Design Site Recovery and Migration Using Azure Site Recovery

Hands-on lab

Azure Site Recovery is a service that enables organizations to protect their on-premises physical services and virtual machines. Site Recovery 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. Site Recovery may even be used to replicate virtual machines from one Azure region to another, thereby enabling a migration scenario for organizations that wish to move their Azure virtual machines from one region to another.

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

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

Contents

Design Site Recovery and Migration Using Azure Site Recovery

Azure Site Recovery is a service that enables organizations to protect their on-premises physical services and virtual machines. Site Recovery 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. Site Recovery may even be used to replicate virtual machines from one Azure region to another, thereby enabling a migration scenario for organizations that wish to move their Azure virtual machines from one region to another.

Primarily, Site Recovery 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

Site Recovery 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 virtual machines located on one or more Hyper-V servers to Azure (no Virtual Machine Manager (VMM) required).
- **VMMServer to Azure:** Replicate virtual machines from Hyper-V host servers located in a VMM private cloud to host servers in Azure.
- **Physical server to Azure:** Replicate a physical Windows or Linux server to Azure—this deployment type also enables migration of virtual machines from one Azure region to another and is the focus of the exercises in this lab.
- **VMware virtual machines to Azure**: Replicate VMware virtual machines to Azure.
- **VMM Server to secondary datacenter**: Replicate virtual machines 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 server 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 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 subscription 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 Azure portal (both the Azure portal and the Azure classic 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 accidently 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 signed 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 then click **Sign up now**.
3. Follow the on-screen instructions to create a new Microsoft account.

   Please ensure that 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 then follow the on-screen 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 for the life of the Microsoft account.

5. Follow the on-screen instructions to activate a new Azure trial.
6. Navigate to **www.manage.windowsazure.com**, and then sign in.
7. In the 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.

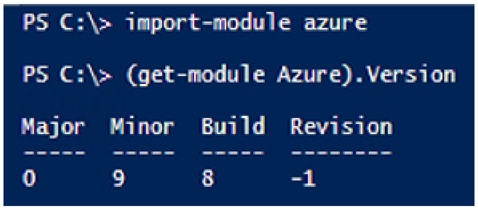
Required Software

1. Microsoft Azure PowerShell - http://go.microsoft.com/?linkid=9811175&clcid=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 to 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 virtual machines 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 the lab environment.

For this course there are four virtual machines 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 virtual machines. To switch to another virtual machine, just click on the appropriate name in the Machines list. Below you will find a listing of the virtual machines 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 synchronization for use in other labs.

The password for all logons in these virtual machines is “Passw0rd!”.

- You can type this in to the virtual machine manually, or use the **Commands→Paste→Paste Password** sequence from the lab environment.
- 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 will demonstrate how to protect on-premises physical servers and how to migrate Azure virtual machines from one region to another using Site Recovery. The reason this lab can meet this 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, 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 Site Recovery process server and the source server you want to protect. These resources are created by running a Windows PowerShell script. In this exercise, you will run the Lab04Start.ps1 script to configure the Azure infrastructure with resources needed for this lab.

> Please only use Windows PowerShell to set up the lab environment.

Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

1. Open **File Explorer**, and then 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 then click **Edit**.

   > The Windows PowerShell ISE console opens.

3. In the Windows PowerShell ISE, on the upper Ribbon, click **Run Script** (green arrow).
4. When prompted, enter a lowercase string that represents your initials, and then press ENTER.

   > Your initials are used to create a unique name 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 then click **Continue**.
6. On the sign in page, enter your password, and then 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, type **Passw0rd!**, and then press ENTER.

At this point, the virtual machines and other resources are provisioned in the East US location. The script will take approximately 10 to 20 minutes to complete.

8. Leave the Windows PowerShell ISE console open for subsequent lab exercises.

Create Site Recovery Target Resources

The Azure Site Recovery target resources include the following:

- **Site Recovery Vault**: Vault for securely storing sensitive configuration information.
- **Configuration Server:** The Site Recovery 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 Azure classic portal.

At the time of this writing Site Recovery is not available using the Resource Manager model.

Create an Azure Site Recovery vault

The Site Recovery vault is the first resource that must be created to configure Azure Site Recovery. The vault serves as a secure repository for sensitive configuration information.

In this exercise, you will create a Site Recovery vault.

Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

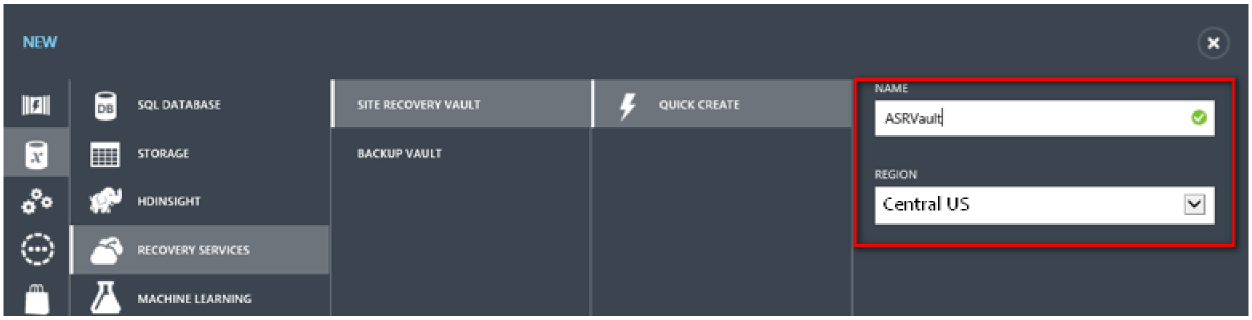
1. Open Microsoft Edge, browse to **https://manage.windowsazure.com**, and then sign in with your subscription.

   At the time of this writing, you can configure the vault using only the Azure classic portal.

2. In the left navigation bar, scroll down, and then 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 **Central US**.

   Do not select any region other than Central US.

   The setup script for this lab created a virtual network in Central US 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 Site Recovery components must be in the same region as well.



NAME: ASRVault

REGION: Central US

7. Click **CREATE VAULT**.
8. Leave the Azure portal open for the next exercise.

Create and configure a configuration server

The configuration server is used for managing Azure Site Recovery.

In this exercise, you will create the configuration server, and then register it in the Site Recovery vault.

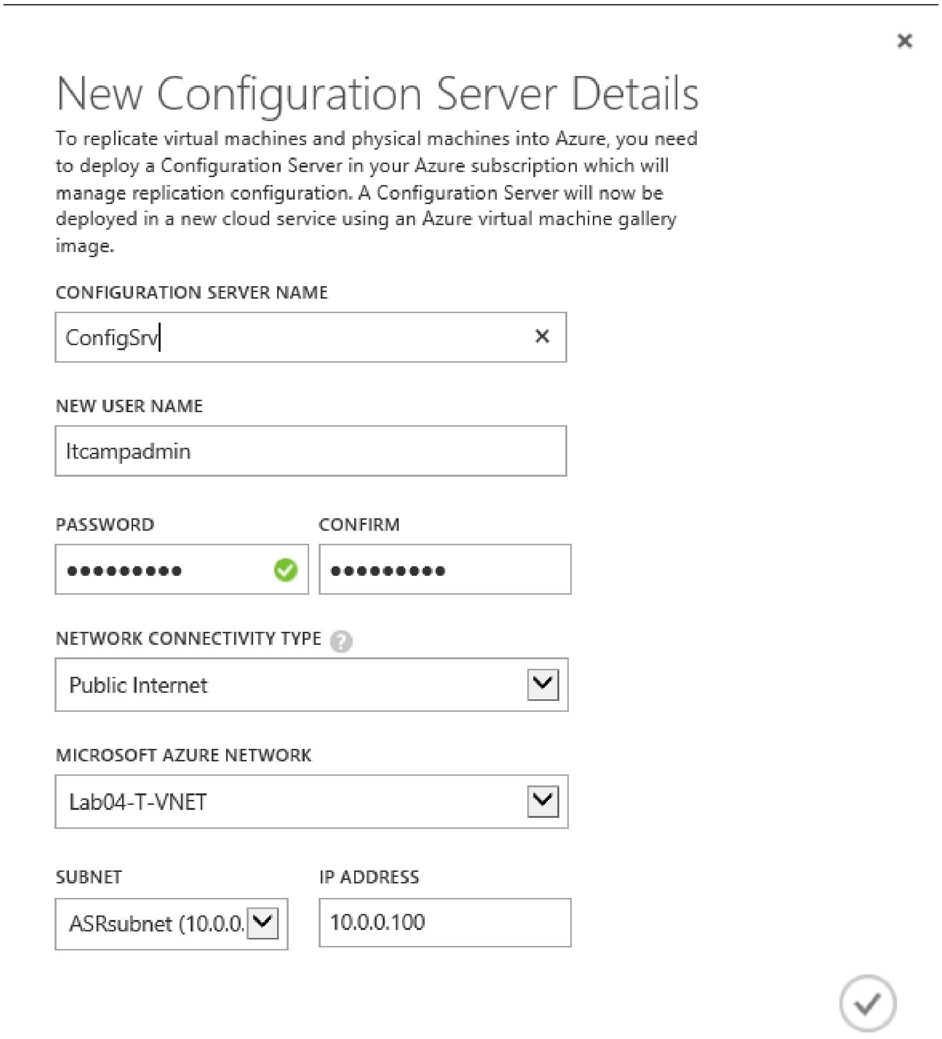
Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

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 :**Itcampadmin**
   - 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: ConfigSrv

NEW USER NAME: Itcampadmin

PASSWORD: ●●●●●●●●●

CONFIRM: ●●●●●●●●●

NETWORK CONNECTIVITY TYPE: Public Internet

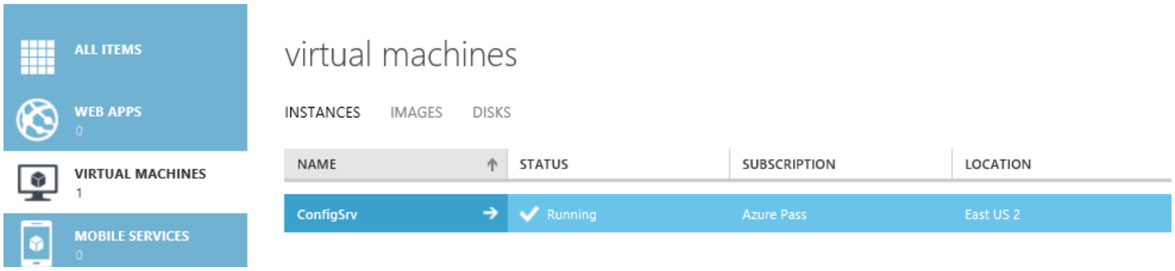
MICROSOFT AZURE NETWORK: Lab04-T-VNET

SUBNET: ASRsubnet (10.0.0.

IP ADDRESS: 10.0.0.100

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.

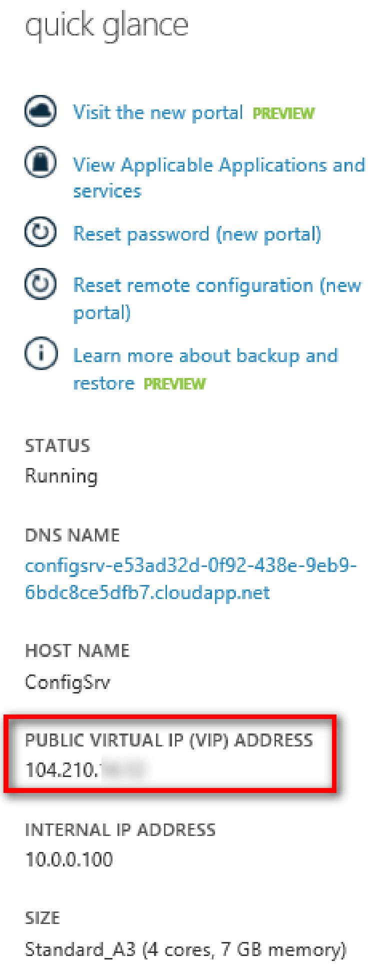
6. Wait until the server provisioning job completes.
7. In the left navigation bar, click **VIRTUAL MACHINES**.



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)

Learn more about backup and restore PREVIEW

STATUS
Running

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

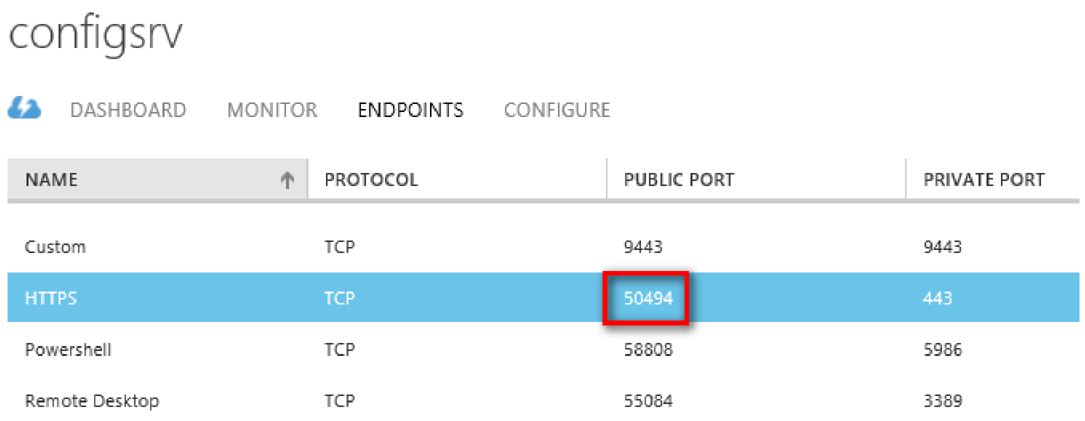
HOST NAME
ConfigSrv

PUBLIC VIRTUAL IP (VIP) ADDRESS
104.210.[redacted]

INTERNAL IP ADDRESS
10.0.0.100

SIZE
Standard_A3 (4 cores, 7 GB memory)

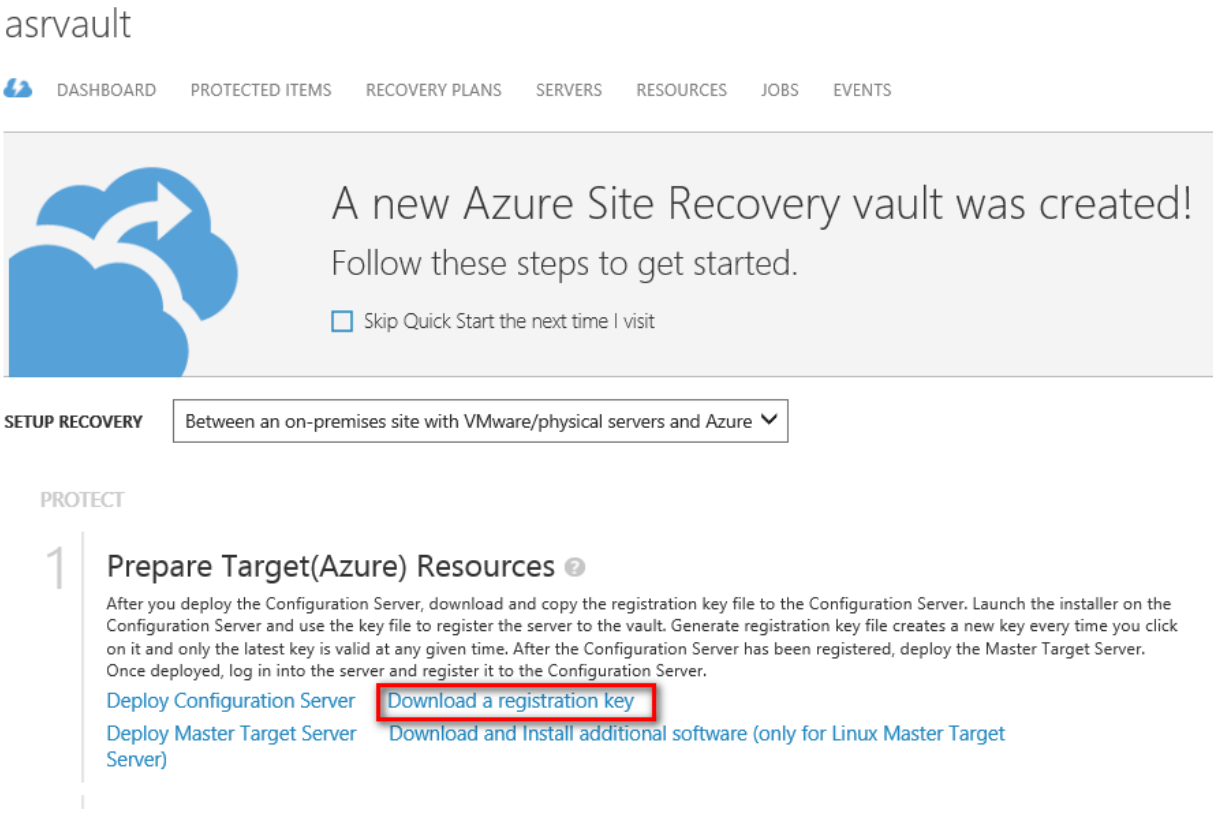
11. On the configsrv page, click **ENDPOINTS**.
12. On the ENDPOINTS tab, identify and record the public port that maps to the HTTPS protocol.
    - You will need to know this port number for subsequent lab steps. Your port number will differ from the one shown in the Screenshot.
    - TIP: put this 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

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 bar, click **RECOVERY SERVICES**.
14. On the recovery services page, click **ASRVault**.
15. On the asrvault page, click **Download a registration key**.



asrvault

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.

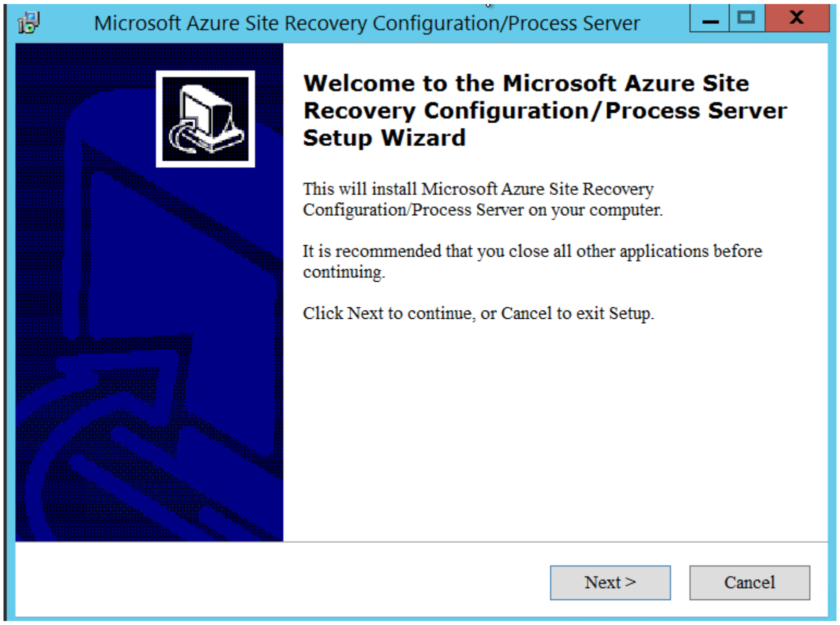
The certificate that is used to register the Configuration Server is valid for 5 days. This is a sensitive file, so it should be protected appropriately.

17. In the left navigation bar, click **VIRTUAL MACHINES**.
18. On the virtual machines page, ensure that **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 then sign in using **Itcampadmin** as the user name and **Passw0rd!** as the password.
22. In the Remote Desktop Connection dialog box, click **Yes**.

   - You are signed in and the desktop starts loading. After a few moments, the Microsoft Azure Site Recovery Configuration/Process Server setup program launches.

   - When the desktop initially loads, you may briefly see a PowerShell window open. Do not close this PowerShell window.



Welcome to the Microsoft Azure Site Recovery Configuration/Process Server Setup Wizard

This will install Microsoft Azure Site Recovery Configuration/Process Server on your computer.

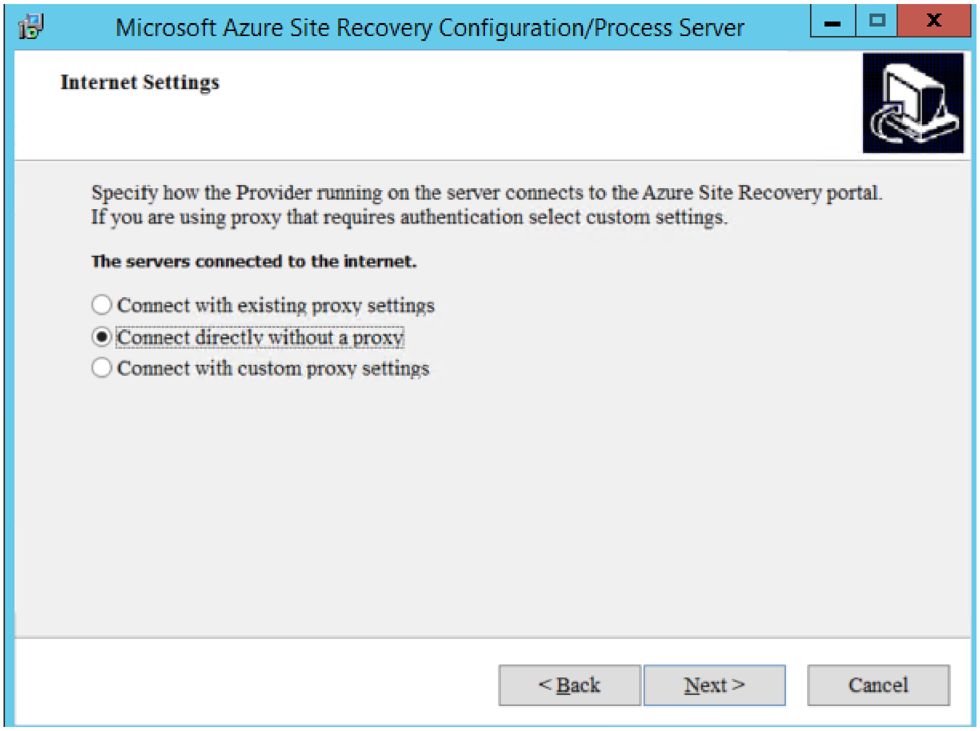
It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

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 then click **Next**.

   - In a production environment, you would choose different, more secure passwords.

26. On the Internet Settings page, click **Connect directly without a proxy**, and then click **Next**.

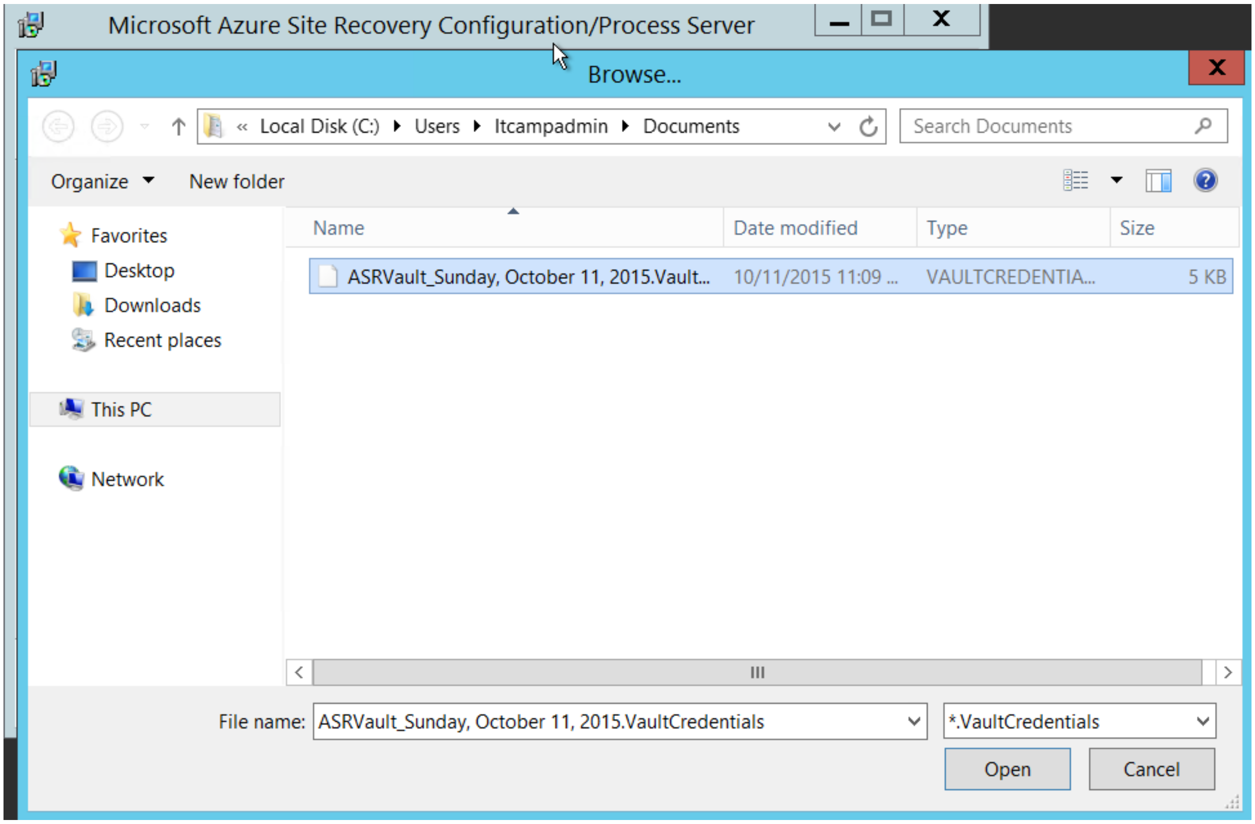


Specify how the Provider running on the server connects to the Azure Site Recovery portal. If you are using proxy that requires authentication select custom settings.

The servers connected to the internet.

○ Connect with existing proxy settings
● Connect directly without a proxy
○ Connect with custom proxy settings

27. On the Provider Error Message Localization Settings page, ensure **English** is selected, and then click **Next**.
28. 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 **AZRCamp-Admin**, your local workstation.
30. Open File Explorer, and then browse to the folder where you saved the .vaultCredentials file you downloaded earlier.
31. Right-click **ASRVault_[date].vaultCredentials**, and then 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.



Name	Date modified	Type	Size
ASRVault_Sunday, October 11, 2015.Vault...	10/11/2015 11:09 ...	VAULTCREDENTIA...	5 KB

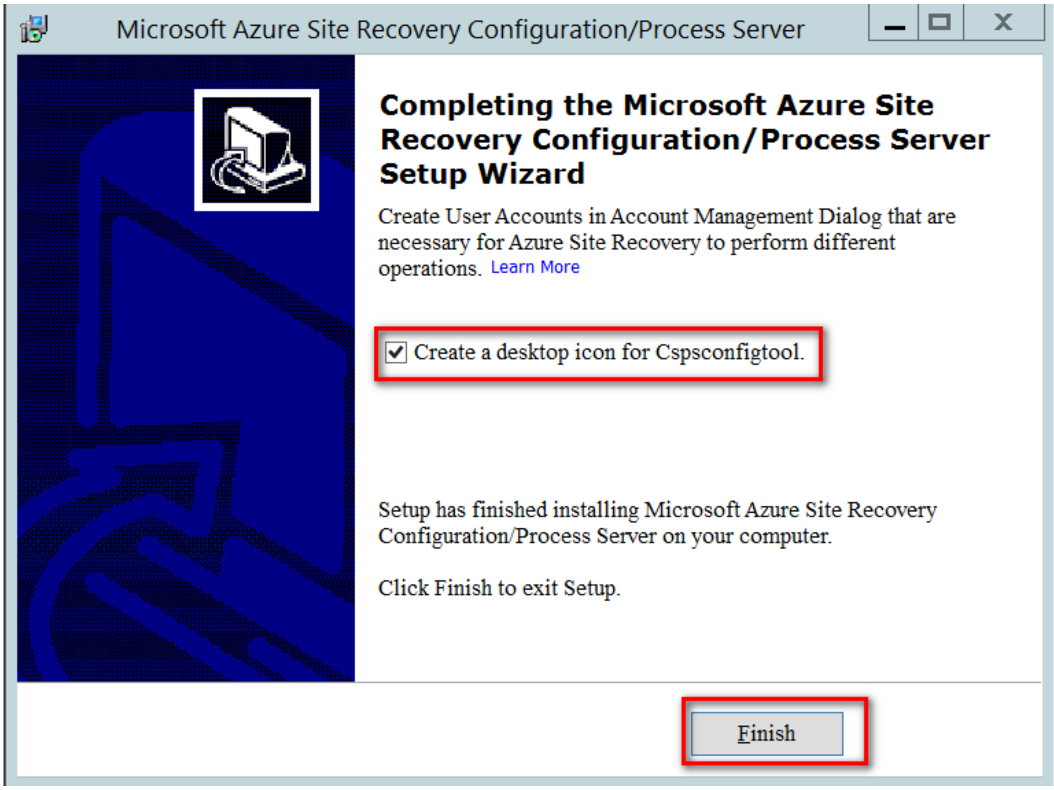
File name: ASRVault_Sunday, October 11, 2015.VaultCredentials

*.VaultCredentials

34. Ensure the file is selected, and then 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 Cspsconfigtool** is selected, and then click **Finish**.


Microsoft Azure Site Recovery Configuration/Process Server

Completing the Microsoft Azure Site Recovery Configuration/Process Server Setup Wizard

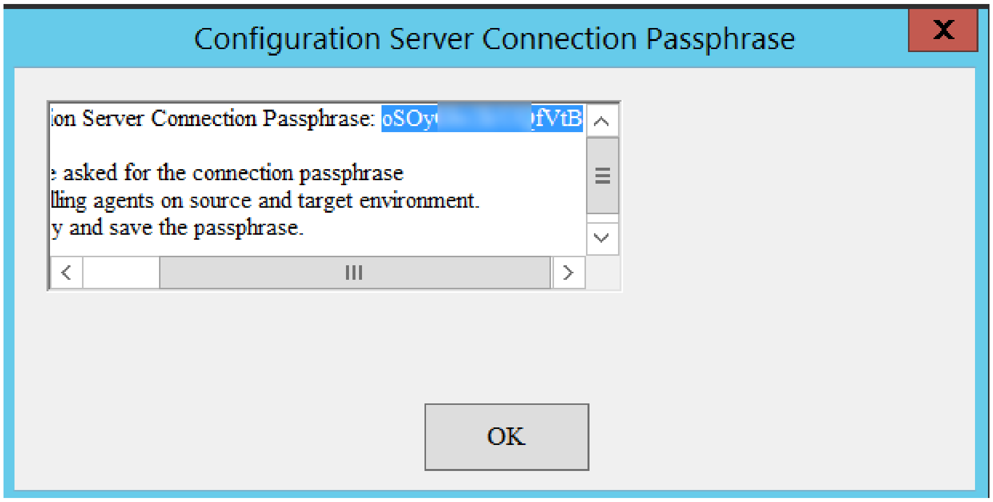
Create User Accounts in Account Management Dialog that are necessary for Azure Site Recovery to perform different operations. Learn More

☑ Create a desktop icon for Cspsconfigtool.

Setup has finished installing Microsoft Azure Site Recovery Configuration/Process Server on your computer.

Click Finish to exit Setup.

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.


Configuration Server Connection Passphrase

ion Server Connection Passphrase: oSOy[redacted]fVtB

: asked for the connection passphrase
lling agents on source and target environment.
y and save the passphrase.

Ensure you copy the entire string.

38. Switch to the local workstation, and then open **Notepad**.

Open 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**.

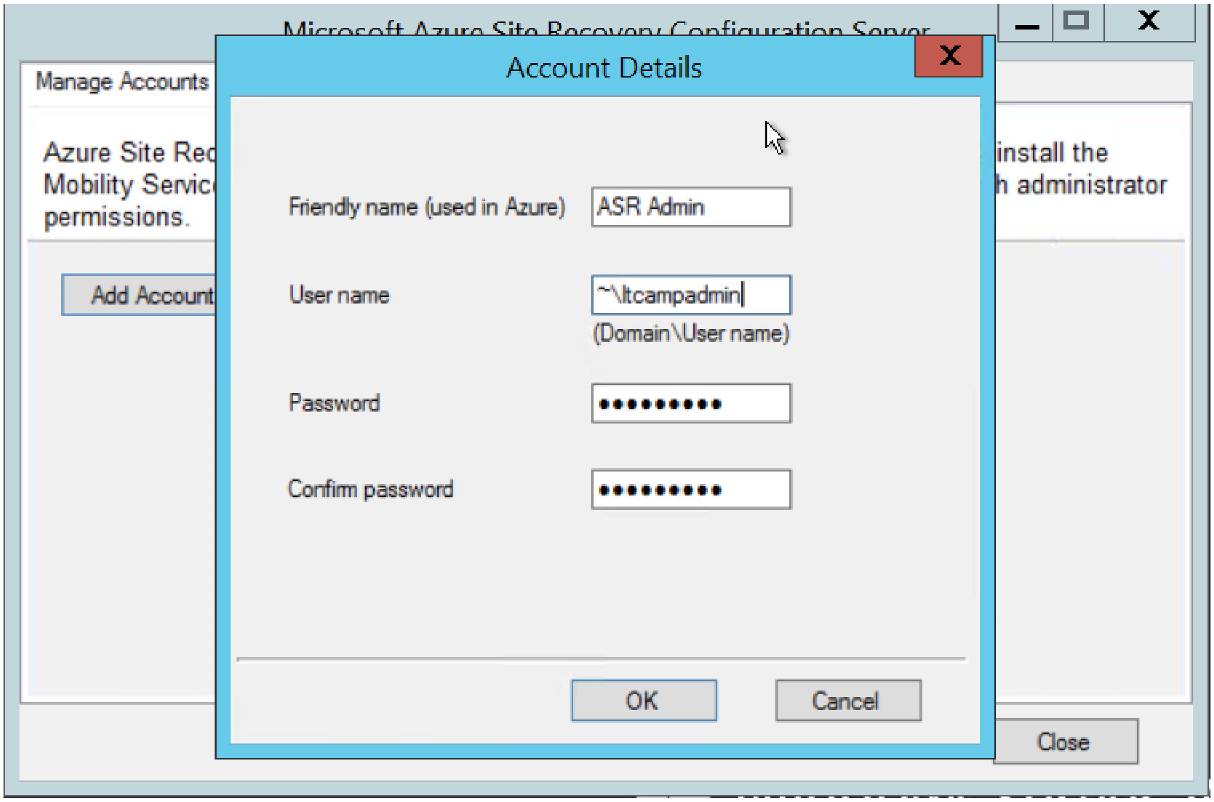
42. In the Configuration Server Passphrase dialog box, click **OK**.

    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: **~\ltcampadmin**
    - Password: **Passw0rd!**
    - Confirm Password: **Passw0rd!**



Account Details

Friendly name (used in Azure): ASR Admin

User name: ~\ltcampadmin
(Domain\User name)

Password: •••••••••

Confirm password: •••••••••

45. Click **OK**.

46. Click **Close**.

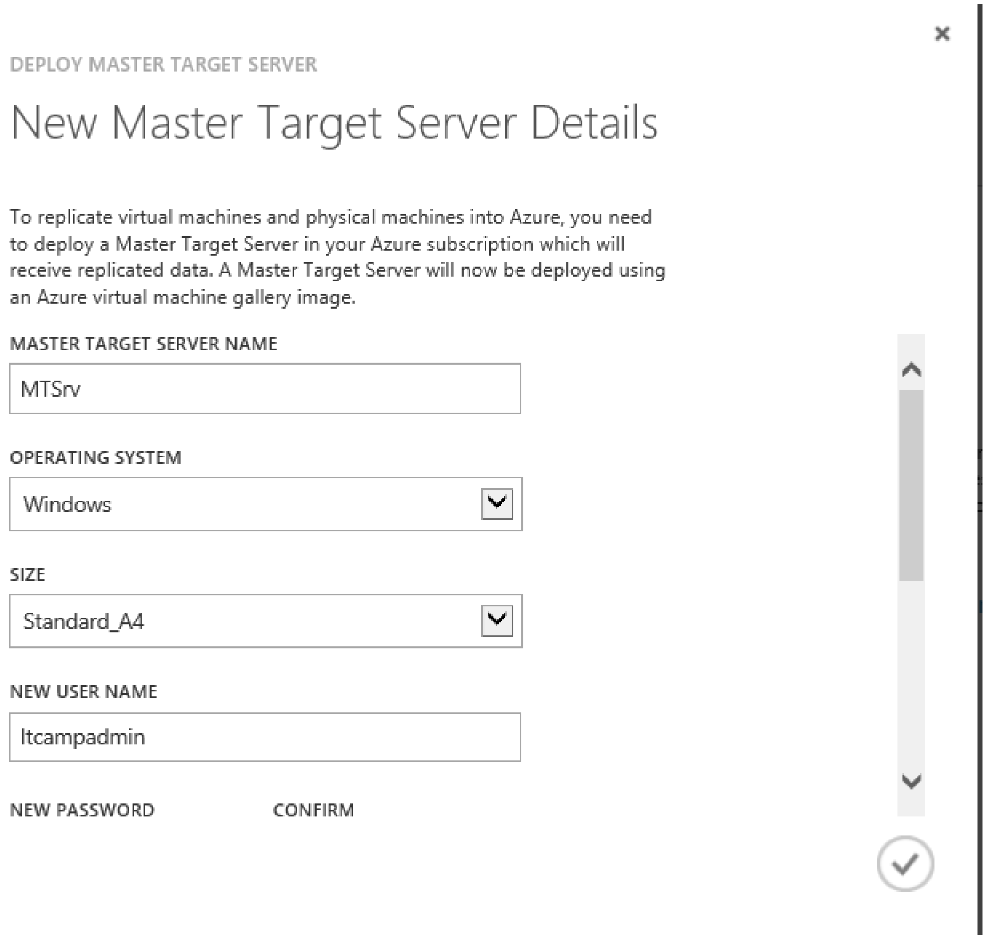
Create and Configure a Master Target Server

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

- Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

1. In the Azure classic portal, in the left navigation bar, 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 Master Target 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

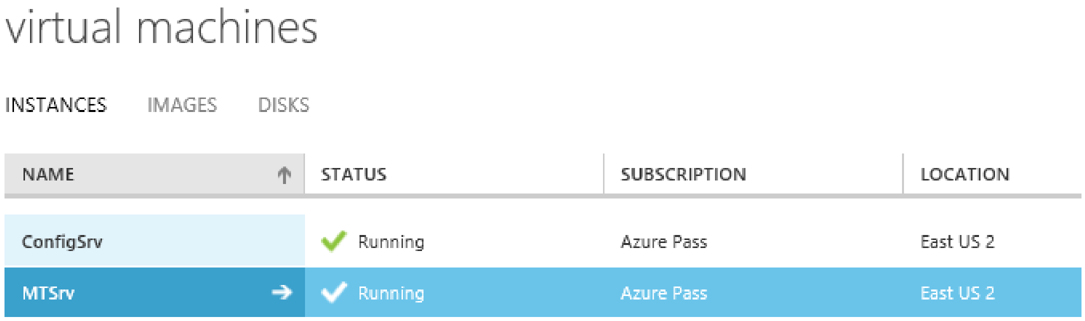
SIZE: Standard_A4

NEW USER NAME: Itcampadmin

NEW PASSWORD

CONFIRM

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



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**.

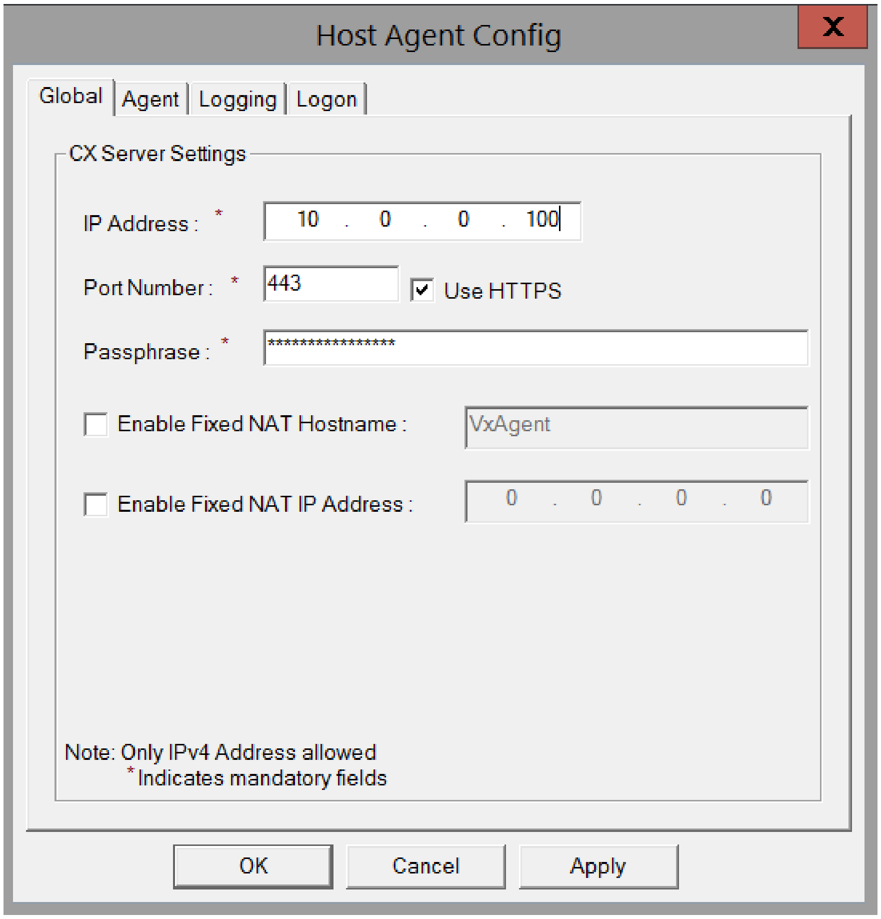
11. In the Windows Security dialog box, click **Use another account**, and then sign in using **Itcampadmin** as the user name and **Passw0rd!** as the password.
12. In the Remote Desktop Connection dialog box, click **Yes**.

When the desktop initially loads, you may briefly see a PowerShell window open. Do not close this PowerShell window.

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 in which you saved 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

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

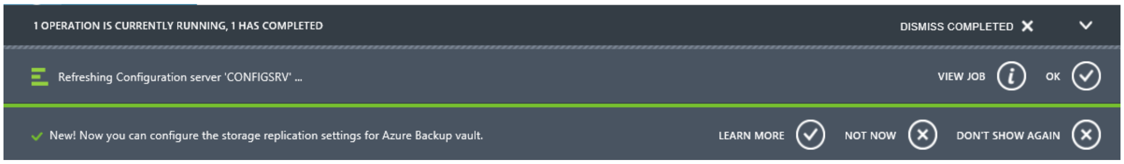
Note: Only IPv4 Address allowed
* Indicates mandatory fields

- 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 Azure classic portal.
19. In the left navigation bar, click **RECOVERY SERVICES**.
20. Click **ASRVault**.
21. On the asrvault page, click **SERVERS**.
22. On the CONFIGURATION SERVERS tab, click **CONFIGSRV**.

- It can take 10 to 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.

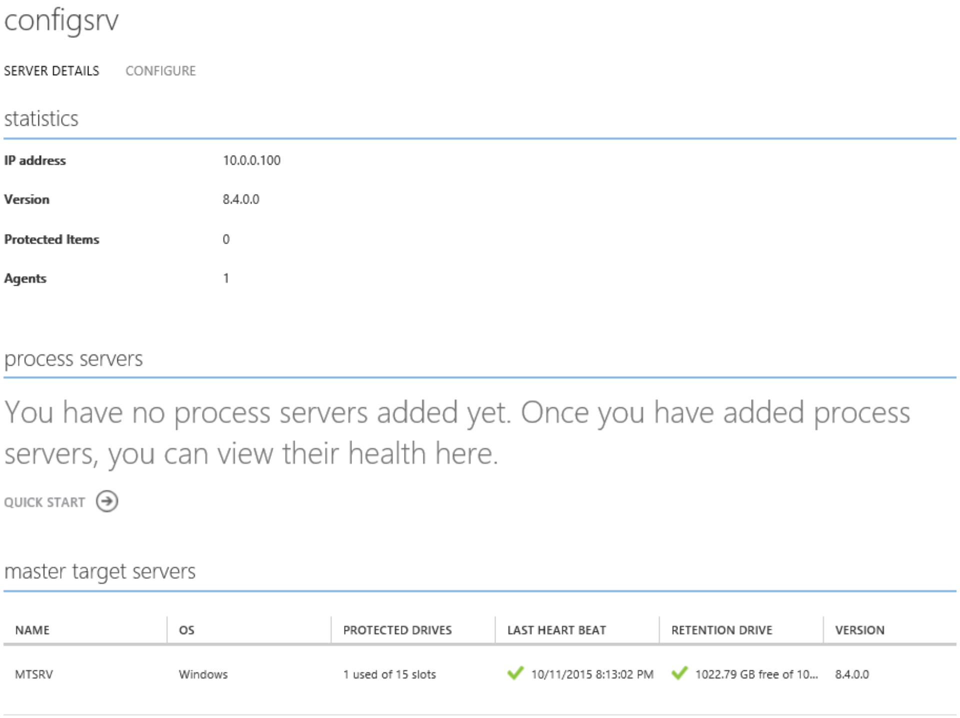


1 OPERATION IS CURRENTLY RUNNING, 1 HAS COMPLETED

Refreshing Configuration server 'CONFIGSRV' ...

✓ New! Now you can configure the storage replication settings for Azure Backup vault.

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.



configsrv

SERVER DETAILS CONFIGURE

statistics

IP address	10.0.0.100
Version	8.4.0.0
Protected Items	0
Agents	1

process servers

You have no process servers added yet. Once you have added process servers, you can view their health here.

QUICK START

master target servers

NAME	OS	PROTECTED DRIVES	LAST HEART BEAT	RETENTION DRIVE	VERSION
MTSRV	Windows	1 used of 15 slots	✓ 10/11/2015 8:13:02 PM	✓ 1022.79 GB free of 10...	8.4.0.0

Configure Site Recovery Source Resources

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

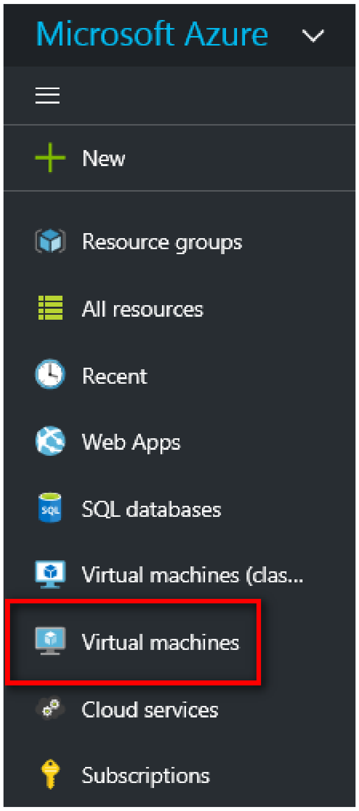
Create and configure the process server

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.

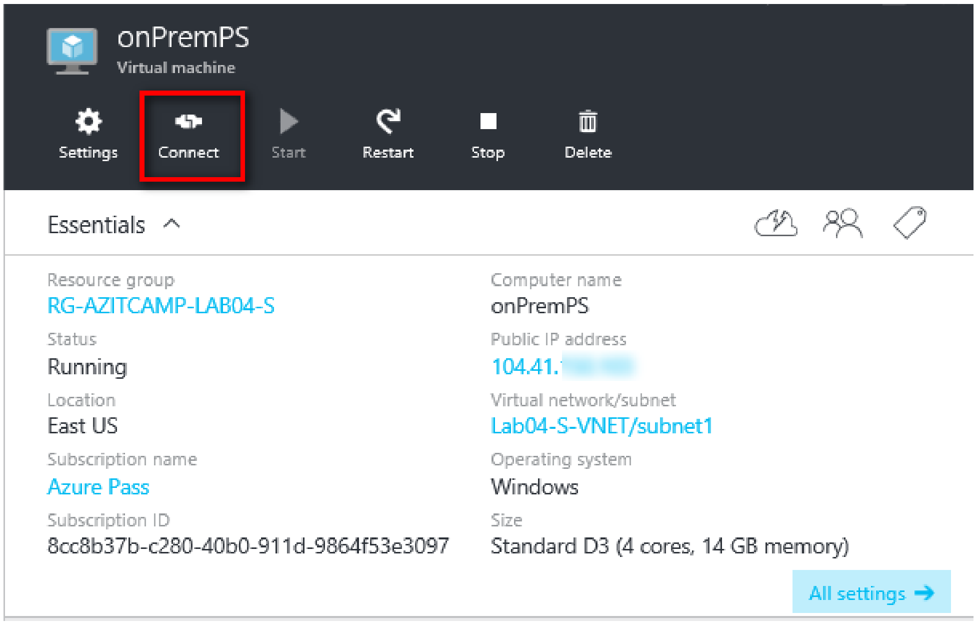
In this exercise, you will configure the process server, and then register it with the configuration server.

- Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

1. In the Azure classic portal, in the upper right, click your account name.
2. In the drop-down list, click **Switch to Azure portal**.
   - The virtual machines that act as the on-premises process server and protected server were created and configured by using an Azure Resource Manager template. They are not available in the Azure classic portal.
3. In the Azure portal, in the left navigation bar, click **Virtual machines**.



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



Resource group
RG-AZITCAMP-LAB04-S

Status
Running

Location
East US

Subscription name
Azure Pass

Subscription ID
8cc8b37b-c280-40b0-911d-9864f53e3097

Computer name
onPremPS

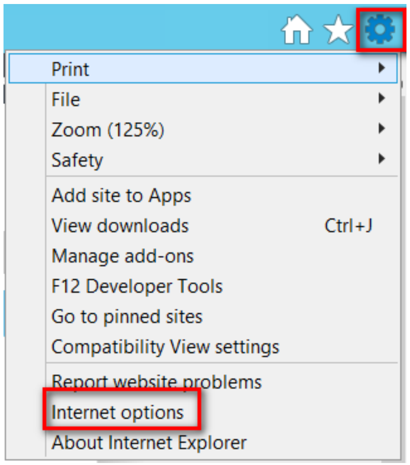
Public IP address
104.41.[redacted]

Virtual network/subnet
Lab04-S-VNET/subnet1

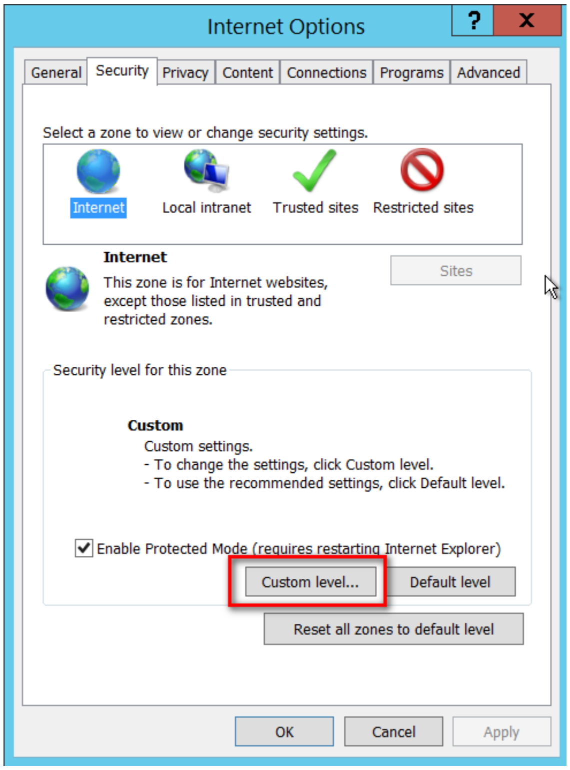
Operating system
Windows

Size
Standard D3 (4 cores, 14 GB memory)

6. Click **Open**, and then sign in to the RDP Session as **Itcampadmin** using the password **Passw0rd!**.
7. On ONPREMPS, open **Internet Explorer**.
8. When prompted to configure Internet Explorer, accept the default settings, and then click **OK**.
9. Browse to **https://manage.windowsazure.com**, and then sign in to the Azure classic 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**.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Sites

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☑ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

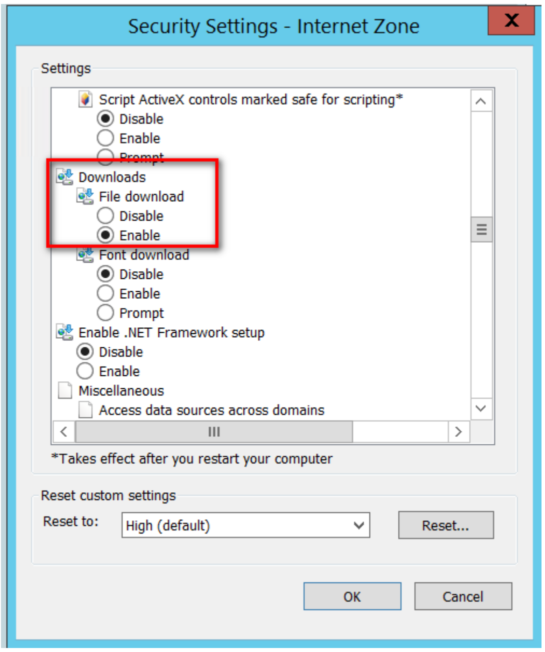
Reset all zones to default level

OK | Cancel | Apply

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.



Security Settings - Internet Zone

Settings

Script ActiveX controls marked safe for scripting*
- ● Disable
- ○ Enable
- ○ Prompt

Downloads
- File download
  - ○ Disable
  - ● Enable
- Font download
  - ● Disable
  - ○ Enable
- ○ Prompt

Enable .NET Framework setup
- ● Disable
- ○ Enable

Miscellaneous
- Access data sources across domains

*Takes effect after you restart your computer

Reset custom settings

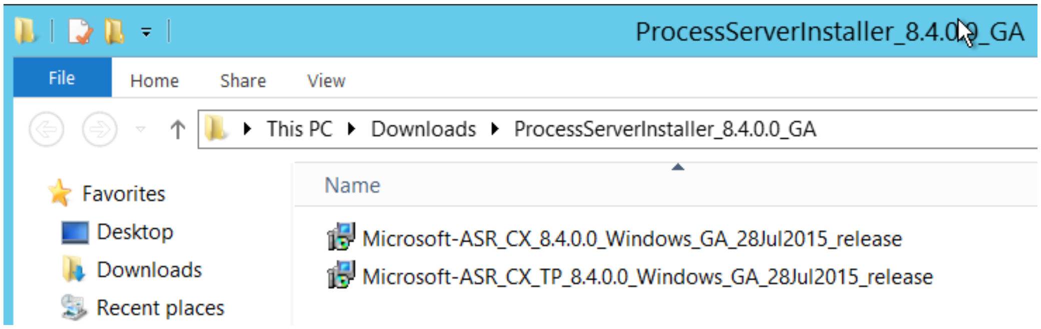
Reset to: High (default) | Reset...

OK | Cancel

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

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

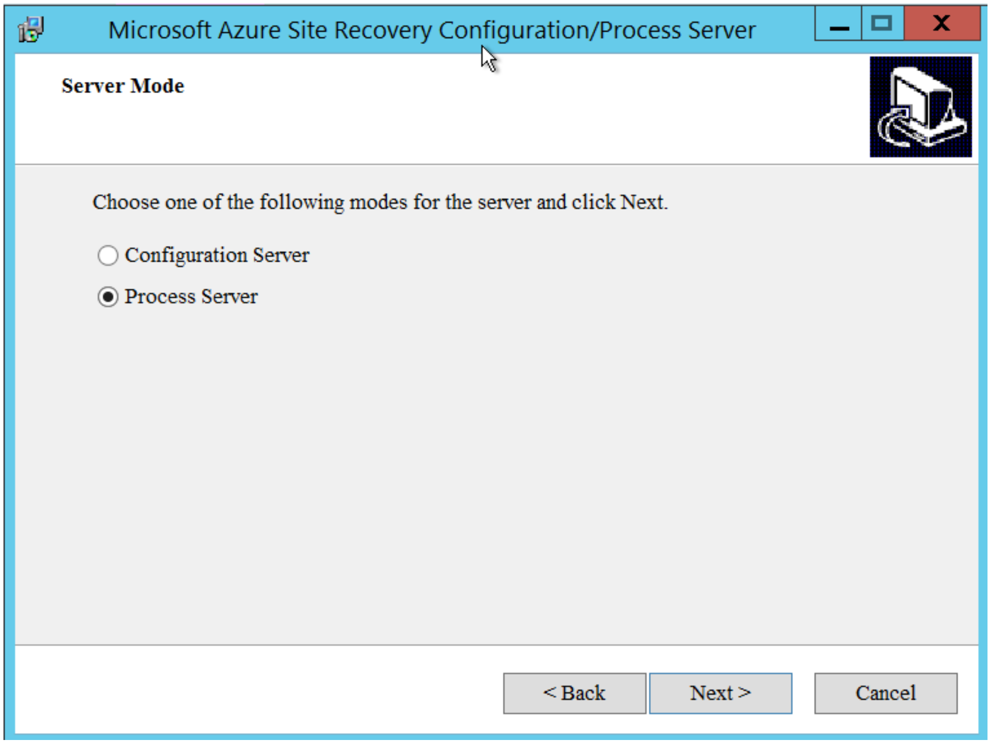
17. Click **ASRVault** to open the quick start page.
18. On the asrvault page, under Prepare Process Servers, click **Download and install Process Server**.
19. Click **Save**.
20. When the download completes, click **Open folder**.
21. Right-click **ProcessServerInstaller_8.4.0.0_GA**, and then click **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 then click **Extract**.
    - Two files are extracted as shown in the Screenshot.



Microsoft-ASR_CX_8.4.0.0_Windows_GA_28Jul2015_release

Microsoft-ASR_CX_TP_8.4.0.0_Windows_GA_28Jul2015_release

23. Double-click **Microsoft-ASR_CX_TP_8.4.0.0_Windows**.
    - This file installs third-party components required for the process server and must be installed first.
24. Click **Run**, and then click **Install**.
25. Click **Finish**.
26. Double-click **Microsoft-ASR_CX _8.4.0.0_Windows**.
27. Click **Run**, and then click **Next**.
28. On the Server Mode page, click **Process Server**, and then click **Next**.



Microsoft Azure Site Recovery Configuration/Process Server

Server Mode

Choose one of the following modes for the server and click Next.

○ Configuration Server

● Process Server

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

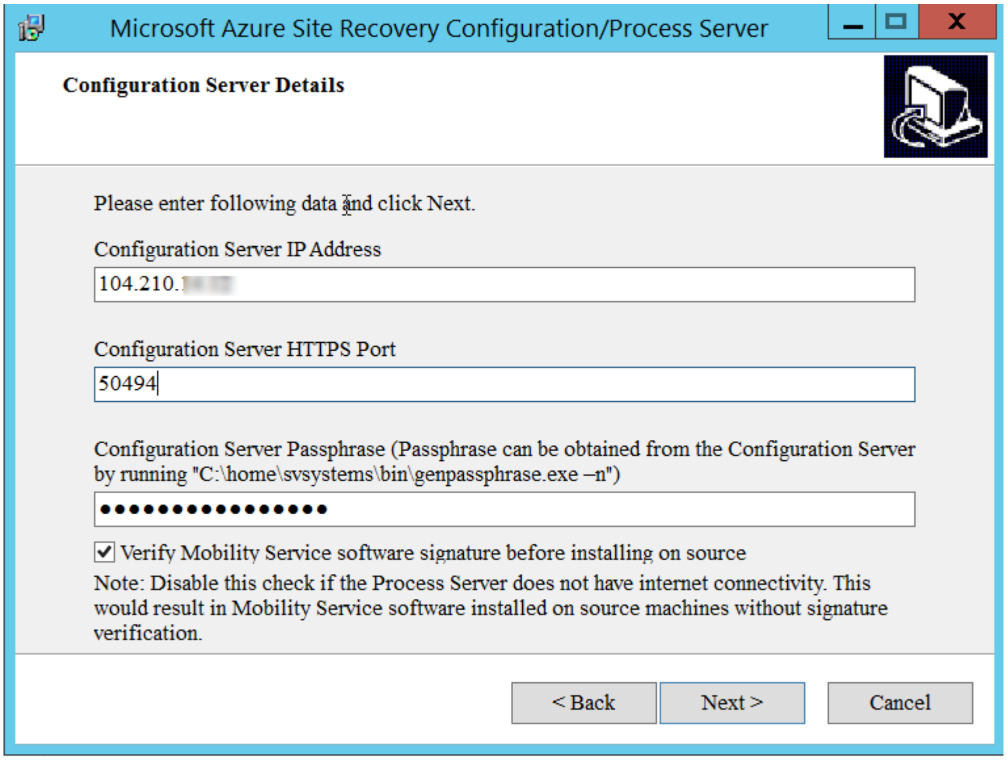
    - The steps for configuring Site Recovery protection for both VMware virtual machines and physical machines are almost identical.

30. On the NIC Selection for Process Server page, click **Next**.

31. 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 in the Screenshot. You recorded this information earlier in the lab.



Configuration Server Details

Please enter following data and click Next.

Configuration Server IP Address

104.210.[redacted]

Configuration Server HTTPS Port

50494

Configuration Server Passphrase (Passphrase can be obtained from the Configuration Server by running "C:\home\svsystems\bin\genpassphrase.exe –n")

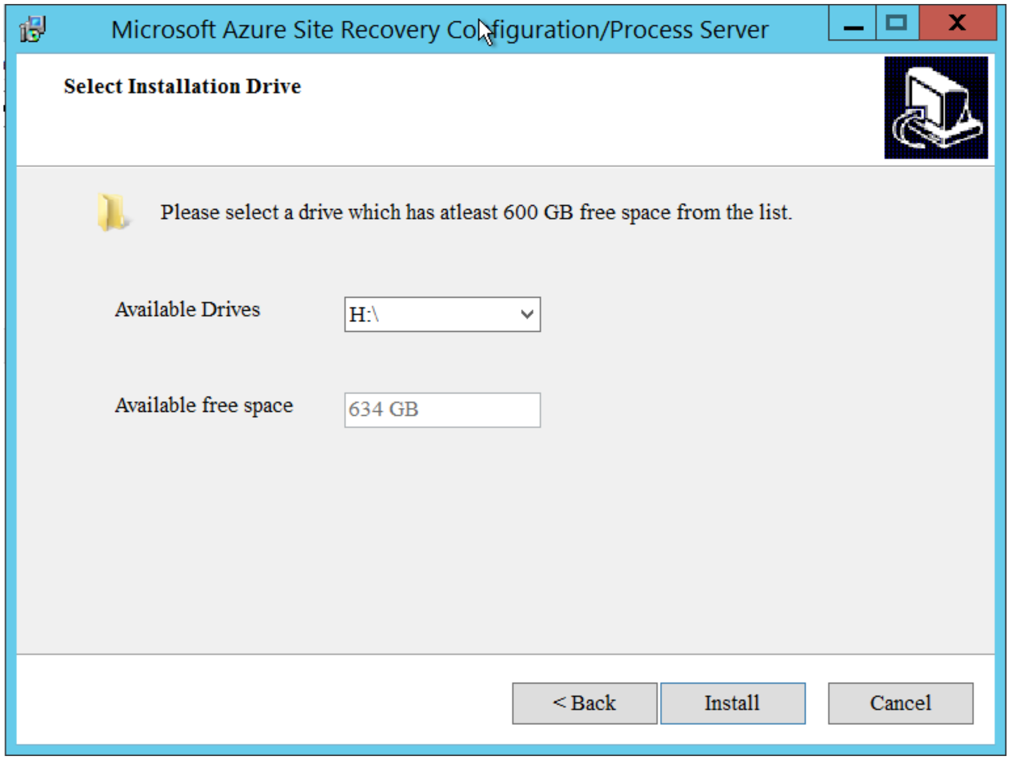
●●●●●●●●●●●●●●●●

☑ Verify Mobility Service software signature before installing on source

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.

32. Click **Next**.
33. 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.



Select Installation Drive

Please select a drive which has atleast 600 GB free space from the list.

Available Drives: H:\

Available free space: 634 GB

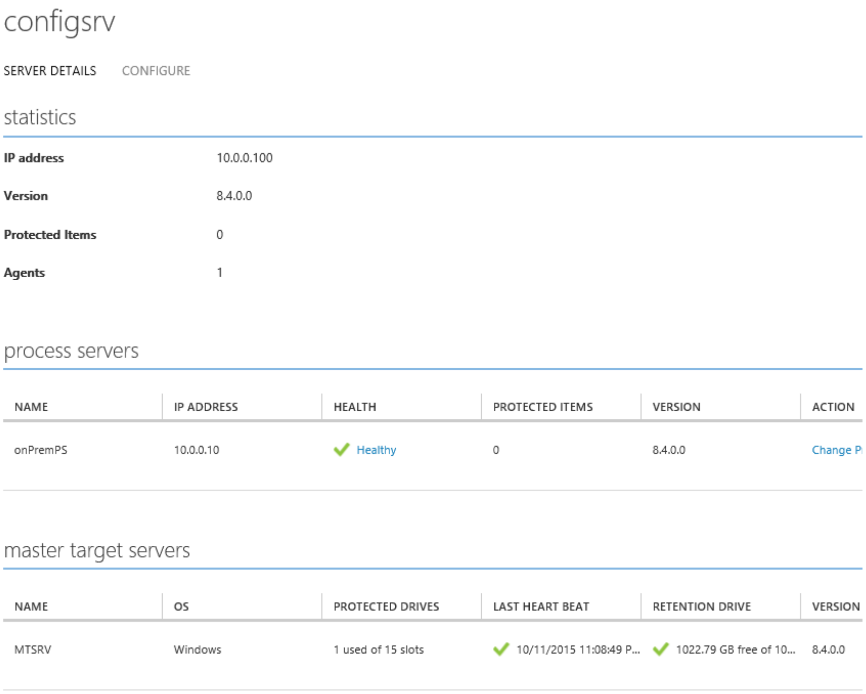
34. On the Completing the Microsoft Azure Site Recovery Configuration/Process Server Setup Wizard page, accept the default to restart the server, and then click **Finish**.
35. In the Setup dialog box, read the notice about the mounting of the H: drive as C:\Home, and then click **OK**.

    The server restarts.

36. On **AZRCamp-Admin**, your local workstation, open the Azure classic portal, if not already open.
37. In the Azure classic portal, in the left navigation bar, click RECOVERY SERVICES.
38. On the Recovery Services page, click **ASRVault**.
39. On the asrvault page, click **SERVERS**.
40. On the CONFIGURATION SERVERS tab, click **CONFIGSRV**.

    It can take 10 to 15 minutes for the process server to be registered.

41. If the process server is not listed on the configsrv page, click **Back** (left arrow).
42. On the command bar, click **REFRESH**, and then wait for the refresh job to complete.
43. Click **CONFIGSRV**.
44. The process server should appear.



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 P

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 Site Recovery Servers

In this 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 (October 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

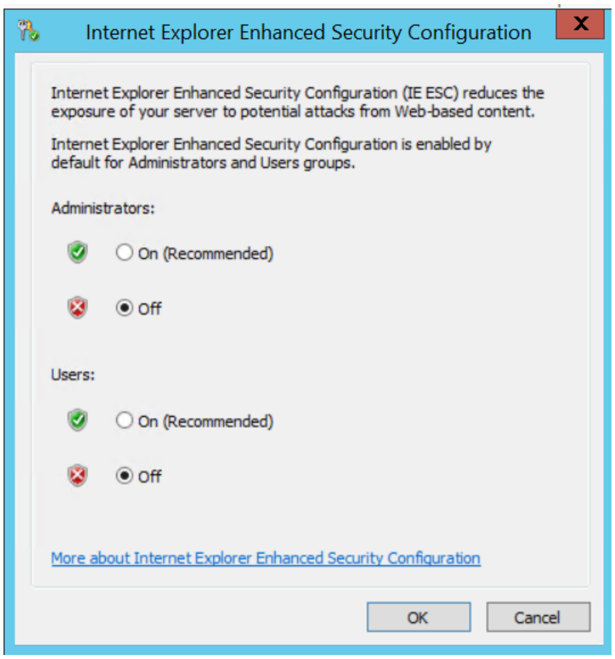
In the lab tasks that follow, please ensure that you follow this order.

Update configuration server

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

Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

1. In the Azure classic portal, in the left navigation bar, 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, sign in as **Itcampadmin** using the password **Passw0rd!**.
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, click **Off**, and then click **OK**.



Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

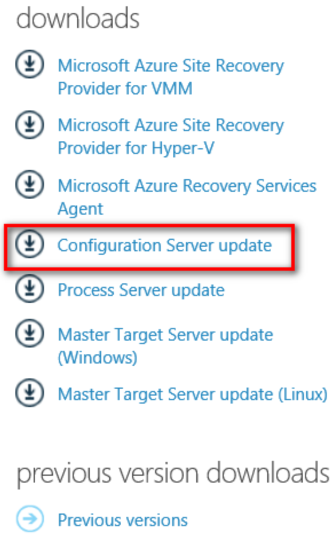
Users:

○ On (Recommended)

● Off

More about Internet Explorer Enhanced Security Configuration

10. Open **Internet Explorer**.
11. When prompted to configure Internet Explorer, accept the default settings, and then click **OK**.
12. Browse to https://manage.windowsazure.com, and then sign in to the Azure classic portal using the credentials associated with your subscription.
13. In the Azure classic portal, in the left navigation bar, 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**.



downloads
Microsoft Azure Site Recovery Provider for VMM
Microsoft Azure Site Recovery Provider for Hyper-V
Microsoft Azure Recovery Services Agent
Configuration Server update
Process Server update
Master Target Server update (Windows)
Master Target Server update (Linux)
previous version downloads
Previous versions

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**.

    - Depending on the circumstances of the current date, there may be no hotfix update. Please ensure that you update the software only if it is appropriate for your particular circumstances.

19. Click **Finish**.

Determine if an update is required for the 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, this software may have been updated.

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

- Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

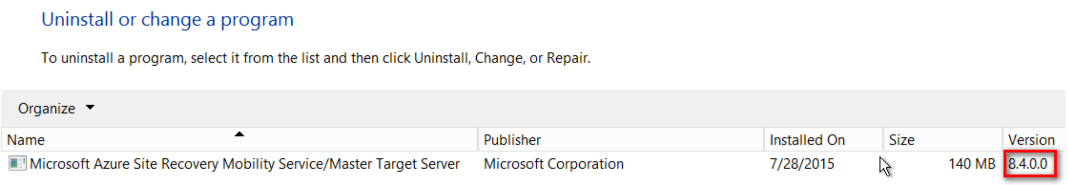
1. Switch to the Azure portal.
2. In the Azure portal, in the left navigation bar, click **Virtual Machines**.
3. On the Virtual machines blade, click **onPremPS**.
4. On the onPremPS blade, click **Connect**.
5. Click **Open**, and then sign in to the RDP Session as **Itcampadmin** using the password **Passw0rd!**.
6. On ONPREMPS, open **Internet Explorer**.
7. When prompted to configure Internet Explorer, accept the default settings, and then click **OK**.
8. Browse to https://manage.windowsazure.com, and then sign in to the Azure classic portal using the credentials associated with your subscription.
9. In the Azure classic portal, in the left navigation bar, 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 an update is required for the master target server

In this exercise, you will determine if the master target server software has been updated, and then take appropriate action.

- Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

1. In the Azure classic portal, in the left navigation bar, 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, sign in as **Itcampadmin** using the password **Passw0rd!**.
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, click **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.



Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Microsoft Azure Site Recovery Mobility Service/Master Target Server	Microsoft Corporation	7/28/2015	140 MB	8.4.0.0

14. Close Control Panel.
15. Open **Internet Explorer**.
16. When prompted to configure Internet Explorer, accept the default settings, and then click **OK**.
17. Browse to https://manage.windowsazure.com, and then sign in to the Azure classic portal using the credentials associated with your subscription.
18. In the Azure classic portal, in the left navigation bar, 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.
    - If the software version is the same as you determined earlier in this exercise, you do not need to take any action. Click **Cancel**.
    - 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 protection.

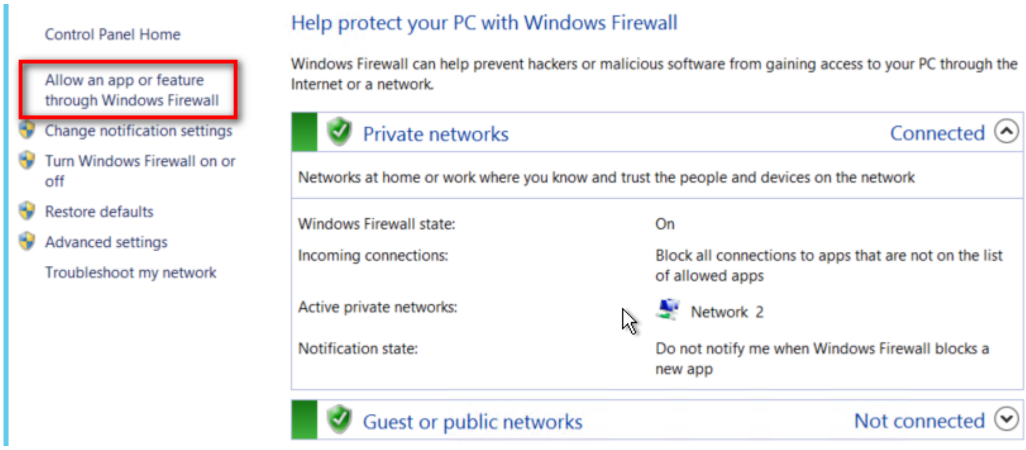
Configure source server

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 exercise, you will modify the local firewall rules, and then examine the previously modified registry value.

Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

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


Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Private networks
Connected
Guest or public networks
Not connected

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

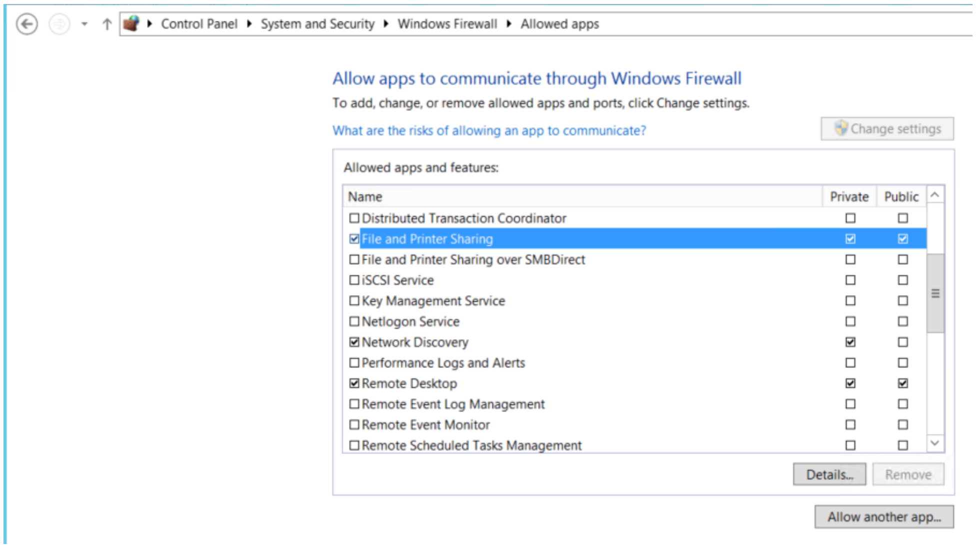
Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network 2

Notification state: Do not notify me when Windows Firewall blocks a new app

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

    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.



Control Panel ▸ System and Security ▸ Windows Firewall ▸ Allowed apps

Allow apps to communicate through Windows Firewall

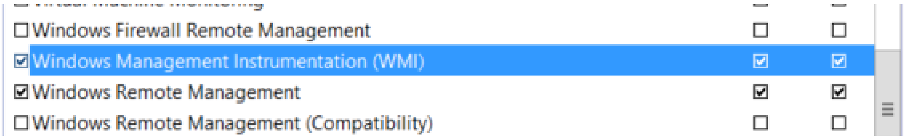
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☐ Distributed Transaction Coordinator	☐	☐
☑ File and Printer Sharing	☑	☑
☐ File and Printer Sharing over SMBDirect	☐	☐
☐ iSCSI Service	☐	☐
☐ Key Management Service	☐	☐
☐ Netlogon Service	☐	☐
☑ Network Discovery	☑	☐
☐ Performance Logs and Alerts	☐	☐
☑ Remote Desktop	☑	☑
☐ Remote Event Log Management	☐	☐
☐ Remote Event Monitor	☐	☐
☐ Remote Scheduled Tasks Management	☐	☐

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

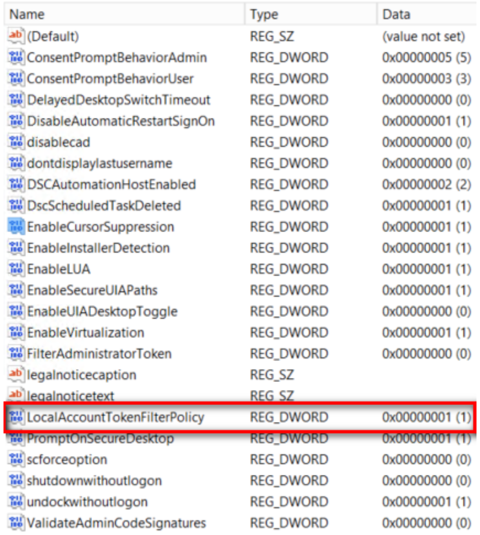


☐ Windows Firewall Remote Management	☐	☐
☑ Windows Management Instrumentation (WMI)	☑	☑
☑ Windows Remote Management	☑	☑
☐ Windows Remote Management (Compatibility)	☐	☐

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)
DscScheduledTaskDeleted	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)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000000 (0)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)

19. Close the 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.

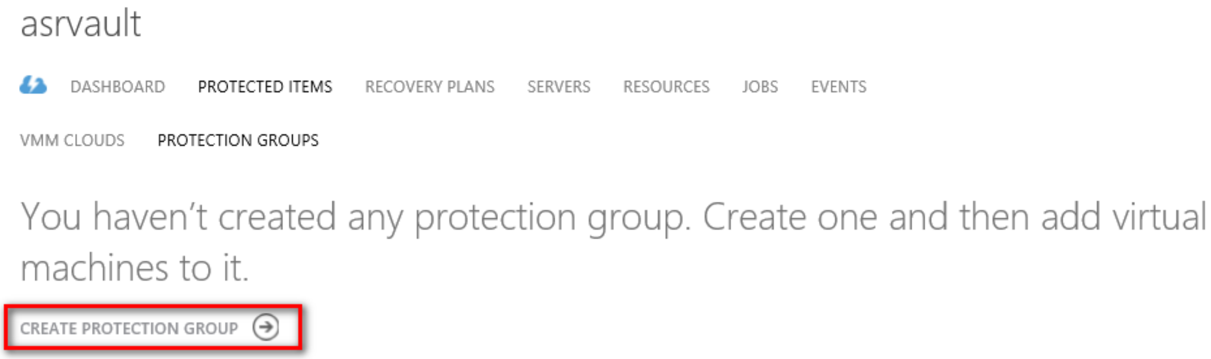
21. Switch to **AZRCamp-Admin**, the local workstation.

Create a protection group

In this exercise, you will create a protection group.

Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

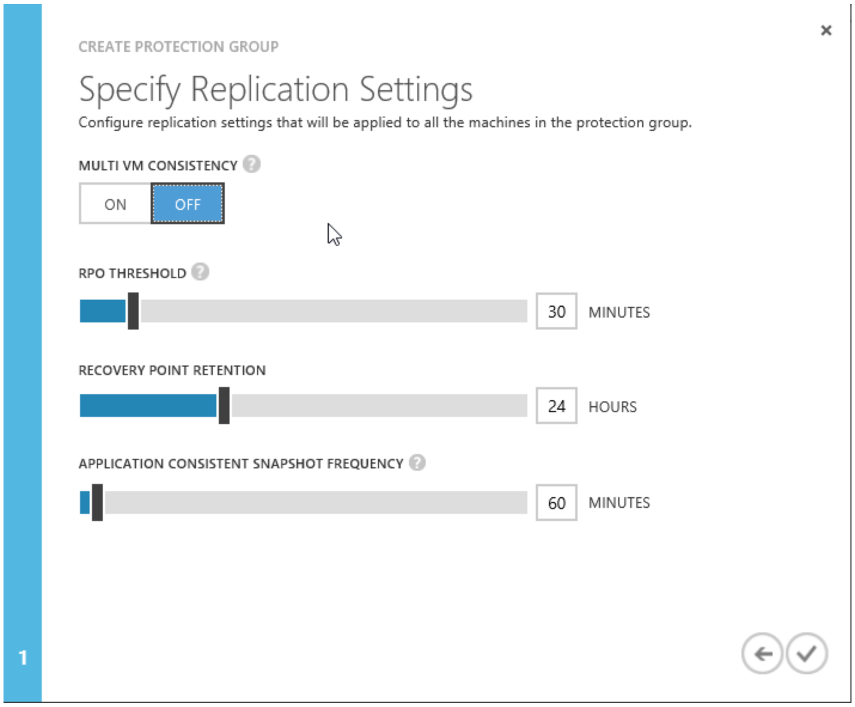
1. In the Azure classic portal, in the left navigation bar, click **RECOVERY SERVICES**.
2. Click **ASRVault** to open the quick start page.
3. Click **PROTECTED ITEMS**, and then click **CREATE PROTECTION GROUP**.



asrvault

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

4. 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).
5. 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 (selected)

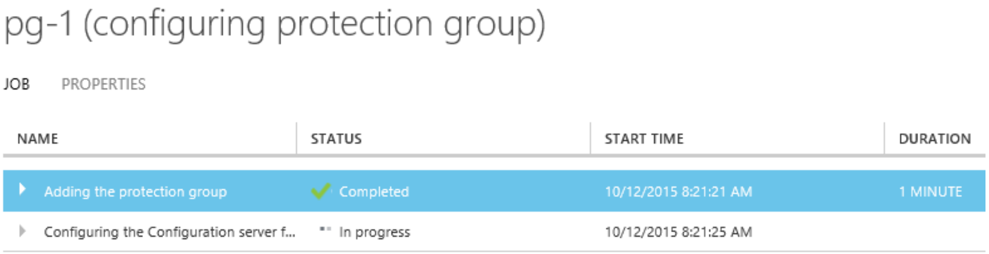
RPO THRESHOLD: 30 MINUTES

RECOVERY POINT RETENTION: 24 HOURS

APPLICATION CONSISTENT SNAPSHOT FREQUENCY: 60 MINUTES

6. Wait for the **Create Protection Group** job to complete.

You can monitor the progress of the job by selecting the appropriate job from the JOB page of the Site Recovery vault. The job should complete within a minute or two.



pg-1 (configuring protection group)

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	

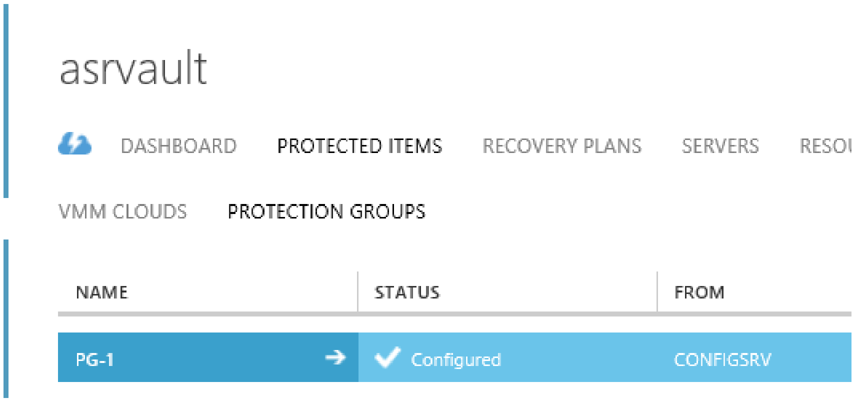
Add a machine to a protection group

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

In this exercise, you will add a virtual 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 tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

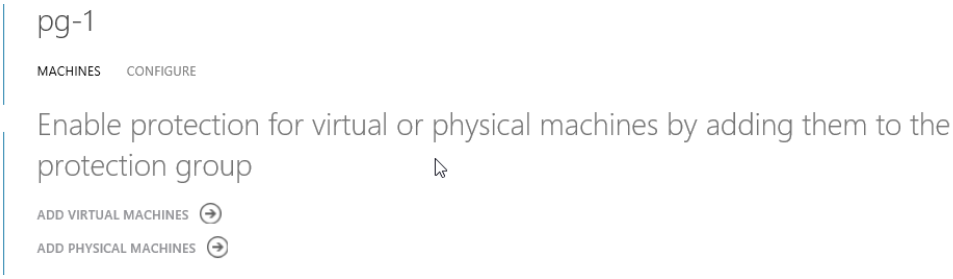
1. In the Azure classic portal, in the left navigation bar, click **RECOVERY SERVICES**.
2. Click **ASRVault** to open the quick start page.
3. Click **PROTECTED ITEMS**.
4. Click **PG-1**.



NAME	STATUS	FROM
PG-1	✓ Configured	CONFIGSRV

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

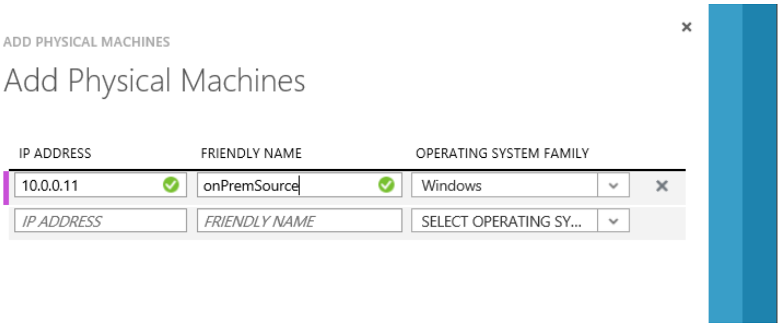
If you wanted to protect virtual machines running on VMware, you would select ADD VIRTUAL MACHINES.



Enable protection for virtual or physical machines by adding them to the protection group

6. On the Add Physical Machines page, enter the following information, and then 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.



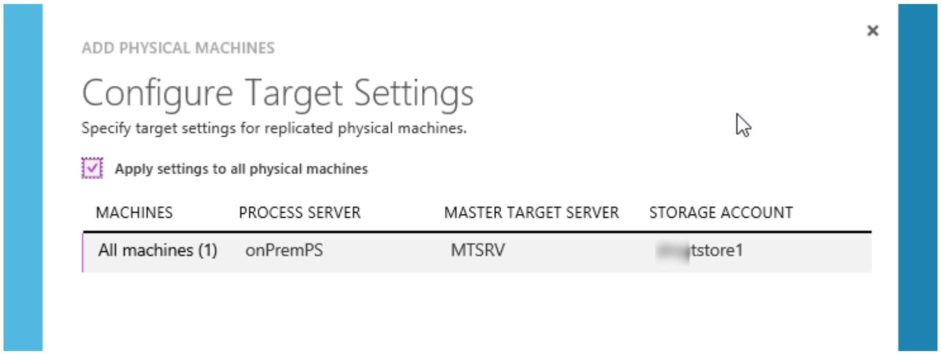
ADD PHYSICAL MACHINES

Add Physical Machines

IP ADDRESS	FRIENDLY NAME	OPERATING SYSTEM FAMILY
10.0.0.11	onPremSource	Windows
IP ADDRESS	FRIENDLY NAME	SELECT OPERATING SY...

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

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



ADD PHYSICAL MACHINES

Configure Target Settings

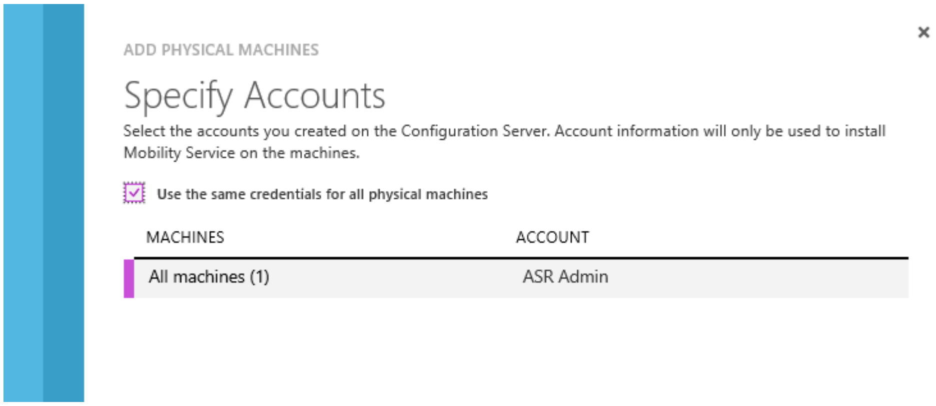
Specify target settings for replicated physical machines.

☑ Apply settings to all physical machines

MACHINES	PROCESS SERVER	MASTER TARGET SERVER	STORAGE ACCOUNT
All machines (1)	onPremPS	MTSRV	[redacted]tstore1

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

The job to configure protection of onPremSource starts.



ADD PHYSICAL MACHINES

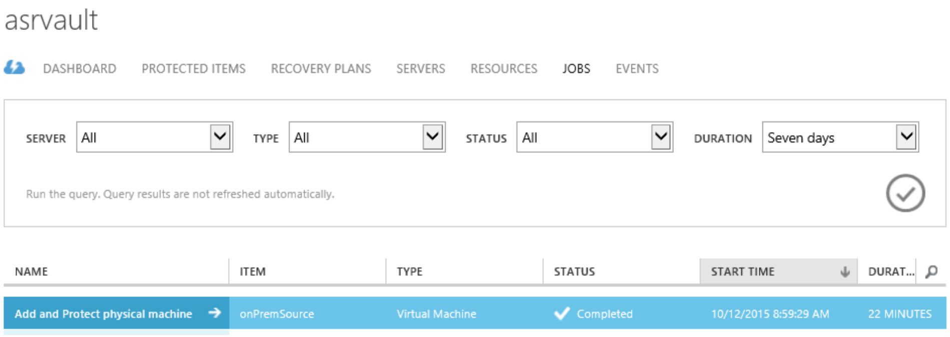
Specify Accounts

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**.



asrvault

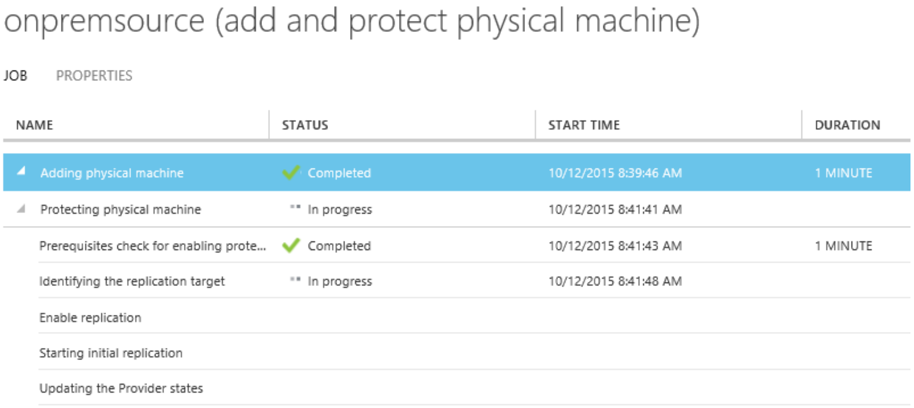
SERVER All TYPE All STATUS All DURATION Seven days

Run the query. Query results are not refreshed automatically.

NAME	ITEM	TYPE	STATUS	START TIME	DURAT...
Add and Protect physical machine	onPremSource	Virtual Machine	✓ Completed	10/12/2015 8:59:29 AM	22 MINUTES

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

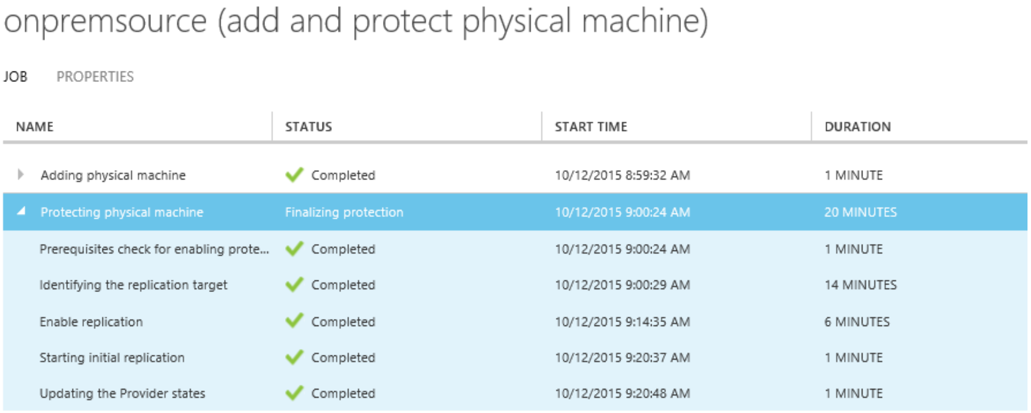
    This allows you to view progress of the job in detail.



onpremsource (add and protect physical machine)

NAME	STATUS	START TIME	DURATION
Adding physical machine	✓ Completed	10/12/2015 8:39:46 AM	1 MINUTE
Protecting physical machine	In progress	10/12/2015 8:41:41 AM	
Prerequisites check for enabling prote...	✓ Completed	10/12/2015 8:41:43 AM	1 MINUTE
Identifying the replication target	In progress	10/12/2015 8:41:48 AM	
Enable replication			
Starting initial replication			
Updating the Provider states			

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

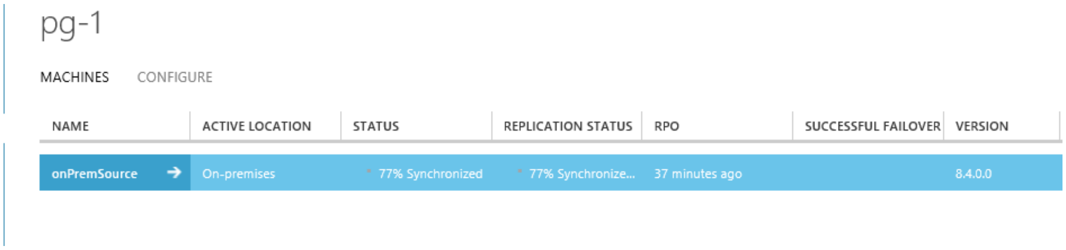


onpremsource (add and protect physical machine)

NAME	STATUS	START TIME	DURATION
Adding physical machine	✓ Completed	10/12/2015 8:59:32 AM	1 MINUTE
Protecting physical machine	Finalizing protection	10/12/2015 9:00:24 AM	20 MINUTES
Prerequisites check for enabling prote...	✓ Completed	10/12/2015 9:00:24 AM	1 MINUTE
Identifying the replication target	✓ Completed	10/12/2015 9:00:29 AM	14 MINUTES
Enable replication	✓ Completed	10/12/2015 9:14:35 AM	6 MINUTES
Starting initial replication	✓ Completed	10/12/2015 9:20:37 AM	1 MINUTE
Updating the Provider states	✓ Completed	10/12/2015 9:20:48 AM	1 MINUTE

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



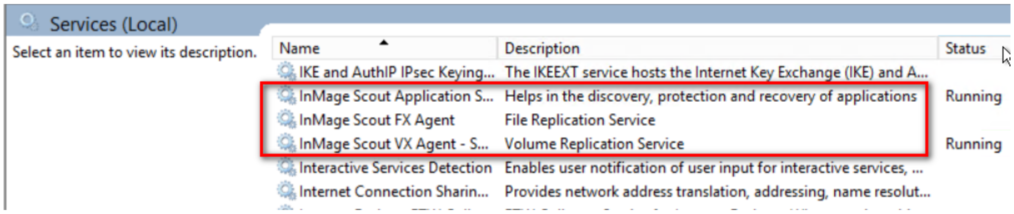
pg-1

MACHINES CONFIGURE

NAME	ACTIVE LOCATION	STATUS	REPLICATION STATUS	RPO	SUCCESSFUL FAILOVER	VERSION
onPremSource	On-premises	77% Synchronized	77% Synchronize...	37 minutes ago		8.4.0.0

15. Establish an RDP session with **OnPremSource**.
16. Open the 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.

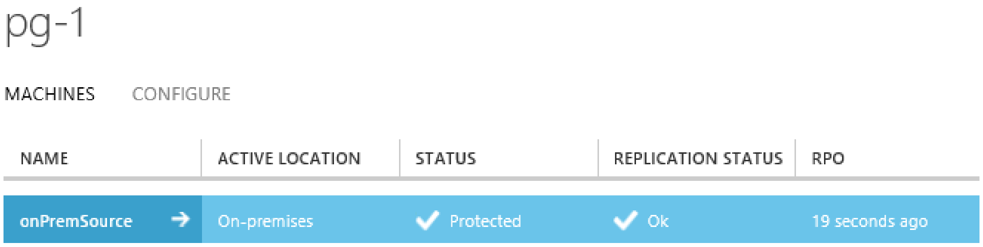


Services (Local)

Select an item to view its description.

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...	

17. Wait until the synchronization job completes before proceeding to the next exercise.



pg-1

MACHINES CONFIGURE

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 Site Recovery, it is possible to modify the protected machine properties.

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

- Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

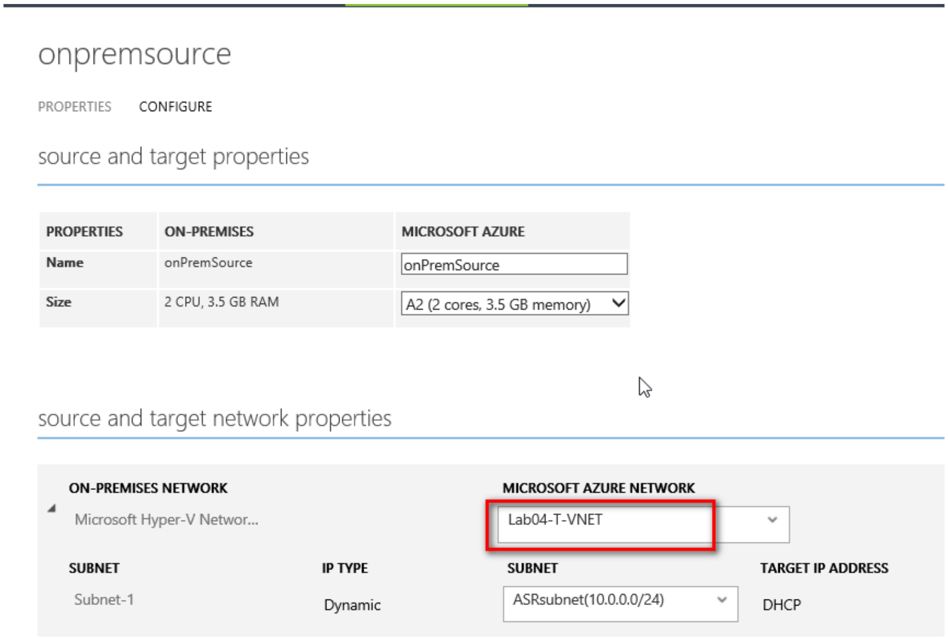
1. In the Azure classic portal, in the left navigation bar, click **RECOVERY SERVICES**.
2. Click **ASRVault** to open the quick start page.
3. Click **PROTECTED ITEMS**.

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 onpremsource 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.



onpremsource

source and target properties

PROPERTIES	ON-PREMISES	MICROSOFT AZURE
Name	onPremSource	onPremSource
Size	2 CPU, 3.5 GB RAM	A2 (2 cores, 3.5 GB memory)

source and target network properties

ON-PREMISES NETWORK		MICROSOFT AZURE NETWORK	
Microsoft Hyper-V Networ...		Lab04-T-VNET	
SUBNET	IP TYPE	SUBNET	TARGET IP ADDRESS
Subnet-1	Dynamic	ASRsubnet(10.0.0.0/24)	DHCP

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

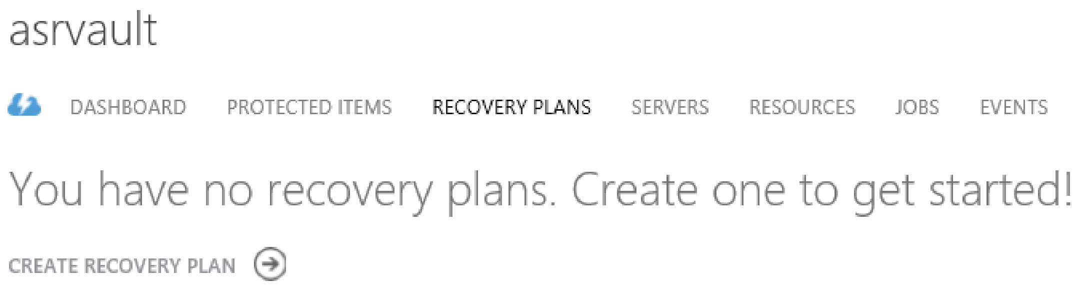
Create a recovery plan

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

- Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

1. In the Azure classic portal, click the **back** (left) arrow until you reach the asrvault page.

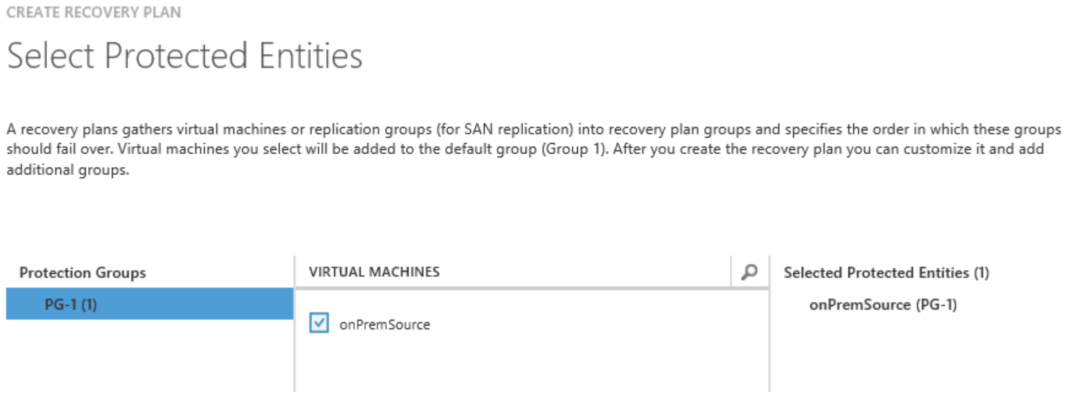
2. On the asrvault page, click **RECOVERY PLANS**.
3. Click **CREATE RECOVERY PLAN**.



asrvault

You have no recovery plans. Create one to get started!

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



CREATE RECOVERY PLAN

Select Protected Entities

A recovery plans gathers virtual machines or replication groups (for SAN replication) into recovery plan groups and specifies the order in which these groups should fail over. Virtual machines you select will be added to the default group (Group 1). After you create the recovery plan you can customize it and add additional groups.

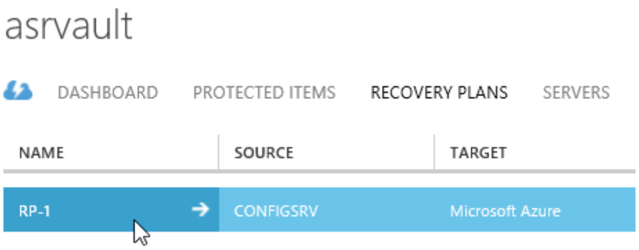
Protection Groups	VIRTUAL MACHINES	Selected Protected Entities (1)
PG-1 (1)	☑ onPremSource	onPremSource (PG-1)

Perform an unplanned failover

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

Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Administrator** using the password **Passw0rd!**.

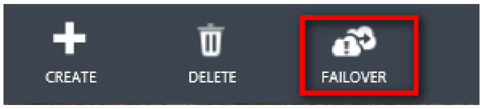
1. In the Azure classic portal, on the asrvault page, ensure that **RP-1** is selected in the RECOVERY PLANS tab.



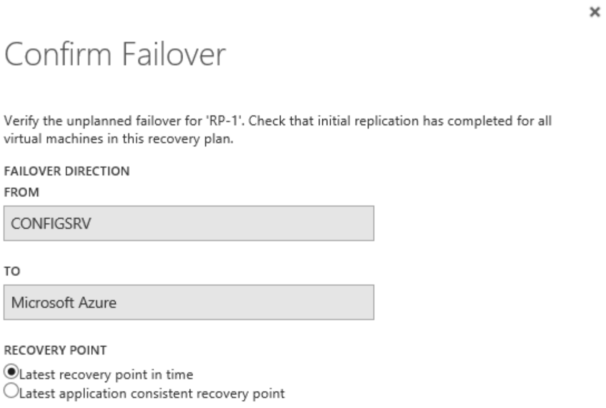
asrvault

NAME	SOURCE	TARGET
RP-1	CONFIGSRV	Microsoft Azure

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



3. On the Confirm Failover page, review the information, accept the default settings, and then 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

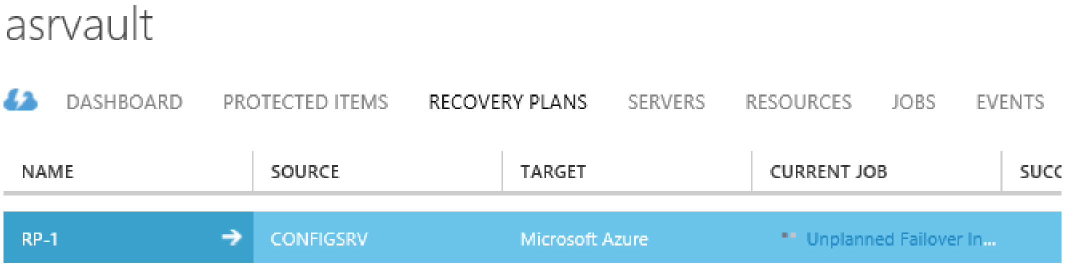
RECOVERY POINT

● Latest recovery point in time

○ Latest application consistent recovery point

The job to failover to the Central US region begins.

4. On the asrvault page, on the RECOVERY PLANS tab, review the **RP-1** job.

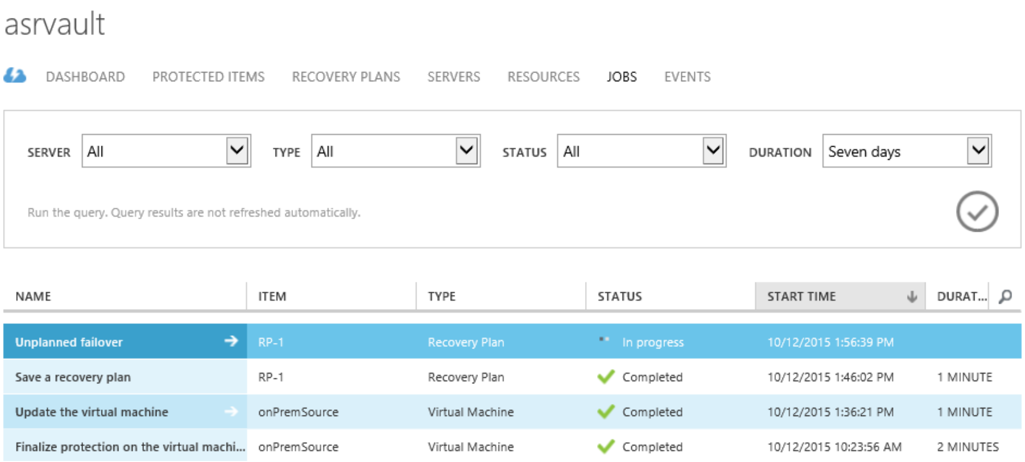


asrvault

NAME	SOURCE	TARGET	CURRENT JOB	SUCC
RP-1	CONFIGSRV	Microsoft Azure	Unplanned Failover In...	

5. Click the **JOBS** tab.

6. On the JOBS tab, click **Unplanned failover**.

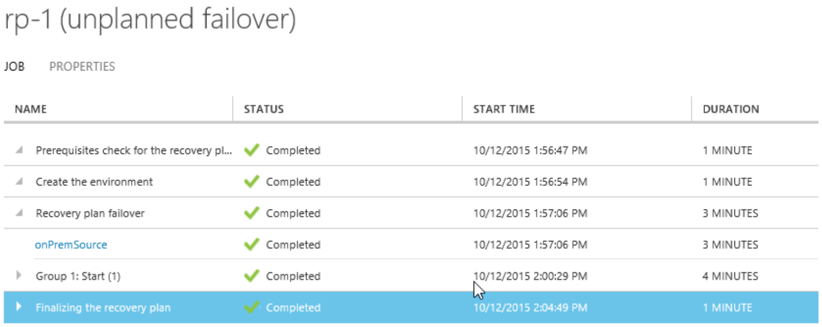


SERVER All TYPE All STATUS All DURATION Seven days

Run the query. Query results are not refreshed automatically.

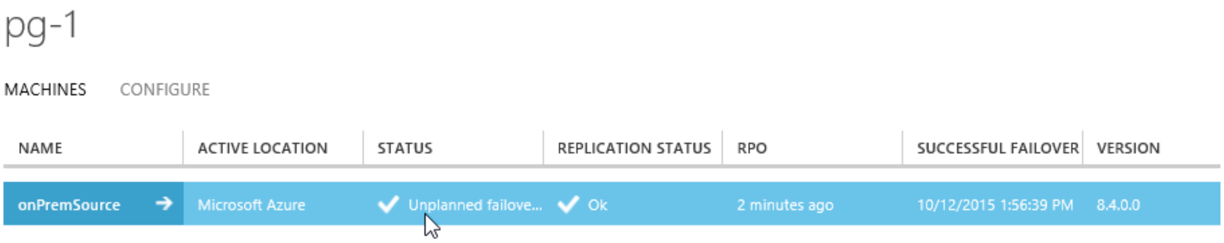
NAME	ITEM	TYPE	STATUS	START TIME	DURAT...
Unplanned failover	RP-1	Recovery Plan	In progress	10/12/2015 1:56:39 PM	
Save a recovery plan	RP-1	Recovery Plan	✓ Completed	10/12/2015 1:46:02 PM	1 MINUTE
Update the virtual machine	onPremSource	Virtual Machine	✓ Completed	10/12/2015 1:36:21 PM	1 MINUTE
Finalize protection on the virtual machi...	onPremSource	Virtual Machine	✓ Completed	10/12/2015 10:23:56 AM	2 MINUTES

7. Wait until the rp-1 (unplanned failover) job has completed, as shown in the Screenshot, before proceeding to the next task.



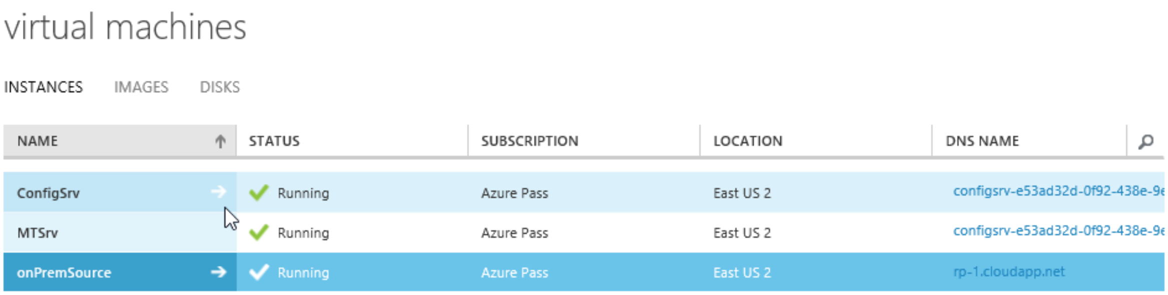
NAME	STATUS	START TIME	DURATION
Prerequisites check for the recovery pl...	✓ Completed	10/12/2015 1:56:47 PM	1 MINUTE
Create the environment	✓ Completed	10/12/2015 1:56:54 PM	1 MINUTE
Recovery plan failover	✓ Completed	10/12/2015 1:57:06 PM	3 MINUTES
onPremSource	✓ Completed	10/12/2015 1:57:06 PM	3 MINUTES
Group 1: Start (1)	✓ Completed	10/12/2015 2:00:29 PM	4 MINUTES
Finalizing the recovery plan	✓ Completed	10/12/2015 2:04:49 PM	1 MINUTE

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



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

11. In the Azure classic portal, in the left navigation bar, click **VIRTUAL MACHINES**.
    - The onPremSource virtual machine is available in the Central US location 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

NAME	STATUS	SUBSCRIPTION	LOCATION	DNS NAME
ConfigSrv	✓ Running	Azure Pass	East US 2	configsrv-e53ad32d-0f92-438e-9e
MTSrv	✓ Running	Azure Pass	East US 2	configsrv-e53ad32d-0f92-438e-9e
onPremSource	✓ Running	Azure Pass	East US 2	rp-1.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 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 clean up the account for 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 Site Recovery service. You must delete this manually.

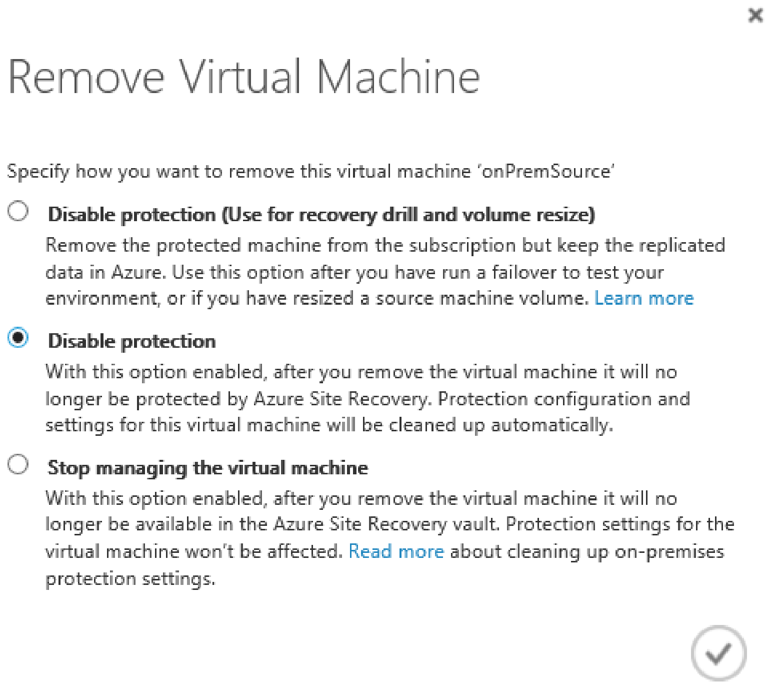
Delete the Site Recovery service

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

- Perform the tasks in this exercise on **AZRCamp-Admin** signed in as **Contoso\Administrator** using the password **Passw0rd!**.

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

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



Remove Virtual Machine

Specify how you want to remove this virtual machine 'onPremSource'

○ **Disable protection (Use for recovery drill and volume resize)**
Remove the protected machine from the subscription but keep the replicated data in Azure. Use this option after you have run a failover to test your environment, or if you have resized a source machine volume. Learn more

● **Disable protection**
With this option enabled, after you remove the virtual machine it will no longer be protected by Azure Site Recovery. Protection configuration and settings for this virtual machine will be cleaned up automatically.

○ **Stop managing the virtual machine**
With this option enabled, after you remove the virtual machine it will no longer be available in the Azure Site Recovery vault. Protection settings for the virtual machine won't be affected. Read more about cleaning up on-premises protection settings.

15. Ensure that **PG-1** is selected, and then, on the command bar, click **DELETE**, and then click **YES**.
16. On the command bar, click **DELETE**, and then click **YES**.

   This will take 5 to 10 minutes or more.

17. Once the PROTECTION GROUP has been deleted, click **Back** to navigate to the recovery services page.
18. Ensure ASRVault is selected, click **DELETE**, and then click **YES**.

Run Lab04Cleanup.ps1 to remove the remaining Azure resources

In this exercise, 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 tasks in this exercise on **AZRCamp-Admin** signed in as **Contoso\Administrator** using the password **Passw0rd!**.

1. If not already open, open the **Windows PowerShell ISE**.
2. On the File menu, click **Open**, browse to **C:\LabFiles\AZITPROCamp\Lab04\**, select **Lab04Cleanup.ps1**, and then click **Open**.
   - This script is also available on GitHub at https://github.com/AZITCAMP/Labfiles/tree/master/lab04.
3. On the menu, click **Run**.
4. When prompted, sign in to your Azure subscription.
   - The command to delete the Azure services and resources in your subscription commences. The command may take as long as 10 to 20 minutes to complete.

End of lab