INDEX

Sr No.	Practical	Date	Sign
1A	Create a private cloud from a host group		
1B	Deploy a guarded host fabric using Microsoft SCVMM 2019		
2A	Deploy and manage SDN Infrastructure using SCVMM 2019		
2B	Deploy and Manage Storage Space Direct (S2D) using SCVMM 2019		
3A	Deploy Service Manager 2019 and install on 4 Computer Scenario		
3B	Setup SQL Server reporting Service using Service Manager 2019		
4A	User Connectors to import data		
4B	Automate IT processes with workflows		
5A	Managing devices with Configuration Manager		
5B	Design a hierarchy of sites using Microsoft End Point Configuration manager.		
6A	Data transfers between sites		
6B	Configure sites and hierarchies		

7A	**Install Orchestrator**		
7B	**Create and test a monitor runbook**		
8A	**Manage Orchestrator Servers - 1**		
8B	**Manage Orchestrator Servers – 2**		
9	**Install and Deploy DPM**		
10	**Protect Workloads.**		

PRACTICAL 1A

AIM: Create a private cloud from a host group

Create a private cloud from a host group

1. Click VMs and Services > Create > Create Cloud, to open the Create Cloud Wizard.
2. In General, specify a Name and optional description for the cloud.
3. Specify whether the cloud will support shielded VMs.
4. In Resources > Host groups, select the groups you want to add to the cloud. Then click Next.
5. In Logical Networks, select each logical network that you want to make available to the private cloud, and then click Next.
Note: Only logical networks that are associated with the physical network adapters on hosts in the selected host groups appear in the list.
6. In Load Balancers, select each load balancer that you want to make available to this private cloud, and then click Next
7. In VIP Templates, select each VIP template that you want to make available to the private cloud, and then click Next.
8. In Port Classifications, select each port classification that you want to make available to the cloud, and then click Next.
9. In Storage, if you have storage managed by VMM, select each storage classification that you want to make available to the private cloud, and then click Next.
Note: Only storage classifications for storage pools that are assigned to the selected host groups appear in the list.
10. In Library > Stored VM path, browse and select the library share you want to use for the self-service users to store VMs. Click OK.
11. In Read-only library shares > Add, select one or more library shares where administrators can provide read-only resources to cloud users. Click OK and then click Next.
12. In Capacity, set capacity limits for the private cloud, and then click Next. You can either accept the default values, or clear the Use Maximum check boxes and set quotas for the following resources
13. In Capability Profiles, select each virtual machine capability profile that you want to add, and then click Next. Select the capability profiles that match the type of hypervisor platforms that are running in the selected host groups. The built-in capability profiles represent the minimum and maximum values that can be configured for a virtual machine for each supported hypervisor platform.
14. In Replication Groups, select the replication groups for the private cloud, and click Next.
15. In Summary page, confirm the settings, and then click Finish. View status in Jobs and ensure the job is complete. To verify that the private cloud was created, check VMs and Services > Clouds. You can also verify in Library > Cloud Libraries, to view the read-only library shares

PRACTICAL 1B

AIM: Deploy a guarded host fabric using Microsoft SCVMM 2019

Deploy a guarded host fabric using Microsoft SCVMM 2019

Before you can add guarded hosts to your VMM compute fabric, you must configure VMM with information about the Host Guardian Service for the fabric. The same HGS will be used for all guarded hosts managed by VMM.

1. Obtain the attestation and key protection URLs for your fabric from your HGS administrator.

2. In the VMM console, click Settings > Host Guardian Service Settings.

3. Enter the attestation and key protection URLs in the respective fields. You do not need to configure the code integrity policies and VM shielding helper VHD sections at this time.

4. Click Finish to save the configuration.

PRACTICAL 2A

AIM: Deploy and manage SDN Infrastructure using SCVMM 2019.

Deployment Steps: -

To set up an SDN network controller

1. Configure hosts and physical network infrastructure: You need access to your physical network devices to configure VLANs, routing etc. You also need Hyper-V hosts to host the SDN infrastructure and tenant VMs. Learn more.

2. Prepare a virtual hard disk: You can prepare a virtual hard disk for the network controller service template in VHD or VHDX format, as appropriate for the service template generation you choose.

3. Download the service templates: Download the network controller service templates and import them to the VMM library.

4. Set up Active Directory security groups: You'll need an Active Directory security group for network controller management, and another security group for network controller clients. Each group will need at least one user account in it.

5. Set up a VMM library share. You can have an optional library file share for keeping diagnostic logs. This library share will be accessed by the network controller to store diagnostics information throughout its lifetime.

6. Set up a VMM host group: Set up a dedicated host group for all of the SDN Hyper-V hosts.

7. Create the management logical network: Create a logical network to mirror management network connectivity for the VMM host, network controller hosts, and tenant VM hosts. If you want to allocate static IP addresses from a pool, create a pool on this logical network.

8. Create and deploy a management logical switch: You create the logical switch, and deploy it on network controller hosts, to provide connectivity to the management network for network controller VMs.

9. Set up a certificate: You need an SSL certificate for secure/HTTPS communication with the network controller.

10. Import the template: Import and customize the network controller service template. 11. Deploy the service: Deploy the network controller service using the service template. Then add it as a VMM service.

PRACTICAL 2B

AIM: Deploy and Manage Storage Space Direct (S2D) using SCVMM 2019.

1. Provision the cluster
2. Set up networking for the cluster
   - Start by creating a logical network to mirror your physical management network.
   - Set up a logical switch with Switch Embedded Teaming (SET) enabled.
   - Create VM networks.
3. Configure DCB settings on the S2D cluster
   - Create a new Hyper-V cluster, select Enable Storage Spaces Direct. DCB Configuration option gets added NOTE to the Hyper-V cluster creation workflow.
   - In DCB configuration, select Configure Data Center Bridging.
   - Provide Priority and Bandwidth values for SMB-Direct and Cluster Heartbeat traffic.
   - Select the network adapters used for storage traffic. RDMA is enabled on these network adapters.
   - Review the summary and select Finish.
4. Manage the pool and create CSVs
   - Click Fabric > Storage > Arrays.
   - Right-click the cluster > Manage Pool, and select the storage pool that was created by default. You can Change the default name, and add a classification.
   - To create a CSV, right-click the cluster > Properties > Shared Volumes.
   - In the Create Volume Wizard > Storage Type, specify the volume name, and select the storage pool.
   - In Capacity, you can specify the volume size, file system, and resiliency settings
   - Click Configure advanced storage and tie ring settings to set up these options.
   - In Summary, verify settings and finish the wizard. A virtual disk will be created automatically when you create the volume.
5. Deploy VMs on the cluster

PRACTICAL 3A

AIM: Deploy Service Manager 2019 and install on 4 Computer Scenario.

To Install the System Center - Service Manager management server, the Service Manager database, the data warehouse management server, data warehouse databases, and the Service Manager console in a four-computer topology.

To install the Service Manager management server, Service Manager database and console: -

1. Log on to the computer that will host the Service Manager management server by using an account that has administrative rights.
2. On the System Center Service Manager installation media, double-click the **Setup.exe** file.
3. On the **Service Manager Setup Wizard** page, click **Service Manager management server**.
4. On the **Product registration** page, in the **Product key** boxes, type the product key that you received with Service Manager, or as an alternative, select **Install as an evaluation edition (180-day trial)**. Read the Microsoft Software License Terms, and, if applicable, click **I have read, understood, and agree with the terms of the license agreement**, and then click **Next**.
5. On the **Installation location** page, verify that sufficient free disk space is available. If necessary, click **Browse** to change the location of where the Service Manager management server will be installed. Click **Next**.
6. On the **System check results** page, make sure that the prerequisite check passed or at least passed with warnings.

   If the prerequisite checker determines that the Microsoft Report Viewer Redistributable has not been installed, click **Install Microsoft Report Viewer Redistributable**. After the Microsoft Report Viewer Redistributable 2008 (KB971119) Setup Wizard completes, click **Check prerequisites again**. Click **Next**.

7. On the **Configure the Service Manager database** page, in the **Database server** field, type the name of the computer that will host the Service Manager database, and press the TAB key. Ensure that **SQL Server instance** box is set to the desired SQL Server instance and that **Create a new database** is selected, and then click **Next**. For example, type **Computer 2** in the **Database server** box.
8. On the **Configure the Service Manager management group** page, complete these steps:

   a. In the **Management group name** box, type a unique name for the group name.
   b. In the **Management group administrators** areas, click **Browse**, enter the user or group that you want to be the Service Manager administrator, and then click **Next**. For example, select the group Woodgrove\SM_Admins.

9. On the **Configure the account for Service Manager services** page, click **Domain account**; specify the user name, password, and domain for the account; and then click **Test Credentials**. After you receive a "The credentials were accepted" message, click **Next**.
10. On the **Configure the Service Manager workflow account** page, click **Domain account**; specify the user name, password, and domain for the account; and then click **Test Credentials**. After you receive a "The credentials were accepted" message, click **Next**.
11. On the **Diagnostic and usage data** page, indicate your preference for sharing your Service Manager diagnostic and usage data with Microsoft. As an option, click **Privacy statement for System Center Service Manager**, and then click **Next**.
12. On the **Use Microsoft Update to help keep your computer secure and up-to-date** page, indicate your preference for using Microsoft Update to check for Service Manager updates. If you want Windows Update to check for updates, select **Initiate machine wide Automatic update**. Click **Next**.
13. On the **Installation summary** page, click **Install**.
14. On the **Setup completed successfully** page, we recommend that you leave **Open the Encryption Backup or Restore Wizard** selected, and then click **Close**.

To install a data warehouse management server: -

1. On the System Center Service Manager installation media, double-click the **Setup.exe** file.
2. On the **Service Manager Setup Wizard** page, click **Service Manager data warehouse management server**.
3. On the **Product registration** page, in the **Product key** boxes, type the product key that you received with Service Manager, or as an alternative, select **Install as an evaluation edition (180-day trial)**. Read the Microsoft Software License Terms, and, if applicable, click **I have read, understood, and agree with the terms of the license agreement**, and then click **Next**.
4. On the **Installation location** page, verify that sufficient free disk space is available, and then click **Next**. If necessary, click **Browse** to change the location where the Service Manager management server will be installed.
5. On the **System check results** page, verify that prerequisites passed or at least passed with warnings, and then click **Next**.
6. On the **Configure data warehouse databases** page, in the **Database server** box, type the computer name of the physical computer that will host the data warehouse databases, the SQL server port, and Database name for all three data warehouse databases, then click **Next**.
7. In the list of the three databases, select **Data Mart**. In the **Database server** box, type the computer name of the server that will host the Data Mart database. For example, type **Computer 4**, and then press the TAB key. When **Default** appears in the **SQL Server instance** box, click **Next**.
8. On the **Configure additional data warehouse datamarts** page, complete these steps:

    a. Click **OM Data mart**. In the **Database server** box, type the computer name of the computer that will host the Operations Manager data mart database. For example, type **Computer 4**, and then press the TAB key.

b. Click **CM Data mart**. In the **Database server** box, type the computer name of the computer that will host the CM data mart database. For example, type **Computer 4**, and then press the TAB key.
c. Click **Next**.

On the **Configure the data warehouse management group** page, complete these steps:

a. In the **Management group name** box, type a unique name for the group name.
b. Click **Browse**, enter the user or group that you want to be the Service Manager administrator, and then click **Next**.

On the **Configure the reporting server for the data warehouse** page, follow these steps:

a. In the **Report server** box, enter the name of the computer that will host the reporting server. In this example, this will be the computer that hosts the data warehouse database, enter **Computer 4**, and then press the TAB key.
b. Verify that **Default** is displayed in the **Report server instance** box.
c. Because you followed the procedure Manual Steps to Configure the Remote SQL Server Reporting Services, select the **I have taken the manual steps to configure the remote SQL Server Reporting Services as described in the Service Manager Deployment Guide** check box, and then click **Next**.

9. On the **Configure the account for Service Manager services** page, click **Domain account**, specify the user name, password, and domain for the account, and then click **Test Credentials**. After you receive a **The credentials were accepted** message, click **Next**.
10. On the **Configure the reporting account** page, specify the user name, password, and domain for the account, and then click **Test Credentials**. After you receive a **The credentials were accepted** message, click **Next**.
11. On the **Configure Analysis Service for OLAP cubes** page, in the **Database server** box, type the computer name of the server that will host the Analysis Services database, and then press the TAB key. When **Default** appears in the **SQL Server instance** box, click **Next**. For example, type **Computer 4** in the **Database server** box.
12. On the **Configure Analysis Services credential** page, select a domain account, click **Domain account**, specify the user name, password, and domain for the account, and then click **Test Credentials**. After you receive a **The credentials were accepted** message, click **Next**.
13. On the **Diagnostic and usage data** page, indicate your preference for sharing your Service Manager diagnostic and usage data with Microsoft. As an option, click **Privacy statement for System Center Service Manager**, and then click **Next**.
14. On the **Use Microsoft Update to help keep your computer secure and up-to-date** page, indicate your preference for using Microsoft Update to check for Service Manager updates. Select **Initiate machine wide Automatic update** if you want Windows Update to check for updates. Click **Next**.
15. On the **Installation summary** page, click **Install**.
16. On the **Setup completed successfully** page, we recommend that you leave **Open the Encryption Backup or Restore Wizard** selected, and then click **Close**.

Practical 3B

AIM: Setup SQL Server reporting Service using Service Manager 2019.

Report Server Configuration Manager (Native Mode)

1. Use the following step that is appropriate for your version of Microsoft Windows:

    - From the Windows Start menu, type **Reporting** and select **Report Server Configuration Manager** from the search results.
    - Select **Start**, point to **All Programs**, point to **Microsoft SQL Server**, and then point to **Configuration Tools**.

      If you want to configure a report server instance from a previous version of SQL Server, open the program folder for that version. For example, point to SQL Server 2014 (12.x) instead of **Microsoft SQL Server** to open the configuration tools for SQL Server 2014 (12.x) server components.

      Select **Report Server Configuration Manager**.

2. The **Reporting Services Configuration Connection** dialog box appears so that you can select the report server instance you want to configure. Select **Connect**.
3. In **Server Name**, specify the name of the computer on which the report server instance is installed. The name of the local computer appears by default, but you can type the name of a remote SQL Server instance if you want to connect to a report server that is installed on a remote computer.
4. If you specify a remote computer, select **Find** to establish a connection.
5. In **Report Server Instance**, select the SQL Server Reporting Services instance that you want to configure. Only report server instances for this version of SQL Server appear in the list. You cannot configure earlier versions of Reporting Services.
6. Select **Connect**.

PRACTICAL 4A

AIM: User Connectors to import data

i) Import data from Active Directory Domain Services

To create an Active Directory connector and to import objects from AD DS

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Active Directory Connector**.
4. Complete these steps in the Active Directory Connector Wizard:

    - On the **Before You Begin** page, click **Next**.
    - On the **General** page, in the **Name** box, type a name for the new connector. Make sure that the **Enable this connector** check box is selected, and then click **Next**.
    - On the **Domain or organizational unit** page, select **Use the domain: *domain name***. Or, select **Let me choose the domain or OU**, and then click **Browse** to choose a domain or an organizational unit (OU) in your environment.
    - In the **Credentials** area, click **New**.
    - In the **Run As Account** dialog box, in the **Display name** box, enter a name for the Run As account. In the **Account** list, select **Windows Account**. Enter the credentials for an account that has rights to read from AD DS, and then click **OK**. On the **Domain or organizational unit** page, click **Test Connection**.

5. In the **Test Connection** dialog box, make sure that **The connection to the server was successful** is displayed, and then click **OK**. On the **Domain or organizational unit** page, click **Next**.
6. On the **Select objects**, do the following:

    - Select **Select individual computers, printers, users or user groups** to import only the Select **All computers, printers, users, and user groups** to import all items or,
    - selected items or,
    - Select **Provide LDAP query filters for computers, printers, users, or user groups** if you want to create your own Lightweight Directory Access Protocol (LDAP) query.

    If you want new users that are added to any groups you import to be added automatically to Service Manager, select **Automatically add users of AD Groups imported by this connector**, and then click **Next**.

7. On the **Schedule** page, in the **Synchronize** list, set the frequency and time of synchronization, and then click **Next**.
8. On the **Summary** page, make sure that the settings are correct, and then click **Create**.

9. On the **Completion** page, make sure that you receive the following confirmation message: *Active Directory connector successfully created.* Then, click **Close.**

ii) Import data and alerts from the Operations Manager: -

To import Operations Manager management packs for an Operations Manager CI connector: -

1. On the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Management Packs**.
3. In the **Tasks** pane, under **Management Packs**, click **Import**.
4. In the **Select Management Packs to Import** box, point to the drive where Service Manager is installed, and then point to Program Files\Microsoft System Center\Service Manager <version>\Operations Manager <version> Management Packs.
5. To the right of the **File name** box, select the file type **MP files (*.mp)**.
6. In the list of files, select all of the management packs, and then click **Open**.
7. In **Import Management Packs**, select all of the management packs, and then click **Import**.
8. When the import process is complete, the message The management pack was imported successfully will appear.
9. Click **OK**.

To create an operations Manager alert connector: -

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Operations Manager Alert Connector**.
4. Complete the following steps to complete the Operations Manager Alert Connector Wizard:

    a. On the **Before You Begin** page, click **Next**.
    b. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that the **Enable** check box is selected, and then click **Next**. Make a note of this name; you will need this name in step 7 of this procedure.
    c. On the **Server Details** page, in the **Server name** box, type the name of the server that is hosting the Operations Manager root management server. Under **Credentials**, click **New**.
    d. In the **Run As Account** dialog box, in the **Display name** box, type a name for this Run As account. In the **Account** list, select **Windows Account**.
    e. In the **User Name**, **Password**, and **Domain** fields, type the credentials for the Run As account, and then click **OK**.
    f. On the **Server Details** page, click **Test Connection**. If you receive the following confirmation message, click **OK**, and then click **Next**:
    g. On the **Alert Routing Rules** page, click **Add**.

h. In the **Add Alert Routing Rule** dialog box, create a name for the rule, select the template that you want to use to process incidents created by an alert, and then select the alert criteria that you want to use. Click **OK**, and then click **Next**.
i. On the **Schedule** page, select **Close alerts in Operations Manager when incidents are resolved or closed** or **Resolve incidents automatically when the alerts in Operations Manager are closed**, click **Next**, and then click **Create**.

Start the Operations Manager console.
In the **Administration** pane, click **Product Connectors**, and then click **Internal Connectors**.
In the **Connectors** pane, click the name of the alert connector.
In the **Actions** pane, click **Properties**.
In the **Alert Sync:** ***name of connector*** dialog box, click **Add**.
In the **Product Connector Subscription Wizard** dialog box, on the **General** page, in the **Subscription Name** box, type the name for this subscription. For example, type **All Alerts**, and then click **Next**.
On the **Approve groups** page, click **Next**.
On the **Approve targets** page, click **Next**.
On the **Criteria** page, click **Create**.
In the **Alert Sync:*name of connector*** dialog box, click **OK**.

iii) Import data from Configuration Manager: -

Import configuration data: -

1. In the Configuration Manager console, click **Assets and Compliance** > **Configuration Items** or **Configuration Baselines**
2. In the **Home** tab, in the **Create** group, click **Import Configuration Data**.
3. On the **Select Files** page of the **Import Configuration Data Wizard**, click **Add**, and then in the **Open** dialog box, select the .cab files you want to import.
4. Select the **Create a new copy of the imported configuration baselines and configuration items** check box if you want the imported configuration data to be editable in the Configuration Manager console.
5. On the **Summary** page, review the actions that will be taken, and then complete the wizard.

The imported configuration data displays in the **Compliance Settings** node of the **Assets and Compliance** workspace.

iv) Import runbooks from Orchestrator: -

To create an Orchestrator connector: -

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Orchestrator connector**.

4. Perform these steps to complete the Orchestrator Connector Wizard:

    a. On the **Before You Begin** page, click **Next**.
    b. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that **Enable this connector** is selected, and then click **Next**.
    c. On the **Connection** page, in the **Server Information** area, type the URL of the Orchestrator Web service.

        - Type the URL of the Orchestrator Web service in the form of http://computer:port/Orchestrator/Orchestrator.svc, where *computer* is the name of the computer hosting the web service and *port* is the port number where the web service is installed. (The default port number is 81.)

    d. On the **Connection** page, in the **Credentials** area, either select an existing account or click **New**, and then do the following:

        - In the **Run As Account** dialog box, in the **Display name** box, type a name for the Run As account. In the **Account** list, select **Windows Account**. Enter the credentials for an account that has rights to connect Orchestrator, and then click **OK**. On the **Connection** page, click **Test Connection**.

        - In the **Test Connection** dialog box, make sure that the message *The connection to the server was successful* appears, and then click **OK**. On the **Connection** page, click **Next**.

    e. On the **Folder** page, select a folder, and then click **Next**.
    f. On the **Web Console URL** page, type the URL for the Orchestrator web console in the form of http://computer:port (the default port number is 82), and then click **Next**.
    g. On the **Summary** page, make sure that the settings are correct, and then click **Create**.
    h. On the **Completion** page, make sure that you receive the message *Orchestrator connector successfully created*, and then click **Close**.

To validate the creation of an Orchestrator connector: -

1. In the **Connectors** pane, locate the Orchestrator connector that you created.
2. Review the **Status** column for a status of **Finished Success**.
3. In the Service Manager console, click **Library**.
4. In the **Library** pane, expand **Library**, and then click **Runbooks**.
5. Review the **Runbooks** pane, and note that your runbooks have been imported.

v) Import data from VMM: -

To create a System Center Virtual Machine Manager connector: -

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.

3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Virtual Machine Manager connector**.
4. Complete these steps to complete the Virtual Machine Manager Connector Wizard:

    a. On the **Before You Begin** page, click **Next**.
    b. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that **Enable this connector** is selected, and then click **Next**.
    c. On the **Connection** page, in the **Server Information** area, type the same of the computer hosting Virtual Machine Manager (VMM).
    d. On the **Connection** page, in the **Credentials** area, either select an existing account or click **New**, and then do the following:

        - In the **Run As Account** dialog box, in the **Display name** box, type a name for the Run As account. In the **Account** list, select **Windows Account**. Enter the credentials for an account that has rights to connect VMM, and then click **OK**. On the **Connection** page, click **Test Connection**.
        - In the **Test Connection** dialog box, make sure that **The connection to the server was successful** appears, and then click **OK**. On the **Connection** page, click **Next**.
        - On the **Summary** page, make sure that the settings are correct, and then click **Create**.
        - On the **Completion** page, make sure that you receive a *Virtual Machine Manager connector successfully created* message, and then click **Close**.

To validate the creation of a System Center Virtual Machine Manager connector: -

1. In the **Connectors** pane, locate the System Center Virtual Machine Manager connector that you created.
2. In the Service Manager console, click **Configuration Items**.
3. In the **Tasks** pane, click **Create Folder**.
4. In the Create New Folder Wizard, do the following:

    - In the **Folder name** box, type a name for the folder. For example, type **Test**.
    - In the **Management pack** area, make sure that an unsealed management pack of your choice is selected, and then click **OK**. For example, select **Service Catalog Generic Incident Request**.

5. In the **Configuration Items** pane, click the folder you just created. For example, click **Test**.

6. In the **Tasks** pane, click **Create View**.

7. In the Create View Wizard, do the following:

    - On the **General** page, in the **Name** area, type a name for this view. For example, type **VMMTemplates**.

- In the **Management pack** area, make sure that an unsealed management pack of your choice is selected. For example, select **Service Catalog Generic Incident Request**.
- In the navigation pane of the wizard, click **Criteria**.
- In the **Advanced Search** area, click **Browse**.
- In the drop-down list (located to the right of the **Type to filter** box), select **All basic classes**.
- In the **Type to filter** box, type **virtual machine template**, click **Virtual Machine Template**, click **OK**, and then click **OK** to save and close the form.

8 In the **Configuration Items** pane, expand the folder you created, and then click the view you created. For example, expand **Test**, and then click **VMMTemplates**

In the **VMMTemplates** pane, you will see the Virtual Machine Manager templates that have been created.

vi) Use a CSV file to import data: -

Import data from a CSV, HTML, or text file: -

1. On the **File** menu, click **Import**.
2. In the **Import** dialog box, click the option for the type of file that you want to import, and then click **Import**.
3. In the **Choose a File** dialog box, locate and click the CSV, HTML, or text file that you want to use as an external data range, and then click **Get Data**.
4. Follow the steps in the Text Import Wizard, where you can specify how you want to divide the text into columns and other formatting options. When you have completed step 3 of the wizard, click **Finish**.
5. In the **Import Data** dialog box, click **Properties** to set query definition, refresh control, and data layout options for the external data that you are importing. When you have finished, click **OK** to return to the **Import Data** dialog box.
6. Do one of the following:

Practical 4B

AIM: Automate IT processes with workflows

i) Add or remove workflow activities: -

To add an activity to a workflow: -

1. In the **Management Pack Explorer**, expand **Workflows**, right-click the workflow you want, and then click **Edit**. This opens the workflow in the authoring pane. For example, right-click **AddComputerToADGroupWF**, and then click **Edit**.
2. In the **Activities Toolbox** pane, locate the appropriate activity group.
3. Drag the activity you want to the authoring pane, and then drop it between the workflow Start and End icons or between two existing activities. The sequence of activities that is displayed in the authoring pane-from the top down-represents the order in which the activities will run. To run activities in a loop or if-else structure, drag the structure activity onto the authoring pane first, and then drop the activities into the structure activity.

   For example, drag **Add AD DS Computer to Group** from the **Active Directory Activities** group to the authoring pane, and then drop it between the workflow Start and End icons. Then, drag **Set Activity Status to Completed** and drop it between the previous activity and the End icon.

4. You can set the properties of an activity immediately after you add it to the authoring pane, or you can set the properties later

To remove an activity from a workflow: -

- In the authoring pane, right-click the activity, and then click **Delete**.
-

ii) Deploy a workflow to Service Manager using the Authoring Tool: -

Import the management pack into Service Manager: -

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Management Packs**.
3. In the **Tasks** pane, under **Management Packs**, click **Import Management Pack**.
4. In the **Select Management Packs to Import** dialog box, select the management pack file that is associated with the workflow, and then click **Open**. For example, select **AddComputerToADGroupMP.xml**.
5. In the **Import Management Packs** dialog box, click **Add** to add the management pack that you want to import.
6. Click **Import**, and then click **OK**.

iii) Configure the Activities Toolbox in the Authoring Tool: -

Create a top-level activity group: -

1. In the **Activities Toolbox** pane, right-click **Activity Groups**, and then click **New Group**.
2. Enter a name for the new group.

Create an activity subgroup: -

1. In the **Activities Toolbox** pane, right-click the parent group, and then click **New Group**.
2. Enter a name for the new group.

Rename a personalized activity group: -

Use this procedure to change the name of a personalized activity group in the Service Manager Authoring Tool.

1. In the **Activities Toolbox** pane, right-click the group, and then click **Rename Group**.
2. Enter a new name for the group.

Remove activities from a personalized activity group: -

1. In the **Activities Toolbox** pane, right-click the group, and then click **Choose Activities**.
2. In the **Choose Activities for a Group** dialog box, scroll the list to find the activities you want to remove. Clear the check boxes for the activities you want to remove, and then click **OK**.

Delete a personalized activity group: -

- In the **Activities Toolbox** pane, right-click the group, and then click **Delete Group**.

PRACTICAL 5A

AIM: Managing devices with Configuration Manager

There are two ways to use the Configuration Manager client software to manage a device. The first way is to discover the device on your network, and then deploy the client software to that device. The other way is to manually install the client software on a new computer, and then have that computer join your site when it joins your network. To discover devices where the client software is not installed, run one or more of the built-in discovery methods. After a device is discovered, use one of several methods to install the client software.

One of the ways that users can control their software deployment experience is to use the **Software Center** client interface. The **Software Center** is automatically installed on client computers and is run from the Windows **Start** menu. The **Software Center** lets users manage their own software and do the following tasks:

1. Install software
2. Schedule software to automatically install outside working hours
3. Configure when Configuration Manager can install software on a device
4. Configure the access settings for remote control, if remote control is set up in Configuration Manager
5. Configure options for power management, if an administrator sets up this option
6. Browse for, install, and request software
7. Configure preference settings
8. When it's set up, specify a primary device for user device affinity

PRACTICAL 5B

AIM: Design a hierarchy of sites using Microsoft End Point Configuration manager.

Before installing the first site of a new Configuration Manager hierarchy, it's a good idea to understand:

1. The available topologies for Configuration Manager
2. The types of available sites and their relationships with each other
3. The scope of management that each type of site provides
4. The content management options that can reduce the number of sites you need to install

Then plan a topology that efficiently serves your current business needs and can later expand to manage future growth.

When planning, keep in mind limitations for adding additional sites to a hierarchy or a stand-alone site:

1. Install a new primary site below a central administration site, up to the supported number of primary sites for the hierarchy.
2. Expand a standalone primary site to install a new central administration site, to then install additional primary sites.
3. Install new secondary sites below a primary site, up to the supported limit for the primary site and overall hierarchy.
4. You can't add a previously installed site to an existing hierarchy to merge two standalone sites. Configuration Manager only supports installation of new sites to an existing hierarchy of sites.

PRACTICAL 6A

AIM: Data transfers between sites

i)Types of data transfer

Configuration Manager uses file-based replication and database replication to transfer different types of information between sites.

ii)File-based replication

Configuration Manager uses file-based replication to transfer file-based data between sites in your hierarchy. This data includes applications and packages that you want to deploy to distribution points in child sites. It also handles unprocessed discovery data records that the site transfers to its parent site and then processes.

File replication route

Each file replication route identifies a destination site to which a site transfers file-based data. Each site supports one file replication route to a specific destination site.

To manage a file replication route, go to the **Administration** workspace. Expand the **Hierarchy Configuration** node, and then select **File Replication**.

Change the following settings for file replication routes:

- File replication account: This account connects to the destination site, and writes data to that site's **SMS_Site** share. The receiving site processes the data written to this share. By default, when you add a site to the hierarchy, Configuration Manager assigns the new site server's computer account as its file replication account. It then adds this account to the destination site's SMS_SiteToSiteConnection_<sitecode> group. This group is local to the computer that grants access to the SMS_Site share. You can change this account to be a Windows user account. If you change the account, make sure you add the new account to the destination site's SMS_SiteToSiteConnection_<sitecode> group.
- Schedule: Set the schedule for each file replication route. This action restricts the type of data and time when data can transfer to the destination site.
- Rate limits: Specify rate limits for each file replication route. This action controls the network bandwidth the site uses when it transfers data to the destination site

iii)Database replication

Configuration Manager database replication uses SQL Server to transfer data. It uses this method to merge changes in its site database with the information from the database at other sites in the hierarchy.

Replication groups

Configuration Manager groups data that replicates by database replication into different replication groups. Each replication group has a separate, fixed replication schedule. The site uses this schedule to determine how frequently it replicates changes to other sites.

Settings

You can modify the following settings for database replication:

- **Database replication links**: Control when specific traffic traverses the network.
- **Distributed views**: When a central administration site (CAS) requests selected site data, it can access the data directly from the database at a child primary site.
- **Schedules**: Specify when a replication link is used, and when different types of site data replicate.
- **Summarization**: Change settings for data summarization about network traffic that traverses replication links. By default, summarization occurs every 15 minutes. It's used in reports for database replication.
- **Database replication thresholds**: Define when the site reports links as degraded or failed. You can also configure when Configuration Manager raises alerts about replication links that have a degraded or failed status.

Database replication links

To control the transfer of data across the replication link, change settings for each link. Each replication link supports separate configurations. Each database replication link includes the following controls:

- Stop the replication of selected site data from a primary site to the CAS. This action causes the CAS to access this data directly from the database of the primary site.
- Schedule selected site data to transfer from a child primary site to the CAS.
- Define the settings that determine when a database replication link has a degraded or failed status.
- Specify when to raise alerts for a failed replication link.
- Specify how frequently Configuration Manager summarizes data about the replication traffic that uses the replication link. It uses this data in reports.

Practical 6B

Aim: Configure sites and hierarchies

i)Add site system roles

1. In the Configuration Manager console, go to the **Administration** workspace. Expand **Site Configuration**, and select the **Servers and Site System Roles** node.
2. In the ribbon, on the **Home** tab, in the **Create** group, select **Create Site System Server**.
3. On the **General** page, specify the general settings for the site system.
4. On the **Proxy** page, if roles on this server require an internet proxy, then specify settings for a proxy server.
5. On the **System Role Selection** page, select the site system roles that you want to add.
6. Complete the wizard. Additional pages may appear for specific roles. **ii) Install site system roles**

ii) Install site system roles

1. In the Configuration Manager console, go to the **Administration** workspace. Expand **Site Configuration**, and select the **Servers and Site System Roles** node. Select the existing site system server on which you want to install new site system roles.
2. In the ribbon, on the **Home** tab, in the **Server** group, select **Add Site System Roles**.
3. On the **General** page, review the settings.
4. On the **Proxy** page, if roles on this server require an internet proxy, then specify settings for a proxy server.
5. On the **System Role Selection** page, select the site system roles that you want to add.
6. Complete the wizard. Additional pages may appear for specific roles.

iii) Install cloud-based distribution points

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select **Cloud Distribution Points**. In the ribbon, select **Create Cloud Distribution Point**.
2. On the **General** page of the Create Cloud Distribution Point Wizard, configure the following settings:

    1. First specify the **Azure environment**.
    2. Select **Azure Resource Manager deployment** as the deployment method. Select **Sign in** to authenticate with an Azure subscription admin account. The wizard auto-populates the remaining fields from the information stored during the Azure AD integration prerequisite. If you own multiple subscriptions, select the **Subscription ID** of the desired subscription to use.
3. Select **Next**. Wait as the site tests the connection to Azure.
4. On the **Settings** page, specify the following settings, and then select **Next**:

1. **Region**: Select the Azure region where you want to create the cloud distribution point.
2. **Resource Group** (Azure Resource Manager deployment method only)

   Use existing: Select an existing resource group from the drop-down list.
   Create new: Enter the new resource group name to create in your Azure subscription.

- **Primary site**: Select the primary site to distribute content to this distribution point.
- **Certificate file**: Select **Browse** and select the .PFX file for this cloud distribution point's server authentication certificate. The common name from this certificate populates the required **Service FQDN** and **Service name** fields.

On the **Alerts** page, set up storage quotas, transfer quotas, and at what percentage of these quotas you want Configuration Manager to generate alerts. Then select **Next**.
Complete the wizard.

iv) Configuration options for site system roles

1. Certificate registration point
2. Distribution point
3. Enrollment point
4. Enrollment proxy point
5. Fallback status point

v) Database replicas for management points

Step 1 - Configure the site database server to publish the database replica

1. Set the SQL Server Agent to automatically start.
2. Create a local user group with the name **ConfigMgr_MPReplicaAccess**. For each database replica server that you use at this site, add its computer account to this group. This action enables those database replica servers to synchronize with the published database replica.
3. Configure a file share with the name **ConfigMgr_MPReplica**.
4. Add the following permissions to the **ConfigMgr_MPReplica** share:

   - Share permissions:

     SYSTEM: **Change**
     ConfigMgr_MPReplicaAccess: **Read**
   - NTFS permissions:
     SYSTEM: **Full Control**
     ConfigMgr_MPReplicaAccess: **Read**, **Read & execute**, and **List folder contents**

Use **SQL Server Management Studio** to connect to the site database and run the following stored procedure as a query: spCreateMPReplicaPublication

Step 2 - Configure the database replica server

1. Set the SQL Server Agent to automatic startup.
2. Use **SQL Server Management Studio** to connect to the local server. Browse to the **Replication** folder, select **Local Subscriptions**, and then select **New Subscriptions**. This action starts the **New Subscription Wizard**.

    1. On the **Publication** page, select **Find SQL Server Publisher**. Enter the name of the site database server, and then select **Connect**.
    2. Select **ConfigMgr_MPReplica**, and then select **Next**.
    3. On the **Distribution Agent Location** page, select **Run each agent at its Subscriber (pull subscriptions)**, and then select **Next**.
    4. On the **Subscribers** page, do one of the following actions:

        Select an existing database from the database replica server to use for the database replica, and then select **OK**.
        Select **New database** to create a new database for the database replica. On the **New Database** page, specify a database name, and then select **OK**.

    e. Select **Next** to continue.
    f. On the **Distribution Agent Security** page, select the properties button **(...)** in the Subscriber Connection row of the dialog box. Then configure the security settings for the connection.

    - Configure the account that runs the Distribution Agent process (*process account*):

        If the SQL Server Agent runs as local system, select **Run under the SQL Server Agent service account (This is not a recommended security best practice.)**
        If the SQL Server Agent runs by using a different account, select **Run under the following Windows account**, and then configure that account. You can specify a Windows account or a SQL Server account.
    - For **Connect to the Distributor**, select **By impersonating the process account**.
    - For **Connect to the Subscriber**, select **By impersonating the process account**.

        After you configure the connection security settings, select **OK** to save them, and then select **Next**.

    a. On the **Synchronization Schedule** page, select **Define schedule**, and then configure the **New Job Schedule**. Set the frequency to occur **Daily**, recur every **5 minute(s)**, and the duration to have **No end date**. Select **Next** to save the schedule, and then select **Next** again.
    b. On the **Wizard Actions** page, enable the option to **Create the subscriptions(s)**, and then select **Next**.
    c. Complete the wizard.

    Immediately after completing the New Subscription Wizard, use **SQL Server Management Studio** to connect to the database replica server database. Run the following

query to enable the TRUSTWORTHY database property: ALTER DATABASE <MP Replica Database Name> SET TRUSTWORTHY ON;
Review the synchronization status to validate that the subscription is successful:

- On the subscriber computer:
  In **SQL Server Management Studio**, connect to the database replica server, and expand **Replication**.
  Expand **Local Subscriptions**, right-click the subscription to the site database publication, and then select **View Synchronization Status**.
- On the publisher computer:
  In **SQL Server Management Studio**, connect to the site database computer, right-click the **Replication** folder, and then select **Launch Replication Monitor**.

To enable common language runtime (CLR) integration for the database replica, use **SQL Server Management Studio** to connect to the database replica on the database replica server. Run the following stored procedure as a query: exec sp_configure 'clr enabled', 1; RECONFIGURE WITH OVERRIDE
For each management point that uses a database replica server, add that management points computer account to the local **Administrators** group on that database replica server

Step 3 - Configure management points to use the database replica

Use the following information to configure a management point to use a database replica:

- To configure a new management point:
  1. On the **Management Point Database** page of the wizard to install the management point, select **Use a database replica**.
  2. Specify the FQDN of the computer that hosts the database replica.
  3. For the **ConfigMgr site database name**, specify the database name of the database replica on that computer.
- To configure a previously installed management point:
  1. Open the properties page of the management point, and switch to the **Management Point Database** tab.
  2. Select **Use a database replica**, and then specify the FQDN of the computer that hosts the database replica.
  3. Next, for **ConfigMgr site database name**, specify the database name of the database replica on that computer.

For each management point that uses a database replica, manually add the computer account of the management point server to the **db_datareader** role for the database replica.

In addition to configuring the management point to use the database replica server, enable **Windows Authentication** in **IIS** on the management point:

1. Open **Internet Information Services (IIS) Manager**.
2. Select the website used by the management point, and open **Authentication**.

3. Set **Windows Authentication** to **Enabled**, and then close **Internet Information Services (IIS) Manager**.

Step 4 -Configure a self-signed certificate for the database replica server

1. Go to the **Start** menu, select **Run**, and type mmc.exe. In the empty console, select **File**, and then select **Add/Remove Snap-in**.
2. In the **Add or Remove Snap-ins** dialog box, select **Certificates** from the list of **Available snap-ins**, and then select **Add**.
3. In the **Certificate snap-in** dialog box, select **Computer account**, and then select **Next**.
4. In the **Select Computer** dialog box, make sure that **Local computer: (the computer this console is running on)** is selected, and then select **Finish**.
5. In the **Add or Remove Snap-ins** dialog box, select **OK**.
6. In the console, expand **Certificates (Local Computer)**, expand **Personal**, and select **Certificates**.
7. Right-click the certificate with the friendly name of **ConfigMgr SQL Server Identification Certificate**, select **All Tasks**, and then select **Export**.
8. Complete the **Certificate Export Wizard** with the default options. Save the certificate with the **.cer** file name extension.

Step 5 - Configure the SQL Server Service Broker for the database replica server

1. Use **SQL Server Management Studio** to connect to the *replica server database*. Then run the following query to enable the Service Broker on the database replica **server: ALTER DATABASE <Replica Database Name> SET ENABLE_BROKER, HONOR_BROKER_PRIORITY ON WITH ROLLBACK IMMEDIATE**
2. On the *database replica server*, configure the Service Broker for client notification and export the Service Broker certificate. Run a SQL Server stored procedure that configures the Service Broker and exports the certificate as a single action. When you run the stored procedure, specify the FQDN of the database replica server, the name of the database replicas database, and specify a location for the export of the certificate file.

   Run the following query to configure the required details on the database replica server, and to export the certificate for the database replica server: EXEC **sp_BgbConfigSSBForReplicaDB '<Replica SQL Server FQDN>', '<Replica Database Name>', '<Certificate Backup File Path>'**

   After you export the certificate from the database replica server, place a copy of the certificate on the primary site database server.

3. Use **SQL Server Management Studio** to connect to the *primary site database*. After you connect to the primary sites database, run a query to import the certificate and specify the Service Broker port that's in use on the database replica server, the FQDN of the database replica server, and name of the database replicas database. This action configures the primary sites database to use the Service Broker to communicate to the database of the database replica server.

Run the following query to import the certificate from the database replica server and specify the required details: **EXEC sp_BgbConfigSSBForRemoteService 'REPLICA', '<SQL Service Broker Port>', '<Certificate File Path>', '<Replica SQL Server FQDN>', '<Replica Database Name>'**

4. On the *site database server*, run the following command to export the certificate for the site database server: **EXEC sp_BgbCreateAndBackupSQLCert '<Certificate Backup File Path>'**

   After you export the certificate from the site database server, place a copy of the certificate on the database replica server.

5. Use **SQL Server Management Studio** to connect to the *replica server database*. After you connect to the replica server database, run a query to import the certificate and specify the site code of the primary site and the Service Broker port that's in use on the site database server. This action configures the database replica server to use the Service Broker to communicate to the database of the primary site.

   Run the following query to import the certificate from the site database server**: EXEC sp_BgbConfigSSBForRemoteService '<Site Code>', '<SQL Service Broker Port>', '<Certificate File Path>'**

A few minutes after you complete the configuration of the site database and the database replica database, the notification manager at the primary site sets up the Service Broker conversation for client notification from the primary site database to the database replica.

Practical 7A

AIM: Install Orchestrator.

A complete Orchestrator installation includes

- a management server,
- one or more runbook servers,
- a SQL Server for hosting the Orchestrator database,
- a web server for hosting the Orchestrator web API service,
- a server for hosting the Runbook Designer and Runbook Tester,
- a web server for hosting the Orchestration Console.

Install Orchestrator management server

1. On the main page of the wizard, click **Install**.
2. On the **Product registration** page, provide the name and company for the product registration, and then click **Next**.
3. On the **Please read this License Terms** page, review, and accept the Microsoft Software License Terms, and then click **Next**. On the **Diagnostic and Usage data** page, review the Diagnostic and Usage data notice, and then click **Next**.
4. On the **Select features to install** page, ensure that **Management Server** is the only feature selected, and then click **Next**.
5. Your computer is checked for required hardware and software. If your computer meets all the requirements, the **All prerequisites are installed** page appears. Click **Next** and proceed to the next step.

Install Orchestrator runbook server

1. On the server where you want to install Orchestrator runbook server, install the Microsoft Visual C++ Redistributable package and start the Orchestrator Setup Wizard.
2. On the main setup page, under **Standalone installations**, click **Runbook server**.
3. On the **Product registration** page, provide the name and company for the product registration, and then click **Next**.
4. On the **Please read this License Terms** page, review, and accept the Microsoft Software License Terms, and then click **Next**.

   On the **Diagnostic and Usage data** page, review the Diagnostic and Usage data notice, and then click **Next**.

5. Your computer is checked for required hardware and software. If your computer meets all the requirements, the **All prerequisites are installed** page appears.

Install Orchestrator Web API service

1. On the server where you want to install the Orchestrator web API, install the Microsoft Visual C++ Redistributable package and start the Orchestrator Setup Wizard.
2. On the main setup page, under **Standalone installations**, click **Web API Service**.
3. On the **Product registration** page, provide the name and company for the product registration, and then click **Next**.
4. On the **Please read this License Terms** page, review, and accept the Microsoft Software License Terms, and then click **Next**.

   On the **Diagnostic and Usage data** page, review the Diagnostic and Usage data notice, and then click **Next**.

5. Your computer is checked for required hardware and software. If your computer meets all the requirements, the **All prerequisites are installed** page appears.

Install Orchestration Console

1. On the server where you want to install the Orchestration Console, install the Microsoft Visual C++ Redistributable package and start the Orchestrator Setup Wizard. To start the wizard on your product media or network share, double-click **SetupOrchestrator.exe**.
2. On the main **Setup** page, under **Standalone installations**, click **Orchestration Console**.
3. On the **Product registration** page, provide the name and company for the product registration, and click **Next**.
4. On the **Please read this License Terms** page, review, and accept the Microsoft Software License Terms, and click **Next**. On the **Diagnostic and Usage data** page, review the Diagnostic and Usage data notice, and click **Next**.
5. Your computer is checked for required hardware and software. If your computer meets all the requirements, **All prerequisites are installed** page appears.

Install Orchestrator Runbook Designer

1. On the server where you want to install the Orchestrator Runbook Designer, install the Microsoft Visual C++ Redistributable package and start the Orchestrator Setup Wizard.
2. To start the wizard on your product media or network share, double-click **SetupOrchestrator.exe.**
3. On the main wizard page, click **Runbook Designer**.
4. On the **Product registration** page, provide the name and company for the product registration, and then click **Next**.
5. On the **Please read this License Terms** page, review, and accept the Microsoft Software License Terms

Connect a Runbook Designer to a management server

1. In the Runbook Designer, select the **Connect to a server** icon in the navigation pane under the **Connections** pane.

2. In **System Center Orchestrator Connection**, enter the name of the server that hosts your Orchestrator management server, and then click **OK.**

Enable network discovery

1. On the desktop of your computer running Windows server, click **Start**, click **Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, click **Choose Home group and Sharing Options**, and then click **Change advanced sharing settings**.
2. To change the **Domain** profile, if needed, click the **Arrow** icon to expand the section options and make any necessary changes.
3. Select **Turn on network discovery**, and then click **Save changes**.

   If you are prompted for an administrator password or confirmation, type the password, or provide confirmation.

View runbook server properties

The properties for a runbook server include an optional description and the account information to use for the Runbook Service. You can modify the description but can only view the service credentials.

1. In the **Connections** pane, select the Runbook Servers folder. In the right pane, right-click the runbook server to select **Properties**.
2. If you want to add or change the **Description** box, type a description for this runbook server, and then click **Finish**

Practical 7B

AIM: Create and test a monitor runbook

Creating and Testing a Sample Runbook

The following topic describes how to create and test a simple runbook. The purpose of this runbook is to detect when a text file is added to a particular folder, copy that file to another folder, read the contents of the file, append a line from the copied file to another file, and then delete the original file.

The runbook starts with a **Monitor File** activity to wait for the text file to be created. It then uses the **Copy File**, **Read Line**, **Append Line**, and **Delete File** activities to perform the other functions. A **Junction** activity is used to coordinate the activities so that the **Copy File** and **Append Line** activities are both completed before the source file is deleted.

Creating the runbook
Use the following procedures to create the runbook by using the required activities.

To create a runbook

1. Click **Start**, point to **All Programs**, click **Microsoft System Center 2016**, click **Orchestrator**, and then click **Runbook Designer**.
2. In the **Connections** pane, right-click **Runbooks** to select **New**, and then click **Runbook**.

   A **New Runbook** tab appears at the top of the **Runbook Designer** Design workspace with the name **New Runbook**.

3. Right-click the **New Runbook** tab to select **Rename**.

   In the **Confirm Check out** dialog box, click **Yes**.

4. Type **Append and Copy Workflow** in the **Input** box, and then press Enter.

You have created a new runbook and are ready to begin adding and configuring activities

To add and configure a Monitor File activity

1. With the newly created **Append and Copy Workflow** runbook open, in the **Activities** pane, expand the **File Management** category.
2. Click and drag the **Monitor File** activity to the **Runbook Designer** Design workspace.
3. Double-click the **Monitor File** activity to open its **Properties** dialog box.
4. In the **In folder** box, type **C:\Drop**.
5. In the **Filters** section, click the **Add** button.
6. In the **Filter Settings** dialog box, in the **Name** list, select **File Name**.
7. In the **Relation** list, select **Matches Pattern**.

8. In the **Value** box, type ***.txt**.
9. Click **OK**.
10. Click the **Triggers** tab.
11. In the **Trigger if one of the files was** section, select the **Created** check box, and then click **Finish**.

The **Monitor File** activity is created and configured to watch for any new text files that are created in the C:\Drop folder.

To add additional activities to the runbook

1. In the **Activities** pane, expand the **File Management** category.
2. Click and drag the **Copy File** activity to the **Runbook Designer** Design workspace.
3. Expand the **Text File Management** category.
4. Click and drag the **Read Line** activity to the **Runbook Designer** Design workspace.
5. To create a link between the **Monitor File** activity and the **Copy File** activity, click and drag the right arrow of the **Monitor File** activity to the **Copy File** activity.
6. To create a link between the **Monitor File** activity and the **Read Line** activity, click and drag the right arrow of the **Monitor File** activity to the **Read Line** activity.

By adding both the **Read Line** activity and the **Copy File** activity, you have created a workflow.

To configure the Copy File activity

1. In the **Append and Copy Workflow** runbook, right-click the **Copy File** activity to select **Properties**.
2. On the **Details** tab, right-click the **File** box to select **Subscribe**, and then click **Published Data** to open the **Published Data** dialog box.

   The **Monitor File** activity is listed at the top of the **Published Data** dialog box because this is the activity just before to the selected activity.

3. In the **Name** column, select **Name and path of the file**, and then click **OK**. This populates the **File** property of the **Copy File** activity with the name of and path to the file from the **Monitor File** activity.
4. In the destination **Folder** box, type **C:\Copy**.
5. Click **Finish**.

The **Copy File** activity is now configured to copy files from the source folder to the destination folder.

To configure the Read Line activity

1. In the **Append and Copy Workflow** runbook, right-click the **Read Line** activity to select **Properties**.

2. On the **Details** tab, right-click the **File** box to select **Subscribe**, and then click **Published Data** to open the **Published Data** dialog box.
3. In the **Activities** list, select **Monitor File**.
4. In the **Name** column, select **Name and path of the file**, and then click **OK**.
5. Click the ellipse (**...**) button to the right of the **File encoding** box, and then select **auto**.
6. In the **Line numbers** box, type **1-END**, and then click **OK**.
7. Click **Finish**.

The Read Line activity is now configured.

To add an Append Line activity

1. In the **Activities** pane, expand the **Text File Management** category.
2. Click and drag the **Append Line** activity to the **Runbook Designer** Design workspace to the right of the **Read Line** activity.
3. To create a link from the **Read Line** activity to the **Append Line** activity, click and drag the right arrow of the **Read Line** activity to the **Append Line** activity.
4. Right-click the **Append Line** activity to select **Properties**.
5. On the **Details** tab in the **File** box, type **C:\Copy\Masterlog.txt**.
6. Click the ellipse (**...**) button to the right of the **File encoding** box, and then select **auto**.
7. Right-click the **Text** box to select **Subscribe**, and then click **Published Data** to open the **Published Data** dialog box.
8. In the **Name** column for the **Read Line** activity, select **Line text**, and then click **OK**.
9. Click **Finish**.

The **Append File** activity is now configured to append files to the **Masterlog.txt** file.

To synchronize branches of a runbook

1. In the **Activities** pane, expand the **Runbook Control** category.
2. Click and drag the **Junction** icon to the **Runbook Designer** Design workspace.
3. To create a link from the **Append Line** activity to the **Junction** activity, click and drag the right arrow of the **Append Line** activity to the **Junction** activity.
4. To create a link from the **Copy File** activity to the **Junction** activity, click and drag the right arrow of the **Copy File** activity to the **Junction** activity.
5. Right-click the **Junction** activity to select **Properties**.
6. Click the ellipse (**...**) button next to the **Return data from** box, and then select **Copy File**. Click **OK**. This action configures the activity to return the same Published Data as the **Copy File** activity.
7. Click **Finish**.

The **Junction** activity is configured to coordinate the workflow so that no further activities run until both the **Copy File** activity and **Append Line** activity finish.

To add and configure the Delete File activity

1. In the **Activities** pane, expand the **File Management** category.
2. Click and drag the **Delete File** icon to the **Runbook Designer** Design workspace.
3. To create a link from the **Junction** activity to the **Delete File** activity, click and drag the right arrow of the **Junction** activity to the **Delete File** activity.
4. Right-click the **Delete File** activity to select **Properties**.
5. Right-click the **Path** box to select **Subscribe**, and then click **Published Data** to open the **Published Data** dialog box.

   In the **Activity** list, select **Copy File**.

6. In the **Name** column, select **Name and path of the original file**, and then click **OK**.
7. Click **Finish**.

The **Append and Copy Workflow** runbook is now completed. It should look similar to the following illustration.

Testing the runbook

You can test the runbook by using the Runbook Tester. This tool lets you run the entire runbook and inspect the completion status and output of each activity. The Runbook Tester runs the activities, so you must first create the folders specified for the runbook.

To test the runbook

1. Create a folder on the runbook server called C:\Drop.
2. Create a folder on the runbook server called C:\Copy.
3. With the **Append and Copy Workflow** runbook selected in the Runbook Designer, on the toolbar, click **Runbook Tester**.
4. Click **Run To Breakpoint**. The **Monitor File** activity is loaded and waits for a text file to be created in the C:\Drop folder.
5. Open **Notepad** and type a few lines of text. Save the file as C:\Drop\File1.txt.
6. Wait a few moments for the other activities to run. Ensure that each of the activities is completed successfully.
7. To view the Published Data and other details of an activity, click **Show Details** for the activity.
8. Open the C:\Drop folder and ensure that the file has been removed.
9. Open the C:\Copy folder and ensure that the file has been copied. Also verify that the MasterLog.txt file has the contents of the original file.

PRACTICAL 8A

AIM: Manage Orchestrator Servers - 1

i)Runbook permissions

To view or modify the permissions of a runbook

1. In the Runbook Designer, in the **Connections** pane, click the **Runbooks** folder.
2. In the **Runbook Designer** Design workspace, right-click the tab for a runbook to select **Permissions**.
3. To give another user or security group access to the runbook, click the **Add** button, and select the user or security group from the local computer or from the domain.
4. If the user or security group should be able to view and run the runbook, select the **Allow** check box next to **Read**.
   If the user or security group should be able to change the runbook, select the **Allow** check box next to **Write**.
   If the user or security group should be able to change permissions for the runbook, select the **Allow** check box next to **Full Control**.
5. To close the **Permissions for Runbook** dialog box and save any changes, click **OK**.

ii) Back up Orchestrator

- Backup of the Orchestrator database.
- File backup of the Orchestrator management server.
- File backup of each Runbook server and Orchestrator web server.

iii) Benchmark

To create a runbook that can be used to benchmark your Orchestrator environment

1. Create a new runbook.
2. Add a **Compare Values** activity from the Standard Activity palette. Double-click the activity to configure it.
3. Click the **General** tab and configure this activity to compare strings (the default value).
4. Click the **Details** tab, type the value **STRING** in the **Test** box and select **is empty**.
5. Click **Finish** to save the updates to the activity.
6. Right-click the activity and select **Looping**.
7. Select the **Enable** checkbox and enter the number **0** (zero) for **Delay between attempts**.
8. Click the **Exit** tab.
9. Change the default exit condition. Click **Compare Values**, check the **Show Common Published Data** checkbox, and select **Loop: Number of attempts**. Click **OK** to save this change.
10. Select **value** from the updated exit condition and type the number **10000** (ten-thousand). Click **OK** to save this change.
11. Click **Finish** to save these updates.
12. Click **Check In** to save the changes to the Orchestrator database.

iv)Configure runbook throttling

1. Navigate to the folder whereby default the Runbook Server Runbook Throttling tool is stored: C:\Program Files\Microsoft System Center\Orchestrator\Management Server.
2. Type one of the following commands:

    - To apply the change to one runbook server:

      aspt <RunbookServerName> <MaximumRunningRunbooks>.

      For example, to set the maximum number of runbooks that RunbookServer1 runs to 40: aspt RunbookServer1 40

    - To apply the change to all runbook servers:

      aspt * <MaximumRunningRunbooks>.

      For example, to set the maximum number of runbooks that all runbook servers run to 40: aspt * 40

2. Restart the **Orchestrator Runbook Service**.

v) Recover a database

Run a backup

1. Back up the service master key for Microsoft SQL Server. This is a one-time operation. Note "password" is the password that will be used to protect the service master key in the file that is created. If the password is lost, the service master key cannot be recovered from the file.

   SQLCopy

   ```
   BACKUP SERVICE MASTER KEY TO FILE = 'path_to_file'
         ENCRYPTION BY PASSWORD = 'password'
   ```

2. Back up the entire Orchestrator database. The backup may be performed when the system is running, but it is best to perform the backup when all runbook authors have checked in any pending changes to their runbooks. Pending changes are cached on the Runbook Designer and are not backed up with a database backup.

To restore the database

1. If you are restoring to the same database server from which the backup was taken, and the service master key has not changed, simply restore the backup.

2. If you are restoring to a different database server with a different service master key, or you are restoring to the same database from which the backup was taken but the service master key has changed, the service master key must be restored to match the one used during the database backup. Use the procedure for restoring the service master key for Microsoft SQL Server.

   SQLCopy

   BACKUP SERVICE MASTER KEY TO FILE =
   'c:\temp_backups\keys\service_master_key'
   ENCRYPTION BY PASSWORD = '3dH85Hhk003GHk2597jheij4'
   Restore the database from the backup.

3. On the Orchestrator Management Server, run the Data Store Configuration utility (DBSetup) from the Start menu.
4. Provide the connection details to connect to the new database.
5. Restart the Management Service.
6. Run the Data Store Configuration utility on each Runbook Server. This utility is not located in the Start menu on Runbook Servers. It can be found in <OrchestratorInstallDir>\Management Server.

   Restart the Runbook Server(s).

7. Follow the Web Components Recovery Process to update the Web Components to connect to the new database.

Practical 8B

AIM: Manage Orchestrator Servers – 2

i)Recover web components

How to recover web components

When you use the Database Configuration utility to modify the Orchestrator database, the tool will not modify the Web Service database reference (only the installer performs this task). You will need to manually modify it after updating with the database configuration utility.

To do this, you will need to complete the following actions:

To modify the Web Service database reference

1. Open a Command Prompt using **Run as administrator**.
2. Execute the following command (assuming the default installation path):

   PowerShellคัดลอก
   C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pdf "connectionStrings" "C:\Program Files (x86)\Microsoft System Center 2016\Orchestrator\Web Service\Orchestrator2016"

3. Open IIS Manager and navigate to the Orchestrator2016 virtual application.
4. Open up Connection Strings and then modify OrchestratorContext. Locate the segment that starts with provider=System.Data.SqlClient;provider connection string and then modify the Data Source and Initial Catalog attributes according to your new SQL Server and Database Catalog name respectively, then click OK.
5. If you want to re-encrypt the connection strings, you can execute the following command at the command prompt:

   PowerShellคัดลอก
   C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pef "cone

ii) Add an integration pack

Register an integration pack

1. On the management server, copy the .OIP file for the integration pack to a local hard drive or network share.
2. Start the Deployment Manager.
3. In the navigation pane of the Deployment Manager, expand Orchestrator Management Server, right-click Integration Packs to select Register IP with the Management Server. The Integration Pack Registration Wizard opens.
4. Click Next.
5. In the Select Integration Packs or Hotfixes dialog box, click Add.

6. Locate the .OIP file that you copied locally from step 1, click Open, and then click Next.
7. In the Completing the Integration Pack Wizard dialog box, click Finish.
8. On the End User Agreement dialog box, read the Microsoft Software License Terms, and then click Accept.

Deploy an integration pack

1. In the navigation pane of Deployment Manager, right-click Integration Packs, click Deploy IP to Action Server or Client.
2. Select the integration pack that you want to deploy, and then click Next.
3. Enter the name of the runbook server or computers with the Runbook Designer installed, on which you want to deploy the integration pack, click Add, and then click Next.
4. Continue to add additional runbook servers and computers running the Runbook Designer, on which you want to deploy the integration pack. Click Next.
5. In the Installation Options dialog box, configure the following settings.
6. To choose a time to deploy the integration pack, select the Schedule installation check box, and then select the time and date from the Perform installation list.
7. Click one of the following:
    - Stop all running runbooks before installing the integration pack to stop all running runbooks before deploying the integration pack.
    - Install the Integration Packs without stopping the running Runbooks to install the integration pack without stopping any running runbooks.
8. Click Next.
9. In the Completing Integration Pack Deployment Wizard dialog box, click Finish.
10. When the integration pack is deployed, the Log Entries dialog box displays a confirmation message.

Upgrade an integration pack

1. On all computers that have a runbook server or Runbook Designer installed, uninstall any earlier version of the integration pack. You can achieve this by doing any one of the following:
    - Remove it by following the instructions in How to Uninstall and Unregister an Integration Pack.
    - Log into each computer and uninstall the integration pack from Programs and Features in Control Panel.
    - On the management server, start the Deployment Manager, and then right click on the deployed integration pack for each Runbook Server or Runbook Designer computer and click Uninstall Integration Pack or Hotfix.
    - Register and deploy the upgraded integration pack.

iii) View Orchestrator data with PowerPivot

View Orchestrator data using PowerPivot

Install PowerPivot

You must install PowerPivot for Excel to enable the product.

Create a connection to an Orchestrator feed

Use PowerPivot to configure a connection to Orchestrator web service. Orchestrator uses the Open Data Protocol (OData), which PowerPivot can consume.

Configure a connection to Orchestrator web service. Orchestrator uses the Open Data Protocol (OData), which PowerPivot can consume.

1. Open Excel.
2. Click the **PowerPivot** tab above the ribbon.
3. Click **PowerPivot Window** on the ribbon. A **PowerPivot for Excel** book opens.
4. Click **From Data Feeds** on the ribbon. A **Table Import Wizard** opens.
5. Enter the Orchestrator web service URL in the **Data Feed URL** box. The web service URL is on port 81 of the Orchestrator SQL Server. For example, http://orchestrator:81/Orchestrator2016/Orchestrator.svc.
6. Click **Test Connection**.
7. If the test connection is successful, click **OK** and proceed to the next step.

   If the test connection fails, do the following:

   1. Click **OK**.
   2. Click **Advanced**. The **Advanced** dialog box opens.
   3. In the **Security** section, change **Integrated Security** to **Basic**.
   4. Change **Persist Security Info** to **True**.
   5. Enter your **User ID** and **Password** in the appropriate boxes.
   6. Click **Test Connection**.
   7. Click **OK** and click **OK**.
8. Click **Next**.
9. Select the check boxes of the table or tables that you want to import.
10. To filter columns, select a table, click **Preview & Filter**, clear any boxes to exclude, and then click **OK**.
11. Click **Finish**. The data is imported.
12. Click **Close**.

Create a summary of runbook results

The following procedure describes the steps to create a pivot table containing a list of all runbooks and the count of results, grouped by the runbook server that ran the runbook instance.

Create a connection to the data feed

1. Open Excel.
2. Click the **PowerPivot** tab above the ribbon.
3. Click **PowerPivot Window** on the ribbon. A **PowerPivot for Excel** book opens.
4. Click **From Data Feeds** on the ribbon. A **Table Import** wizard opens.
5. Enter the Orchestrator web service URL in the **Data Feed URL** box.
6. Click **Next**.
7. Select the check boxes of the **Runbooks**, **RunbookInstances**, and **RunbookServers** tables.
8. Click **Finish**. The data is imported.

9. Click **Close**

Create relationships in PowerPivot

1. In the **PowerPivot for Excel** window, select the **RunbookInstance** tab.
2. Right-click the header of the **RunbookId** column to select **Create Relationship**.
3. In the **Related Lookup Table** list, select **Runbooks**, and in the **Related Lookup Column** list, select **Id**, and then click **Create**.
4. Right-click the header of the **RunbookServerId** column to select **Create Relationship**.
5. In the **Related Lookup Table** list, select **RunbookServers**, and in the **Related Lookup Column** list, select **Id**, and then click **Create**.

Create a pivot table

1. In the **PowerPivot for Excel** window, click **PivotTable** on the ribbon, and select **PivotTable**.
2. In the **Create PivotTable** dialog box, select **New Worksheet**, and then click **OK**.
3. In the **PowerPivot Field List**, under **RunbookServers**, click and drag **Name** to the **Row Labels** box.
4. In the **PowerPivot Field List**, under **Runbooks**, click and drag **Name** to the **Row Labels** box.
5. In the **PowerPivot Field List**, under **RunbookInstances**, click and drag **Status** to the **Column Labels** box.
6. In the **PowerPivot Field List**, under **RunbookInstances**, click and drag **RunbookId** to the **Sum Values** box.
7. Right-click **RunbookId** to select **Summarize by**, and then click **Count**.

You can now modify the default labels and format your table for presentation.

iv) Change Orchestrator user groups

Modify the Orchestrator users group

You might want to change the Orchestrator users group after installation because of changes in your environment. For example, you might want to use a local group during installation, and then change it to a domain account later.

PermissionsConfig tool

You can change the Orchestrator Users group by using the PermissionsConfig tool, which is located on the management server in **<InstallDir>\Management Server**. The syntax of this tool is as follows:

PowerShellCopy
PermissionsConfig -OrchestratorUsersGroup <GroupName> -OrchestratorUser <UserName> [-remote]

Note that the PermissionsConfig tool does not send results to standard output. To view the results of the command, check the **%errorlevel%** in the Orchestrator log file that is located at **C:\Users\SCXSVC\AppData\Local\SCO\LOGS**. The results are 1 for failure, 0 for success.

You can get an explanation of the parameters for the PermissionsConfig tool by typing the following command:

PowerShellCopy
PermissionsConfig -help
For example, to change the Orchestrator users group to a group that is named Orchestrator Users in a domain that is named Contoso, use the following command:
PowerShellCopy
PermissionsConfig -OrchestratorUsersGroup "Contoso\Orchestrator Users" -remote

v) Common activity properties
Common Activity Properties
All activities have properties. The Properties dialog box for each activity has multiple tabs that provide access to the settings for the activity. The particular set of tabs varies between activities, but there are several common property types.

Details
This tab contains various properties specific to an activity. Many activities require you to at least enter a computer name, IP address, file name, file path, or file folder location.

Run Behavior
This tab contains the properties that determine how the activity handles multi-value Published Data. It also defines the notifications created if the activity fails or runs for an excessive period.

Published Data Behavior

By default, Published Data is passed as multiple individual outputs. You can alternatively specify that all values be flattened into a single comma-delimited value (.csv) file.

When you enable the Flatten feature, you also choose a multi-value formatting option.

Event Notifications

Some activities are expected to take a limited amount of time to finish. If the activity does not finish within the specified period, the activity can be stalled or another issue prevents the activity from finishing. You can define the number of seconds to wait for completion of the activity, after which a platform event is sent to report the delay in completion. You can also choose whether to generate a platform event if the activity returns a failure.

Security Credentials
The settings on the Security Credentials tab let you specify the account that runs the Runbook Server Service. This is useful when the activity performs activities with resources on a remote computer.

vi) Computer groups

System Center - Orchestrator is designed to interact with all of your data center systems. Computer groups let you target selected activities against a set of similar computer systems instead of a single computer. By configuring the activities in your runbook to use a computer group, you have the flexibility to add computers dynamically by adding them to the computer group.

You can create computer groups by using Active Directory queries, and you can manage the list of computers in a group outside of Orchestrator. For example, if you have a computer group that is created from an Active Directory query that retrieves all instances of Microsoft SQL Server, when an instance of SQL Server is added to your Active Directory system, it is automatically included in that group.

Manage computer groups

To use computer groups in your activities, create a computer group, and then add computers to it.

You can also organize your computer groups into folders. Use the following steps to create a new folder.

Create a folder

1. In the **Connections** pane in the Runbook Designer, click the **Computer Groups** folder or a subfolder.
2. Right-click to select **New**, and then click **Folder**.

Use the following procedure to add a computer group. To add computers by using an Active Directory query or a Configuration Manager collection, use the Active Directory Integration Pack or the Integration Pack for Configuration Manager.

Add a computer group

1. In the **Connections** pane, right-click the **Computer Groups** folder or a subfolder.
2. Select **New**, and then click **Computer Group** to open the **New Computer Group** dialog box.
3. In the **New Computer Group** dialog box, on the **General** tab, in the **Name** and **Description** boxes, type a name and description of the computer group.
4. Click the **Contents** tab. The list displays all the computer entries that make up this computer group.
5. Click **Add** to open the **Add Computer to Computer Group** dialog box.
6. Enter the name of the computer that you are adding, or click the ellipsis **(...)** button next to the **Computer** box, and then select the applicable computer. Click **OK** to add the computer.
7. To add more computers to the group, repeat the previous two steps.

Modify settings

1. To modify the settings of an entry you added, click the entry on the **Contents** tab, and then click **Modify**.
2. To remove an entry on the **Contents** tab, click the entry, and then click **Remove**.

Use a computer group in an activity

Any standard activity that requires you to identify a **Computer** name in the **Configuration Properties** dialog box, such as the **Send Event Log Message** activity, can use a computer group. Other activities can use the **Computer Group** where you define a remote system or computer.

Use the following procedure to use a computer group.

1. Right-click the applicable activity from your runbook, select **Properties** on the menu, and then select the **Details** tab to open the **Activities Properties** dialog box.
2. In the **Computer** box, right-click to open a menu, select **Subscribe**, and then select **Computer Group** to open the **Select Computer Group** dialog box.
3. Select the computer group, and then click **OK**.

   A placeholder {computer group name} is inserted next to the computer name in the **Computer** box.

   When the activity runs, it runs on each computer in the group.

Practical 9

AIM: Install and Deploy DPM.

i) Install DPM: -

1. If required, extract the DPM 2016.exe (for DPM 2016)/DPM 2019.exe (for DPM 2019) file onto the machine on which you want to run DPM. To do this, run the exe file, and on the **Welcome** screen, select **Next**. In **Select Destination Location**, specify where you want to extract the installation files to. In **Ready to Extract**, select **Extract**. After the extraction finishes, go to the specified location and run **Setup.exe**.
2. On the **Welcome** page of DPM Setup, select **Next**. On the **License Terms** page, accept the agreement > **OK**.
3. On the **Prerequisites Check** page, wait for the check and resolve any issues before proceeding.
4. On the **Product Registration** page, select **Next**. On the **Microsoft Update Opt-In** page, choose whether you want to include DPM in your Microsoft Updates.
5. On the **Summary of Settings** page, check the settings and select **Install**. After the installation is completed, select **Close**. It will automatically launch a Windows update to check for changes.

ii) Deploy the DPM protection agent: -

1. In DPM Administrator Console, select **Management** > **Agents**. Select **Install** on the tool ribbon to open the Protection Agent Installation Wizard.
2. On the **Select Agent Deployment Method** page, select **Install agents** > **Next**.
3. On the **Select Computers** page, DPM displays a list of available computers that are in the same domain as the DPM server. Add the required computer.

    - The first time you use the wizard, DPM queries Active Directory to get a list of available computers. After the first installation, DPM stores the list of computers in its database, which is updated once every day by the auto-discovery process.
    - To find a computer in another domain that has a two-way trust relationship with the domain that the DPM server is located in, you must type the fully qualified domain name (FQDN) of the computer that you want to protect. For example, *<Computer1>.Domain1.contoso.com*, where *Computer1* is the name of the computer that you want to protect and *Domain1.contoso.com* is the domain to which the target computer belongs.
    - The **Advanced** button page is enabled only when there's more than one version of a protection agent available for installation on the computers. You can use this option to install a previous version of the protection agent that was installed before you upgraded DPM server to a more recent version.

    On the **Enter Credentials** page, type the username and password for a domain account that is a member of the local Administrators group on all selected computers.

    - In the **Domain** box, accept or type the domain name of the user account that you're using to install the protection agent on the target computer. This account may belong

to the domain that the DPM server is located in or to a domain that has a two-way trust relationship with the domain that the DPM server is located in.

- If you're installing a protection agent on a computer across a trusted domain, enter your current domain user credentials. You can be a member of any domain that has a two-way trust relationship with the domain that the DPM server is located in, and you must be member of the local Administrators group on all selected computers on which you want to install an agent.
- If you select a node in a cluster, DPM detects all additional nodes in the cluster and displays the **Select Cluster Nodes** page.

On the **Select Cluster Nodes** page, select an option that you want DPM to use for installing agents on additional nodes in the cluster and then select **Next**.

On the **Choose Restart Method** page, select the method to use to restart the selected computers after the protection agent is installed. The computer must be restarted before you can start protecting data. A restart is necessary to load the volume filter that DPM uses to track and transfer block-level changes between the DPM server and the protected computers.

- If you select to restart the computers later, the protection agent installation status isn't refreshed automatically on the **Agents** tab in the **Management** task area after the computer restarts, and you'll need to select **Refresh Information**.
- You don't need to restart the computer if you're installing a protection agent on another DPM server.
- If any of the computers that you selected are nodes in a cluster, an additional **Choose Restart Method** page appears, which you can use to select the method to restart the clustered computers. You'll need to install a protection agent on all the nodes in a cluster to successfully protect the clustered data. The computers must be restarted before you can start protecting data. As time is required to start services, it might take a few minutes after a restart before DPM can contact the agent on the cluster.
- DPM won't automatically restart a computer that belongs to a Microsoft Cluster Server (MSCS) cluster. You must manually restart computers in an MSCS cluster.

On the **Summary** page, select **Install** to begin the installation. If the EULA appears, accept it for the installation to start. On the **Task** tab of the installation page, you can see whether the installation is successful. You can select **Close** before the wizard is finished and monitor the installation progress in the **Agents** tab in the **Management** task area. If the installation is unsuccessful, you can view the alerts in the **Monitoring** task area on the **Alerts** tab.

iii) Deploy protection groups: -

- **Data sources** - The servers, computers, and workloads you want to protect.
- **Back-up storage** - How the protected data should be backed up in the short-term and long-term.
- **Recovery points** - The recovery points from which replicated data can be recovered.
- **Allocated disk space** - The disk space allocated to data from the storage pool.
- **Initial replication** - How the initial replication of data should be handled using either over the network or manually offline.
- **Consistency checks** - How the replicated data should be checked for consistency.

iv) Configure firewall settings: -

1. In Server Manager, select **Local Server** > **Tools** > **Windows Firewall with Advanced Security**.
2. In the **Windows Firewall with Advanced Security** console, verify that Windows Firewall is on for all profiles and then select **Inbound Rules**.
3. To create an exception, in the **Actions** pane, select **New Rule** to open the **New Inbound Rule** Wizard.

   On the **Rule Type** page, verify that **Program** is selected and then select **Next**.

4. Configure exceptions to match the default rules that would have been created by DPM Setup if Windows Firewall had been enabled when DPM was installed.

   a. To manually create the exception that matches the default Microsoft System Center 2012 R2 Data Protection Manager rule on the **Program** page, select **Browse** for the **This program path** box and then browse to **<system drive letter>:\Program Files\Microsoft DPM\DPM\bin** > **Msdpm.exe** > **Open**> **Next**.

      On the Action page, leave the default setting of **Allow the connection** or change the settings according to your organization's guidelines > **Next**.

      On the **Profile** page, leave the default settings of **Domain**, **Private**, and **Public** or change the settings according to your organization's guidelines > **Next**.

      On the **Name** page, type a name for the rule and optionally a description > **Finish**.

   b. Now follow the same steps to manually create the exception that matches the default Microsoft System Center 2012 R2 Data Protection Replication Agent rule by browsing to **<system drive letter>:\Program Files\Microsoft DPM\DPM\bin** and selecting **Dpmra.exe**.

If you're running System Center 2012 R2 with SP1, the default rules will be named by using **Microsoft System Center 2012 Service Pack 1 Data Protection Manager**.

PRACTICAL 10

AIM: Protect Workloads.

i. Back up Hyper-V virtual machines.

System Center Data Protection Manager (DPM) protects Hyper-V virtual machines by backing up the data of virtual machines. You can back up data at the Hyper-V host level to enable VM-level and file-level data recovery or back up at the guest-level to enable application-level recovery.

Add the following machine accounts to the backup operator groups and share permissions:

- If protecting a highly available (HA) VM, provide the machine account name of the host cluster and cluster nodes and DPM server.
- If protecting a non-HA VM, provide the machine name of the Hyper-V host and the DPM server.

To add the machine accounts to the backup operator groups, run the following steps for each node in the SOFS cluster:

1. Open the command prompt, and type **lusrmgr.msc** to open Local Users and Groups.
2. In the Local Users and Groups page, select **Groups**.
3. In the list of groups, select and hold **Backup Operators** and select **Properties**.

   The **Backup Operators Properties** page opens.

4. In the **Backup Operators Properties** page, select **Add**.
5. In the **Select Users, Computers, Services Accounts, or Groups** page, select **Object Types**. The **Object Types** page opens.
6. In the **Object Types** page, select **Computers** and select **OK**. The **Object Types** page closes.
7. In the **Select Users, Computers, Service Accounts, or Groups** page, enter the name of the server or cluster and select **Check Names**.
8. Once you've identified the computers, restart the node.

To give permissions to the share, do the following:

1. On a server where the SOFS/SMB share is hosted, open **Server Manager** > **File and Storage Services** > **Shares**.
2. Select and hold the VM storage share, and then select **Properties**.
3. In the **Properties** page, on the left navigation menu, select **Permissions**.
4. Select **Customize permissions** to open the Advanced Security Settings page.
5. On the **Permissions** tab, select **Add**.
6. Select **Select a Principal**.
7. In the **Select User, Computer, Services Account, or Group** page, select **Object Types**.
8. In the **Object Types** page, select **Computers** and select **OK**.

9. In the **Select User, Computer, Service Account, or Group** page, enter the name of the Hyper-V node or cluster name you want to have permission for.
10. Select **Check Names** to resolve the name and select **OK**.
11. In the **Permission Entry for Share** page, select **Full Control** and select **OK**.
12. In the **Advanced Security Settings for Share** page, select the **Share** tab and repeat steps 6-11 for the **Share** tab instead of the **Permissions** tab.
13. When you've finished adding permissions for the servers, select **Apply**.

    This prepares the VMs on SOFS shares for the backup process.

The following are requirements for maintaining protection during live migration:

- The Hyper-V hosts for the virtual machines must be located in a System Center VMM cloud on a VMM server running at least System Center 2012 with SP1.
- The DPM protection agent must be installed on all Hyper-V hosts.
- DPM servers must be connected to the VMM server. All Hyper-V host servers in the VMM cloud must also be connected to the DPM servers. This allows DPM to communicate with the VMM server so that the DPM can find out on which Hyper-V host server the virtual machine is currently running and to create a new backup from that Hyper-V server. If a connection can't be established to the Hyper-V server, the backup fails with a message that the DPM protection agent is unreachable.
- All the DPM servers, VMM servers, and Hyper-V host servers must be in the same domain.

ii) Back up SQL Server with DPM: -

System Center Data Protection Manager (DPM) provides backup and recovery for SQL Server databases. In addition to backing up SQL Server databases, you can run a system backup or full bare-metal backup of the SQL Server computer. Here's what DPM can protect:

- A standalone SQL Server instance
- A SQL Server Failover Cluster instance (FCI)

- A SQL Server AlwaysOn availability group with these preferences:
  - Prefer Secondary
  - Secondary only
  - Primary
  - Any Replica

Why back up SQL Server with DPM?

- DPM was designed to protect the advanced configurations of SQL Server.
- DPM can be set to protect SQL Server as frequently as every 15 minutes.
- DPM reduces potential conflicts between backup tools and SQL Server protection schedules.
- DPM can protect SQL Server at the instance level or database level. When protection at the instance level is turned on, DPM detects new databases on that instance, and automatically adds them to its protection group.

- DPM is an affordable option. It's a good fit for a small SQL Server footprint and can scale for organizations that have a larger SQL Server footprint.
- DPM has a Self-Service Recovery Tool (SSRT) that extends database administrators' options for self-service recovery of SQL databases.
- If you're upgrading to SQL Server 2014, DPM will continue to back up already protected databases after the SQL Server upgrade. You should avoid backup jobs during the SQL Server upgrade.

Set up monitoring notifications

1. In the DPM Administrator Console, select **Monitoring** > **Action** > **Options**.
2. Select **SMTP Server**, type the server name, port, and email address from which notifications will be sent. The address must be valid.
3. In **Authenticated SMTP server**, type a username and password. The username and password must be the domain account name of the person whose "From" address is described in the previous step; otherwise, notification delivery fails.
4. To test the SMTP server settings, select **Send Test E-mail**, type the email address where you want DPM to send the test message, and then select **OK**.
   Select **Options** > **Notifications** and select the types of alerts about which recipients want to be notified. In **Recipients**, type the email address for each recipient to whom you want DPM to send copies of the notifications.

Restore SQL Server data

You can recover SQL data as follows:

- Recover a database to the original location
- Recover the database with a new name to its original location or to a different instance of SQL Server
- Recover the database to a different instance of SQL Server
- Copy the database to a network folder
- Copy the database to tape

Recover a database from the DPM console as follows:

1. In the DPM Administrator Console, select **Recovery** on the navigation bar. Using the browse functionality, select the database you want to recover.
2. On the calendar, select any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point. On the **Recovery time** menu, select the recovery point you want to use.
3. In the **Actions** pane, select **Recover** to start the Recovery Wizard.
4. On the **Review recovery selection** page, select **Next**.
5. If you selected a recovery point other than **Latest** on the Specify Database State page, select **Leave database operational**.
6. Specify recovery options for network bandwidth usage throttling, SAN-based recovery, and email notifications, and then select **Next**.

7. On the **Summary** page, review the recovery settings, and then select **Recover**.

The user should open the DPM Self-Service Recovery Tool, select **Connect to DPM server** and specify the DPM server name.

1. After a connection is established, the user should select **New Recovery Job** to start the Recovery Wizard.
2. On the **Specify Database Details** page of the wizard, specify the SQL Server instance and database name to recover. If you're using availability groups, specify the group name in the format: **AGNAME.ClusternameFQDN\AGNAME**.
3. On the **Specify Recovery Point** page, select the data and time of the recovery point.
4. On the **Select Recovery Type** page, select whether to recover to any instance on the same SQL Server or a different one. Specify whether to recover to a network folder
5. If you're recovering to a database, on the **Specify Database State** page, specify whether the database should remain operational after recovery and specify whether you want to copy the SQL transaction logs.
6. On the **Specify Recovery Options** page, specify whether you want to retain security settings from the source server or apply settings from the destination server. You can also specify that an email notification should be sent when the recovery finishes.

Recover a database from the DPM console as follows:

1. In the DPM Administrator Console, select **Recovery** on the navigation bar. Using the browse functionality, select the database you want to recover.
2. On the calendar, select any date in bold to obtain the recovery points available for that date. The **Recovery time** menu lists the time for each available recovery point. On the **Recovery time** menu, select the recovery point you want to use.
3. In the **Actions** pane, select **Recover** to start the Recovery Wizard.
4. On the **Review recovery selection** page, select **Next**.

Users with self-service recovery permissions should recover as follows:

1. The user should open the DPM Self-Service Recovery Tool, select **Connect to DPM server** and specify the DPM server name.
2. After a connection is established, the user should select **New Recovery Job** to start the Recovery Wizard.
3. On the **Specify Database Details** page of the wizard, specify the SQL Server instance and database name to recover. If you're using availability groups, specify the group name in the format: **AGNAME.ClusternameFQDN\AGNAME**.
4. On the **Specify Recovery Point** page, select the data and time of the recovery point.
5. On the **Select Recovery Type** page, select whether to recover to any instance on the same SQL Server or a different one. Specify whether to recover to a network folder.
6. If you're recovering to a database, on the **Specify Database State** page, specify whether the database should remain operational after recovery and specify whether you want to copy the SQL transaction logs.

7. On the **Specify Recovery Options** page, specify whether you want to retain security settings from the source server or apply settings from the destination server. You can also specify that an email notification should be sent when the recovery finishes.

iii) Back up file data with DPM: -

You can use System Center Data Protection Manager (DPM) to back up file data on server and client computers.

1. **Deploy DPM** - Verify that DPM is installed and deployed correctly. We recommend that you review the following articles:

   Set up storage - You can store backed up data on disk, on tape, and in the cloud with Azure. Read more in Prepare data storage.
   Set up the DPM protection agent - You'll need to install the DPM protection agent on every machine you want to back up. Read Deploy the DPM protection agent.

Back up file data

After you have your DPM infrastructure set up you can enable protection machines that have file data you want to back up.

1. To create a protection group, click **Protection** > **Actions** > **Create Protection Group** to open the **Create New Protection Group** wizard in the DPM console.
2. In **Select Protection Group Type** select **Servers**.
3. In **Select Group Members** you'll add the machines for which you want to back up file data to the protection group. On those machines you select the locations, shares, and folders you want to protect. Deploy protection groups. You can select different types of folders (such as Desktop) or different file or the entire volume. You can also exclude specific locations from protection.
4. If you are protecting the volume on which the deduplication is enabled, ensure that the Data Deduplication server role is installed on the DPM server.

1. In **Select data protection method** specify how you want to handle short and long-term backup. Short-term back up is always to disk first, with the option of backing up from the disk to the Azure cloud with Azure backup (for short or long-term). As an alternative to long-term backup to the cloud you can also configure long-term back up to a standalone tape device or tape library connected to the DPM server.
2. In **Select short-term goals** specify how you want to back up to short-term storage on disk.
   In **Retention range** you specify how long you want to keep the data on disk.
   In **Synchronization frequency** you specify how often you want to run an incremental backup to disk. If you don't want to set a back up interval you can check Just before a recovery point so that DPM will run an express full backup just before each recovery point is scheduled.
3. If you want to store data on tape for long-term storage in **Specify long-term goals** indicate how long you want to keep tape data (1-99 years). In Frequency of backup specify how

often backups to tape should run. The frequency is based on the retention range you've specified:

- When the retention range is 1-99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly.
- When the retention range is 1-11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly.
- When the retention range is 1-4 weeks, you can select backups to occur daily or weekly.

On a stand-alone tape drive, for a single protection group, DPM uses the same tape for daily backups until there is insufficient space on the tape. You can also co-locate data from different protection groups on tape.

On the **Select Tape and Library Details** page specify the tape/library to use, and whether data should be compressed and encrypted on tape.

In the **Review disk allocation** page review the storage pool disk space allocated for the protection group.
In **Choose replica creation method** select how you want to handle the initial full data replication. If you select to replicate over the network we recommended you choose an off-peak time. For large amounts of data or less than optimal network conditions, consider replicating the data offline using removable media.
In **Choose consistency check options**, select how you want to automate consistency checks. You can enable a check to run only when replica data becomes inconsistent, or according to a schedule. If you don't want to configure automatic consistency checking, you can run a manual check at any time by right-clicking the protection group in the **Protection** area of the DPM console, and selecting **Perform Consistency Check**.
If you've selected to back up to the cloud with Azure Backup, on the **Specify online protection data** page make sure the workloads you want to back up to Azure are selected.
In **Specify online backup schedule** specify how often incremental backups to Azure should occur. You can schedule backups to run every day/week/month/year and the time/date at which they should run. Backups can occur up to twice a day. Each time a back up runs a data recovery point is created in Azure from the copy of the backed up data stored on the DPM disk.
In **Specify online retention policy** you can specify how the recovery points created from the daily/weekly/monthly/yearly backups are retained in Azure.
In **Choose online replication** specify how the initial full replication of data will occur. You can replicate over the network, or do an offline backup (offline seeding). Offline backup uses the Azure Import feature.
On the **Summary** page review your settings. After you click **Create Group** initial replication of the data occurs. When it finishes the protection group status will show as **OK** on the **Status** page. Backup then takes place in line with the protection group settings.

Recover data

Recover data from the DPM console as follows:

1. In DPM console click **Recovery** on the navigation bar. and browse for the data you want to recover. In the results pane, select the data.
2. Available recovery points are indicated in bold on the calendar in the recovery points section. Select the bold date for the recovery point you want to recover.
3. In the **Recoverable item** pane, click to select the recoverable item you want to recover.
4. In the **Actions** pane, click **Recover** to open the Recovery Wizard.
5. You can recover data as follows:

    a. **Recover to the original location**. Note that this doesn't work if the client computer is connected over VPN. In this case use an alternate location and then copy data from that location.
    b. **Recover to an alternate location**.
    c. **Copy to tape**. This option copies the volume that contains the selected data to a tape in a DPM library. You can also choose to compress or encrypt the data on tape.

    Specify your recovery options:

a. **Existing version recovery behavior**. Select **Create copy**, **Skip**, or **Overwrite**. This option is enabled only when you're recovering to the original location.
b. **Restore security**. Select **Apply settings of the destination computer** or **Apply the security settings of the recovery point version**.
c. **Network bandwidth usage throttling**. Click **Modify** to enable network bandwidth usage throttling.
d. **Enable SAN based recovery using hardware snapshots**. Select this option to use SAN-based hardware snapshots for quicker recovery.

This option is valid only when you have a SAN where hardware snapshot functionality is enabled, the SAN has the capability to create a clone and to split a clone to make it writable, and the protected computer and the DPM server are connected to the same SAN.

e. **Notification**. Click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.

Click **Next** after you have made your selections for the preceding options.

Review your recovery settings, and click **Recover**. Note that any synchronization job for the selected recovery item will be canceled while the recovery is in progress.

iv) Backup system state and bare metal: -

1. Click **Protection** > **Actions** > **Create Protection Group** to open the **Create New Protection Group** wizard in the DPM console.
2. In **Select protection group** type click **Servers**.
3. In **Select Group Members** expand the machine and select **BMR** or **system state**

   Remember that you can't protect BMR and system state for the same machine in different groups, and that when you select BMR system state is automatically enabled. Learn more in Deploy protection groups.
4. In **Select data protection method** specify how you want to handle short and long-term backup. Short-term backup is always to disk first, with the option of backing up from the disk to the Azure cloud with Azure backup (for short or long-term). As an alternative to long-term backup to the cloud you can also configure long-term back up to a standalone tape device or tape library connected to the DPM server.
5. In **Select short-term goals** specify how you want to back up to short-term storage on disk. In Retention range you specify how long you want to keep the data on disk. In Synchronization frequency you specify how often you want to run an incremental backup to disk. If you don't want to set a back-up interval, you can check, just before a recovery point so that DPM will run an express full backup just before each recovery point is scheduled.
6. If you want to store data on tape for long-term storage in **Specify long-term goals** indicate how long you want to keep tape data (1-99 years). In Frequency of backup specify how often backups to tape should run. The frequency is based on the retention range you've specified:
   - When the retention range is 1-99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly.
   - When the retention range is 1-11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly.
   - When the retention range is 1-4 weeks, you can select backups to occur daily or weekly.

v) Backup and restore VMware servers: -

1. In the DPM Administrator Console, click **Management**.
2. In the list of assets to manage, click **Production Servers**.
3. In the tool ribbon, click **Manage VMware Credentials**. The **Manage Credentials** dialog opens. Using the **Manage Credentials** dialog, you can add, Back up virtual machine to Tape

1. In the DPM Administrator console, click **Protection** > **Create protection group** to open the Create New Protection Group wizard.
2. On the **Select Group Members** page, select the VMware VMs you want to protect.

3. On the **Select Data Protection Method** page, select **I want long-term protection using tape**.
4. In **Specify Long-Term Goals** > **Retention range**, specify how long you want to keep your tape data (1-99 years). In Frequency of backup, select the backup frequency that you want.
5. On the **Select Tape and Library Details** page, specify the tape and library that'll be used for back up of this protection group. You can also specify whether to compress or encrypt the backup data.

Restore a recovery point: -

1. In the DPM Administrator Console, click **Recovery** view.
2. Using the Browse pane, browse or filter to find the VM you want to recover. Once you select a VM or folder, the Recovery points for pane displays the available recovery points.
3. In the **Recovery points for** field, use the calendar and drop-down menus to select a date when a recovery point was taken. Calendar dates in bold have available recovery points.
4. On the tool ribbon, click **Recover** to open the **Recovery Wizard**.
5. Click **Next** to advance to the **Specify Recovery Options** screen.
6. On the **Specify Recovery Options** screen, if you want to enable network bandwidth throttling, click **Modify**. To leave network throttling disabled, click **Next**. No other options on this wizard screen are available for VMware VMs. If you choose to modify the network bandwidth throttle, in the Throttle dialog, select **Enable network bandwidth usage throttling** to turn it on. Once enabled, configure the **Settings** and **Work Schedule**.
7. On the **Select Recovery Type** screen, choose whether to recover to the original instance, or to a new location, and click **Next**.
    - If you choose **Recover to original instance**, you don't need to make any more choices in the wizard. The data for the original instance is used.
    - If you choose **Recover as virtual machine on any host**, then on the **Specify Destination** screen, provide the information for **ESXi Host**, **Resource Pool**, **Folder**, and **Path**.
8. On the **Summary** screen, review your settings and click **Recover** to start the recovery process. The **Recovery status** screen shows the progression of the recovery operation.

vi) Backup and restore VMM servers: -

1. Click **Protection** > **Actions** > **Create Protection Group** to open the **Create New Protection Group** wizard in the DPM console.
2. In **Select protection group** type click **Clients**. You only select clients if you want to back up data on a Windows computer running a Windows client operating system. For all other workloads select server.
3. In **Select Group Members** expand the VMM machine and select **VMM Express Writer**.
4. In **Select data protection method** specify how you want to handle short and long-term backup. Short-term back-up is always to disk first, with the option of backing up from the disk to the Azure cloud with Azure backup (for short or long-term). As an alternative to long-term backup to the cloud you can also configure long-term back up to a standalone tape device or tape library connected to the DPM server.

5. In **Select short-term goals** specify how you want to back up to short-term storage on disk. In Retention range you specify how long you want to keep the data on disk.
   In **Synchronization frequency** you specify how often you want to run an incremental backup to disk. If you don't want to set a back-up interval you can check just before a recovery point so that DPM will run an express full backup just before each recovery point is scheduled.
6. If you want to store data on tape for long-term storage in **Specify long-term goals** indicate how long you want to keep tape data (1-99 years). In Frequency of backup specify how often backups to tape should run. The frequency is based on the retention range you've specified:
   - When the retention range is 1-99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly.
   - When the retention range is 1-11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly.
   - When the retention range is 1-4 weeks, you can select backups to occur daily or weekly.

   On a stand-alone tape drive, for a single protection group, DPM uses the same tape for daily backups until there is insufficient space on the tape. You can also co-locate data from different protection groups on tape.

   On the **Select Tape and Library Details** page specify the tape/library to use, and whether data should be compressed and encrypted on tape.

   In **Review disk allocation** page review the storage pool disk space allocated for the protection group. **Data size** shows the size of the data you want to back up, and **Disk space** shows the space that DPM recommends for the protection group.
   Select **Automatically grow the volumes** to automatically increase size when more disk space is required for backing up data.

   In **Choose replica creation method** select how you want to handle the initial full data replication. If you select to replicate over the network we recommended you choose an off-peak time. For large amounts of data or less than optimal network conditions, consider replicating the data offline using removable media.

   In **Choose consistency check options**, select how you want to automate consistency checks. You can enable a check to run only when replica data becomes inconsistent, or according to a schedule. If you don't want to configure automatic consistency checking, you can run a manual check at any time by right-clicking the protection group in the **Protection** area of the DPM console, and selecting **Perform Consistency Check**.

   If you've selected to back up to the cloud with Azure Backup, on the **Specify online protection data** page make sure the workloads you want to back up to Azure are selected.

   In **Specify online backup schedule** specify how often incremental backups to Azure should occur. You can schedule backups to run every day/week/month/year and the time/date at which they should run. Backups can occur up to twice a day. Each time a back-up runs a data recovery point is created in Azure from the copy of the backed-up data stored on the DPM disk.

In **Specify online retention policy** you can specify how the recovery points created from the daily/weekly/monthly/yearly backups are retained in Azure.

In Choose online replication specify how the initial full replication of data will occur. You can replicate over the network, or do an offline backup (offline seeding). Offline backup uses the Azure Import feature.

On the Summary page review your settings. After you click Create Group initial replication of the data occurs. When it finishes the protection group status will show as OK on the Status page. Backup then takes place in line with the protection group settings.