Azure Site Recovery (Portal)

(LAB-300-02A-01)

Part A: Create Windows Virtual Machine

1. The first thing to do when creating virtual machines with the Azure Portal is log in to Azure with your administrative credentials.

2. Click the ***virtual machines*** link in the left-hand navigation bar.

3. Click the ***add*** button to start the creation process.

4. You will be required to fill in specific information regarding your virtual machine, including:
    a. *Subscription*: Select default subscription group

    b. *Resource Group*: Create resource group **RG-300-02-01-VM1**

    c. *Name*: Provide virtual machine name **myWinPRVM01**

    d. *Region*: Select region **East US**

    e. *Image*:
        i. Select "***Browse all image ….”***
        ii. Select "***Compute***"
        iii. Search "***Windows Server 2019 Datacenter***"
        iv. Select "***Windows Server 2019 Datacenter [Microsoft]”***

    f. ***Size***:
        I. Select "**Search**"
        II. Select "***Appropriate size for the virtual machine***"

    g. ***Administrator Account***:
        i. Provide "***Username***"
        ii. Provide "***Password***"

    h. ***Inbound Port Rules***:
        i. Select "***Allow selected ports***"
        ii. Select
            - ***Port 3389***

5. Click the "***Next: Disks***" button to continue.

6. Click the "***Next***: ***Networking***" button to continue.

7. Click the "***Next: Management***" button to continue.
8. Click on the "***Next: Guest***" config to continue.
9. Click the "***Next: Tags***" button to continue.
10. Click the "***Next: Review + create***" button to continue.
11. Click the "***Create***" button.

Part B: Create a Recovery Services vault

Create the vault in any region, except the source region.

1. Sign into the Azure portal
2. Go to left side, select Create a Resource
3. Search for Backup and Site Recovery (OMS)
4. Select Create & configure:
    1. In **Name**, specify a friendly name to identify the vault.
    2. Select the default subscription
    3. Create a resource group **RG-300-02-01-RSV**
    4. Specify an Azure region, other than **East US**.
    5. Click **Create**

Part C: Enable replication for a VM

5. Go to the left side, click on Resource Group
6. Select **RG-300-02-01-RSV** resource group
7. Select the Recovery Services vaults & open
8. Select **+Replicate**
9. In **Source**, select **Azure**
10. In **Source location**, select the source Azure region East US where your VMs are currently running
11. Select the default **source subscription** where the virtual machines are running

12. Select the Source resource group **RG-300-02-01-VM1** and click **OK** to save the settings.

Part D: Select the VMs

Site Recovery retrieves a list of the VMs associated with the subscription and resource group/cloud service.

1. In **Virtual Machines**, select the **myWinPRVM01** VMs you want to replicate.
2. Click **OK**.

Part E: Configure replication settings

Site Recovery creates default settings and replication policy for the target region. You can change the settings as required.

1. Click **Settings** to view the target and replication settings
2. To override the default target settings, click **Customize** next to **Resource group, Network, Storage and Availability**.
3. Customize target settings as summarized in the table.
    a. **Target subscription**: By default, the target subscription is the same as the source subscription.
    b. **Target location**: The target region used for disaster recovery.
    c. **Target resource group**: The resource group in the target region that holds Azure VMs after failover.

    By default, Site Recovery creates a new resource group in the target region with an "***asr***" suffix. The location of the target resource group can be any region except the region in which your source virtual machines are hosted.

    d. **Target virtual network**: The network in the target region that VMs are located after failover.

    By default, Site Recovery creates a new virtual network (and subnets) in the target region with an "***asr***" suffix.

e. **Cache storage accounts**: Site Recovery uses a storage account in the source region. Changes to source VMs are sent to this account before replication to the target location.

f. **Target availability zones**: By default, Site Recovery assigns the same zone number as the source region in target region if the target region supports availability zones.

   If the target region doesn't support availability zones, the target VMs are configured as single instances by default.

Leave other settings as default

4. To customize replication policy settings, click **Customize** next to **Replication policy**, and modify the settings as needed.

   a. **Replication policy name**: Provide **policy name**

   b. **Recovery point retention:** By default, Site Recovery keeps recovery points for 24 hours. You can configure a value between 1 and 72 hours.

   c. **App-consistent snapshot frequency**: By default, Site Recovery takes an app-consistent snapshot every 4 hours. You can configure any value between 1 and 12 hours.

      An app-consistent snapshot is a point-in-time snapshot of the application data inside the VM. Volume Shadow Copy Service (VSS) ensures that app on the VM are in a consistent state when the snapshot is taken.

   Leave other settings as default

5. Then click **OK**

6. Click on **Create target resources**

7. Click on **Enable replication**

Part F: Track replication status

1. In **Settings**, click **Refresh** to get the latest status.
2. Track progress and status as follows:

- Track progress of the Enable protection job. In **Settings,** select **Jobs,** select **Site Recovery Jobs**.
- Select **Replicated Items**, you can view the status of VMs and the initial replication progress.
- Click the VM to drill down into its settings.

Part G: Run a failover to the secondary region

1. In **Replicated items**, select the VM that you want to fail over
2. Select **Failover**
3. In **Failover**, select a **Recovery Point** to fail over to. You can use one of the following options:
   - **Latest** (default): Processes all the data in the Site Recovery service and provides the lowest Recovery Point Objective (RPO).
   - **Latest processed**: Reverts the virtual machine to the latest recovery point that has been processed by Site Recovery service.
   - **Custom**: Fails over to a recovery point. This option is useful for performing a test failover.
4. Select **Shut down machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source VMs before triggering the failover.

   Failover continues even if shutdown fails. Site Recovery does not clean up the source after failover.
5. Press **OK**
6. Select the **Skip failover test**
7. Follow the failover progress on the **Jobs** page.
8. After the failover, validate the virtual machine by logging in to it.
9. Once you are satisfied with the failed over virtual machine, you can **Commit** the failover. Committing deletes all the recovery points available with the service. You won't now be able to change the recovery point.

Part H: Reprotect the secondary VM

After failover of the VM, you need to re-protect it so that it replicates back to the primary region.

1. Make sure that the VM is in the **Failover committed** state, and check that the primary region is available, and you're able to create and access new resources in it.
2. Select **Replicated items**, right-click the VM that's been failed over, and then select **Re-Protect**.
3. Verify that the direction of protection, secondary to primary region, is already selected.
4. Review the **Resource group, Network, Storage, and Availability sets** information. Any resources marked as new are created as part of the re-protect operation.
5. Click **OK** to trigger a re-protect job. This job seeds the target site with the latest data. Then, it replicates the deltas to the primary region. The VM is now in a protected state.