CAF Server Migration Deployment Guide Ver2.0



**MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.**

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[1 Introduction 1](#_Toc40298006)

[2 Target Audience 1](#_Toc40298007)

[3 Azure Server Migration Scenarios 1](#_Toc40298008)

[4 Azure Server Migration Architecture 1](#_Toc40298009)

[5 Requirements 2](#_Toc40298010)

[5.1 Operational Requirements 2](#_Toc40298011)

[6 Migration Prerequisites 2](#_Toc40298012)

[6.1 Ensure prerequisites have been fulfilled 3](#_Toc40298013)

[6.2 Physical and VMs Servers to be migrated 3](#_Toc40298014)

[6.3 Azure Subscription target 3](#_Toc40298015)

[6.3.1 Azure Role Based Access 3](#_Toc40298016)

[6.4 Azure Region to Target 4](#_Toc40298017)

[6.5 Azure Resource Groups Targeted 4](#_Toc40298018)

[6.5.1 Azure Resource Groups – Subscription (Prod) 4](#_Toc40298019)

[6.5.2 Azure Resource Groups – Subscription (Dev\Test) 5](#_Toc40298020)

[6.6 Azure VPN Gateway 5](#_Toc40298021)

[6.7 Azure VPN Tunnel in Site1 5](#_Toc40298022)

[6.8 Azure Local Network Gateway 5](#_Toc40298023)

[6.9 Azure Virtual Networks and Subnets 6](#_Toc40298024)

[7 Azure Migration Process 6](#_Toc40298025)

[7.1.1 Before you begin 6](#_Toc40298026)

[7.1.2 Azure Foundations Deployment script 7](#_Toc40298027)

[7.1.2.1 Onboard PowerShell 7](#_Toc40298028)

[7.1.2.2 Run Azure Foundations Script 11](#_Toc40298029)

[7.1.3 Specify DNS 12](#_Toc40298030)

[7.1.4 Create the VPN gateway 12](#_Toc40298031)

[7.1.5 Create the local network gateway 14](#_Toc40298032)

[7.1.6 Configure your VPN device 15](#_Toc40298033)

[7.1.6.1 Configure your VPN device 16](#_Toc40298034)

[7.1.7 Create the VPN connection 16](#_Toc40298035)

[7.1.8 Verify the VPN Connection 17](#_Toc40298036)

[7.1.8.1 Troubleshooting: Reset the VPN Connection 18](#_Toc40298037)

[7.2 How to Connect to a VM via VPN 19](#_Toc40298038)

[7.3 Domain Controller Configuration 20](#_Toc40298039)

[7.3.1 Prepare Active Directory 20](#_Toc40298040)

[7.3.2 Temporarily set DNS Servers to non-Azure 22](#_Toc40298041)

[7.3.3 Create Domain Controller and Replicate AD\DNS 22](#_Toc40298042)

[7.4 Assess and Migrate Hyper-V VMs & Physical Servers 28](#_Toc40298043)

[7.4.1 Prepare Hyper-V VMs & Physical Servers for Assessment and Migrate 28](#_Toc40298044)

[7.4.2 Assess Hyper-V VMs & Physical Servers for Migration 33](#_Toc40298045)

[7.4.3 Migrate Hyper-V VMs & Physical Servers to Azure 42](#_Toc40298046)

[7.5 Replicate and failover Windows / Linux Physical Servers, Hyper-V VM’s or VMware VM’s to Azure Checklist 50](#_Toc40298047)

[7.5.1 High Level Summary - Replication and Failover Checklist 50](#_Toc40298048)

[7.5.2 Verify Supported Operating Systems Process 51](#_Toc40298049)

[7.5.3 Setup Source Environment for Physical / HyperV / VMware VMs 51](#_Toc40298050)

[7.5.4 Create Migration User 52](#_Toc40298051)

[7.5.5 Prepare Machine for Management Server Installation 52](#_Toc40298052)

[7.5.6 Install Configuration Server 52](#_Toc40298053)

[7.5.7 Install Configuration Server – Configure Settings 58](#_Toc40298054)

[7.5.8 Configure and manage replication policies for VMware replication 64](#_Toc40298055)

[7.6 Prepare Hyper V/ VMware Machine for Migration (Required) 65](#_Toc40298056)

[7.6.1 Prepare Machine for Azure 66](#_Toc40298057)

[7.6.2 Install Mobility Service 66](#_Toc40298058)

[7.6.3 Enable Replication 68](#_Toc40298059)

[7.6.4 View and Manage VM properties 71](#_Toc40298060)

[7.6.5 Configure networks and IP addresses 72](#_Toc40298061)

[7.6.6 Verify Protection of Machine 73](#_Toc40298062)

[7.7 Prepare Workload for Migration 73](#_Toc40298063)

[7.7.1 ASR Agent Unsupported 73](#_Toc40298064)

[7.7.1.1 Manual VM Build Process 73](#_Toc40298065)

[7.7.2 Terminal Services 83](#_Toc40298066)

[7.7.3 Domain Services 83](#_Toc40298067)

[7.7.4 File Services 83](#_Toc40298068)

[7.7.5 Print Services 83](#_Toc40298069)

[7.8 Test Failover (Test Migration) in Site Recovery 83](#_Toc40298070)

[7.8.1 Create a network for test failover 83](#_Toc40298071)

[7.8.2 Ensure AD is prepared in the Test Network 84](#_Toc40298072)

[7.8.3 Prepare DNS and DHCP 84](#_Toc40298073)

[7.8.4 Virtualization Safeguards 84](#_Toc40298074)

[7.8.5 After AD is in the test network - Remove references to other domain controllers 84](#_Toc40298075)

[7.8.6 Run a Test Failover (Test Migration) 84](#_Toc40298076)

[7.8.7 Post Test Failover Considerations 86](#_Toc40298077)

[7.9 Migrate to Azure 87](#_Toc40298078)

[7.9.1 Test Full Failover to a production network in the recovery site 87](#_Toc40298079)

[7.9.2 Failover and Migrate to Azure Completion 89](#_Toc40298080)

[7.10 Verify Post Migration Components (Required) 91](#_Toc40298081)

[7.10.1 Verify Windows Activation 91](#_Toc40298082)

[8 Appendix A 92](#_Toc40298083)

[8.1 Helpful Links and Technical Information 92](#_Toc40298084)

# Introduction

This document is a major deliverable produced from the Azure Migration. It will detail the entire deployment from requirements to implementation. It is intended to be used by Customer & Partner to perform Azure Migration for any Data Center.

# Target Audience

This document is Level 400+ technical migration guide primarily intended for Azure Specialists, Cloud Solution Architects, Migration experts, System Administrators & anyone else who are going to be hands-on in executing the on-premise to Azure migrations. It is assumed that the audience has deep insights into their on-premise workload architectures, storage & networking capabilities along with the interdependencies across multiple services/components involved like Active Directory, RDS deployments, Microsoft Azure and its core services (compute, storage & Network).

Please note that this document will primarily focus on the detailed migration process and is NOT a primer for the technologies afore mentioned.

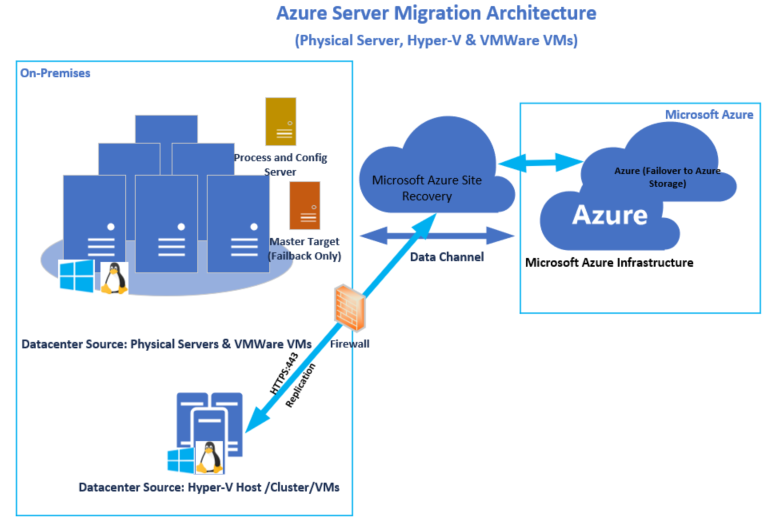
# Azure Server Migration Scenarios

Server migration to Azure covers the below 3 major senarios.

| Scenarios | Tools | Notes |
| --- | --- | --- |
| Physical Servers | Azure Migrate: Server Assessment Tool | Discover Physical Server  Collect machine metadata and performance metadata and migrate to Azure |
| Hyper-V VMs | Azure Migrate: Server Assessment Tool | Discover Hyper-V Vms  Collect Machine metadata and performance metadata and migrate |
| VMWare VMs | Azure Migrate: Server Assessment Tool | Discover VMWare Vms  Collect Machine metadata and performance metadata and migrate |

# Azure Server Migration Architecture

Below architecture diagram defines 3 senarios that covers the Physical to Azure Migration , Hyper-V to Azure Migration and VMWare to Azure Migration also includes Windows and Linux Operating System.



# Requirements

Below is a list of requirements for various configurations needed for the deployment of the Migration Process.

* Physical Servers and VMs: List any VMs or servers included in the Assessment workload.
* Storage: List of all the storage configured for servers and capacity included in the workload
* Applications: List any applications included in this Assessment workload.
* Operating Systems: List of any operating systems inlcuded in the Assesment workload.
* Dependencies: List any asset dependencies not included in the Accessment workload.

## Operational Requirements

The following is a list of operational requirements:

* The Servers to be migrated are Supported by the deployment method and Healthy
* Active Directory installed and healthy
* ExpressRoute S2S connectivity from On-premises to Azure
* Coordination with Customer on outage is necessary
* Each Application is tested and certified on the utilized resources (Azure)

# Migration Prerequisites

The Migration Prerequisites are listed below,

## Ensure prerequisites have been fulfilled

Table 1 prerequisites fulfilled prior to Installation

| Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- |
| AD and Azure are Ready |  | Subscription |
| Firewall Ports for Replication are Open |  | Firewall and Security |
| Networking Ready for Location |  | Networking |
| Configuration Server installed and Available |  | Server & Application |
| Client Outage time coordinated |  | End User Computing |
| Server / Network & App list |  |  |
| Verify App Tester team after migration |  |  |
| Notification of End User awareness for testing |  |  |
| VPN \ Jumpbox \ Credentials |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

## Physical and VMs Servers to be migrated

Below is the list of tables required to capture the current Infrastructure on Server, Network, Application eviornment

Table 2 Physical and VM’s Server to be migrated

| # | Physical / VM Server Name | Protected Y|N? | Workload |
| --- | --- | --- | --- |
|  | - |  | *Domain Controller, DNS/DHCP Server, WINS Server if any* |
|  | - |  | *Infratsructure Servers like Mail Server, Backup Server, Storage management server, Network management Server, IT Support Servers, Linux Server* |
|  | - |  | *Application Server like Data Base Server, Web Server, Deployment server* |
|  | - |  | *Virtualization Environment like Cisco UCS, HyperV, VMware , Citrix* |

## Azure Subscription target

Here are the Azure subscriptions targeted

Table 3 Azure Subscription targeted

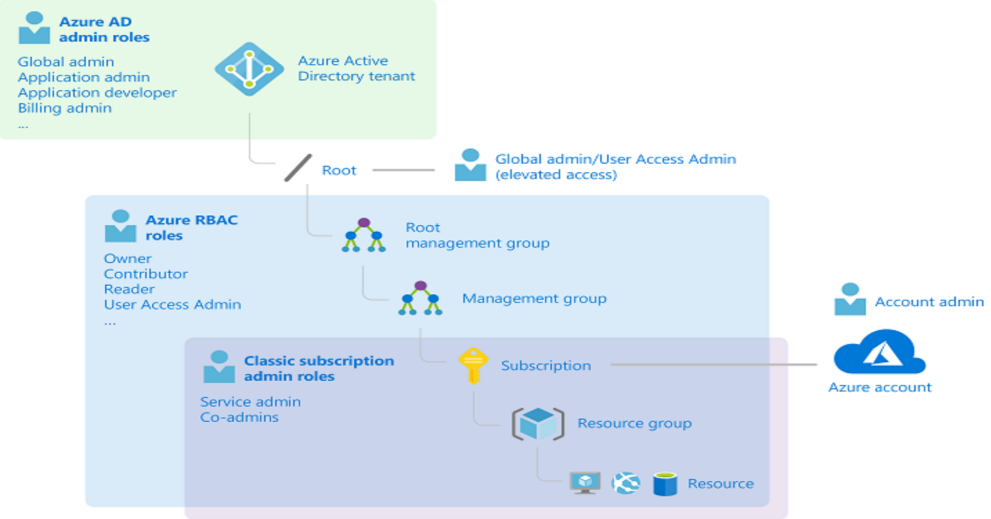
| # | Subscription Name | Type | Provisioned Y|N | ID |
| --- | --- | --- | --- | --- |
|  | <Microsoft Azure> | Production |  | ########-####-####-####-############ |
|  | <Microsoft Azure Dev\Test> | Dev\Test |  | ########-####-####-####-############ |

### Azure Role Based Access

Reference: <https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

If you are new to Azure, you may find it a little challenging to understand all the different roles in Azure. This article helps explain the following roles and when you would use each:

* Classic subscription administrator roles
* Azure role-based access control (RBAC) roles
* Azure Active Directory (Azure AD) administrator roles

The following diagram is a high-level view of how the classic subscription administrator roles, Azure RBAC roles, and Azure AD administrator roles are related.

## Azure Region to Target

Based on the Assesment data identify the region to target and create VNET1 in that specific region and then create VNET2 in another region. The two data centers have their own dark fiber for a lower latency and can be used as Active / Active or as a Site Recovery.

## Azure Resource Groups Targeted

### Azure Resource Groups – Subscription (Prod)

Table 4 Azure Resource Groups targeted

| # | Resource Group Name | Provisioned Y|N | Notes |
| --- | --- | --- | --- |
|  | RG\_VNET1\_Prod |  |  |
|  | RG\_VNET2\_Tier1 |  |  |
|  | RG\_VNET3\_Dev |  |  |
|  | RG\_VNET4\_Storage |  |  |
|  | RG\_VNET5\_Services |  |  |

### Azure Resource Groups – Subscription (Dev\Test)

Table 5 Azure Resource Groups targeted

| # | Resource Group Name | Provisioned Y|N | Notes |
| --- | --- | --- | --- |
|  | RG\_VNET1A\_Test |  |  |

## Azure VPN Gateway

The first VPN connection pairs details will be defined in this connection document.

Table 6 Azure Network targeted

| # | VPN Details | Provisioned Y|N | Notes |
| --- | --- | --- | --- |
|  | Name: VNET1\_Services \_gw  Region:  Gateway Type: VPN  SKU: VpnGw1  Virtual Network: VNET1\_Services  Gateway Subnet address range: 10.x.x.x/27  Public IP address name: VNET1\_Services\_ gw\_ip  Public IP address SKU: Basic  Assignment: Dynamic vs Static  Enable active-active mode: Enabled\Disabled  Configure BGP ASN: Enabled\Disabled |  |  |

## Azure VPN Tunnel in Site1

The first VPN connection pairs details will be defined in this connection document.

Table 7 Azure Network targeted

| # | Gateway Details | Provisioned Y|N | Notes |
| --- | --- | --- | --- |
|  | Site1 Tunnel Address1:  Site1 Tunnel Address2:  ASN Number: 65521  Neighbor Address 1:  Neighbor Address 2: |  |  |

## Azure Local Network Gateway

The first VPN connection pairs details will be defined in this connection document.

Table 8 Azure Local Network Gateway and Connection details

| # | Gateway Details | Provisioned Y|N | Notes |
| --- | --- | --- | --- |
|  | **Name:** ABC1  **Connection Type:** Site-to-Site (IPsec)  **Connections:** vnet1\_services\_ gw\_2\_ ABC1  ABC1\_2\_vnet1\_services\_ gw  **Device Vendor:**  **Device Family:**  **Firmware:**  **Tunnel IP Address:**  **Shared Key:**  **ASN Number:**  **BGP Neighbors Address:**  **Weight:** |  | **Approved Device Vendors:** <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#devicetable> |

## Azure Virtual Networks and Subnets

A list of Virtual Networks, Subnets, Network Security Groups, and Peering will be collected as part of the inventory.

For the configuration of the access control list (ACL) required to segment traffic use the following summaries. The VNET table shows the summaries of what type of workload will be used. For example, if you want to segment the workloads that are of a specific tier and only allow these workloads to talk with developers and other tier specific networks, an ACL can be established to summarize these workloads and what they are allowed to talk with.

The next level of granularity, and probably priority is the subnets. Each subnet will define a tier in the network that the workload is allowed to perform. Typically DMZ subnets are designed to be the only workloads that are authorized to have an internet endpoint.

# Azure Migration Process

The following sections outline the installation process for imaging computers in a standardized manner.

### Before you begin

Verify that you have met the following criteria before beginning your configuration:

* Make sure you have a compatible VPN device and someone who can configure it.
* Verify that you have an externally facing public IPv4 address for your VPN device. This IP address cannot be located behind a NAT.
* If you are unfamiliar with the IP address ranges located in your on-premises network configuration, you need to coordinate with someone who can provide those details for you. When you create this configuration, you must specify the IP address range prefixes that Azure will route to your on-premises location. None of the subnets of your on-premises network can overlap with the virtual network subnets that you want to connect to.

### Azure Foundations Deployment script

Azure Foundations Deployment script will deploy all respective Resource Groups, Virtual Networks, Subnets (incl GatewaySubnet, and Network Security Groups. You must onboard PowerShell to the machine where the scripts will be run.

#### Onboard PowerShell

Run the PS.Onboarding.ps1 for onboarding to PowerShell Az Modules. You can use the AzureRM modules in backwards compatibility, but it is suggested to change all modules and scripts to Az.

Table 9 PowerShell Onboarding checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Open PowerShell ISE and Ensure that the PS Execution Policy is unrestricted or remote signed |  | Set-Executionpolicy -executionpolicy unrestricted |
|  | Run PS.Onboarding.ps1 |  |  |
|  | Ensure all modules are imported for Az |  | |  | | --- | | PS C:\Users\user> Get-Module -name az\*  ModuleType Version Name ExportedCommands  ---------- ------- ---- ----------------  Script 1.7.0 az  Script 1.5.0 Az.Accounts {Add-AzEnvironment, Clear-AzContext, Clear-AzDefault, Connect-AzAccount...}  Script 1.0.1 Az.Aks {Get-AzAks, Import-AzAksCredential, New-AzAks, Remove-AzAks...}  Script 1.1.0 Az.AnalysisServices {Add-AzAnalysisServicesAccount, Export-AzAnalysisServicesInstanceLog, Get-AzAnalysisServicesSe...  Script 1.0.0 Az.ApiManagement {Add-AzApiManagementApiToProduct, Add-AzApiManagementProductToGroup, Add-AzApiManagementRegion...  Script 1.0.0 Az.ApplicationInsights {Get-AzApplicationInsights, Get-AzApplicationInsightsApiKey, Get-AzApplicationInsightsContinuo...  Script 1.2.1 Az.Automation {Export-AzAutomationDscConfiguration, Export-AzAutomationDscNodeReportContent, Export-AzAutoma...  Script 1.0.0 Az.Batch {Disable-AzBatchAutoScale, Disable-AzBatchComputeNodeScheduling, Disable-AzBatchJob, Disable-A...  Script 1.0.0 Az.Billing {Get-AzBillingInvoice, Get-AzBillingPeriod, Get-AzConsumptionBudget, Get-AzConsumptionMarketpl...  Script 1.1.0 Az.Cdn {Confirm-AzCdnEndpointProbeURL, Disable-AzCdnCustomDomain, Disable-AzCdnCustomDomainHttps, Ena...  Script 1.0.1 Az.CognitiveServices {Get-AzCognitiveServicesAccount, Get-AzCognitiveServicesAccountKey, Get-AzCognitiveServicesAcc...  Script 1.7.0 Az.Compute {Add-AzContainerServiceAgentPoolProfile, Add-AzImageDataDisk, Add-AzVhd, Add-AzVMAdditionalUna...  Script 1.0.1 Az.ContainerInstance {Get-AzContainerGroup, Get-AzContainerInstanceLog, New-AzContainerGroup, Remove-AzContainerGroup}  Script 1.0.1 Az.ContainerRegistry {Get-AzContainerRegistry, Get-AzContainerRegistryCredential, Get-AzContainerRegistryReplicatio...  Script 1.1.0 Az.DataFactory {Get-AzDataFactory, Get-AzDataFactoryActivityWindow, Get-AzDataFactoryDataset, Get-AzDataFacto...  Script 1.0.0 Az.DataLakeAnalytics {Add-AzDataLakeAnalyticsDataSource, Add-AzDataLakeAnalyticsFirewallRule, Get-AzDataLakeAnalyti...  Script 1.1.0 Az.DataLakeStore {Add-AzDataLakeStoreFirewallRule, Add-AzDataLakeStoreItemContent, Add-AzDataLakeStoreTrustedId...  Script 1.0.0 Az.DevTestLabs {Get-AzDtlAllowedVMSizesPolicy, Get-AzDtlAutoShutdownPolicy, Get-AzDtlAutoStartPolicy, Get-AzD...  Script 1.0.0 Az.Dns {Add-AzDnsRecordConfig, Get-AzDnsRecordSet, Get-AzDnsZone, New-AzDnsRecordConfig...}  Script 1.1.0 Az.EventGrid {Get-AzEventGridSubscription, Get-AzEventGridTopic, Get-AzEventGridTopicKey, Get-AzEventGridTo...  Script 1.0.1 Az.EventHub {Get-AzEventHub, Get-AzEventHubAuthorizationRule, Get-AzEventHubConsumerGroup, Get-AzEventHubG...  Script 1.0.0 Az.HDInsight {Add-AzHDInsightClusterIdentity, Add-AzHDInsightComponentVersion, Add-AzHDInsightConfigValues,...  Script 1.0.2 Az.IotHub {Add-AzIotHubCertificate, Add-AzIotHubEventHubConsumerGroup, Add-AzIotHubKey, Add-AzIotHubRout...  Script 1.1.0 Az.KeyVault {Add-AzKeyVaultCertificate, Add-AzKeyVaultCertificateContact, Add-AzKeyVaultKey, Add-AzKeyVaul...  Script 1.2.1 Az.LogicApp {Get-AzIntegrationAccount, Get-AzIntegrationAccountAgreement, Get-AzIntegrationAccountAssembly...  Script 1.0.0 Az.MachineLearning {Add-AzMlWebServiceRegionalProperty, Export-AzMlWebService, Get-AzMlCommitmentAssociation, Get...  Script 1.0.0 Az.MarketplaceOrdering {Get-AzMarketplaceTerms, Set-AzMarketplaceTerms}  Script 1.0.0 Az.Media {Get-AzMediaService, Get-AzMediaServiceKeys, Get-AzMediaServiceNameAvailability, New-AzMediaSe...  Script 1.0.1 Az.Monitor {Add-AzAutoscaleSetting, Add-AzLogProfile, Add-AzMetricAlertRule, Add-AzWebtestAlertRule...}  Script 1.6.0 Az.Network {Add-AzApplicationGatewayAuthenticationCertificate, Add-AzApplicationGatewayBackendAddressPool...  Script 1.0.0 Az.NotificationHubs {Get-AzNotificationHub, Get-AzNotificationHubAuthorizationRules, Get-AzNotificationHubListKeys...  Script 1.1.0 Az.OperationalInsights {Disable-AzOperationalInsightsIISLogCollection, Disable-AzOperationalInsightsLinuxCustomLogCol...  Script 1.0.0 Az.PolicyInsights {Get-AzPolicyEvent, Get-AzPolicyRemediation, Get-AzPolicyState, Get-AzPolicyStateSummary...}  Script 1.0.0 Az.PowerBIEmbedded {Get-AzPowerBIEmbeddedCapacity, Get-AzPowerBIWorkspace, Get-AzPowerBIWorkspaceCollection, Get-...  Script 1.2.0 Az.RecoveryServices {Backup-AzRecoveryServicesBackupItem, Disable-AzRecoveryServicesBackupAutoProtection, Disable-...  Script 1.0.0 Az.RedisCache {Export-AzRedisCache, Get-AzRedisCache, Get-AzRedisCacheFirewallRule, Get-AzRedisCacheKey...}  Script 1.0.0 Az.Relay {Get-AzRelayAuthorizationRule, Get-AzRelayHybridConnection, Get-AzRelayKey, Get-AzRelayNamespa...  Script 1.3.0 Az.Resources {Add-AzADGroupMember, Export-AzResourceGroup, Get-AzADAppCredential, Get-AzADApplication...}  Script 1.0.0 Az.ServiceBus {Complete-AzServiceBusMigration, Get-AzServiceBusAuthorizationRule, Get-AzServiceBusGeoDRConfi...  Script 1.0.1 Az.ServiceFabric {Add-AzServiceFabricApplicationCertificate, Add-AzServiceFabricClientCertificate, Add-AzServic...  Script 1.0.2 Az.SignalR {Get-AzSignalR, Get-AzSignalRKey, New-AzSignalR, New-AzSignalRKey...}  Script 1.8.0 Az.Sql {Add-AzSqlDatabaseToFailoverGroup, Add-AzSqlManagedInstanceTransparentDataEncryptionCertificat...  Script 1.2.0 Az.Storage {Add-AzRmStorageContainerLegalHold, Add-AzStorageAccountManagementPolicyAction, Add-AzStorageA...  Script 1.0.0 Az.StreamAnalytics {Get-AzStreamAnalyticsDefaultFunctionDefinition, Get-AzStreamAnalyticsFunction, Get-AzStreamAn...  Script 1.0.1 Az.TrafficManager {Add-AzTrafficManagerCustomHeaderToEndpoint, Add-AzTrafficManagerCustomHeaderToProfile, Add-Az...  Script 1.1.2 Az.Websites {Edit-AzWebAppBackupConfiguration, Enter-AzWebAppContainerPSSession, Get-AzAppServicePlan, Get...  Script 0.2.4.2 AzureAutomationAuthoringToolkit {Get-AutomationCertificate, Get-AutomationConnection, Get-AutomationVariable, Get-AzureAutomat... | |
|  | Verify onboarding |  |  |

#### Run Azure Foundations Script

Run the Azure Foundations script file to deploy Virtual Networks, Subnets and GatewaySubnet, Network Security Groups.

***Note:*** *This deployment script builds a Test Network assumed to be in a separate subscription. Foundations Default does not use VNET1A for Test. Foundations Default is usually PreProd but Test here is Research so that is why we built an extra Test VNET.*

*In Azure Foundations, VNET1A typically could be used for appliances and so on.*

Table 10 Azure Foundations deployment checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | On a dedicated deployment workstation, Open PowerShell ISE and Ensure that the PS Execution Policy is unrestricted or remote signed |  | Set-Executionpolicy -executionpolicy unrestricted **Note:** this deployment will take about an hour to complete |
|  | Set the directory of PowerShell to the root of the Azure Foundation Folder |  | C:\AzureFoundation\ |
|  | Ensure the subscription has been changed in all hardcoded areas of the script including Production and Dev\Test subscriptions |  | Open Folder in Visual Studio Code and change all occurrences of subscriptionid |
|  | Run deploy with the subscription parameters |  | PS C:\AzureFoundation\> .\Deploy.ps1 -subscriptionid 019cd503-b0b3-4997-a1a8-491e2 |
|  | Check deployment status, this should take about an hour to complete. |  |  |

### Specify DNS

DNS is not required to create a Site-to-Site connection. However, if you want to have name resolution for resources that are deployed to your virtual network, you should specify a DNS server. This setting lets you specify the DNS server that you want to use for name resolution for this virtual network. It does not create a DNS server.

Table 11 Specify a DNS Server

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | On the Settings page for your virtual network, navigate to DNS Servers and click to open the DNS servers page. |  | * DNS Servers: Select Custom. * **Add DNS server:** Enter the IP address of the DNS server that you want to use for name resolution. |
|  | When you are done adding DNS servers, click Save at the top of the page. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Create the VPN gateway

Table 12 Create the VPN gateway checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | On the left side of the portal page, click + and type 'Virtual Network Gateway' in search. In Results, locate and click Virtual network gateway. |  |  |
|  | At the bottom of the 'Virtual network gateway' page, click Create. This opens the Create virtual network gateway page. |  |  |
|  | On the Create virtual network gateway page, specify the values for your virtual network gateway. |  | [Configuration note in the VPN Gateway Section](#_Azure_VPN_Gateway)  [Configuration note in the VPN Tunnel in Site1 Section](#_Azure_VPN_Tunnel)   * Name: Name your gateway. This is not the same as naming a gateway subnet. It's the name of the gateway object you are creating. * Region: Select region * Gateway type: Select VPN. VPN gateways use the virtual network gateway type VPN. * VPN type: Select the VPN type that is specified for your configuration. Most configurations require a Route-based VPN type. * SKU: Select the gateway SKU from the dropdown. The SKUs listed in the dropdown depend on the VPN type you select. For more information about gateway SKUs, see Gateway SKUs. * Location: You may need to scroll to see Location. Adjust the Location field to point to the location where your virtual network is located. If the location is not pointing to the region where your virtual network resides, when you select a virtual network in the next step, it will not appear in the drop-down list. * Virtual network: Choose the virtual network to which you want to add this gateway. Click Virtual network to open the 'Choose a virtual network' page. Select the VNet. If you don't see your VNet, make sure the Location field is pointing to the region in which your virtual network is located. * Gateway subnet address range: You will only see this setting if you did not previously create a gateway subnet for your virtual network. If you previously created a valid gateway subnet, this setting will not appear. * First IP configuration: The 'Choose public IP address' page creates a public IP address object that gets associated to the VPN gateway. The public IP address is dynamically assigned to this object when the VPN gateway is created.   + First, click Create gateway IP configuration to open the 'Choose public IP address' page, then click +Create new to open the 'Create public IP address' page.   + Next, input a Name for your public IP address. Leave the SKU as Basic unless there is a specific reason to change it to something else, then click OK at the bottom of this page to save your changes.   Note: this will be a dynamic IP that will only change if the GW is removed and recreated. |
|  | Verify the settings. You can select Pin to dashboard at the bottom of the page if you want your gateway to appear on the dashboard. |  |  |
|  | Click Create to begin creating the VPN gateway. The settings are validated, and you'll see the "Deploying Virtual network gateway" tile on the dashboard. **Creating a gateway can take up to 45 minutes**. You may need to refresh your portal page to see the completed status. |  | *After the gateway is created, view the IP address that has been assigned to it by looking at the virtual network in the portal. The gateway appears as a connected device. You can click the connected device (your virtual network gateway) to view more information.* |
|  | Verify the configuration status |  |  |
|  | To troubleshoot connection issues, the blog links to the side may help. |  | * <https://docs.microsoft.com/en-us/archive/blogs/keithmayer/step-by-step-capturing-azure-resource-manager-arm-vnet-gateway-diagnostic-logs> * <https://blogs.technet.microsoft.com/rrasblog/2009/08/12/troubleshooting-common-vpn-related-errors/> |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Create the local network gateway

The local network gateway typically refers to your on-premises location. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you will create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

Table 13 Create the local network gateway checklist

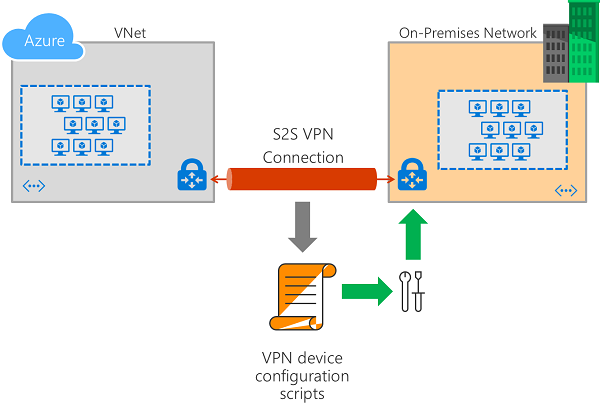
| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | In the portal, click +Create a resource |  |  |
|  | In the search box, type Local network gateway, then press Enter to search. This will return a list of results. Click Local network gateway, then click the Create button to open the Create local network gateway page. |  |  |
|  | On the Create local network gateway page, specify the values for your local network gateway. |  | [Configuration note in the Local Network Gateway](#_Azure_Local_Network)   * Name: Specify a name for your local network gateway object. * IP address: This is the public IP address of the VPN device that you want Azure to connect to. Specify a valid public IP address. The IP address cannot be behind NAT and must be reachable by Azure. * Address Space refers to the address ranges for the network that this local network represents. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks that you want to connect to. Azure will route the address range that you specify to the on-premises VPN device IP address. Use your own values here if you want to connect to your on-premises site, not the values shown in the example. * Configure BGP settings: Use only when configuring BGP. Otherwise, don't select this. * Subscription: Verify that the correct subscription is showing. * Resource Group: Select the resource group that you want to use. You can either create a new resource group or select one that you have already created. * Location: Select the location that this object will be created in. You may want to select the same location that your VNet resides in, but you are not required to do so. |
|  | When you have finished specifying the values, click the Create button at the bottom of the page to create the local network gateway. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Configure your VPN device

Site-to-Site connections to an on-premises network require a VPN device. In this step, you configure your VPN device. When configuring your VPN device, you need the following:

* A shared key. This is the same shared key that you specify when creating your Site-to-Site VPN connection. In our examples, we use a basic shared key. We recommend that you generate a more complex key to use.
* The Public IP address of your virtual network gateway. You can view the public IP address by using the Azure portal, PowerShell, or CLI. To find the Public IP address of your VPN gateway using the Azure portal, navigate to Virtual network gateways, then click the name of your gateway.



#### Configure your VPN device

Table 14 Configure your VPN device checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | See the following links for additional configuration information: |  | * For information about compatible VPN devices, see [VPN Devices](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices). * Before configuring your VPN device, check for any [Known device compatibility issues](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#known) for the VPN device that you want to use. * For links to device configuration settings, see [Validated VPN Devices](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#devicetable). The device configuration links are provided on a best-effort basis. * For an overview of VPN device configuration, see [Overview of 3rd party VPN device configurations](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-3rdparty-device-config-overview). * For IPsec/IKE policy configuration steps, see [Configure IPsec/IKE policy for S2S VPN or VNet-to-VNet connections](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-ipsecikepolicy-rm-powershell). * To connect multiple policy-based VPN devices, see [Connect Azure VPN gateways to multiple on-premises policy-based VPN devices using PowerShell](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps). |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

### Create the VPN connection

Create the Site-to-Site VPN connection between your virtual network gateway and your on-premises VPN device.

Table 15 Create VPN Connection Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Navigate to and open the page for your virtual network gateway. There are multiple ways to navigate. You can navigate to the gateway '' by going to VNet -> Overview -> Connected devices -> GW. |  |  |
|  | On the page for the VNet GW, click Connections. At the top of the Connections page, click +Add to open the Add connection page. |  |  |
|  | On the Add connection page, configure the values for your connection. |  | * For information about compatible VPN devices, see VPN Devices. * Before configuring your VPN device, check for any Known device compatibility issues for the VPN device that you want to use. * For IPsec/IKE policy configuration steps, see Configure IPsec/IKE policy for S2S VPN or VNet-to-VNet connections. * To connect multiple policy-based VPN devices, see Connect Azure VPN gateways to multiple on-premises policy-based VPN devices using PowerShell. |
|  | Click OK to create your connection. You'll see Creating Connection flash on the screen. |  |  |
|  | You can view the connection in the Connections page of the virtual network gateway. The Status will go from Unknown to Connecting, and then to Succeeded. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Verify the VPN Connection

In the Azure portal, you can view the connection status of a Resource Manager VPN Gateway by navigating to the connection. The following steps show one way to navigate to your connection and verify.

Table 16 VPN Verification Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | In the Azure portal, click All resources and navigate to your virtual network gateway. |  |  |
|  | On the blade for your virtual network gateway, click Connections. You can see the status of each connection. |  |  |
|  | Click the name of the connection that you want to verify to open Essentials. In Essentials, you can view more information about your connection. The Status is 'Succeeded' and 'Connected' when you have made a successful connection. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

#### Troubleshooting: Reset the VPN Connection

You can reset a Resource Manager VPN gateway using the Azure portal for troubleshooting purposes.

Table 17 Reset the VPN Connection Checklist (Use ONLY if needed for troubleshooting)

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Open the Azure portal and navigate to the Resource Manager virtual network gateway that you want to reset. | n/a |  |
|  | On the blade for the virtual network gateway, click 'Reset'. | n/a |  |
|  | On the Reset blade, click the Reset button. | n/a |  |
|  | If you prefer PowerShell, you can use this command: | n/a | |  | | --- | | $gw = Get-AzureRmVirtualNetworkGateway -Name VNet1GW -ResourceGroup TestRG1  Reset-AzureRmVirtualNetworkGateway -VirtualNetworkGateway $gw |   Result:  When you receive a return result, you can assume the gateway reset was successful. However, there is nothing in the return result that indicates explicitly that the reset was successful. If you want to look closely at the history to see exactly when the gateway reset occurred, you can view that information in the Azure portal. In the portal, navigate to 'GatewayName' -> Resource Health. |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

## How to Connect to a VM via VPN

You can connect to a VM that is deployed to your VNet by creating a Remote Desktop Connection to your VM. The best way to initially verify that you can connect to your VM is to connect by using its private IP address, rather than computer name. That way, you are testing to see if you can connect, not whether name resolution is configured properly.

Table 18 Connect to a VM Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Locate the private IP address. You can find the private IP address of a VM in multiple ways. Below, we show the steps for the Azure portal and for PowerShell. | n/a | * Azure portal - Locate your virtual machine in the Azure portal. View the properties for the VM. The private IP address is listed. * PowerShell - Use the example to view a list of VMs and private IP addresses from your resource groups. You don't need to modify this example before using it.  |  | | --- | | $VMs = Get-AzureRmVM  $Nics = Get-AzureRmNetworkInterface | Where VirtualMachine -ne $null  foreach($Nic in $Nics)  {  $VM = $VMs | Where-Object -Property Id -eq $Nic.VirtualMachine.Id  $Prv = $Nic.IpConfigurations | Select-Object -ExpandProperty PrivateIpAddress  $Alloc = $Nic.IpConfigurations | Select-Object -ExpandProperty PrivateIpAllocationMethod  Write-Output "$($VM.Name): $Prv,$Alloc"  } | |
|  | Verify that you are connected to your VNet using the VPN connection. | n/a |  |
|  | Open Remote Desktop Connection by typing "RDP" or "Remote Desktop Connection" in the search box on the taskbar, then select Remote Desktop Connection. You can also open Remote Desktop Connection using the 'mstsc' command in PowerShell. | n/a | Be sure to check the RDP port number on the source machine. |
|  | In Remote Desktop Connection, enter the private IP address of the VM. You can click "Show Options" to adjust additional settings, then connect. | n/a |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

## Domain Controller Configuration

Enterprise applications such as SharePoint, Dynamics AX, and SAP depend on Active Directory and a DNS infrastructure to function correctly. When you set up disaster recovery for applications, you often need to recover Active Directory and DNS before you recover other application components, to ensure correct application functionality.

You can use Site Recovery to create a disaster recovery plan for Active Directory. When a disruption occurs, you can initiate a failover. You can have Active Directory up and running in a few minutes. If you have deployed Active Directory for multiple applications in your primary site, for example, for SharePoint and SAP, you might want to fail over the complete site. You can first fail over Active Directory using Site Recovery. Then, fail over the other applications, using application-specific recovery plans.

### Prepare Active Directory

Table 19 Prepare Active Directory Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Login to a computer with Active Directory Sites and Services |  |  |
|  | Create a new site |  | Example Site Name: AZ1-ABC  Example Code:   |  | | --- | | New-ADReplicationSiteLink -Name " AZ1-ABC" | |
|  | Associate the Subnet Address space to the new site. |  | Example Subnet: 10.x.x.x/21 |
|  | Create a site link called OnPrem-Azure |  |  |
|  | Click OK on the creation window |  |  |
|  | Verify record creation is complete in \_msdcs.domain.local |  | <screenshot of records> |
|  | On the DC, open Windows PowerShell and then type Repadmin /kcc  \*\* This command recalculates the inbound replication topology for the server.  \*\* Knowledge Consistency Checker (KCC) helps generate and optimize the replication automatically between domain controllers within a site.  \*\* type Repadmin /showrepl  — To display the replication connections of a domain controller and make sure you verify that the last replication with the DC was successful…  Next, type Repadmin /bridgeheads  \*\* This command displays the bridgehead servers for the site topology…  then type : Repadmin /replsummary  \*\* This command displays a summary of replication tasks. Verify that no errors appear…  Next, type DCDiag /test:replications  \*\* Verify that all connectivity and replication tests pass successfully… |  |  |
|  | Based on the above configuration you may need to make site links for every site |  | You may need to create additional site links depending on on-prem network layout. The below configuration is to match the Azure network configuration:  LocalSite:  Site A:  Site B: |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Temporarily set DNS Servers to non-Azure

Table 20 Temporarily set DNS Servers to non-Azure Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Go to the Azure Network and select DNS non-Azure |  | <Primary DNS IP><Secondary DNS IP> |
|  | This will get changed to the DNS Servers we build in the next step |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Create Domain Controller and Replicate AD\DNS

* Best Practice for AD is to place the SYSVOL, Data, Logs on Drive E:.
* Drive C: OS, Drive D: Swap, DRIVE E: SYSVOL, Data, and Logs.

Table 21 Create Domain Controller Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Run PowerShell – Example noted in Comments |  | Example Code:  Change SiteName and DomainName and SYSVOL, Data, Logs  Best practice is Drive E  #  # Windows PowerShell script for AD DS Deployment  #  Import-Module ADDSDeployment  Install-ADDSDomainController `  -NoGlobalCatalog:$false `  -CreateDnsDelegation:$false `  -Credential (Get-Credential) `  -CriticalReplicationOnly:$false `  -DatabasePath "E:\Windows\NTDS" `  -DomainName "domain.local" `  -InstallDns:$true `  -LogPath "E:\Windows\NTDS" `  -NoRebootOnCompletion:$false `  -SiteName "TEST-AZ1 " `  -SysvolPath "E:\Windows\SYSVOL" `  -Force:$true |
|  | Enter Domain Name and Enter SafeModeAdministratorPassword then confirm the password |  |  |
|  | Manual Entry using the Server Manager GUI |  | Configure this server as an additional Active Directory domain controller for the domain "domain.local".  Site Name: TEST-AZ1  Additional Options:  Read-only domain controller: No  Global catalog: Yes  DNS Server: Yes  Update DNS Delegation: No  Source domain controller: any writable domain controller  Database folder: E:\Windows\NTDS  Log file folder: E:\Windows\NTDS  SYSVOL folder: E:\Windows\SYSVOL  The DNS Server service will be configured on this computer.  This computer will be configured to use this DNS server as its preferred DNS server. |
|  | Installation continues, and you will be signed out to complete the domain controller promotion process |  |  |
|  | Verify DC |  | <domain controller ADUC OU>  <ntds of new DC> |
|  | Verify DC Deployment |  | |  | | --- | | #Verifying domain controller deployment  $ComputerName = " AZ-DC1"  #You can also use Windows PowerShell to verify the results of installing AD DS on remote servers and promoting them as domain controllers. For example, you can use the cmdlets of the BestPractices module to perform BPA scans on remote servers. To illustrate this and continue the preceding scenario, begin by using Invoke-Command on local server to execute the Invoke-BPAModule cmdlet on remote server:  Invoke-Command -ComputerName $ComputerName -ScriptBlock  {Invoke-BpaModel -ModelId Microsoft/Windows/DirectoryServices}  #You can then execute the Get-BPAResult cmdlet on the remote server to display the results of the scan you performed by using this command:  Invoke-Command -ComputerName $ComputerName -ScriptBlock  {Get-BpaResult Microsoft/Windows/DirectoryServices} | |
|  | Change DNS on VNET to point to new DNS server in Azure.  Setup the Network config as Static Assignment for the NIC and ensure no Public IP exists. |  |  |
|  | Try to create a user and ensure a replication cycle shows the user that was created on one domain controller, exists on the other DC. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

## Assess and Migrate Hyper-V VMs & Physical Servers

### Prepare Hyper-V VMs & Physical Servers for Assessment and Migrate

To prepare for assessment of on-premises Hyper-V VMs & Physical Servers with Azure Migrate:Server Assessment, and migration of Hyper-V VMs with Azure Migrate:Server Migration.

Below is the high level steps,

* Prepare Azure. Set up permissions for your Azure account and resources to work with Azure Migrate.
* Prepare on-premises Hyper-V hosts and VMs for server assessment. You can prepare using a configuration script, or manually.
* Prepare for deployment of the Azure Migrate appliance. The appliance is used to discover and assess on-premises VMs.
* Prepare on-premises Hyper-V hosts and VMs for server migration.

**Prepare Azure**

Azure Permissions

Below is the Permission required for Azure Migration deployment

|  |  |
| --- | --- |
| **Task** | **Details** |
| Create an Azure Migrate Project | Azure Account needs Contributer or Owner Permissions to cerate a Project |
| Register resource provides | Azure Migrate uses a lightweight Azure Migrate applicance to discover and assess Hyper-V VMs with Azure Migrate Server Assessment.  During Applicance registration, resource providers are registered with the subscription chosen in the applicance.  To register the resource providers, you need a Contributor or Owner role on the subscription. |
| Create Azure AD app | When registering the appliance, Azure Migrate creates an Azure Active Directory (Azure AD) app that’s used for communication between the agents running on the appliance with their respective services running on Azure. |

**Assign permissions to create project**

Check you have permissions to create an Azure Migrate project.

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.
3. You should have **Contributor** or **Owner** permissions.
   * If you just created a free Azure account, you're the owner of your subscription.
   * If you're not the subscription owner, work with the owner to assign the role.

**Assign permissions to register the appliance**

You can assign permissions for Azure Migrate to create the Azure AD app during appliance registration, using one of the following methods:

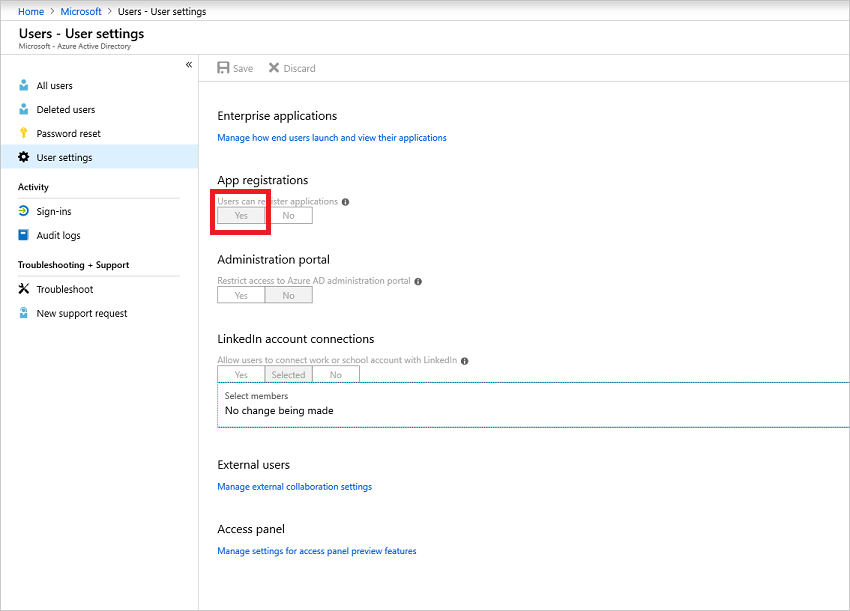
* A tenant/global admin can grant permissions to users in the tenant, to create and register Azure AD apps.
* A tenant/global admin can assign the Application Developer role (that has the permissions) to the account.

**Note**: The app does not have any other access permissions on the subscription other than those described above.

* You only need these permissions when you register a new appliance. You can remove the permissions after the appliance is set up.

**Grant account permissions**

The tenant/global admin can grant permissions as follows:

1. In Azure AD, the tenant/global admin should navigate to **Azure Active Directory** > **Users** > **User Settings**.
2. The admin should set **App registrations** to **Yes**.

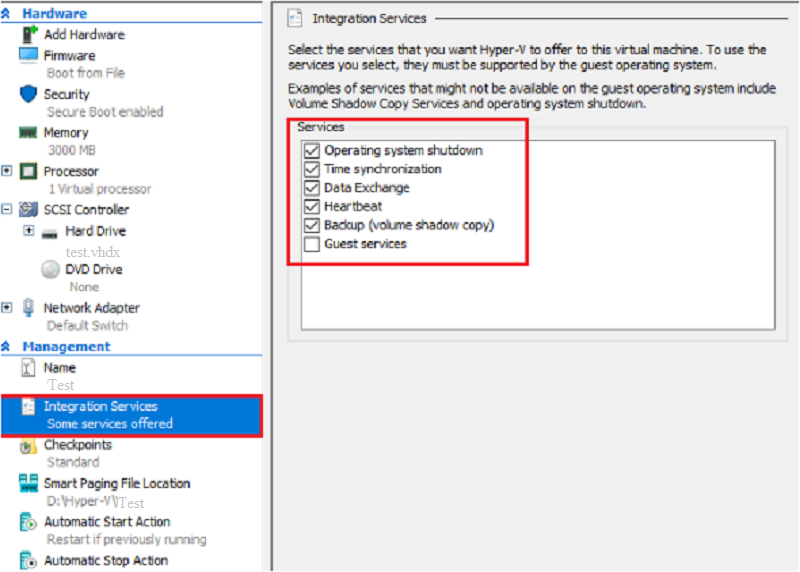
**Note**: This is a default setting that isn't sensitive.

**Assign Application Developer role**

The tenant/global admin can assign the Application Developer role to an account.

**Prepare Hyper-V for assessment**

You can prepare Hyper-V for VM assessment manually, or using a configuration script. Preparation steps are as follows:

* [Verify](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v#hyper-v-host-requirements) Hyper-V host settings, and make sure that the [required ports](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v#port-access) are open on Hyper-V hosts.
* Set up PowerShell remoting on each host, so that the Azure Migrate appliance can run PowerShell commands on the host, over a WinRM connection.
* Delegate credentials if VM disks are located on remote SMB shares.
* Set up an account that the appliance will use to discover VMs on Hyper-V hosts.
* Set up Hyper-V Integration Services on each VM you want to discover and assess. The default settings when you enable Integration Services are sufficient for Azure Migrate.

**Prepare with a script**

The script does the following:

* Checks that you're running the script on a supported PowerShell version.
* Verifies that you (the user running the script) have administrative privileges on the Hyper-V host.
* Allows you to create a local user account (not administrator) that the Azure Migrate service uses to communicate with the Hyper-V host. This user account is added to these groups on the host:
  + Remote Management Users
  + Hyper-V Administrators
  + Performance Monitor Users
* Checks that the host is running a supported version of Hyper-V, and the Hyper-V role.
* Enables the WinRM service, and opens ports 5985 (HTTP) and 5986 (HTTPS) on the host (needed for metadata collection).
* Enables PowerShell remoting on the host.
* Checks that the Hyper-V Integration Services is enabled on all VMs managed by the host.
* Enables CredSSP on the host if needed.

Run the script as follows:

1. Make sure you have PowerShell version 4.0 or later installed on the Hyper-V host.
2. Download the script from the [Microsoft Download Center](https://aka.ms/migrate/script/hyperv). The script is cryptographically signed by Microsoft.
3. Validate the script integrity using either MD5, or SHA256 hash files. Hashtag values are below. Run this command to generate the hash for the script:

Copy

C:\>CertUtil -HashFile <file\_location> [Hashing Algorithm]

Example usage:

Copy

C:\>CertUtil -HashFile C:\Users\Administrators\Desktop\ MicrosoftAzureMigrate-Hyper-V.ps1

SHA256

1. After validating the script integrity, run the script on each Hyper-V host with this PowerShell command: PS C:\Users\Administrators\Desktop> MicrosoftAzureMigrate-Hyper-V.ps1

**Hashtag values**

Hash values captured

**Prepare manually**

Follow the procedures in this section to prepare Hyper-V manually, instead of using the script.

**Verify PowerShell version**

Make sure you have PowerShell version 4.0 or later installed on the Hyper-V host.

**Set up an account for VM discovery**

Azure Migrate needs permissions to discover on-premises VMs.

* Set up a domain or local user account with administrator permissions on the Hyper-V hosts/cluster.
  + - You need a single account for all hosts and clusters that you want to include in the discovery.
    - The account can be a local or domain account. We recommend it has Administrator permissions on the Hyper-V hosts or clusters.
    - Alternatively, if you don't want to assign Administrator permissions, the following permissions are needed:
      * Remote Management Users
      * Hyper-V Administrators
      * Performance Monitor Users

**Verify Hyper-V host settings**

1. Verify [Hyper-V host requirements](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v#hyper-v-host-requirements) for server assessment.
2. Make sure the [required ports](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v#port-access) are open on Hyper-V hosts.

**Enable PowerShell remoting on hosts**

Set up PowerShell remoting on each host, as follows:

1. On each host, open a PowerShell console as admin.
2. Run this command:

Copy

Enable-PSRemoting -force

**Enable Integration Services on VMs**

Integration Services should be enabled on each VM so that Azure Migrate can capture operating system information on the VM.

On VMs that you want to discover and assess, enable [Hyper-V Integration Services](https://docs.microsoft.com/windows-server/virtualization/hyper-v/manage/manage-hyper-v-integration-services) on each VM.

**Enable CredSSP on hosts**

If the host has VMs with disks are located on SMB shares, complete this step on the host.

* You can run this command remotely on all Hyper-V hosts.
* If you add new host nodes on a cluster they are automatically added for discovery, but you need to manually enable CredSSP on the new nodes if needed.

Enable as follows:

1. Identify Hyper-V hosts running Hyper-V VMs with disks on SMB shares.
2. Run the following command on each identified Hyper-V host:

Copy

Enable-WSManCredSSP -Role Server -Force

When you set up the appliance, you finish setting up CredSSP by enabling it on the appliance. This is described in the next tutorial in this series.

**Prepare for appliance deployment**

Before setting up the Azure Migrate appliance and beginning assessment in the next tutorial, prepare for appliance deployment.

1. [Verify](https://docs.microsoft.com/en-us/azure/migrate/migrate-appliance#appliance---hyper-v) appliance requirements.
2. Review the Azure URLs that the appliance will need to access in the public and government clouds. If you're using a URL-based firewall or proxy, ensure it allows access to the required URLs.
3. Review the data that the appliance will collect during discovery and assessment.
4. [Review](https://docs.microsoft.com/en-us/azure/migrate/migrate-appliance#collected-data---hyper-v) port access requirements for the appliance.

**Prepare for Hyper-V migration**

1. [Review](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v-migration#hyper-v-hosts) Hyper-V host requirements for migration, and the Azure URLs to which Hyper-V hosts and clusters need access for VM migration.
2. [Review](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v-migration#hyper-v-vms) the requirements for Hyper-V VMs that you want to migrate to Azure.

### Assess Hyper-V VMs & Physical Servers for Migration

To Assess On-Premises Hyper-V VMs & Physical Servers using the [Azure Migrate:Server Assessment](https://docs.microsoft.com/en-us/azure/migrate/migrate-services-overview#azure-migrate-server-assessment-tool) tool.

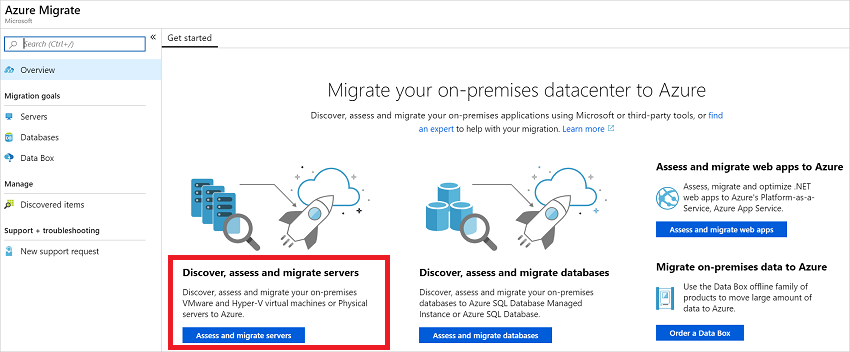
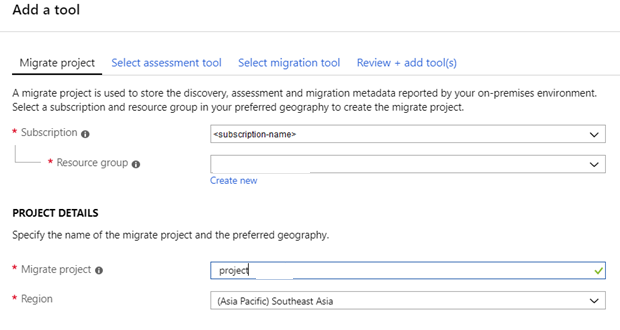
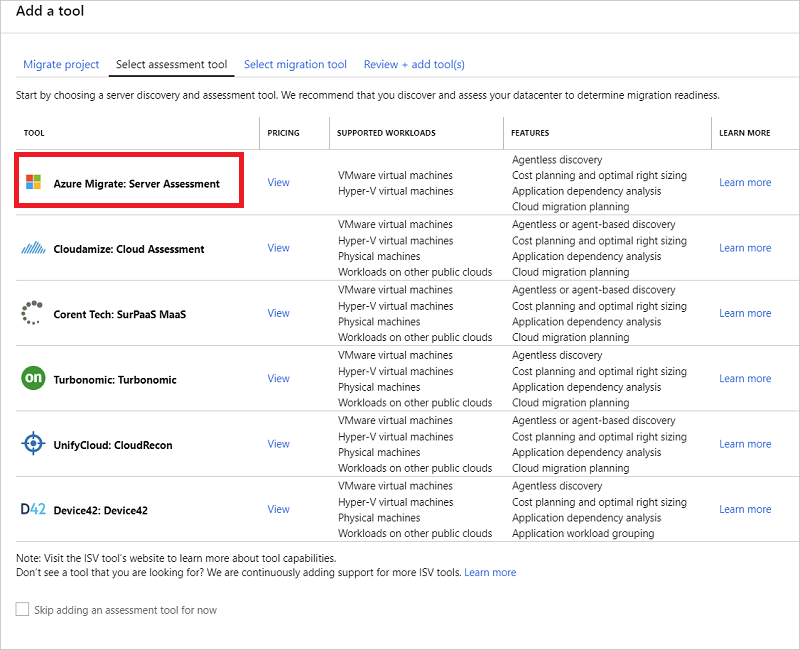
Below is the high level steps on assessing Hyper-V VMs & Physical Servers for Migraiton,

* Set up an Azure Migrate project.
* Set up and register an Azure Migrate appliance.
* Start continuous discovery of on-premises VMs.
* Group discovered VMs, and assess the group.
* Review the assessment.

**Prerequisites**

* Prepare Azure to work with Azure Migrate.
* Prepare Hyper-V hosts and VMs assessment.
* Verify what you need in order to deploy the Azure Migrate appliance for Hyper-V assessment.

**Set up an Azure Migrate project**

1. In the Azure portal > **All services**, search for **Azure Migrate**.
2. In the search results, select **Azure Migrate**.
3. In **Overview**, under **Discover, assess and migrate servers**, click **Assess and migrate servers**.
4. In Getting started, click Add tools.
5. In the Migrate project tab, select your Azure subscription, and create a resource group if you don't have one.
6. In Project Details, specify the project name, and the region in which you want to create the project. Review supported geographies for [public](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix#supported-geographies-public-cloud) and [government clouds](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix#supported-geographies-azure-government).
   * The project region is used only to store the metadata gathered from on-premises VMs.
   * You can select a different Azure target region when you migrate the VMs. All Azure regions are supported for migration target.
7. Click **Next**.
8. In **Select assessment tool**, select **Azure Migrate: Server Assessment** > **Next**.
9. In **Select migration tool**, select **Skip adding a migration tool for now** > **Next**.
10. In **Review + add tools**, review the settings, and click **Add tools**.
11. Wait a few minutes for the Azure Migrate project to deploy. You'll be taken to the project page. If you don't see the project, you can access it from **Servers** in the Azure Migrate dashboard.

**Set up the Azure Migrate appliance**

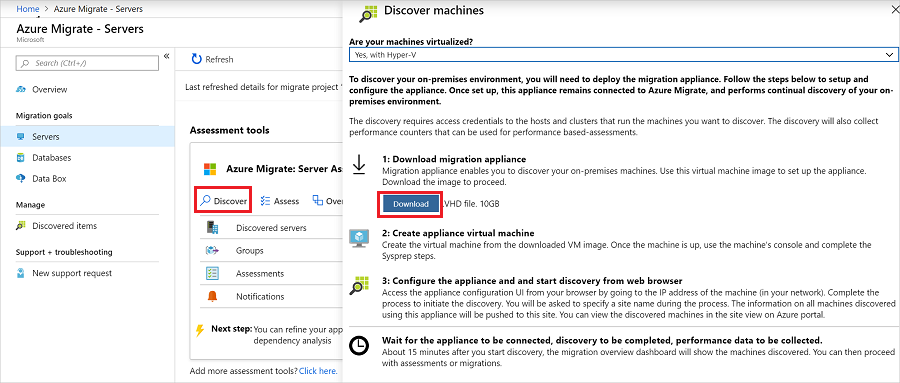
Azure Migrate:Server Assessment uses a lightweight Azure Migrate appliance. The appliance performs VM discovery and sends VM metadata and performance data to Azure Migrate. The appliance can be set up in a number of ways.

* Set up on a Hyper-V VM using a downloaded Hyper-V VHD. This is the method used in this tutorial.
* Set up on a Hyper-V VM or physical machine with a PowerShell installer script. [This method](https://docs.microsoft.com/en-us/azure/migrate/deploy-appliance-script) should be used if you can't set up a VM using the VHD, or if you're in Azure Government.

After creating the appliance, you check that it can connect to Azure Migrate:Server Assessment, configure it for the first time, and register it with the Azure Migrate project.

**Download the VHD**

Download the zipped VHD template for the appliance.

1. In **Migration Goals** > **Servers** > **Azure Migrate: Server Assessment**, click **Discover**.
2. In **Discover machines** > **Are your machines virtualized?**, click **Yes, with Hyper-V**.
3. Click **Download** to download the VHD file.

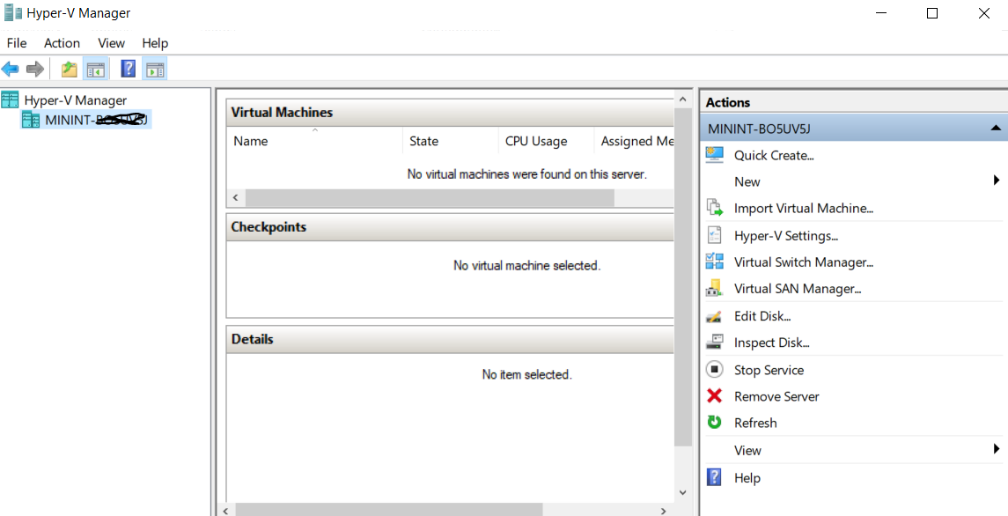
**Verify security**

Check that the zipped file is secure, before you deploy it.

1. On the machine to which you downloaded the file, open an administrator command window.
2. Run the following PowerShell command to generate the hash for the ZIP file
   * C:\>Get-FileHash -Path <file\_location> -Algorithm [Hashing Algorithm]
   * Example usage: C:\>Get-FileHash -Path ./AzureMigrateAppliance\_v1.19.06.27.zip -Algorithm SHA256
3. For appliance version 2.19.07.30, the generated hash should match these settings.

**Create the appliance VM**

Import the downloaded file, and create the VM.

1. After downloading the zipped VHD file to the Hyper-V host on which the appliance VM will be placed, extract the zipped file.
   * In the extracted location, the file unzips into a folder called **AzureMigrateAppliance\_VersionNumber**.
   * This folder contains a subfolder, also called **AzureMigrateAppliance\_VersionNumber**.
   * This subfolder contains three further subfolders - **Snapshots**, **Virtual Hard Disks**, and **Virtual Machines**.
2. Open Hyper-V Manager. In **Actions**, click **Import Virtual Machine**.
3. In the Import Virtual Machine Wizard > **Before you begin**, click **Next**.
4. In **Locate Folder**, select the **Virtual Machines** folder. Then click **Next**.
5. In **Select Virtual Machine**, click **Next**.
6. In **Choose Import Type**, click **Copy the virtual machine (create a new unique ID)**. Then click **Next**.
7. In **Choose Destination**, leave the default setting. Click **Next**.
8. In **Storage Folders**, leave the default setting. Click **Next**.
9. In **Choose Network**, specify the virtual switch that the VM will use. The switch needs internet connectivity to send data to Azure.
10. In **Summary**, review the settings. Then click **Finish**.
11. In Hyper-V Manager > **Virtual Machines**, start the VM.

**Verify appliance access to Azure**

Make sure that the appliance VM can connect to Azure URLs for [public](https://docs.microsoft.com/en-us/azure/migrate/migrate-appliance#public-cloud-urls) and [government](https://docs.microsoft.com/en-us/azure/migrate/migrate-appliance#government-cloud-urls) clouds.

**Configure the appliance**

Set up the appliance for the first time.

**Note**: If you set up the appliance using a [PowerShell script](https://docs.microsoft.com/en-us/azure/migrate/deploy-appliance-script) instead of the downloaded VHD, the first two steps in this procedure aren't relevant.

1. In Hyper-V Manager > **Virtual Machines**, right-click the VM > **Connect**.
2. Provide the language, time zone, and password for the appliance.
3. Open a browser on any machine that can connect to the VM, and open the URL of the appliance web app: **https://*appliance name or IP address*: 44368**.

Alternately, you can open the app from the appliance desktop by clicking the app shortcut.

1. In the web app > **Set up prerequisites**, do the following:
   * **License**: Accept the license terms, and read the third-party information.
   * **Connectivity**: The app checks that the VM has internet access. If the VM uses a proxy:
     + Click **Proxy settings**, and specify the proxy address and listening port, in the form http://ProxyIPAddress or http://ProxyFQDN.
     + Specify credentials if the proxy needs authentication.
     + Only HTTP proxy is supported.
   * **Time sync**: Time is verified. The time on the appliance should be in sync with internet time for VM discovery to work properly.
   * **Install updates**: Azure Migrate Server Assessment checks that the appliance has the latest updates installed.

**Register the appliance with Azure Migrate**

1. Click **Log In**. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.
2. On the new tab, sign in using your Azure credentials.
   * Sign in with your username and password.
   * Sign-in with a PIN isn't supported.
3. After successfully signing in, go back to the web app.
4. Select the subscription in which the Azure Migrate project was created. Then select the project.
5. Specify a name for the appliance. The name should be alphanumeric with 14 characters or less.
6. Click **Register**.

**Delegate credentials for SMB VHDs**

If you're running VHDs on SMBs, you must enable delegation of credentials from the appliance to the Hyper-V hosts. This requires the following:

* You enable each host to act as a delegate for the appliance. If you followed the tutorials in order, you did this in the previous tutorial, when you prepared Hyper-V for assessment and migration. You should have either set up CredSSP for the hosts manually, or by running a script that does this.
* Enable CredSSP delegation so that the Azure Migrate appliance can act as the client, delegating credentials to a host.

Enable on the appliance as follows:

**Option 1**

On the appliance VM, run this command. HyperVHost1/HyperVHost2 are example host names.

Copy

Enable-WSManCredSSP -Role Client -DelegateComputer HyperVHost1.contoso.com HyperVHost2.contoso.com -Force

Example: Enable-WSManCredSSP -Role Client -DelegateComputer HyperVHost1.contoso.com HyperVHost2.contoso.com -Force

**Option 2**

Alternatively, do this in the Local Group Policy Editor on the appliance:

1. In **Local Computer Policy** > **Computer Configuration**, click **Administrative Templates** > **System** > **Credentials Delegation**.
2. Double-click **Allow delegating fresh credentials**, and select **Enabled**.
3. In **Options**, click **Show**, and add each Hyper-V host you want to discover to the list, with **wsman/** as a prefix.
4. Then, in **Credentials Delegation**, double-click **Allow delegating fresh credentials with NTLM-only server authentication**. Again, add each Hyper-V host you want to discover to the list, with **wsman/** as a prefix.

**Start continuous discovery**

Connect from the appliance to Hyper-V hosts or clusters, and start VM discovery.

1. In **User name** and **Password**, specify the account credentials that the appliance will use to discover VMs. Specify a friendly name for the credentials, and click **Save details**.
2. Click **Add host**, and specify Hyper-V host/cluster details.
3. Click **Validate**. After validation, the number of VMs that can be discovered on each host/cluster is shown.
   * If validation fails for a host, review the error by hovering over the icon in the **Status** column. Fix issues, and validate again.
   * To remove hosts or clusters, select > **Delete**.
   * You can't remove a specific host from a cluster. You can only remove the entire cluster.
   * You can add a cluster, even if there are issues with specific hosts in the cluster.
4. After validation, click **Save and start discovery** to start the discovery process.

This starts discovery. It takes around 1.5 minutes per host for metadata of discovered servers to appear in the Azure portal.

**Verify VMs in the portal**

After discovery finishes, you can verify that the VMs appear in the portal.

1. Open the Azure Migrate dashboard.
2. In **Azure Migrate - Servers** > **Azure Migrate: Server Assessment** page, click the icon that displays the count for **Discovered servers**.

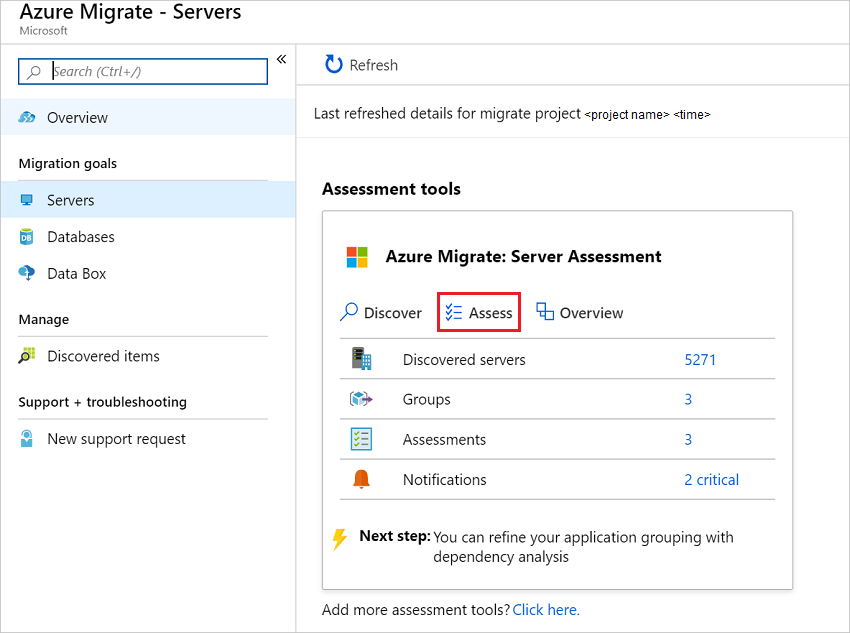
**Set up an assessment**

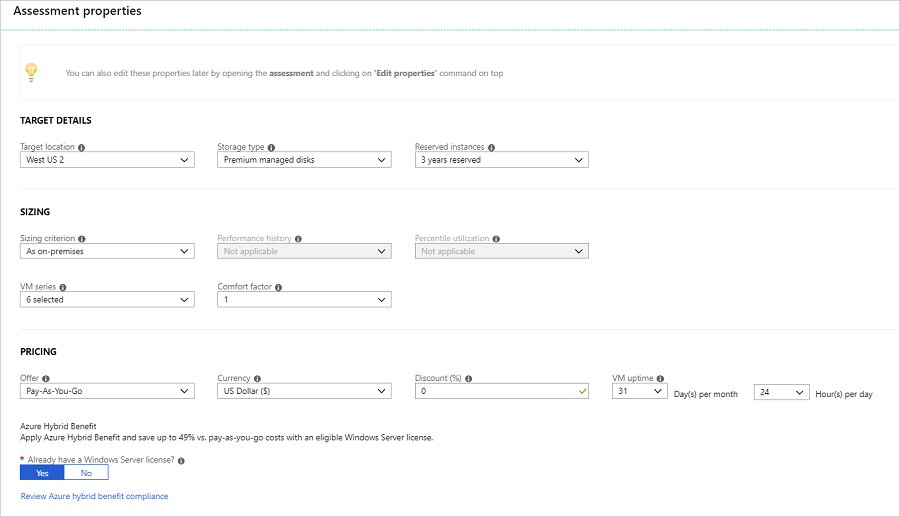
There are two types of assessments you can run using Azure Migrate Server Assessment.

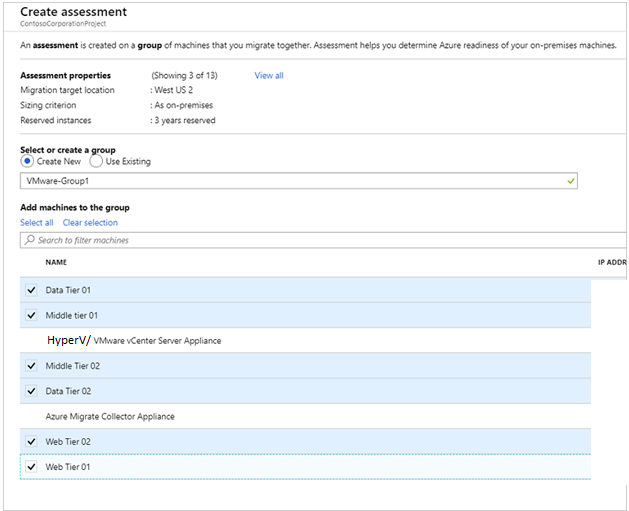
| **Assessment** | **Details** | **Data** |
| --- | --- | --- |
| **Performance-based** | Assessments based on collected performance data | **Recommended VM size**: Based on CPU and memory utilization data.  **Recommended disk type (standard or premium managed disk)**: Based on the IOPS and throughput of the on-premises disks. |
| **As on-premises** | Assessments based on on-premises sizing. | **Recommended VM size**: Based on the on-premises VM size  **Recommended disk type**: Based on the storage type setting you select for the assessment. |

**Run an assessment**

Run an assessment as follows:

1. Review the [best practices](https://docs.microsoft.com/en-us/azure/migrate/best-practices-assessment) for creating assessments.
2. In **Servers** > **Azure Migrate: Server Assessment**, click **Assess**.
3. In **Assess Servers**, specify a name for the assessment.
4. Click **View all** to review the assessment properties.



1. In **Select or create a group**, select **Create New**, and specify a group name. A group gathers one or more VMs together for assessment.
2. In **Add machines to the group**, select VMs to add to the group.
3. Click **Create Assessment** to create the group, and run the assessment.
4. After the assessment is created, view it in **Servers** > **Azure Migrate: Server Assessment**.
5. Click **Export assessment**, to download it as an Excel file.

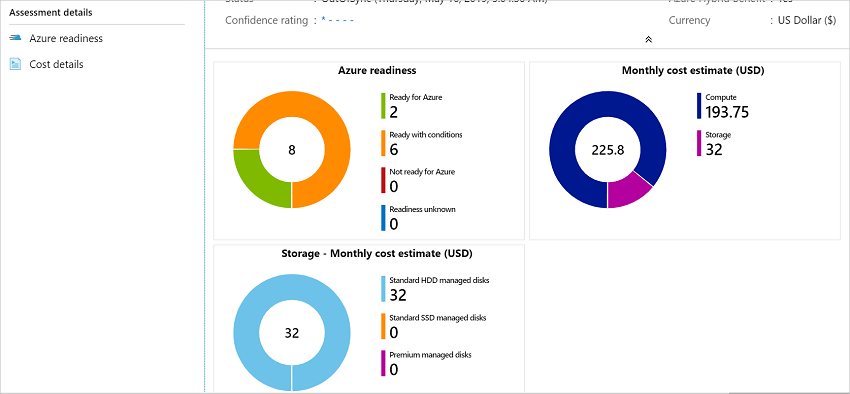
**Review an assessment**

An assessment describes:

* **Azure readiness**: Whether VMs are suitable for migration to Azure.
* **Monthly cost estimation**: The estimated monthly compute and storage costs for running the VMs in Azure.
* **Monthly storage cost estimation**: Estimated costs for disk storage after migration.

**View an assessment**

1. In **Migration goals** > **Servers** > **Azure Migrate: Server Assessment**, click **Assessments**.
2. In **Assessments**, click on an assessment to open it.

Example snapshot of Assessment details:

**Review Azure readiness**

1. In **Azure readiness**, verify whether VMs are ready for migration to Azure.
2. Review the VM status:
   * **Ready for Azure**: Azure Migrate recommends a VM size and cost estimates for VMs in the assessment.
   * **Ready with conditions**: Shows issues and suggested remediation.
   * **Not ready for Azure**: Shows issues and suggested remediation.
   * **Readiness unknown**: Used when Azure Migrate can't assess readiness, due to data availability issues.
3. Click on an **Azure readiness** status. You can view VM readiness details, and drill down to see VM details, including compute, storage, and network settings.

**Review cost details**

This view shows the estimated compute and storage cost of running VMs in Azure.

1. Review the monthly compute and storage costs. Costs are aggregated for all VMs in the assessed group.
   * Cost estimates are based on the size recommendations for a machine, and its disks and properties.
   * Estimated monthly costs for compute and storage are shown.
   * The cost estimation is for running the on-premises VMs as IaaS VMs. Azure Migrate Server Assessment doesn't consider PaaS or SaaS costs.
2. You can review monthly storage cost estimates. This view shows aggregated storage costs for the assessed group, split over different types of storage disks.
3. You can drill down to see details for specific VMs.

### Migrate Hyper-V VMs & Physical Servers to Azure

Migrate On-Premises Hyper-V VMs & Physical Servers to Azure using Agentless Migration with Azure Migrate: Server Migration Tool.

Azure Migrate provides a central hub to track discovery, assessment, and migration of your on-premises apps and workloads, and private/public cloud VMs, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

Below is the High level details on requirement,

* Prepare Azure and your on-premises Hyper-V environment
* Set up the source environment.
* Set up the target environment.
* Enable replication.
* Run a test migration to make sure everything's working as expected.
* Run a full migration to Azure.

**Prerequisites**

Before you begin below steps has to be verified:

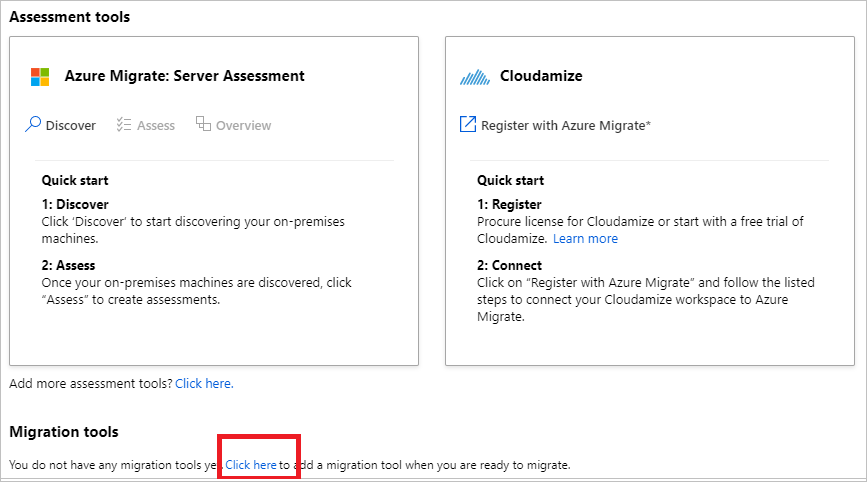
1. [Review](https://docs.microsoft.com/en-us/azure/migrate/hyper-v-migration-architecture) the Hyper-V migration architecture.
2. [Review](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v-migration#hyper-v-hosts) Hyper-V host requirements, and the Azure URLs that the Hyper-V hosts need to access.
3. [Review](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v-migration#hyper-v-vms) requirements for Hyper-V VMs that you want to migrate. Hyper-V VMs must conform with [Azure VM requirements](https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-hyper-v-migration#azure-vm-requirements).

Note: For migrating Hyper-V VMs, Azure Migrate:Server Migration runs software agents (Microsoft Azure Site Recovery provider and Microsoft Azure Recovery Service agent) on Hyper-V Hosts or cluster nodes, to orchestrate and replicate data to Azure Migrate. The Azure Migrate appliance isn't used for Hyper-V migration.

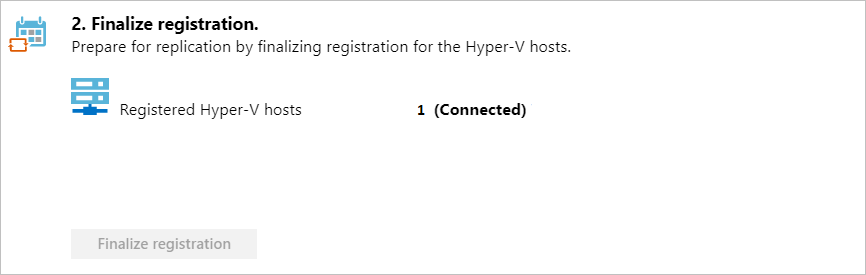
1. Make sure that your Azure account is assigned the Virtual Machine Contributor role, so that you have permissions to:
   * Create a VM in the selected resource group.
   * Create a VM in the selected virtual network.
   * Write to an Azure managed disk.
2. Set up an Azure network. When you migrate to Azure, the created Azure VMs are joined to an Azure network you specify when you set up migration.

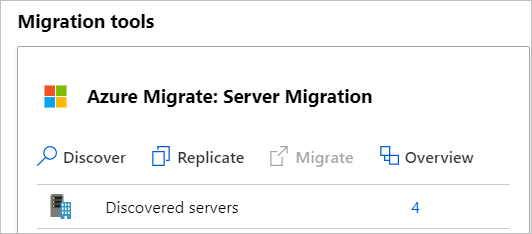
**Add the Azure Migrate:Server Migration tool**

If you have a project set up, add the tool as follows:

1. In the Azure Migrate project, click **Overview**.
2. In **Discover, assess, and migration servers**, click **Assess and migrate servers**.
3. In **Migration tools**, select **Click here to add a migration tool when you are ready to migrate**.
4. In the tools list, select **Azure Migrate: Server Migration** > **Add tool**

**Prepare Hyper-V hosts**

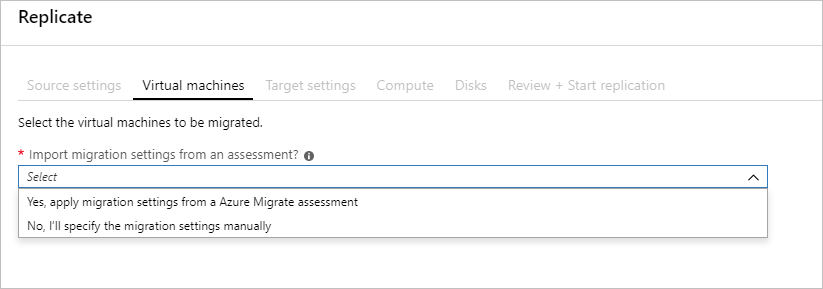
1. In the Azure Migrate project > **Servers**, in **Azure Migrate: Server Migration**, click **Discover**.
2. In **Discover machines** > **Are your machines virtualized?**, select **Yes, with Hyper-V**.
3. In **Target region**, select the Azure region to which you want to migrate the machines.
4. Select **Confirm that the target region for migration is region-name**.
5. Click **Create resources**. This creates an Azure Site Recovery vault in the background.
   * If you've already set up migration with Azure Migrate Server Migration, this option won't appear since resources were set up previously.
   * You can't change the target region for this project after clicking this button.
   * All subsequent migrations are to this region.
6. In **Prepare Hyper-V host servers**, download the Hyper-V Replication provider, and the registration key file.
   * The registration key is needed to register the Hyper-V host with Azure Migrate Server Migration.
   * The key is valid for five days after you generate it.
7. Copy the provider setup file and registration key file to each Hyper-V host (or cluster node) running VMs you want to replicate.
8. Run the provider setup file on each host, as described in the next procedure.
9. After installing the provider on hosts, in **Discover machines**, click **Finalize registration**.

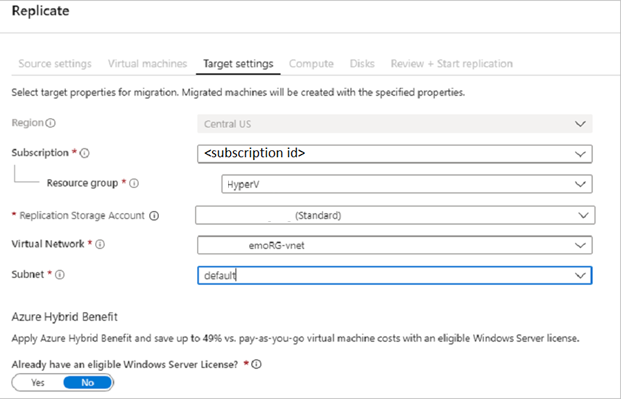
It can take up to 15 minutes after finalizing registration until discovered VMs appear in Azure Migrate Server Migration. As VMs are discovered, the **Discovered servers** count rises.

**Replicate Hyper-V VMs**

With discovery completed, you can begin replication of Hyper-V VMs to Azure.

Note: You can replicate up to 10 machines together. If you need to replicate more, then replicate them simultaneously in batches of 10.

1. In the Azure Migrate project > **Servers**, **Azure Migrate: Server Migration**, click **Replicate**.
2. In **Replicate**, > **Source settings** > **Are your machines virtualized?**, select **Yes, with Hyper-V**. Then click **Next: Virtual machines**.
3. In **Virtual machines**, select the machines you want to replicate.
   * If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. To do this, in **Import migration settings from an Azure Migrate assessment?**, select the **Yes** option.
   * If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** options.
   * If you selected to use the assessment, select the VM group, and assessment name.
4. In **Virtual machines**, search for VMs as needed, and check each VM you want to migrate. Then, click **Next: Target settings**.
5. In **Target settings**, select the target region to which you'll migrate, the subscription, and the resource group in which the Azure VMs will reside after migration.
6. In **Replication Storage Account**, select the Azure Storage account in which replicated data will be stored in Azure.
7. **Virtual Network**, select the Azure VNet/subnet to which the Azure VMs will be joined after migration.
8. In **Azure Hybrid Benefit**:
   * Select **No** if you don't want to apply Azure Hybrid Benefit. Then, click **Next**.
   * Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions, and you want to apply the benefit to the machines you're migrating. Then click **Next**.



1. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with Azure requirements.
   * **VM size**: If you're using assessment recommendations, the VM size dropdown will contain the recommended size. Otherwise Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in **Azure VM size**.
   * **OS disk**: Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
   * **Availability set**: If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.
2. In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium-managed disks) in Azure. Then click **Next**.
   * You can exclude disks from replication.
   * If you exclude disks, won't be present on the Azure VM after migration.
3. In **Review and start replication**, review the settings, and click **Replicate** to start the initial replication for the servers.

**Note:** You can update replication settings any time before replication starts, in **Manage** > **Replicating machines**. Settings can't be changed after replication starts.

**Provisioning for the first time**

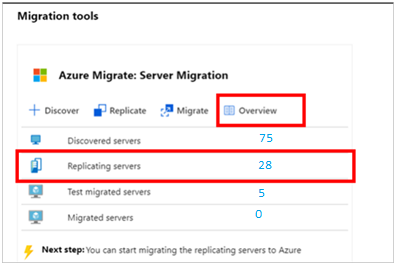
If this is the first VM you're replicating in the Azure Migrate project, Azure Migrate: Server Migration automatically provisions these resources in same resource group as the project.

* **Service bus**: Azure Migrate: Server Migration uses the Service Bus to send replication orchestration messages to the appliance.
* **Gateway storage account**: Azure Migrate: Server Migration uses the gateway storage account to store state information about the VMs being replicated.
* **Log storage account**: The Azure Migrate appliance uploads replication logs for VMs to a log storage account. Azure Migrate applies the replication information to the replica-managed disks.
* **Key vault**: The Azure Migrate appliance uses the key vault to manage connection strings for the service bus, and access keys for the storage accounts used in replication. You should have set up the permissions that the key vault needs to access the storage account when you prepared Azure for Hyper-V VM assessment and migration.

**Track and monitor**

* When you click **Replicate** a Start Replication job begins.
* When the Start Replication job finishes successfully, the machines begin their initial replication to Azure.
* After initial replication finishes, delta replication begins. Incremental changes to on-premises disks are periodically replicated to Azure.

You can track job status in the portal notifications.

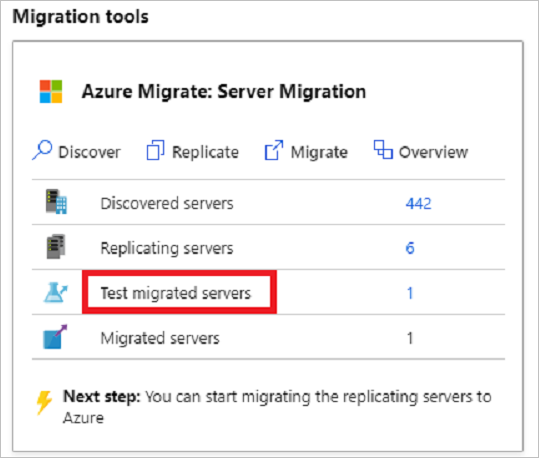
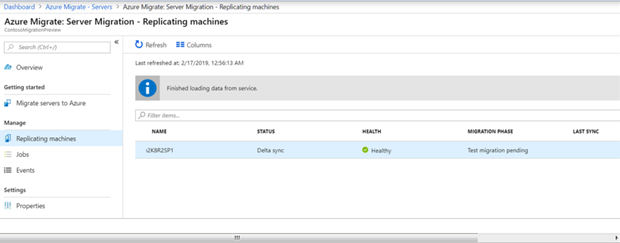
You can monitor replication status by clicking on **Replicating servers** in **Azure Migrate: Server Migration**.

**Run a test migration**

When delta replication begins, you can run a test migration for the VMs, before running a full migration to Azure. We highly recommend that you do this at least once for each machine, before you migrate it.

* Running a test migration checks that migration will work as expected, without impacting the on-premises machines, which remain operational, and continue replicating.
* Test migration simulates the migration by creating an Azure VM using replicated data (usually migrating to a non-production Azure VNet in your Azure subscription).
* You can use the replicated test Azure VM to validate the migration, perform app testing, and address any issues before full migration.

Do a test migration as follows:

1. In **Migration goals** > **Servers** > **Azure Migrate: Server Migration**, click **Test migrated servers**.
2. Right-click the VM to test, and click **Test migrate**.
3. In **Test Migration**, select the Azure virtual network in which the Azure VM will be located after the migration. We recommend you use a non-production virtual network.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.
6. After the test is done, right-click the Azure VM in **Replicating machines**, and click **Clean up test migration**.

**Migrate VMs**

After you've verified that the test migration works as expected, you can migrate the on-premises Servers and HyperV VMs.

1. In the Azure Migrate project > **Servers** > **Azure Migrate: Server Migration**, click **Replicating servers**.
2. In **Replicating machines**, right-click the VM > **Migrate**.
3. In **Migrate** > **Shut down virtual machines and perform a planned migration with no data loss**, select **Yes** > **OK**.
   * By default Azure Migrate shuts down the on-premises VM, and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This ensures no data loss.
   * If you don't want to shut down the VM, select **No**
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

**Complete the migration**

1. After the migration is done, right-click the VM > **Stop migration**. This does the following:
   * Stops replication for the on-premises machine.
   * Removes the machine from the **Replicating servers** count in Azure Migrate: Server Migration.
   * Cleans up replication state information for the VM.
2. Install the Azure VM Windows or Linux agent on the migrated machines.
3. Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
4. Perform final application and migration acceptance testing on the migrated application now running in Azure.
5. Cut over traffic to the migrated Azure VM instance.
6. Remove the on-premises VMs from your local VM inventory.
7. Remove the on-premises VMs from local backups.
8. Update any internal documentation to show the new location and IP address of the Azure VMs.

**Post-migration best practices**

* For increased resilience:
  + Keep data secure by backing up Azure VMs using the Azure Backup service.
  + Keep workloads running and continuously available by replicating Azure VMs to a secondary region with Site Recovery.
* For increased security:
  + Lock down and limit inbound traffic access with Azure Security Center - Just in time administration.
  + Restrict network traffic to management endpoints with Network Security Groups.
  + Deploy Azure Disk Encryption to help secure disks, and keep data safe from theft and unauthorized access.
  + Read more about securing IaaS resources, and visit the Azure Security Center.
* For monitoring and management:
* Consider deploying Azure Cost Management to monitor resource usage and spending.

## Replicate and failover Windows / Linux Physical Servers, Hyper-V VM’s or VMware VM’s to Azure Checklist

Here is a link that explains how to prepare for replication or migration to Azure:

<https://docs.microsoft.com/en-us/azure/site-recovery/tutorial-prepare-azure>

### High Level Summary - Replication and Failover Checklist

Table 23 Replication and failover Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| Task | Task Description | Completed (Y/N) | Comments\Notes |
|  | Run Capacity Planning Tool with Cloud Discovery Assessment and Cloud Cost Analytics |  |  |
|  | Create or verify Azure Subscription to replicate to |  |  |
|  | Verify DPOR on subscription or CSP |  |  |
|  | Gather list of Physical / Hyper / VMware VM’s and right-sized VM from Cloud Discovery Assessment and Cost Analytics |  |  |
|  | Setup Networking and VNet Configurations for Site to Site and VPN |  |  |
|  | Create storage accounts to replicate virtual machines to |  |  |
|  | Install the Configuration and Process Servers and run the ASR configuration wizard |  |  |
|  | Validate the Configuration Server and Scale out Process servers are registered to the vault |  |  |
|  | Prepare Active Directory with DNS and AD Sites and Services |  |  |
|  | Build and Promote Domain Controller for Site AD Replication to Azure |  |  |
|  | Create a replication policy and map it for use with the Configuration Server |  |  |
|  | Add a HyperV/ vCenter server to the replication policy and discover Physical / Hyper / VMware virtual machines |  | *Need to validate list of servers for deployment and ready for Mobility Service installation. No downtime expected.* |
|  | Validate Physical /VM list can use ASR or if third party tools are required |  | *Need to validate tool used for replication. Possible to use Zerto or VM Converter scripts used within SCVMM or custom.* |
|  | Gather Outage preferences and associate replication respectively |  |  |
|  | Prepare Machines for Mobility Agent deployment and Installation |  |  |
|  | Replicate Physical /HyperV / VMware virtual machines to Azure storage accounts |  |  |
|  | Configure failover settings for replicating virtual machines |  |  |
|  | Perform a test failover, validate application, and cleanup test failover. |  |  |
|  | Verification of Outage window for cutover sequence |  |  |
|  | Migrate \ Failover to Azure. |  |  |
|  | Verify and Test Applications |  |  |
|  | Cleanup and Documentation Handover |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Verify Supported Operating Systems Process

Table 24 Verify Supported Operating Systems Readiness Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Get list of Servers and OS’s associated as well as IPs |  |  |
|  | Compare list with the system requirements |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures..*

### Setup Source Environment for Physical / HyperV / VMware VMs

Table 25 Setup Source Environment for Physical / HyperV/VMware VMs Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | In the Azure portal, go to the Recovery Services vault blade and select your vault. |  |  |
|  | On the resource menu of the vault, go to Getting Started > Site Recovery > Step 1: Prepare Infrastructure > Protection goal. |  | Protection Goal: |
|  | In Protection goal, select To Azure, and choose Yes, with HyperV /VMware vSphere Hypervisor. Then click OK. |  |  |
|  | Continue to prepare and setup the configuration server |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Create Migration User

Table 26 Create Migration User Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Create a HyperV/ vCenter user to use for connections via the Configuration Server |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Prepare Machine for Management Server Installation

Table 27 Prepare Management Server Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Download the following Installations and stage on a computer |  | * Deployment Planner: <http://aka.ms/asr-deployment-planner> * PowerCLI: <http://aka.ms/downloadpowercli> * Download OVF template for ASR: <http://aka.ms/asrconfigurationserver_wus> * Prepare for Upload VHD image to Azure: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image> |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Install Configuration Server

Adding Configuration server may take 15 minutes to 30 minutes

Table 28 Install Configuration Server Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Ensure to install the Deployment Planner to accurately estimate network bandwidth storage and other requirements |  | <http://aka.ms/asr-deployment-planner> |
|  | Ensure System Requirements are met |  | <https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-deploy-configuration-server> |
|  | Download the Configuration server virtual machine template:   1. In the vault, go to Prepare Infrastructure > Source. 2. In Prepare source, select +Configuration server. 3. In Add Server, check that Configuration server for VMware appears in Server type. 4. Download the Open Virtualization Format (OVF) template for the configuration server. |  | <http://aka.ms/asrconfigurationserver_wus> |
|  | Import the Configuration server virtual machine template into your vCenter server using the Deploy OVF Template wizard.   1. Sign in to the VMware vCenter server or vSphere ESXi host by using the VMWare vSphere Client. 2. On the File menu, select Deploy OVF Template to start the Deploy OVF Template wizard. 3. In Select source, enter the location of the downloaded OVF. 4. In Review details, select Next. 5. In Select name and folder and Select configuration, accept the default settings. 6. In Select storage, for best performance select Thick Provision Eager Zeroed in Select virtual disk format. You can select the options that best fit your needs. 7. In the rest of the wizard pages, accept the default settings. 8. In Ready to complete:  * To add an additional network interface, clear Power on after deployment, and then select Finish. By default, the configuration server template is deployed with a single NIC. You can add additional NICs after deployment. * To set up the VM with the default settings, select Power on after deployment > Finish. |  | Deploy OVF Template screenshot:    Installation Parameters:    Depending on provisioning, this may take a while until the Deployment Completed Successfully:  CPU  HD1    HD2    HD3 |
|  | Add an additional network adapter:   1. In the VCenter /VMware inventory, right-click the VM and select Edit Settings. 2. In Hardware, select Add > Ethernet Adapter. Then select Next. 3. Select an adapter type and a network. 4. To connect the virtual NIC when the VM is turned on, select Connect at power on. Then select Next > Finish > OK. |  | If you want to add an additional NIC to the configuration server, add it before you register the server in the vault. Adding additional adapters isn't supported after registration.  Two Network adapters added with the same properties: |
|  | Connect to the virtual machine’s console once it has successfully booted up. |  | ***Note: you may see the server reboot once or twice during DISM and setup process.*** |
|  | Complete the Windows Server installation by accepting the license agreement and setting up an Administrator account.   1. Enter the password twice 2. Press Enter |  | ***Note: The license page may freeze up on you or may not display correctly. You can press enter at the license screen, then you will see the customize settings screen.*** |
|  | Log into the computer using the Administrator account and password you provided |  |  |
|  | You may be prompted to enter a name for the computer. Enter a Computer name, then press Tab, then press Enter |  | Computer name prompt: AZURE-ASR-CS01  Must press Tab and then Enter to register name: |
|  | You will see the computer perform some configuration steps. Press Tab, then press Enter to go back, or press tab+tab, then Enter to progress forward. |  | Config Steps: |
|  | You will see the sign in to your account page for Microsoft Azure. Use the account you have associated to the process and click Next, then enter the password and click Sign in. |  | Sign in page: |
|  | Configuration steps will complete |  | Configuration page:    Services may stop, then the server may restart to deploy the new configurations: |
|  | Log into the Server (Ctrl+Alt+Insert) as the Administrator account |  | A web page may launch: https://AZURE-asr-abc01:44315  It may take a few moments for the web page to connect: |
|  | If the configuration page does note show; Launch the Azure Site Recovery Configuration Manager wizard and follow the steps to register your Configuration server with Azure Site Recovery. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

### Install Configuration Server – Configure Settings

Table 29 Install Configuration Server – Configure Settings Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | In the configuration server management wizard, select Setup connectivity. Select the NIC to receive replication traffic, and then select Save. You can't change this setting after it's been configured. | Y |  |
|  | In Select Recovery Services vault, select your Azure subscription and the relevant resource group and vault.   1. You will see a window to accept permissions for the app, click Accept 2. Make Vault selections, click Continue | Y | Vault Page:  Vault Selections:  Subscription = …  Resource Group = …  Recovery Services Vault = … |
|  | In Install third-party software, accept the license agreement. Select Download and Install to install MySQL Server. Click Continue when the installation completes. |  | Install MySQL page |
|  | In Validate appliance configuration, prerequisites are verified before you continue. |  | Static IP Warning: You can create a reservation in DHCP or make the address static  < DHCP reservation> |
|  | In Configure vCenter Server/vSphere ESXi server, enter the FQDN or IP address of the vCenter server, or vSphere host, where the VMs you want to replicate are located. Enter the port on which the server is listening and a friendly name for the VMware server in the vault. Once all is entered, click Add to verify the connection properties. |  | Add vCenter:    Validation page shows addition: |
|  | Enter credentials to be used by the configuration server to connect to the VMware server. Site Recovery uses these credentials to automatically discover VMware VMs that are available for replication. Select Add, and then select Continue. |  | ***Add credentials page:*** |
|  | You may be prompted at the Protect Linux virtual machines windows to select Yes or No, select Yes if you do not want to protect Linux. |  | ***Protect Linux selection window:*** |
|  | Select Finalize configuration to finish registration. |  | ***Finalize Configuration page:***    ***Status will continue for the following:***   1. Configuring server 2. Registering with Azure Site Recovery 3. Adding vCenter Server/vSphere ESXi server   ***Success:*** |
|  | After registration finishes, in the Azure portal, verify that the configuration server and VMware server are listed on the Source page in the vault. Then select OK to configure target settings. | Y | ***Configuration Server***  < vault registration>  ***Shows Connected:***  < connection>  ***Click on Properties:*** |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

### Configure and manage replication policies for VMware replication

Table 30 Create a policy

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Select Manage > Site Recovery Infrastructure. |  |  |
|  | For VMware and Physical machines, select Replication policies. |  |  |
|  | Click +Replication policy, and specify the policy name. |  |  |
|  | In RPO threshold, specify the RPO limit. Alerts are generated when continuous replication exceeds this limit. |  |  |
|  | In Recovery point retention, specify (in hours) the duration of the retention window for each recovery point. Protected machines can be recovered to any point within a retention window. Up to 24 hours of retention is supported for machines replicated to premium storage. Up to 72 hours is supported for standard storage. |  |  |
|  | In App-consistent snapshot frequency, specify how often (in minutes) recovery points that contain application-consistent snapshots will be created. |  |  |
|  | Click OK. The policy should be created in 30 to 60 seconds. |  |  |
|  | When you create a replication policy, a matching failback replication policy is automatically created, with the suffix "failback". After creating the policy, you can edit it by selecting it > Edit Settings. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

Table 31 Associate a configuration server

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Click Associate, and select the configuration server. |  |  |
|  | Click OK. The configuration server should be associated in one to two minutes. |  | ­ |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

Table 32 Disassociate or delete a replication policy

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Choose the replication policy. a. To dissociate the policy from the configuration server, make sure that no replicated machines are using the policy. Then, click Dissociate. b. To delete the policy, make sure it's not associated with a configuration server. Then, click Delete. It should take 30-60 seconds to delete. | n/a |  |
|  | Click OK. | n/a |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

## Prepare Hyper V/ VMware Machine for Migration (Required)

When replicating HyperV /VMware virtual machines:

* Your Azure user account needs to have certain permissions to enable replication of a new virtual machine to Azure.
* VMs are discovered every 15 minutes. It might take 15 minutes or longer for them to appear in the Azure portal after discovery. Likewise, discovery can take 15 minutes or more when you add a new vCenter server or vSphere host.
* Environment changes on the virtual machine (such as VMware tools installation) can take 15 minutes or more to be updated in the portal.
* You can check the last discovered time for VMs in the Last Contact At field for the vCenter server/vSphere host, on the Configuration Servers page.
* To add machines for replication without waiting for the scheduled discovery, highlight the configuration server (don’t click it), and click the Refresh button.
* When you enable replication, if the machine is prepared, the process server automatically installs the Mobility Service on it.

### Prepare Machine for Azure

This article gives a great reference of the settings needed to be configured to ensure streamlined migration to Azure.

[Prepare Windows to upload to Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image) article has the following references below:

* Set Windows configurations for Azure
* Check the Windows services
* Update Remote Desktop registry settings
* Configure Windows Firewall rules
* Verify VM is healthy, secure, and accessible with RDP
* Complete recommended configurations

### Install Mobility Service

The guidance for the installation options are in the link below:

<https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-install-mobility-service>

*IMPORTANT: Beginning with version 9.7.0.0, on Windows VMs, the Mobility Service installer also installs the latest available Azure VM agent. When a computer fails over to Azure, the computer meets the agent installation prerequisite for using any VM extension.*

Table 33 Install Mobility Service by push installation from Azure Site Recovery Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Ensure that there's network connectivity between the Windows computer and the process server. |  | NOTE: During or after setup you may need to check the following logs:  The setup logs can be found under **%ProgramData%\ASRSetupLogs\ASRUnifiedAgentInstaller.log**  The AgentConfiguration logs can be found under **%ProgramData%\ASRSetupLogs\ASRUnifiedAgentConfigurator.log** |
|  | Create an account that the process server can use to access the computer. The account should have administrator rights, either local or domain. Use this account only for the push installation and for agent updates. |  | Note:  If you don't use a domain account, disable Remote User Access control on the local computer. To disable Remote User Access control, under HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System registry key, add a new DWORD: LocalAccountTokenFilterPolicy. Set the value to 1. To do this task at a command prompt, run the following command:   |  | | --- | | REG ADD HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG\_DWORD /d 1 | |
|  | In Windows Firewall on the computer you want to protect, select Allow an app or feature through Firewall. Enable File and Printer Sharing and Windows Management Instrumentation (WMI). For computers that belong to a domain, you can configure the firewall settings by using a Group Policy object (GPO). |  |  |
|  | Add the account that you created in CSPSConfigtool. Follow these steps:   1. Sign in to your configuration server. 2. Open cspsconfigtool.exe. It's available as a shortcut on the desktop and in the %ProgramData%\home\svsystems\bin folder. 3. On the Manage Accounts tab, select Add Account. 4. Add the account you created. 5. Enter the credentials you use when you enable replication for a computer. |  |  |
|  | You should see replication synchronization perform. |  |  |
|  | If synchronization is stuck at 0% due to flow control errors, you may need to unprotect the VM, give it a few moments and then reprotect. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Enable Replication

Verify each component is working, communicating and configured correctly before continuing.

Common Issues:

* Each disk should be less than 1 TB in size.
* The OS disk should be a basic disk and not a dynamic disk.
* For generation 2/UEFI-enabled virtual machines, the operating system family should be Windows and the boot disk should be less than 300 GB.
* Please see the section - Pre-requisites to enable RDP Before Failover

Table 34 Enable Replication Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Click Step 1: Replicate application > Source. After you've enabled replication for the first time, click +Replicate in the vault to enable replication for additional machines. |  | Note: If a VM is prepared for push installation, the process server automatically installs the Mobility service when you enable replication. |
|  | In the Source page > Source, select the configuration server. |  |  |
|  | In Machine type, select Virtual Machines or Physical Machines. |  |  |
|  | In vCenter/vSphere Hypervisor, select the vCenter server that manages the vSphere host, or select the host. This setting isn't relevant if you're replicating physical machines. |  |  |
|  | Select the process server, which will be the name of the configuration server if you haven't created any additional process servers. Then click OK. |  | < source> |
|  | In Target, select the subscription and the resource group where you want to create the failed-over virtual machines. Choose the deployment model that you want to use in Azure for the failed-over virtual machines. |  |  |
|  | Select the Azure Storage account you want to use for replicating data. |  | Note:   * You can select a premium or standard storage account. If you select a premium account, you need to specify an additional standard storage account for ongoing replication logs. Accounts must be in the same region as the Recovery Services vault. * If you want to use a different storage account, you can create one. To create a storage account by using Resource Manager, click Create new. |
|  | Select the Azure network and subnet to which Azure VMs will connect when they're spun up after failover. The network must be in the same region as the Recovery Services vault. Select Configure now for selected machines to apply the network setting to all machines you select for protection. Select Configure later to select the Azure network per machine. If you don't have a network, you need to create one. To create a network by using Resource Manager, click Create new. Select a subnet if applicable, and then click OK. |  |  |
|  | In Virtual Machines > Select virtual machines, select each machine you want to replicate. You can only select machines for which replication can be enabled. Then click OK. |  |  |
|  | In Properties > Configure properties, select the account used by the process server to automatically install the Mobility Service on the machine. |  |  |
|  | By default, all disks are replicated. To exclude disks from replication, click All Disks and clear any disks you don't want to replicate. Then click OK. You can set additional properties later. |  | <step 4> |
|  | In Replication settings > Configure replication settings, verify that the correct replication policy is selected. You can modify replication policy settings in Settings > Replication policies > (policy name) > Edit Settings. Changes you apply to a policy also apply to replicating and new machines. |  |  |
|  | Enable Multi-VM consistency if you want to gather machines into a replication group. Specify a name for the group, and then click OK. |  | Note:   * Machines in a replication group replicate together and have shared crash-consistent and app-consistent recovery points when they fail over. * Gather VMs and physical servers together so that they mirror your workloads. Enabling multi-VM consistency can impact workload performance. Use only if machines are running the same workload and you need consistency. |
|  | Click Enable Replication. You can track progress of the Enable Protection job in Settings > Jobs > Site Recovery Jobs. After the Finalize Protection job runs, the machine is ready for failover. |  | ***Note:***  *If the machine is prepared for push installation, the Mobility Service component is installed when protection is enabled. After the component is installed on the machine, a protection job starts and fails. After the failure, you need to manually restart each machine. After the restart, the protection job begins again and initial replication occurs.* |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

### View and Manage VM properties

Next, you verify the properties of the source machine. Remember that the Azure VM name needs to conform with Azure virtual machine requirements.

Table 35 View and Manage VM properties Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Click Settings > Replicated items >, and then select the machine. The Essentials page shows information about machine settings and status. |  |  |
|  | In Properties, you can view replication and failover information for the VM. |  |  |
|  | In Compute and Network > Compute properties, you can specify the Azure VM name and target size. Modify the name to comply with Azure requirements if necessary. |  |  |
|  | If you need an RDP endpoint, you can provision a Public IP Address and Associate it to the VM for management or application purposes if required. |  |  |
|  | You can select a resource group from which a machine becomes part of a post failover. You can change this setting any time before failover. Post failover, if you migrate the machine to a different resource group, the protection settings for that machine break. |  |  |
|  | You can select an availability set if your machine needs to be part of a post failover. While you're selecting an availability set, keep in mind that:   * Only availability sets belonging to the specified resource group are listed. * Machines with different virtual networks cannot be a part of the same availability set. * Only virtual machines of the same size can be a part of an availability set. |  |  |
|  | You can also view and add information about the target network, subnet, and IP address assigned to the Azure VM. |  |  |
|  | In Disks, you can see the operating system and data disks on the VM to be replicated. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

### Configure networks and IP addresses

Verify each component is working, communicating and configured correctly before continuing.

Table 36 Configure networks and IP addresses Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | You can set the target IP address. If you don't provide an address, the failed-over machine uses DHCP. If you set an address that isn't available at failover, the failover doesn't work. If the address is available in the test failover network, the same target IP address can be used for test failover. |  |  |
|  | The number of network adapters is dictated by the size you specify for the target virtual machine, as follows:   * If the number of network adapters on the source machine is less than or equal to the number of adapters allowed for the target machine size, then the target has the same number of adapters as the source. * If the number of adapters for the source virtual machine exceeds the number allowed for the target size, then the target size maximum is used. For example, if a source machine has two network adapters and the target machine size supports four, the target machine has two adapters. If the source machine has two adapters but the supported target size only supports one, then the target machine has only one adapter. * If the virtual machine has multiple network adapters, they all connect to the same network. Also, the first one shown in the list becomes the Default network adapter in the Azure virtual machine. |  |  |
|  | You may want to add a Public IP Address for management or application purposes if required. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

### Verify Protection of Machine

Verify each component is working, communicating and configured correctly before continuing.

Table 37 Verify Protection of Machine Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Verify Machine is showing as protected |  |  |
|  | Ensure to resize the VM according to capacity and planning stages |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures. Please refer to Design Documentation per Process or Role to ensure all prerequisites have been fulfilled.*

## Prepare Workload for Migration

### ASR Agent Unsupported

Recommended to use the following free or paid methods:

* Zerto for [VMware](https://www.zerto.com/products/on-premises-disaster-recovery/vmware-vsphere-replication-recovery/) or Microsoft [Azure](https://www.zerto.com/zerto-for-microsoft-azure/)
* [MVMC](https://www.microsoft.com/en-us/download/details.aspx?id=42497)

* [StarWind V2V Converter](https://www.starwindsoftware.com/converter)
* [vCenter Converter](https://docs.vmware.com/en/vCenter-Converter-Standalone/6.2/com.vmware.convsa.guide/GUID-08F9E93F-B849-4BEB-90EB-D6DB78E384C5.html)
  + [Download](https://www.vmware.com/products/converter.html)

#### Manual VM Build Process

You can use this method if you need to manually clone a VMware VM and create it as an Azure Virtual Machine

Table 38 Manually build VMware VM as Azure VM Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Prepare the VM - <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image>  <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-vm-specialized-portal>  Then - Clone the VMware VM |  | Make note of any RDP port numbers that may be different than default: |
|  | Name the VM and select a host |  |  |
|  | At the Host / Cluster page click the Host or Cluster to clone this to |  |  |
|  | Select the virtual disk format – preferred to utilize Thin Provision and to ensure the OS or Data disks are as small as possible for the copy |  |  |
|  | Ensure to uncheck Power on this virtual machine after creation. (unchecked by default) |  |  |
|  |  |  |  |
|  | Ensure the VM cloning task completes successfully |  |  |
|  | Check the Disk File location for the cloned vmdk |  |  |
|  | Unregister the VM from VCenter |  | This will ensure that the VM wont start and processes aren’t utilizing the disk |
|  | On a computer with StarWind V2V installed, open VMware vSphere and connect to the datacenter and browse the datastore location where the cloned disk is located, then select all and right-click, then download |  |  |
|  | Using StarWind Converter, locate the image file and select to convert to VHD image, then wait for the conversion process to complete successfully. |  | Ensure to select the 1 KB file |
|  | Using Add-AzureRMvhd or another copy method including Storage Explorer, copy the converted image to Azure Storage for the VM – you may use premium disks here |  | <https://docs.microsoft.com/en-us/azure/lab-services/devtest-lab-upload-vhd-using-storage-explorer>  Ensure to select page blob  IF using powershell, ensure the threads command is passed for efficiency on calculation of the MD5 Hash |
|  | You may notice the machine performing the upload encounters a blue screen – make sure to disable automatically restart in startup and recovery of windows  <https://support.microsoft.com/en-us/help/2028504/windows-kernel-event-id-41-error-the-system-has-rebooted-without-clean>  This article mentions processor types that cause the vm bluescreen  <https://kb.vmware.com/s/article/2073791>  Troubleshooting a bluescreen on vmware  <https://kb.vmware.com/s/article/1019064>  vmware-1.log shows:  Ethernet1 MAC Address:  vcpu-0| PIIX4: PM Soft Off. Good-bye.  vmx| Stopping VCPU threads |  |  |
|  | Create a VM from a VHD using the Azure Portal |  | <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-vm-specialized-portal> |
|  | Create VM from Disk |  |  |
|  | You may receive this error related to “Only blobs formatted as VHDs can be imported.”  PHYSICALDRIVE0-Azure\_VM01 |  |  |
|  | In this case you may need to reupload the vm to the storage account. |  | https://TESTstgwuspre1.blob.core.windows.net/clone/CLONE.vhd |
|  | This was the command used to build the VM |  | #Install-Module AzureRM -RequiredVersion 6.0.0  Connect-AzureRmAccount  #Get the Storage Account  Get-AzureRmStorageAccount  #$resourceGroupName = "Azure-RS-RG1"  #$destinationResourceGroupName = "Azure-RS-RG1"  #$location = "US"  #$osDiskName = Azure -TST01'  #$osDisk = Get-AzureRmDisk `  #-ResourceGroupName $resourceGroupName `  #-DiskName $osDiskName  ##upload to azure  #$urlOfUploadedVhd = "https://Azuregwuspre1.blob.core.windows.net/Azure-ts01-test/Azure-ts01-test.vhd"  #Add-AzureRmVhd -ResourceGroupName $resourceGroupName `  # -Destination $urlOfUploadedVhd `  # -LocalFilePath "E:\Azure-TST01\Azure-tsT01-test.vhd"  #create managed disk  $resourceGroupName = “Azure-RS-RG1"  $destinationResourceGroup = "TEST-RS-RG1"  $location = "US"  $sourceUri = ("https.vhd")  $osDiskName = 'PHYSICALDRIVE0-TEST\_TS01'  $osDisk = New-AzureRmDisk -DiskName $osDiskName -Disk `  (New-AzureRmDiskConfig -AccountType Premium\_LRS `  -Location $location -CreateOption Import `  -SourceUri $sourceUri) `  -ResourceGroupName $destinationResourceGroup  start-sleep 120  #create vm config  $vmName = "TEST-TS01"  $virtualNetworkName = 'TEST-VNET1'  $vnet = Get-AzureRmVirtualNetwork -Name $virtualNetworkName -ResourceGroupName $resourceGroupName  $vmConfig = New-AzureRmVMConfig -VMName $vmName -VMSize "Standard\_DS2\_v2"  $nic = New-AzureRmNetworkInterface -Name ($vmName.ToLower()+'\_nic') -ResourceGroupName $resourceGroupName -Location $snapshot.Location -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $publicIp.Id  $VirtualMachine = Add-AzureRmVMNetworkInterface -VM $VirtualMachine -Id $nic.Id  start-sleep 120  #set vm to use the disk  $vmName = "TEST-TS01"  $vm = Set-AzureRmVMOSDisk -VM $vm -ManagedDiskId $osDisk.Id -StorageAccountType Premium\_LRS `  -DiskSizeInGB 256 -CreateOption Attach -Windows  #create new vm from managed disk  New-AzureRmVM -ResourceGroupName $destinationResourceGroup -Location $location -VM $vm |
|  | Build VM script  Change subscriptionid |  | #clear memory  [System.GC]::Collect()  #Provide the subscription Id  $subscriptionId = '###’  $resourceGroupName ='TEST-RS-RG1'  $location = 'East US 2'  $NetworkLocation = 'eastus2'  #config  $vmName = ''TEST-VM01'  $virtualNetworkName = 'TEST -VNET1'  $subnetname = 'TEST-SUBNET1-VNET1'  $storageaccountname = 'TESTstgwuspre1'  $osDiskName = 'PHYSICALDRIVE0-TEST\_VM01'  $osDisk = Get-AzureRmDisk `  -ResourceGroupName $resourceGroupName `  -DiskName $osDiskName  #Install-Module AzureRM -RequiredVersion 6.0.0  Connect-AzureRmAccount  #Get the Storage Account  Get-AzureRmStorageAccount -ResourceGroupName $resourceGroupName -storageaccountname $storageaccountname  #set vm config  $vmConfig = New-AzureRmVMConfig -VMName $vmName -VMSize "Standard\_DS2\_v2"  #get network and subnet  $vnet = Get-AzureRmVirtualNetwork | where {$\_.name -eq $virtualNetworkName}  $subnet = Get-AzureRmVirtualNetwork | where {$\_.name -eq $virtualNetworkName} | get-AzureRmVirtualNetworkSubnetConfig | where {$\_.name -eq $Subnetname}  $ipName = $vmName + “-PIP1”  $pip = get-AzureRmPublicIpAddress -Name $ipName -ResourceGroupName $resourceGroupName  $nicName = $vmName + “-NIC1”  #$nic = get-AzureRmNetworkInterface -Name $nicName -ResourceGroupName $resourceGroupName -Location 'west us' -SubnetId $vnet.Subnets[1].Id -PublicIpAddressId $pip.Id  $nic = get-AzureRmNetworkInterface -Name $nicName -ResourceGroupName $resourceGroupName  $vm = Add-AzureRmVMNetworkInterface -VM $vmConfig -Id $nic.Id  #set vm to use the disk  $vmName = "TEST-VM01"  $vm = Set-AzureRmVMOSDisk -VM $vmConfig -ManagedDiskId $osDisk.Id -StorageAccountType Premium\_LRS `  -DiskSizeInGB 256 -CreateOption Attach -Windows  #create new vm from managed disk  New-AzureRmVM -ResourceGroupName $destinationResourceGroup -Location $location -VM $vm  #verify the vm was created  $vmList = Get-AzureRmVM -ResourceGroupName $destinationResourceGroup  $vmList.Name |

### Terminal Services

Enable Disaster Recovery of RDS using Azure Site Recovery following this [link](https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-enable-dr-with-asr)

### Domain Services

Us this article for guidance on “How to upload existing on-premises Hyper-V domain controllers to Azure by using Azure PowerShell: <https://support.microsoft.com/en-us/help/2904015/how-to-upload-existing-on-premises-hyper-v-domain-controllers-to-azure>

### File Services

Protect a file server by using Azure Site Recovery following this [link](https://docs.microsoft.com/en-us/azure/site-recovery/file-server-disaster-recovery)

Backup and Restore NTFS and Share Permissions using this [link](https://support.microsoft.com/en-us/help/125996/saving-and-restoring-existing-windows-shares?wa=wsignin1.0) or this blog example [link](https://blogs.technet.microsoft.com/askds/2008/11/24/how-to-back-up-and-restore-ntfs-and-share-permissions/)

### Print Services

Deploy Windows Server Hybrid Cloud Print with Pre-Authentication following this [link](https://docs.microsoft.com/en-us/windows-server/administration/hybrid-cloud-print/hybrid-cloud-print-deploy)

## Test Failover (Test Migration) in Site Recovery

* Before you do a failover\migration, do a test failover to ensure that everything is working as expected.
* Prepare the network at target location before you do a failover.
* Ensure DC or DNS is replicated in the Test network

### Create a network for test failover

We recommended that for test failover, you choose a network that's isolated from the production recovery site network specific in the Compute and Network settings for each VM. By default, when you create an Azure virtual network, it is isolated from other networks. The test network should mimic your production network:

* The test network should have same number of subnets as your production network. Subnets should have the same names.
* The test network should use the same IP address range.
* Update the DNS of the test network with the IP address specified for the DNS VM in Compute and Network settings.

### Ensure AD is prepared in the Test Network

The considerations noted in the [ASR Test failover considerations here](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-active-directory#test-failover-considerations) not that you must create a domain controller in the isolated network to be used for test failover.

### Prepare DNS and DHCP

[Prepare DHCP and DNS using the link here](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-vmm-test-failover#prepare-dhcp) and ensure DNS settings are updated prior to failover

### Virtualization Safeguards

Beginning with Windows Server 2012, additional safeguards are built into Active Directory Domain Services (AD DS). These safeguards help protect virtualized domain controllers against USN rollbacks if the underlying hypervisor platform supports VM-GenerationID. Azure supports VM-GenerationID. Because of this, domain controllers that run Windows Server 2012 or later on Azure virtual machines have these additional safeguards.

Because this domain controller is used only in a test failover, virtualization safeguards aren't necessary. To ensure that the VM-GenerationID value for the domain controller virtual machine doesn't change, you can change the value of following DWORD to 4 in the on-premises domain controller:

|  |
| --- |
| HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\gencounter\Start |

### After AD is in the test network - Remove references to other domain controllers

When you initiate a test failover, don't include all the domain controllers in the test network. To remove references to other domain controllers that exist in your production environment, you might need to [seize FSMO Active Directory roles](http://aka.ms/ad_seize_fsmo) and do [metadata cleanup](https://technet.microsoft.com/library/cc816907.aspx) for missing domain controllers.

You may want to note which servers are responding and remove the servers that are not going to be in the test network for test failover purposes. This includes Computer Objects, DNS records, WINS (if exists), and AD Sites and Services.

### Run a Test Failover (Test Migration)

When you run a test failover, the following happens:

* A prerequisites check runs to make sure all the conditions required for failover are in place.
* Failover processes the data, so that an Azure VM can be created. If select the latest recovery point, a recovery point is created from the data.
* An Azure VM is created using the data processed in the previous step.

The following occurs during test failover to a secondary site:

1. If you're replicating to another on-premises site and you use DHCP, set up DNS and DHCP for test failover.
2. Do a test failover of the domain controller virtual machine that runs in the isolated network. Use the latest available application consistent recovery point of the domain controller virtual machine to do the test failover.
3. Run a test failover for the recovery plan that contains virtual machines that the application runs on.
4. When testing is complete, clean up the test failover on the domain controller virtual machine. This step deletes the domain controller that was created for test failover.

Table 39 Run a Test Failover Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | In Settings > Replicated Items, click the VM > +Test Failover. |  | Note: You may want to review the section named – [‘Pre-requisites to enable RDP Before Failover’](#_Pre-requisites_to_enable) |
|  | Select the Latest processed recovery point for this tutorial. This fails over the VM to the latest available point in time. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO (recovery time objective). |  | ***Note:***  ***The option to choose a recovery point is only available when you are failing over to Azure.*** |
|  | In Test Failover, select the target Azure network to which Azure VMs will be connected after failover occurs. |  | This was modified in the Compute and Network configuration settings: |
|  | Click OK to begin the failover. You can track progress by clicking on the VM to open its properties. Or you can click the Test Failover job in vault name > Settings > Jobs > Site Recovery jobs. |  |  |
|  | After the failover finishes, the replica Azure VM appears in the Azure portal > Virtual Machines. Check that the VM is the appropriate size, that it's connected to the right network, and that it's running. |  |  |
|  | You should now be able to connect to the replicated VM in Azure and log into it. |  |  |
|  | To delete Azure VMs created during the test failover, click Cleanup test failover on the VM. In Notes, record and save any observations associated with the test failover. |  | *Repeated note for reference:*  *In some scenarios, failover requires additional processing that takes around eight to ten minutes to complete. You might notice longer test failover times for VMware Linux machines, VMware VMs that don't have the DHCP service enables, and VMware VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.* |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Post Test Failover Considerations

Table 40 Post Failover Consideration Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Retaining drive letter after failover |  | To retain the drive letter on virtual machines after failover, you can set the SAN Policy for the virtual machine to OnlineAll. [Read more here](https://support.microsoft.com/en-us/help/3031135/how-to-preserve-the-drive-letter-for-protected-virtual-machines-that-are-failed-over-or-migrated-to-azure) |
|  | RDP Connectivity |  | * You can follow [Prepare to connect to Azure VM’s after failover here](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-test-failover-to-azure#prepare-to-connect-to-azure-vms-after-failover) * If you experience issues: You may want to review the troubleshooting notes in this guide for RDP - <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/troubleshoot-rdp-connection> |
|  | Public IP Address |  | You may want to enable PIP and make the Private IP static |
|  | Ensure the Time is updated on the machine after failover |  |  |
|  | You may need to run ipconfig /flushdns and ipconfig /registerdns to get the machine to ping the domain |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

## Migrate to Azure

Run a failover for the machines you want to migrate. In some scenarios, failover requires additional processing that takes around eight to ten minutes to complete.

**IMPORTANT**: You might notice longer test failover times for physical servers, VMware Linux machines, VMware VMs which have the following characteristics:

1. Don't have the DHCP service enabled, and
2. VMware VMs that don't have the following boot drivers:

* storvsc
* vmbus
* storflt
* intelide
* atapi

### Test Full Failover to a production network in the recovery site

Although we recommended that you use a test network separate from your production network, if you do want to test a disaster recovery drill into your production network, note the following:

* Make sure that the primary VM is shut down when you run the test failover. Otherwise there will be two VMs with the same identity, running in the same network at the same time. This can lead to unexpected consequences.
* Any changes to VMs created for test failover are lost when you clean up the failover. These changes are not replicated back to the primary VM.
* Testing in your production environment leads to a downtime of your production application. Users shouldn't use apps running on VMs when the test failover is in progress.

Table 41 Failover Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | In Settings > Replicated items click the machine > Failover. |  |  |
|  | In Failover select a Recovery Point to fail over to. Select the latest recovery point. |  |  |
|  | The encryption key setting may not be relevant for this scenario. |  |  |
|  | Select Shut down machine before beginning failover. Site Recovery will attempt to do a shutdown of source virtual machines before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the Jobs page. |  |  |
|  | Check that the Azure VM appears in Azure as expected. |  |  |
|  | In Replicated items, right-click the VM > Complete Migration. This finishes the migration process, stops replication for the VM, and stops Site Recovery billing for the VM. |  | ***Warning: Don't cancel a failover in progress: VM replication is stopped before failover starts. If you cancel a failover in progress, failover stops, but the VM won't replicate again.*** |
|  | Ensure Startup settings for all machines migrated are set to disabled in Host > Configuration > Virtual Machine Startup/Shutdown > Disabled |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Failover and Migrate to Azure Completion

Table 42 Failover and Migrate to Azure Completion Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Ensure VM is ready for shutdown and RPO is at threshold for outage window  Ensure the NSG Is prepared - <https://gallery.technet.microsoft.com/Azure-Recovery-script-to-0c950702>  (NSG preconfigured by IT Responsive) |  | For VMware, ASR replicates data continually using CDP. Failover gives the user the option to failover to the Latest data (including post application shut-down)  1. Plan a maintenance window as per the change management process  2.Notify users of upcoming downtime  3. Take the user-facing application offline.  4. Initiate a Planned Failover using ASR portal to the Latest point after the application is offline. Use the "Unplanned Failover" option on the portal and select the Latest point to failover. The on-premises virtual machine is automatically shut-down.  Effective application data loss = 0  A journal of recovery points in a retention window is provided for a customer who wants to use an older recovery point. (72 hours of retention for VMware). |
|  | In Settings > Replicated items click the machine > Failover. |  |  |
|  | In Failover select a Recovery Point to fail over to. Select the latest recovery point. |  |  |
|  | The encryption key setting may not be relevant for this scenario. |  |  |
|  | Select Shut down machine before beginning failover. Site Recovery will attempt to do a shutdown of source virtual machines before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the Jobs page. |  |  |
|  | Check that the Azure VM appears in Azure as expected. |  |  |
|  | In Replicated items, right-click the VM > Complete Migration. This finishes the migration process, stops replication for the VM, and stops Site Recovery billing for the VM. |  | ***Warning: Don't cancel a failover in progress: VM replication is stopped before failover starts. If you cancel a failover in progress, failover stops, but the VM won't replicate again.*** |
|  | Ensure Startup settings for all machines migrated are set to disabled in Host > Configuration > Virtual Machine Startup/Shutdown > Disabled |  |  |
|  | Ensure to change the NIC settings after the Failover |  |  |
|  | Ensure Health of Failover |  |  |
|  | Ensure any Computers that did not utilize ASR can also complete migration. |  | * ERROR - SERVER – domain expiry of copy, unable to connect to computer. Need to re-clone, convert VMDK to VHD, then copy to Azure utilizing [StarWind V2V Converter](https://www.starwindsoftware.com/converter) * Backout plan – stop Azure VM, Start onpremises VM, reclone for next outage window as scheduled. |

## Verify Post Migration Components (Required)

Verify each component is working, communicating and configured correctly before continuing.

Table 43 Post Migration Verification Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Verify Health of application environments |  |  |
|  | Get application owner approval of health certification |  |  |
|  | In Azure Portal, complete failover, then clean up any leftover pieces if no ASR is to be utilized any longer including the Configuration Server. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

### Verify Windows Activation

Table 44 Verify Windows Activation Checklist

| Task | Task Description | Complete Y|N? | Comments\Notes |
| --- | --- | --- | --- |
|  | Azure Hybrid Benefit:  Microsoft Software Assurance customers can use Azure Hybrid Benefit to save on licensing costs for Windows Server machines that are migrated to Azure, or to use Azure for disaster recovery. If you're eligible to use the Azure Hybrid Benefit, you can specify that the virtual machine assigned this benefit is the one Azure Site Recovery creates if there's a failover. To do this:   1. Go to the Compute and Network properties section of the replicated virtual machine. 2. Answer the question that asks if you have a Windows Server License that makes you eligible for Azure Hybrid Benefit. 3. Select the check box to confirm that you have an eligible Windows Server license with Software Assurance, which you can use to apply the Azure Hybrid Benefit on the machine that will be created on failover. 4. Save settings for the replicated machine. |  |  |

***Note:*** *Additional Prerequisites maybe necessary according to Application Needs, Internal Policies and Procedures.*

# Appendix A

## Helpful Links and Technical Information

Azure RBAC

<https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

IP Addressing Pricing

<https://azure.microsoft.com/en-us/pricing/details/ip-addresses/>

Azure Storage Files

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

Azure B2B

<https://docs.microsoft.com/en-us/azure/active-directory/b2b/what-is-b2b>

Azure B2C

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/>

Azure Storage Limits

<https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits#storage-limits>

Azure Redundant Storage

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#zone-redundant-storage>

Azure Backup – Restore Files Tutorial

<https://docs.microsoft.com/en-us/azure/backup/tutorial-restore-files>

Azure VPN Gateway Pricing

<https://azure.microsoft.com/en-us/pricing/details/vpn-gateway/>

Virtual Desktop Pricing

<https://azure.microsoft.com/en-us/pricing/details/virtual-desktop/>

Windows Server S2D

<https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/storage-spaces-direct-disaster-recovery>

Network Controller

<https://docs.microsoft.com/en-us/windows-server/networking/sdn/technologies/network-controller/network-controller>

Distance and Regional Pair Datacenters

<https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions>

[https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions#what-are-paired-regions](https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions)

<https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions>

High Compute and VMs that scale quickly – Build 1000 VMs tutorial\case study

<https://azure.microsoft.com/en-us/services/storage/avere-vfxt/>

Azure Avere

<https://github.com/Azure/Avere>

<https://github.com/Azure/Avere/blob/master/docs/azure_vm_provision_best_practices.md>

Pass thru – AAD Connect

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-how-it-works>

Azure Datacenter

<https://azure.microsoft.com/en-us/blog/microsoft-reimagines-open-source-cloud-hardware/>

<https://www.youtube.com/watch?v=D8hMu4jJAwo>

Microsoft vs. VMware TCO calculator

<http://datacenter-tco-tool.azurewebsites.net/home>

TCO Calculator

<https://azure.microsoft.com/en-us/pricing/tco/calculator/>

Supported Endpoint Protection Solutions

[https://docs.microsoft.com/en-us/azure/security-center/security-center-os-coverage#supported-endpoint-protection-solutions](https://docs.microsoft.com/en-us/azure/security-center/security-center-os-coverage)

Encryption

<https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-how-to-enable-replication-ade-vms>

Server 2016 Hardening

<https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-for-disabling-system-services-in-windows-server>

AD Connect

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect>

SCVMM Vmware Support

[https://docs.microsoft.com/en-us/system-center/vmm/system-requirements?view=sc-vmm-2019#vmware-servers-in-the-vmm-fabric](https://docs.microsoft.com/en-us/system-center/vmm/system-requirements?view=sc-vmm-2019)

Cluster Sets

<https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/cluster-sets>

DIAD – Tier Model

<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

Add Existing VM to Availability Set

<https://gallery.technet.microsoft.com/Set-Azure-Resource-Manager-f7509ec4>

Change Availability Set

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/change-availability-set>

Load Balancer

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-load-balancing-azure>

Traffic Manager

<https://docs.microsoft.com/en-us/azure/traffic-manager/>

New Azure PowerShell Az Module

<https://docs.microsoft.com/en-us/powershell/azure/new-azureps-module-az?view=azps-1.7.0>

IP Address Types and allocation methods in Azure

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-ip-addresses-overview-arm>

Application Proxy

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>

Azure Security

<https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices>

Build Azure Map – Locations

<https://map.buildazure.com/>

Retain IP after failover

<https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-retain-ip-azure-vm-failover>

SLAs in Azure

<https://azure.microsoft.com/en-us/support/legal/sla/>

Azure Site Recovery

<https://azure.microsoft.com/en-us/services/site-recovery/>

Gartner on Azure

<https://www.gartner.com/doc/reprints?id=1-57832FE&ct=180716&st=sb>

Real time actually means near time

<https://www.zerto.com/the-platform/real-time-hypervisor-based-replication/>

NetApp OnTap Cloud integration with Azure

<https://cloud.netapp.com/ontap-cloud>

NetApp Storage with Express Route Direct and Azure

<https://www.netapp.com/us/media/ds-3608.pdf>

<https://azure.microsoft.com/en-us/services/storage/netapp/>

Securing Privileged Access in AD

<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

Azure Backup and Site Recovery

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-faq>

Limitations

<https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits>

BGP and ASN

[https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview#faq](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview)

Azure Pricing Calculator

<https://azure.microsoft.com/en-us/pricing/calculator/>

ASR Deployment Planning

<https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-deployment-planner>

Support Matrix – VM Replication

[https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix#replicated-machines](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix)

One of the popular features of Azure Managed Disks is the Point in time backups (snapshots) of the VM. Customer like using this feature to get the core VMs up and running quickly and using Azure Backup to manage the Data Disks.

Section on how to move VMs across Storage Accounts:

<https://azure.microsoft.com/en-us/blog/migrate-azure-virtual-machines-between-storage-accounts/>

<http://scug.be/wim/category/microsoft-azure-storage-explorer/>

Section on how to move VMs across to Managed Disks:

<https://social.technet.microsoft.com/wiki/contents/articles/37613.azure-converting-vm-unmanaged-disks-to-managed-disks.aspx>

The defaults for a Tenant Subscription

<https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits>

<https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-plan-capacity-vmware>