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

## Scenario

You're working as an administrator at Contoso, Ltd. Contoso wants to assess and configure new disaster recovery and backup features and technologies. As the system administrator, you have been tasked with performing that assessment and implementation. You decided to evaluate **Hyper-V Replica** and Windows Server Backup.

## Objectives

After completing this lab, you'll be able to:

* Configure and implement **Hyper-V Replica**.
* Configure and implement backup with Windows Server Backup.

## Lab setup

Estimated time: **45 minutes**

Virtual machines: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-SVR1**, **WS-011T00A-SEA-SVR2**, and **WS-011T00A-SEA-ADM1**

User name: **Contoso\Administrator**

Password: **Pa55w.rd**

1. Ensure that the **SEA-DC1**, **SEA-ADM1**, **SEA-SVR1**, and **SEA-SVR2** virtual machines (VMs) are running.
2. Select **SEA-ADM1**.
3. Sign in by using the following credentials:

* User name: **Administrator**
* Password: **Pa55w.rd**
* Domain: **Contoso**

1. When instructed in the lab, repeat these steps for **SEA-DC1**, **SEA-SVR1**, and **SEA-SVR2**.

## Exercise 1: Implementing Hyper-V Replica

### Scenario

Before you start with a cluster deployment, you have decided to evaluate the new technology in Hyper-V for replicating VMs between hosts. You want to be able to manually mount a copy of a VM on another host if the active copy or host fails.

The main tasks for this exercise are to:

1. Configure a replica on both host machines: **SEA-SVR1** and **SEA-SVR2**.
2. Configure replication for the **SEA-CORE1** VM.
3. Validate a failover.

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

1. On **SEA-ADM1**, open Windows PowerShell as an administrator.
2. In the PowerShell window, create a new remote PowerShell session to **sea-svr1.contoso.com**. Use **Contoso\Administrator** credentials to connect to the remote PowerShell on **SEA-SVR1**.
3. In the remote PowerShell session on **sea-svr1.contoso.com**, use the **Enable-Netfirewallrule** cmdlet to enable the firewall rule named Hyper-V Replica HTTP Listener (TCP-In).
4. Use the **Get-Netfirewallrule** cmdlet to verify that the Hyper-V Replica HTTP Listener (TCP-In) rule is enabled.
5. Use the following command to configure **SEA-SVR1** for **Hyper-V Replica**:

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

1. Use the **Get-VM** cmdlet to verify that the **SEA-CORE1** VM is present on **SEA-SVR1**.
2. Open a new remote PowerShell session for **sea-svr2.contoso.com** in a new PowerShell window. Repeat steps 2 through 5 to configure **SEA-SVR2** for **Hyper-V Replica**.

### Task 2: Configure replication

1. Switch to the PowerShell window where you have the 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. Start replication with the following command:

powershell Start-VMInitialReplication SEA-CORE1

1. After you've 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. Also ensure that **Primary server** is set to **SEA-SVR1** and that **ReplicaServer** is set to **SEA-SVR2**.

1. Switch to 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 get-vm

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

### 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

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

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

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

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 the 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. Close the PowerShell sessions.

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

### Scenario

You must evaluate Windows Server Backup for your member servers. You decided to configure Windows Server Backup of the **SEA-SVR1** server and to perform a trial backup to the network share on **SEA-ADM1**.

The main tasks for this exercise are to:

1. Configure Windows Server Backup on **SEA-SVR1**.
2. Perform a backup to the network share on **SEA-ADM1**.

### Task 1: Configure Windows Server Backup options

1. Use File Explorer to create a **C:\BackupShare** folder on **SEA-ADM1**. Share the folder so that **Authenticated Users** have Read/Write permissions.
2. In PowerShell, create a new remote PowerShell session to **sea-svr1.contoso.com**. Use **Contoso\Administrator** credentials to connect to the remote PowerShell on **SEA-SVR1**.
3. Use the **Install-WindowsFeature** cmdlet to install the **Windows-Server-Backup** feature on **SEA-SVR1**.
4. Use the **wbadmin /?** and **Get-Command** commands to get a list of the available commands 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:" ```

1. After running the commands from the previous step, where you defined the variables for the backup policy and the file path to the backup, 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 you receive the sign-in prompt, 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 backup 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 a "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.

©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.