University of Mumbai

PRACTICAL JOURNAL – ELECTIVE II

PSIT3P3c

Cloud Management

SUBMITTED
BY

SACHIN DADHIBAL JAISWAR

SEAT NO 30440

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR QUALIFYING M.Sc. (I.T.) PART-II (SEMESTER – III)
EXAMINATION

2023-2024

DEPARTMENT OF INFORMATION TECHNOLOGY 3RD
FLOOR, DR. SHANKAR DAYAL SHARMA BHAVAN, VIDYANAGRI,
SANTACRUZ (E), MUMBAI – 400098.

University of Mumbai

Department of Information Technology

Certificate

This is to certify that **Mr. Sachin Dadhibal jaiswar Seat No. 30440** studying in **Master of Science** in **Information Technology Part II Semester III** has satisfactorily completed the Practical of **PSIT3P3c Cloud Management** as prescribed by University of Mumbai, during the academic year **2023-24**.

_____
Signature
Subject-In-Charge

_____
Signature
Head of the Department

_____
Signature
External Examiner

College Seal: _____ **Date:** _____

INDEX

9	Install and Deploy DPM i. Install DPM ii. Deploy the DPM protection agent iii. Deploy protection groups iv. Configure firewall settings	45	
10	Protect Workloads i. Back up Hyper-V virtual machines ii. Back up SQL Server with DPM iii. Back up file data with DPM iv. Backup system state and bare metal v. Backup and restore VMware servers vi. Backup and restore VMM servers	49	

Practical No.1

A. Create and Manage Cloud using SCVMM 2019

Step 1: Click **VMs and Services** > **Create** > **Create Cloud**, to open the Create Cloud Wizard.

Step 2: In **General**, specify a **Name** and optional description for the cloud.

Step 3: Specify whether the cloud will support shielded VMs.

Step 4: In **Resources** > **Host groups**, select the groups you want to add to the cloud. Then click **Next**.

Step 5: In **Logical Networks**, select each logical network that you want to make available to the private cloud, and then click **Next**.

Step 6: In **Load Balancers**, select each load balancer that you want to make available to this private cloud, and then click **Next**.

Step 7: In **VIP Templates**, select each VIP template that you want to make available to the private cloud, and then click **Next**.

Step 8: In **Port Classifications**, select each port classification that you want to make available to the cloud, and then click **Next**.

Step 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**.

Step 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**.

Step 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**.

Step 12: In **Capacity**, set capacity limits for the private cloud, and then click **Next**.

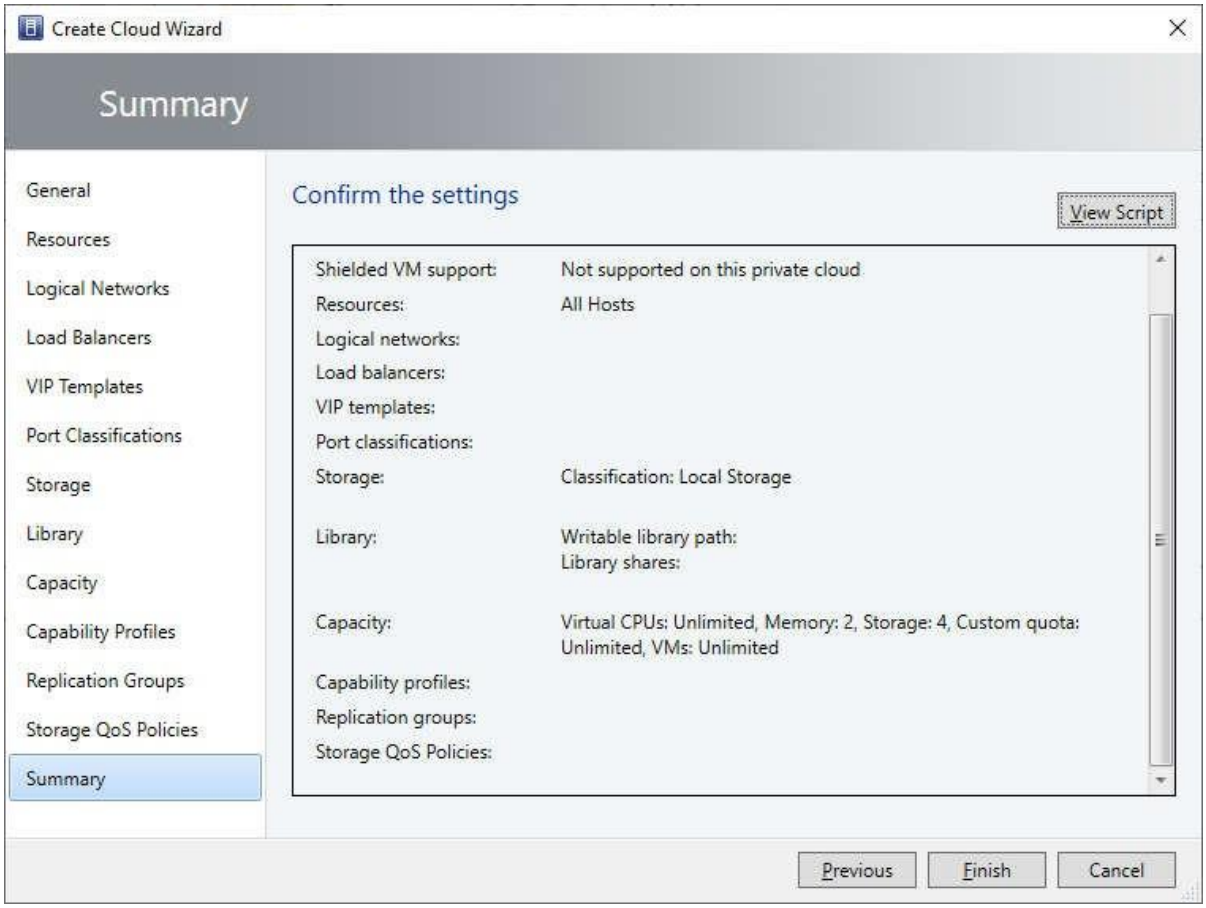
Step 13: In **Capability Profiles**, select each virtual machine capability profile that you want to add, and then click **Next**. Select the capability profiles that match the type of hypervisor platforms that are running in the selected host groups. The built-in capability profiles represent the minimum and maximum values that can be configured for a virtual machine for each supported hypervisor platform.

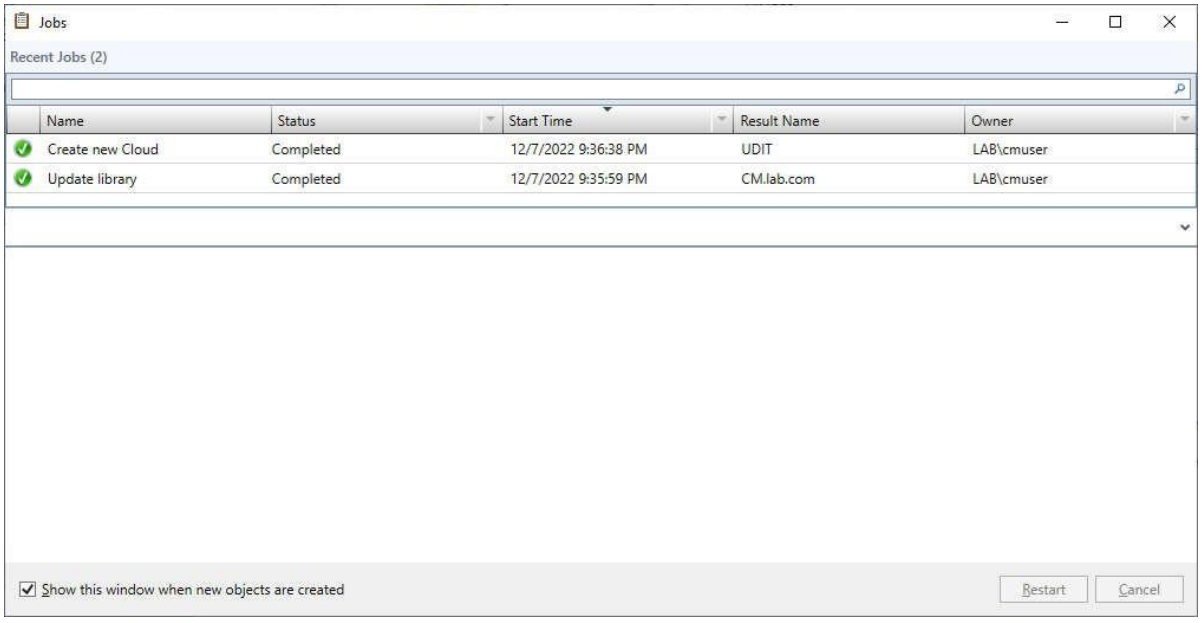
Step 14: In **Replication Groups**, select the replication groups for the private cloud, and click **Next**.

Step 15: In **Summary** page, confirm the settings, and then click **Finish**.

Step 16: View status in **Jobs** and ensure the job is complete.

OUTPUT:


Create Cloud Wizard
Summary
General
Resources
Logical Networks
Load Balancers
VIP Templates
Port Classifications
Storage
Library
Capacity
Capability Profiles
Replication Groups
Storage QoS Policies
Summary
Confirm the settings
View Script
Shielded VM support: Not supported on this private cloud
Resources: All Hosts
Logical networks:
Load balancers:
VIP templates:
Port classifications:
Storage: Classification: Local Storage
Library: Writable library path:
Library shares:
Capacity: Virtual CPUs: Unlimited, Memory: 2, Storage: 4, Custom quota: Unlimited, VMs: Unlimited
Capability profiles:
Replication groups:
Storage QoS Policies:
Previous
Finish
Cancel


Jobs
Recent Jobs (2)
Name
Status
Start Time
Result Name
Owner
Create new Cloud
Completed
12/7/2022 9:36:38 PM
UDIT
LAB\cmuser
Update library
Completed
12/7/2022 9:35:59 PM
CM.lab.com
LAB\cmuser
Show this window when new objects are created
Restart
Cancel

B. Deploy a guarded host fabric using Microsoft SCVMM 2019

Step 1 - Verify HGS prerequisites

Step 2 - Configure first HGS node

Step 3 - Configure additional HGS nodes

Step 4 - Configure fabric DNS

Step 5 - Verify host prerequisites (Key) and Verify host prerequisites (TPM)

Step 6 - Create host key (Key) and Collect host information (TPM)

Step 7 - Configure HGS with host information

Step 8 - Confirm hosts can attest

Step 9 - Configure VMM (optional)

Step 10 - Create template disks

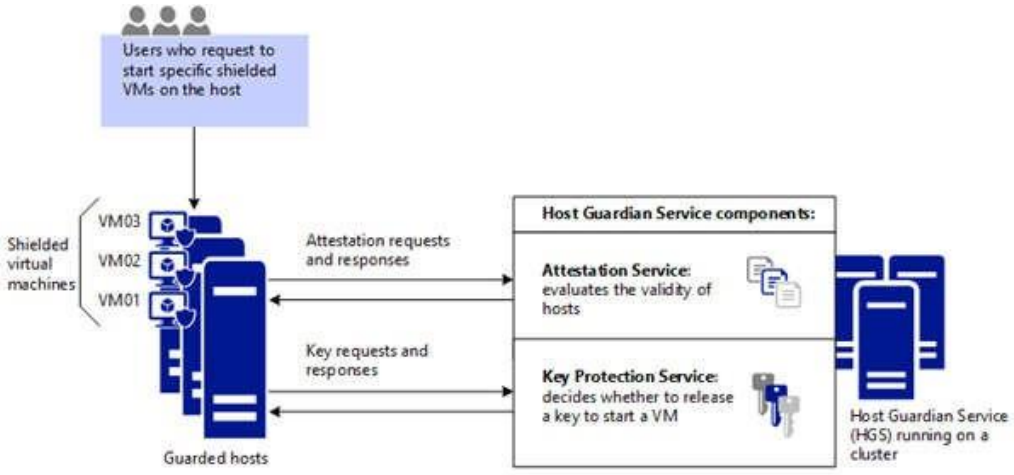
Step 11 - Create a VM shielding helper disk for VMM (optional)

Step 12 - Set up Windows Azure Pack (optional)

Step 13 - Create shielding data file

Step 14 - Create shielded VMs using Windows Azure Pack

Step 15 - Create shielded VMs using VMM



Practical No.2

A. Deploy and manage SDN Infra structure using SCVMM 2019

SDN virtualizes your network to abstract physical hardware network elements, such as switches and routers. Using SDN, you can dynamically manage your datacenter networking to meet workload and app requirements. Network policies can be implemented consistently, at scale, even as you deploy new workloads or move workloads across virtual or physical networks.

If you deploy SDN in the VMM fabric, you can:

- Provision and manage virtual networks at scale.
- Deploy and manage the SDN infrastructure, including network controllers, software load balancers, and gateways.
- Define and control virtual network policies centrally and link them to your applications or workloads. When your workload is deployed or moved, the network configuration adjusts itself automatically. This is important because it removes the need for manual reconfiguration of network hardware, thereby reducing operational complexity while saving your valuable resources for higher-impact work.
- Control traffic flow between virtual networks, including the ability to define guaranteed bandwidth for your critical applications and workloads.

SDN combines many technologies, among them:

- **Network Controller**: The network controller allows you to automate the configuration of your network infrastructure instead of manually configuring network devices and services.
- **RAS Gateway for SDN**: RAS Gateway is a software-based, multitenant BGP capable router that is designed for CSPs and enterprises that host multiple tenant virtual networks using HNV.
- **Software Load Balancing (SLB) for SDN**: SDN can use Software Load Balancing (SLB) to evenly distribute tenant and tenant customer network traffic among virtual network resources. The Windows Server SLB enables multiple servers to host the same workload, providing high availability and scalability.

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

Storage Spaces Direct (S2D) was introduced in Windows Server 2016. It groups physical storage drives into virtual storage pools to provide virtualized storage. With virtualized storage, you can:

- Manage multiple physical storage sources as a single virtual entity.
- Get inexpensive storage, with and without external storage devices.
- Gather different types of storage into a single virtual storage pool.
- Easily provision storage and expand virtualized storage on demand by adding new drives.

How does it work?

S2D creates pools of storage from storage that's attached to specific nodes in a Windows Server cluster. The storage can be internal on the node or disk devices that are directly attached to a single node. Supported storage drives include NVMe, SSD connected via SATA or SAS, and HDD.

When you enable S2D on a Windows Server cluster, S2D automatically discovers eligible storage and adds it to a storage pool for the cluster.

S2D also creates a built-in server-side storage cache to maximize performance. The fastest drives are used for caching and the remaining drives for capacity.

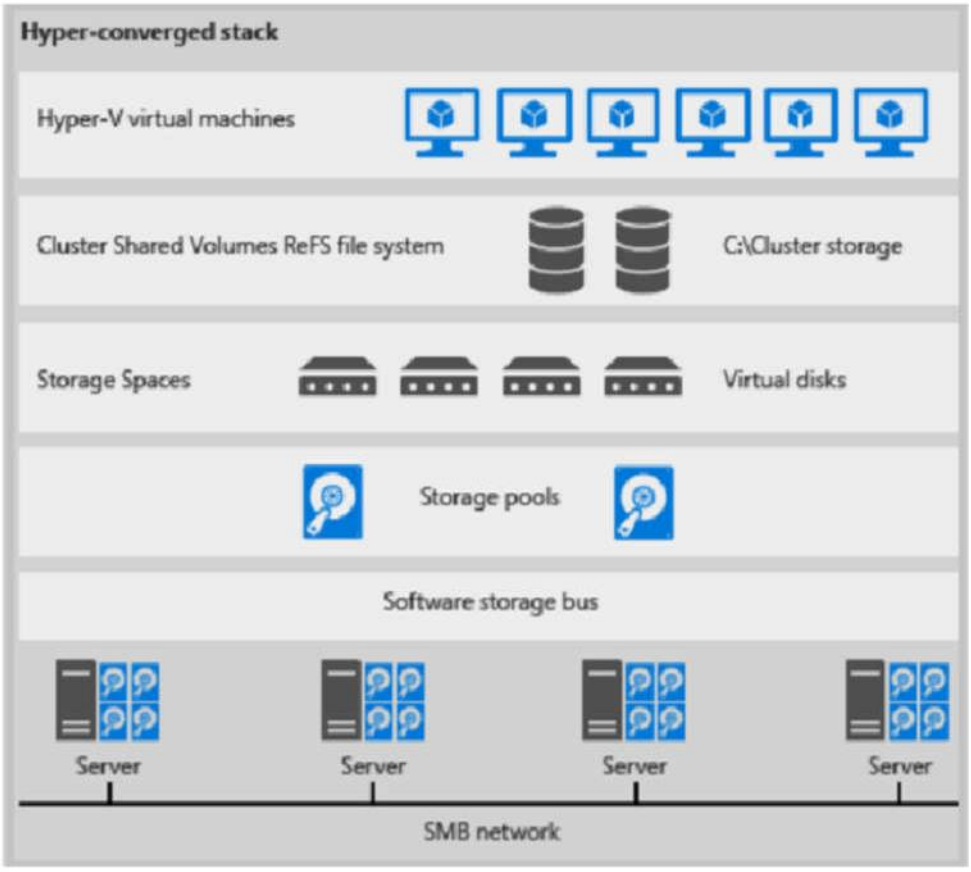
You create volumes from a storage pool. Creating a volume creates the virtual disk (storage space), partitions and formats it, adds it to the cluster, and converts it to a cluster shared volume (CSV).

You configure different levels of fault tolerance for a volume, to specify how virtual disks are spread across physical disks in the pool, using SMB 3.0. You can configure a volume with no resiliency or with mirror or parity resilience.

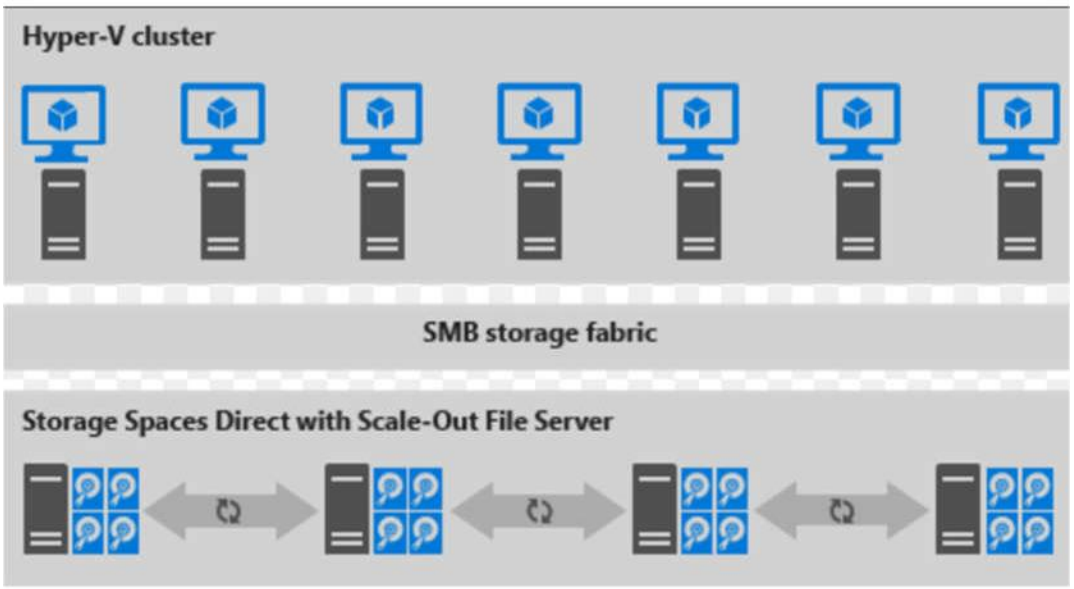
Converged and non-converged deployment

A cluster running S2D can be deployed in a couple of ways:

- **Hyper-converged deployment**: Hyper-V compute and S2D storage run within the same cluster, with no separation between them. This provides simultaneous scaling of compute and storage resources.



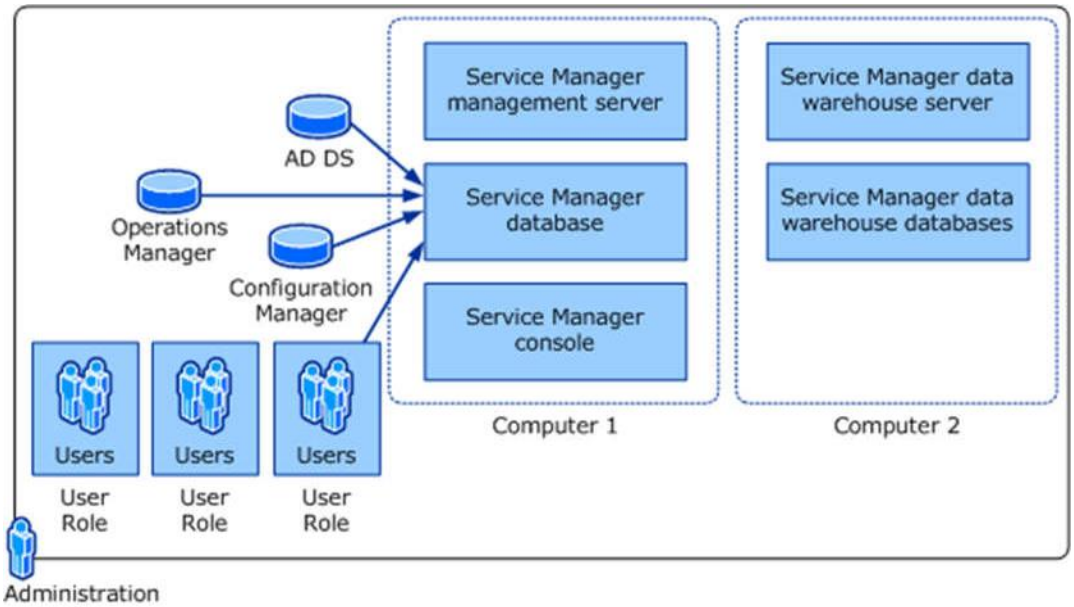
- **Disaggregated deployment**: Compute resources run on one Hyper-V cluster. S2D storage runs on a different cluster. You scale the clusters separately for finely tuned management.



Practical No.3

A. Deploy Service Manager 2019 and install on 4 Computer Scenario

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.



B. Setup SQL Server reporting Service using Service Manager 2019

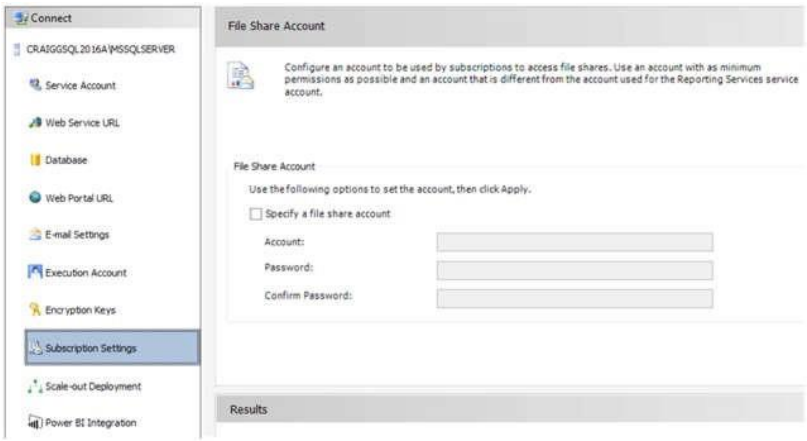
To start the Report Server Configuration Manager

- In the Windows start menu, type reporting and in the Apps search results, click Report Server Configuration Manager.

Or
Click Start, then click Programs, then click Microsoft SQL Server, then click Configuration Tools, and then click Report Server Configuration Manager.

- The Report Server Installation Instance Selection dialog box appears so that you can select the report server instance you want to configure.
- In Server Name, specify the name of the computer on which the report server instance is installed. The name of the local computer is specified by default, but you can also type the name of a remote SQL Server instance.
- If you specify a remote computer, click Find to establish a connection. The report server must be configured for remote administration in advance. For more information, see Configure a Report Server for Remote Administration.
- In Instance Name, choose the SQL Server Reporting Services instance that you want to configure. Only SQL Server 2008 and later report server instances appear in the list. You can't configure earlier versions of Reporting Services.
- Click Connect.

To verify that you launched the tool, compare your results to the following image:



Practical No.4

A. User Connectors to import data:

i. Import data from Active Directory Domain Services

Step 1: In the Service Manager console, click Administration.

Step 2: In the Administration pane, expand Administration, and then click Connectors.

Step 3: In the Tasks pane, under Connectors, click Create Connector, and then click Active Directory Connector.

Step 4: Complete these steps in the Active Directory Connector Wizard:

Step 5: On the Before You Begin page, click Next.

Step 6: 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.

Step 7: 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.

Step 8: In the Credentials area, click New.

Step 9: 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.

Step 10: 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.

On the Select objects, do the following:

Step 11: Select All computers, printers, users, and user groups to import all items or,

Step 12: Select Select individual computers, printers, users or user groups to import only the selected items or,

Step 13: 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.

Step 14: 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.

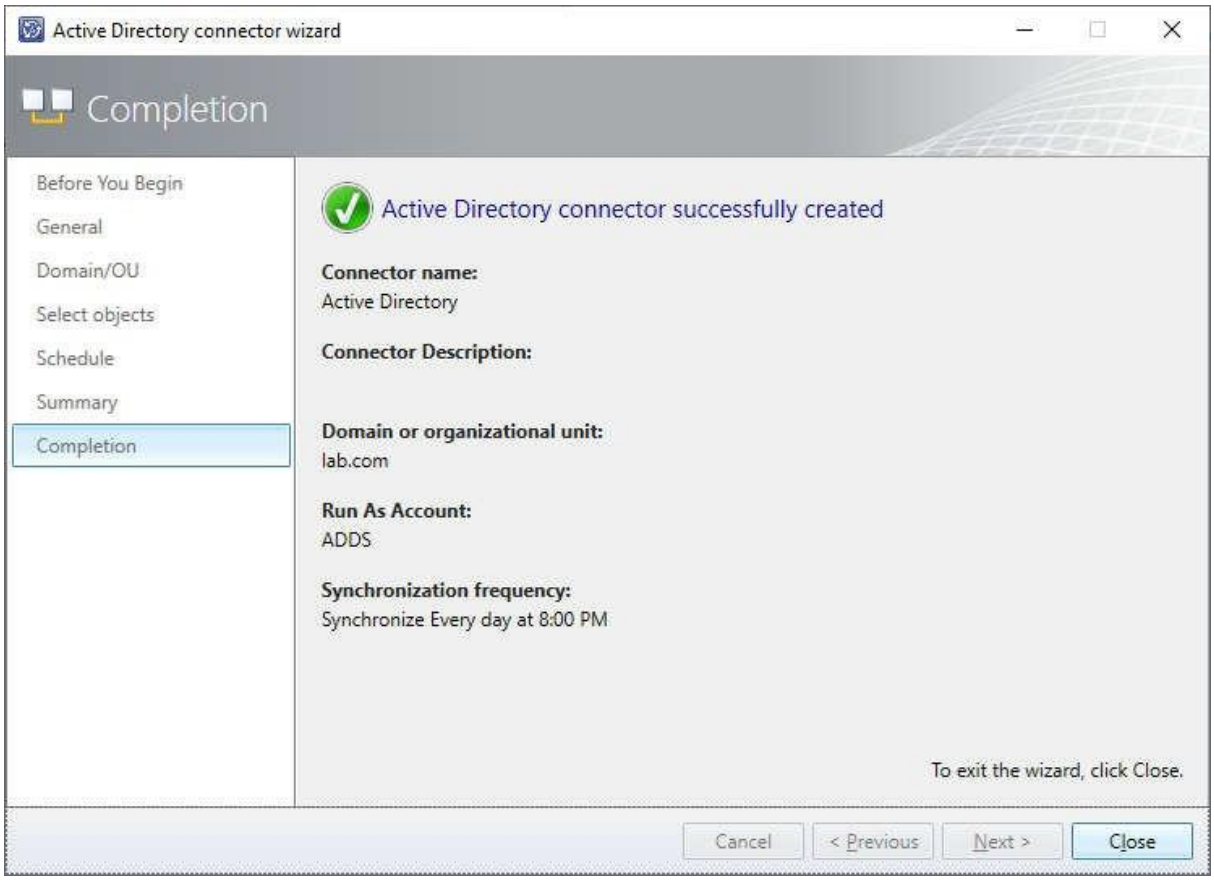
Step 15: On the Schedule page, in the Synchronize list, set the frequency and time of synchronization, and then click Next.

Step 16: On the Summary page, make sure that the settings are correct, and then click Create.

Step 17: 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 Operations Manager

To create an Operations Manager alert connector

- **Step 1:** In the Service Manager console, click **Administration**.
- **Step2:** In the **Administration** pane, expand **Administration**, and then click **Connectors**.
- **Step3:** In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Operations Manager Alert Connector**.

Complete the following steps to complete the Operations Manager Alert 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** 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.

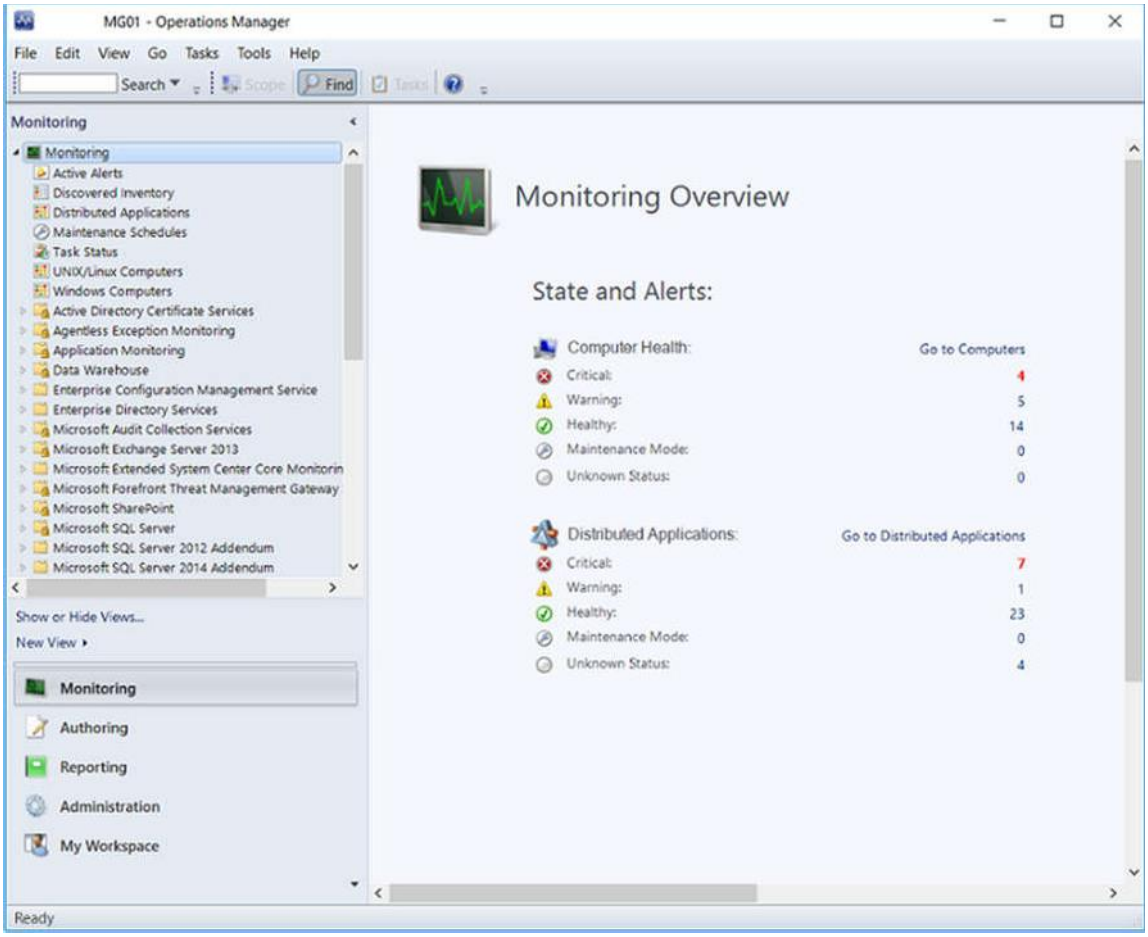
- On the **Server Details** page, in the **Server name** box, type the name of the server that is hosting the Operations Manager root management server. Under **Credentials**, click **New**.
- In the **Run As Account** dialog box, in the **Display name** box, type a name for this Run As account. In the **Account** list, select **Windows Account**.
- In the **User Name**, **Password**, and **Domain** fields, type the credentials for the Run As account, and then click **OK**.
- On the **Server Details** page, click **Test Connection**. If you receive the following confirmation message, click **OK**, and then click **Next**:
  The connection to the server was successful.
- On the **Alert Routing Rules** page, click **Add**.
- 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**.
- 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**.

To validate the creation of an Operations Manager alert connector

- Confirm that the connector you created is displayed in the Service Manager console in the **Connectors** pane.
- Confirm that incidents are created in Service Manager from alerts in Operations Manager.

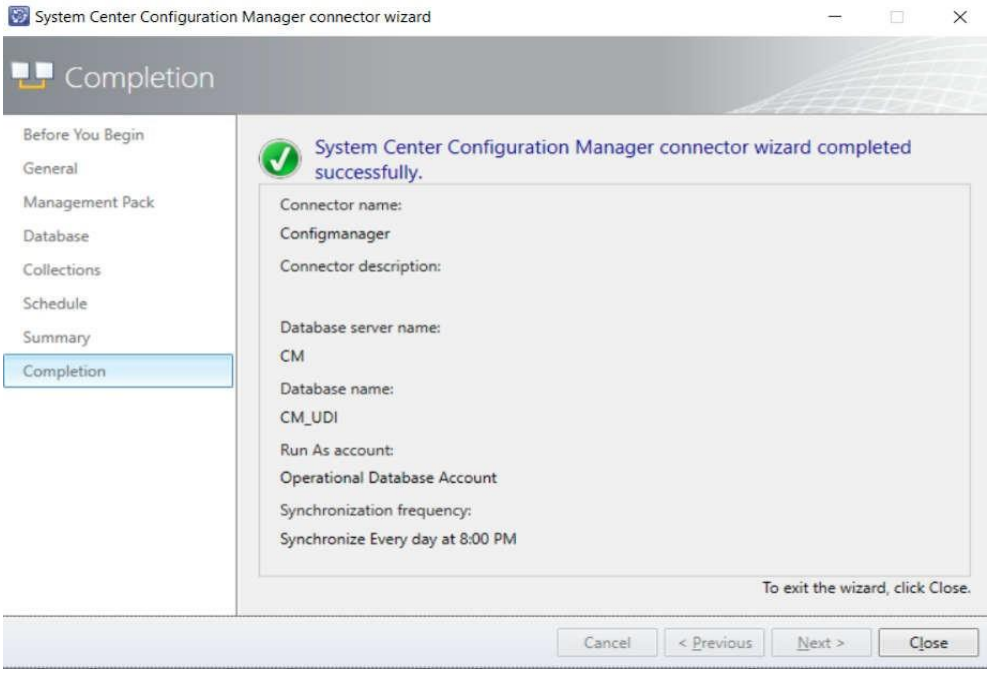


Import data from Configuration Manager

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 Configuration Manager Connector. The Configuration Manager Connector Wizard starts.
4. On the Before You Begin page, click Next.
5. On the General page, do the following:
6. In the Name box, type a name for the new connector. For example, type Configuration Manager Connector to Seattle.
7. In the Description box, type a description for the new connector. For example, type A Configuration Manager connector to site Seattle.
8. Make sure that the Enabled check box is selected, and then click Next.
9. On the Select Management Pack page, in the Management Pack list, select either System Center Configuration Manager Connector Configuration and then click Next.

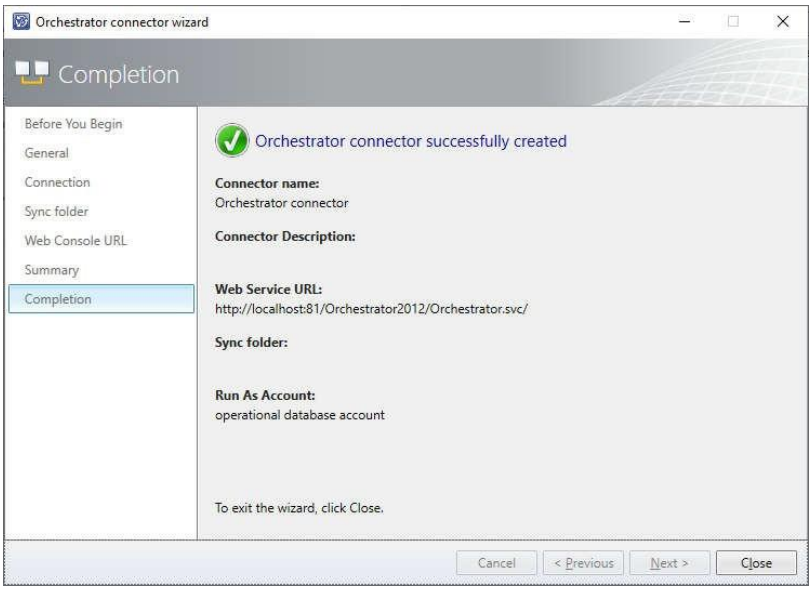
On the Connect to System Center Configuration Manager Database page, do the following:

1. In the Database Server Name box, type the server name of the server that is hosting the Configuration Manager site database and the database named instance, if applicable. For example, at the hypothetical Woodgrove Bank, you might type woodgrove\instance1 if the Configuration Manager database is on a named instance of Microsoft SQL Server, or type woodgrove if the database is on a default instance of SQL Server.
2. In the Database Name box, type the name of the Configuration Manager site database. For example, type SMS_CM1.
3. In the Credentials area, select a Run As account, or create a new Run As account. The user account that you specify as the Run As account must be a member of the smsdbrole_extract and the db_datareader groups for the Configuration Manager site database.
4. In the Credentials area, click Test Connection.
5. In the Credentials dialog box, in the Password box, type the password for the account, and then click OK.
6. In the Test Connection dialog box, if you receive the following confirmation message, click OK: The connection to the server was successful.
7. Click Next.
8. On the Collections page, select the appropriate collection, and then click Next.
9. On the Schedule page, in the Synchronize list, set the frequency and time of synchronization, and then click Next.
10. On the Summary page, confirm the connector settings you made, and then click Create.
11. On the Confirmation page, make sure that you receive the following confirmation message: *You have successfully completed the System Center Configuration Manager Connector Wizard.* Then, click Close.



iii. Import runbooks from Orchestrator

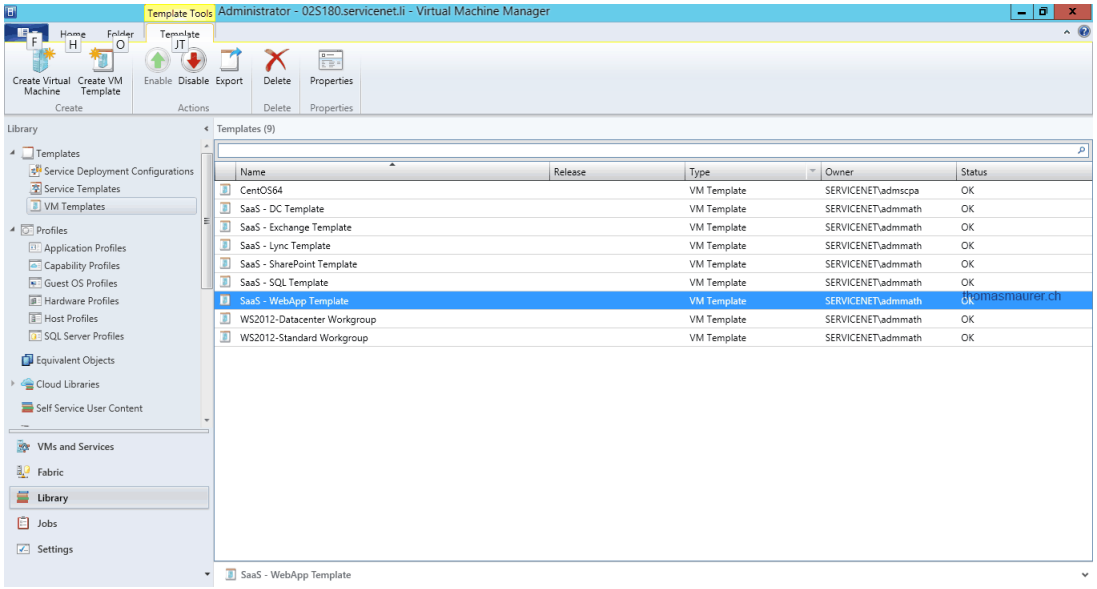
1. In the Service Manager console, click Administration.
2. In the Administration pane, expand Administration, and then click Connectors.
3. In the Tasks pane, under Connectors, click Create Connector, and then click Orchestrator connector.
4. Perform these steps to complete the Orchestrator Connector Wizard:
5. On the Before You Begin page, click Next.
6. 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.
7. On the Connection page, in the Server Information area, type the URL of the Orchestrator Web service.
8. 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.)
9. On the Connection page, in the Credentials area, either select an existing account or click New, and then do the following:
10. 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.
11. 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.
12. On the Folder page, select a folder, and then click Next.
13. 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.
14. On the Summary page, make sure that the settings are correct, and then click Create.
15. On the Completion page, make sure that you receive the message *Orchestrator connector successfully created,* and then click Close.



v. Import data from VMM

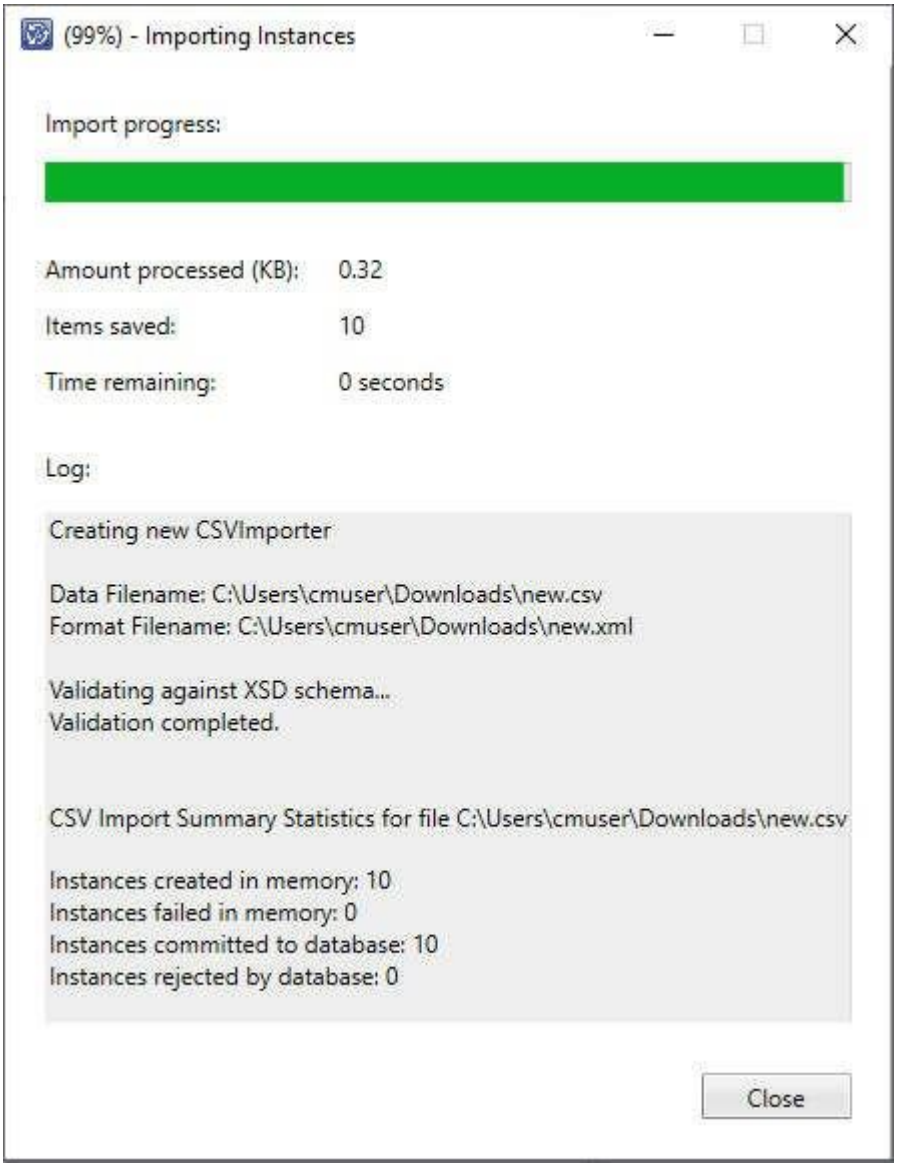
1. Create a Virtual Machine Manager connector
2. Use the following procedures to create a System Center Virtual Machine Manager connector and validate the creation of the connector.
3. To create a System Center Virtual Machine Manager connector
4. In the Service Manager console, click **Administration**.
5. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
6. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Virtual Machine Manager connector**.
7. Complete these steps to complete the Virtual Machine Manager Connector Wizard:
8. On the **Before You Begin** page, click **Next**.
9. 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**.
10. On the **Connection** page, in the **Server Information** area, type the same of the computer hosting Virtual Machine Manager (VMM).
11. On the **Connection** page, in the **Credentials** area, either select an existing account or click **New**, and then do the following:
12. 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**.
1. 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.
2. On the Summary page, make sure that the settings are correct, and then click Create.
3. On the Completion page, make sure that you receive a *Virtual Machine Manager connector successfully created* message, and then click Close.
4. To validate the creation of a System Center Virtual Machine Manager connector
5. In the Connectors pane, locate the System Center Virtual Machine Manager connector that you created.
6. Review the Status column for a status of Running.
7. In the Service Manager console, click **Configuration Items**.
8. In the **Tasks** pane, click **Create Folder**.
9. In the Create New Folder Wizard, do the following:
10. In the **Folder name** box, type a name for the folder. For example, type **Test**.
11. 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**.
12. In the **Configuration Items** pane, click the folder you just created. For example, click **Test**.
13. In the **Tasks** pane, click **Create View**.
14. In the Create View Wizard, do the following:
15. On the **General** page, in the **Name** area, type a name for this view. For example, type **VMMTemplates**.
16. 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**.
17. In the navigation pane of the wizard, click **Criteria**.

18. In the **Advanced Search** area, click **Browse**.
19. In the drop-down list (located to the right of the **Type to filter** box), select **All basic classes**.
20. 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.
21. 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**
22. In the **VMMTemplates** pane, you will see the Virtual Machine Manager templates that have been created.



vi. Use a CSV file to import data

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, click **Import from CSV file**.
4. In the **Import Instances from CSV File** dialog box, do the following:
5. Next to the **XML format file** box, click **Browse**, and then select the format file. For example, select **Newcomputers.xml**, and then click **Open**.
6. Next to the **Data file** box, click **Browse**, and then select the data file. For example, select **Newcomputers.csv**, and then click **Open**.
7. In the **Import Instances from CSV File** dialog box, click **Import**.
8. In the **Import Instances from CSV File** dialog box, verify that the numbers next to **Items saved**, **Instances created in memory**, and **Instances committed to database** are equal to the number of rows in the data file, and then click **Close**.


(99%) - Importing Instances
Import progress:
Amount processed (KB): 0.32
Items saved: 10
Time remaining: 0 seconds
Log:
Creating new CSVImporter
Data Filename: C:\Users\cmuser\Downloads\new.csv
Format Filename: C:\Users\cmuser\Downloads\new.xml
Validating against XSD schema...
Validation completed.
CSV Import Summary Statistics for file C:\Users\cmuser\Downloads\new.csv
Instances created in memory: 10
Instances failed in memory: 0
Instances committed to database: 10
Instances rejected by database: 0
Close

B. Automate IT processes with workflows

vii. Add or remove workflow activities

- **To add an activity to a workflow**

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.

In the Activities Toolbox pane, locate the appropriate activity group.

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 (such as For Each Loop) 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.

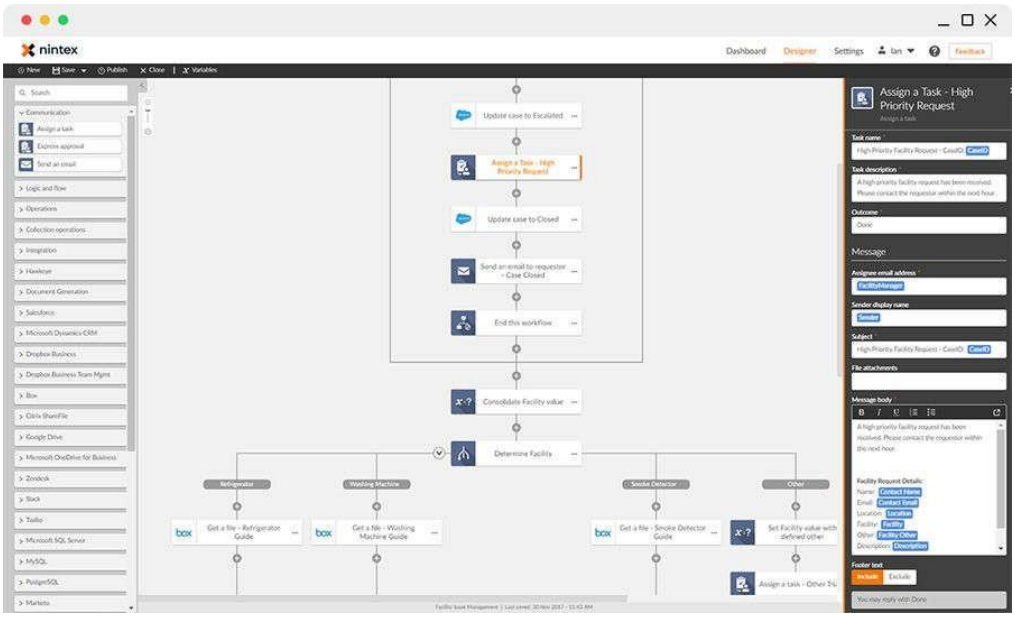
You can set the properties of an activity immediately after you add it to the authoring pane, or you can set the properties later.

- **Remove an activity from a workflow**

Use this procedure to remove an activity from a workflow in the Service Manager Authoring Tool. This operation does not remove the activity from the Activity Library or from the **Activities Toolbox** pane.

- **To remove an activity from a workflow**

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



ix. Deploy a workflow to Service Manager using the Authoring Tool

1. Move the management pack and workflow files
2. On the computer that is running the Authoring Tool, browse to the folder where you saved the management pack, and then copy the management pack and workflow files. The workflow file is automatically created in the same folder as the management pack. For example,
   copy **AddComputerToADGroupMP.xml** and **AddComputerToADGroupWF.dll**.
3. On the computer that is running the Service Manager console, browse to the Service Manager installation folder, for example, C:\Program Files\Microsoft System Center\Service Manager <version>.
4. Paste the copied management pack and workflow files into this folder. For example, paste **AddComputerToADGroupMP.xml** and **AddComputerToADGroupWF.dll**.
5. Import the management pack into Service Manager
6. In the Service Manager console, click **Administration**.
7. In the **Administration** pane, expand **Administration**, and then click **Management Packs**.
8. In the **Tasks** pane, under **Management Packs**, click **Import Management Pack**.
9. 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**.
10. In the **Import Management Packs** dialog box, click **Add** to add the management pack that you want to import.
11. Click **Import**, and then click **OK**.

Install a custom activity assembly

So that you can use custom or third-party Windows Workflow Foundation (WF) activities in workflows, the activity assembly files must first be installed. You must have administrative permissions on the computer running the Service Manager Authoring Tool and the computer running Service Manager. Like the default activities, custom activities must be available on the computer running Service Manager as well as on the computer running the Authoring Tool.

On the computer running the Authoring Tool, browse to the Authoring Tool Workflow Activity Library folder, for example, D:Program Files (x86)Microsoft System CenterService Manager <version> AuthoringWorkflow Activity Library. Paste the custom activity assembly into this folder.

On the computer running Service Manager, browse to the Service Manager installation folder, and then paste the custom activity assembly into this folder.

After you have installed the custom activity assembly, notify the Authoring Tool users that they can now add the custom activities to personalized activity groups, by using the following procedures:

Remove a custom activity assembly

To remove a custom activity assembly, you must have administrative permissions on the computer running the Service Manager Authoring Tool and on the computer running the Service Manager console. After the custom activity assembly has been removed, the activities compiled into that assembly are no longer available in personalized activity groups.

On the computer running the Authoring Tool, browse to the Authoring Tool Workflow Activity Library folder, for example, D:Program Files (x86)Microsoft System CenterService Manager <version> AuthoringWorkflow Activity Library. Remove the custom activity assembly from this folder.

On the computer running the Service Manager console, browse to the Service Manager installation folder. Remove the custom activity assembly from this folder.

After you have removed the custom activity assembly, notify the Authoring Tool users that the custom activities are no longer available.

Personalize the activities toolbox

- Create a top-level activity group

In the **Activities Toolbox** pane, right-click **Activity Groups**, and then click **New Group**.

- Enter a name for the new group.

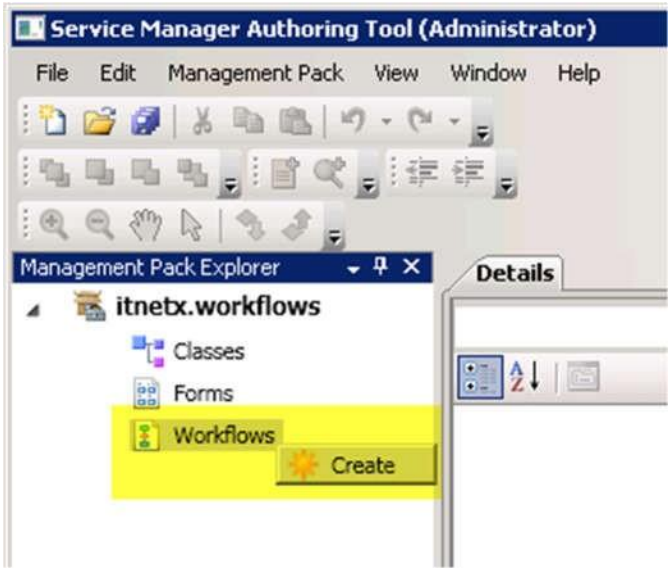
Create an activity subgroup

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

Enter a name for the new group.

Delete a personalized activity group

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



Practical No. 5

A. Managing devices with Configuration Manager

Configuration Manager can manage two broad categories of devices:

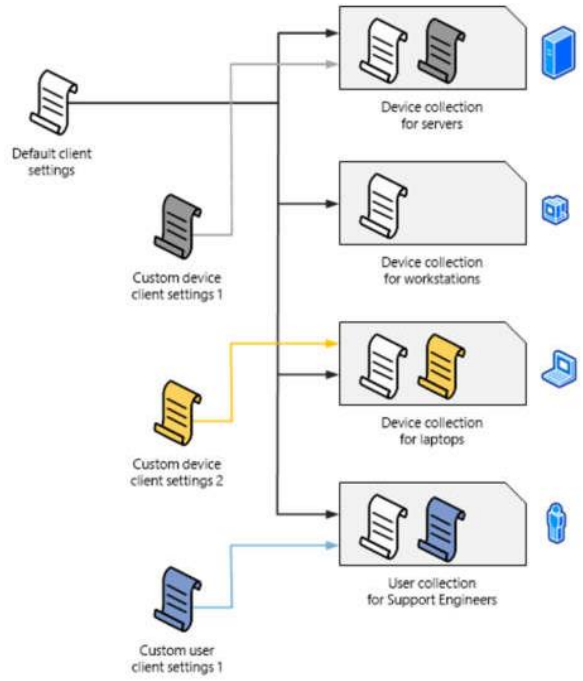
Clients are devices like workstations, laptops, servers, and mobile devices where you install the Configuration Manager client software. Some management functions, like hardware inventory, require this client software.

Managed devices can include *clients*, but typically it's a mobile device where the Configuration Manager client software isn't installed. On this kind of device, you manage by using the built-in on-premises mobile device management in Configuration Manager.

Managing devices with the Configuration Manager client

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. Common installation methods include:

- Client push installation
- Software update-based installation
- Group policy
- Manual installation on a computer
- Including the client as part of an OS image that you deploy



User-based management

Configuration Manager supports collections of Azure Active Directory and Active Directory Domain Services users. When you use a user collection, you can install software on all computers that members of the collection use. To make sure that the software you deploy only installs on the devices that are specified as a user's primary device, set up user device affinity. A user can have one or more primary devices.

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:

Install software:

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

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

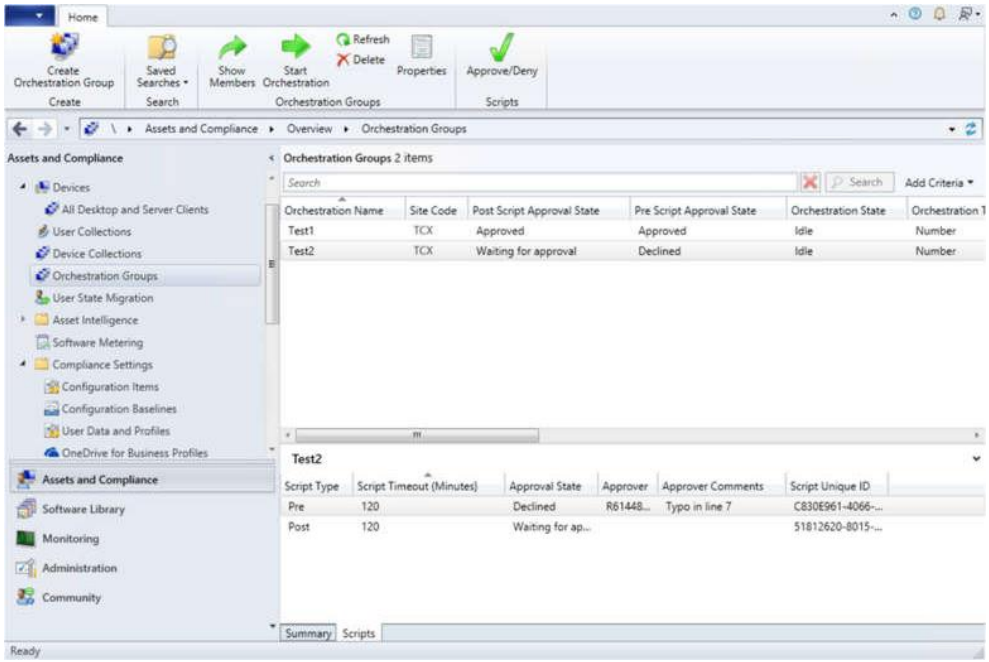
Before installing the first site of a new Configuration Manager hierarchy, it's a good idea to understand:

- The available topologies for Configuration Manager
- The types of available sites and their relationships with each other
- The scope of management that each type of site provides
- 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:

- Install a new primary site below a central administration site, up to the supported number of primary sites for the hierarchy.
- Expand a standalone primary site to install a new central administration site, to then install additional primary sites.
- Install new secondary sites below a primary site, up to the supported limit for the primary site and overall hierarchy.
- 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 No. 6

A. Data transfers between sites

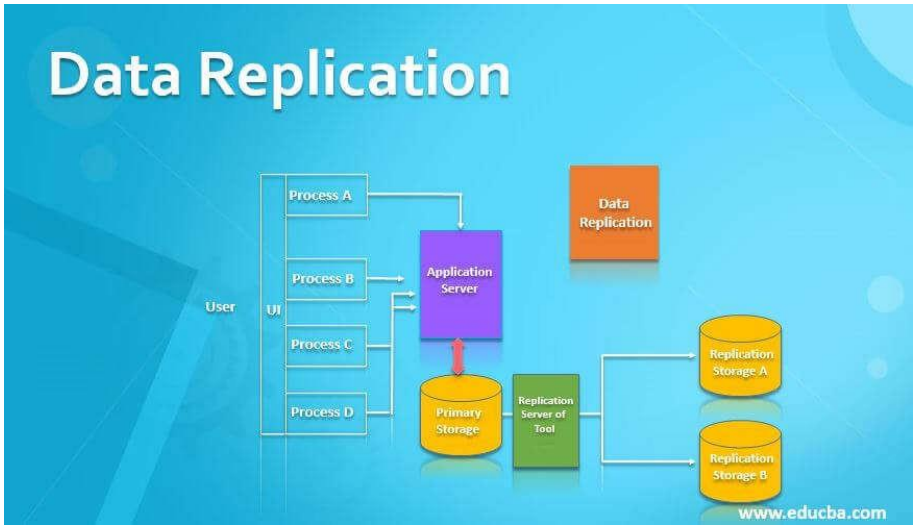
Configuration Manager uses *file-based replication* and *database replication* to transfer different types of information between sites. Learn about how Configuration Manager moves data between sites, and how you can manage the transfer of data across your network.

i. 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.

ii. 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.



B. Configure sites and hierarchies

i. **Add Site System Roles**: Add site system roles to an existing site system server in the site

ii. **Install roles on an existing site system server**

- 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.
- In the ribbon, on the **Home** tab, in the **Server** group, select **Add Site System Roles**.
- On the **General** page, review the settings.
- On the **Proxy** page, if roles on this server require an internet proxy, then specify settings for a proxy server.
- On the **System Role Selection** page, select the site system roles that you want to add.
- Complete the wizard. Additional pages may appear for specific roles.

iii. **Install cloud-based distribution points**

- Use the following checklist to make sure you have the necessary information and prerequisites to create a cloud distribution point:
- The site server can connect to Azure. If your network uses a proxy, configure the site system role.
- The **Azure environment** to use. For example, the Azure Public Cloud or the Azure US Government Cloud.
- Use the **Azure Resource Manager deployment**. It has the following requirements:
- Integration with Azure Active Directory for **Cloud Management**. Azure AD user discovery isn't required.
- The Azure **Subscription ID**.
- The Azure **Resource Group**.
- A **subscription admin account** needs to sign in during the wizard.
- A **server authentication certificate**, exported as a .PFX file.
- A globally unique **service name** for the cloud distribution point.
- The Azure **region** for this deployment.
- Configuration options for site system roles
- Most configuration options for Configuration Manager site system roles are self-explanatory or are explained in the wizard or dialog boxes when you configure them. The following sections explain site system roles whose settings might require additional information.
- Certificate registration point

1. Distribution point

Install and configure IIS if required by Configuration Manager

Select this option to let Configuration Manager install and set up IIS on the site system if it's not already installed. IIS must be installed on all distribution points, and you must select this setting to continue in the wizard.

2. **Enrolment point**

Enrolment points are used to install macOS computers and enroll devices that you manage with on-premises mobile device management

3. **Enrolment proxy point**
4. **Fallback status point**

Each computer that successfully installs the Configuration Manager client sends the following four state messages to the fallback status point:

- Client deployment started
- Client deployment succeeded
- Client assignment started
- Client assignment succeeded

iv.

v. Database replicas for management points

Configuration Manager primary sites can use a database replica to reduce the CPU load placed on the site database server by management points as they service requests from clients. When a management point uses a database replica, it requests data from the SQL Server computer that hosts the database replica instead of from the site database server.

Prerequisites

1. SQL Server requirements
2. The SQL Server that hosts the database replica has the same requirements as the site database server. The replica server doesn't need to run the same version or edition of SQL Server as the site database server, if it runs a supported version and edition of SQL Server. For more information, see Support for SQL Server versions.
3. The SQL Server service on the computer that hosts the replica database must run as the **System** account.
4. Both the SQL Server that hosts the site database and that hosts a database replica must have **SQL Server replication** installed.
5. The site database must *publish* the database replica, and each remote database replica server must *subscribe* to the published data.
6. Configure both SQL Servers to support a **max text repl size** of 2 GB. For more information and how to configure this setting for SQL Server, see Configure the max text repl size Server Configuration Option.

To configure a database replica, the following steps are required:

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

Step 2 - Configuring the database replica server

Step 3 - Configure management points to use the database replica

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

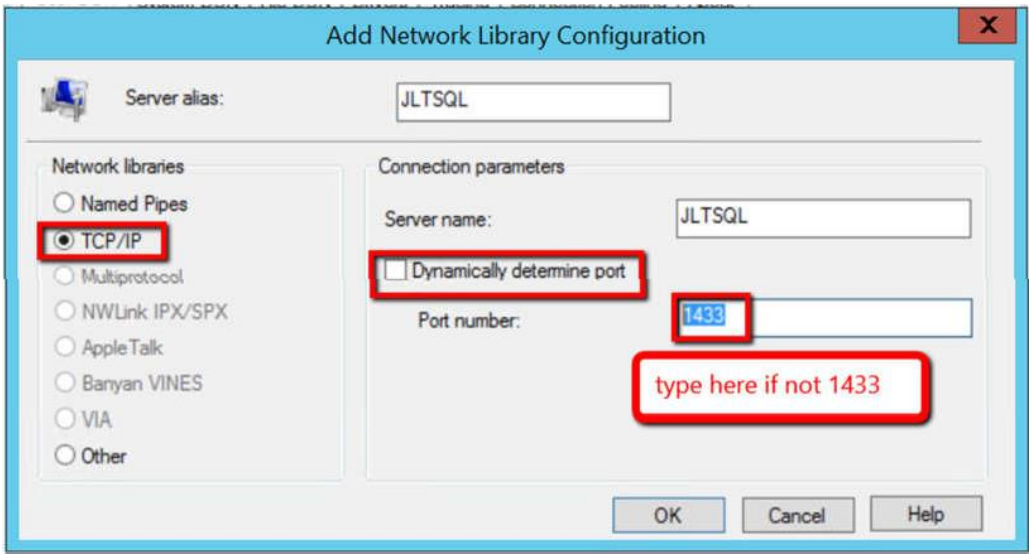
Step 5 - Configure the SQL Server Service Broker for the database replica server

Practical No. 7

A. Install Orchestrator

1. On the server where you want to install Orchestrator, 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 page of the wizard, click **Install**.
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, and then click **Next**.
6. On the **Diagnostic and Usage data** page, review the Diagnostic and Usage data notice, and then click **Next**.
7. On the **Select features to install** page, ensure that **Management Server** is the only feature selected, and then click **Next**.
8. 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.
9. Review the items that did not pass the prerequisite check. For some requirements, such as Microsoft .NET Framework 4, you can use the link provided in the Setup Wizard to install the missing requirement. The Setup Wizard can install or configure other prerequisites, such as the Internet Information Services (IIS) role.
10. After you resolve the missing prerequisites, click **Verify prerequisites again**.
11. Click **Next** to continue.
12. On the **Configure the service account** page, enter the username and password for the Orchestrator service account. Click **Test** to verify the account credentials. If the credentials are accepted, then click **Next**.
13. On the **Configure the database server** page, enter the name of the server and the name of the instance of Microsoft SQL Server that you want to use for Orchestrator. You can also specify whether to use Windows Authentication or SQL Server Authentication, and whether to create a new database or use an existing database. Click **Test Database Connection** to verify the account credentials. If the credentials are accepted, click **Next**.
14. On the **Configure the database** page, select a database, or create a new database, and then click **Next**.
15. On the **Configure Orchestrator users group** page, accept the default configuration or enter the name of the Active Directory user group to manage Orchestrator, and then click **Next**.
1. On the **Select the installation location** page, verify the installation location for Orchestrator and change it if you want to, and then click **Next**.
2. On the **Microsoft Update** page, optionally indicate whether you want to use the Microsoft Update services to check for updates, and then click **Next**.
3. On the **Help improve Microsoft System Center Orchestrator** page, optionally indicate whether you want to participate in **Error Reporting**, and then click **Next**.

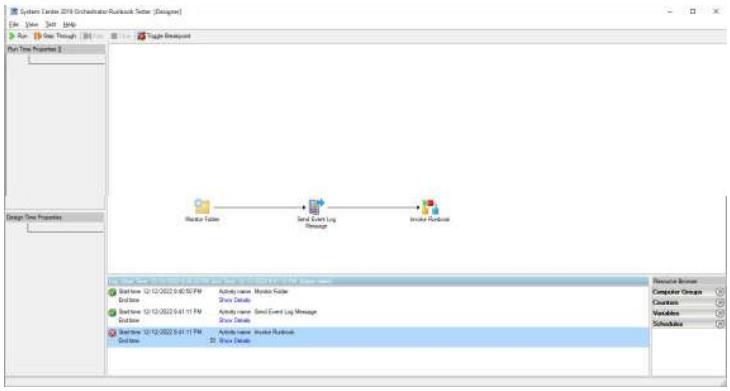
4. Review the **Installation summary** page, and then click **Install**.
5. The **Installing features** page appears and displays the installation progress.
6. On the **Setup completed successfully** page, optionally indicate whether you want to start Runbook Designer, and then click **Close** to complete the installation.



B. Create and test a monitor runbook

1. To create the workflow
2. In the Runbook Designer **Connections** pane, right-click the **Runbooks** folder to select **New**, and then click **Runbook**.
3. Right-click the **New Runbook** tab to select **Rename**.
4. In the **Confirm Check out** dialog box, click **Yes**.
5. Type a name for the runbook, such as **Monitor Runbook**, and then press Enter.
6. In the **Activities** pane, click **File Management** to expand the category, and then drag the **Monitor Folder** activity into the **Runbook Designer** Design workspace.
7. In the **Activities** pane, click **Notification** to expand the category, and then drag the **Send Event Log Message** activity into the **Runbook Designer** Design workspace, to the right of the **Monitor Folder** activity.
8. In the **Runbook Designer** Design workspace, move your pointer over the right side of the **Monitor Folder** activity to display the smart link arrow.
9. Click the smart link arrow, and then drag it to the **Send Event Log Message** activity.
10. In the **Activities** pane, click **Runbook Control** to expand the category, and then drag the **Invoke Runbook** activity into the **Runbook Designer** Design workspace, to the right of the **Send Event Log Message** activity.
11. In the **Runbook Designer** Design workspace, move your pointer over the right side of the **Send Event Log Message** activity to display the smart link arrow.
12. Click the smart link arrow, and then drag it to the **Invoke Runbook** activity.
13. To configure the workflow
14. In the **Runbook Designer** Design workspace, double-click the **Monitor Folder** activity.
15. In the **Monitor Folder Properties** dialog box, click the **General** tab.
16. In the **Name** box, change the name of the activity to something informative, for example **Monitor C:\Monitor Folder**.
17. Click the **Details** tab.
18. On the **Details** tab, in the **Path** box, type the path of the folder you want to monitor, for example **C:\Monitor**.
19. Below the **File Filters** list, click **Add**.
20. In the **Filter Settings** dialog box, set the following:
21. In the **Name** list box, select **File Name**.
22. In the **Relation** list box, select **Matches pattern**.
23. In the **Value** box, type ***.txt**.
24. This setting directs the monitor to look for files with the **txt** extension. This field accepts regular expression syntax.
25. Click **OK**.
26. Select the **Triggers** tab.
27. Select the **Number of files is** option, set the value in the list to **greater than**, and then type **0** in the edit box.
28. Click **Finish**.
29. In the **Runbook Designer** Design workspace, double-click the **Send Event Log Message**.
30. In the **Send Event Log Message Properties** dialog box, on the **Details** tab, in the **Properties** section, set the following:

31. In the **Computer** box, type the name of the computer to receive the Event message.
32. This is typically the computer where you are running Runbook Designer.
33. In the **Message** box, type the message to display in the Event log, for example, **File Detected**.
34. Leave the **Severity** level at **Information**.
35. Click **Finish**.
36. To prepare your computer
37. Right-click **Start** to select **Open Windows Explorer**.
38. Create a **C:\Monitor** folder on your computer.
39. Create a **C:\Source** folder on your computer.
40. In the **C:\Source** folder, create a file with a **txt** extension, for example **text.txt**.
41. To test the runbook
42. In the **Runbook Designer** Design workspace, select the **Monitor Runbook** tab.
43. On the toolbar above the **Runbook Designer** Design workspace, click **Runbook Tester**.
44. In the **Confirm Check out** dialog box, click **Yes**.
45. In **Runbook Tester**, on the toolbar, click **Step Over** to start stepping through the runbook.
46. In Windows Explorer, browse to the **C:\Source** folder.
47. Copy **test.txt** to **C:\Monitor**.
48. Close Windows Explorer.
49. On the Runbook Tester toolbar, click **Next**.
50. After a few moments, note that the **Log** pane entry updates and shows an event for the **Monitor Folder** activity.
51. On the **Log** pane Click the **Show Details** link to see the contents of the data bus for that runbook.
52. Scroll down the list of properties. Note that the activity status is **success** indicating that the **Monitor Folder** activity detected the change in the folder.
53. On the Runbook Tester toolbar, click **Next**.
54. Notice that the **Log** pane changes and shows an event for the **Send Event Log Message** activity.
55. Click the **Show Details** link and note that the activity status is **success** indicating that the **Send Event Log Message** activity detected the change in the folder.
56. Close **Runbook Tester**.
57. On the **Runbook Designer** toolbar, click **Check In**.

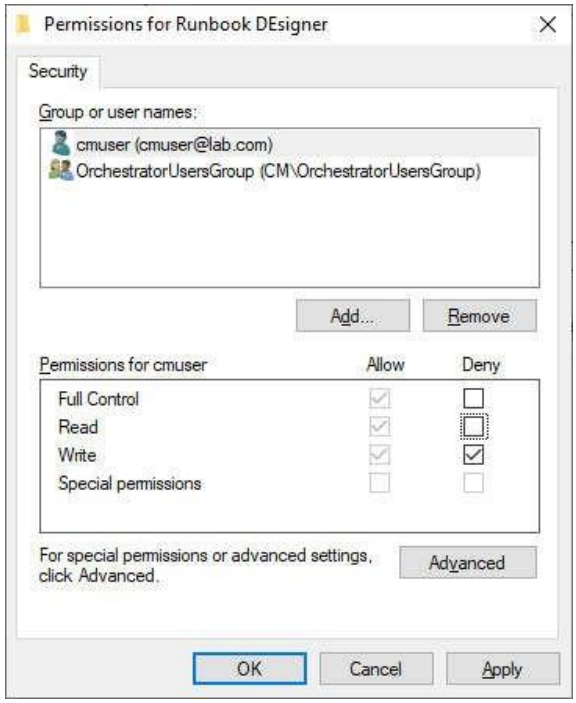


Practical No. 8

A. Manage Orchestrator Servers - 1

i. Runbook permissions

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**.
5. If the user or security group should be able to change the runbook, select the **Allow** check box next to **Write**.
6. If the user or security group should be able to change permissions for the runbook, select the **Allow** check box next to **Full Control**.
7. To close the **Permissions for Runbook** dialog box and save any changes, click **OK**.

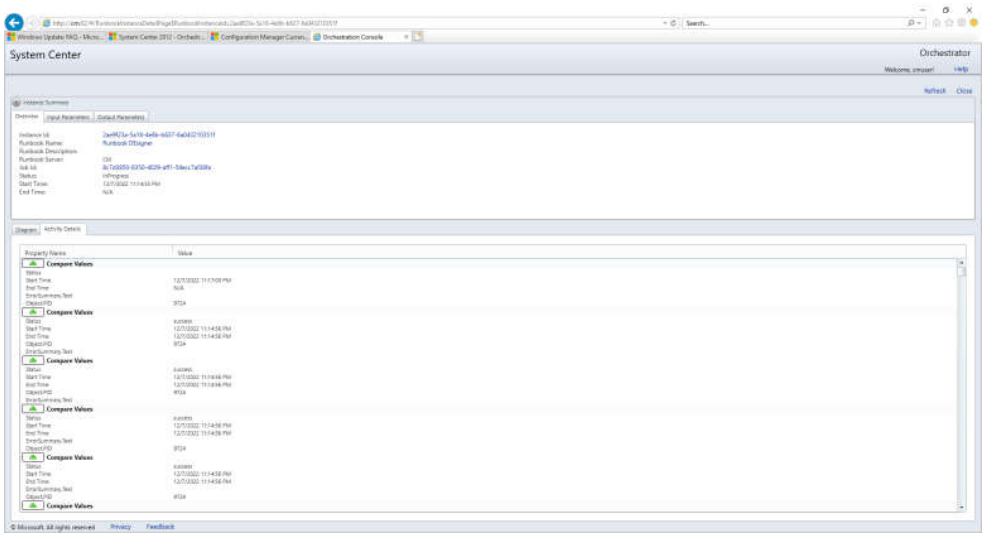


ii. Back up Orchestrator

1. A complete backup of an Orchestrator environment consists of the following:
2. Backup of the Orchestrator database.
3. File backup of the Orchestrator management server.
4. File backup of each Runbook server and Orchestrator web server.
5. Orchestrator supports Volume Shadow copy Service (VSS) for backup and restore with System Center - Data Protection Manager (DPM). VSS is a framework that allows volume backups to be performed while an application continues to run.

iii. Bench mark

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. Optimize performance of .Net activities

When a runbook containing an activity that references the .NET assemblies executes, the job process has to load the referenced assembly when such an activity is executed. Any subsequent execution of the same activity or other activities from the assembly will reuse the loaded assembly.

Loading an assembly may cause a delay of up to 30 seconds. This delay can also occur when a runbook is started on a computer without Internet access, because Windows can't verify the Microsoft Authenticode signature for the .NET assemblies.

To remove the delay you can either
deactivate generatePublisherEvidence in PolicyModule.exe, or you can create a profile for the service account.

Deactivate generatePublisherEvidence in policymodule.exe.config

Locate the file C:\Program Files\Microsoft System Center\Orchestrator\Runbook Server\policymodule.exe.config on the runbook server that executes runbooks containing an activity referencing a .NET assembly.

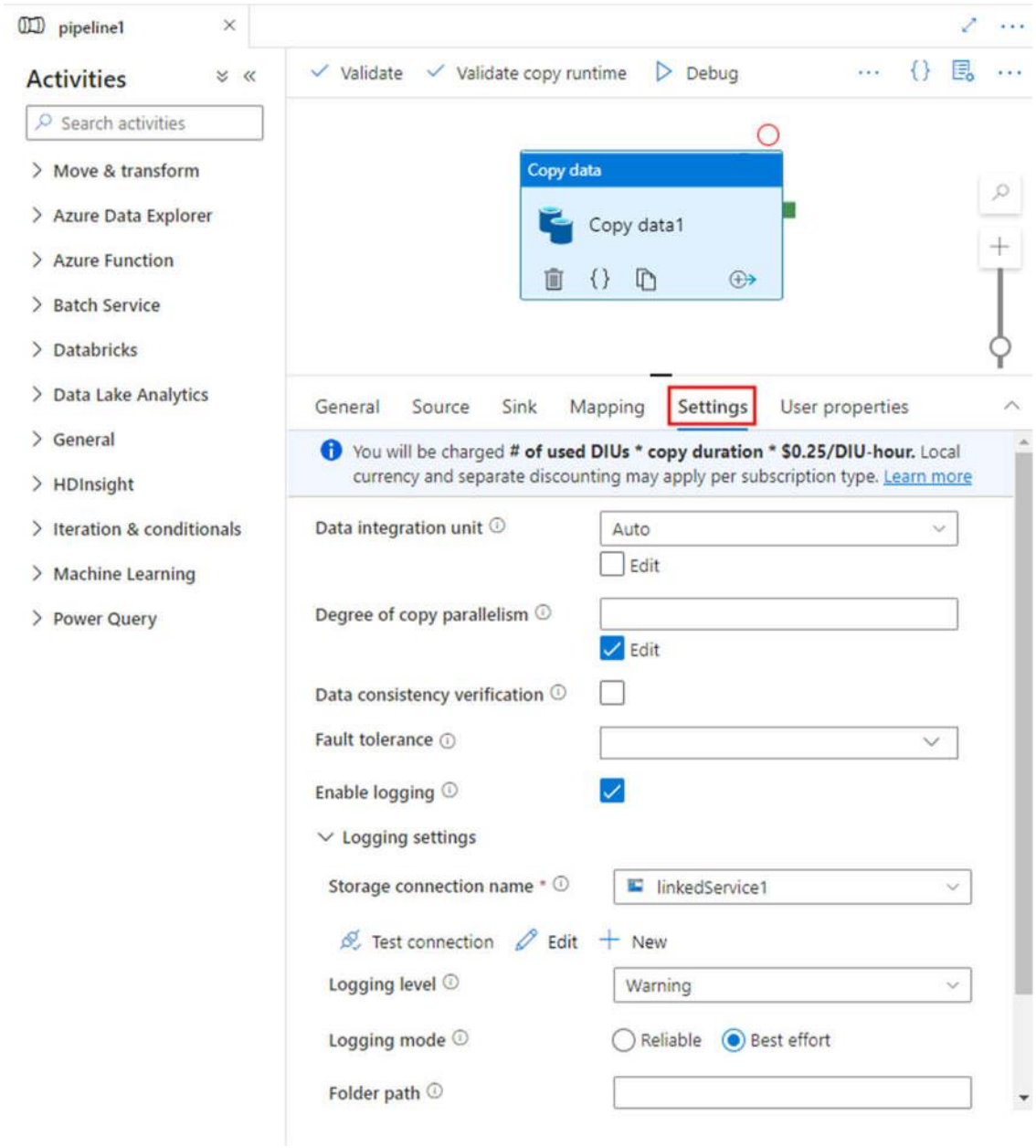
Add the following code to policymodule.exe.config:

XMLCopy

```
<runtime>
  <generatePublisherEvidence enabled="false"/>
</runtime>
```

Create a profile for the service account

On the runbook server where runbooks run that contain an activity referencing the .NET assemblies, sign in to the computer using the service account credentials. A profile is created on first sign-in.


pipeline1
Activities
Search activities
Move & transform
Azure Data Explorer
Azure Function
Batch Service
Databricks
Data Lake Analytics
General
HDInsight
Iteration & conditionals
Machine Learning
Power Query
Validate
Validate copy runtime
Debug
Copy data
Copy data1
General
Source
Sink
Mapping
Settings
User properties
You will be charged # of used DIUs * copy duration * $0.25/DIU-hour. Local currency and separate discounting may apply per subscription type. Learn more
Data integration unit
Auto
Edit
Degree of copy parallelism
Edit
Data consistency verification
Fault tolerance
Enable logging
Logging settings
Storage connection name *
linkedService1
Test connection
Edit
New
Logging level
Warning
Logging mode
Reliable
Best effort
Folder path

v. Configure runbook throttling

To configure the maximum number of runbooks that a runbook server processes

Navigate to the folder whereby default the Runbook Server Runbook Throttling tool is stored: C:\Program Files\Microsoft System Center\Orchestrator\Management Server.

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

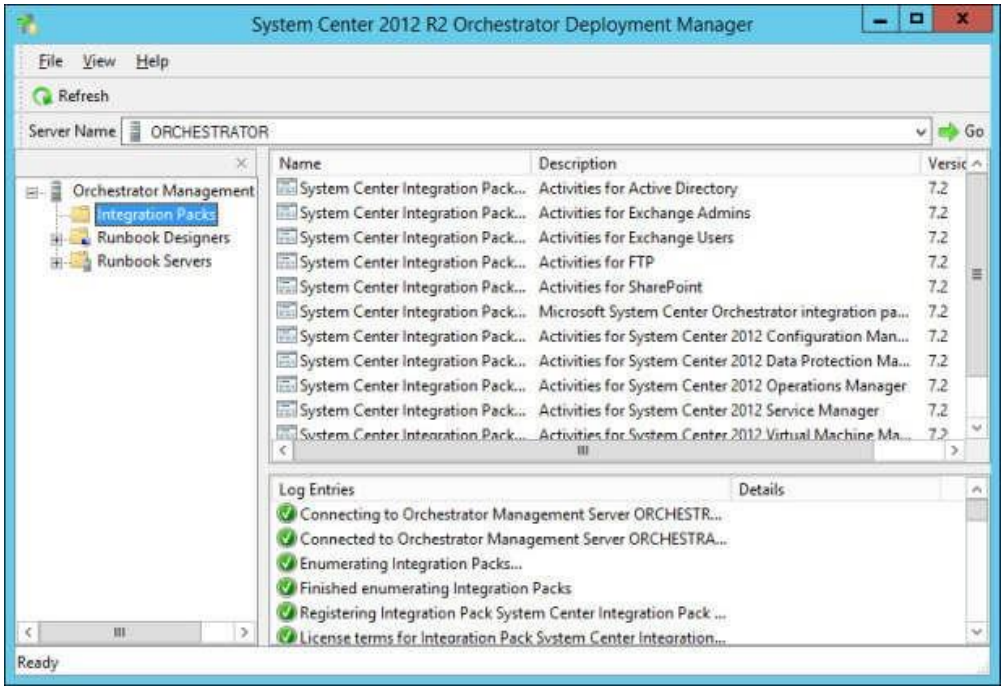
To apply the change to all runbook servers:

aspt * <MaximumRunningRunbooks>.

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

aspt * 40

Restart the **Orchestrator Runbook Service**.



B. 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

Open the installation location of the WebAPI, typically it is <OrchestratorInstallDir>\WebApi.

You can use IIS Manager to navigate to the WebAPI folder as well.

Edit the environmentVariable element in system.webServer > aspNetCore > environmentVariables in the web.config using a text editor. Particularly, you'd want to change the values of the DATABASE_* variables.

The full list of Database connection settings is available in Connection String syntax. First determine the keys you need to specify for your scenario, for example the Trusted_Connection (or its alias Integrated Security) may require other keys like User ID.

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.
9. Deploy an integration pack
10. In the navigation pane of Deployment Manager, right-click Integration Packs, click Deploy IP to Action Server or Client.

11. Select the integration pack that you want to deploy, and then click Next.
12. 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.
13. Continue to add additional runbook servers and computers running the Runbook Designer, on which you want to deploy the integration pack. Click Next.
14. In the Installation Options dialog box, configure the following settings.
15. 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.
16. 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.
- Click Next.
- In the Completing Integration Pack Deployment Wizard dialog box, click Finish.
- 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:
2. Remove it by following the instructions in How to Uninstall and Unregister an Integration Pack.
3. Log into each computer and uninstall the integration pack from Programs and Features in Control Panel.
4. 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.
5. Register and deploy the upgraded integration pack.

iii. View Orchestrator data with PowerPivot

1. Create a connection to an Orchestrator feed
2. Open Excel.
3. Click the **PowerPivot** tab above the ribbon.
4. Click **PowerPivot Window** on the ribbon. A **PowerPivot for Excel** book opens.
5. Click **From Data Feeds** on the ribbon. A **Table Import Wizard** opens.
6. 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
7. Click Test Connection.
8. If the test connection is successful, click OK and proceed to the next step.
9. If the test connection fails, do the following:
10. Click OK.

11. Click Advanced. The Advanced dialog box opens.
12. In the Security section, change Integrated Security to Basic.
13. Change Persist Security Info to True.
14. Enter your User ID and Password in the appropriate boxes.
15. Click Test Connection.
16. Click OK and click OK.
17. Click Next.
18. Select the check boxes of the table or tables that you want to import.
19. To filter columns, select a table, click Preview & Filter, clear any boxes to exclude, and then click OK.
20. Click Finish. The data is imported.
21. Click Close.
22. Create a summary of runbook results
23. 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.
24. Create a connection to the data feed
25. Open Excel.
26. Click the **PowerPivot** tab above the ribbon.
27. Click **PowerPivot Window** on the ribbon. A **PowerPivot for Excel** book opens.
28. Click **From Data Feeds** on the ribbon. A **Table Import** wizard opens.
29. Enter the Orchestrator web service URL in the **Data Feed URL** box.
30. Click **Next**.
31. Select the check boxes of the **Runbooks**, **RunbookInstances**, and **RunbookServers** tables.
32. Click **Finish**. The data is imported.
33. Click **Close**.
34. Create relationships in PowerPivot
35. In the **PowerPivot for Excel** window, select the **RunbookInstance** tab.
36. Right-click the header of the **RunbookId** column to select **Create Relationship**.
37. In the **Related Lookup Table** list, select **Runbooks**, and in the **Related Lookup Column** list, select **Id**, and then click **Create**.
38. Right-click the header of the **RunbookServerId** column to select **Create Relationship**.
39. In the **Related Lookup Table** list, select **RunbookServers**, and in the **Related Lookup Column** list, select **Id**, and then click **Create**.
40. Create a pivot table
41. In the **PowerPivot for Excel** window, click **PivotTable** on the ribbon, and select **PivotTable**.
42. In the **Create PivotTable** dialog box, select **New Worksheet**, and then click **OK**.
43. In the **PowerPivot Field List**, under **RunbookServers**, click and drag **Name** to the **Row Labels** box.
44. In the **PowerPivot Field List**, under **Runbooks**, click and drag **Name** to the **Row Labels** box.
45. In the **PowerPivot Field List**, under **RunbookInstances**, click and drag **Status** to the **Column Labels** box.

46. In the **PowerPivot Field List**, under **RunbookInstances**, click and drag **RunbookId** to the **Sum Values** box.
47. Right-click **RunbookId** to select **Summarize by**, and then click **Count**.

vi. Change Orchestrator user groups

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.

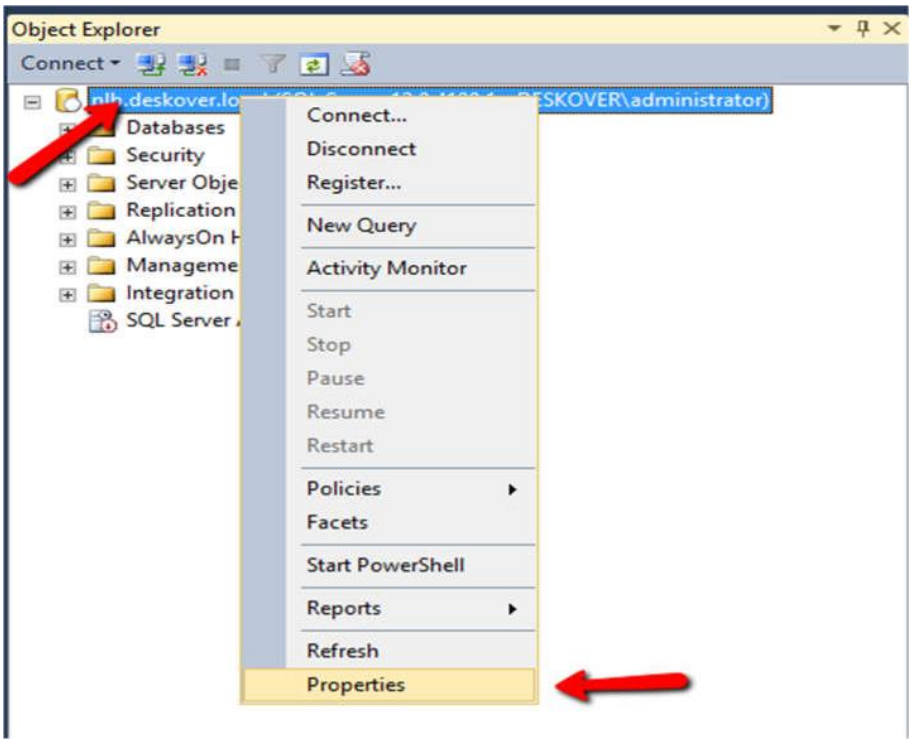
PermissionsConfig tool

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:

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

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

PermissionsConfig -help

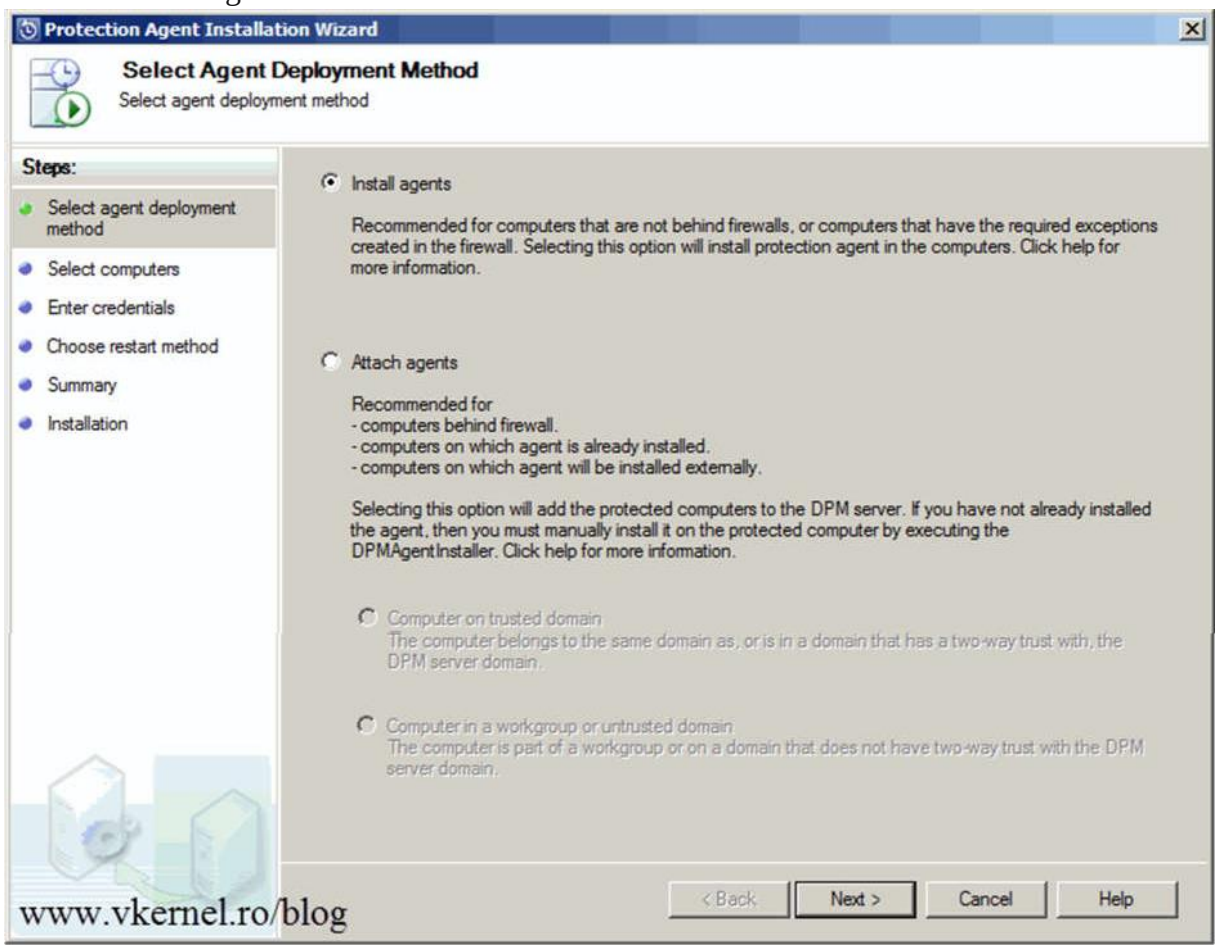


Practical No. 9

Install and Deploy DPM

i. Install DPM

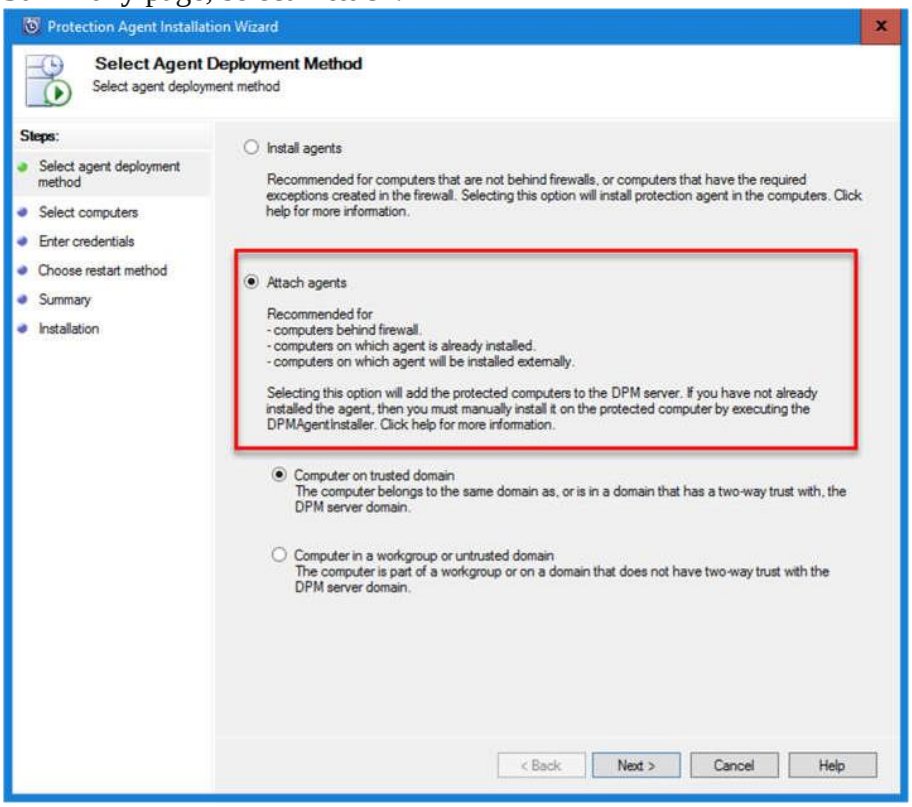
1. If required, extract the DPM 2016.exe (for DPM 2016)/DPM 2019.exe (for DPM 2019) file onto the machine on which you want to run DPM. To do this, run the exe file, and on the **Welcome** screen, select **Next**. In **Select Destination Location**, specify where you want to extract the installation 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. After you've installed the DPM agent manually, you'll need to attach the agent to the DPM server.

2. In the DPM Administrator Console, on the navigation bar, select **Management** > **Agents**. In the **Actions** pane, select **Install**.
3. On the **Select Agent Deployment Method** page, select **Attach agents** > **Computer on a trusted domain** > **Next**. The Protection Agent Installation Wizard opens.
4. On the **Select Computers** page, DPM displays a list of available computers in the same domain as the DPM server. Select one or more computers (50 maximum) from the **Computer name** list > **Add** > **Next**.
5. If this is the first time you've used the wizard, DPM queries Active Directory to get a list of potential computers. After the first installation, DPM displays the list of computers in its database, which is updated once each day by the auto-discovery process.
6. To add multiple computers by using a text file, select the **Add From File** button, and in the **Add From File** dialog box, type the location of the text file or select **Browse** to navigate to its location.
7. 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 trusted domain. 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 trusted domain, and you must be a member of the local Administrators group on all selected computers that you want to protect.
8. On the **Summary** page, select **Attach**.



iii. Deploy protection groups

A System Center Data Protection Manager (DPM) protection group is a collection of data sources such as volumes, shares, or application workloads, which have common backup and restore settings. The protection group settings specify:

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.

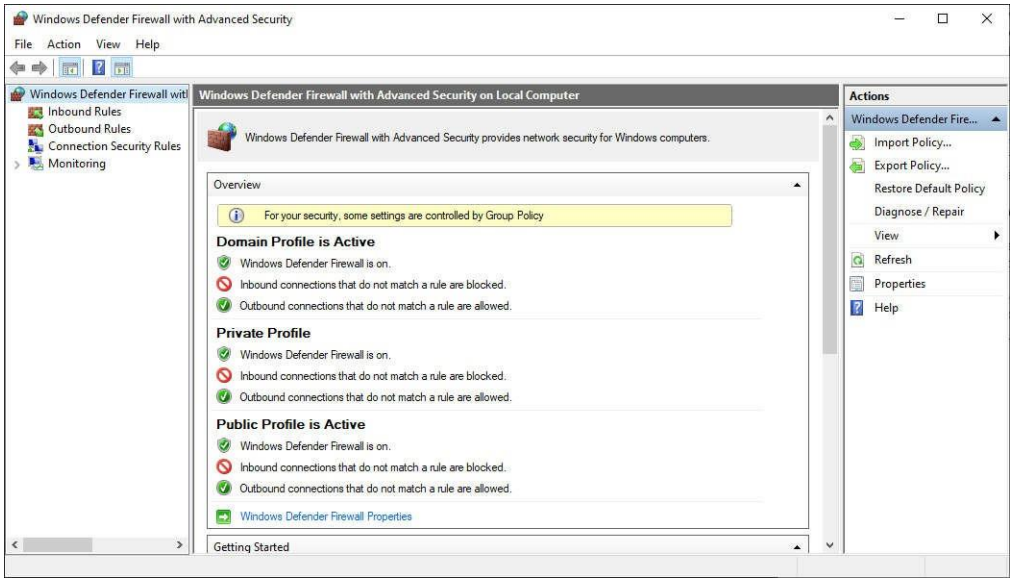
Consistency checks - How the replicated data should be checked for consistency.

iv. Configure firewall settings

To open Windows Firewall, go to the **Start** menu, select **Run**, type **WF.msc**, and then select **OK**.

Keep default settings

When you open the Windows Defender Firewall for the first time, you can see the default settings applicable to the local computer. The Overview panel displays security settings for each type of network to which the device can connect.

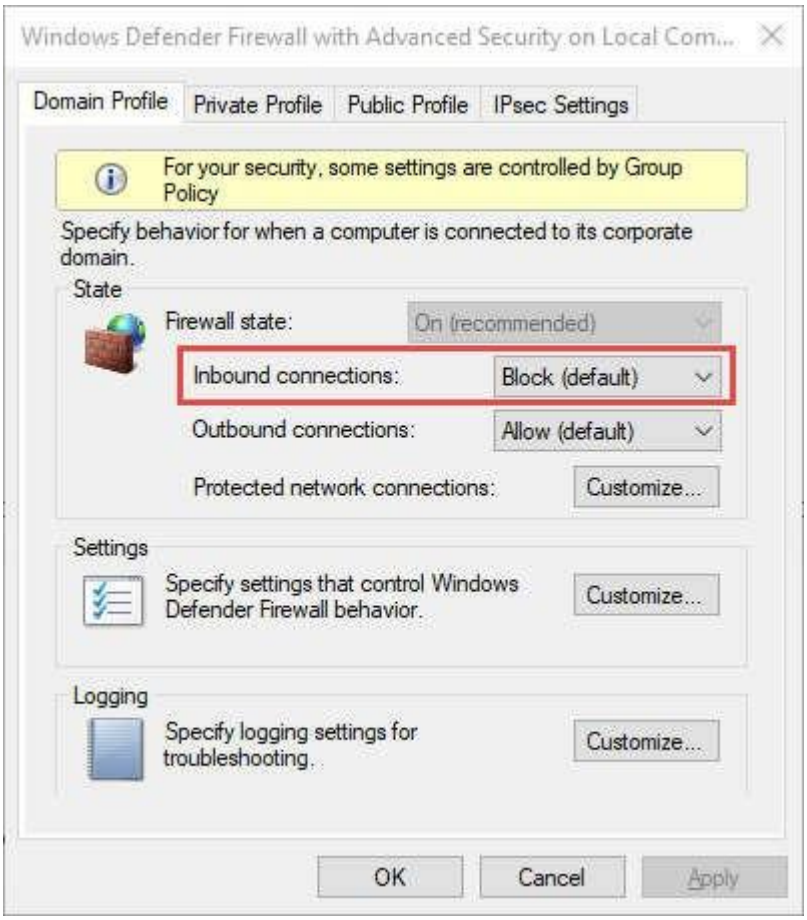


- Domain profile: Used for networks where there's a system of account authentication against an Active Directory domain controller
- Private profile: Designed for and best used in private networks such as a home network

- Public profile: Designed with higher security in mind for public networks, like Wi-Fi hotspots, coffee shops, airports, hotels, or stores

View detailed settings for each profile by right-clicking the top-level Windows Defender Firewall with Advanced Security node in the left pane and then selecting Properties.

Maintain the default settings in Windows Defender Firewall whenever possible. These settings have been designed to secure your device for use in most network scenarios. One key example is the default Block behavior for Inbound connections.



Practical No. 10

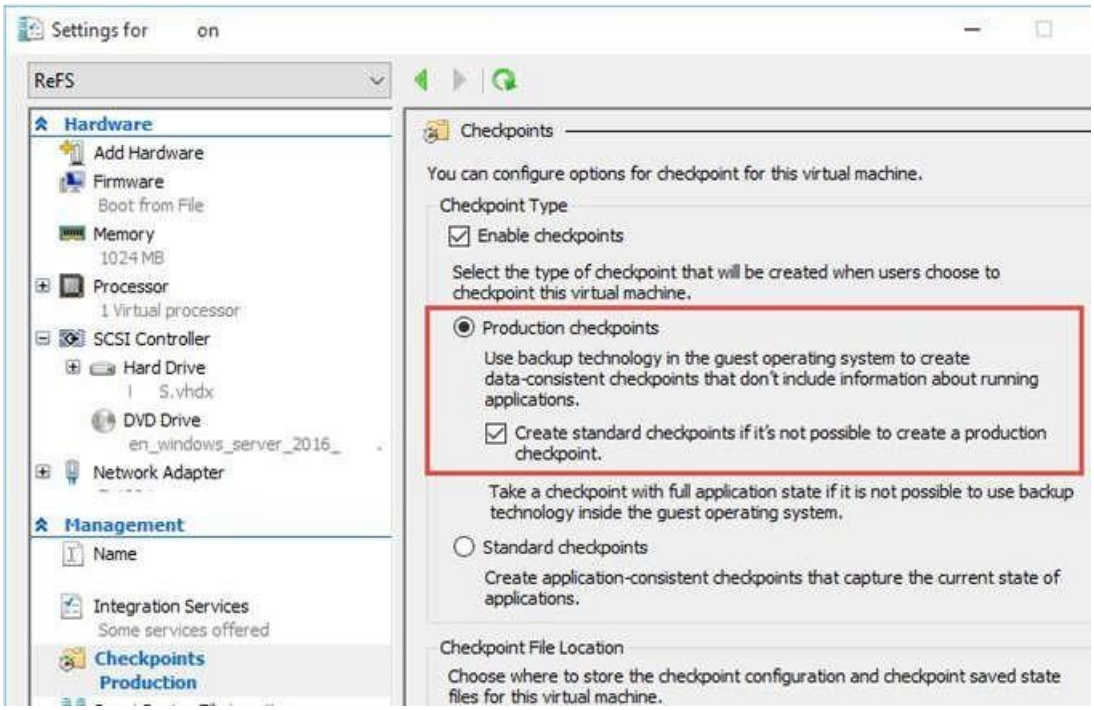
Protect Workloads

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.

DPM can back up virtual machines running on Hyper-V host servers in the following scenarios:

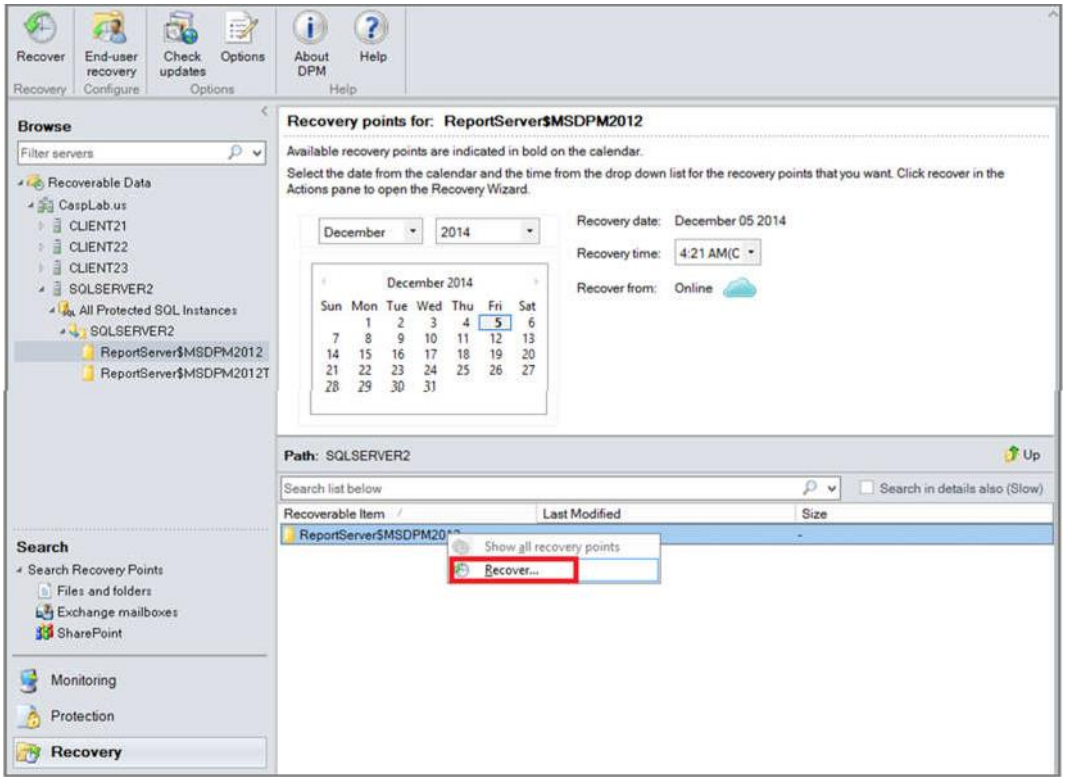
1. **Virtual machines with local or direct storage** - Back up virtual machines hosted on Hyper-V host standalone servers that have local or directly attached storage. For example, a hard drive, a storage area network (SAN) device, or a network attached storage (NAS) device. The DPM protection agent must be installed on all hosts.
2. **Virtual machines in a cluster with CSV storage** - Back up virtual machines hosted on a Hyper-V cluster with Cluster Shared Volume (CSV) storage. DPM 2012 SP1 introduced express full backup, parallel backups, and cluster query improvements for CSV backup. The DPM protection agent is installed on each cluster node.
3. **Virtual machines with SMB storage** - Back up virtual machines hosted on a Hyper-V standalone server or cluster with SMB 3.0 file server storage. SMB shares are supported on a standalone file server or on a file server cluster. If you're using an external SMB 3.0 file server, the DPM protection agent should be installed on it. If the storage server is clustered, the agent should be installed on each cluster node. You'll need full-share and folder-level permissions for the machine's account of the application server on the SMB share.
4. **Back up virtual machines configured for live migration** - Live migration allows you to move virtual machines from one location to another while providing uninterrupted access. You can migrate virtual machines between two standalone servers, within a single cluster, or between standalone and cluster nodes. Multiple live migrations can run concurrently. You can also perform a live migration of virtual machine storage so that virtual machines can be moved to new storage locations while they continue to run. DPM can back up virtual machines that are configured for live migration. Read more.
5. **Back up replica virtual machines** - Back up replica virtual machines running on a secondary server (DPM 2012 R2 only).



ii. Back up SQL Server with DPM

1. To create a protection group, select **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**, select the SQL Server instances on the server you want to protect.
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 backup 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 backup interval, you can select **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:
7. When the retention range is 1-99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly.
8. When the retention range is 1-11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly.

9. When the retention range is 1-4 weeks, you can select backups to occur daily or weekly.
10. On a standalone tape drive, for a single protection group, DPM uses the same tape for daily backups until there's insufficient space on the tape. You can also colocate data from different protection groups on tape.
11. On the **Select Tape and Library Details** page, specify the tape/library to use and whether data should be compressed and encrypted on tape.
12. In the **Review disk allocation** page, review the storage pool disk space allocated for the protection group.
13. **Total Data size** is the size of the data you want to back up, and **Disk space to be provisioned on DPM** is the space that DPM recommends for the protection group. DPM chooses the ideal backup volume based on the settings. However, you can edit the backup volume choices in the **Disk allocation details**. For the workloads, select the preferred storage in the dropdown menu. Your edits change the values for **Total Storage** and **Free Storage** in the **Available Disk Storage** pane. Underprovisioned space is the amount of storage DPM suggests you add to the volume to continue with backups smoothly in the future.
14. 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 recommend 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.
15. 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 selecting and holding the protection group in the **Protection** area of the DPM console and selecting **Perform Consistency Check**.
16. If you've selected to back up to the cloud with Azure Backup, on the **Specify online protection data** page, ensure to select the workloads that you want to back up to Azure.
17. 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 backup runs, a data recovery point is created in Azure from the copy of the backed-up data stored on the DPM disk.
18. In **Specify online retention policy**, you can specify how the recovery points created from the daily/weekly/monthly/yearly backups are retained in Azure.
19. 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. For more information, see Offline seeding using Azure Data Box.
20. On the **Summary** page, review your settings. After you select **Create Group**, the 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.



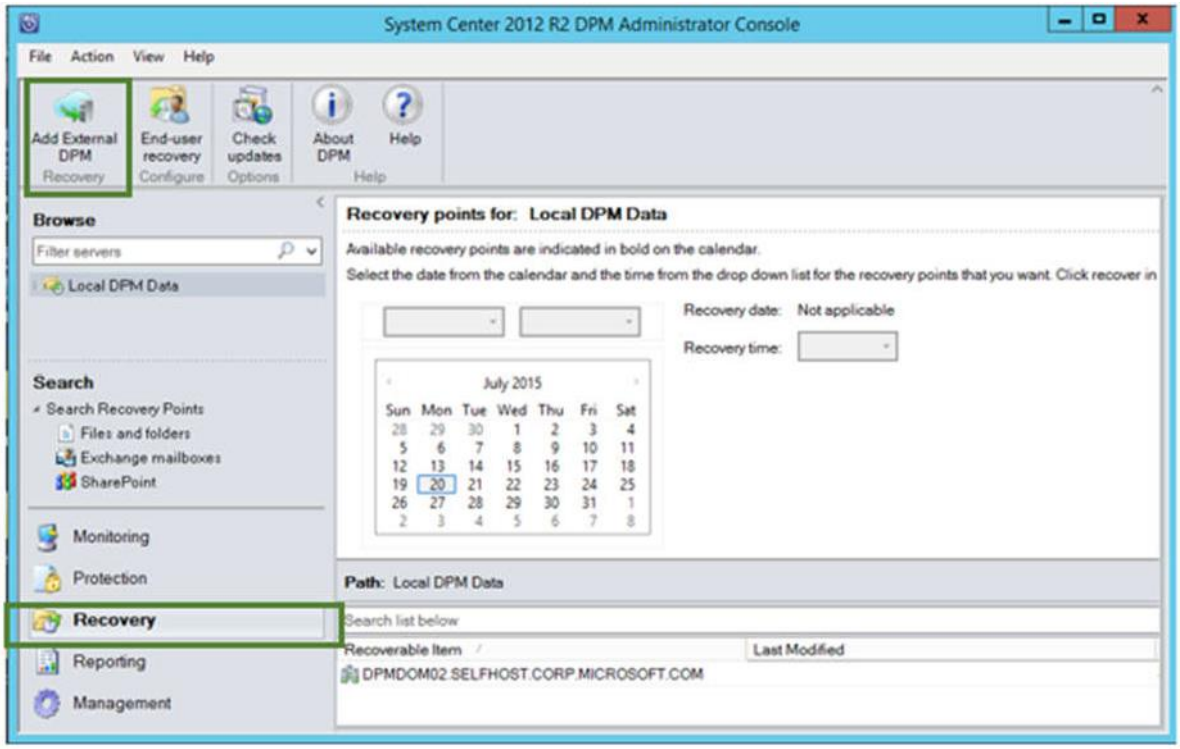
iii. Back up file data with DPM

1. You can use System Center Data Protection Manager (DPM) to back up file data on server and client computers
2. **Deploy DPM** - Verify that DPM is installed and deployed correctly.
3. **Set up storage** - You can store backed-up data on disk, on tape, and in the cloud with Azure.
4. **Set up the DPM protection agent** - You'll need to install the DPM protection agent on every machine you want to back up.
5. Back up file data
6. After you set up your DPM infrastructure, you can enable protection machines that have file data you want to back up.
7. To create a protection group, select **Protection** > **Actions** > **Create Protection Group** to open the **Create New Protection Group** wizard in the DPM console.
8. In **Select Protection Group Type**, select **Servers**.
9. 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.
10. 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 backup to a standalone tape device or tape library connected to the DPM server.

11. In **Select short-term goals**, specify how you want to back up to short-term storage on disk. In **Retention range**, specify how long you want to keep the data on disk.
    In **Synchronization frequency**, specify how often you want to run an incremental backup to disk. If you don't want to set a backup 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.
12. 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:
13. When the retention range is 1-99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly.
14. When the retention range is 1-11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly.
15. When the retention range is 1-4 weeks, you can select backups to occur daily or weekly.
16. On a standalone tape drive, for a single protection group, DPM uses the same tape for daily backups until there's insufficient space on the tape. You can also co-locate data from different protection groups on tape.
17. On the **Select Tape and Library Details** page, specify the tape/library to use and whether data should be compressed and encrypted on tape.
18. In the **Review disk allocation** page, review the storage pool disk space allocated for the protection group.
19. **Total Data size** is the size of the data you want to back up, and **Disk space to be provisioned on DPM** is the space that DPM recommends for the protection group. DPM chooses the ideal backup volume based on the settings. However, you can edit the backup volume choices in the **Disk allocation details**. For the workloads, select the preferred storage in the dropdown menu. Your edits change the values for **Total Storage** and **Free Storage** in the **Available Disk Storage** pane. Underprovisioned space is the amount of storage DPM suggests you add to the volume to continue with backups smoothly in the future.
20. 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 recommend 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.
21. 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 selecting and holding the protection group in the **Protection** area of the DPM console and selecting **Perform Consistency Check**.
22. If you've selected to back up to the cloud with Azure Backup, on the **Specify online protection data** page, ensure to select the workloads that you want to back up to Azure.
23. 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 backup runs, a data recovery point is created in Azure from the copy of the backed-up data stored on the DPM disk.

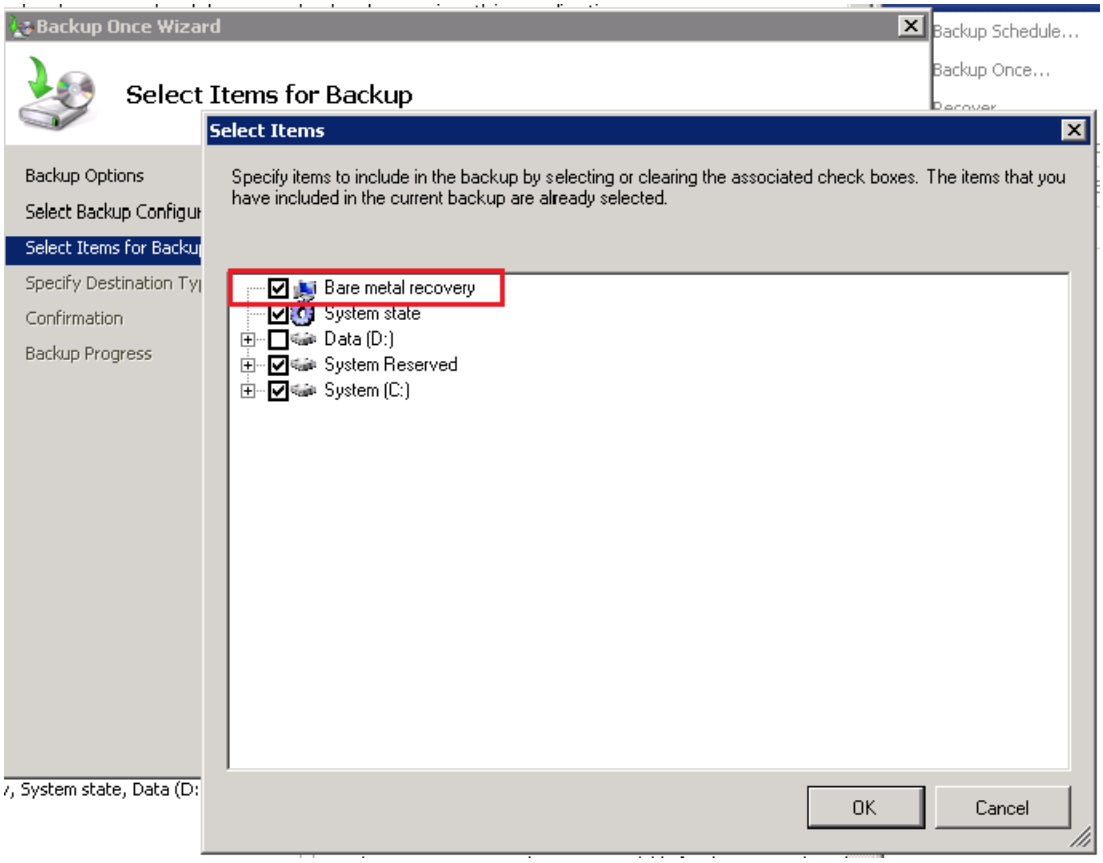
24. In **Specify online retention policy**, you can specify how the recovery points created from the daily/weekly/monthly/yearly backups are retained in Azure.
25. In **Choose online replication**, specify how the initial full replication of data will occur. You can replicate over the network or do an offline backup (offline seeding). Offline backup uses the Azure Import feature.
26. On the **Summary** page, review your settings. After you select **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.



iv. Backup system state and bare metal

1. System Center Data Protection Manager (DPM) can back up system state and provide bare metal recovery (BMR) protection.
2. **System state backup**: Backs up operating system files, enabling you to recover when a machine starts but you've lost system files and registry. A system state backup includes:
3. Domain member: Boot files, COM+ class registration database, registry
4. Domain controller: Active Directory (NTDS), boot files, COM+ class registration database, registry, system volume (sysvol folder)
5. Machine running cluster services: Additionally backs up cluster server metadata
6. Machine running certificate services: Additionally backs up certificate data

7. **Bare metal backup**: Backs up operating system files and all data except user data on critical volumes. By definition, a BMR backup includes a system state backup. It provides protection when a machine won't start and you have to recover everything.



v. Backup and restore VMware servers

1. Select **Protection** > **Actions** > **Create Protection Group** to open the **Create New Protection Group** wizard in the DPM console.
2. In **Select protection group** type, select **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. Learn more in Deploy protection groups.
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 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 backup 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, specify how long you want to keep the data on disk.
   In **Synchronization frequency**, specify how often you want to run an incremental backup to disk. If you don't want to set a backup 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:
7. When the retention range is 1-99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly.
8. When the retention range is 1-11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly.
9. When the retention range is 1-4 weeks, you can select backups to occur daily or weekly.
10. On a standalone tape drive, for a single protection group, DPM uses the same tape for daily backups until there's insufficient space on the tape. You can also co-locate data from different protection groups on tape.
11. On the **Select Tape and Library Details** page, specify the tape/library to use and whether data should be compressed and encrypted on tape.
12. 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.
13. 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 recommend 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.
14. 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 selecting and holding the protection group in the **Protection** area of the DPM console and selecting **Perform Consistency Check**.
15. If you've selected to back up to the cloud with Azure Backup, on the **Specify online protection data** page, ensure to select the workloads that you want to back up to Azure.
16. 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 backup runs, a data recovery point is created in Azure from the copy of the backed-up data stored on the DPM disk.
17. In **Specify online retention policy**, specify how the recovery points created from the daily/weekly/monthly/yearly backups are retained in Azure.
18. 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.

19. On the **Summary** page, review your settings. After you select **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.