White paper

December 2016

Disaster Recovery Solution for XenApp and XenDesktop using Microsoft Azure Site Recovery

Summary: This document provides a step-by-step guidance for implementing disaster recovery solution for Citrix XenApp and XenDesktop deployments using Azure Site Recovery.

Author:

Subbareddy Dega

Citrix Systems, Inc.

Email: subbareddy.dega@citrix.com

S

Table of Contents

Overview

Citrix XenDesktop is a desktop virtualization solution that delivers desktops and applications as an on-demand service to any user, anywhere. With FlexCast delivery technology, XenDesktop can quickly and securely deliver applications and desktops to users.

Today, Citrix XenApp does not provide any out-of-the-box disaster recovery capabilities. Regardless of the type and scale of a disaster, recovery involves the use of a standby data center that you can recover the farm to. Standby data centers are required for scenarios where local redundant systems and backups cannot recover from the outage at the primary data center.

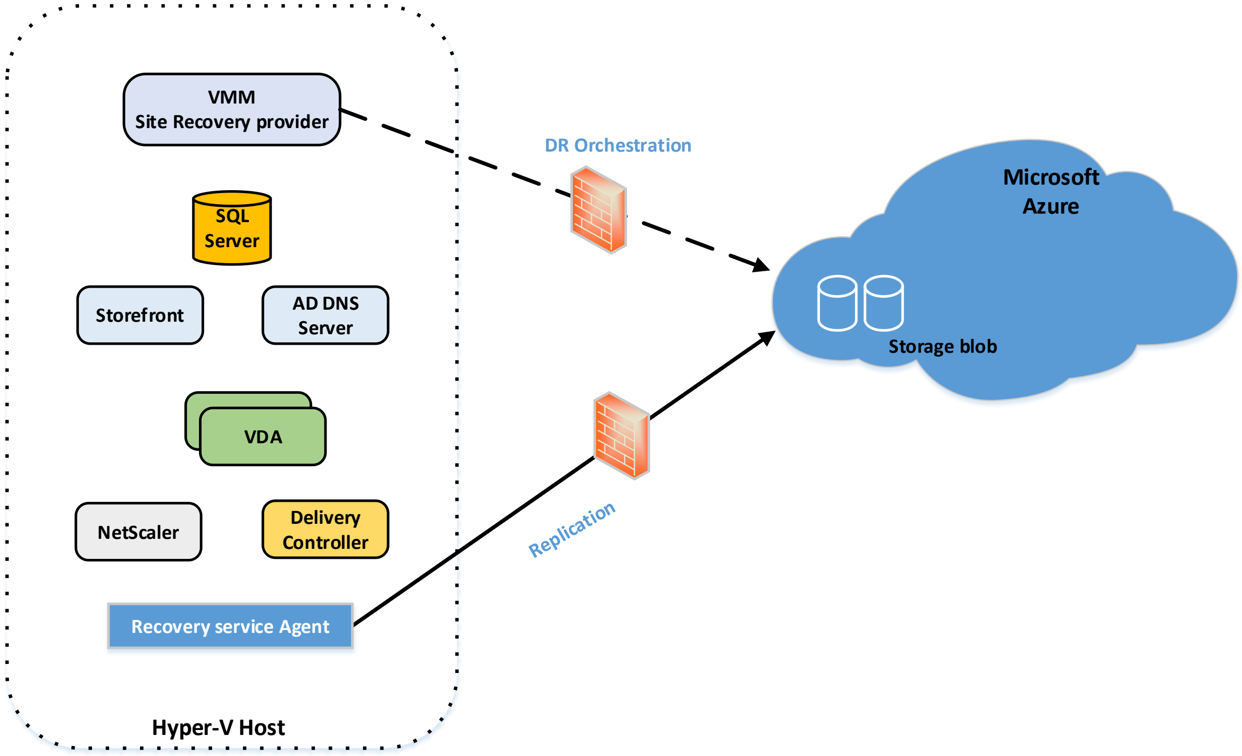
Azure Site Recovery is Microsoft's Disaster Recovery as a Service (DRaaS) solution and provides disaster recovery capabilities by orchestrating replication, failover and recovery of virtual machines. Azure Site Recovery supports a number of replication technologies to consistently replicate, protect, and seamlessly failover virtual machines to secondary site or to Azure.

This document provides a step-by-step guidance for building a disaster recovery solution for your Citrix XenApp deployments based on Hyper-V and VMware vSphere, perform a test failover and unplanned failover using recovery plan, supported configurations and prerequisites.

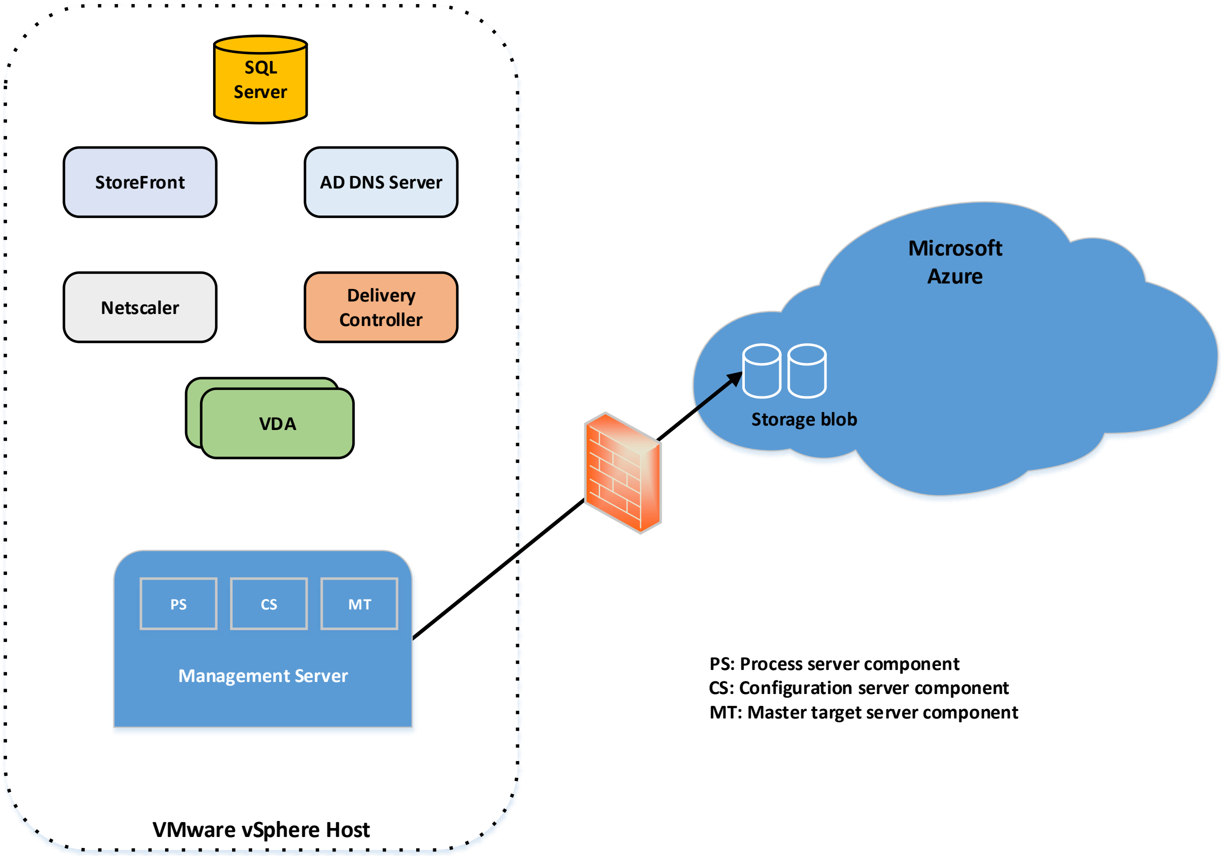
The audience is expected to be familiar with Citrix XenApp and XenDesktop and Azure Site Recovery.

Citrix XenApp and ASR architecture

The following figures illustrates the Azure Site Recovery configuration for an on-premises XenApp deployments on both Hyper-V and VMware vSphere.



On-premises XenApp deployment on Hyper-V



On-premises XenApp deployment on VMware vSphere

Supported Azure Site Recovery Deployment Options

Customers can deploy XenApp components as Virtual Machines running on Hyper-V or VMware or as Physical Servers. Azure Site Recovery can protect both physical and Virtual deployments to either a secondary Site or to Azure. The following table lists the supported XenApp deployments in Site to Site and Site to Azure scenarios.

	Hyper-V		***VMware***		***Physical***	
XenApp deployment type	**Site to Site**	**Site to Azure**	**Site to Site**	**Site to Azure**	**Site to Site**	**Site to Azure**
	Yes	Yes	Yes	Yes	Yes	Yes

ASR Configuration

This section provides step-by-step procedure for configuring ASR to protect the on-premises XenApp environments running on VMware vSphere and Hyper-V.

Prerequisites

Implementing disaster recovery for XenApp deployment using Azure Site Recovery requires the following prerequisites completed.

Azure prerequisites

- You need a Microsoft Azure account
- Set up an Azure network
- Set up an Azure storage account
- Azure Site Recovery Services vault has been created in Microsoft Azure subscription

Hyper-V prerequisites

- An on-premises XenApp environment running on Windows Server 2012 R2 Hyper-V host has been setup
- VMM server running on System Center 2012 R2. VMM server should have one or more clouds configured. A cloud should contain VMM host group.

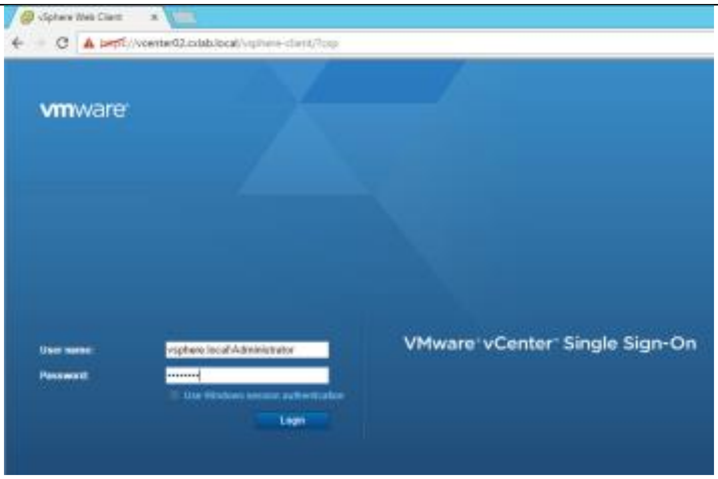
VMware vSphere prerequisites

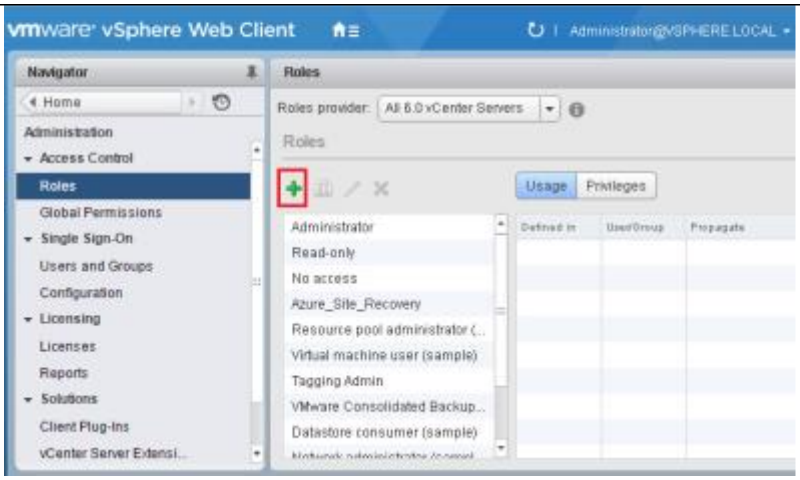
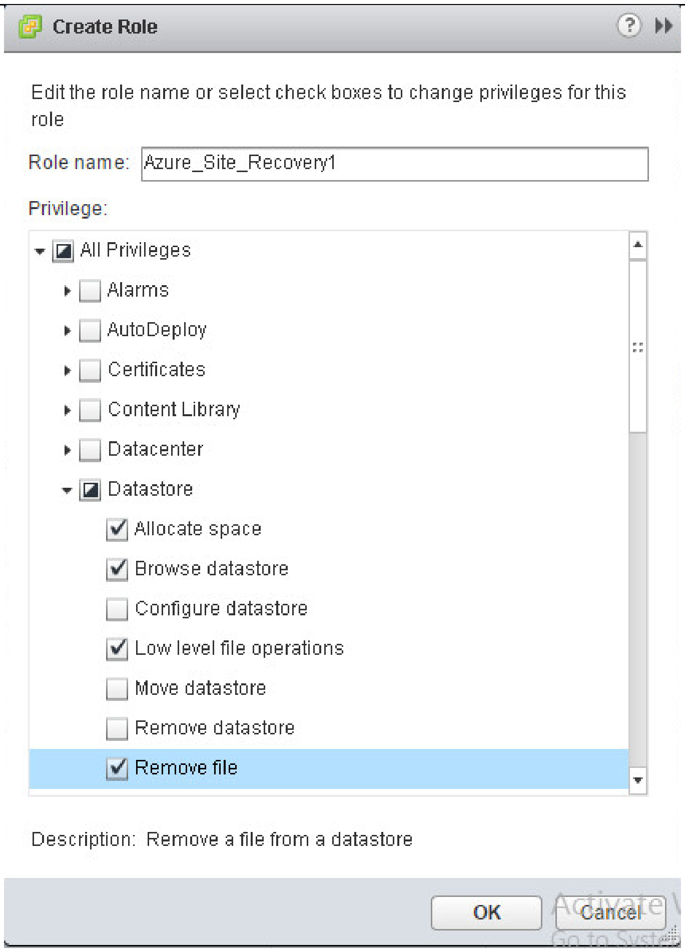
- An on-premises XenApp environment running on VMware vSphere host has been setup
- Create an account on the vCenter or vSphere hosts so that Site Recovery can automatically detect VMware VMs that are added
- Prepare the configuration server and install vSphere PowerCLI 6.0

Create a vCenter account for VM automatic discovery

The process server can automatically discover VMware VMs that are managed by a vCenter server. For automatic discovery Site Recovery needs an account and credentials that can access the vCenter server.

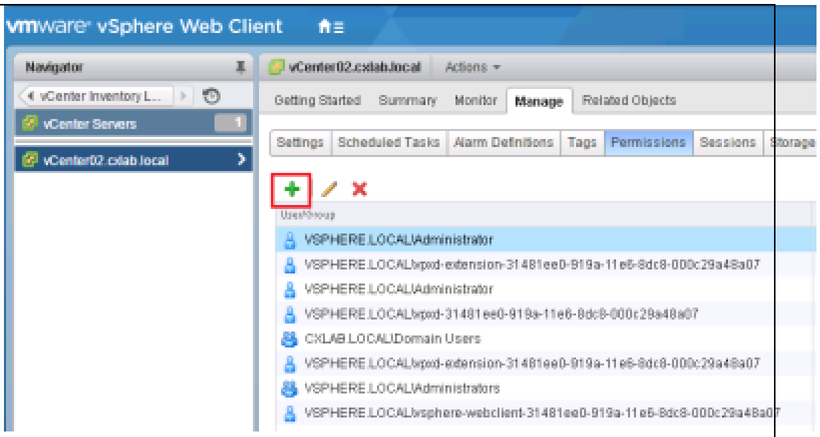
Create a default user in your on-premises active directory, in this example created vcenterasr@cxlab.local

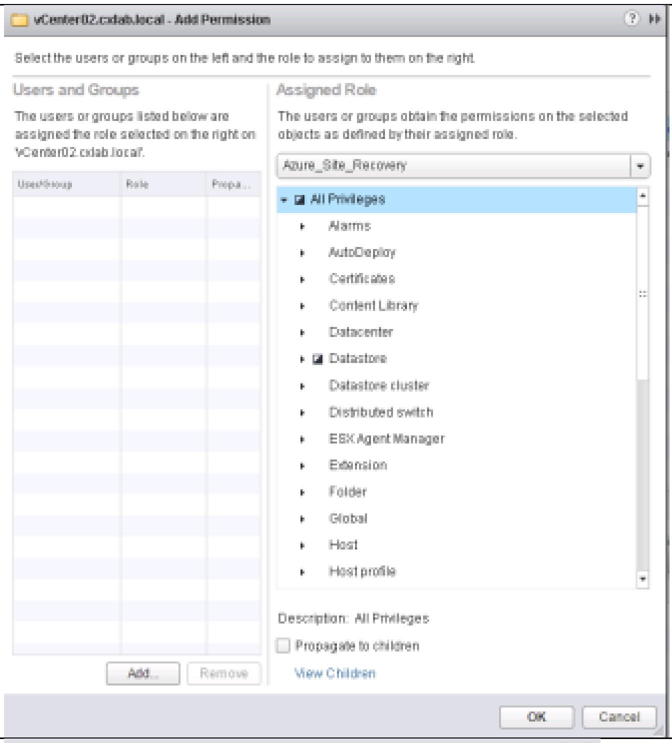
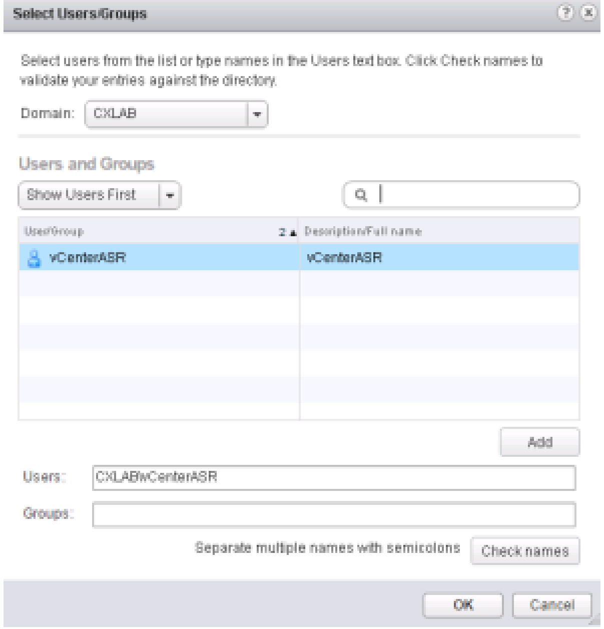
Login to vCenter Server and open a vSphere Web Client connection to the vCenter Server.	 https://vcenter02.cxlab.local/vsphere-client/?csp User name: vsphere.local\Administrator Password: •••••••• vSphere Web Client vmware VMware vCenter Single Sign-On Use Windows session authentication Login

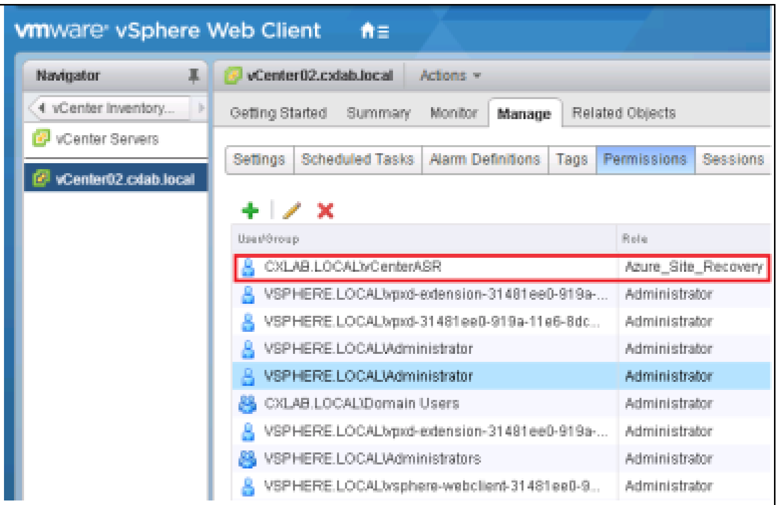
Navigate **Home** -> **Administration** -> **Roles** -> **Create Role Action**	 vmware vSphere Web Client Administrator@VSPHERE.LOCAL Navigator Home Administration Access Control Roles Global Permissions Single Sign-On Users and Groups Configuration Licensing Licenses Reports Solutions Client Plug-Ins vCenter Server Extensi... Roles Roles provider: All 6.0 vCenter Servers Roles Usage Privileges Administrator Read-only No access Azure_Site_Recovery Resource pool administrator (... Virtual machine user (sample) Tagging Admin VMware Consolidated Backup... Datastore consumer (sample) Defined in User/Group Propagate
Create a Azure_Site_Recovery role with following settings: **Datastore**: Allocate space, Browse datastore, Low level file operations **Remove file:**Update virtual machine files **Network:** Network assign **Resource:** Assign virtual machine to resource pool, Migrate powered off virtual machine, Migrate powered on virtual machine **Tasks:** Create task, update task **Virtual machine:** Configuration **Virtual machine, Interact**: Answer question , Device connection, Configure CD media, Configure floppy media, Power off, Power on, VMware tools install	 Create Role Edit the role name or select check boxes to change privileges for this role Role name: Azure_Site_Recovery1 Privilege: ◩ All Privileges □ Alarms □ AutoDeploy □ Certificates □ Content Library □ Datacenter ◩ Datastore ☑ Allocate space ☑ Browse datastore □ Configure datastore ☑ Low level file operations □ Move datastore □ Remove datastore ☑ Remove file Description: Remove a file from a datastore

Virtual machine, Inventory: Create, Register, Unregister **Virtual machine, Provisioning**: Allow virtual machine download, Allow virtual machine files upload **Virtual machine, Snapshots**: Remove Snapshots	

Assign Azure_Site_Recovery Privileges to earlier created domain user (in this example vcenterasr@cxlab.local)

At the vCenter entity level, click the **Manage** tab and select**Permissions** -> Click **Add Permission**	 vmware vSphere Web Client Navigator vCenter Inventory L... vCenter Servers 1 vCenter02.cxlab.local vCenter02.cxlab.local Actions Getting Started Summary Monitor Manage Related Objects Settings Scheduled Tasks Alarm Definitions Tags Permissions Sessions Storage User/GroupVSPHERE.LOCAL\Administrator VSPHERE.LOCAL\vpxd-extension-31481ee0-919a-11e6-8dc8-000c29a48a07 VSPHERE.LOCAL\Administrator VSPHERE.LOCAL\vpxd-31481ee0-919a-11e6-8dc8-000c29a48a07 CXLAB.LOCAL\Domain Users VSPHERE.LOCAL\vpxd-extension-31481ee0-919a-11e6-8dc8-000c29a48a07 VSPHERE.LOCAL\Administrators VSPHERE.LOCAL\vsphere-webclient-31481ee0-919a-11e6-8dc8-000c29a48a07

Select Azure_Site_recovery from the **Assigned Role** drop-down menu and select "**Propagate to children**". Then click **add**.	 vCenter02.cxlab.local - Add Permission Select the users or groups on the left and the role to assign to them on the right. Users and Groups The users or groups listed below are assigned the role selected on the right on 'vCenter02.cxlab.local'. User/Group · Role · Propa... Add... · Remove Assigned Role The users or groups obtain the permissions on the selected objects as defined by their assigned role. Azure_Site_Recovery All Privileges Alarms AutoDeploy Certificates Content Library Datacenter Datastore Datastore cluster Distributed switch ESX Agent Manager Extension Folder Global Host Host profile Description: All Privileges □ Propagate to children View Children OK · Cancel
Search earlier created user and select it, click **Add** -> **Ok** Click **Ok**.	 Select Users/Groups Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory. Domain: CXLAB Users and Groups Show Users First User/Group · Description/Full name vCenterASR · vCenterASR Add Users: CXLAB\vCenterASR Groups: Separate multiple names with semicolons · Check names OK · Cancel

Now we have a user with all needed rights on vCenter.	

User/Group	Role
CXLAB.LOCAL\vCenterASR	Azure_Site_Recovery
VSPHERE.LOCAL\vpxd-extension-31481ee0-919a-...	Administrator
VSPHERE.LOCAL\vpxd-31481ee0-919a-11e6-8dc...	Administrator
VSPHERE.LOCAL\Administrator	Administrator
VSPHERE.LOCAL\Administrator	Administrator
CXLAB.LOCAL\Domain Users	Administrator
VSPHERE.LOCAL\vpxd-extension-31481ee0-919a-...	Administrator
VSPHERE.LOCAL\Administrators	Administrator
VSPHERE.LOCAL\vsphere-webclient-31481ee0-9...	Administrator

Prepare for deployment

Hyper-V deployment

Follow this Microsoft article and configure the replication for on-premises Hyper-V virtual machines managed in System Center VMM clouds to Azure.

VMware deployment

Follow this Microsoft article and configure the replication for on-premises VMware virtual machines to Azure.

Enable protection for XenApp VMs

The following components of the Citrix XenApp deployment need to be protected to enable the complete replication and recovery.

- Protection of AD DNS server
- Protection of SQL database server
- Protection of Citrix Delivery Controller
- Protection of StoreFront server.
- Protection of XenApp Master (VDA)
- Protection of Citrix XenApp License Server

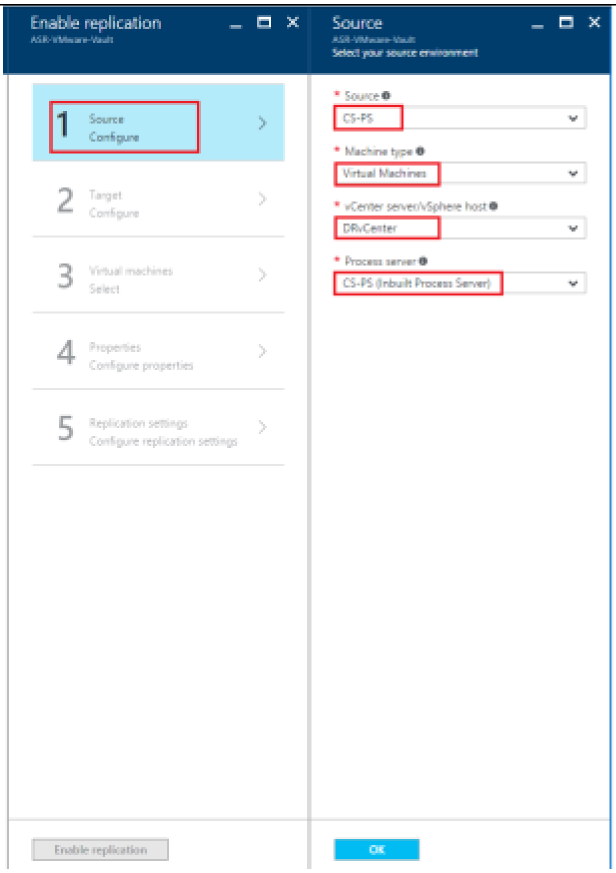
AD DNS replication

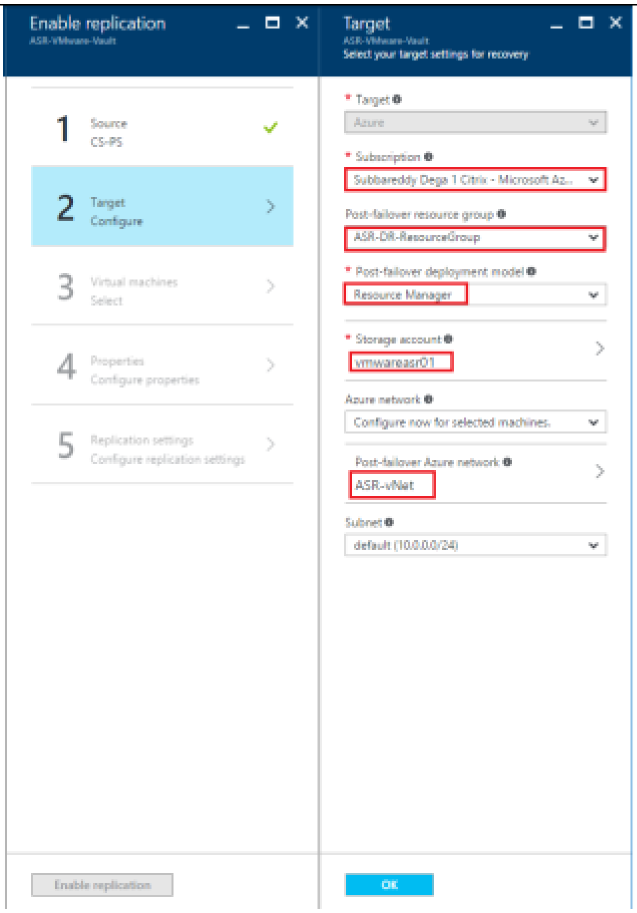
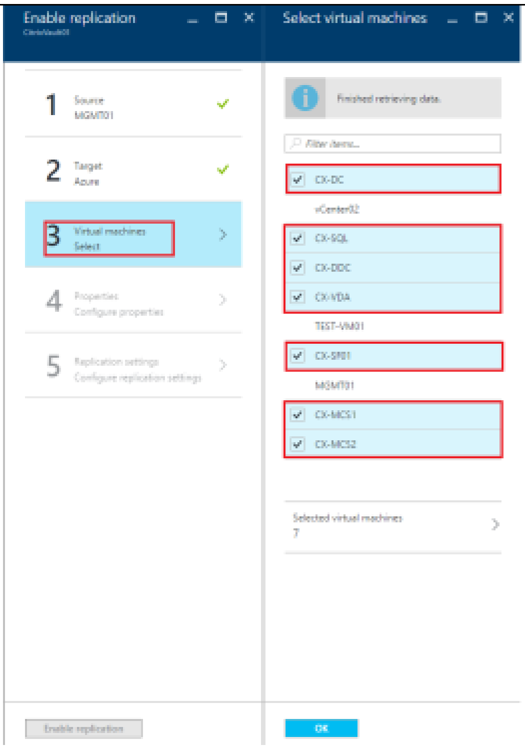
Please refer to Protect Active Directory and DNS with Azure Site Recovery on making a domain controller available on DR site.

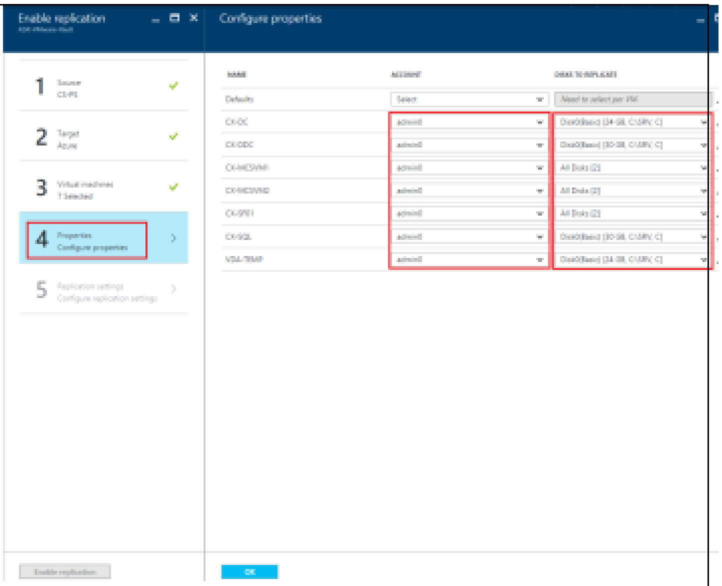
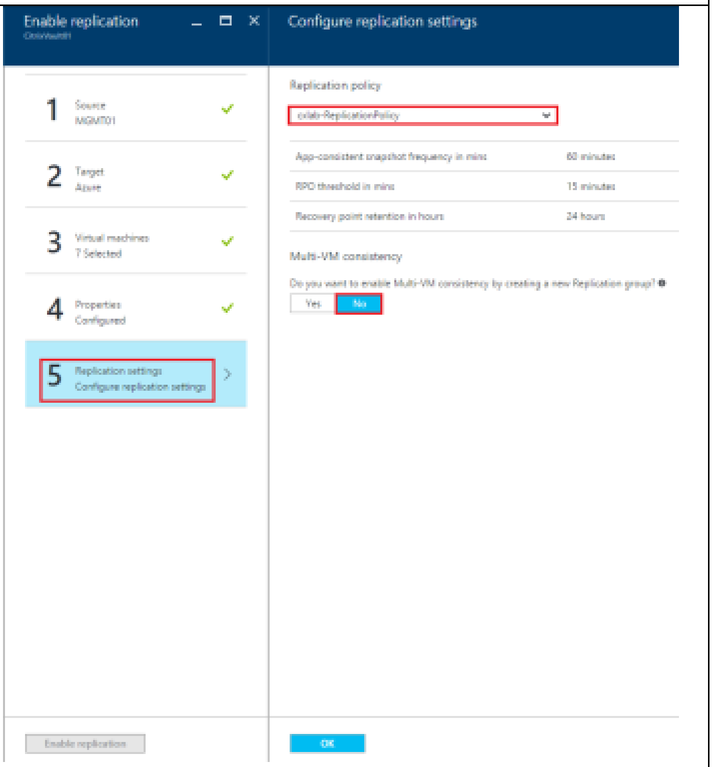
SQL Server replication

Please refer to Protect SQL Server with SQL Server disaster recovery and Azure Site Recovery for detailed technical guidance on the recommended option for protecting SQL server

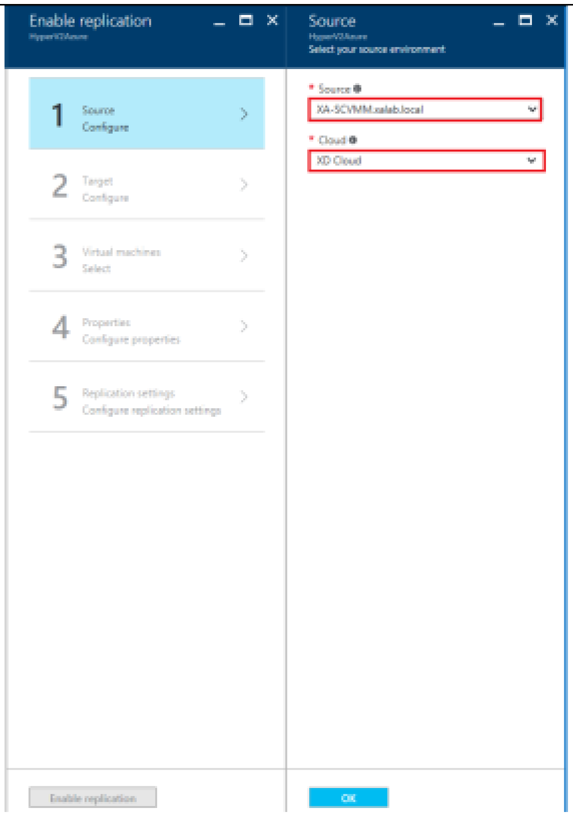
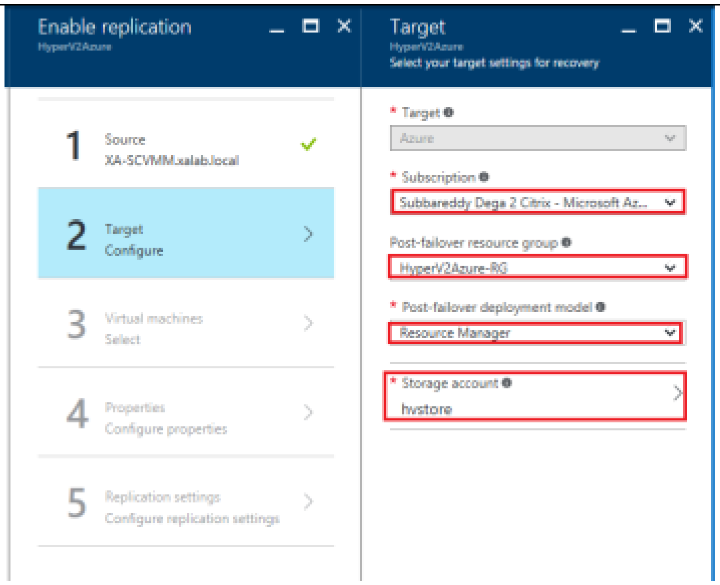
Enable replication for VMware virtual machines

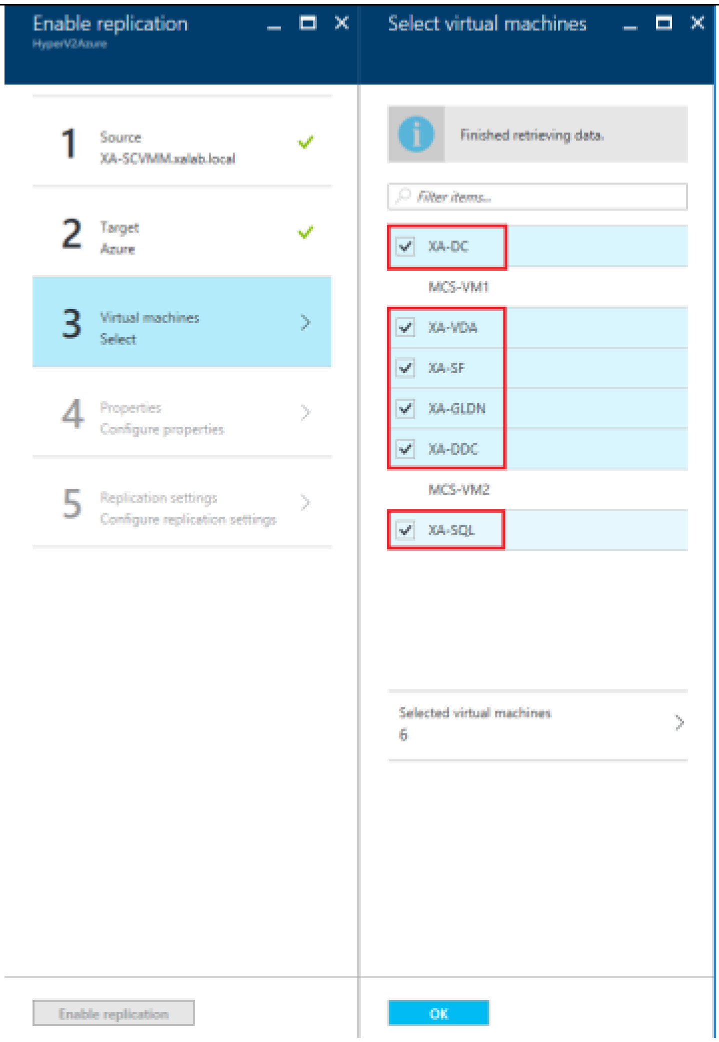
Click **Step 2: Replicate application** -> **Source**. Select the configuration server. **Machine type**, select Virtual Machines. **vCenter/vSphere Hypervisor**, select the vCenter server that manages the vSphere host. Select the **Process server.** Then click **OK**.	 Enable replication ASR-VMware-Vault 1 Source Configure 2 Target Configure 3 Virtual machines Select 4 Properties Configure properties 5 Replication settings Configure replication settings Source ASR-VMware-Vault Select your source environment * Source: CS-PS * Machine type: Virtual Machines * vCenter server/vSphere host: DRvCenter * Process server: CS-PS (Inbuilt Process Server)

Select the subscription, and in Post-failover deployment model, select the **Resource Manager**. Select the Azure storage account you want to use for replicating data. Select the Azure network and subnet to which Azure VMs will connect. 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. Then click **OK**.	 Enable replication ASR-VMware-Vault 1 Source CS-PS ✓ 2 Target Configure 3 Virtual machines Select 4 Properties Configure properties 5 Replication settings Configure replication settings Enable replication Target ASR-VMware-Vault Select your target settings for recovery * Target: Azure * Subscription: Subbareddy Dega 1 Citrix - Microsoft Az... Post-failover resource group: ASR-DR-ResourceGroup * Post-failover deployment model: Resource Manager * Storage account: vmwareasr01 Azure network: Configure now for selected machines. Post-failover Azure network: ASR-vNet Subnet: default (10.0.0.0/24) OK
In **Virtual Machines** -> **Select virtual machines**, click and select all XenApp VMs you want to replicate. Then click **OK**.	 Enable replication CitrixVault01 1 Source MGMT01 ✓ 2 Target Azure ✓ 3 Virtual machines Select 4 Properties Configure properties 5 Replication settings Configure replication settings Enable replication Select virtual machines Finished retrieving data. Filter items... ☑ CX-DC vCenter02 ☑ CX-SQL ☑ CX-DDC ☑ CX-VDA TEST-VM01 ☑ CX-SF01 MGMT01 ☑ CX-MCS1 ☑ CX-MCS2 Selected virtual machines 7 OK

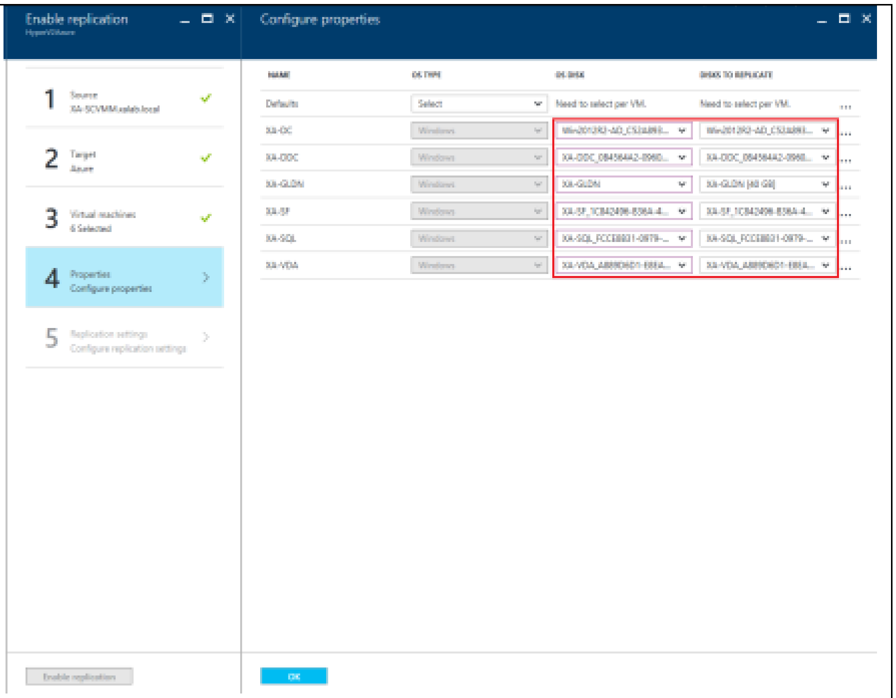
In **Configure properties**, select the account that will be used by the process server to automatically install the Mobility service on the machine. By default all disks are replicated. Then click **OK**.	 Enable replication 1 Source CS-PS ✓ 2 Target Azure ✓ 3 Virtual machines 7 Selected ✓ 4 Properties Configure properties 5 Replication settings Configure replication settings Configure properties NAME | ACCOUNT | DISKS TO REPLICATE Defaults | Select | Need to select per VM CX-DC | admin0 | Disk0[Basic] [24 GB, C:\SRV, C] CX-DDC | admin0 | Disk0[Basic] [30 GB, C:\SRV, C] CX-MCSVM1 | admin0 | All Disks [2] CX-MCSVM2 | admin0 | All Disks [2] CX-SF01 | admin0 | All Disks [2] CX-SQL | admin0 | Disk0[Basic] [30 GB, C:\SRV, C] VDA-TEMP | admin0 | Disk0[Basic] [24 GB, C:\SRV, C] Enable replication OK
In Replication settings > Configure replication settings, verify that the correct replication policy is selected Select **No** for **Enable Multi-VM consistency.** Then click **OK**. Click **Enable Replication**.	 Enable replication CitrixVault01 1 Source MGMT01 ✓ 2 Target Azure ✓ 3 Virtual machines 7 Selected ✓ 4 Properties Configured ✓ 5 Replication settings Configure replication settings Configure replication settings Replication policy ctlab-ReplicationPolicy App-consistent snapshot frequency in mins: 60 minutes RPO threshold in mins: 15 minutes Recovery point retention in hours: 24 hours Multi-VM consistency Do you want to enable Multi-VM consistency by creating a new Replication group? Yes [✓ No] Enable replication OK

Enable replication for Hyper-V virtual machines

Click **Step 2: Replicate application** > **Source**. In the **Source** blade, select the VMM server, and the cloud in which the Hyper-V hosts are located. Then click **OK**.	 Source HyperV2Azure Select your source environment * Source: XA-SCVMM.xalab.local * Cloud: XD Cloud Enable replication HyperV2Azure 1 Source Configure 2 Target Configure 3 Virtual machines Select 4 Properties Configure properties 5 Replication settings Configure replication settings Enable replication OK
In **Target**, select the subscription, post-failover deployment model, and the storage account you're using for replicated data. Then click **OK**.	 Target HyperV2Azure Select your target settings for recovery * Target: Azure * Subscription: Subbareddy Dega 2 Citrix - Microsoft Az... Post-failover resource group: HyperV2Azure-RG * Post-failover deployment model: Resource Manager * Storage account: hvstore Enable replication HyperV2Azure 1 Source XA-SCVMM.xalab.local 2 Target Configure 3 Virtual machines Select 4 Properties Configure properties 5 Replication settings Configure replication settings

In **Virtual Machines** > **Select virtual machines**, select all XenApp component virtual machine you want to replicate. Then click **OK**.	 Enable replication HyperV2Azure 1 Source XA-SCVMM.xalab.local ✓ 2 Target Azure ✓ 3 Virtual machines Select 4 Properties Configure properties 5 Replication settings Configure replication settings Enable replication Select virtual machines Finished retrieving data. Filter items... ☑ XA-DC MCS-VM1 ☑ XA-VDA ☑ XA-SF ☑ XA-GLDN ☑ XA-DDC MCS-VM2 ☑ XA-SQL Selected virtual machines 6 OK

In **Properties** > **Configure properties**, select the operating system for the selected VMs, and the OS disk. Then click **OK.**



Enable replication
HyperV2Azure

1 Source
XA-SCVMM.xalab.local ✓

2 Target
Azure ✓

3 Virtual machines
6 Selected ✓

4 Properties
Configure properties

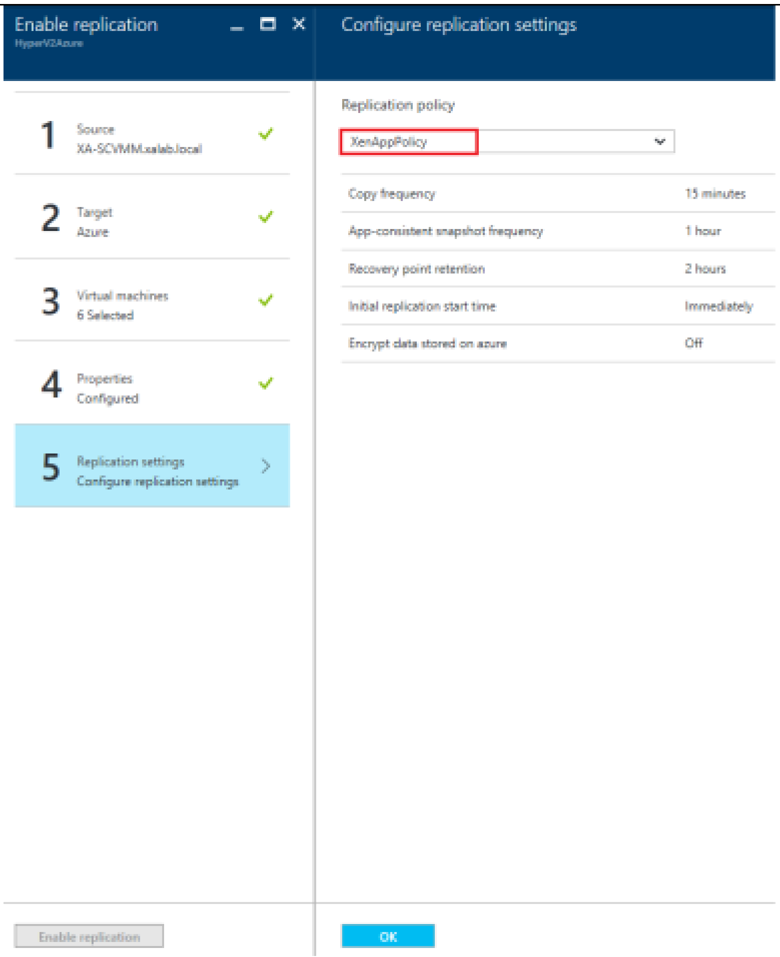
5 Replication settings
Configure replication settings

Configure properties

NAME	OS TYPE	OS DISK	DISKS TO REPLICATE
Defaults	Select	Need to select per VM.	Need to select per VM.
XA-DC	Windows	Win-2012R2-AD_C52A893...	Win-2012R2-AD_C52A893...
XA-DDC	Windows	XA-DDC_08456442-0960...	XA-DDC_08456442-0960...
XA-GLDN	Windows	XA-GLDN	XA-GLDN [40 GB]
XA-SF	Windows	XA-SF_1CB42498-B58A-4...	XA-SF_1CB42498-B58A-4...
XA-SQL	Windows	XA-SQL_FCCEB031-0879-...	XA-SQL_FCCEB031-0879-...
XA-VDA	Windows	XA-VDA_A889D6D1-E8E4...	XA-VDA_A889D6D1-E8E4...

In **Replication settings** > **Configure replication settings**, select the replication policy you want to apply for the protected VMs. Then click **OK**.

Click **Enable Replication**.



Enable replication
HyperV2Azure

1 Source
XA-SCVMM.xalab.local ✓

2 Target
Azure ✓

3 Virtual machines
6 Selected ✓

4 Properties
Configured ✓

5 Replication settings
Configure replication settings

Configure replication settings

Replication policy
XenAppPolicy

Copy frequency	15 minutes
App-consistent snapshot frequency	1 hour
Recovery point retention	2 hours
Initial replication start time	Immediately
Encrypt data stored on azure	Off

Create and configure recovery plan

Now that replication and protection are enabled for XenApp VMs, the final step is to configure a recovery plan in Azure.

A recovery plan groups Virtual machines together for purposes of failover and recovery. You can create a recovery plan in ASR to automate the failover process. Add the XenApp component virtual machines in the Recovery Plan.

Click **Recovery Plans** -> **+ Recovery Plan**. Provide an intuitive name for the recovery plan.

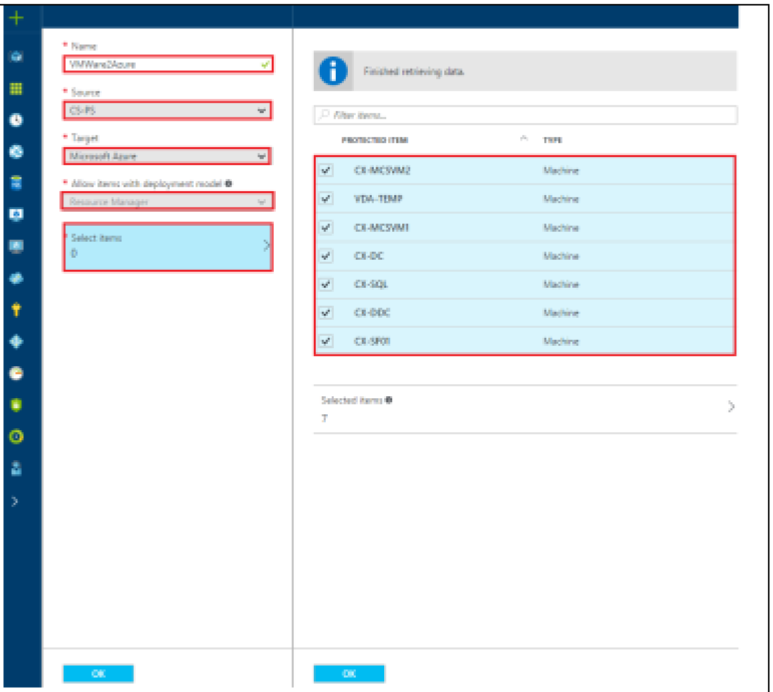
VMware only step:

Select source **as VMWare process server**, target as **Microsoft Azure**, and deployment model as **Resource Manager** and click **Select items**.

Hyper-V only step:

Select source **as VMM server**, target as **Microsoft Azure**, and deployment model as **Resource Manager** and click **Select items**

Select the XenApp deployment VMs and click **OK**.



* Name: VMWare2Azure

* Source: CS-PS

* Target: Microsoft Azure

* Allow items with deployment model: Resource Manager

* Select items: 0

Finished retrieving data.

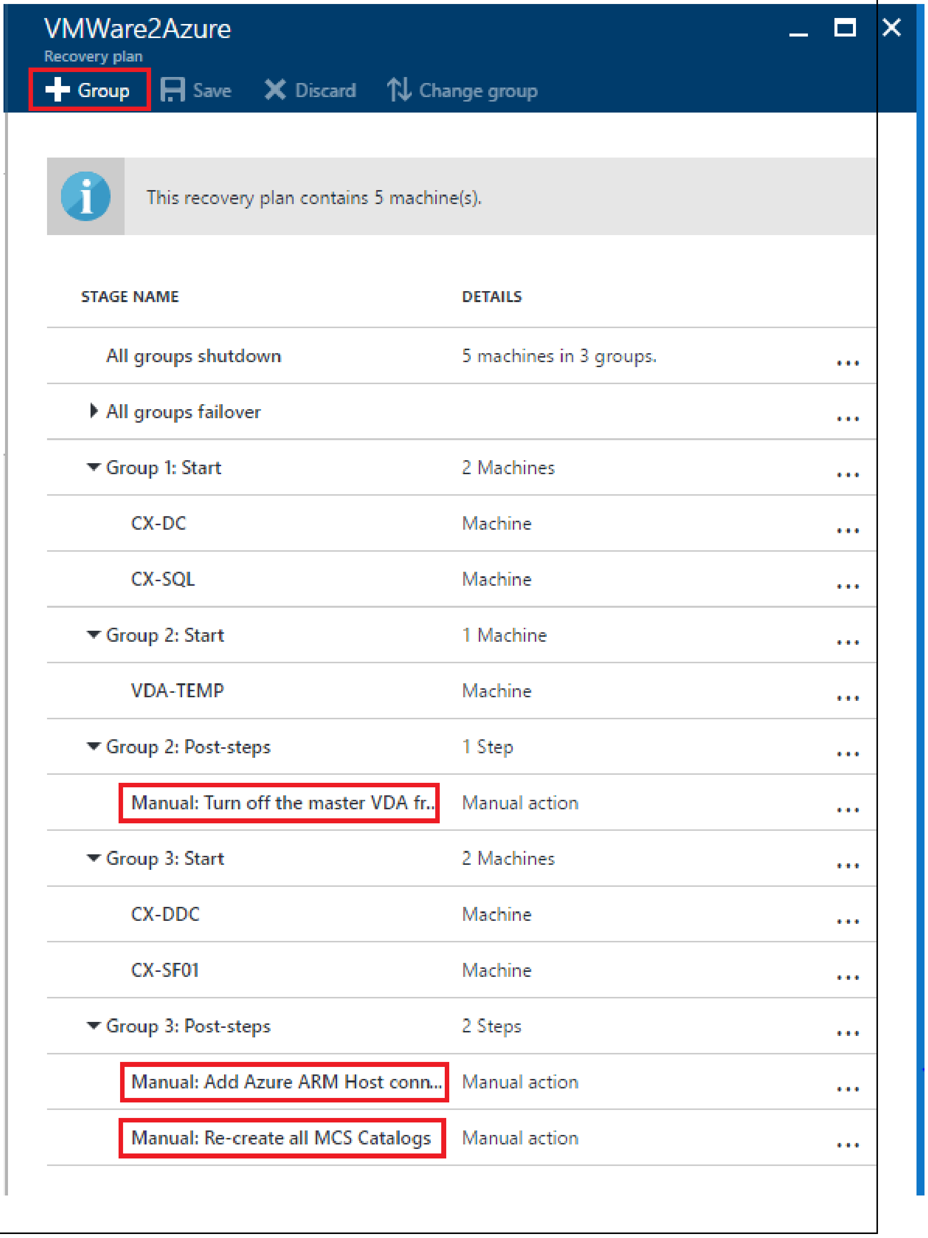
PROTECTED ITEM	TYPE
☑ CX-MCSVM2	Machine
☑ VDA-TEMP	Machine
☑ CX-MCSVM1	Machine
☑ CX-DC	Machine
☑ CX-SQL	Machine
☑ CX-DDC	Machine
☑ CX-SF01	Machine

Selected items: 7

Recovery plans can customized to add additional groups for specified startup order, additional virtual machines, scripts or manual actions. Scripts can be run, before or after a specific group in a recovery plan. Manual actions can be performed during failover, unplanned or test. Once the group order is set, the recovery plan can be saved, and run from the main recovery plans dashboard in the Azure portal.

This snapshot shows the complete customized XenApp recovery plan after adding all groups and steps.

Note: Recovery plan customization is same for both **Hyper-V** and **VMware**.



This recovery plan contains 5 machine(s).

STAGE NAME	DETAILS
All groups shutdown	5 machines in 3 groups.
All groups failover	
Group 1: Start	2 Machines
CX-DC	Machine
CX-SQL	Machine
Group 2: Start	1 Machine
VDA-TEMP	Machine
Group 2: Post-steps	1 Step
Manual: Turn off the master VDA fr..	Manual action
Group 3: Start	2 Machines
CX-DDC	Machine
CX-SF01	Machine
Group 3: Post-steps	2 Steps
Manual: Add Azure ARM Host conn...	Manual action
Manual: Re-create all MCS Catalogs	Manual action

Recovery plan customization Steps:

1. *Failover Group1: AD DNS and SQL Server VMs*

2. Failover Group2: VDA Master Image VM

3. Group 2 Manual or script action: Shutdown master VDA VM

   The Master VDA VM when failover to Azure will be in running state. To create new MCS catalogs using Azure ARM hosting the master VDA VM require in Stopped (de allocated) state. Shutdown the VM from Azure Portal.

4. Failover Group3: Delivery Controller and StoreFront server VMs

5. Group3 manual or script action 1: Add Azure RM host connection

   Create Azure ARM host connection in Delivery Controller machine to provision new MCS catalogs in Azure. Follow the steps as explained in this article.

6. Group3 manual or script action 2: Re-create MCS Catalogs in Azure

   The existing MCS or PVS clones on the primary site will not be replicated to Azure. You need to recreate these clones using the replicated master VDA and Azure ARM provisioning from Delivery controller.

   Follow the steps as explained in this article to create MCS catalogs in Azure.

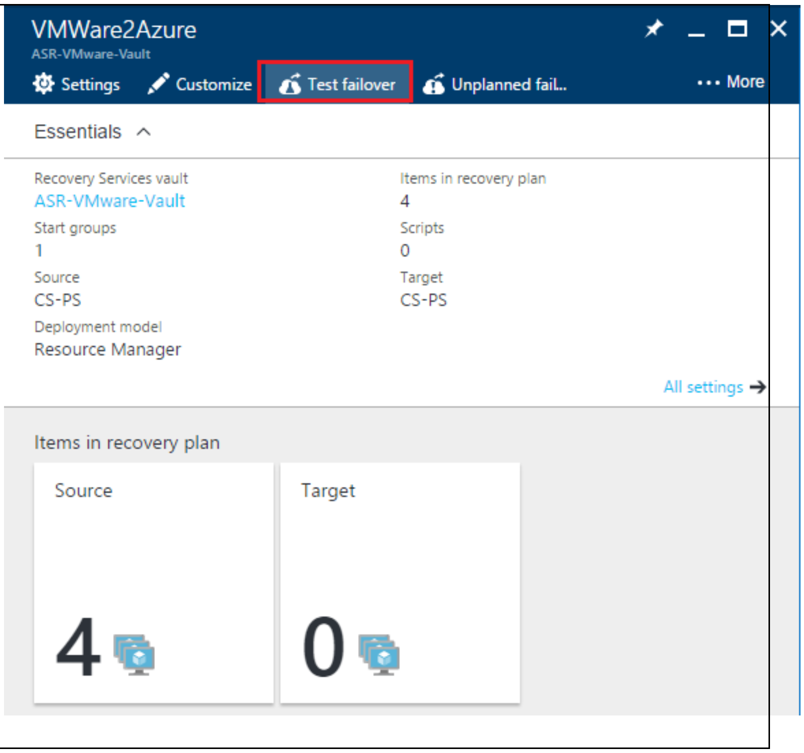
Perform a Test Failover

Using Test Failover you can test the recovery plan to verify if it will actually work before having to do it live. Testing can be done without impacting the live environment. Test failover is available only for VMware virtual machines and doesn't support for Hyper-V virtual machines.

Go to Azure manage portal and select your Site Recovery vault.

Click on the recovery plan you just created for XenApp.

Click on **Test Failover**.



Recovery Services vault: ASR-VMware-Vault

Items in recovery plan: 4

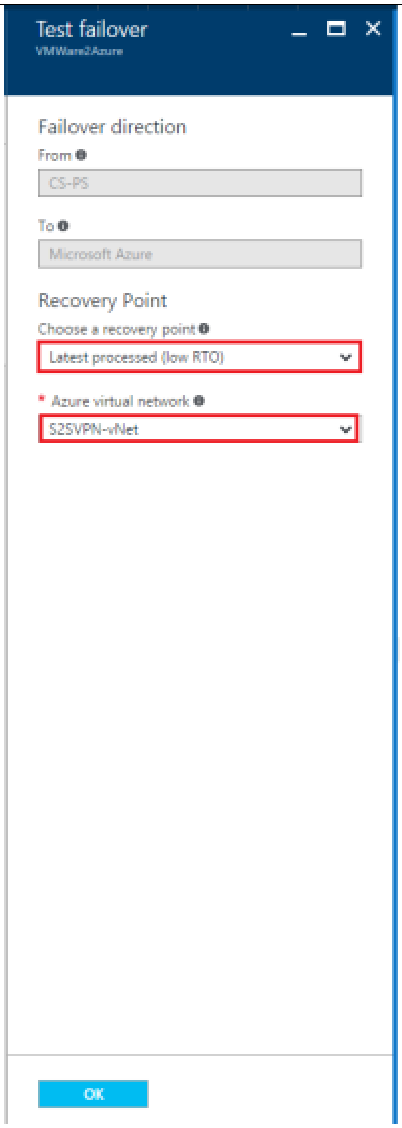
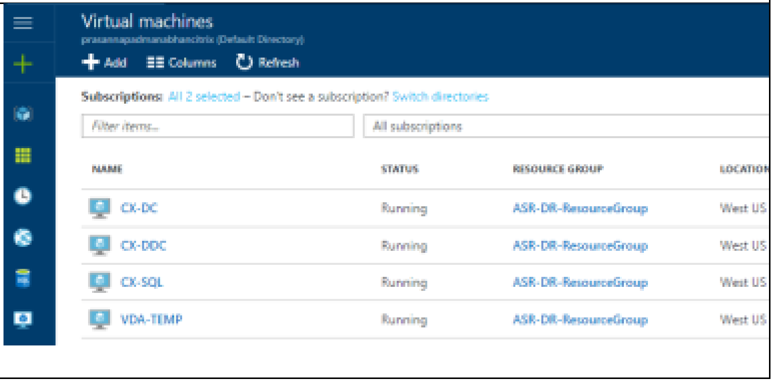
Start groups: 1

Scripts: 0

Source: CS-PS

Target: CS-PS

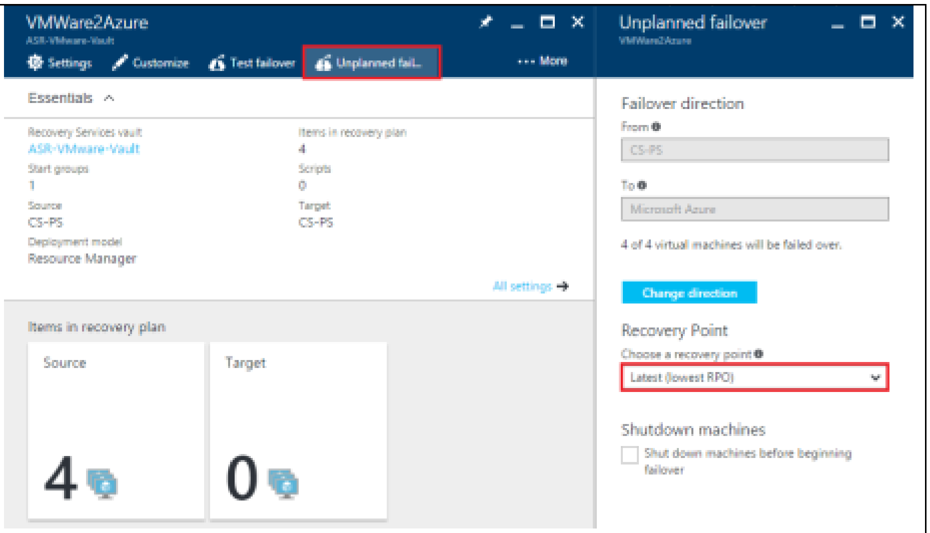
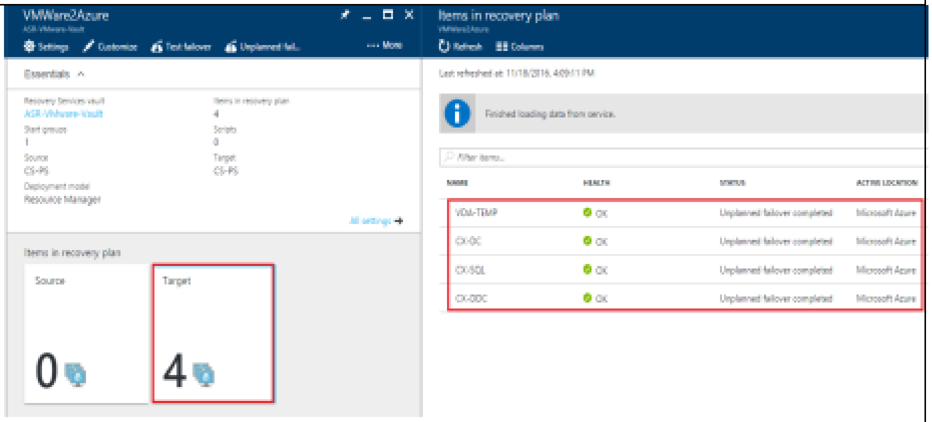
Deployment model: Resource Manager

Choose **Recovery point** as Latest processed (low RTO) and select **Azure virtual network** to failover. Click **OK** to begin failover.	 Test failover VMWare2Azure Failover direction From: CS-PS To: Microsoft Azure Recovery Point Choose a recovery point: Latest processed (low RTO) * Azure virtual network: S2SVPN-vNet OK
View the replica XenApp virtual machines in the Azure portal. Verify that the virtual machines starts successfully.	 Virtual machines prasannapadmanabhancitrix (Default Directory) Add Columns Refresh Subscriptions: All 2 selected – Don't see a subscription? Switch directories Filter items... All subscriptions NAME | STATUS | RESOURCE GROUP | LOCATION CX-DC | Running | ASR-DR-ResourceGroup | West US CX-DDC | Running | ASR-DR-ResourceGroup | West US CX-SQL | Running | ASR-DR-ResourceGroup | West US VDA-TEMP | Running | ASR-DR-ResourceGroup | West US

Perform an Unplanned Failover

Unplanned failover would be used in cases where an unexpected event results in an outage at primary Site.

To initiate an unplanned failover, go to Azure manage portal and select your Site Recovery vault.

Click on the recovery plan you created for XenApp. Click on **Unplanned Failover.** Choose a **Recovery point** and click **OK** to begin failover.	 VMWare2Azure ASR-VMware-Vault Settings / Customize / Test failover / Unplanned fail... / ··· More Essentials Recovery Services vault: ASR-VMware-Vault Items in recovery plan: 4 Start groups: 1 Scripts: 0 Source: CS-PS Target: CS-PS Deployment model: Resource Manager All settings → Items in recovery plan Source 4 Target 0 Unplanned failover VMWare2Azure Failover direction From: CS-PS To: Microsoft Azure 4 of 4 virtual machines will be failed over. Change direction Recovery Point Choose a recovery point: Latest (lowest RPO) Shutdown machines □ Shut down machines before beginning failover
Wait until the status shows "Unplanned failover completed" for all VMs.	 VMWare2Azure ASR-VMware-Vault Settings / Customize / Test failover / Unplanned fail... / ··· More Essentials Recovery Services vault: ASR-VMware-Vault Items in recovery plan: 4 Start groups: 1 Scripts: 0 Source: CS-PS Target: CS-PS Deployment model: Resource Manager All settings → Items in recovery plan Source 0 Target 4 Items in recovery plan VMWare2Azure Refresh / Columns Last refreshed at: 11/18/2016, 4:09:11 PM Finished loading data from service. Filter items... NAME / HEALTH / STATUS / ACTIVE LOCATION VDA-TEMP / ● OK / Unplanned failover completed / Microsoft Azure CX-DC / ● OK / Unplanned failover completed / Microsoft Azure CX-SQL / ● OK / Unplanned failover completed / Microsoft Azure CX-DDC / ● OK / Unplanned failover completed / Microsoft Azure

View the replicated XenApp virtual machines in the Azure portal. Verify that the virtual machine starts successfully and you can initiate a Remote Desktop connection to the virtual machines and verify the XenApp functionality.

Perform a Failback

Failback needs a VPN or ExpressRoute connection from the Azure network in which the Azure VMs are located to the on-premises site.

1. Go to Azure manage portal and select your Site Recovery vault.

2. Click on the recovery plan created for XenApp.
3. Click on **More** and select **Re-protect**.
4. In Re-protect select **Azure to on-premises** and click **OK.**
5. Select the appropriate options – Process and Master server, data store, Retention Drive and Failback Policy options.
6. Click OK to start the Failback process.

Best Practices

Capacity planning and readiness assessment

Hyper-V

Use Capacity planner tool to design the server, storage and network infrastructure for your Hyper-V Replica environment.

Azure

You can run the Azure Virtual Machine Readiness Assessment tool on VMs to ensure that they are compatible with Azure VMs and Azure Site Recovery Services. The Readiness Assessment Tool checks VM configurations and warns when configurations are incompatible with Azure.

Capacity planning is made up of at least two important components:

- Mapping on-premises Hyper-V/vSphere VMs to Azure VM sizes.
- Determining the required Internet bandwidth.

Network bandwidth considerations

Use the capacity planner tool to calculate the bandwidth that you need for VMs replication (initial replication and then delta). Configure the throttling to control the amount of bandwidth used for replication.

Master VDA VM instance selection to create MCS clones

Use Azure Dv2 instances for optimal user session density. For example, an Azure D13v2 instance supports 70 XenApp users under the default Login VSI Task Worker workload. A catalog of 5 D13v2 VMs can support up to 5x70=350 user sessions. You can provision a MCS catalog of 5 machines with in less than one hour.

Implementation Checklist

Step 1
Create Azure Site Recovery vault in Microsoft Azure subscription.
Check the prerequisites to protect your XenApp deployment.
Step 2
Hyper-V only step - Download Microsoft Azure Site Recovery Provider, and install it on VMM server.

VMware only step - Configure Protection server, Configuration server and Master Target servers appropriately
Step 3
Prepare resources.
Add an Azure Storage account.
Hyper-V only step - Download the Microsoft Azure Recovery Services Agent, and install it on Hyper-V host servers.
VMware only step – Make sure the mobility service is installed on all the VMs
Step 4
Enable protection for XenApp VMs in Hyper-V VMM clouds / VMware sites
Step 5
Map resources. Map on-premises networks to Azure VNET.
Step 7
Create the recovery plan
Perform test failover using the recovery plan
Ensure that all VMs have access to required resources, such as Active Directory
Ensure that network redirections for RDS are working
Step 8
Perform DR drill using planned and unplanned failovers
Ensure that all VMs have access to required resources, such as Active Directory
Ensure that XenApp is functional after failover to Azure

Limitations and known issues

Protection of MCS/PVS clones

Azure Site Recovery cannot replicate and protect the existing on-premises MCS or PVS clones. You need to recreate these clones using the Azure RM provisioning from Delivery controller.

Protection of NetScaler

Since the NetScaler is based on Free BSD and Azure Site Recovery does not support the FreeBSD OS. So NetScaler cannot be protected using the Azure Site Recovery. You need to deploy and configure a new NetScaler appliance from Azure Market place.

Troubleshooting

Remote desktop troubleshooting after failover

If the **Connect** button in the portal is grayed-out, and you are not connected to Azure via an Express Route or Site-to-Site VPN connection, you need to create and assign your virtual machine a public IP address before you can use Remote Desktop. You can then add a Public IP on the network interface of the virtual machine.

Follow this monitoring and troubleshooting guide to learn how to track replication health and troubleshoot techniques for Azure Site Recovery.

Summary

Using Azure Site Recovery, you can create a disaster recovery plan for your XenApp deployment. You can initiate the failover within seconds from anywhere in the event of a disruption and get the application up and running in a few minutes.

References

Replicating Hyper-V virtual machines to Azure with ASR: https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-vmm-to-azure

Replicating VMware virtual machines to Azure with ASR: https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-vmware-to-azure#run-a-test-failover

ASR planning and deployment best practices:https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-best-practices