# Lab answer key: Implementing Hyper-V Replica and Windows Server Backup

## Exercise1: Implementing Hyper-V Replica

### Task 1: Configure a replica on both host machines

1. On **SEA-ADM1**, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
2. Select **Start**, and then enter **powershell**. Right-click or access the context menu for Windows PowerShell, and then select **Run as administrator**.
3. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* $cred=Get-Credential

When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* powershell $sess = New-PSSession -Credential $cred -ComputerName sea-svr1.contoso.com

Next, enter the following command, and then select Enter:

powershell Enter-PSSession $sess

You should get a [sea-svr1.contoso.com] title in your command prompt. From this point, all the commands that you enter run on **SEA-SVR1**. 1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

powershell Get-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener (TCP-In)"

You'll receive the properties of this firewall rule. Search for the value of the *Enabled* variable. It should be set to **False**. To enable **SEA-SVR1** as a replication host, you must enable this firewall rule. 1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

powershell Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener (TCP-In)"

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

powershell Get-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener (TCP-In)"

You'll receive the properties of this firewall rule. Search for the value of the *Enabled* variable. Now it should be set to **True**. 1. To configure **SEA-SVR1** as a Replica server for **Hyper-V Replica**, enter the following command in the PowerShell window, and then select Enter:

powershell Set-VMReplicationServer -ReplicationEnabled $true -AllowedAuthenticationType Kerberos -ReplicationAllowedFromAnyServer $true -DefaultStorageLocation c:\ReplicaStorage

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

powershell Get-VMReplicationServer

You should get the configuration setting that you configured in the previous step, which is as follows:

* **RepEnabled:True**
* **AuthType:Kerb**
* **KerAuthPort:80**
* **CertAuthPort:443**
* **AllowAnyServer:True**

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* Get-VM
* **SEA-CORE1** should be listed as a virtual machine (VM) that's configured on this Hyper-V server. Leave the **Administrator: Windows PowerShell** window open.

1. Select **Start**, and then enter **powershell**. Right-click or access the context menu for Windows PowerShell, and then select **Run as administrator**. This will open another instance of Windows PowerShell.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* $cred=Get-Credential
* When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* $sess1 = New-PSSession -Credential $cred -ComputerName sea-svr2.contoso.com
* Next, enter the following command, and then select Enter:
* Enter-PSSession $sess1
* You should get a [sea-svr2.contoso.com] title in your command prompt. From this point, all commands that you enter run on **SEA-SVR2**.

1. Repeat steps 5 through 10 in the PowerShell window where you have a session opened on **sea-svr2.contoso.com**. This will configure **SEA-SRV2** for **Hyper-V Replica**. In step 10, you should get no result when running the **Get-VM** command because no VMs are configured on **SEA-SVR2**.
2. Leave both PowerShell sessions open for the next task.

### Task 2: Configure replication

1. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following command, and then select Enter:

powershell Enable-VMReplication SEA-CORE1 -ReplicaServerName SEA-SVR2.contoso.com -ReplicaServerPort 80 -AuthenticationType Kerberos -computername SEA-SVR1.contoso.com

1. After you have verified that you didn't receive any error message from the previous command, enter the following command, and then select Enter:

powershell Start-VMInitialReplication SEA-CORE1

This starts the initial replication process for VM **SEA-CORE1**, from **SEA-SVR1** to **SEA-SVR2**.

1. After you have verified that you didn't receive any error message from the previous command, enter the following command, and then select Enter:

powershell Get-VMReplication

This command retrieves the replication status.

In the result table, search for the value in the **State** column. It should be **InitialReplicationInProgress**. Wait for 4–5 minutes, and then repeat this command. Verify that the value in the **State** column is **Replicating**. Don't proceed to the next steps until you get this value. Additionally, ensure that **Primary server** is set to **SEA-SVR1** and **ReplicaServer** is set to **SEA-SVR2**.

1. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

powershell get-vm

Verify that you now have the **SEA-CORE1** VM on **SEA-SVR2**. This means that the VM successfully replicated.

1. Leave both Windows PowerShell sessions open for the next task.

### Task 3: Validate failover

1. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following command, and then select Enter:

powershell Start-VMFailover -Prepare -VMName SEA-CORE1 -computername SEA-SVR1.contoso.com

When prompted, enter **Y**, and then select Enter. This command prepares for the planned failover of **SEA-CORE1** by replicating any pending changes. 1. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

powershell Start-VMFailover -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com

When prompted, enter **Y**, and then select Enter. This command fails over the replica VM. 1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

powershell Set-VMReplication -Reverse -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com

This command switches the replica VM to a primary VM. 1. In the PowerShell window where you have the remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

powershell Start-VM -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com

This command starts the VM that has been switched from a replica VM to a primary VM. 1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

powershell Get-VM

In the result table, search for the value in the **State** column. It should be **Running**. 1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

powershell Get-VMReplication

In the result table, search for the value in the **State** column. It should be **Replicating**. Additionally, ensure that the **Primary server** is now set to **SEA-SVR2** and that **ReplicaServer** is set to **SEA-SVR1**. 1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

powershell Stop-VM SEA-CORE1

1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following commands, and then select Enter:

powershell Exit-PSSession Remove-PSSession $sess

1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following commands, and then select Enter:

powershell Exit-PSSession Remove-PSSession $sess1

1. Close both PowerShell windows and leave the VMs running.

**Note:** If you want to verify the results of this exercise by using GUI tools, you can start Hyper-V Manager on **SEA-ADM1**, and then add the **SEA-SVR1** and **SEA-SVR2** servers to the **Hyper-V** console. You can then verify that the **SEA-CORE1** VM exists on both **SEA-SVR1** and **SEA-SVR2** and that replication is running from **SEA-SVR2** to **SEA-SVR1**.

**Results**: After completing this exercise, you should have configured **Hyper-V Replica** and tested failover.

## Exercise 2: Implementing backup and restore with Windows Server Backup

### Task1: Configure Windows Server Backup options

1. If necessary, sign in to **SEA-ADM1** as **Contoso\Administrator** with password **Pa55w.rd**.
2. Select **File Explorer** on the taskbar.
3. In the **File Explorer** window, select **Local Disk (C:)** in the **navigation** pane.
4. Right-click or access the context menu in an empty space in the **details** pane, select **New**, and then select **Folder**. You can also open **File Explorer**, select the **Home** menu, and then select the **New Folder** option.
5. Name the folder **BackupShare**. Right-click or access the context menu for the **BackupShare** folder, select **Give access to**, and then select **Specific people**.
6. In the **Network access** window, enter **Authenticated Users**, and then select **Add**. In the **Permission Level** column, set the value for **Authenticated Users** to **Read/Write**, select **Share**, and then select **Done**.
7. Select **Start**, and then enter **powershell**. Right-click or access the context menu for Windows PowerShell, and then select **Run as administrator**.
8. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

powershell $cred=Get-Credential

When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

powershell $sess = New-PSSession -Credential $cred -ComputerName sea-svr1.contoso.com

Next, enter the following command, and then select Enter:

powershell Enter-PSSession $sess

You should get a [sea-svr1.contoso.com] title in your command prompt. From this point, all commands that you enter run on **SEA-SVR1**.

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* Import-Module Servermanager
* Next, enter the following command, and then select Enter:
* Get-WindowsFeature Windows-Server-Backup
* Ensure that the **Install State for Windows Server Backup** feature is **Available**.

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* Install-WindowsFeature Windows-Server-Backup
* Wait until you get the result. Ensure that **True** displays in the **Success** column.

1. Repeat the command:

* Get-WindowsFeature Windows-Server-Backup
* Ensure that the **Install State for Windows Server Backup** feature is now **Installed**.

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* wbadmin /?
* You'll get the list of commands that are available for the Windows Server Backup command-line tool.

1. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

* Get-Command -Module WindowsServerBackup -CommandType Cmdlet
* You'll get a list of available PowerShell cmdlets for Windows Server Backup.

### Task 2: Perform a backup

1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following commands, and then select Enter:

powershell $Policy = New-WBPolicy $Filespec = New-WBFileSpec -FileSpec "C:\Files"

1. After you have run the commands from the previous step, where you defined variables for the backup policy and the file path to back up, add this to the backup policy by entering the following command, and then selecting Enter:

powershell Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec

1. Now, you must configure a backup location on the **SEA-AD1** network share by entering the following commands, and then selecting Enter:

powershell $Cred = Get-Credential $NetworkBackupLocation = New-WBBackupTarget -NetworkPath "\\SEA-ADM1\BackupShare" -Credential $Cred

**Note**: When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

1. Now you must add this backup location to the backup policy by entering the following command, and then selecting Enter (if prompted, enter Y, and then select Enter):

powershell Add-WBBackupTarget -Policy $Policy -Target $NetworkBackupLocation

1. Before starting a backup job, you must configure more options to enable Volume Shadow Copy Service backups by entering the following command, and then selecting Enter:

powershell Set-WBVssBackupOptions -Policy $Policy -VssCopyBackup

1. To start a backup job, in order to back up the content of the **C:\Files** folder on **SEA-SVR1** to a network share on **SEA-ADM1**, you must enter the following command, and then select Enter:

powershell Start-WBBackup -Policy $Policy

Wait until you receive the "The backup operation completed" message.

1. On **SEA-ADM1**, open File Explorer, and then browse to **C:\BackupShare**. Open the folder, and then ensure that the backup files are there.
2. Close all PowerShell windows.

**Results**: After completing this exercise, you should have configured Windows Server Backup and performed a backup on **SEA-SVR1**.

©2019 Microsoft Corporation. All rights reserved. The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are ***not*** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.