG rules set up enable outbound replication traffic. You can use service tags that Microsoft provides to define such outbound traffic rules. This ensures that any IP changes in the Microsoft services are automatically applied to your environment, as the service tags are updated by Microsoft when such changes occur, supporting uninterrupted replication for your workloads.

Azure–to–Azure disaster recovery walkthrough

The following section walks you through the process of setting up and testing Azure–to–Azure replication for a VM using the Azure Portal.

> ***IMPORTANT*** **If you are following along, you'll want to select resources and unique resource names based on your environment for each of your deployments.**

> ***IMPORTANT*** **If you are following along, delete any unwanted resources after you have completed testing to reduce charges being levied by Microsoft for these resources.**

Using Azure Portal

SETUP AZURE REPLICATION

To set up Azure–to–Azure VM replication using the Azure Portal, follow these steps:

1. Log in to the Azure Portal, browse to the VM you want to replicate, and click it to select it.

2. In the left pane of the selected VM's configuration blade (see Figure 2-1), click **Disaster Recovery** to start the Azure Site Recovery wizard.

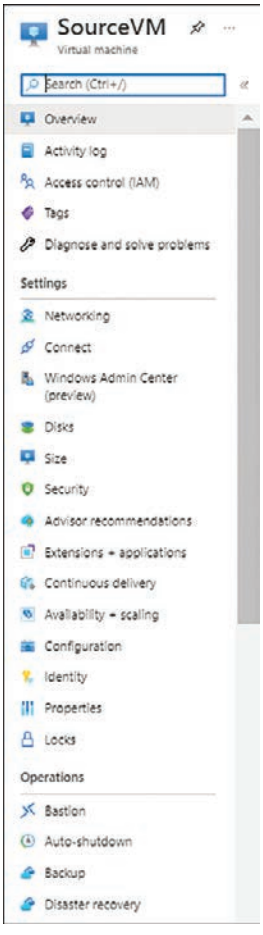


FIGURE 2-1 Options in the SourceVM configuration blade.

3. In the **Basics** tab of the Azure Site Recovery wizard, open the **Target Region** drop-down list and choose the region in which you would like to replicate the VM. (See Figure 2-2.) Then click **Next: Advanced Settings**.

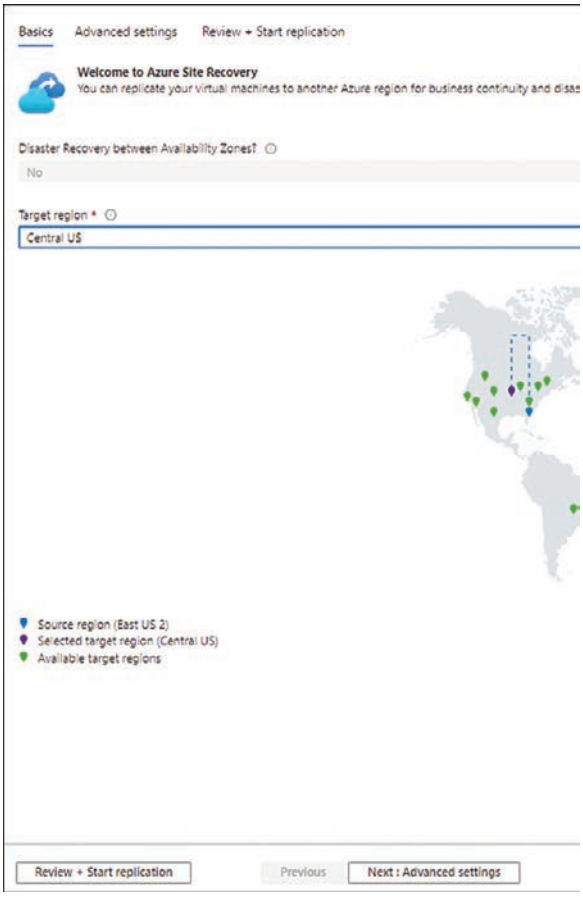


FIGURE 2-2 Basics tab.

4. In the **Advanced Settings** tab (see Figure 2-3), enter the following information and click **Next: Review + Start Replication**:
   - **Subscription** Select the subscription in which you want to create the replica VM.
   - **VM Resource Group** Select the resource group in which to create the replica VM. Alternatively, the wizard will create one automatically.
   - **Virtual Network** Select the virtual network to use for the replica VM. Alternatively, the wizard will create one automatically.
   - **Availability** Specify whether the replica VM should be set up with availability enabled or leave it set to the default (Single Instance).
   - **Proximity Placement Group** Specify whether the replica VM should be placed in a proximity placement group.
   - **Cache Storage Account** Select an existing Azure storage account to use as the replication cache. Alternatively, the wizard will create one automatically.

- **Vault Subscription** Select the subscription in which to set up the Recovery Services vault.
- **Recovery Services Vault** Select an existing Recovery Services vault. Alternatively, the wizard will create one automatically.
- **Vault Resource Group** Select an existing resource group in the target location. Alternatively, the wizard will create one automatically.
- **Replication Policy** Select an existing replication policy from the drop-down list. Alternatively, the wizard will create one automatically.
- **Update Settings** Specify whether ASR should manage all update settings or if you will do so manually.
- **Automation Account** Select an existing automation account to use for the site recovery configuration. Alternatively, the wizard will create one automatically.

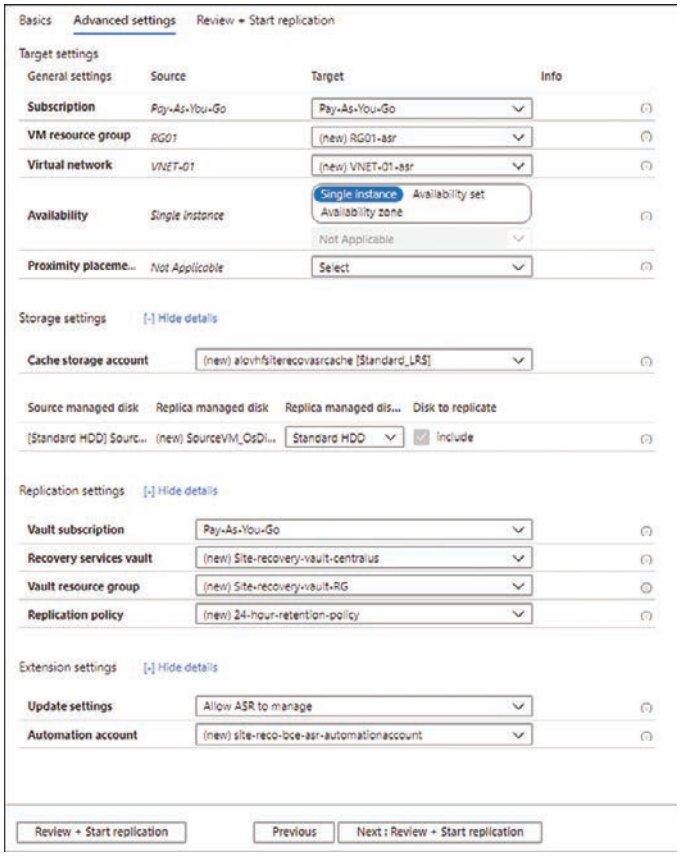


FIGURE 2-3 Advanced Setting tab.

5. On the **Review + Start Replication** tab, check your settings and click **Start Replication**. (See Figure 2-4.)

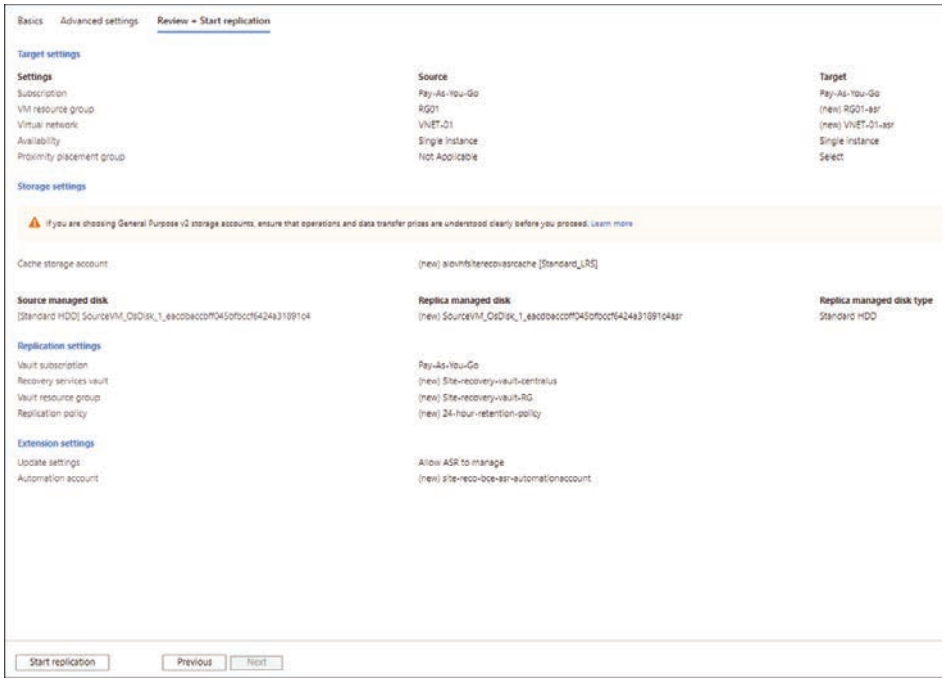


FIGURE 2-4 Review + Start Replication tab.

ASR creates the resources you requested, starting a number of jobs one after another to create all the different components.

6. Monitor the jobs to ensure they all complete successfully. (See Figure 2-5.)

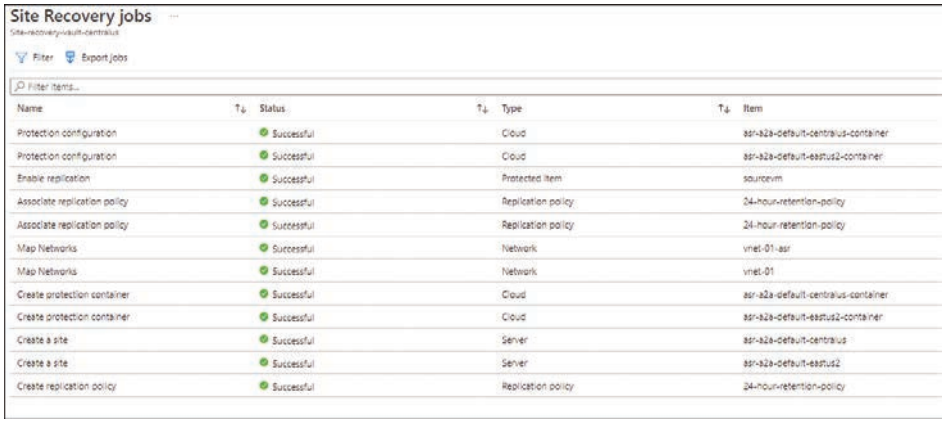


FIGURE 2-5 Site Recovery Jobs page.

NOTE **In the event of any errors or failures, you will need to select the error message to view more details to identify the root cause and resolve the issue. You will then have to reinitiate the entire process.**

MONITOR REPLICATION

When all the jobs are complete, in the Site Recovery service, under Replicated Items, you will see the SourceVM you just replicated.

7. Click **SourceVM** under **Replicated Items**.

   A SourceVM **Overview** page displays the status of the replication, or sync. Notice in Figure 2-6 that **Replication Health** is **Healthy**, but **Status** is **0% Synchronized**.

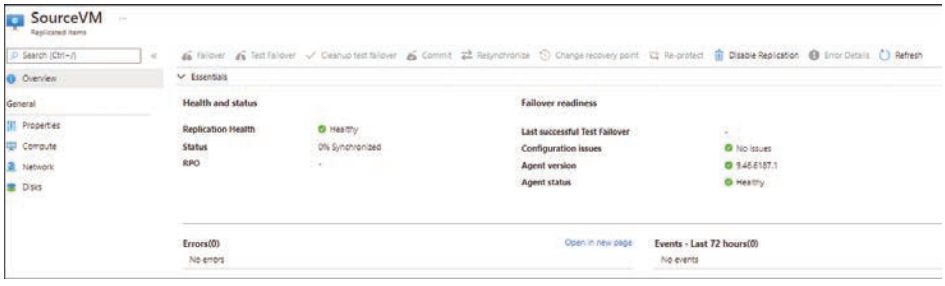


FIGURE 2-6 The SourceVM Overview page with Replication Health and Status data.

8. Refresh and monitor this page until synchronization is complete.

   When synchronization is complete, Status will change to Protected. (See Figure 2-7.) At this point, you can make changes to the replica VM configuration.

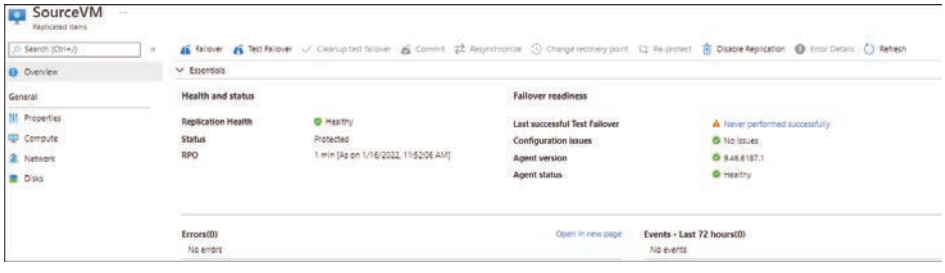


FIGURE 2-7 The SourceVM overview page with the updated Replication Health and Status data.

CUSTOMIZE REPLICA CONFIGURATIONS

9. In the left pane of the SourceVM's Replicated Items configuration blade, click **Compute**.
10. On the **Compute Properties** page (see Figure 2-8), enter the following information and click **Save**:
    - **Name** Type the VM name in the **Name** row of the **Target Settings** column.
    - **Resource Group** Enter the resource group in the **Resource Group** row of the **Target Settings** column.
    - **Size** Enter the size in the **Size** row of the **Target Settings** column.

FIGURE 2-8 Compute settings.

11. In the left pane of the SourceVM's Replicated Items configuration blade, click **Network**.

12. Click **Edit** to make changes to the following settings, if desired. (See Figure 2-9.) Then click **Save**:

- **Target Network**
- **Test Failover Network**
- **Accelerated Networking**
- **Subnet**
- **Network Security Group**
- **Private IP Address**
- **Public IP**

FIGURE 2-9 Network settings.

13. In the left pane of the SourceVM's Replicated Items configuration blade, click **Disks** to monitor pending changes to the source VM to assess how the sync is progressing. (See Figure 2-10.)

FIGURE 2-10 Disks replication status.

Next, you'll perform a test failover to test the replica VM.

14. Back in the **Overview** page in the SourceVM's Replicated Items configuration blade, click the **Test Failover** button. (See Figure 2-11.) A Test Failover page opens.

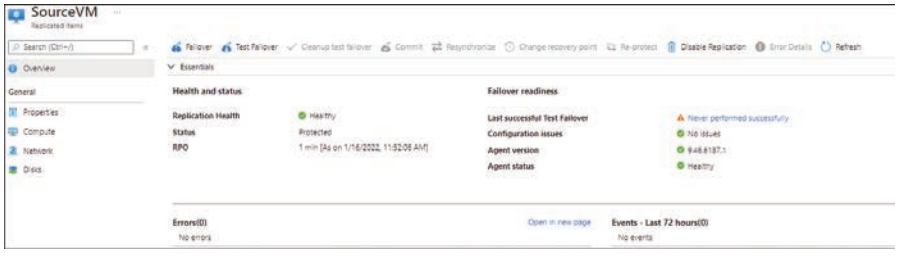


FIGURE 2-11 Click the Test Failover button.

15. In the **Test Failover** page (see Figure 2-12), set the following options as shown and click **OK**:

- **From** This automatically lists the Azure region where your source VM is running.
- **To** This automatically lists the Azure region where your replica VM is set to be created.
- **Choose a Recovery Point** Choose the recovery point to restore to and create the replica VM. You will generally want to select **Latest Processes (Low RTO)** for the least data loss possible.
- **Azure Virtual Network** This automatically lists the Azure virtual network where your replica VM is set to be created.

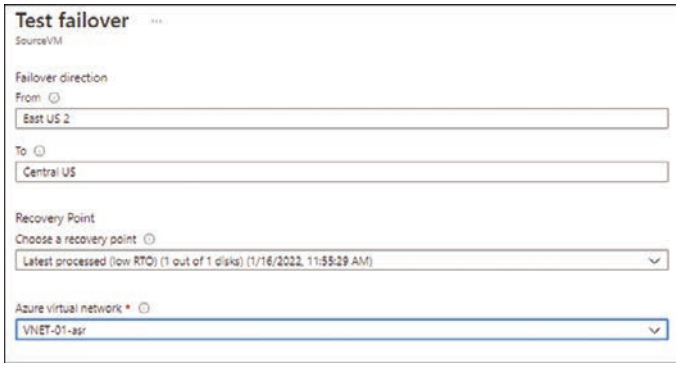


FIGURE 2-12 Test Failover page.

ASR stores the recovery point in the target region and creates a new VM with a name similar to the source VM. For example, if the source VM were named DC01, the new VM would be named DC01-test. Figure 2-13 shows the result.

NOTE **You can log in to the VM using Azure Bastion (if provisioned in the target region) or by assigning a public IP to the VM.**

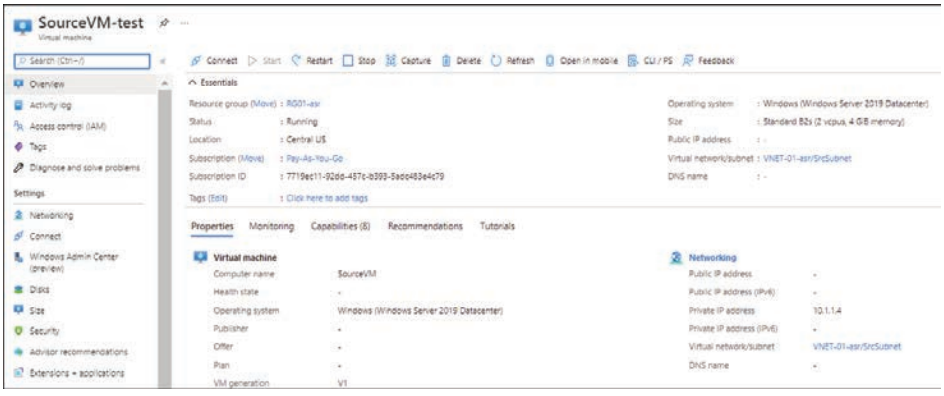


FIGURE 2-13 SourceVM-test Overview page.

16. Log in to the new VM and verify that all the data, apps, and services reflect correctly.

Now that you have finished testing, you're ready to clean up the test environment.

CLEANUP TEST FAILOVER

17. Back in the **Overview** page in the SourceVM's Replicated Items configuration blade (see Figure 2-14), click the **Cleanup Test Failover** button.

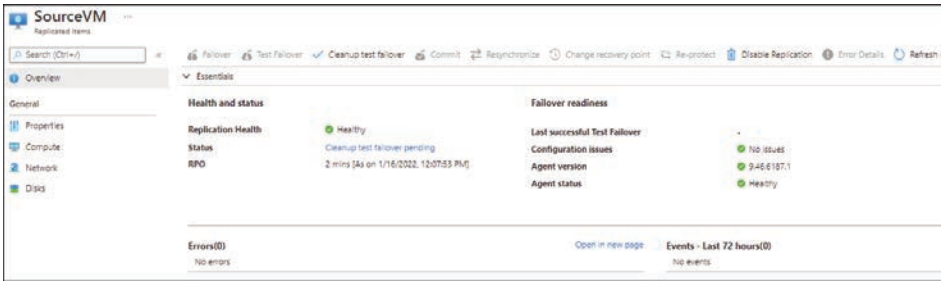


FIGURE 2-14 Click the Clean Test Failover button.

18. In the **Test Failover Cleanup** dialog box (see Figure 2-15), type any notes from the test that you would like to record in the **Notes** box. These could include the test participants, test outcomes, issues encountered, or changes to incorporate in future tests or after testing the replication configuration.

FIGURE 2-15 The Test Failover Cleanup dialog box.

19. Select the **Testing Is Complete. Delete Test Failover Virtual Machine(s)** check box and click **OK** to initiate the cleanup job.
20. From the **Test Failover Cleanup** page (see Figure 2-16), monitor the cleanup job to ensure it completes successfully.

FIGURE 2-16 Test Failover Cleanup page, showing the progress of the cleanup job.

If all your tests have completed successfully, you're ready to perform a full failover of the VM to the Azure region to which you are replicating.

PERFORM FAILOVER

21. Back in the **Overview** page in the SourceVM's Replicated Items configuration blade (see Figure 2-17), click the **Failover** button.

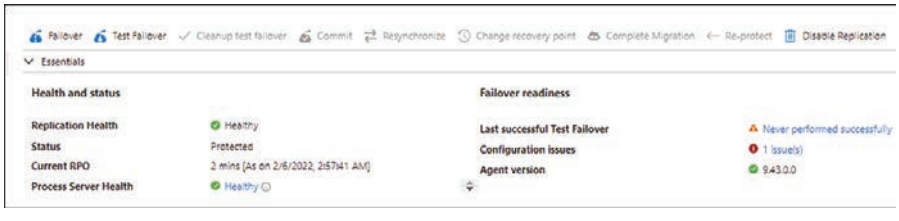


FIGURE 2-17 Click the Failover button.

22. In the **Failover** dialog box (see Figure 2-18), verify your settings, select the **Shut Down Machine Before Beginning Failover** check box if desired, and click **OK** to launch the ASR failover job.

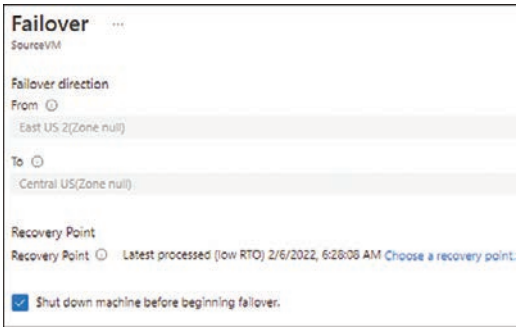


FIGURE 2-18 Failover dialog box.

23. On the **Failover** page (see Figure 2-19), monitor the progress of the replication job to ensure all the steps complete successfully. If any errors occur, they will appear highlighted on the page, and you will need to analyze and fix them before re-running the failover job.

FIGURE 2-19 Failover job summary page.

24. When the failover is complete, browse to the failed-over VM in the target region, log in to the VM, and validate that your application, database, or required services are online and working as intended.

    Now it's time to commit the VM. When you commit the VM, you will no longer be able to change the recovery point. Committing the VM will allow you to set up re-protect to enable the sync of the failed-over VM back to the source location, if required.

25. Back in the **Overview** page in the SourceVM replica's configuration blade (see Figure 2-20), click the **Commit** button. Then, when prompted, click the **Confirm** button.

FIGURE 2-20 Click the Commit button.

Now you can set up re-protection for the failed-over VM with the source VM. This provides redundancy for the failed-over VM in case of a disaster in the new site.

26. To set up re-protection, in the **Overview** page in the SourceVM's Replicated Items configuration blade, click the **Re-protect** button.

27. In the **Re-protect** page (see Figure 2-21), validate or customize the settings as needed and click **OK** to start the re-protection job.

FIGURE 2-21 Re-protect page.

28. Monitor the progress of the re-protection job to confirm that all the steps finish successfully. (See Figure 2-22.)

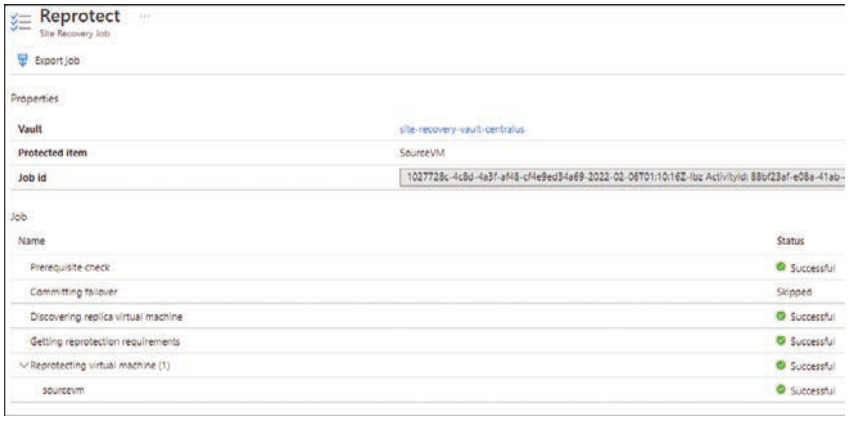


FIGURE 2-22 Reprotect page for the Site Recovery job.

29. When the re-protection job is complete, return to the **Overview** page in the SourceVM's configuration blade to monitor the replication status. (See Figure 2-23.) When Status is at 100% or Healthy, you can test failover or failover the VM if you want to switch back to your primary site.

FIGURE 2-23 Overview page of the SourceVM replica showing the replication status.

Hyper-V–to–Azure disaster recovery

Companies that use Hyper-V with or without System Center Virtual Machine Manager (SCVMM) can benefit from using ASR to set up a disaster recovery for their on-premises environment in Azure. Considering the costs associated with ASR and its comprehensive integration with Hyper-V and SCVMM, it is an ideal solution for organizations of any size.

In the past, setting up a disaster-recovery (DR) site meant hosting infrastructure in another datacenter and managing all the associated networking components, upgrades, and updates for each infrastructure layer on an ongoing basis. Due to the initial setup and ongoing maintenance costs of such a design, most small and mid-size businesses shied away from setting up a DR site, and instead relied on offsite backups for their recovery strategy. Today, however, thanks to cost benefits and ease of management and maintenance, all organizations can benefit from ASR.

ASR supports Hyper-V hosts starting from Windows Server 2012 R2 (with the latest updates) to the latest Windows Server release. Similarly, for VMM, the minimum supported version is Virtual Machine Manager 2012 R2 to the latest release.

For Hyper-V VMs, you can replicate all VMs that are supported for hosting in Azure. It is therefore important that you check for the most recent guidance from Microsoft published online regarding the latest support matrix for Hyper-V hosts, VMM servers, and Hyper-V VMs. This guidance changes from time to time as different operating systems reach end of life or end of support.

> ***NOTE*** **ASR integrates with Microsoft applications such as SharePoint, Exchange, Dynamics, SQL Server, and Active Directory, and works closely with leading vendors, including Oracle, SAP, IBM, and Red Hat.**

Replication components

ASR uses different components, depending on your Hyper-V environment:

- **Hyper-V with VMM/Hyper-V cluster with VMM** In this scenario (see Figure 2-24), you deploy the ASR Provider agent on the VMM server and the Recovery Services agent on each Hyper-V host. The Hyper-V VMs do not require anything to be installed on them.
- **Hyper-V without VMM/Hyper-V cluster without VMM** In this scenario, you deploy the ASR Provider agent and Recovery Services agent on each Hyper-V host. The Hyper-V VMs do not require anything to be installed on them. (See Figure 2-25.)

Each scenario requires you to provision a Recovery Services vault, a storage account, and a virtual network in the same Azure region to reference during replication setup. Replication can be set as frequently as every 30 seconds (except in scenarios where premium storage is used for replication) or as infrequently as every 5 minutes, enabling you to achieve extremely low recovery point objectives and low data loss.

NOTE **Although LRS and GRS storage account types are supported, it is recommended to use GRS, if costs permit, so your replicated data is maintained in multiple Azure regions. This way, a failover can be initiated in a secondary region if the primary Azure region is also down when an on-premises outage occurs.**

NOTE **Initial replication from on-premises must be performed over the network. Offline replication for the initial data or any subsequent data transfers is not supported.**

Replication policy

Similar to Azure–to–Azure replication, you must create a replication policy and associate it with your replication configuration during the DR setup process. This involves setting the following options:

- **Copy Frequency** This defines how often delta sync occurs after the initial replication is completed. Options range from 30 seconds to 5 minutes.
- **Recovery Point Retention** This defines how far back in time ASR allows for recovery, as the service retains recovery points based on retention timelines that you define. The maximum supported recovery-point retention at this time is 24 hours.
- **App-Consistent Recovery Points** These are snapshots of the on-disk data along with all processes, data, and transactions running in memory. They are captured using the Volume Shadow Copy Service on Windows Servers. App-consistent snapshots take longer than crash-consistent snapshots and can add load to the server depending on the available resources and frequency defined. You should test to make sure these snapshots are not causing significant overhead or resize your VM workload to accommodate the additional load. The minimum frequency supported for this snapshot is 1 hour.

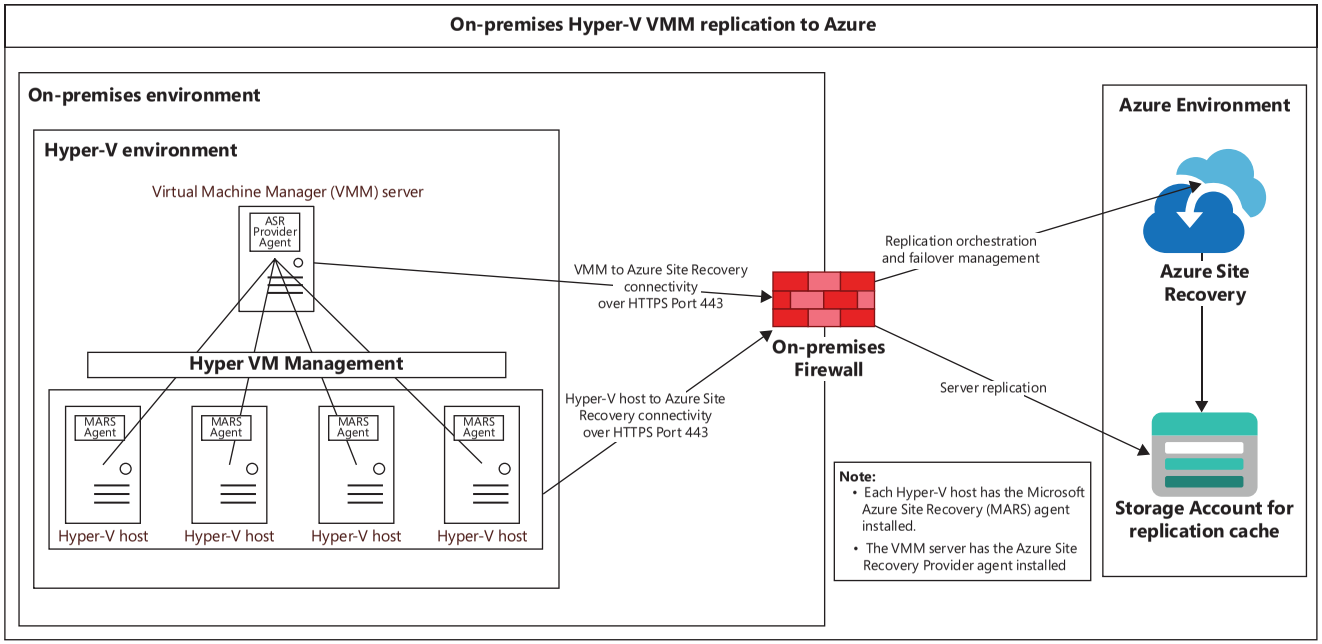


FIGURE 2-24 Hyper-V with VMM/Hyper-V cluster with VMM topology.

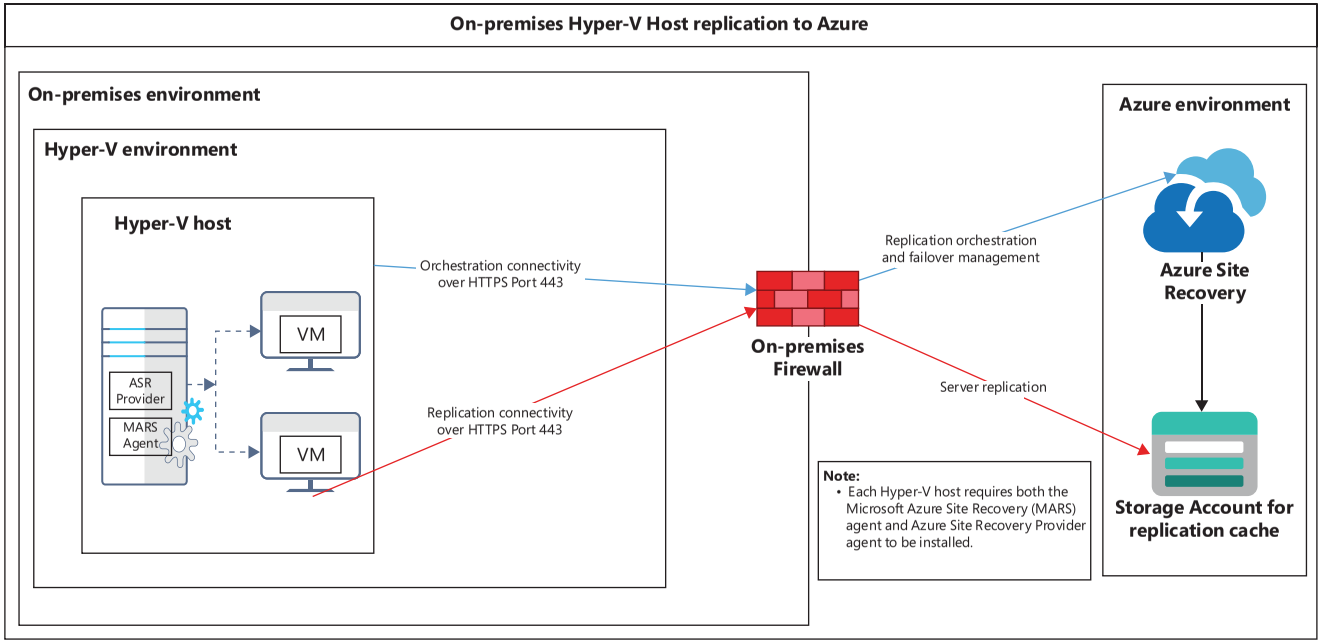


FIGURE 2-25 Hyper-V without VMM/Hyper-V cluster without VMM topology.

You can also define whether the replication should initialize immediately once the configuration is completed or schedule it to be initiated at a later time in the day.

Data security

Similar to the Azure–to–Azure DR scenario, ASR does not intercept, scan, or analyze data transferred between your on-premises and Azure target regions. This makes the entire process transparent to the service and eliminates the risk of the replicated data being used for malicious purposes. ASR only obtains metadata information to monitor replication health and coordinate failover activities. Data is encrypted in transit as well as encrypted while at rest when stored in the target region.

Failover and failback

In case of a disaster in the on-premises Hyper-V environment, you can failover the Azure VM to the target region using the ASR service. You will be asked to select the recovery point to use for the restoration. The target VM will then be created based on settings you've defined and the replicated data.

The target VM is created in an unprotected state. Once the on-premises datacenter is back online, you can set up failback replication for the VM from Azure to the on-premises Hyper-V host. At this time, you can choose to either perform a delta sync, during which ASR will check the source disk for consistency and determine the missing changes to replicate over, or, if that is not possible, to choose the full download option so the entire disk is replicated from Azure back on-premises. (In most cases when the Azure VM has been running for quite a few days, you will have to perform the full download option to set up failback.) Once replicated, you can perform a failback in the same manner as the failover whenever you have the appropriate amount of downtime available.

Test, planned, and unplanned failovers

Similar to Azure–to–Azure disaster recovery, ASR supports test and planned failover options even for Hyper-V VMs replicating to Azure. In addition, it supports unplanned failover in case the primary site has gone offline without giving you the ability to perform a graceful failover to Azure.

In a test failover, ASR creates a VM in a test network defined by you, with the replicated data for that Hyper-V VM. It is recommended that you set up an isolated test network without connectivity to the primary network to avoid accidental writes from test applications to the primary database or other unexpected issues. The test VM does not commit write operations to the replication data. This enables you to make changes to the test VM—for example, application or database upgrades—without affecting the primary server or the replication in any way. You can perform test failovers to validate your VM and its workload failover as needed in Azure to perform application or database upgrade testing or for compliance auditory reasons. This can also help in scenarios in which you are running low on resources on-premises and need a temporary test environment to quickly validate application changes. When you are finished

Index

A

B

C

D

E

F

H

I

J-K-L

M

N

O-P

Q-R

S

T

U

V

W-X-Y-Z