



Design Site Recovery and Migration Using Azure Site Recovery (ASR)



Hands-on lab

Azure Site Recovery (ASR) is a service that enables organizations to protect their on-premises physical services and virtual machines. ASR automates the replication of on-premises physical servers and virtual machines to Azure datacenters or to secondary datacenters, such as a disaster recovery site, controlled by the respective organizations. ASR may even be used to replicate virtual machines from one Azure region to another, thereby enabling a migration scenarios for those organizations who wish to move their Azure virtual machines from one region to another.

In this lab, you will learn how to configure ASR to protect an on-premises machine.

Produced by HynesITe, Inc
Version 1.0
10/2/2015



This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. 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, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright 2014 © Microsoft Corporation. All rights reserved.

Microsoft Active Directory, Azure Active Directory, Azure, Hyper-V, Windows, and Windows Server 2012 are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

Contents	3
Design Site Recovery and Migration Using Azure Site Recovery.....	5
Deployment Types	5
Before You Begin.....	6
Cleanup Script	6
Azure Pass.....	6
Hosted Workstations	7
Use of Own System	7
GitHub repository for Lab Files.....	8
Required Software	8
Minimum Microsoft Azure module version	8
Access the Lab Environment	9
Introduction and Scenario	10
Prepare the Azure Infrastructure	11
Run Lab04Start setup script.....	11
Create ASR Target Resources	13
Create Azure Recovery Services vault.....	13
Create and Configure a Configuration Server	14
Create and Configure a Master Target Server.....	23
Configure ASR Source Resources	27
Create and Configure the Process Server	27
Update ASR Servers.....	35
Update configuration server	35
Determine if update is required for process server	37
Determine if update is required for master target server.....	38
Configure Protection for Servers.....	40
Configure source server	40
Create a protection group.....	42
Add a Machine to a Protection Group	43
Modify Protection Group Properties.....	47
Create a Recovery Plan.....	48

Design Site Recovery and Migration Using Azure Site Recovery

Perform an unplanned failover.....	49
Clean up Azure resources used in the lab	53
Delete ASR service.....	53
Run Lab04Cleanup.ps1 to remove remaining Azure resources	54

Design Site Recovery and Migration Using Azure Site Recovery

Azure Site Recovery (ASR) is a service that enables organizations to protect their on-premises physical services and virtual machines. ASR automates the replication of on-premises physical servers and virtual machines to Azure datacenters or to secondary datacenters, such as a disaster recovery site, controlled by the respective organizations. ASR may even be used to replicate virtual machines from one Azure region to another, thereby enabling a migration scenario for those organizations who wish to move their Azure virtual machines from one region to another.

Primarily, ASR enables—or contributes to pre-existing—business continuity and disaster recovery (BCDR) solutions for organizations that need to be able to continue operations and to recover IT services quickly after a significant event, such as a natural disaster (fire, hurricane, tornado, earthquake, etc.) or other calamitous event, has damaged or harmed their IT infrastructure and compromised the availability and integrity of their data and services.

Deployment Types

ASR provides near-synchronous continuous backup replication with recovery point objectives (RPO) as low as 30 seconds. This enables protection of most critical applications and workloads located on on-premises physical servers or virtual machines. The following lists the supported deployment scenarios:

- **Hyper-V site to Azure:** replicate VMs located on one or more Hyper-V servers to Azure (no VMM required)
- **VMMServer to Azure:** replicate VMs from Hyper-V host servers located in a VMM private cloud to host servers to Azure.
- **Physical server to Azure:** replicate a physical Windows or Linux server to Azure—this deployment type also enables migration of VMs from one Azure region to another and is the focus of the lab exercises that follow.
- **VMWare VMs to Azure:** replicate VMWare virtual machines to Azure.
- **VMM Server to secondary datacenter:** Replicate VMs from Hyper-V host server located in a VMM private cloud to secondary VMM servers in a secondary datacenter, such as a disaster recovery (DR) site.
- **VMM Server with SAN:** Replicate virtual machines from Hyper-V servers in a VMM cloud to a secondary VMM server using SAN replication.
- **Single VMM server to secondary datacenter:** Replicate virtual machines from an on-premises Hyper-V host servers in a VMM private cloud to a secondary cloud on the same VMM server.

Before You Begin

This lab relies almost exclusively on lab resources that you create exclusively in an Azure subscription. The virtual machine requirements for configuring Azure Site Recovery exceed the limits of Free Trial subscriptions, which are limited to 4 cores. For this reason, if you are using an Azure Free Trial account, you may not be able to do this lab because the Azure Virtual Machines that are required for this lab, consume 12 cores. Azure Free Trial accounts are limited to a maximum of 4 cores. You must, therefore, acquire an Azure Pass using a promo code or you must use an MSDN or an Enterprise account.

- ❖ If you are using an Azure pass, please ensure you have sufficient credit in your account. When lab resources are fully deployed, the current cost is approximately \$15.00 - \$20.00 per day.

Cleanup Script

The cleanup script for this lab attempts to delete as much as it can in the Azure subscription you run the script against.

- ❖ The cleanup script does NOT discriminate between resources created for the lab and other resource that may exist in your subscription — including production resources. It will delete both lab and other, possibly important, resources in your subscription.

If you are using your own subscription, you should not use the provided cleanup script. Rather, you should manually delete the resources created in this lab using the portal UI (both the preview and the full portal).

Azure Pass

This IT Camp lab requires a valid Azure subscription. While you may use an existing subscription such as a subscription associated MSDN account or existing corporate account, it is strongly recommended to use an Azure Pass. By using an Azure Pass, you will avoid any charges against your MSDN or corporate subscription that would result from doing the exercises in this camp. Perhaps more importantly, the cleanup script for this lab is aggressive and will attempt to delete everything in the subscription. Using an Azure Pass will ensure that the cleanup script, *if used properly*, will not delete important data in your other Azure subscriptions. If you do not have access to an Azure Pass, you will likely want to delete the Azure resources created in the lab exercises manually.

Your instructor may be able to provide you with a pre-provisioned Microsoft Account that already has an Azure Pass subscription associated with it. Alternatively, your instructor may be able to provide you with an Azure promotional code.

To activate the promotional code and create a new Azure Pass account perform the following steps.

1. If you are not using the lab virtual machine to activate your Azure Pass promotional code, ensure you open an InPrivate browser session before performing these steps.
 - ❖ It is critically important that you do not accidentally associate the promotional code with any account that has previously been associated with or linked to an Azure subscription. Use an InPrivate browser

session to ensure that no credentials are unintentionally forwarded during the process to activate and redeem the promotional code. If you fail to activate the code because you logged in with the wrong account, you will render the code useless and will not be able to use it again.

2. Navigate to www.live.com and click **Sign up now**.
3. Follow the on-screen instructions to create a new Microsoft Account.
 - ✦ Please ensure, you create an outlook.com, live.com or Hotmail.com account. Do not use accounts that have country code suffixes, such as .dk, ca, uk, etc. in their names.
4. Navigate to <http://www.microsoftazurepass.com> and follow the onscreen instructions to redeem the promotional code.
 - ✦ Once you have submitted the promotional code, it will take a few minutes for the account to become activated. Only one promo code can be redeemed per the life of the Microsoft ID.
5. Follow the on-screen instructions to activate a new Windows Azure Trial.
6. Navigate to Manage.windowsazure.com and sign in.
7. In Microsoft Azure portal, in the upper left, click your user name, and then click **View my bill**.
8. Click your current trial subscription, and then click **Edit subscription details**.
9. Type a name you will recognize in SUBSCRIPTION NAME, such as ITCamps, and then click the **Done** icon.

Hosted Workstations

This particular lab does not require the use of a hosted lab environment, as long as personal workstation has the most recent version of the Microsoft Azure PowerShell module installed and you have access to the lab files on GitHub. Other labs in this camp are written to be completed on a pre-configured workstation, because, for example, the lab requires an on-premises environment consisting of multiple servers. For this and these other labs, a hosted lab environment is available to you. Your instructor will provide a link to this environment.

If you are using the hosted workstation environment, use **Administrator** as the username and **Passw0rd!** as the password.

Use of Own System

You may complete lab instructions using your own workstation (either Windows 10 or Windows 8.1), providing you download the appropriate files used for the lab from GitHub and have the following software installed.

GitHub repository for Lab Files

If you are not using the hosted virtual machine and are using your own workstation, any custom files the lab instruction call out can be found in a GitHub repository. The repository is located here:

<https://github.com/AZITCAMP/Labfiles>.

Required Software

1. Microsoft Azure PowerShell - <http://go.microsoft.com/?linkid=9811175&clid=0x409> (also installs the Web Platform Installer)
2. Visual Studio Code - <https://code.visualstudio.com/>

Minimum Microsoft Azure module version

Please note that these lab exercises require a minimum version of 0.9.8 of the Microsoft Azure module for PowerShell. To determine the module version installed on your system, open a Windows PowerShell prompt, type the following commands, and then press ENTER.

```
↪ import-module Azure  
↪ get-module Azure).version
```

```
PS C:\> import-module azure  
PS C:\> (get-module Azure).Version  
  
Major  Minor  Build  Revision  
-----  
0      9      8      -1
```


Access the Lab Environment

For this lab, you may be accessing a hosted environment that contains all the VMs and resources you require. Your instructor will provide you with a link to this environment.

You should be able to connect with any recent web browser, including Microsoft Edge. Once you have connected to the lab environment, take a few minutes to familiarize yourself with Launchpad.

For this course there are four VMs that you will work in. If you look at the Machines tab on the right side of the lab environment you will find a listing of all the VMs. To switch to another VM, just click on the appropriate name in the Machines list. Below you will find a listing of the VMs for this course.

Virtual Machine	Role
AZRCamp-Admin	Windows 10. A member of the Contoso.com domain. Used for Azure management.
AZRCamp-Edge	A Stand-alone Windows Server 2012 R2 Server. Routing and Remote Access has been installed and it is acting as the default gateway for all outbound traffic.
AZRCamp-DC	Windows Server 2012 R2 domain controller and DNS server.
AZRCamp-Sync	Directory Sync for use in other Labs.

The password for all logons in these VMs is "Passw0rd!".

- ✦ You can type this in to the VM manually, or use the **Commands→Paste→Paste Password** sequence from the Launchpad.
- ✦ Please note, for this lab, if you are using the hosted in environment, you will perform all the tasks on the AZRCamp-Admin virtual machine.

Introduction and Scenario

As a Contoso fabric administrator, you are asked to determine how best to enable protection for various applications within the Contoso datacenters. In its datacenters, Contoso is running a number of non-virtualized workloads (Physical machines), along with a number of virtualized workloads using both Hyper-V and VMware stacks. Since you have different SLAs for different applications, you plan to protect them differently. Additionally, Contoso has Azure resources that have been identified for migration to another Azure region. Management has identified that protection of non-virtualized workloads is a priority.

Prepare the Azure Infrastructure

This lab serves a dual purpose: 1) to demonstrate how to protect on-premises physical servers and 2) to demonstrate how to migrate Azure VMs from one region to another using ASR. The reason this lab can meet this dual purpose is that the steps for configuring the source resources you wish to protect and the target resources are almost identical.

All the resources you require for this lab, with the exception of a workstation to run a PowerShell script, are configured in Azure.

In this lab exercise, you will configure the source and target resources required to complete the lab steps. These resources include storage accounts, virtual networks, and virtual machines.

Run Lab04Start setup script

To perform the subsequent lab exercises, you need to create two virtual machines that act as the ASR process server and the source server you want to protect. These resources are created by running a Windows PowerShell script. In this task, you will run the Lab04Start.ps1 script to configure the Azure infrastructure with resources needed for this lab.

⚠ Please only use the Windows PowerShell to setup the lab environment.

✎ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password.

1. Open **File Explorer** and navigate to **C:\LabFiles\AZRITPROCamp\Lab04 – Design Azure Site Recovery solution**.

✎ You may also download files used for this lab from the GitHub repository for the course at <https://github.com/AZITCAMP/Labfiles>.

2. Right-click **Lab04Start.ps1**, and click **Edit**.

✎ The Windows PowerShell ISE console opens.

3. In Windows PowerShell ISE, on the upper Ribbon, click **Run Script** (green arrow).

4. When prompted, enter a lower-case string that represents your initials, and press ENTER.

✎ Your initials are used to create unique names for the Azure storage account.

5. In the Sign in to Windows Azure PowerShell dialog box, enter the email address of the account associated with your Azure subscription, and click **Continue**.

6. On the sign in page, enter your password, and click **Sign in**.

✎ The script starts running and then creates the storage account, virtual network, and resource group that will be used for the lab.

7. When prompted for the Admin Password parameter, type **Passw0rd!** and press ENTER.

8. At this point, the virtual machines and other resources are provisioned in the East US location. The script will take approximately 10 – 20 minutes to complete.
9. Leave the Windows PowerShell ISE console open for subsequent lab exercises.

Create ASR Target Resources

The ASR target resources include the following:

- **Site Recovery Vault:** Vault for securely storing sensitive configuration information.
- **Configuration Server:** The ASR management server setup in the Azure subscription that acts as command and control for all operations. This is the first server that will be deployed after configuring the Site Recovery Vault. This server is registered with the Site Recovery vault.
- **Master Target Server:** The server which stores and writes all the replicated data. This server is registered with a CONFIGURATION SERVER during setup.

In this lab exercise, you will configure these target resources using the full management portal.

✦ At the time of this writing ASR is not available using the Resource Manager model.

Create Azure Recovery Services vault

The site recovery vault is the first resource that must be created to configure ASR. The vault serves as a secure repository for sensitive configuration information.

In this task, you will create a site recovery vault.

✎ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

1. Open Microsoft Edge, and browse to <https://manage.windowsazure.com> and log on with your subscription.

✦ At the time of this writing, you can configure the vault using only the full management portal.

2. In the left navigation, scroll down, and click **RECOVERY SERVICES**.
3. On the recovery services page, click **CREATE A NEW VAULT**.
4. On the NEW page, click **SITE RECOVERY VAULT**, and then click **QUICK CREATE**.
5. In NAME, type **ASRVault**.
6. In REGION, select **East US 2**.

⚠ Do not select any region other than East US 2.

✦ The setup script for this lab created a virtual network in East US 2 for the purposes of the lab. The configuration server and master target server need to be placed in the same VNET; additionally, the storage account used by the ASR components must be in the same region as well.



7. Click **CREATE VAULT**.
8. Leave the Azure Portal open for the next task.

Create and Configure a Configuration Server

The configuration server is used for managing ASR.

In this task, you will create the Configuration Server and then register it in the ASR vault.

 Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

1. On the recovery services page, click **ASRVault**.
2. If the BEFORE YOU START page appears, close it.
 - ❖ The BEFORE YOU START page may reappear periodically throughout the lab. If it does, close it to continue.
3. On the asrvault page, ensure that SETUP RECOVERY is set to **Between an on-premises site with VMware/physical servers and Azure**.
4. Under Prepare Target (Azure) Resources, click **Deploy Configuration Server**.
5. On the New Configuration Server details page, enter the following information and then click **Done** (check mark).
 - CONFIGURATION SERVER NAME: **ConfigSrv**
 - NEW USER NAME :**ltcampadmin**
 - PASSWORD: **Passw0rd!**
 - NETWORK CONNECTIVITY TYPE: **Public Internet**
 - MICROSOFT AZURE NETWORK: **Lab04-T-VNET**
 - SUBNET: **ASRsubnet**
 - IPADDRESS: **10.0.0.100**

New Configuration Server Details

To replicate virtual machines and physical machines into Azure, you need to deploy a Configuration Server in your Azure subscription which will manage replication configuration. A Configuration Server will now be deployed in a new cloud service using an Azure virtual machine gallery image.

CONFIGURATION SERVER NAME

NEW USER NAME

PASSWORD

CONFIRM

NETWORK CONNECTIVITY TYPE ?

MICROSOFT AZURE NETWORK

SUBNET

IP ADDRESS



- ✦ The configuration server is deployed to a new cloud service and assigned a reserved public IP address. This ensures that the public IP address of the configuration remains constant across reboots of the server. If you decommission the configuration, you will need to remove the reservation.

- Wait until the server provisioning job completes.
- In the left navigation, click **VIRTUAL MACHINES**.

NAME	STATUS	SUBSCRIPTION	LOCATION
ConfigSrv	Running	Azure Pass	East US 2

- ✦ If you do not see the ConfigSrv virtual machine, you may have to refresh the page.

8. On the virtual machines page, click **ConfigSrv**.
9. On the configsrv page, click **DASHBOARD**.
10. In the quick glance column on the left, identify and record the PUBLIC IP (VIP) ADDRESS.
 - 💡 You will need to know this address in subsequent lab steps to register the master target and process servers.

quick glance

- 🌐 Visit the new portal **PREVIEW**
- 🔒 View Applicable Applications and services
- 🔄 Reset password (new portal)
- 🔄 Reset remote configuration (new portal)
- ℹ️ Learn more about backup and restore **PREVIEW**

STATUS
Running

DNS NAME
configsrv-e53ad32d-0f92-438e-9eb9-6bdc8ce5dfb7.cloudapp.net

HOST NAME
ConfigSrv

PUBLIC VIRTUAL IP (VIP) ADDRESS
104.210.100.100

INTERNAL IP ADDRESS
10.0.0.100

SIZE
Standard_A3 (4 cores, 7 GB memory)

11. On the configsrv page, click **ENDPOINTS**.
12. On the ENDPOINTS tab, identify and record the public port that maps to the HTTPS protocol.
 - 💡 You will need to know this port number for subsequent lab steps. Your port number will differ from the one shown in the screen shot below.
 - 🌟 TIP: put this information in a text file. You will also need to record a passphrase later in this lab. This passphrase should also be recorded in the same text file. You will need the IP address, port number, and passphrase when you configure the process server in subsequent lab steps.

configsrv

[DASHBOARD](#) [MONITOR](#) [ENDPOINTS](#) [CONFIGURE](#)

NAME	↑	PROTOCOL	PUBLIC PORT	PRIVATE PORT
Custom		TCP	9443	9443
HTTPS		TCP	50494	443
Powershell		TCP	58808	5986
Remote Desktop		TCP	55084	3389


13. In the left navigation, click **RECOVERY SERVICES**.

14. On the recovery services page, click **ASRvault**.

15. On the asrvault page, click **Download a registration key**.

asrvault

[DASHBOARD](#) [PROTECTED ITEMS](#) [RECOVERY PLANS](#) [SERVERS](#) [RESOURCES](#) [JOBS](#) [EVENTS](#)



A new Azure Site Recovery vault was created!
Follow these steps to get started.

☐ Skip Quick Start the next time I visit

SETUP RECOVERY Between an on-premises site with VMware/physical servers and Azure

PROTECT

1 Prepare Target(Azure) Resources

After you deploy the Configuration Server, download and copy the registration key file to the Configuration Server. Launch the installer on the Configuration Server and use the key file to register the server to the vault. Generate registration key file creates a new key every time you click on it and only the latest key is valid at any given time. After the Configuration Server has been registered, deploy the Master Target Server. Once deployed, log in into the server and register it to the Configuration Server.

[Deploy Configuration Server](#)
[Download a registration key](#)
[Deploy Master Target Server](#)
[Download and Install additional software \(only for Linux Master Target Server\)](#)

16. When the download prompt appears, save the file in a convenient location for use in a later step.

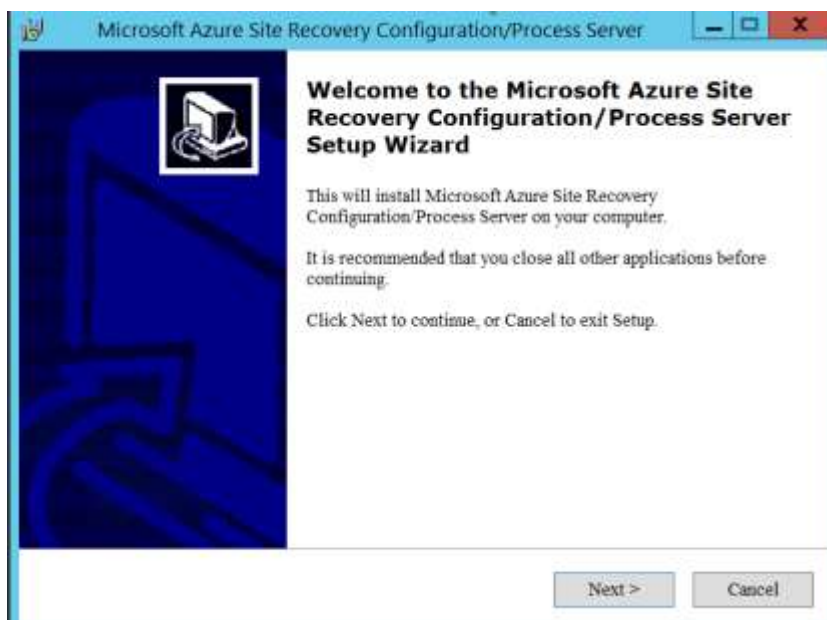
✦ The certificate that is used to register the Configuration Server is valid for 5 days. This is a sensitive file, so it should be protected appropriately.

17. In the left navigation, click **VIRTUAL MACHINES**.

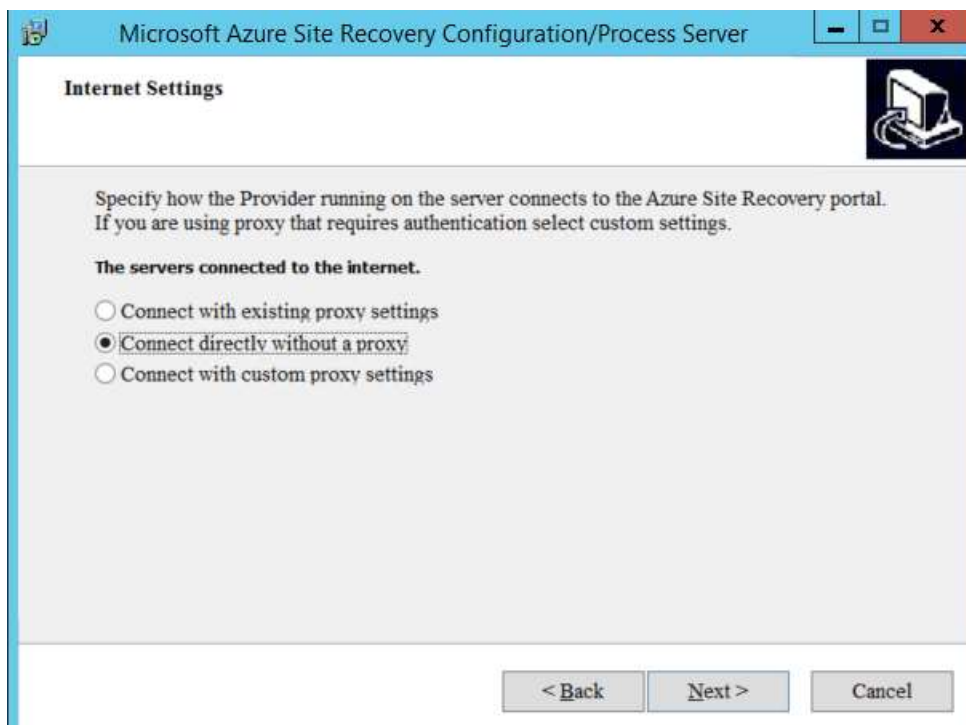
18. On the virtual machines page, ensure ConfigSrv is selected.

19. On the command bar, click **CONNECT**, and then click **Open** when prompted.
20. In the Remote Desktop Connection dialog box, click **Connect**.
21. In the Windows Security dialog box, select **Use another account** and log on using **Itcampadmin** as the user name and **Passw0rd!** as the password.
22. In the Remote Desktop Connection dialog box, click **Yes**.

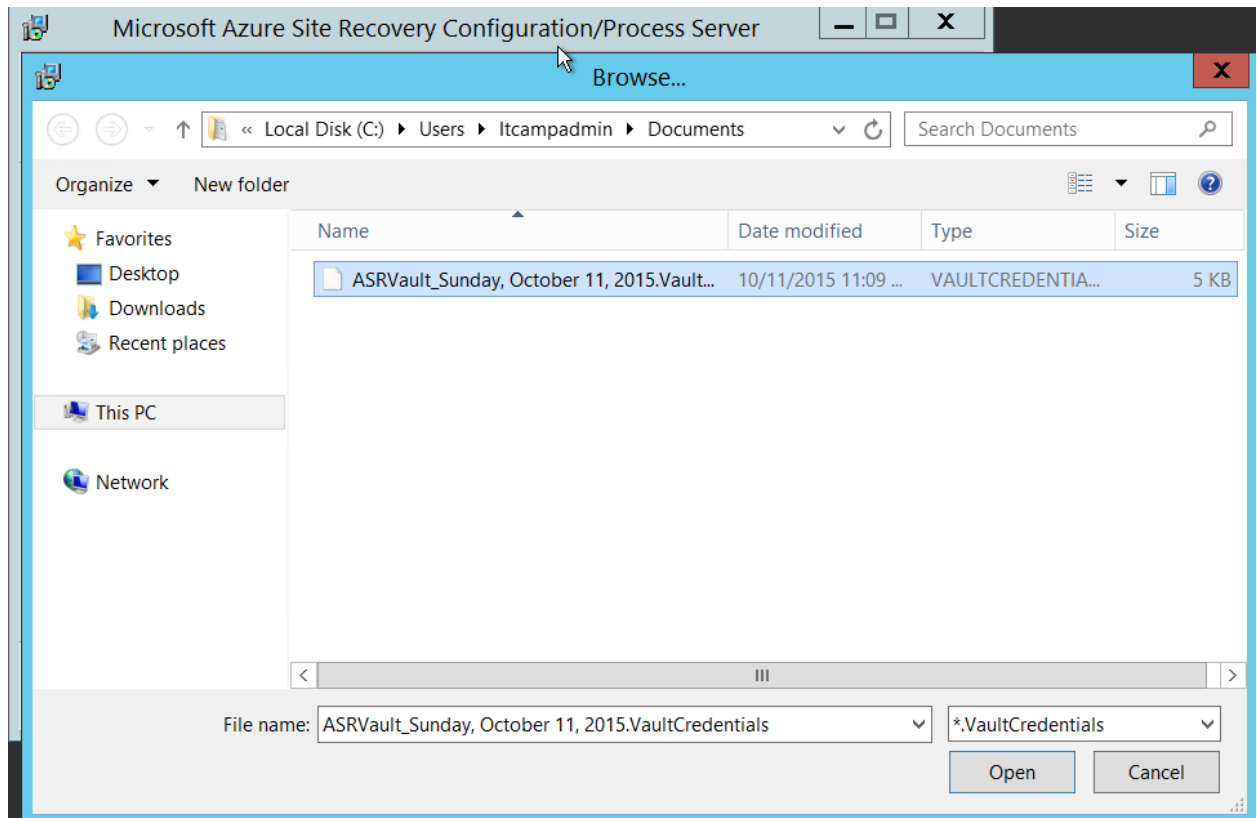
- ✦ You are logged in and the desktop starts loading. After a few moments, the Microsoft Azure Site Recover Configuration/Process Server setup program launches.
- ✦ When the desktop initially loads, you may briefly see a PowerShell Window open. Do not close this the PowerShell windows.



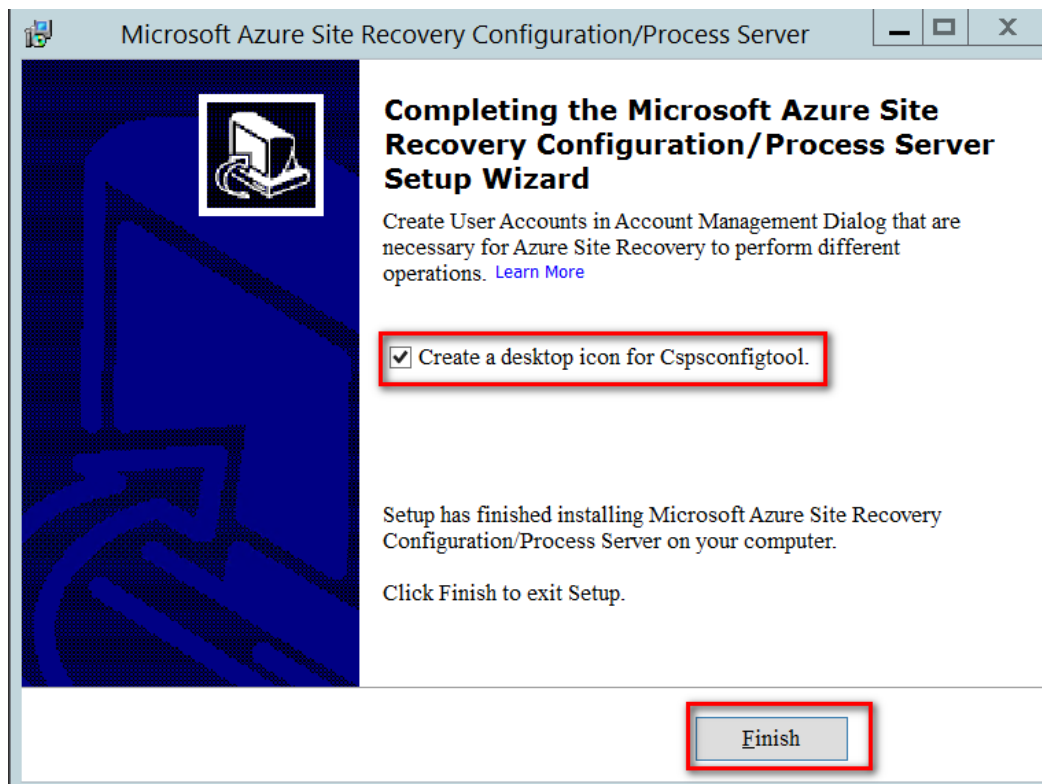
23. On the Welcome page of the setup program, click **Next**.
24. On the Third Party Software Installation page, click **I Accept**.
25. On the MySQL Server details page, for both the MySQL Root Password and the MySQL Database User Password, type **Passw0rd!** and click **Next**.
- ✦ In a production environment, you would choose different, more secure passwords.
26. On the Internet Settings page, select **Connect directly without a proxy**, and click **Next**.



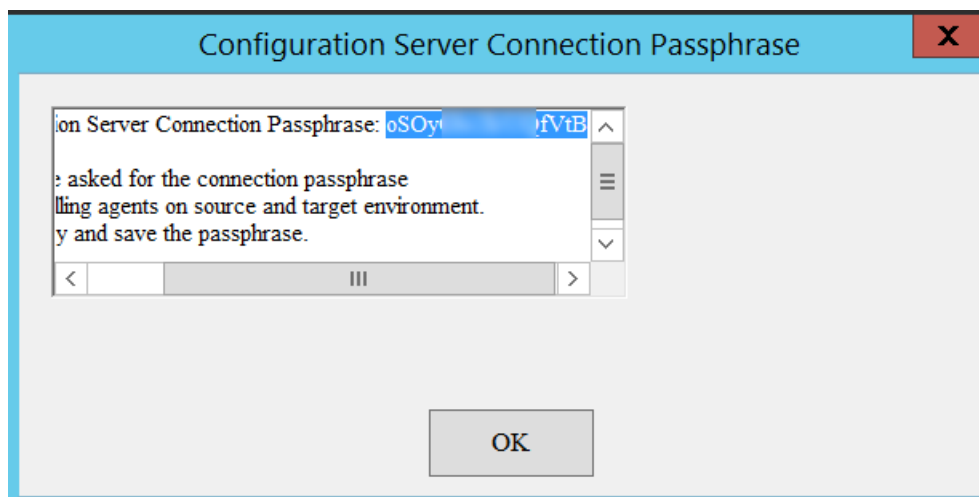
27. On the Provider Error Message Localization Settings page, ensure **English** is selected, and then click **Next**.
28. On the On the Azure Site Recovery Registration page, click **Browse**.
 - ✦ No files are present in the folder. In the next steps, you will copy the .vaultCredentials file from your local workstation to the folder location you have open.
29. Switch to your local workstation (AZRCamp-Admin).
30. Open File Explorer, and browse to the folder where you save the .vaultCredentials file you downloaded earlier.
31. Right-click **ASRVault_[date].vaultCredentials**, and click **Copy**.
32. Switch to the RDP session for ConfigSrv.
33. Right-click the empty folder, and then click **Paste**.
 - ✦ The .vaultCredentials file is copied to the folder.



34. Ensure the file is selected, and click **Open**.
35. On the Azure Site Recovery Registration page, click **Install**.
 - ❖ The installation will take approximately 10 minutes to complete.
36. When the installation is complete, ensure the option to **Create a desktop icon for Cspconfigtool** is selected, and then click **Finish**.



37. In the Configuration Server Connection Passphrase dialog box, select the entire passphrase, right-click the selected text, and then press CTRL + C to copy the passphrase to the clipboard.



❖ Ensure you copy the entire string.

38. Switch to the local workstation, and open **Notepad**.
- ★ TIP: use the same text file where you recorded the IP address and port number for the configuration server earlier in this lab.
39. In Notepad, press CTRL+V to copy the passphrase to Notepad.

40. Save the file in a convenient folder using a memorable name.

💡 Please ensure you save the passphrase. You will need it to complete remaining steps in the lab.

41. Switch to the RDP session with ConfigSrv.

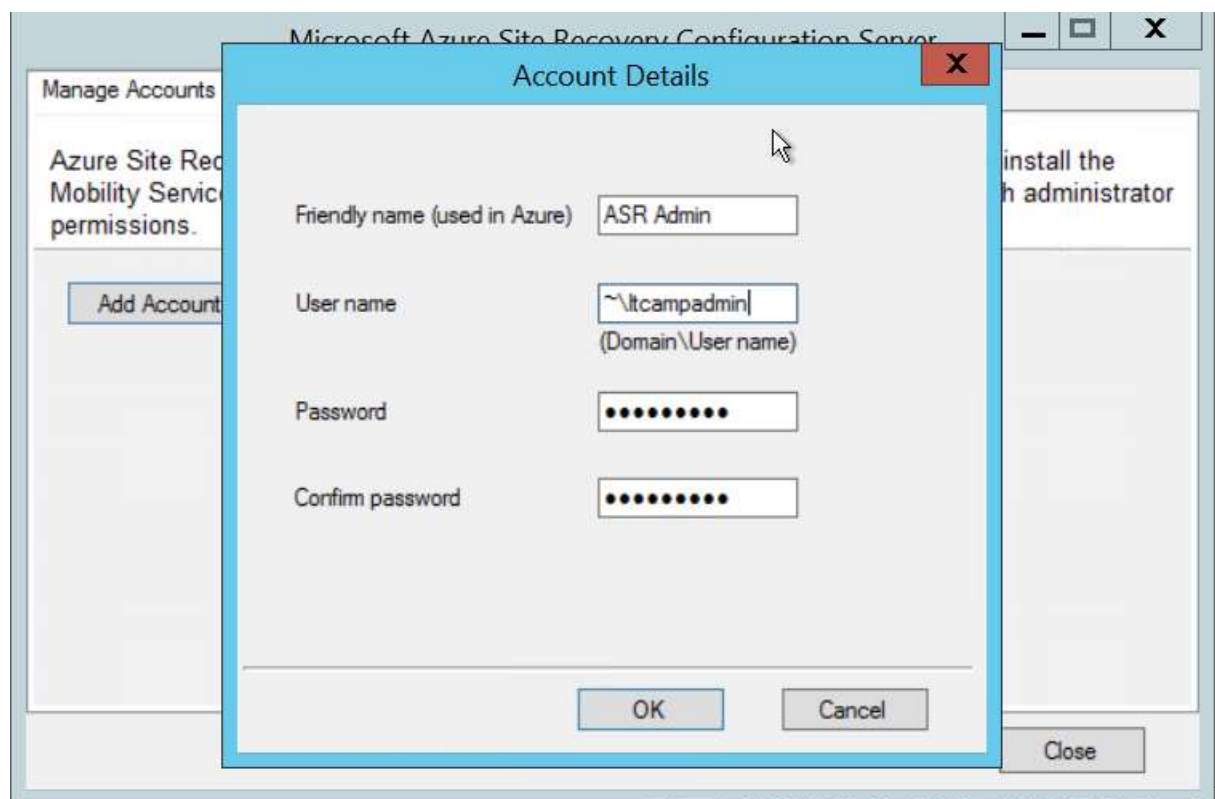
42. In the Configuration Server Passphrase dialog box, click **OK**.

✦ The Microsoft Azure Site Recovery Configuration Server dialog box appears.

43. In the Microsoft Azure Site Recovery Configuration Server dialog box, click **Add Account**.

44. In the Account details page, add the following information and then click **OK**.

- Friendly Name (used in Azure): **ASR Admin**
- User name: **~\Itcampadmin**
- Password: **Passw0rd!**
- Confirm Password: **Passw0rd!**



45. Click **OK** again.

46. Click **Close**.

Create and Configure a Master Target Server

The master target server is used for storing replicated data from the configured sources. The server must be installed as the configuration server you register it with and that you deployed earlier.

In this task, you will create the Master Target Server and then register it with the configuration server.

 Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

1. In the full Azure portal, in the left navigation, click RECOVERY SERVICES.
2. On the recovery services page, click **ASRVault**.
3. If the BEFORE YOU START page appears, close it.
4. On the asrvault page, under Prepare Target (Azure) Resources, click **Deploy Master Target Server**.
5. On the New Configuration Server details page, enter the following information and then click **Done** (check mark).
 - CONFIGURATION SERVER NAME: **MTSrv**
 - OPERATING SYSTEM: **Windows**
 - SIZE: **Standard_A4**
 - NEW USER NAME :**Itcampadmin**
 - PASSWORD: **Passw0rd!**
 - CONFIGURATION SERVER: **CONFIGSRV**
 - MICROSOFT AZURE NETWORK: **Lab04-T-VNET**
 - SUBNET: **ASRsubnet**
 - IPADDRESS: **10.0.0.101**

DEPLOY MASTER TARGET SERVER

New Master Target Server Details

To replicate virtual machines and physical machines into Azure, you need to deploy a Master Target Server in your Azure subscription which will receive replicated data. A Master Target Server will now be deployed using an Azure virtual machine gallery image.

MASTER TARGET SERVER NAME

MTSrv

OPERATING SYSTEM

Windows

SIZE

Standard_A4

NEW USER NAME

Itcampadmin

NEW PASSWORD

CONFIRM

6. Wait until the server provisioning job completes.
7. In the left navigation, click **VIRTUAL MACHINES**.

virtual machines

INSTANCES IMAGES DISKS

NAME	STATUS	SUBSCRIPTION	LOCATION
ConfigSrv	✓ Running	Azure Pass	East US 2
MTSrv	✓ Running	Azure Pass	East US 2

✦ If you do not see the MTSrv virtual machine, you may have to refresh the page.

8. On the virtual machines page, click the cell to the right of **MTSrv**.

✦ If you click MTSrv, you will open the quick start page.
9. On the command bar, click **CONNECT**, and then click **Open** when prompted.
10. In the Remote Desktop Connection dialog box, click **Connect**.

11. In the Windows Security dialog box, select **Use another account** and log on using **Itcampadmin** as the user name and **Passw0rd!** as the password.
12. In the Remote Desktop Connection dialog box, click **Yes**.
 - 💡 When the desktop initially loads, you may briefly see a PowerShell Window open. Do not close this the PowerShell windows.
 - ✦ After a few moments, the Host Agent Config dialog box appears.
13. While the host agent software is initializing, switch to your local Workstation.
14. Open the Notepad file where you save the Configuration Server passphrase.
15. Copy the passphrase to the clipboard.
16. Switch to the MTSrv RDP session.
17. In the Host Agent Config dialog box, enter the following configuration information, and then click **OK**,
 - IP Address: **10.0.0.100**
 - Port Number: **443**
 - Passphrase: **the passphrase you copied to the clipboard**

Host Agent Config

Global | Agent | Logging | Logon

CX Server Settings

IP Address : * 10 . 0 . 0 . 100

Port Number : * 443 ☒ Use HTTPS

Passphrase : * *****

☐ Enable Fixed NAT Hostname : VxAgent

☐ Enable Fixed NAT IP Address : 0 . 0 . 0 . 0

Note: Only IPv4 Address allowed
* Indicates mandatory fields

OK Cancel Apply

Design Site Recovery and Migration Using Azure Site Recovery

- ✦ You do not need to configure any NAT settings. The master target is on the same subnet as the configuration server.
- ✦ After a few moments, the desktop appears.

18. Switch to the full Azure portal.

19. In the left navigation, click **RECOVERY SERVICES**.

20. Click **ASRVault**.

21. On the asrvault page, click **SERVERS**.

22. On the CONFIGURATION SERVERS tab, click **CONFIGSRV**.

✦ It can take up to 10 or 15 minutes for the master target server to be registered.

23. If no servers appear listed on the configsrv page, click **Back** (left arrow).

24. On the command bar, click **REFRESH**, and wait for the refresh job to complete.



25. Click **CONFIGSRV**.

26. The master target server should appear. No process servers appear. This is expected. You will add a process server in subsequent steps.



Configure ASR Source Resources

In this lab exercise, you will configure the process server and the computer you wish to protect with ASR.

Create and Configure the Process Server

The server acting as the on-premises gateway receives all the changes in real time from the machines being protected and sends them to master target servers. This server is registered to a configuration server during setup.

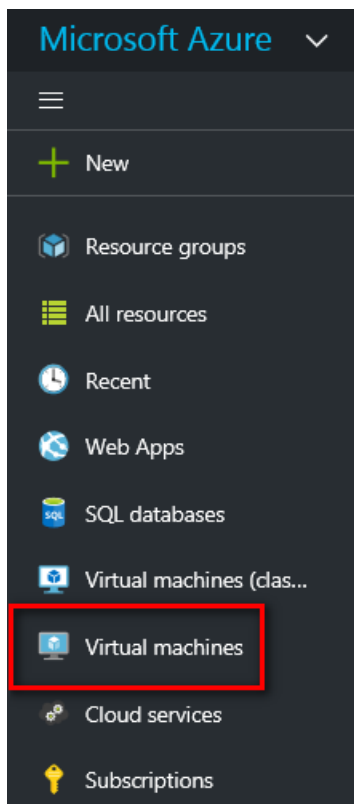
In this task, you will configure the process server and then register it with the configuration server.

- ✎ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

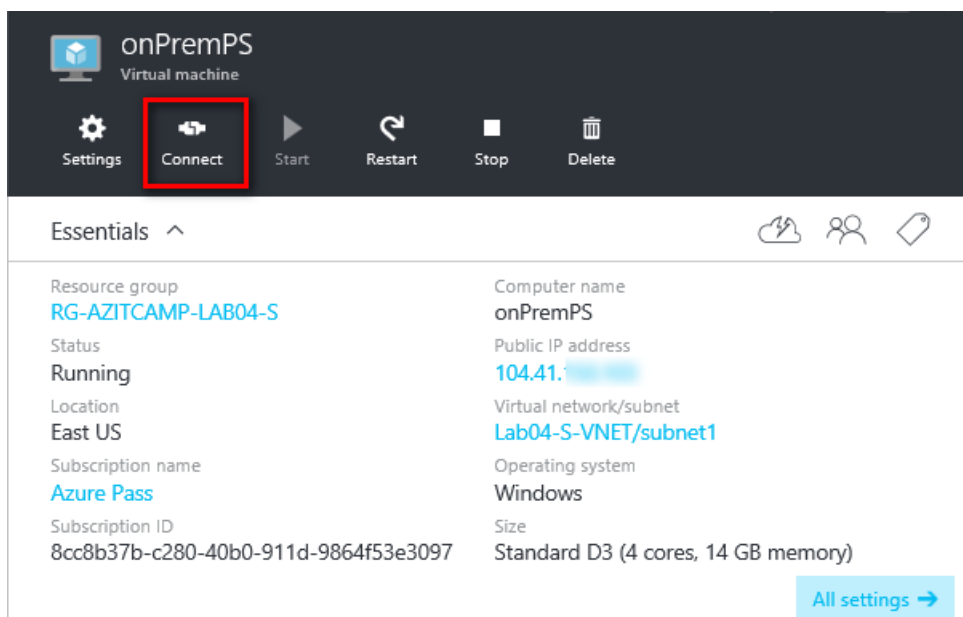
1. In the full Azure portal, in the upper right, click your account name.
2. In the drop down, click **Switch to Azure Preview Portal**.

✦ The virtual machines that act as the on premise process server and protected server were created and configure by using an Azure Resource Manager template. They are not available in the full Azure portal.

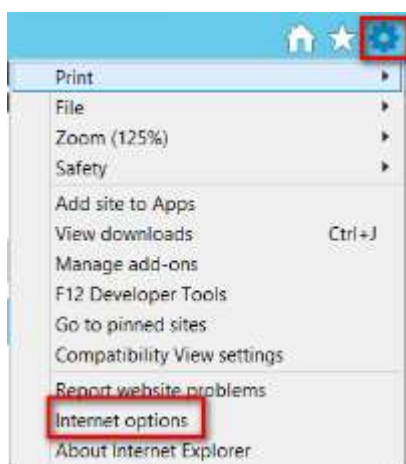
3. In the Azure Preview portal, in the left navigation, click **Virtual machines**.



4. In the Virtual machines blade, click **onPremPS**.
5. In the onPremPS blade, click **Connect**.

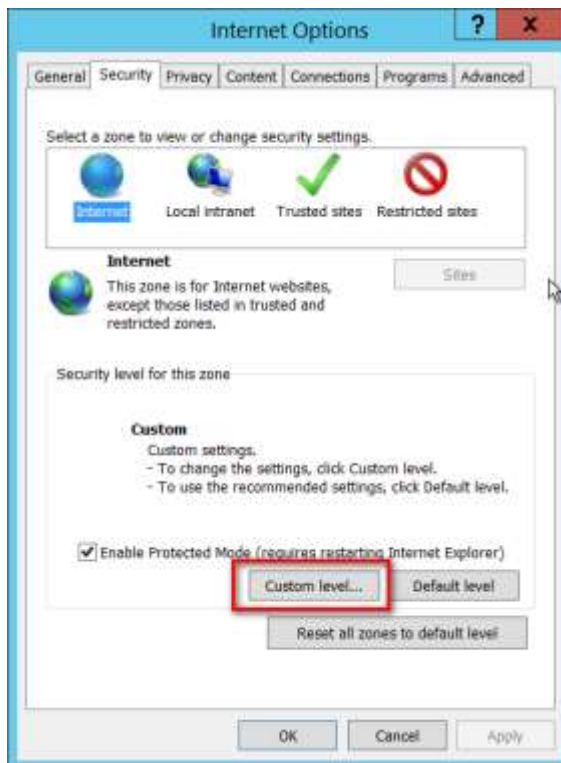


6. Click **Open**, and then log onto the RDP Session as **Itcampadmin** using **Passw0rd!** as the password.
7. On ONPREMPS, open **Internet Explorer**.
8. When prompted to configure Internet Explorer, accept the default setting and click **OK**.
9. Browse to **<https://manage.windowsazure.com>**, and log on to the full Azure portal using the credentials associated with your subscription.
10. In Internet Explorer, in the upper right, click the gear icon, and then click **Internet options**.



11. In the Internet Options dialog box, click the **Security** tab.
12. On the Security tab, click **Custom Level**.

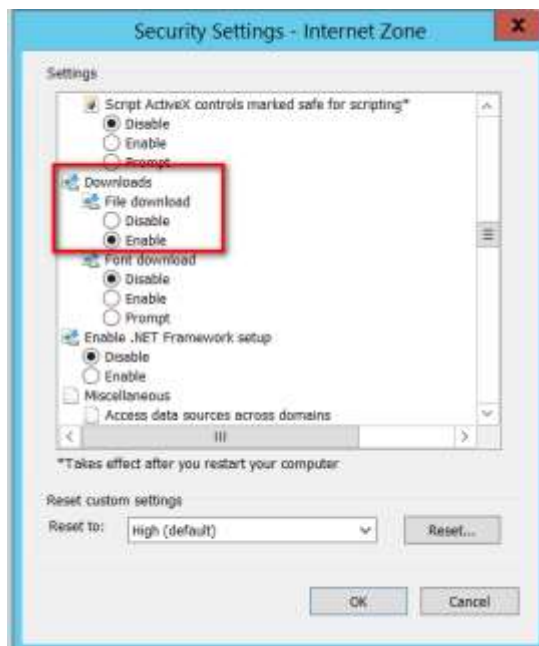
Design Site Recovery and Migration Using Azure Site Recovery



13. In the Security Settings – Internet Zone dialog box, scroll down and locate **Downloads**.

14. In the Downloads section, click **Enable**.

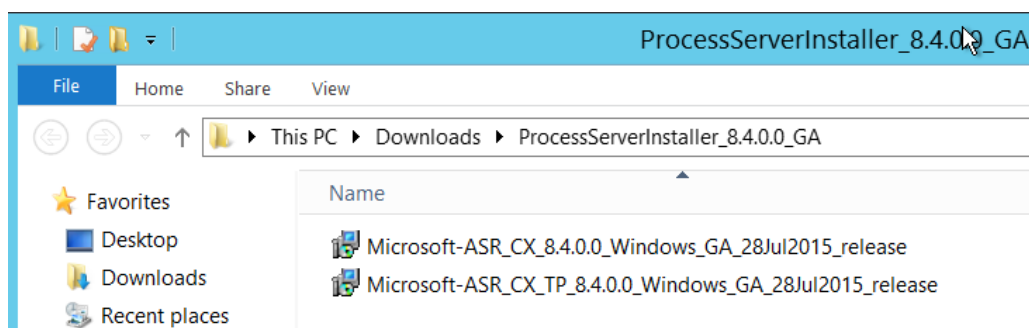
✦ It is necessary to change this setting for subsequent steps in the lab to work.



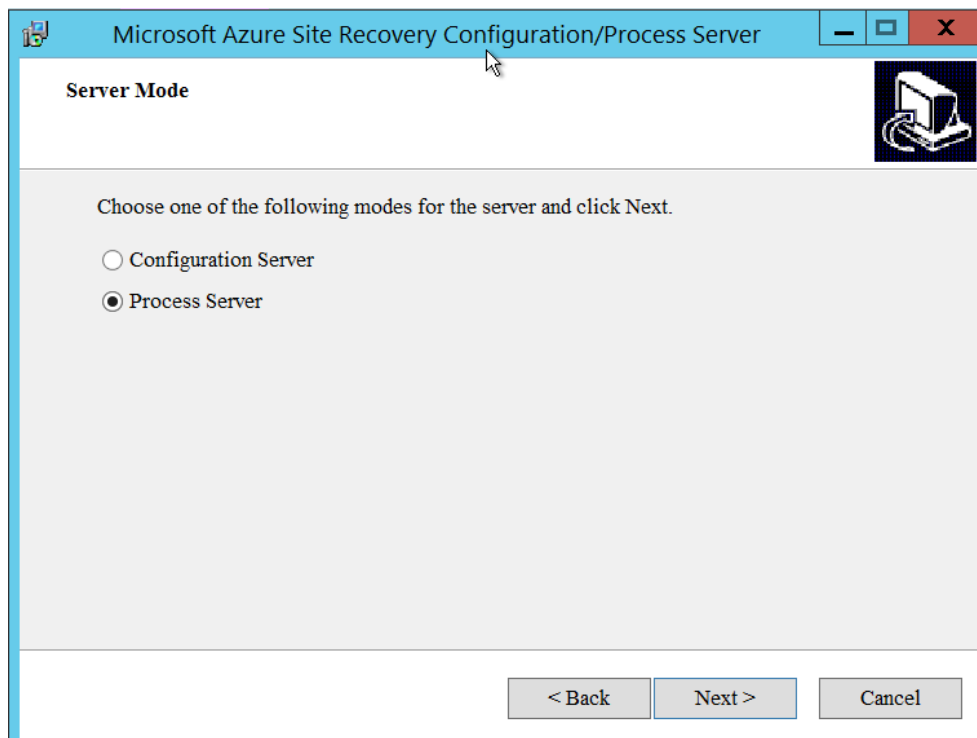
15. Click **OK**, click **Yes**, and then click **OK** again to close all the dialog boxes.

16. In the full Azure portal, in the left navigation, click **RECOVERY SERVICES**.

17. Click **ASRvault** to open the quick start page.
18. On the asrvault page, under Prepare Process Servers, click **Download and install Process Server**.
19. Click **Save**.
20. When the download completes, click **Open folder**.
21. Right-click **ProcessServerInstaller_8.4.0.0_GA**, and then click **Extract All**.
 - ✦ Depending on when you are performing this lab, the lab name may be slightly different to reflect a later version.
22. In the Extract Compress (Zipped) Folders dialog box, accept the default path, and click **Extract**.
23. Two files are extracted as shown below.

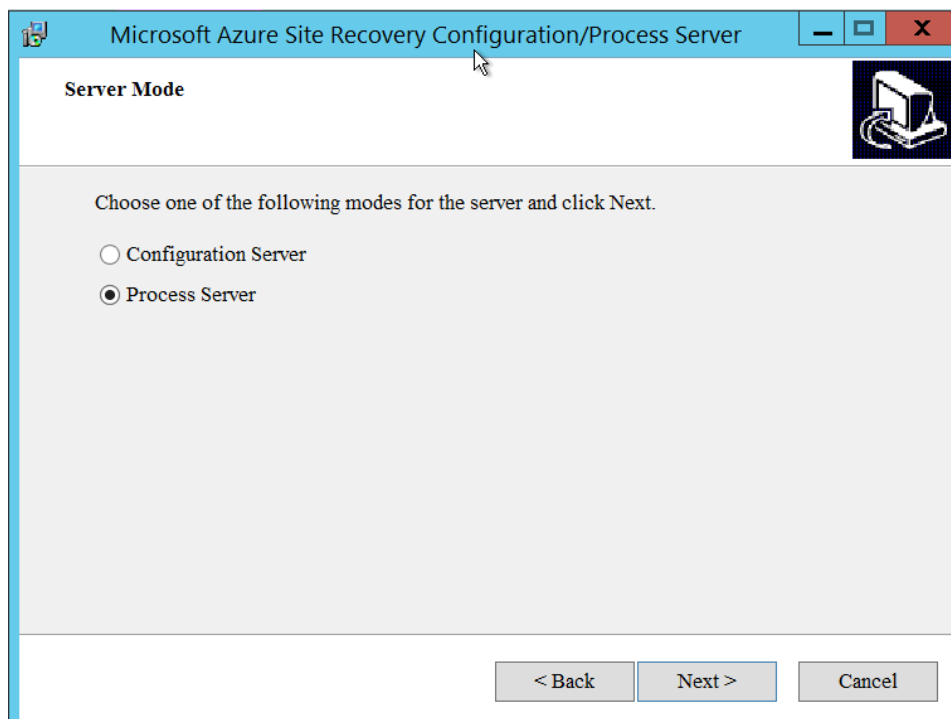


24. Double-click **Microsoft-AXR_CX_TP_8.4.0.0_Windows**.
 - ✦ This file installs third-party components required for the process server and must be installed first.
25. Click **Run**, and then click **Install**.
26. Click **Finish**.
27. Double-click **Microsoft-AXR_CX_8.4.0.0_Windows**.
28. Click **Run**, and then click **Next**.
29. On the Server Mode page, click **Process Server**, and then click **Next**.

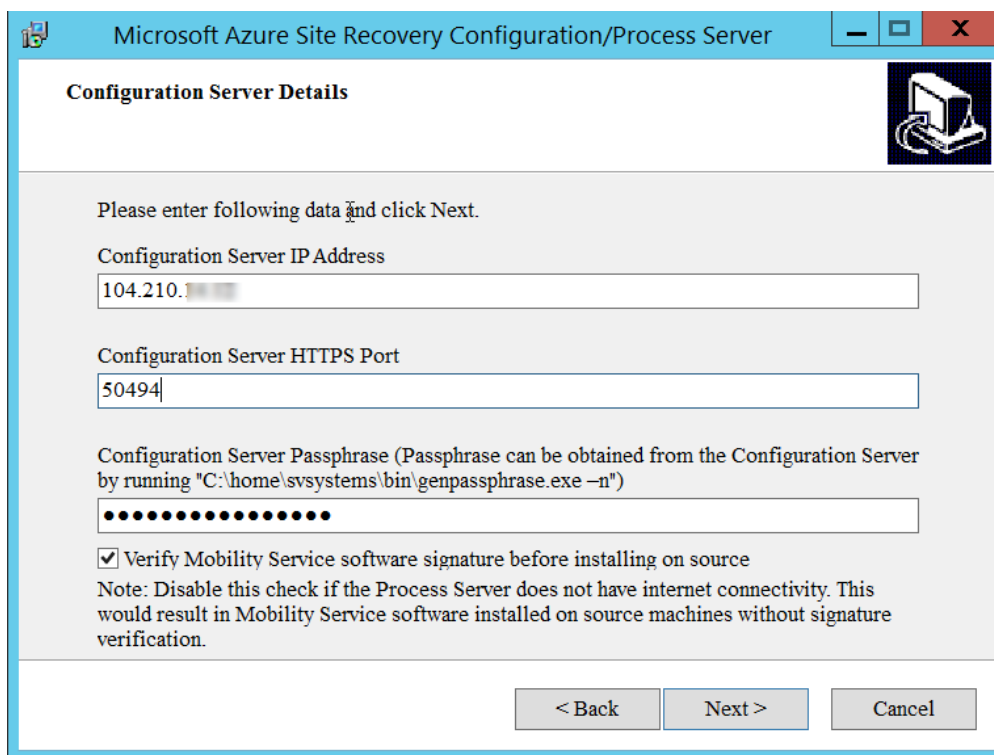


30. On the Environment Details page, click **No** to indicate that you will not be protecting VMWare virtual machines, and then click **Next**.

✦ The steps for configuring ASR protection for both VMWare virtual machines and physical machines are almost identical.



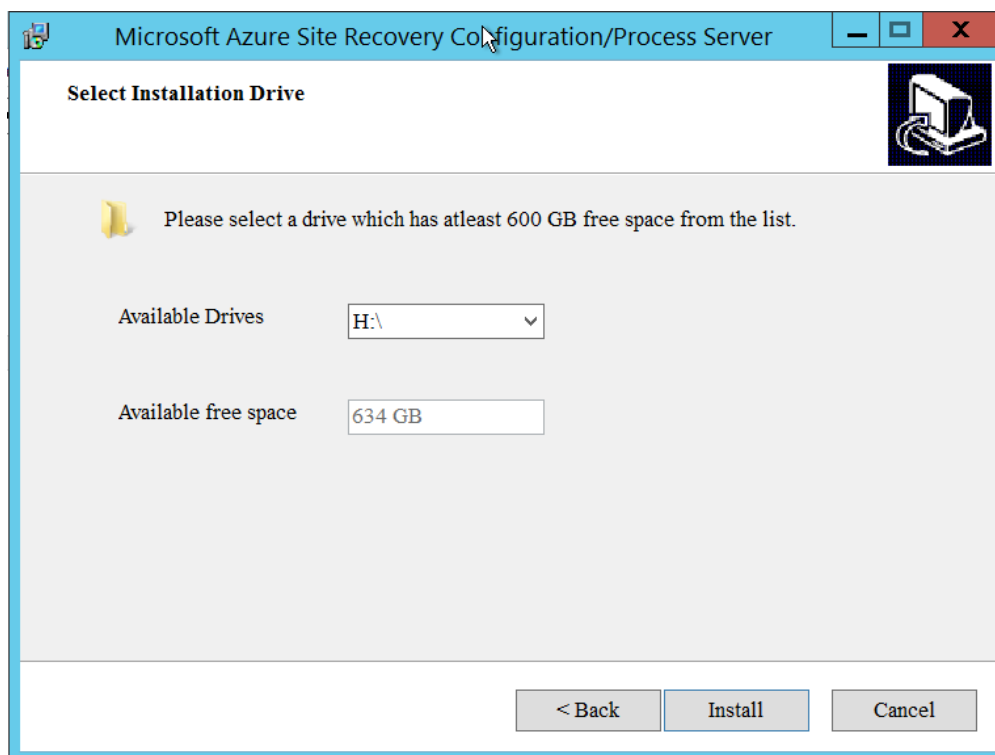
31. On the NIC Selection for Process Server page, click **Next**.
32. On the Configuration Server Details page, enter the public IP address for the configuration server, the public port number that maps to port TCP 443 internally and the passphrase from the configuration server.
 - ✦ Note that if you were connected by means of a VPN to the VNET where the configuration server resides, you would use TCP port 443.
 - ✦ Your IP address and port number will differ from those shown below. You recorded this information earlier in the lab.



The screenshot shows a Windows-style window titled "Microsoft Azure Site Recovery Configuration/Process Server". The window has a blue title bar with standard minimize, maximize, and close buttons. The main content area is titled "Configuration Server Details" and contains the following elements:

- A message: "Please enter following data and click Next."
- A text input field labeled "Configuration Server IP Address" containing the value "104.210.100.100".
- A text input field labeled "Configuration Server HTTPS Port" containing the value "50494".
- A text input field labeled "Configuration Server Passphrase (Passphrase can be obtained from the Configuration Server by running 'C:\home\svsystems\bin\genpassphrase.exe -n')". The field is filled with 12 dots.
- A checkbox labeled "Verify Mobility Service software signature before installing on source" which is checked.
- A note below the checkbox: "Note: Disable this check if the Process Server does not have internet connectivity. This would result in Mobility Service software installed on source machines without signature verification."
- At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

33. Click **Next**.
34. On the Select Installation Drive page, select **H:**, and then click **Install**.
 - ✦ The process server requires a cache drive that is at least 600 GB in size. Also, because the cache drive could potentially have IO intensive workloads, the cache drive should be capable of high IO. The virtual machine that was created for this lab uses 5-striped disks in a storage pool for the H: drive.



35. On the Completing the Microsoft Azure Site Recovery Configuration / Process Server Setup Wizard page, accept the default to restart the server, and click **Finish**.
36. In the Setup dialog box, read the notice about the mounting of the H: drive as C:\Home, and click **OK**.
✦ The server restarts.
37. On your local workstation, open the full Azure portal, if not already open.
38. In the full Azure portal, in the left navigation, click RECOVERY SERVICES.
39. On the recovery services page, click **ASRVault**.
40. On the asrvault page, click **SERVERS**.
41. On the CONFIGURATION SERVERS tab, click **CONFIGSRV**.
✦ It can take up to 10 or 15 minutes for the process server to be registered.
42. If the process server is not listed on the configsrv page, click **Back** (left arrow).
43. On the command bar, click **REFRESH**, and wait for the refresh job to complete.
44. Click CONFIGSRV.
45. The process server should appear.

Design Site Recovery and Migration Using Azure Site Recovery

configsrv

SERVER DETAILS CONFIGURE

statistics

IP address	10.0.0.100
Version	8.4.0.0
Protected Items	0
Agents	1

process servers

NAME	IP ADDRESS	HEALTH	PROTECTED ITEMS	VERSION	ACTION
onPremPS	10.0.0.10	✓ Healthy	0	8.4.0.0	Change IP

master target servers

NAME	OS	PROTECTED DRIVES	LAST HEART BEAT	RETENTION DRIVE	VERSION
MtSRV	Windows	1 Used of 15 slots	✓ 10/11/2015 11:08:49 P...	✓ 1022.79 GB free of 10...	8.4.0.0

Update ASR Servers

In this lab exercise, you will ensure that the configuration server, process server, and master target server have the latest updates installed. At the time of this writing (Oct., 2015) an update was available only for the Configuration Server. However, this may change in the future. The servers should be updated in the following order:

1. Configuration server
2. Process server
3. Master target server

❖ In the lab tasks that follow, please ensure that you follow this order.

Update configuration server

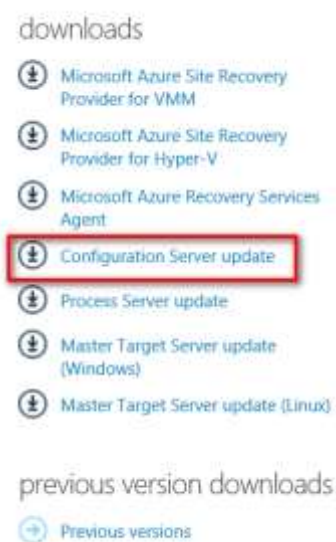
In this task, you will update the configuration server. You will first disable Internet Explorer Enhanced Security Configuration. This will allow you to logon to Azure and download the executable update file from the Azure portal.

✎ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

1. In the full Azure portal, in the left navigation, click **VIRTUAL MACHINES**.
2. On the virtual machines page, select **ConfigSrv**, and then on the command bar, click **CONNECT**.
3. Click **Open**, and then click **Connect**.
4. When prompted by the Windows Security dialog box, log on as **Itcampadmin** using **Passw0rd!** as the password.
5. In the Remote Desktop Connection dialog box, click **Yes**.
6. Open **Server Manager**.
7. In Server Manager, click **Local Server**.
8. In the properties tiles for ConfigSrv, to the right of IE Enhanced Security Configuration, click **On**.
9. In the Internet Explorer Enhanced Security Configuration dialog box, under both Administrators and Users, select **Off**, and then click **OK**.



10. Open **Internet Explorer**.
11. When prompted to configure Internet Explorer, accept the default setting and click **OK**.
12. Browse to **<https://manage.windowsazure.com>**, and log on to the full Azure portal using the credentials associated with your subscription.
13. In the full Azure portal, in the left navigation, click **RECOVERY SERVICES**.
14. Click **ASRvault** to open the quick start page.
15. Click **DASHBOARD**.
16. On the DASHBOARD page, under downloads, click **Configuration Server Update**.



17. When prompted to run or save the executable, click **Run**.
18. On the Welcome to the Microsoft Azure Site Recovery Configuration / Process Server Hotfix-1 Setup Wizard page, click **Install**.
 - ✦ It may be case, depending on the circumstances of the current date, that there is no hotfix update.
Please ensure that you update the software only if it is appropriate for your particular circumstances.
19. Click **Finish**.

Determine if update is required for process server

At the time of the time of this writing, the July 28, 2015 release of the process server software that you installed earlier was the most current release. At the current date, it may be the case that this software has been updated.

In this task, you will determine if the software has been updated and take the appropriate action.

- ✦ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:
 1. Switch to the Azure preview portal.
 2. In the Azure Preview portal, in the left navigation, click **Virtual Machines**.
 3. In the Virtual machines blade, click **onPremPS**.
 4. In the onPremPS blade, click **Connect**.
 5. Click **Open**, and then log onto the RDP Session as **Itcampadmin** using **Passw0rd!** as the password.
 6. On ONPREMPS, open Internet Explorer.
 7. When prompted to configure Internet Explorer, accept the default setting and click **OK**.
 8. Browse to **<https://manage.windowsazure.com>**, and log on to the full Azure portal using the credentials associated with your subscription.
 9. In the full Azure portal, in the left navigation, click **RECOVERY SERVICES**.
 10. Click ASRVault to open the quick start page.
 11. Click **DASHBOARD**.
 12. On the DASHBOARD page, under downloads, click **Process Server Update**.
 13. When prompted to run or save the executable, click **Save**.
 14. When the File has completed downloading, click **Open Folder**.
 15. Extract the compressed file.
 16. Compare the contents of the two extracted folders in the Downloads folder. If they are the same, no further action is required; if they are different, install the updates.

Determine if update is required for master target server

In this task, you will update the master target server.

 Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

1. In the full Azure portal, in the left navigation, click **VIRTUAL MACHINES**.
2. On the virtual machines page, select **MTSrv**, and then on the command bar, click **CONNECT**.
3. Click **Open**, and then click **Connect**.
4. When prompted by the Windows Security dialog box, log on as **Itcampadmin** using **Passw0rd!** as the password.
5. In the Remote Desktop Connection dialog box, click **Yes**.
6. Open **Server Manager**.
7. In Server Manager, click **Local Server**.
8. In the properties tiles for ConfigSrv, to the right of IE Enhanced Security Configuration, click **On**.
9. In the Internet Explorer Enhanced Security Configuration dialog box, under both Administrators and Users, select **Off**, and then click **OK**.
10. Open **Control Panel**.
11. In Control Panel, click **Programs**.
12. Click **Programs and Features**.
13. Note the version number of the installed software.



14. Close Control Panel.
15. Open **Internet Explorer**.
16. When prompted to configure Internet Explorer, accept the default setting and click **OK**.
17. Browse to **https://manage.windowsazure.com**, and log on to the full Azure portal using the credentials associated with your subscription.
18. In the full Azure portal, in the left navigation, click **RECOVERY SERVICES**.
19. Click **ASRvault** to open the quick start page.

20. Click **DASHBOARD**.
21. On the DASHBOARD page, under downloads, click **Master Target Server update (Windows)**.
22. You are prompted to run, save, or cancel the file download.
23. If the software version is the same as you determined earlier in this task, you do not need to take any action. Click **Cancel**.
24. However, if you are prompted to install a more recent version, take the appropriate action to install the updated version.

Configure Protection for Servers

In this lab exercise, you will prepare the server that you want to protect and then configure a protection.

Configure source server

In order to push the mobility service on to the source service, it is necessary to ensure the local firewall allows File and Print Sharing and Windows Management Instrumentation (WMI) traffic. Additionally, if the account that is used to push the mobility service is not a member of a domain, it is necessary to modify the registry of the source machine to disable Remote User Access control.

In this task, you will modify the local firewall rules and examine the previously modified registry value.

✎ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

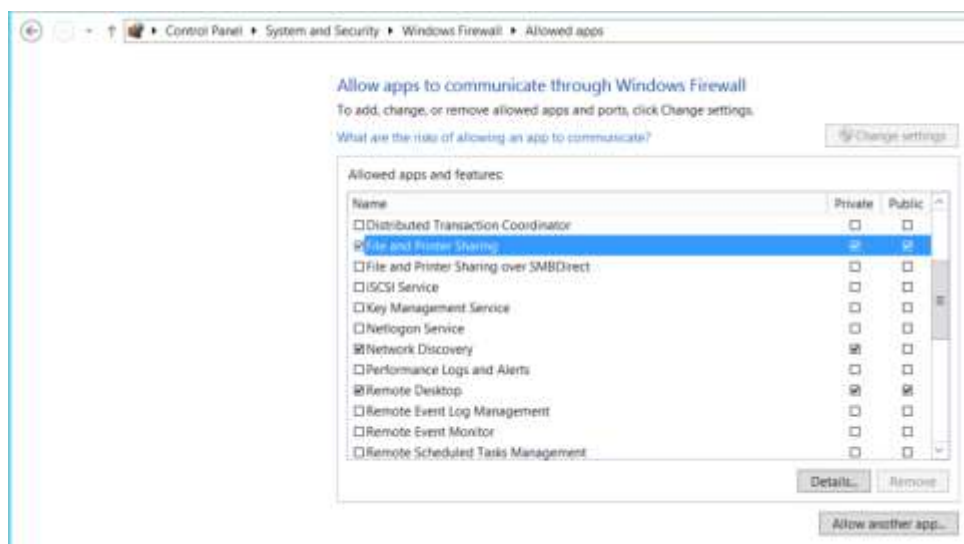
1. Switch to the Azure preview portal.
2. In the Azure Preview portal, in the left navigation, click **Virtual Machines**.
3. In the Virtual machines blade, click **onPremSource**.
4. In the onPremSource blade, click **Connect**.
5. Click **Open**, click **Connect**, and then log onto the RDP Session as **Itcampadmin** using **Passw0rd!** as the password.
6. Click **Yes**.
7. Click **Start**, and then click **Control Panel**.
8. Click **System and Security**.
9. Click **Windows Firewall**.
10. Click **Allow an app or feature through Windows Firewall**.



11. On the Allows apps to communicate through Windows firewall, enable **File and Printer Sharing** for both the Public and Private networks.

Design Site Recovery and Migration Using Azure Site Recovery

- ✦ This setting is more relaxed than it likely needs to be. However, it will ensure that the traffic will be allowed if you were prompted to choose a setting for the network and chose public.



12. Scroll down and enable the setting to allow **Windows Management Instrumentation (WMI)** traffic for both the public and private networks.



13. Click **OK**, and then close Control Panel.
14. Right-click **Start**, and then click **Run**.
15. In the Run dialog box, type **regedit**, and then click **OK**.
16. In Registry Editor, in the tree pane, expand **HKEY_LOCAL_MACHINE / Software / Microsoft / Windows / CurrentVersion / policies**.
17. Click **System**.
18. In the details pane, note the DWORD **LocalAccountTokenFilterPolicy**.
 - ✦ If you are using a non-domain account to push the mobility service software, this DWORD value must be present.
 - ✦ This DWORD value is not present by default and was added during the provisioning of the Azure virtual machine.

Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000005 (5)
ConsentPromptBehaviorUser	REG_DWORD	0x00000003 (3)
DelayedDesktopSwitchTimeout	REG_DWORD	0x00000000 (0)
DisableAutomaticRestartSignOn	REG_DWORD	0x00000001 (1)
disablecad	REG_DWORD	0x00000000 (0)
dontdisplaylastusername	REG_DWORD	0x00000000 (0)
DSCAutomationHostEnabled	REG_DWORD	0x00000002 (2)
DnsScheduledTaskDeleted	REG_DWORD	0x00000001 (1)
EnableCursorSuppression	REG_DWORD	0x00000001 (1)
EnableInstallerDetection	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUIAPaths	REG_DWORD	0x00000001 (1)
EnableUIADesktopToggle	REG_DWORD	0x00000000 (0)
EnableVirtualization	REG_DWORD	0x00000001 (1)
FilterAdministratorToken	REG_DWORD	0x00000000 (0)
legalnoticecaption	REG_SZ	
legalnoticetext	REG_SZ	
LocalAccountTokenFilterPolicy	REG_DWORD	0x00000001 (1)
PromptOnSecureDesktop	REG_DWORD	0x00000001 (1)
sctforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000000 (0)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)

19. Close Registry Editor.

20. Restart ONPREMSOURCE.

✈ You are restarting ONPREMSOURCE to ensure that there is no pending restart that will interfere with the push installation of the mobility service that you will configure in later steps.

21. Switch to the local workstation.

Create a protection group

In this task, you will create a protection group.

✍ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

1. In the full Azure portal, in the left navigation, click **RECOVERY SERVICES**.
2. Click **ASRvault** to open the quick start page.
3. Click **PROTECTED ITEMS**.
4. Click **CREATE PROTECTION GROUP**.

asrvault

 DASHBOARD PROTECTED ITEMS RECOVERY PLANS SERVERS RESOURCES JOBS EVENTS

VMM CLOUDS PROTECTION GROUPS

You haven't created any protection group. Create one and then add virtual machines to it.

CREATE PROTECTION GROUP 

5. On the Specify Protection Group Settings Page, in PROTECTION GROUP NAME, type **PG-1**, accept the default FROM value (CONFIGSRV) and then click **Next** (right arrow).
6. On the Specify Replication Settings page, accept the default settings and then click **Done** (check mark).

CREATE PROTECTION GROUP

Specify Replication Settings

Configure replication settings that will be applied to all the machines in the protection group.

MULTI VM CONSISTENCY ?

ON OFF

RPO THRESHOLD ?

30 MINUTES

RECOVERY POINT RETENTION

24 HOURS

APPLICATION CONSISTENT SNAPSHOT FREQUENCY ?

60 MINUTES

7. Wait for the completion of Create Protection Group Job.

✈ You can monitor the progress of the job by selecting the appropriate Job from the Jobs page of the ASR vault. The job should complete within a minute or two.

pg-1 (configuring protection group)

JOB PROPERTIES

NAME	STATUS	START TIME	DURATION
Adding the protection group	Completed	10/12/2015 8:21:21 AM	1 MINUTE
Configuring the Configuration server f...	In progress	10/12/2015 8:21:25 AM	

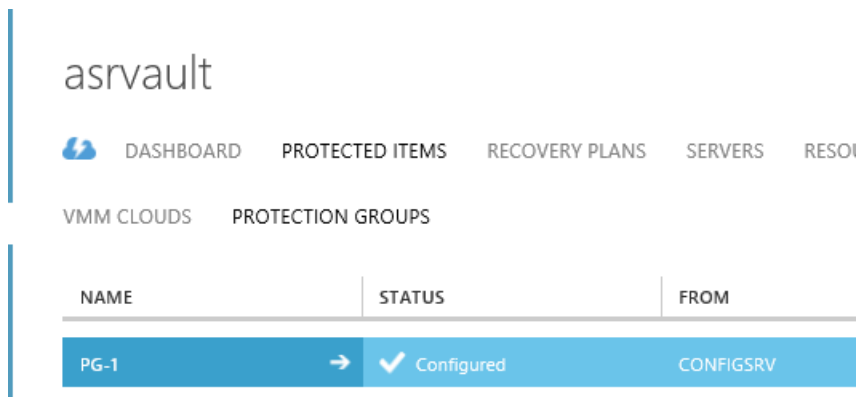
Add a Machine to a Protection Group

Protection groups are logical groupings of virtual machines that share the same protection settings.

In this task, you will add a machine to the protection group you just created. Although you will add an Azure virtual machine that resides in US East, the onPremSource virtual machine stands in for a physical machine. The steps for protecting this Azure virtual machine are identical to the steps you would take to protect a physical machine.

✎ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:

1. In the full Azure portal, in the left navigation, click **RECOVERY SERVICES**.
2. Click **ASRvault** to open the quick start page.
3. Click **PROTECTED ITEMS**.
4. Click **PG-1**.



5. On the pg-1 page, click **ADD PHYSICAL MACHINES**.

✎ If you wanted to protect virtual machines running on VMWare, you would select **ADD VIRTUAL MACHINES**.



6. On the Add Physical Machines page, enter the following information and click **Next**.

- IPADDRESS: **10.0.0.11**
- FRIENDLY NAME: **onPremSource**
- OPERATING SYSTEM: **Windows**

✎ Note that the IP address is from the point of view of the process server. The source server you wish to protect needs to be reachable from the VNET / Network where the process server resides.

ADD PHYSICAL MACHINES

Add Physical Machines

IP ADDRESS	FRIENDLY NAME	OPERATING SYSTEM FAMILY
10.0.0.11	onPremSource	Windows
<input type="text"/>	<input type="text"/>	<input type="text"/>

7. On the Configure Target Settings page, select the following settings, and click **Next**.

- PROCESS SERVER: **OnPremPS**
- MASTER TARGET SERVER: **MTSRV**
- STORAGE ACCOUNT: **[yourinitials]store#**

ADD PHYSICAL MACHINES

Configure Target Settings

Specify target settings for replicated physical machines.

☒ Apply settings to all physical machines

MACHINES	PROCESS SERVER	MASTER TARGET SERVER	STORAGE ACCOUNT
All machines (1)	onPremPS	MTSRV	[yourinitials]store1

8. On the Specify Accounts page, ensure that **ASR Admin** is selected as the account, and click **Done**.

✈ The job to configure protection of onPremSource starts.

ADD PHYSICAL MACHINES

Specify Accounts

Select the accounts you created on the Configuration Server. Account information will only be used to install Mobility Service on the machines.

☒ Use the same credentials for all physical machines

MACHINES	ACCOUNT
All machines (1)	ASR Admin

9. Navigate to the asrvault quick start page, and then click **JOBS**.

10. On the JOBS tab, click **Add and protect physical machine**.

Design Site Recovery and Migration Using Azure Site Recovery



11. On the onpremsource (add and protect physical machine) page, expand **Protecting physical machine**.

12. This allows you to view progress of the job in detail.



13. After about 20 minutes or so, replication between the target and the source should begin.



14. Navigate the asrvault quick start page, and then click **PROTECTION ITEMS**.

15. On the PROTECTION GROUPS tab, click **PG-1**.

- ✦ You will be able to view the status of the synchronization. The initial synchronization should take about an hour.

Design Site Recovery and Migration Using Azure Site Recovery



NAME	ACTIVE LOCATION	STATUS	REPLICATION STATUS	RPO	SUCCESSFUL FAILOVER	VERSION
onPremSource	On-premises	17% Synchronized	17% Synchronizing	17 minutes ago		5.4.0.0

16. Establish an RDP session with OnPremSource.

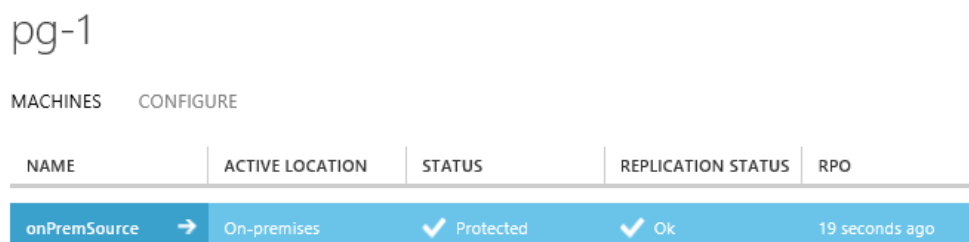
17. Open Services console, and note the presence of a number of InMage services.

- ✦ The InMage Scout application (acquired by Microsoft in 2014) provides continuous data backup protection and was installed on onPremSource when you pushed the mobility service client.



Name	Description	Status
IKE and AuthIP IPsec Keying...	The IKEEXT service hosts the Internet Key Exchange (IKE) and A...	
InMage Scout Application S...	Helps in the discovery, protection and recovery of applications	Running
InMage Scout FX Agent	File Replication Service	
InMage Scout VX Agent - S...	Volume Replication Service	Running
Interactive Services Detection	Enables user notification of user input for interactive services, ...	
Internet Connection Sharin...	Provides network address translation, addressing, name resolut...	

18. Wait until the synchronization job completes and then proceed to the next exercise.



NAME	ACTIVE LOCATION	STATUS	REPLICATION STATUS	RPO
onPremSource	On-premises	✓ Protected	✓ Ok	19 seconds ago

Modify Protection Group Properties

Once the source machine is protected by the ASR, it is possible to modify the protected machine properties.

In this task, you will examine the properties you can modify.

- ✦ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **PasswOrd!** as the password:

1. In the full Azure portal, in the left navigation, click **RECOVERY SERVICES**.
2. Click **ASRvault** to open the quick start page.
3. Click **PROTECTED ITEMS**.

4. Click **PG-1**.
5. On the pg-1 page, ensure the status is **Protected**, and then click **onPremSource**.
6. Spend a few moments examining the information on the omprem source page, and then click **CONFIGURE**.
 - ✦ It is possible to change the name and virtual machine size when failing over from the source to the destination.
7. On the CONFIGURE tab, under source and target network properties, under MICROSOFT AZURE NETWORK, select **Lab-4-T-VNET**.
 - ✦ Depending on the type of source and destination network and whether or not a static IP address is configured for the source, you can specify a static target IP address. Because the lab environment does not meet the required criteria, the option to specify a static IP address is not available.

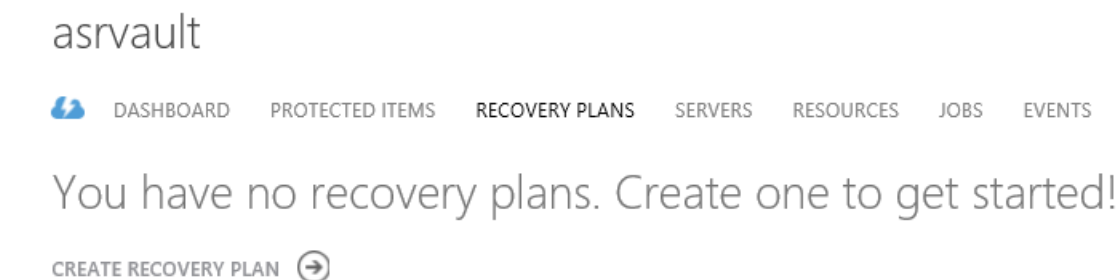
8. On the command bar, click **SAVE**, and then click **Yes**.
9. Wait for the job to complete before proceeding to the next task.

Create a Recovery Plan

In this task, you will create a recovery plan for your protected servers.

- ✦ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:
1. In the full Azure portal, click the back (left) arrow until you reach the asrvault page.

2. On the asrvault page, click **RECOVERY PLANS**.
3. Click **CREATE RECOVERY PLAN**.



4. On the Specify source, target, and a name page, in NAME, type **RP-1**, accept the remaining default values, and click **Next**.
5. On the Select Protected Entities page, select **onPremSource**.
6. Click **Done** (check mark)



Perform an unplanned failover

In this task, you will perform a failover from your simulated "on-premises" machine to the Azure. You can also consider the failover you perform in this task as a demonstration of using ASR to migrate an Azure virtual machine from one region to another.

- ✎ Perform the following tasks on **AZRCamp-Admin** logged on as **Administrator** using **Passw0rd!** as the password:
1. In the full Azure portal, on the asrvault page, ensure that **RP-1** is selected in the RECOVERY PLANS tab of the asrvault page.

Design Site Recovery and Migration Using Azure Site Recovery

asrvault

DASHBOARD PROTECTED ITEMS RECOVERY PLANS SERVERS		
NAME	SOURCE	TARGET
RP-1	→ CONFIGSRV	Microsoft Azure

- On the command bar, click **FAILOVER**.



- On the Confirm Failover page, review the information, accept the default settings, and click **Done**.

Confirm Failover

Verify the unplanned failover for 'RP-1'. Check that initial replication has completed for all virtual machines in this recovery plan.

FAILOVER DIRECTION

FROM

CONFIGSRV

TO

Microsoft Azure

RECOVERY POINT

☒ Latest recovery point in time

☐ Latest application consistent recovery point

- The job to failover to the East US 2 region begins.

asrvault

DASHBOARD PROTECTED ITEMS RECOVERY PLANS SERVERS RESOURCES JOBS EVENTS				
NAME	SOURCE	TARGET	CURRENT JOB	SUCC
RP-1	→ CONFIGSRV	Microsoft Azure	Unplanned Failover In...	

- Click the **JOBS** tab.
- On the JOBS tab, click **Unplanned failover**.

Design Site Recovery and Migration Using Azure Site Recovery

asrvault

DASHBOARD PROTECTED ITEMS RECOVERY PLANS SERVERS RESOURCES JOBS EVENTS

SERVER: All TYPE: All STATUS: All DURATION: Seven days

Run the query. Query results are not refreshed automatically.

NAME	ITEM	TYPE	STATUS	START TIME	DURAT...
Unplanned failover	RP-1	Recovery Plan	In progress	10/12/2015 1:56:59 PM	
Save a recovery plan	RP-1	Recovery Plan	Completed	10/12/2015 1:46:02 PM	1 MINUTE
Update the virtual machine	onPremSource	Virtual Machine	Completed	10/12/2015 1:36:21 PM	1 MINUTE
Finalize protection on the virtual machi...	onPremSource	Virtual Machine	Completed	10/12/2015 10:23:58 AM	2 MINUTES

- Wait until the rp-1 (unplanned failover) job has completed, as shown below, before proceeding to the next step.

rp-1 (unplanned failover)

JOB PROPERTIES

NAME	STATUS	START TIME	DURATION
Prerequisites check for the recovery pl...	Completed	10/12/2015 1:56:47 PM	1 MINUTE
Create the environment	Completed	10/12/2015 1:56:54 PM	1 MINUTE
Recovery plan failover	Completed	10/12/2015 1:57:06 PM	3 MINUTES
onPremSource	Completed	10/12/2015 1:57:06 PM	3 MINUTES
Group 1: Start (1)	Completed	10/12/2015 2:00:29 PM	4 MINUTES
Finalizing the recovery plan	Completed	10/12/2015 2:00:46 PM	1 MINUTE

- In the Azure Portal, click **Back**, and then, on the asrvault page, click **PROTECTED ITEMS**.
- On the PROTECTION GROUPS tab, click **PG-1**.
- The pg-1 page is updated to indicate the time of the successful failover.

pg-1

MACHINES CONFIGURE

NAME	ACTIVE LOCATION	STATUS	REPLICATION STATUS	RPO	SUCCESSFUL FAILOVER	VERSION
onPremSource	Microsoft Azure	Unplanned failove...	Ok	2 minutes ago	10/12/2015 1:56:39 PM	8.4.0.0

- In the Azure Portal, in the left navigation, click **VIRTUAL MACHINES**.
 - The onPremSource virtual machine is available in the East US 2 and has been created in a cloud service named after your recovery plan.
 - You may have to refresh the page to see the addition of the onPremSource virtual machine.

virtual machines

INSTANCES IMAGES DISKS

NAME		STATUS	SUBSCRIPTION	LOCATION	DNS NAME	
ConfigSrv		Running	Azure Pass	East US 2	configsrv-e53ed32d-0f92-438e-9e	
MTSrv		Running	Azure Pass	East US 2	configsrv-e53ed32d-0f92-438e-9e	
onPremSource		Running	Azure Pass	East US 2	rg-f.cloudapp.net	

Clean up Azure resources used in the lab

Because each lab in this series begins with an empty resource and because Azure resources are potentially billable, it is necessary to remove any Azure resources or services you have created and used in this lab. Unlike previous labs in this series of labs, in this lab, you have created Azure resources using the service management model. For example, you have created a number of cloud services and virtual machines using the service management model. The script used here, therefore, to clean up Azure resources you have created in this lab is significantly more aggressive than other scripts you may have used in this lab series. In other labs, the script to clean up the lab environment deleted only the specific resource groups and the resources in those groups that you created.

This cleanup script will attempt to **delete everything** in your subscription. This script is **not safe** to use if you want to preserve other resources in your subscription: the script will delete those resources as well as the resources you created for the lab. For example, if you used a paid account or an MSDN account that contained pre-existing cloud services, virtual machines, virtual networks, resource groups, etc. Those will be deleted as well.

This script is intended primarily to cleanup those who have acquired an Azure pass account or are using another type of subscription only for these labs. If you care about resources that existed previously in your subscription before doing this lab, do not use this script. Instead, delete the objects you created in this lab manually.

The script does attempt to delete as many resources as possible, but it does not delete all of them. In particular, it does not delete the ASR service. You must delete this manually.

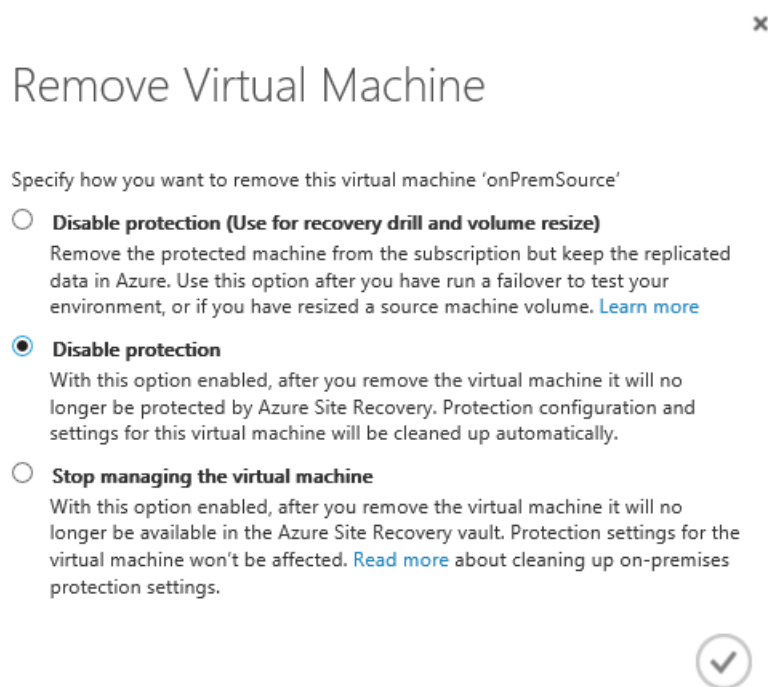
Delete ASR service

In this task, you will manually delete the ASR service you created earlier. This requires that you delete the recovery plan, protection group, configuration server, and the vault.

 Perform the following tasks on **AZRCAMP-ADMIN** logged on as **Contoso\Administrator** using **PasswOrd!** as the password:

1. If not already open, open the full Azure portal.
2. Switch the full Azure portal.
3. In the left navigation, click **ALL ITEMS**.
4. On the all items page, click **ASRVault**.
5. Click **RECOVERY PLANS**.
6. Select **RP-1**.
7. On the command bar, click **DELETE**, and then click **YES**.
8. On the ASRVault page, click **SERVERS**.
9. On the CONFIGURATION SERVERS tab, ensure CONFIGSRV is selected, click **DELETE**.

10. On the Confirm Removal page, in the REASON drop-down, select **Just testing. I'm done now**, and then click **Done**.
11. On the asrvault page, click the **PROTECTED ITEMS** tab.
12. On the PROTECTION GROUPS tab, click **PG-1**.
13. On pg-1 page, ensure **onPremSource** is selected.
14. On the command bar, click **DELETE**, and then click **YES**.
15. On the Remove Virtual Machine page, click **Disable Protection**, and then click **Done**.



16. Ensure that **PG-1** is selected, and then, on the command bar, click **DELETE** and then **YES**.
17. On the command bar, click **DELETE**, and then click **YES**.
✦ This will take 5-10 minutes or more.
18. Once the PROTECTION GROUP has been deleted, click Back to navigate to the recovery services page.
19. Ensure ASRVault is selected, click **DELETE**, and the click **YES**.

Run Lab04Cleanup.ps1 to remove remaining Azure resources

In this task you will run a Windows PowerShell script to remove as many Azure services and resources from a particular subscription as possible.

✦ **NOTE:** You will still have to do some manual cleanup after this script has completed.

⚠ Do NOT use this script if you want to preserve any Azure resources or services outside of those resources you created in the lab.

✎ Perform the following tasks on **AZRCAMP-ADMIN** logged on as **Contoso\Administrator** using **Passw0rd!** as the password:

20. If not already open, open Windows PowerShell ISE.

21. Click **File**, click **Open**, browse to **C:\LabFiles\AZITPROCamp\Lab04**, select **Lab04Cleanup.ps1**, and click **Open**.

✈ This script is also available on GitHub at <https://github.com/AZITCAMP/Labfiles/tree/master/lab04>.

22. On the menu, click **Run**.

23. When prompted, log into your Azure subscription.

✈ The commands to delete the Azure services and resources in your subscription commences. The command may take as long as 10 or 20 minutes to complete.

End of lab