

Module 12 Lab 1: Protecting Hyper-V VMs by using Azure Site Recovery

Exercise 1: Preparing the Azure Environment for Azure Site Recovery

- ASR helps keep your business apps up and running during planned and unplanned outages. ASR manages and orchestrates disaster recovery of on-premises machines and Azure virtual machines (VMs), including replication, failover, and recovery.

In this practice, you will:

- Verify that your Azure account has replication permissions.
- Create an Azure storage account. Images of replicated machines are stored in it.
- Create a Recovery Services vault. A vault holds metadata and configuration information for VMs, and other replication components.
- Set up an Azure network. When Azure VMs are created after failover, they're joined to this Azure network.

Task 1: Verify account permissions

- You already have an Azure Subscription and you're the administrator of your subscription. If you're not the subscription administrator, work with the administrator to assign the permissions you need. To enable replication for a new virtual machine, you must have permission to:
- Create a VM in the selected resource group.
 - Create a VM in the selected virtual network.
 - Write to the selected storage account.

To complete these tasks your account should be assigned the Virtual Machine Contributor built-in role. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor build-in role.

Task 2: Create a storage account

- Images of replicated machines are held in Azure storage. Azure VMs are created from the storage when you fail over from on-premises to Azure. The storage account must be in the same region as the Recovery Services vault. We're using **EastUS** in this task.

- 1. On **LON-HV1** virtual machine and send the **CTRL+ALT+DEL** command. Login using the username **Administrator** and password **Pa55w.rd**
- 2. Open a browser and navigate to the **Azure Portal** (<https://portal.azure.com>) and login with username **sheikhnasirLJTC0@gdcs4.com** and password **exIIPIgecfNyVk3R**
- 3. Search for and select **Storage accounts**.

The screenshot shows the Microsoft Azure portal homepage. A search bar at the top contains the text 'storage'. Below the search bar, the 'Azure services' section is visible, featuring a 'Create a resource' button, a 'Function App' icon, and a 'Navigate' section with 'Subscriptions' and 'Dashboard' links. The main content area displays search results under 'Services'. The 'Storage accounts' option is highlighted with a red box. Other listed services include Storage explorer, Storage accounts (classic), Storage Sync Services, Data Lake Storage Gen1, HPC caches, Disks (classic), OS images (classic), VM images (classic), and Free services. To the right of the search results, there's a 'Marketplace' section with links to Enterprise File Fabric, Storage account, StorSimple Virtual Device Series, and M365 Workplace Cloud Storage | Easy Intune Storage. Below the marketplace is a 'Documentation' section with links to Change feed in Azure Blob Storage | Microsoft Docs, Enable AD DS authentication to Azure file shares ..., Storage account overview - Azure Storage | Microsoft Docs, and Use Azure Storage with the Azure SDK for Python At the bottom right, a 'Resource Groups' section indicates 'No results were found.'

Tools



[Microsoft Learn](#)
Learn Azure with free online
courses and tutorials



[Azure Monitor](#)
Monitor your apps and
infrastructure



[Security Center](#)
Secure your apps and
infrastructure

- 4. Select + **Create**.
- 5. On **Create storage account** blade under **Resource Group** select **myRG-T17DSTITV**.
- 6. Scroll down to the Storage account name field and enter a name for the account. *The name you select must be unique within Azure and be between 3 and 24 characters, with numbers and lowercase letters only.*
- 7. In **Region**, select **East US**.
- 8. In **Performance**, select **Standard**
- 9. In **Redundancy**, select **Locally-redundant storage (LRS)**
- 10. In the **Data Protection** tab uncheck the below options:
 - **Enable Soft Delete for Blobs**
 - **Enable Soft Delete for Containers**
 - **Enable Soft Delete for File shares**
- 9. Select **Review + Create**.
- 10. On the Validation screen click **Create**.

Validation passed

Basics Networking Data protection Advanced Tags Review + create

Basics

Subscription	CloudShare4
Resource group	myRG-72NKXTAJW3
Location	East US
Storage account name	az303asr
Deployment model	Resource manager
Account kind	Storage (general purpose v1)
Replication	Locally-redundant storage (LRS)
Performance	Standard

Networking

Connectivity method	Public endpoint (all networks)
---------------------	--------------------------------

Create < Previous Next > Download a template for automation

Task 3: Create a Recovery Services vault

1. In the Azure portal, search for and select **Recovery Services vaults**.

The screenshot shows the Microsoft Azure portal homepage. At the top, there is a search bar with the text "Recovery". Below the search bar, there are two main sections: "Services" and "Resources". Under "Services", the "Recovery Services vaults" item is highlighted with a red box. The "Resources" section shows a message: "No results were found." To the right of the search results, there are several links under "Marketplace" and "Documentation". The "Documentation" section includes links to "Azure Instant Restore Capability - Azure Backup ...", "Back up Azure Files FAQ - Azure Backup | Microsoft Docs", "Create Recovery Services vaults - Azure Backup | Microso", and "Plan capacity for VMware disaster recovery with Azure Si". Below the search results, there is a "Resource Groups" section with a message: "No results were found." At the bottom of the page, there is a "Tools" section with icons for Microsoft Learn, Azure Monitor, and Security Center. The status bar at the bottom right shows the time as 8:22 AM and the date as 6/7/2020.

- 2. Click + **Create**.
- 3. In **Resource group**, select **myRG-T17DSTITVP**
- 4. In **Name**, enter a friendly name of **myVault** to identify the vault.
- 5. In **Location** select **East US**.

Create Recovery Services vault

Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription * CS-SUB-1452

Resource group * myRG

myRG

Create new

Instance Details

Vault name * myVault

Region * East US

Review + create

Next: Tags

- 6. Click **Review + create** then select **Create**.

Task 4: Set up an Azure network

- When Azure VMs are created from storage after failover, they're joined to this network.
- 1. In the Azure portal, select **Create a resource > Networking > Virtual network**.
- 2. Select **+Create**
- 3. In **Subscription**, select your subscription.
- 4. Select the resource group **myRG-T17DSTITVP**
- 5. In **Name**, enter **myVNet**
- 6. In **Location**, select **East US**. The network must be in the same region as the Recovery Services vault.

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/?configHash=zP1X7l2ngtNT&iepolyfill:> in the address bar. The page title is "Create virtual network - Mi...". The top navigation bar includes "Microsoft Azure", a search bar, and various icons. A user profile "Test_StudentDWWXB@..." is visible on the right.

Home > New >

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ

CS-SUB-1452



Resource group * ⓘ

myRG



[Create new](#)

Instance details

Name *

myVNet



Region *

(US) East US



[Review + create](#)

< Previous

Next : IP Addresses >

[Download a template for automation](#)



7. Select the **IP Addresses** tab.

8. In **Address range**, enter the range for the network .

9. In **Subnet**, enter the range for the subnet .

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet Remove subnet

Subnet name	Subnet address range
<input type="checkbox"/> default	10.0.0.0/24

Review + create < Previous Next : Security > Download a template for automation

10. Click **Review + create** then click **Create**.

⚠ The virtual network takes a few seconds to create.

Task 5: Prepare to connect to Azure VMs after failover

⚠ Note: These steps have already been carried out in the lab environment for you and no configuration is necessary, this section is informational.

- ② During a failover scenario you may want to connect to your replicated on-premises network.

To connect to Windows VMs using RDP after failover, allow access as follows:

- To access over the internet, enable RDP on the on-premises VM before failover. Make sure that TCP, and UDP rules are added for the Public profile, and that RDP is allowed in Windows Firewall > Allowed Apps for all profiles.
- To access over site-to-site VPN, enable RDP on the on-premises machine. RDP should be allowed in the Windows Firewall -> Allowed apps and features for Domain and Private networks. Check that the operating system's SAN policy is set to OnlineAll. Learn more. There should be no Windows updates pending on the VM when you trigger a failover. If there are, you won't be able to log in to the virtual machine until the update completes.
- On the Windows Azure VM after failover, check Boot diagnostics to view a screenshot of the VM. If you can't connect, check that the VM is running and review these troubleshooting tips.

Exercise 2: Set up disaster recovery of on-premises Hyper-V VMs to Azure

Task 1: Select a replication goal

1. In the Azure portal, select **All Services > Recovery Services vaults**, select the vault that was prepared in the previous task, **myVault**.
2. On the Recovery Services vault blade, select **Settings -> Properties**.
3. In the properties pane, select **Security Settings -> Update**.
4. In the security settings pane, under **Soft Delete**, select **Disabled**.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a vertical menu with sections like Tags, Diagnose and solve problems, Settings (Identity, Private endpoint connections, Properties, Locks, Export template), Getting started (Backup, Site Recovery), and Protected items (Backup items, Replicated items). The 'Properties' link under 'Settings' is highlighted with a red box. The main content area is titled 'Security Settings' for 'myVault'. It includes a 'Save' and 'Discard' button. A 'Configuration' section asks if Multi-Factor Authentication is configured, with a dropdown menu. Below it is a 'Soft Delete (For Azure Virtual Machines)' section, which is currently set to 'Disabled' (button highlighted with a red box). A warning message states: 'All Future deletes will be immediate and will not have soft delete protection.' The 'Security Features' section shows 'Enabled' status and provides instructions for enabling security features using specific agent versions. The bottom right corner shows the date and time: 8:31 AM, 6/7/2020.

- 5. Click **Save**
- 6. On the **MyVault** blade, in the vertical menu, in the **Getting started** section, select **Site Recovery**
- 7. On the **MyVault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **1. Prepare infrastructure**.

ws2019-08-hvm0-7ytizovdo7ync.eastus.cloud... https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi Microsoft Azure ws2019-08a-rsvault - Micro...

Home > Recovery Services vaults > ws2019-08a-rsvault

ws2019-08a-rsvault | Site Recovery

Recovery Services vault

Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Identity
- Private endpoint connections
- Properties
- Locks

Getting started

- Backup
- Site Recovery**

Protected items

Hyper-V machines to Azure

Protect your Hyper-V virtual machines for disaster recovery by replicating to Azure.

1: Prepare infrastructure (highlighted with a red box)

2: Enable replication

3: Manage recovery plans

Protect your Hyper-V machines by replicating to another Hyper-V site

1: Prepare infrastructure

2: Enable replication

8. On the **Deployment planning** tab of the **Prepare infrastructure** blade, in the **Deployment planning completed?** drop-down list, select **Yes, I have done it** and select **Next**.

ws2019-08-hvm0-7ytizovdo7ync.eastus.cloud... https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi Microsoft Azure Prepare infrastructure - Mic...

Home > Recovery Services vaults > ws2019-08a-rsvault >

Prepare infrastructure

Hyper-V machines to Azure

1 Deployment planning (highlighted with a blue underline)

2 Source settings **3 Target settings** **4 Replication policy** **5 Review**

Tip: Looking for a way to migrate your virtual machines? We strongly recommend that you use the new 'Azure Migrate: Server Migration' capability. Go to [Azure Migrate](#)

Allocate sufficient network bandwidth and other resources to avoid any replication issues.

Download and run [deployment planner](#) to estimate network bandwidth, storage and other requirements. [Learn more](#)

Deployment planning completed? *

Previous

- 9. On the **Source settings** tab of the **Prepare infrastructure** blade, next to the **Are you Using System Center VMM to manage Hyper-V hosts** label, select the **No** option.
- 10. On the **Source settings** tab of the **Prepare infrastructure** blade, select the **Add Hyper-V site** link, on the **Create Hyper-V Site** blade, in the **Name** text box, enter **OnPremsite** and select **OK**.
- 11. On the **Source settings** tab of the **Prepare infrastructure** blade, select the **Add Hyper-V server** link.
- 12. On the **Add Server** blade, select the **Download** link in step 4 to download the vault credentials file.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Prepare infrastructure' blade is displayed under 'Hyper-V machines to Azure'. It has four tabs: Deployment planning (marked with a checkmark), Source settings (selected), Target settings, and Replication. Under 'Source settings', there is a question 'Are you Using System Center VMM to manage Hyper-V hosts?' with 'No' selected. Below it, a 'Hyper-V site' field contains 'ws2019-08 Hyper-V Site' and a 'Add Hyper-V site' button. A success message says 'Successfully created Hyper-V site. (View job)'. Under 'Hyper-V servers', it says 'No servers found in the selected Hyper-V site. Please may take approximately 15 min to 30 mins.' and has a 'Add Hyper-V server' button. On the right, the 'Add Server' blade for 'ws2019-08a-rsvault' is shown. It specifies 'Hyper-V server' as the 'Server type'. A note says 'Adding Hyper-V server may take 15 minutes to 30 minutes'. Below it, instructions for registering a Hyper-V host (Windows Server 2012 R2 or above) are listed. At the bottom of the 'Add Server' blade is a blue 'Download' button, which is highlighted with a red rectangle.

- 13. On the **Add Server** blade, select the **Download** link in step 3 of the procedure for adding on-premises Hyper-V hosts in order to download the Microsoft Azure Site Recovery Provider.

<https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>

Prepare infrastructure

Hyper-V machines to Azure

✓ Deployment planning 2 Source settings 3 Target settings 4 Replication

Are you Using System Center VMM to manage Hyper-V hosts? * Yes No

Hyper-V site * On Prem Site [Add Hyper-V site](#)

 Successfully created Hyper-V site. [\(View job\)](#)

Hyper-V servers [\(i\)](#)

No servers found in the selected Hyper-V site. Please may take approximately 15 min to 30 mins.

[Add Hyper-V server](#)

Previous Next

14. When prompted, in the browser window, select Run to launch **AzureSiteRecoveryProvider.exe. This will start the **Azure Site Recovery Provider Setup (Hyper-V server)** wizard.**

<https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>

Prepare infrastructure

Hyper-V machines to Azure

✓ Deployment planning 2 Source settings 3 Target settings 4 Replication

Are you Using System Center VMM to manage Hyper-V hosts? * Yes No

Hyper-V site * ws2019-08 Hyper-V Site [Add Hyper-V site](#)

 Successfully created Hyper-V site. [\(View job\)](#)

Hyper-V servers [\(i\)](#)

No servers found in the selected Hyper-V site. Please may take approximately 15 min to 30 mins.

[Add Hyper-V server](#)

Do you want to run or save **AzureSiteRecoveryProvider.exe (46.6 MB) from download.microsoft.com?**

Run **Save** **Cancel**

15. On the **Microsoft Update** page, select **Off** and select **Next**.

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>. The page title is "Add Server - Microsoft Azure". The main content area is titled "Prep Microsoft Update". On the left, there's a sidebar with sections for "Hyper-V" and "Azure Site Recovery Provider Setup (Hyper-V server)". The "Hyper-V" section has a checked checkbox labeled "De" and a blue radio button labeled "Microsoft Update". Below it is another blue radio button labeled "Installation". To the right of the sidebar, there's a detailed description of Microsoft Update, two radio button options ("On (recommended)" and "Off"), and links to "Microsoft Update FAQ" and "Microsoft Update Privacy Statement". At the bottom right of the main content area are "Next" and "Cancel" buttons.

16. On the **Provider installation** page, select **Install**.

Prep Provider Installation

Microsoft Update

Installation

Specify where you want to install the Microsoft Azure Site Recovery Provider. This setup will install Azure Site Recovery Provider and Azure Recovery Services Agent on this computer.

Installation Location: C:\Program Files\Microsoft Azure Site Recovery Provider [Browse](#)

[Install](#) [Cancel](#)

[Previous](#) [Next](#)

5. Install the Provider on the Hyper-V host and use the registration key to register the host in the vault. [Learn more](#).

17. Switch to the Azure portal and, on the **Add Server** blade, select the **Download** button in step 4 of the procedure for registering on-premises Hyper-V hosts in order to download the vault registration key. When prompted, select **Save** to save the vault credentials file in the **Downloads** folder.

Add Server

ws2019-08a-rsvault

Server type: Hyper-V server

Source settings

Are you Using System Center VMM to manage Hyper-V hosts? * Yes No

Hyper-V site * [Add Hyper-V site](#) (ws2019-08 Hyper-V Site) (Successfully created Hyper-V site. [View job](#))

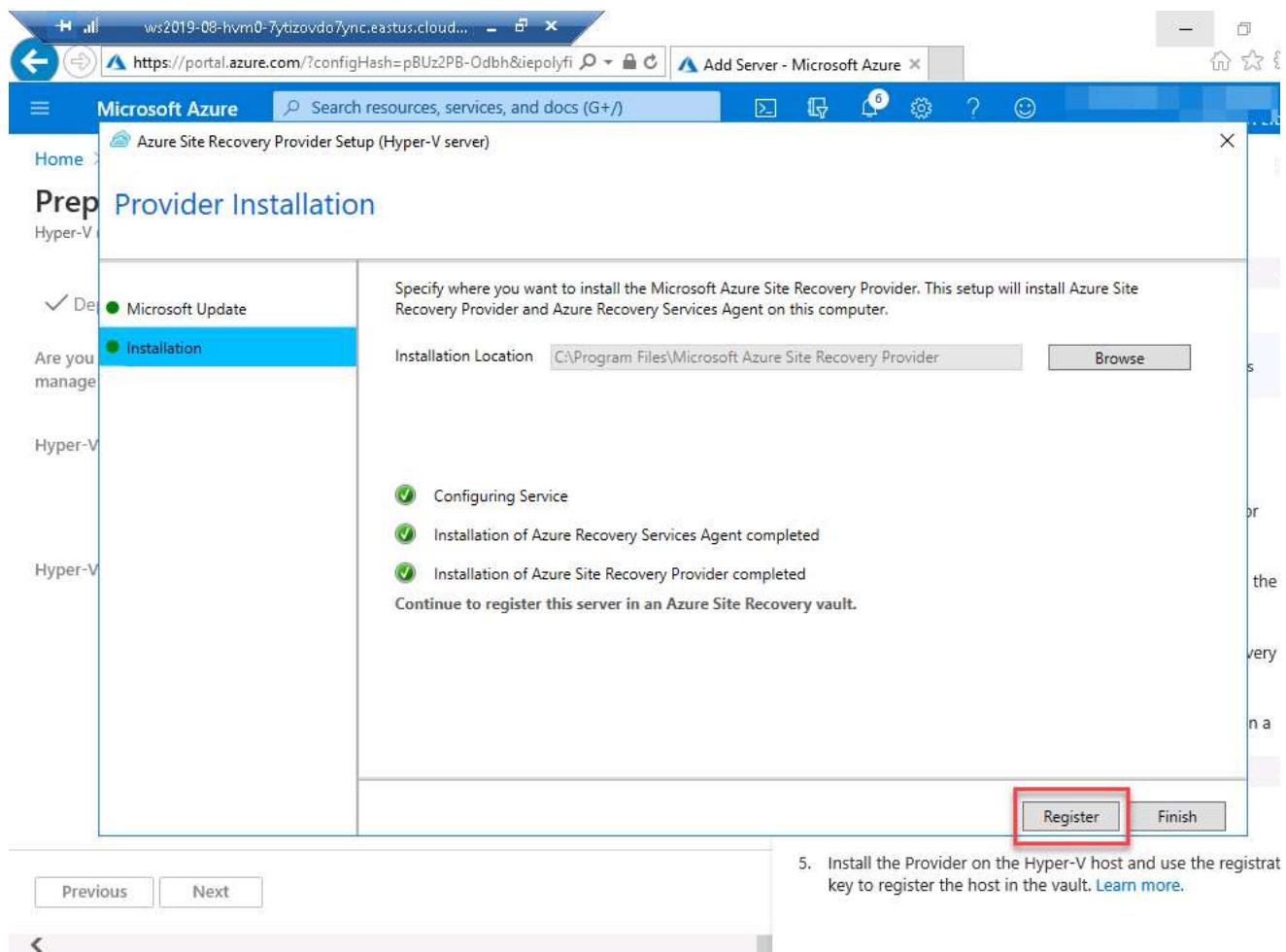
Hyper-V servers [Add Hyper-V server](#) (No servers found in the selected Hyper-V site. Please wait approximately 15 min to 30 mins.)

Adding Hyper-V server may take 15 minutes to 30 minutes

Register your Hyper-V host(s) On-premises

1. Make sure the host is running Windows Server 2012 R2 or above. [Learn more](#).
2. Configure Proxy setting and ensure each host can access the [Service URLs](#).
3. [Download](#) the installer for the Microsoft Azure Site Recovery Provider.
4. [Download](#) the vault registration key to register the host in a Hyper-V site (ws2019-08 Hyper-V Site) [Download](#)
5. Install the Provider on the Hyper-V host and use the registration key to register the host in the vault. [Learn more](#).

18. Switch to the **Provider installation** wizard window and select **Register**. This will start the **Microsoft Azure Site Recovery Registration Wizard**.



19. On the **Vault Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Browse**, in the **Open** window, navigate to the **Downloads** folder, select the vault credentials file, and select **Open**.

5. Install the Provider on the Hyper-V host and use the registration key to register the host in the vault. [Learn more](#).

ws2019-08-hvm0-7ydzovdo7ync.eastus.cloud... https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi Add Server - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+) Home Microsoft Azure Site Recovery Registration Wizard Prep Vault Settings... Hyper-V ✓ Define your vault settings... Are you managing your vault? Hyper-V Hyper-V Vault Settings Select the registration key file you downloaded from the Azure Site Recovery portal and specify vault settings. [Learn More](#)

Key file ws2019-08a-rsvault_ws2019-08 Hyper-V Site_Tue Sep 22 2020.VaultCre [Browse](#)

Subscription 3725d2ba-9e32-4c51-96d9-af445f4cd20d

Vault name ws2019-08a-rsvault

Hyper-V site name ws2019-08 Hyper-V Site

Next Cancel

Previous Next

5. Install the Provider on the Hyper-V host and use the registration key to register the host in the vault. [Learn more](#).

- 20. Back on the **Vault Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Next**.
- 21. On the **Proxy Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, accept the default settings and select **Next**.

The screenshot shows the Microsoft Azure Site Recovery Registration Wizard. The title bar says "Microsoft Azure" and "Add Server - Microsoft Azure". The main area is titled "Prep" and "Proxy Settings...". On the left, there's a sidebar with sections for "Vault Settings", "Proxy Settings" (which is selected), and "Registration". The main pane contains instructions: "Specify how the Provider running on the server connects to Azure Site Recovery. Connectivity will be verified when you click Next." It also says "Click next to check connectivity with Azure Site Recovery Service." with two radio button options: "Connect directly to Azure Site Recovery without a proxy server" (selected) and "Connect to Azure Site Recovery using a proxy server". At the bottom are "Previous", "Next", and "Cancel" buttons.

5. Install the Provider on the Hyper-V host and use the registration key to register the host in the vault. [Learn more](#).

22. On the **Registration** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Finish**.

The screenshot shows the Microsoft Azure Site Recovery Registration Wizard. The title bar says "Microsoft Azure" and "Add Server - Microsoft Azure". The main area is titled "Prep" and "Registration". On the left, there's a sidebar with sections for "Vault Settings", "Proxy Settings" (which is selected), and "Registration". The main pane displays a green checkmark icon and the message "The server was registered in the Azure Site Recovery vault". At the bottom are "Previous", "Next", and "Finish" buttons.

5. Install the Provider on the Hyper-V host and use the registration key to register the host in the vault. [Learn more](#).

23. Switch back to the browser window displaying the Azure portal and refresh the page. When prompted, select **Leave this page**.

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>. The page title is "Add Server - Microsoft Azure". The main content area is titled "Prepare infrastructure" and "Hyper-V machines to Azure". It includes sections for "Deployment planning", "Source settings", "Target settings", and "Replication". Under "Source settings", there is a question "Are you Using System Center VMM to manage Hyper-V hosts? *". The "No" radio button is selected. Below it, there is a "Hyper-V site" dropdown set to "ws2019-08a-rsvault" and a "Hyper-V servers" section with a note about no servers found. On the right side, there is a "Server type" section set to "Hyper-V server" and a "Download" button for the "ws2019-08 Hyper-V Site". A modal dialog box titled "Windows Internet Explorer" is open, asking "Are you sure you want to leave this page?" with "Leave this page" and "Stay on this page" options. The "Leave this page" option is highlighted.

24. Back on the **myVault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **1. Prepare infrastructure**.

https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi

myVault - Microsoft Azure

Home >

myVault | Site Recovery

Recovery Services vault

Search (Ctrl+ /)

«

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Identity

Private endpoint connections

Properties

Locks

Getting started

Backup

Site Recovery

Protected items

Backup items

25. On the **Deployment planning** tab of the **Prepare infrastructure** blade, in the **Deployment planning completed?** drop-down list, select **Yes, I have done it** and select **Next**.
26. On the **Source settings** tab of the **Prepare infrastructure** blade, next to the **Are you Using System Center VMM to manage Hyper-V hosts** label, select the **No** option.
27. Verify that the **Hyper-V site** and **Hyper-V servers** settings are set correctly and select **Next**.

3: Manage recovery plans



Hyper-V machines to Azure

Protect your Hyper-V virtual machines for disaster recovery by replicating to Azure.

1: Prepare infrastructure

2: Enable replication

3: Manage recovery plans



Protect your Hyper-V machines by replicating to another Hyper-V site

[View documentation](#)

<https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>

Prepare infrastructure

Hyper-V machines to Azure

✓ Deployment planning 2 Source settings 3 Target settings 4 Replication policy 5 Review

Are you Using System Center VMM to manage Hyper-V hosts? *

Yes
 No

Hyper-V site *

On Prem Site

Add Hyper-V site

Hyper-V servers

Name	Connection stat...
LON-HV1.corp.local	Connected

Previous Next

28. On the **Target settings** tab of the **Prepare infrastructure** blade, accept the default settings and select **Next**.

<https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>

Prepare infrastructure

Hyper-V machines to Azure

✓ Deployment planning ✓ Source settings 3 Target settings 4 Replication policy 5 Review

Subscription *

CloudShare4

Post-failover deployment model *

Resource Manager

Storage account(s)

Found az303asr (Standard) storage account.

Network(s)

myVNet

Previous Next

29. On the **Replication policy** tab of the **Prepare infrastructure** blade, select **Create new policy and associate**.

The screenshot shows the 'Prepare infrastructure' blade for a Hyper-V machine named 'ws2019-08a-rsvault'. The 'Replication policy' tab is selected. A dropdown menu under 'Replication policy' has an option 'Create new policy and associate' highlighted with a red box.

30. On the **Create and associate policy** blade, specify the following settings (leave others with their default values) and select **OK**:

Table 11: Policy settings

Setting	Value
Name	replicationpolicy
Copy frequency	30 seconds

31. Back on the **Replication policy** tab of the **Prepare infrastructure** blade, wait until the site has been associated with the policy and select **Next**.

32. On the **Review** tab of the **Prepare infrastructure** blade, select **Prepare**

https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi

Microsoft Azure

Search resources, services, and docs (G+/)

Prepare infrastructure - Mic... x

Home > myVault >

Prepare infrastructure

Hyper-V machines to Azure

✓ Deployment planning ✓ Source settings ✓ Target settings ✓ Replication policy 5 Review

Deployment planning
Deployment planning Completed

Source settings
Hyper-V site On Prem Site
Hyper-V servers 1 (1 connected, 0 disconnected)

Target settings
Subscription CloudShare4
Post-failover deployment model Resource Manager
Storage account(s) Found az303asr (Standard) storage account.
Network(s) myVNet

Replication policy
Replication policy Replication Policy

Previous Prepare

Task 2: Enable replication of a Hyper-V virtual machine

1. In the Azure portal, on the **ws2019-08a-rsvault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **2. Enable replication**.

ws2019-08-hvm0-7ydzovdo7ync.eastus.cloudapp.azure.com https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi ws2019-08a-rsvault - Micro... Microsoft Azure Search resources, services, and docs (G+) Home > ws2019-08a-rsvault | Site Recovery Recovery Services vault

Search (Ctrl+ /) Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings

Identity Private endpoint connections Properties Locks

Getting started

Backup Site Recovery

Protected items

Backup items

2. On the **Source environment** tab of the **Enable replication** blade, in the **Source location** drop-down list, select **On Prem site** and select **Next**.

Hyper-V machines to Azure
Protect your Hyper-V virtual machines for disaster recovery by replicating to Azure.

1: Prepare infrastructure
2: Enable replication
3: Manage recovery plans

Protect your Hyper-V machines by replicating to another Hyper-V site

1: Prepare infrastructure
2: Enable replication
3: Manage recovery plans

⚠ If the **Onpremsite** option does not appear, Please refresh your browser.

Source location *

Previous

1. On the **Target environment** tab of the **Enable replication** blade, specify the following settings (leave others with their default values) and select **Next**:

Table 12: Target environment settings

Setting	Value
Subscription	CloudShare4
Post-failover resource group	myRG-T17DSTITVP
Post-failover deployment model	Resource Manager
Storage account	the name of the storage account you created in the first task of this exercise
Azure network	Configure now for selected machines
Virtual network	myVNet
Subnet	default (10.0.0.0/24)

https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi

Enable replication - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/-)

Home > myVault >

Enable replication

Hyper-V machines to Azure

Source environment **Target environment** **Virtual machine selection** **Replication settings** **Replication policy**

Subscription and resource group

Subscription * Post-failover resource group *

Deployment model

Post-failover deployment model *

Storage

Storage account *

Network

Virtual network * Subnet *

Previous **Next**

2. On the **Virtual machine selection** tab of the **Enable replication** blade, select the **LON-APP1** checkbox and select **Next**.

https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi

Enable replication - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/-)

Home > myVault >

Enable replication

Hyper-V machines to Azure

Source environment **Target environment** **Virtual machine selection** **Replication settings** **Replication policy**

Unable to view / select your VMs? Click [here](#) to know why.

Finished retrieving data.

Filter items... LON-APP1

Selected machines: 1

Previous **Next**

3. On the **Replication settings** tab of the **Enable replication** blade, in the **Defaults** row and **OS type** column, select **Windows** from the drop-down list and select **Next**.

Enable replication

Hyper-V machines to Azure

✓ Source environment ✓ Target environment ✓ Virtual machine selection 4 Replication settings 5 Replication policy

Unable to view / select your disks? Click here to know why.

Name	OS type	OS disk	Disks to replicate
Defaults	Select	Need to select per VM.	Need to select per VM.
LON-APP1	Windows	LON-APP1	All Disks [1]

Previous Next

4. On the **Replication policy** tab of the **Enable replication** blade, accept the default settings and select **Next**.

<https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>

Enable replication

Hyper-V machines to Azure

✓ Source environment ✓ Target environment ✓ Virtual machine selection ✓ Replication settings 5 Replication policy

Replication policy *

Copy frequency	30 Seconds
Recovery point retention	2 Hours
App consistent snapshot frequency	1 Hour
Initial replication start time	Immediately
Encrypt data stored on Azure	Off
VMM settings	Not configured

Previous Next

5. On the **Review** tab of the **Enable replication** blade, select **Enable replication**.

<https://portal.azure.com/?configHash=pBUz2PB-Odbh&iepolyfi>

Enable replication

Hyper-V machines to Azure

✓ Target environment ✓ Virtual machine selection ✓ Replication settings ✓ Replication policy 6 Review

Source environment

Hyper-V site	On Prem Site
--------------	--------------

Target selection summary

Subscription	CloudShare4
Resource group	myRG-72NKXTAJW3
Post-failover deployment model	ResourceManagement
Storage account	az303asr
Network	myVNet

Virtual machine selection summary

Virtual Machines	1
------------------	---

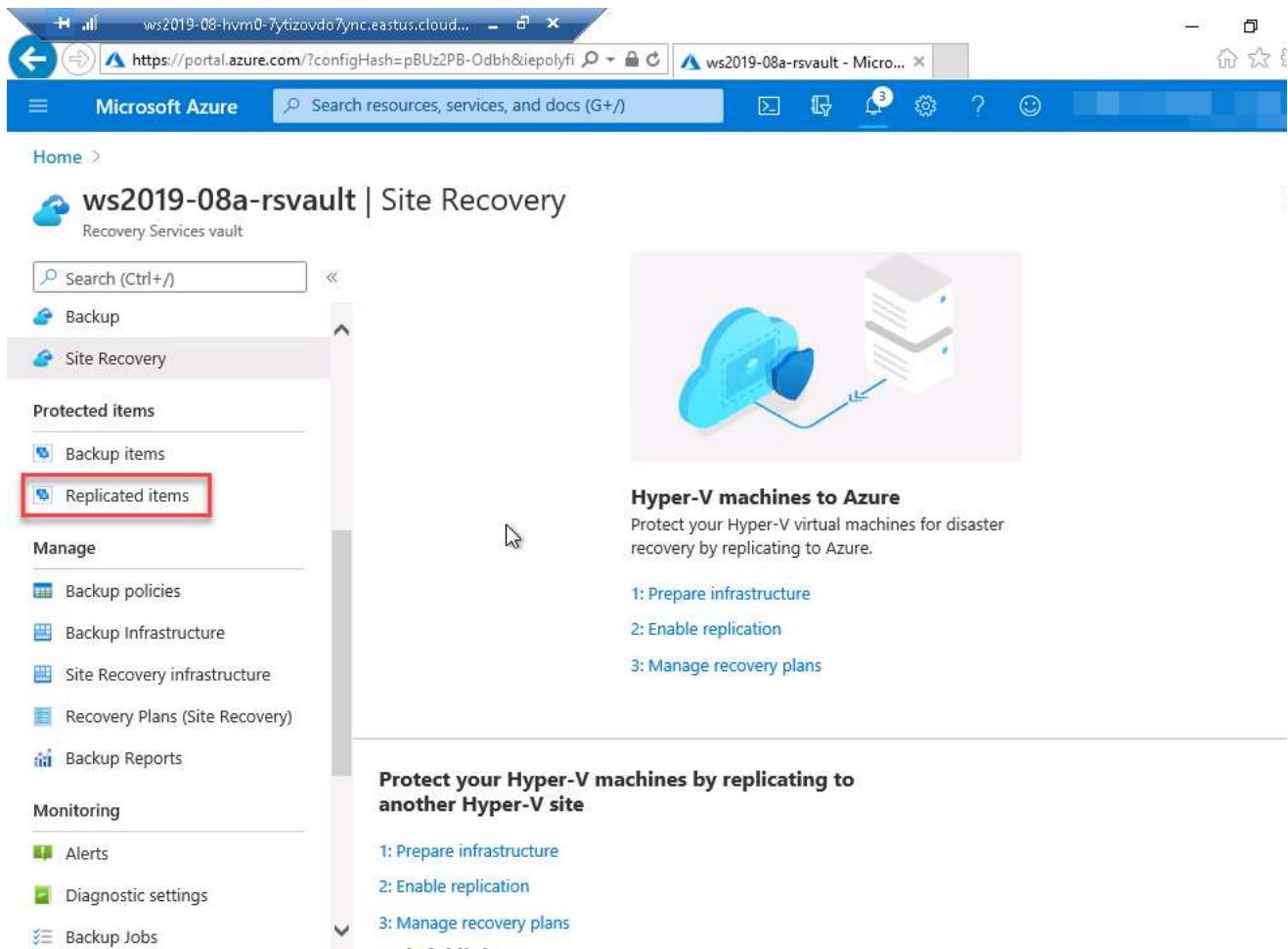
Replication settings and policy

Replication settings	Configured
Replication policy	Replication Policy

Previous Enable replication

Task 3: Review Azure VM replication settings

1. In the Azure portal, back on the **myVault | Site Recovery** blade, in the vertical menu, select **Replicated items**.



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. Below the navigation bar, the page title is "ws2019-08a-rsvault | Site Recovery" under a "Recovery Services vault" section. On the left, there is a vertical sidebar with several sections: "Protected items" (Backup items, Replicated items - highlighted with a red box), "Manage" (Backup policies, Backup Infrastructure, Site Recovery infrastructure, Recovery Plans (Site Recovery), Backup Reports), and "Monitoring" (Alerts, Diagnostic settings, Backup Jobs). To the right of the sidebar, there is a large graphic illustrating a cloud connection to a server. Below the graphic, the heading "Hyper-V machines to Azure" is followed by the subtext "Protect your Hyper-V virtual machines for disaster recovery by replicating to Azure." Underneath this, three steps are listed: "1: Prepare infrastructure", "2: Enable replication", and "3: Manage recovery plans". Further down, another section titled "Protect your Hyper-V machines by replicating to another Hyper-V site" lists the same three steps: "1: Prepare infrastructure", "2: Enable replication", and "3: Manage recovery plans".

2. On the **myVault | Replicated items** blade, ensure that there is an entry representing the **LON-APP1** virtual machine and verify that its **Replication Health** is listed as **Healthy** and that its **Status** is listed as either **Enabling protection**, **Waiting for first recovery point**, or displaying a current percentage of synchronization progress.

⚠ Note: You might need to wait a few minutes until the **LON-APP1** entry appears on the **myVault | Replicated items** blade.

3. On the **myVault | Replicated items** blade, select the **LON-APP1** entry.

4. On the **LON-APP1** replicated items blade, review the **Health and status**, **Failover readiness**, **Latest recovery points**, and **Infrastructure view** sections. Note the **Planned Failover**, **Failover** and **Test Failover** toolbar icons.

⚠ Note: Wait until the status changes to **Protected**. This might take additional 15-20 minutes. You will need to refresh the browser page for the status to be updated.

myVault | Replicated items

Recovery Services vault

Search (Ctrl+ /)

Refresh Replicate Columns Filter

You can run your machines on managed disks after a failover or migration from on-premises to Azure. Set the option to use managed disks in Replicated item -> Settings -> Compute and Network.

Last refreshed at: 9/22/2020 9:37:29 AM

Finished loading data from service.

Filter items...

Name	Replication Health	Status	Active location
LON-APP1	Healthy	Initial replication is in pro...	On Prem Site

- 5. On the **LON-APP1** replicated items blade, select **Latest recovery points** and review **Latest crash-consistent** and **Latest app-consistent** recovery points.
- 6. On [LON-HV1](#), in the browser window displaying the Azure portal, on the **LON-APP1** replicated items blade click **Compute and Network**.
- 7. Click **Edit** then change the VM size to **D2s_v3** and click **Save**.

Task 4: Failover to Azure

- 1. In **Protected items > Replicated items**, click **LON-APP1 > Failover**.

LON-APP1

Replicated items

Planned Failover Failover Test Failover Cleanup test failover Commit ...

Overview

General Properties Compute and Network Disks

Health and status

Replication: Healthy Health: Last successful Test Failover: Never

Status: Protected Configuration issues: No issues

RPO: 3 secs [As on 6/7/2020 9:19:42 AM]

Errors(0) Open in new page Events - Last 72 hours(0) Open in new page

No errors No events

Latest recovery points: Click above to see the latest recovery points.

2. Click **I understand the risk. Skip test failover** check box.

Note: In a real world environment you would test the failover to ensure it would be success in the event of a disaster.

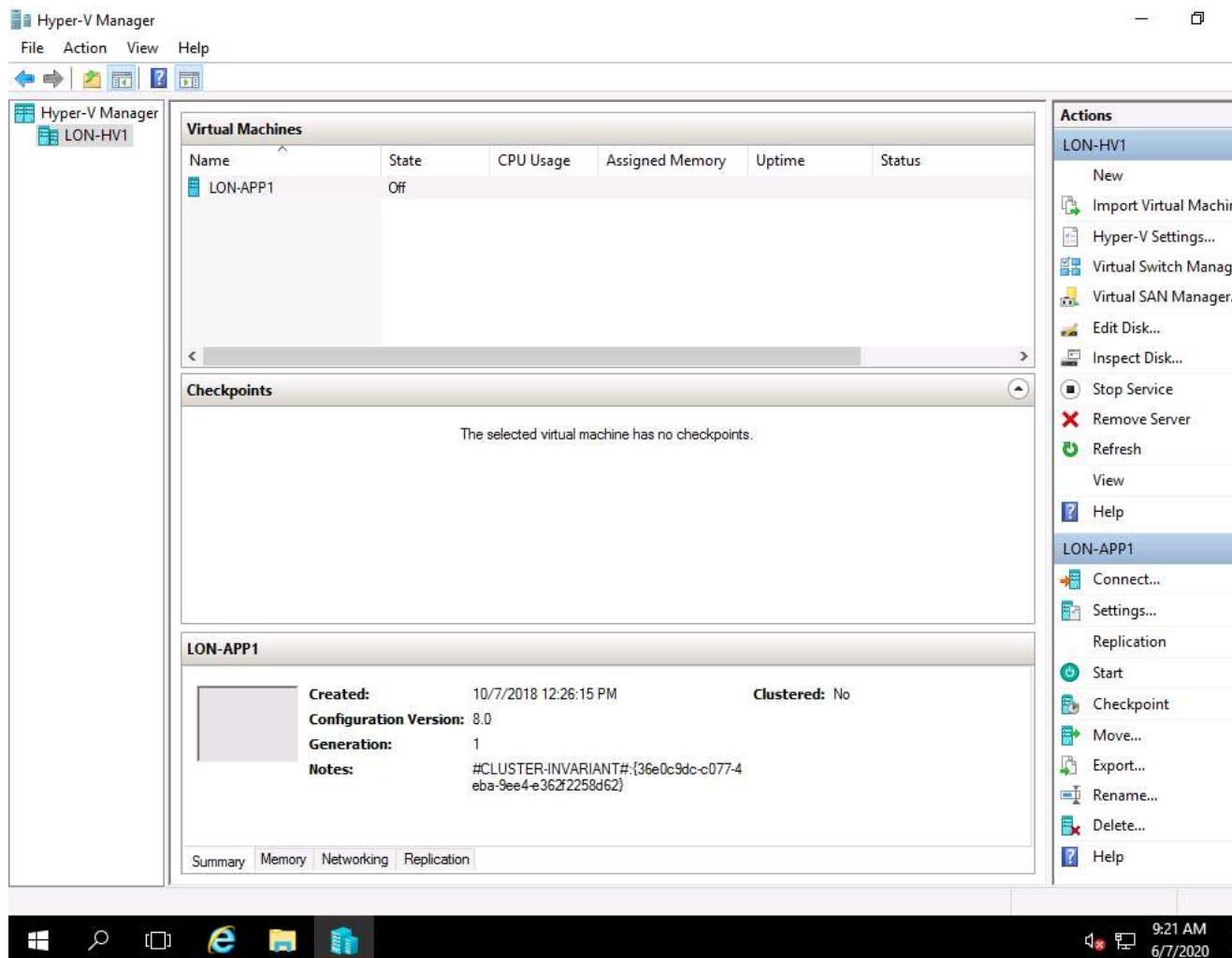
3. In **Failover**, select the **Latest processed (low RTO)** recovery point.

4. Select **Shutdown machine before beginning failover** and click **OK**.

Note: Site Recovery attempts to do a shutdown of source VMs before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.

Note: Never cancel a **Failover in progress**: If you cancel in progress, failover stops, but the VM won't replicate again.

5. Open Hyper-V manager and after a short period you will see the virtual machine is shutdown.



Task 5: Verify the failover to Azure

1. In the **Azure Portal** click **Virtual Machines** and select **LON-APP1**.

Screenshot of the Microsoft Azure portal showing the Virtual machines page. The URL is https://portal.azure.com/?configHash=zP1X7l2ngtNT&iepolyfill:. The page title is Virtual machines - Microsoft Azure. The top navigation bar includes Microsoft Azure, a search bar, and various icons. The main content area shows a table of virtual machines. The first row, which contains the entry LON-APP1, is highlighted with a red border.

Name	Type	Status	Resource group	Location	Source
LON-APP1	Virtual machine	Running	myRG	East US	Disk

2. On the overview blade note that the Virtual Machine is running.

9:24 AM
6/7/2020

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with icons for back, forward, search, and account information. Below it, the main header reads "Microsoft Azure" and "LON-APP1 - Microsoft Azure". A search bar says "Search resources, services, and docs (G+)".

The main content area displays the "Overview" tab for the virtual machine "LON-APP1". On the left, a sidebar lists other tabs like Activity log, Access control (IAM), Tags, and Settings. Under Settings, Networking is selected. The main pane shows the following details:

Setting	Value
Resource group (change)	myRG
Status	Running
Location	East US
Subscription (change)	CS-SUB-1452
Subscription ID	b336c065-f175-43a2-a4f0-6124626bba96
Computer name (not available)	
Operating system	Windows
Size	Standard B1s (1 vcpus, 1 GiB memory)
Tags (change)	Click here to add tags

A red box highlights the "Status" field, which is set to "Running".

At the bottom, there's a taskbar with various icons and a clock showing "9:24 AM" and the date "6/7/2020".

3. Click Networking. Notice that the Virtual Machine now has an IP Address from the Virtual Network you created in an earlier task.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with icons for back, forward, search, and account information. Below the navigation bar, the main header reads "LON-APP1 | Networking". On the left side, there is a sidebar titled "Settings" with several options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Networking (which is highlighted with a red box), Connect, Disks, Size, Security, Advisor recommendations, Extensions, Continuous delivery, and Availability + scaling.

The main content area is titled "IP configuration" and shows an IP configuration named "ipConfigLON-APP1cc9f3114-f05b-45ec-acd5-b52cc2319b7d". It displays the following details:

- Virtual network/subnet: myVNet/default
- NIC Public IP: -
- NIC Private IP: **10.0.0.4**
- Accelerated networking: **Disabled**

Below this, there are tabs for "Inbound port rules", "Outbound port rules", "Application security groups", and "Load balancing". A note states: "This network interface does not contain network security groups".

At the bottom right of the screen, there is a taskbar with icons for Start, Search, Task View, Edge browser, File Explorer, and File History. The date and time are shown as 9:25 AM, 6/7/2020.

4. Click on the **Network Interface**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the URL <https://portal.azure.com/?configHash=zP1X7l2ngtNT&iepolyfill:>, a search bar, and various account and service icons. The main title is "LON-APP1 | Networking".

The left sidebar has a "Search (Ctrl+/" input field and a list of navigation items: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings. Under Settings, "Networking" is selected and highlighted.

The main content area displays the "IP configuration" section for "ipConfigLON-APP1cc9f3114-f05b-45ec-acd5-b52cc2319b7d". It shows the "Topology" tab selected, with the network interface name "LON-APP1cc9f3114-f05b-45ec-acd5-b52cc2319b7d" highlighted with a red box. Below it, the "Effective security rules" section is visible.

Below the IP configuration, there are tabs for Inbound port rules, Outbound port rules, Application security groups, and Load balancing. A note states: "This network interface does not contain network security groups".

The bottom right corner of the screen shows the Windows taskbar with icons for Start, Search, Task View, Edge browser, File Explorer, and File History, along with the system tray showing the date and time (9:25 AM, 6/7/2020).

5. Click **IP Configurations**.

Screenshot of the Microsoft Azure portal showing the IP configurations for a virtual machine.

The URL in the address bar is <https://portal.azure.com/?configHash=zP1X7l2ngtNT&iepolyfill:>

The page title is LON-APP1cc9f3114-f05b-45ec-acd5-b52cc2319b7d | IP configurations

The left sidebar shows the following navigation items:

- Overview
- Activity log
- Access control (IAM)
- Tags
- IP configurations** (selected and highlighted with a red box)
- DNS servers
- Network security group
- Properties
- Locks
- Export template

The main content area displays the following settings:

- IP forwarding settings:
 - IP forwarding: **Disabled** (button)
- Virtual network: myVNet
- IP configurations:
 - Subnet: default (10.0.0.0/24)
 - Search IP configurations
 - Table of IP configurations:

Name	IP Version	Type	Private IP address
ipConfigLON-APP1c...	IPv4	Primary	10.0.0.4 (Dynamic)

The bottom right corner shows the system tray with the date and time: 9:25 AM 6/7/2020.

6. Click on ipConfig1.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various navigation icons. The main content area displays the details for a network interface named "LON-APP1cc9f3114-f05b-45ec-acd5-b52cc2319b7d". On the left, a sidebar menu is open under the "Settings" section, with "IP configurations" selected. The main panel shows "IP forwarding settings" with "IP forwarding" set to "Disabled". It also displays the "Virtual network" as "myVNet". Under "IP configurations", there is a table with one row:

Name	IP Version	Type	Private IP address
ipConfigLON-APP1c...	IPv4	Primary	10.0.0.4 (Dynamic)

A red box highlights the "Name" column of the first row in the table.

7. On the Public IP Address click **Associate** and then click **Create New** and Enter a name for your public IP Address. Click **Ok**. This will create a new Public IP and allocated it to the Network Interface of the Virtual Machine.

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is <https://portal.azure.com/?configHash=zP1X7l2ngtNT&iepolyfill:>. The page title is "ipConfigLON-APP1cc9f3114-f05b-45ec-a...". The main content area displays "Public IP address settings". Under "Public IP address", there is a "Disassociate" button and an "Associate" button, with the "Associate" button highlighted by a red box. Below it is a section labeled "IP address" with the text "Configure required settings" and a red box around it. Other sections visible include "Private IP address settings", "Virtual network/subnet" (set to "myVNet/default"), and "Assignment" (set to "Dynamic"). The IP address is listed as "10.0.0.4". At the bottom right of the portal window, there is a timestamp "9:26 AM" and a date "6/7/2020".

- 8. Click **Save** and wait for the deployment to complete.
- 9. Navigate back to the **Virtual Machine** blade and notice the Virtual Machine now as a Public IP Address.

The screenshot shows the Microsoft Azure portal interface. At the top, the URL is https://portal.azure.com/?configHash=zP1X7l2ngtNT&iepolyfill: and the title bar says LON-APP1 - Microsoft Azure. The main navigation bar includes Home, Virtual machines, and a search bar. Below the navigation, the virtual machine name LON-APP1 is displayed with a blue icon and the status 'Virtual machine'. A toolbar with actions like Connect, Start, Restart, Stop, Move, Delete, and Refresh is visible. On the left, a sidebar menu lists Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings (Networking, Connect, Disks, Size, Security, Advisor recommendations, Extensions, Continuous delivery, Availability + scaling). The main content area displays the VM details. Key information includes:

Setting	Value
Resource group (change)	myRG
Status	Running
Location	East US
Subscription (change)	CS-SUB-1452
Subscription ID	b336c065-f175-43a2-a4f0-6124626bba96
Computer name (not available)	
Operating system	Windows
Size	Standard B1s (1 vcpus, 1 GiB memory)
Tags (change)	Click here to add tags
Public IP address	52.188.58.141
Private IP address	10.0.0.4
Public IP address (IPv6)	-
Private IP address (IPv6)	-
Virtual network/subnet	myVNet/default
DNS name	Configure

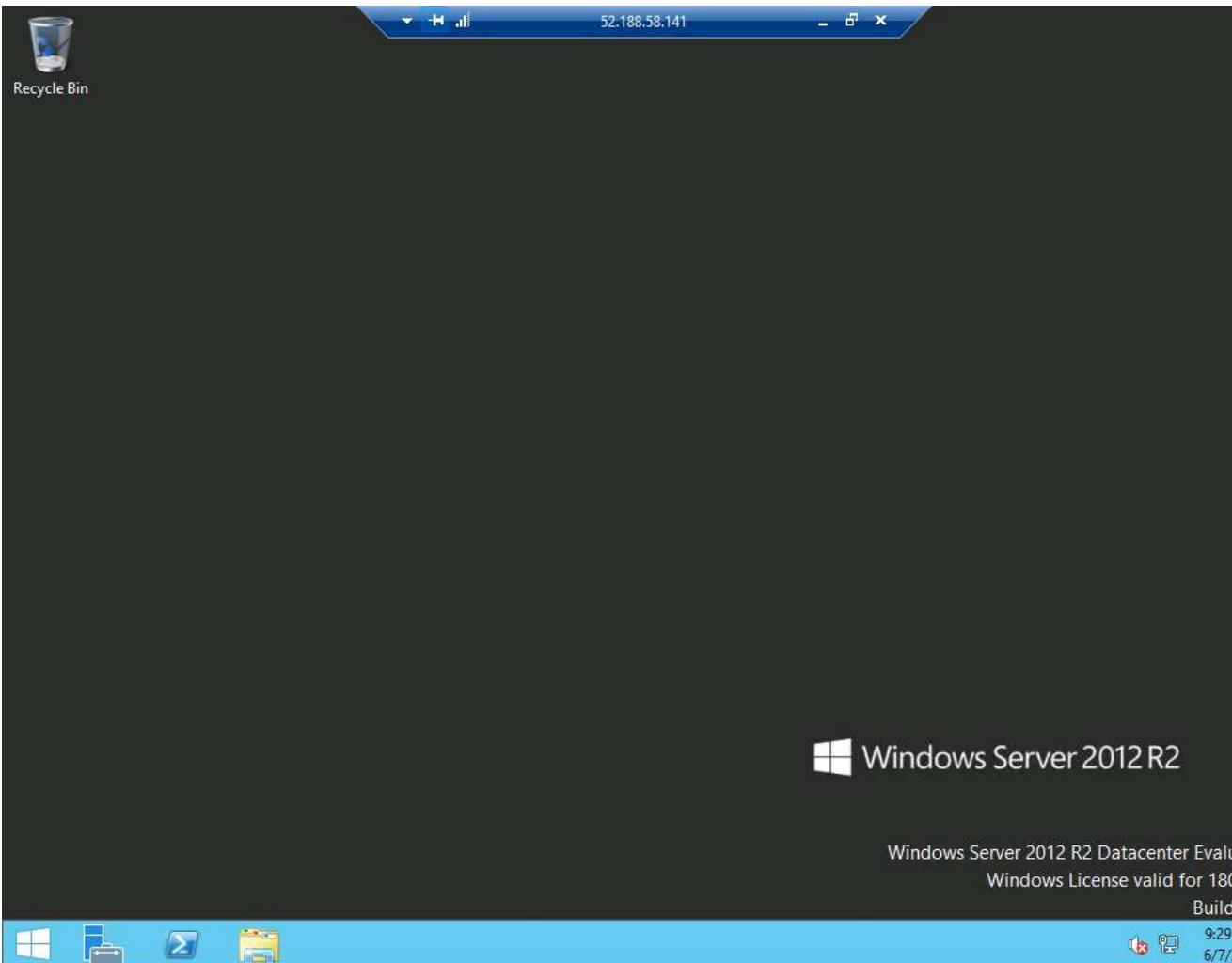
A red box highlights the 'Public IP address' field, which contains the value 52.188.58.141.

10. Click **Connect** > **RDP** and download and open the RDP file and click Connect.

11. Login with the following credentials:

- **Username:** [.\administrator](#)

- **Password:** [Pa55w.rd](#)



- 1. Exit the Virtual Machine RDP connection.
- 2. Navigate back to your **Recovery Services vault** > **Replicated Items**
- 3. Click ...**More** and click **Commit** and then click **OK**. It deletes all the available recovery points.

The screenshot shows the Microsoft Azure portal interface for a Recovery Services vault named "myVault". The left sidebar lists "Protected items" with "Replicated items" selected. The main content area displays a table of replicated items, showing one item named "LON-APP1" with a status of "Failover completed". A context menu is open on the right side, with the "Commit" option highlighted by a red box. The status bar at the bottom indicates the date and time as "6/7/2020 9:31:06 AM".

myVault | Replicated items

Recovery Services vault

Search (Ctrl+ /)

Refresh Replicate Columns Filter

Locks Export template

Last refreshed at: 6/7/2020 9:31:06 AM

Finished loading data from service.

Filter items...

Name	Replication Health	Status
LON-APP1	-	Failover completed

Manage

- Backup policies
- Backup Infrastructure
- Site Recovery infrastructure
- Recovery Plans (Site Recovery)
- Backup Reports

9:31 AM
6/7/2020

4. Click ...**More** and then click **Complete Migration** then click **OK**.

The screenshot shows the Microsoft Azure portal interface. The left sidebar lists various services: Create a resource, All services, Favorites, Dashboard, All resources, Resource groups, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and Cost Management + Bill... The main content area displays the 'myVault - Replicated items' blade for 'LON-APP2'. The 'Failover' tab is active. On the right, there's a 'Planned Failover' section with tabs for 'Planned Failover', 'Failover', and 'Test Failover'. Below it is an 'Essentials' summary table with columns for 'Health and status' and 'Failover readiness'. The 'Status' row shows 'Failover committed' and 'Last successful Test Failover'. The 'RPO' row shows '-'. Under 'Configuration issues', there's a green checkmark and 'No issues'. At the bottom, there are sections for 'Errors(0)' and 'Events'. The 'Events' section has tabs for 'TIME' and 'EVENT NAME - SEVERITY'. A red box highlights the 'Complete Migration' button in the 'Events' section.

5. Wait for the commit task to complete.

Task 6: Clean up the environment.

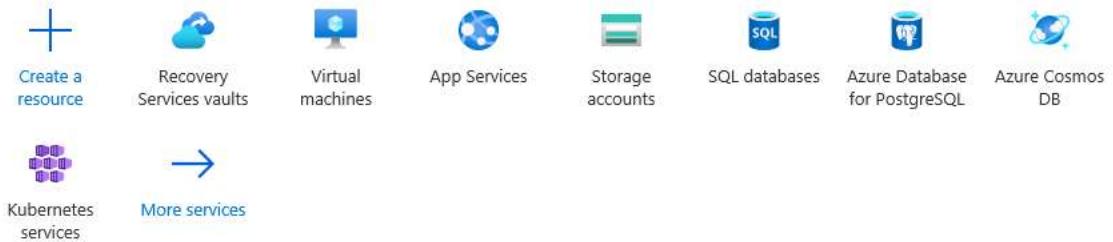
1. Open the Cloud Shell PowerShell and type the following command:

```
$vault = Get-AzRecoveryServicesVault -Name "myVault"
```

```
Remove-AzRecoveryServicesVault -Vault $vault
```

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a navigation bar with back, forward, and search icons. The URL is https://portal.azure.com/?configHash=zP1X7l2ngtNT&iepolyfill:. Below the URL is the title "Microsoft Azure" and a search bar with the placeholder "Search resources, services, and docs (G+/-)". To the right of the search bar are several icons: a gear, a question mark, a smiley face, and a refresh symbol. A notification badge with the number "3" is also visible. On the far right, there's a link to "Test_StudentDWWXB@..." and "GO DEPLOY (CLOUD SHARE (SUB...))".

Azure services



Recent resources

The screenshot shows the Azure Cloud Shell interface. It features a terminal window with a dark background and light-colored text. The terminal output includes:

```
PowerShell | ⚡ ? ⚙️ { } ⚡
Connecting terminal...
Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

MOTD: Switch to Bash from PowerShell: bash

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/test_studentdwwxb: $vault = Get-AzRecoveryServicesVault -Name "myVault"
PS /home/test_studentdwwxb: Remove-AzRecoveryServicesVault -Vault $vault
```

A red rectangular box highlights the command "Remove-AzRecoveryServicesVault -Vault \$vault".

2. Close the Cloud Shell and delete any remaining Resource Groups from the Azure Portal.

✓ **Results** : You have now completed this lab.