OfficeScan 11 with Windows 2012 R2 Failover Clustering Guide

Revisions

Version	Revised Date	Author	Changes

Table of Contents

1 Preface

1.1 Audience

The audience for this document is system administrators who are responsible for the setup and maintenance of Windows servers and OfficeScan server. Readers should have a working knowledge of Windows Failover Clustering and the OfficeScan server.

1.2 Purpose

This document provides the information and guidelines of OfficeScan 11 server installation on Windows 2012 R2 Failover Clustering.

2 Installing OfficeScan 11 on Windows Server 2012 R2 Failover Clustering

Note：OfficeScan server only support Active/Passive clusters

This process must be followed on each node. To install OfficeScan:

1. Execute the OfficeScan 11 installer on Node1. Click **Next**.

Figure 1. Installation program start screen

2. Read the license agreement carefully and accept the license agreement terms to proceed with installation. Click **Next**.

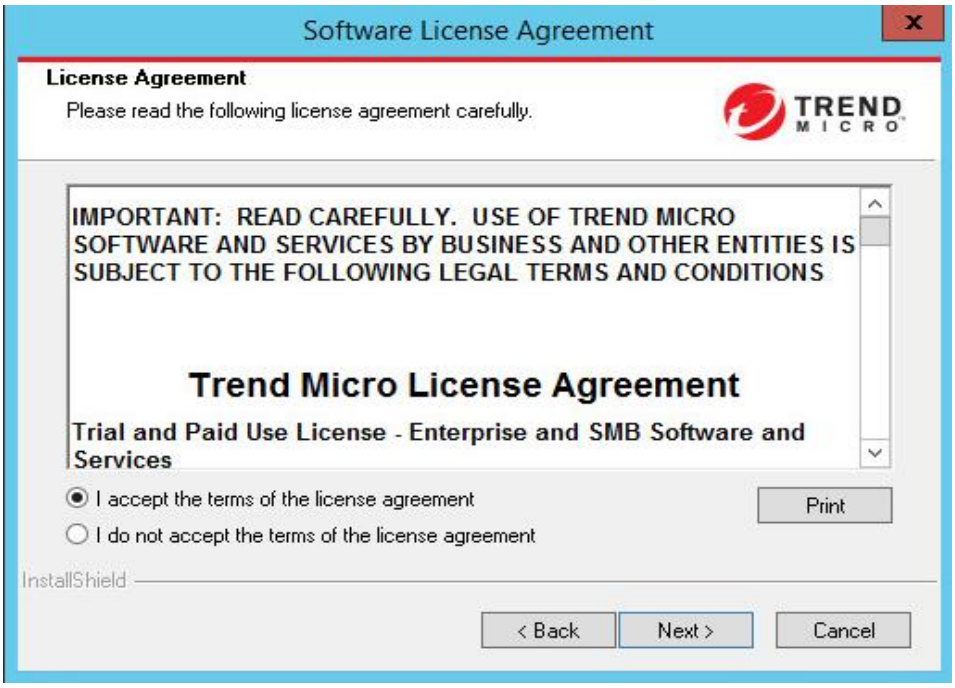

Figure 2. License Agreement screen

3. Run Setup and install the OfficeScan server on the current endpoint. Click **Next**.

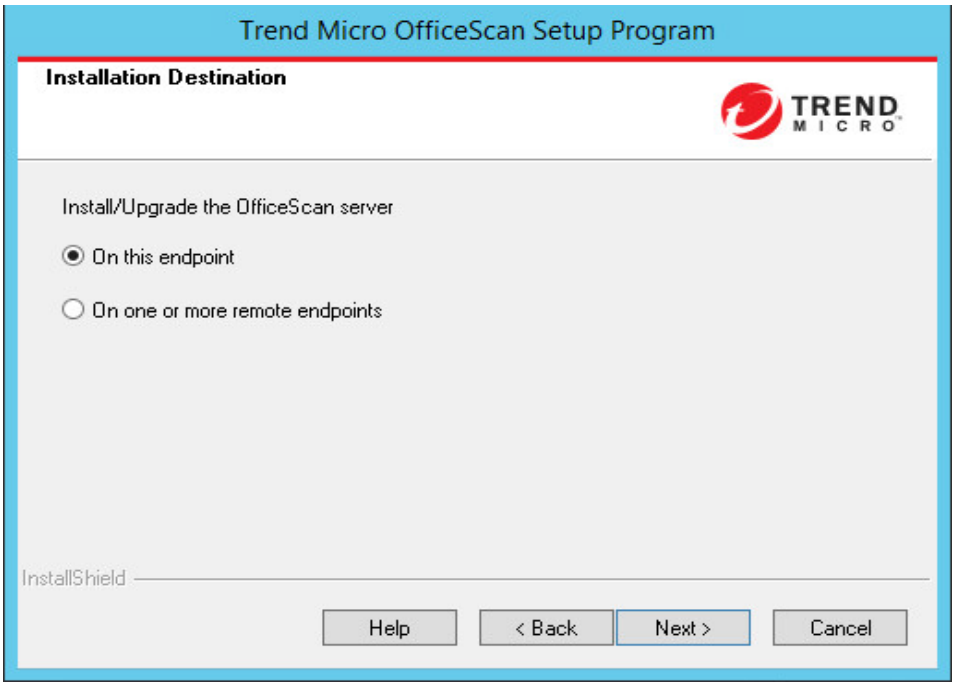

Figure 3. Installation Destination screen

4. Choose whether to Scan or do not scan the target endpoint. Click **Next**.

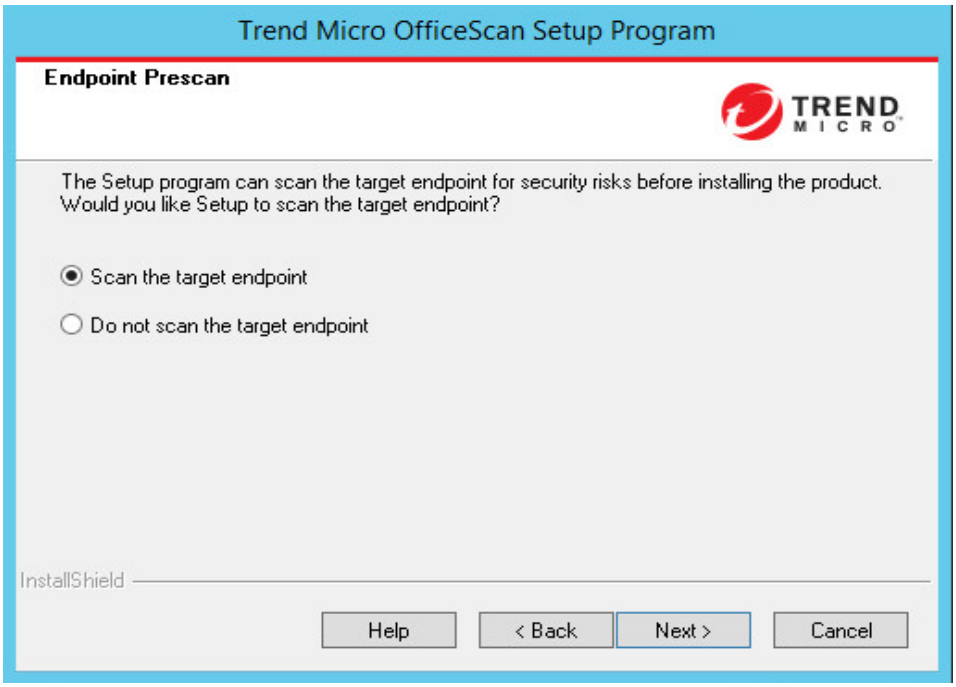

Figure 4. Endpoint Prescan screen

5. Click Browse button and then select Cluster Storage disk as installation path. Click **Next**.

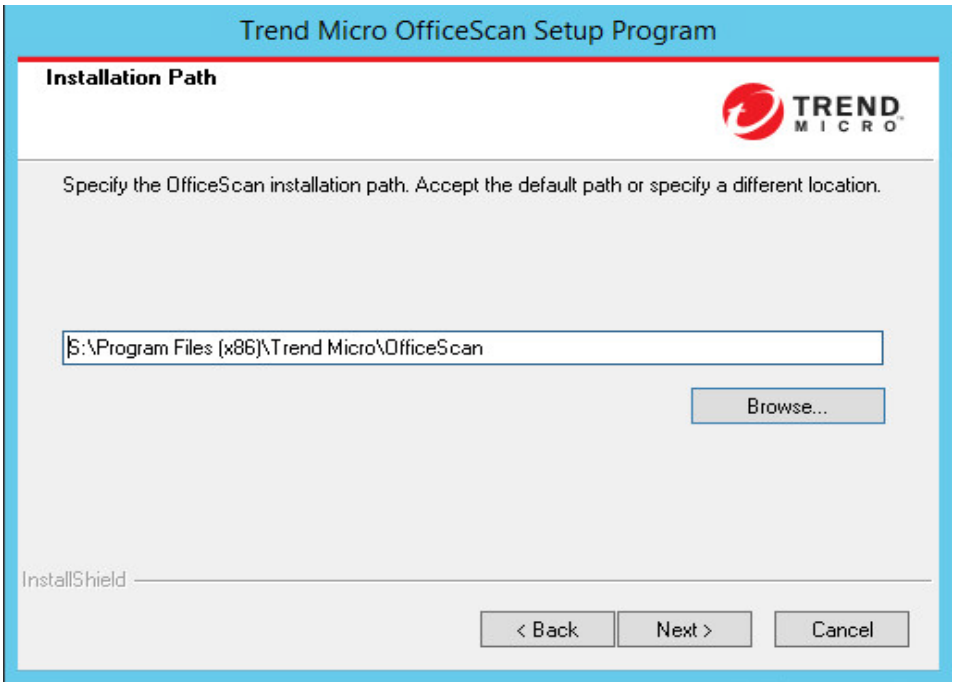

Figure 5. Installation Path screen

6. You can enable proxy settings on this page. Click **Next**.

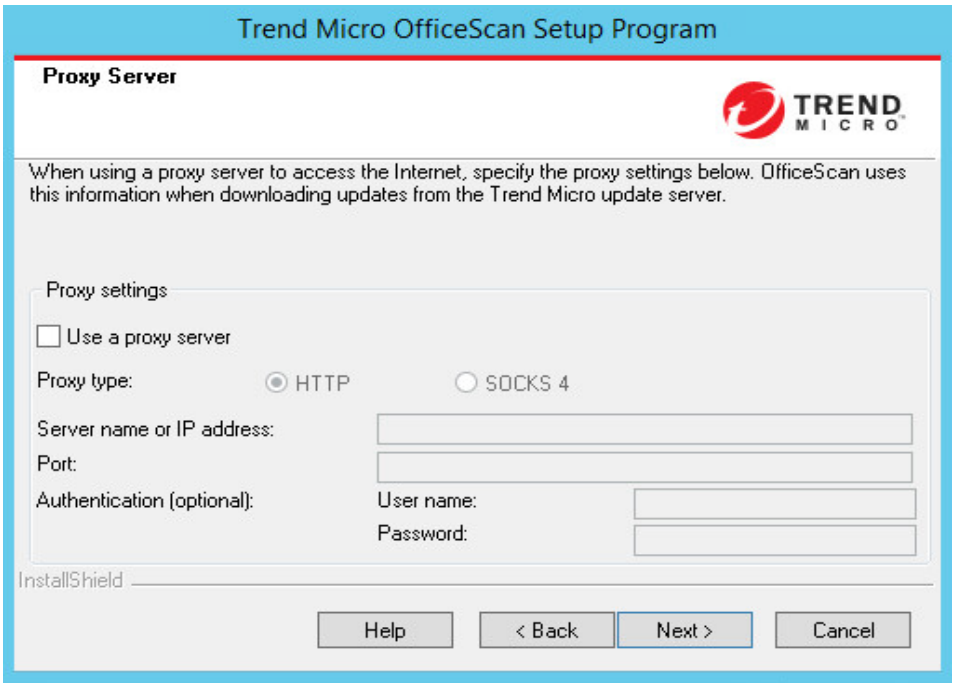

Figure 6. Proxy Server screen

7. Choose IIS web server. Click **Next**.

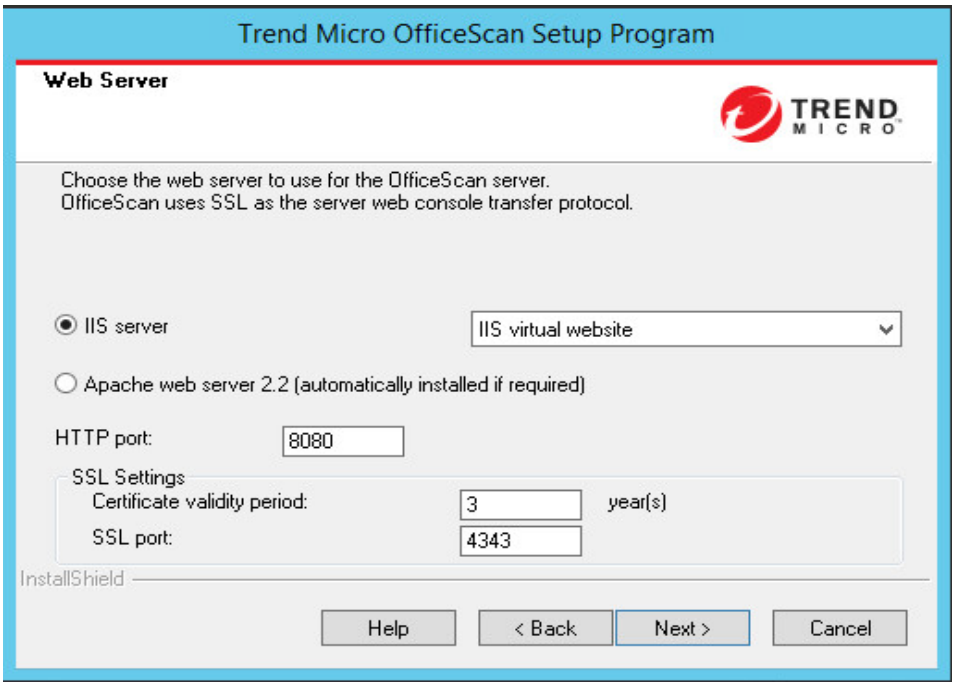

Figure 7. Web Server screen

8. Enter a name or IP address that agents uses to access the OfficeScan server. Enter a unique IP address or FQDN name. Click **Next**.

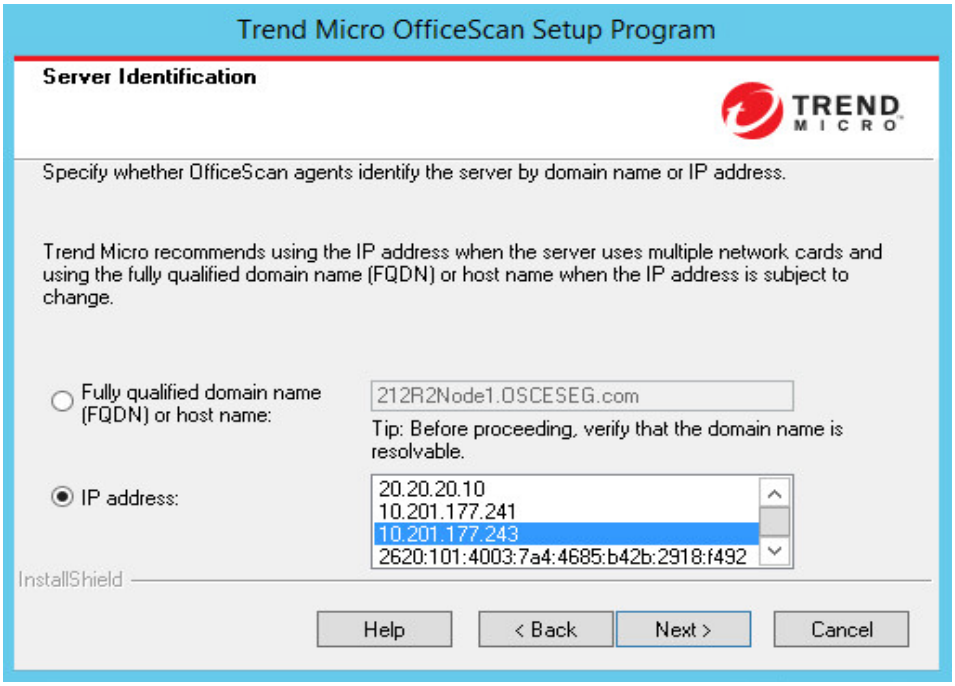

Figure 8. Server Identification screen

Note：Do not use host name for server agents connection.

9. Click **Next**.
10. Enter OfficeScan AC code. Click **Next**.

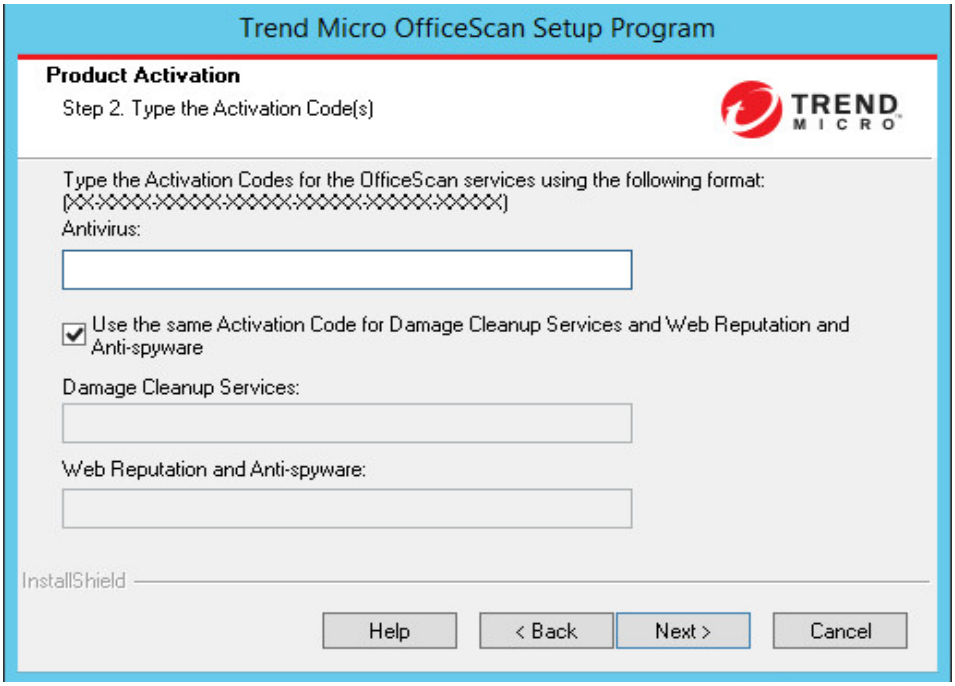

Figure 9. Product Activation screen

11. Click **Next**.
12. Choose whether to install Integrated Smart Scan Protection Server. Click **Next**.

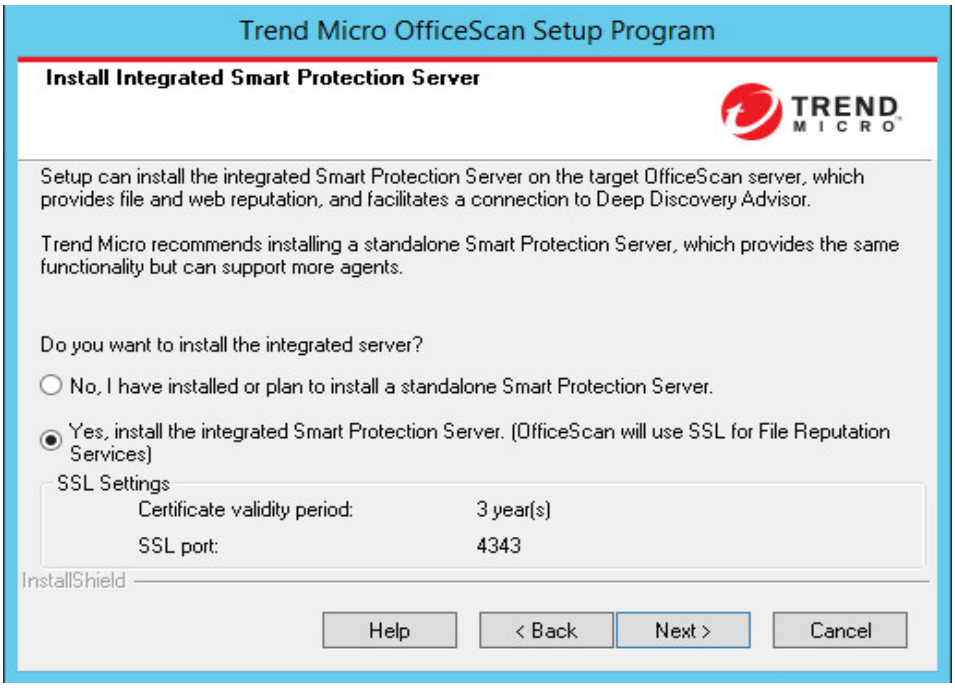

Figure 10. Install Integrated Smart Protection screen

13. Choose whether to install the OfficeScan agent on the target endpoint. Click **Next**.

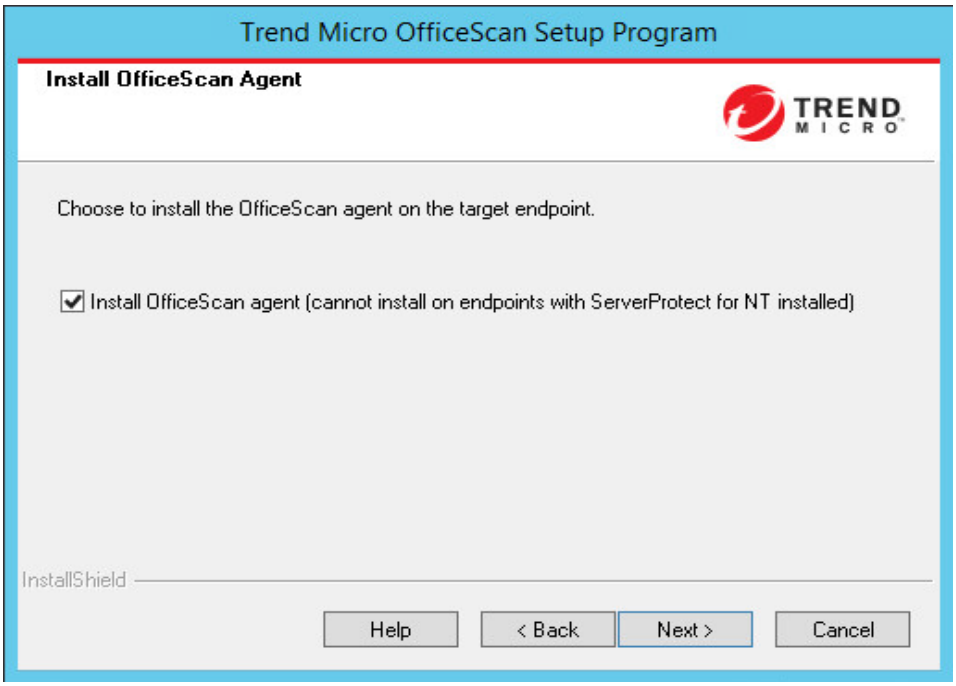

Figure 11. Install OffcieScan Agent screen

Note：If you are running OfficeScan Agent on a cluster, make sure that you exclude these locations from virus scanning:

- Q:\ (Quorum drive)
- C:\Windows\Cluster

14. Click **Next**.
15. Choose whether to enable TrendMicro Smart Feedback. Click **Next**.

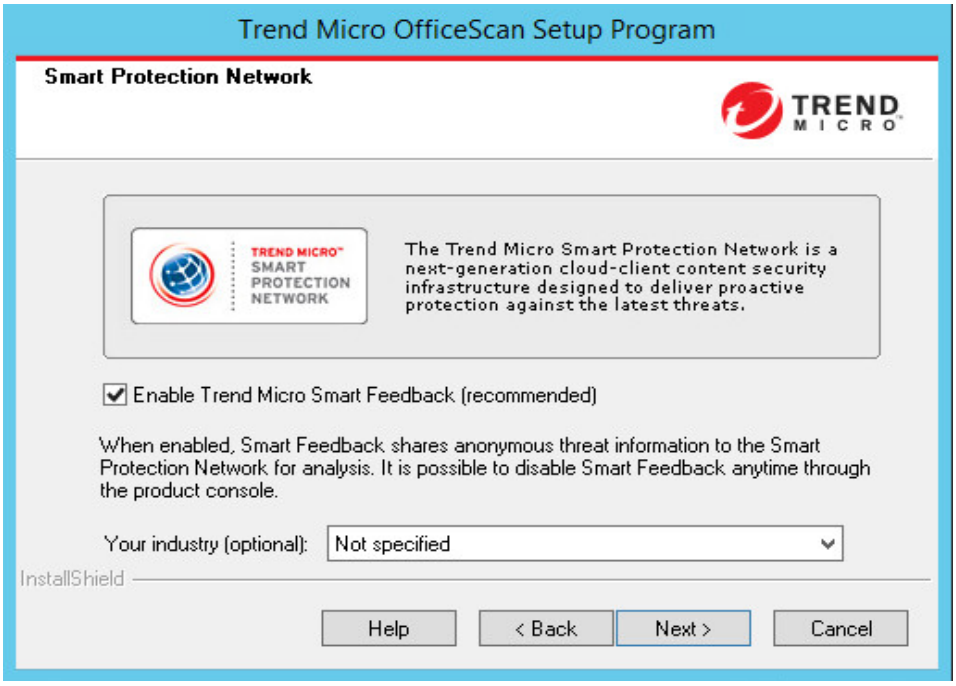

Figure 12. Smart Scan Network screen

16. Enter the OfficeScan web console password, agents unload and uninstall password. Click **Next**.

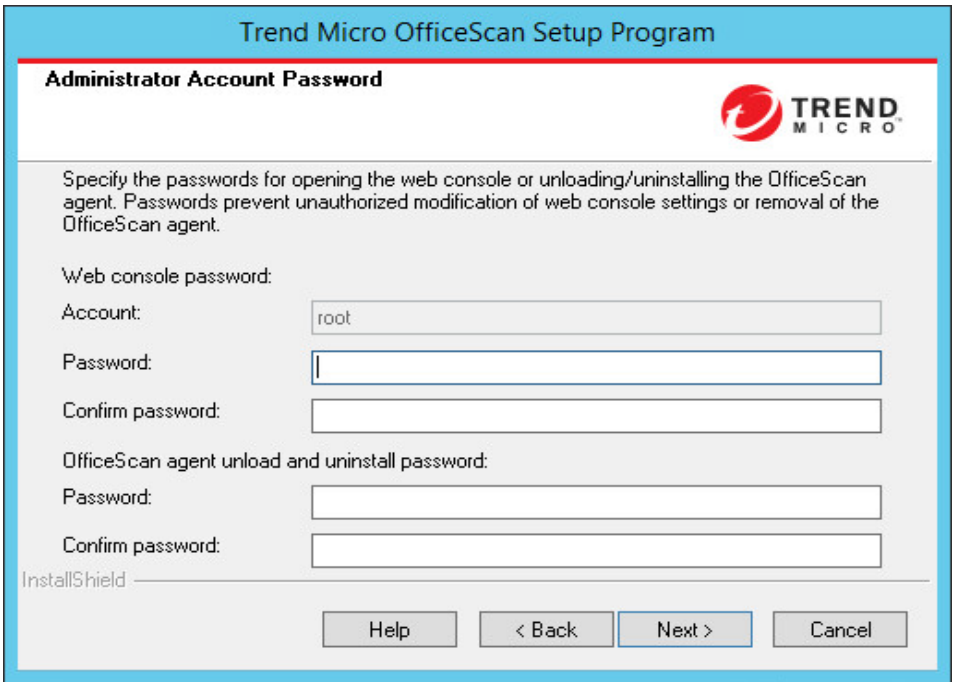

Figure 13. Administration Account Password screen

17. Click **Next**.
18. Click **Next**.
19. Choose whether to enable assessment mode. Click **Next**.

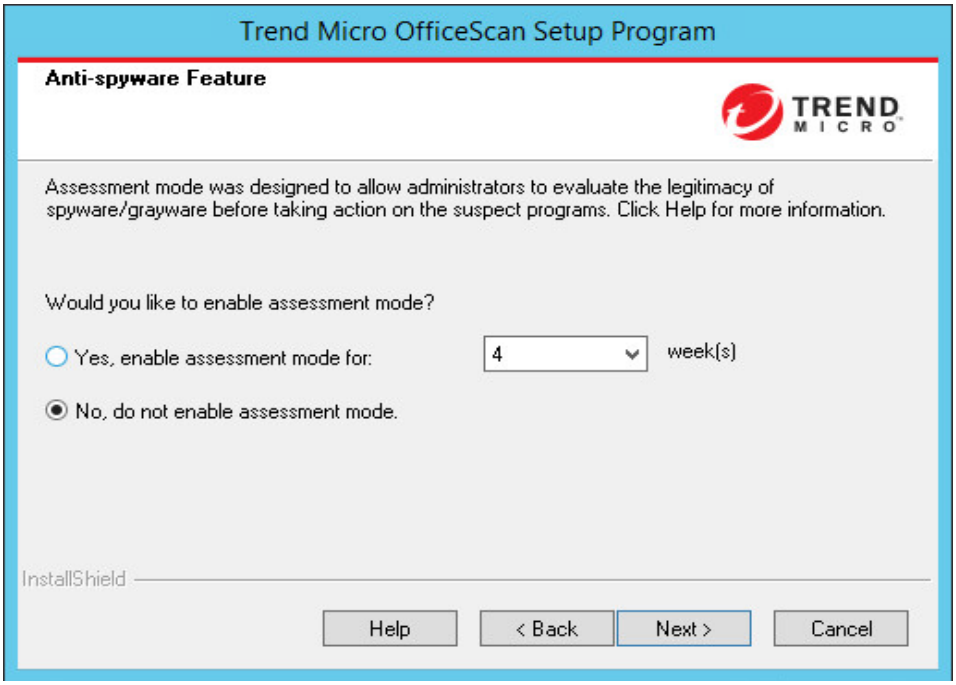

Figure 14. Anti-spyware Feature screen

20. Click **Next**.

21. Generate a new authentication certificate and enter the password. Click **Next**.

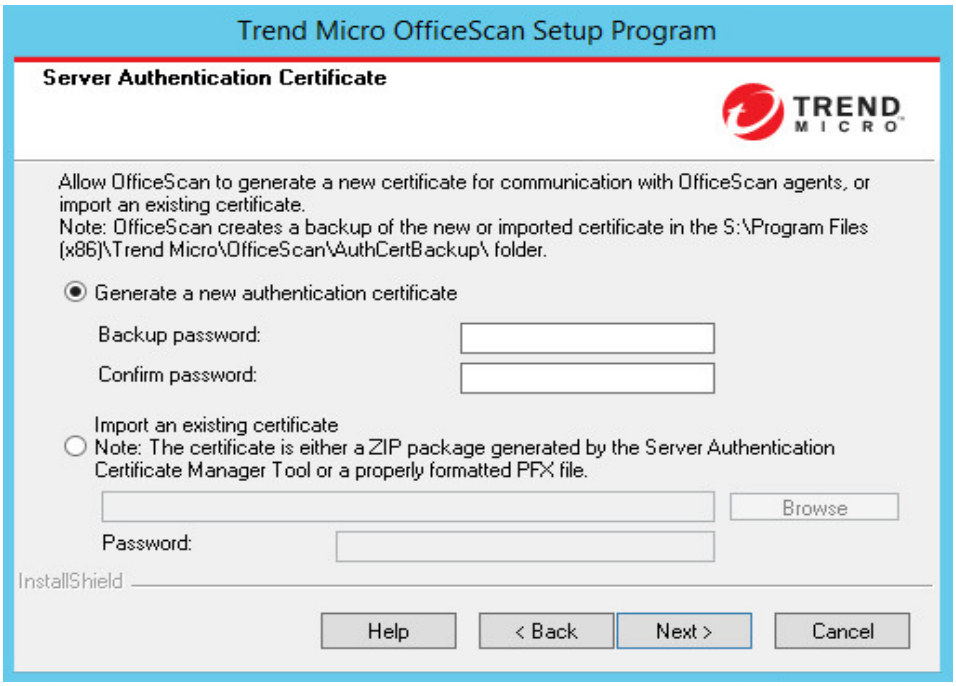

Figure 15. Server Authentication Certificate screen for new certificates

22. The shortcut folder name should be the same on each node. Click **Next**.

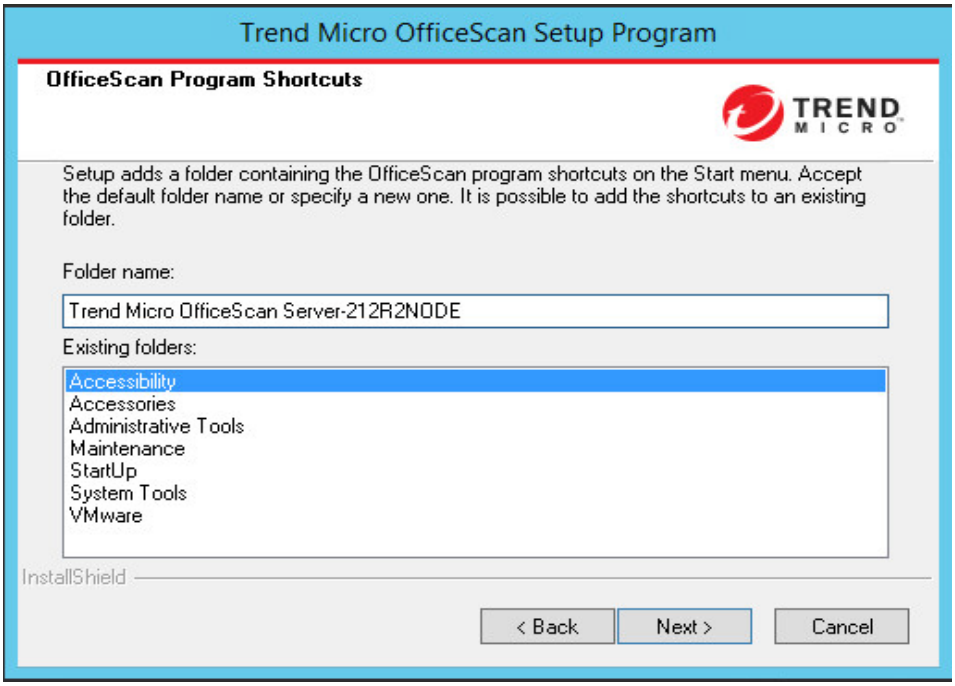

Figure 16. OfficeScan Program Shortcut screen

23. Click **Install**.

24. After the installation process, stop following OfficeScan services.
    - OfficeScan Master Service
    - OfficeScan Active Directory Integration Service
    - OfficeScan Log Receiver Service
    - OfficeScan Plug-in Manager
    - Trend Micro Local Web Classification Service
    - Trend Micro Smart Scan Server

25. Change the cluster storage owner to Node 2.
26. Delete OfficeScan installation folder “Cluster storage disk\Trend Micro\OfficeScan\PCCSRV”.
27. Do step1-20 on Node 2.
28. On server authentication certificate screen, **Browse** and import the existing certificate on “cluster storage disk \Trend Micro\OfficeScan\AuthCertBAckup”. Enter the password which you set on Node1. Click **Next**.

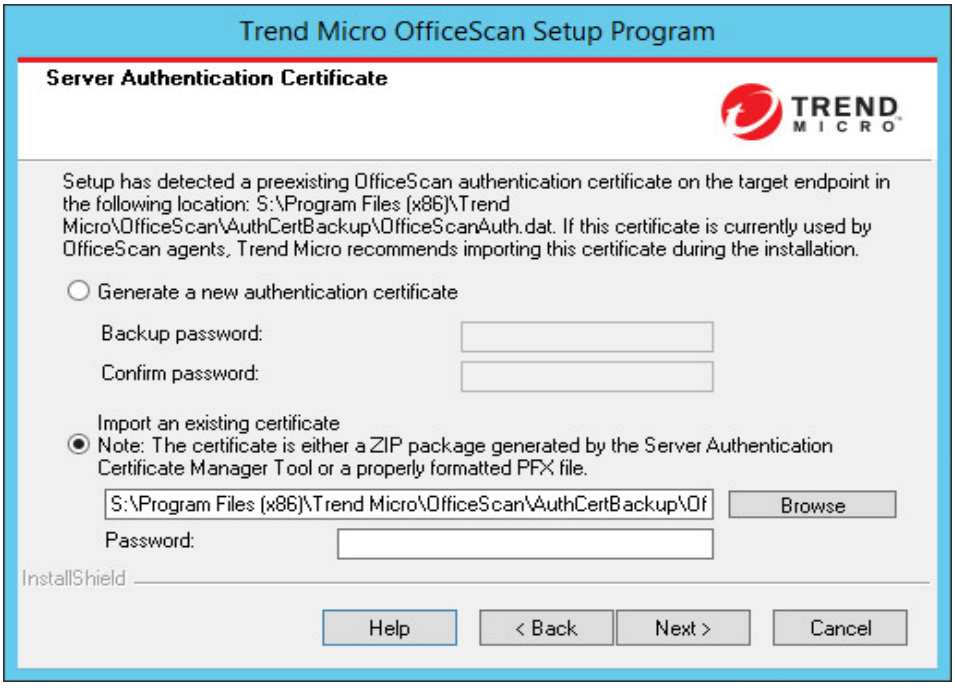

Figure 17. Server Authentication Certificate screen for preexisting certificates

29. Click **Next**, and process the OfficeScan installation on Node2.

3 IIS server authentication

This process must be followed on each node. To configure IIS settings：

1. Start Internet Information Services (IIS) Manager from the **Start** screen → **Administrative Tools** → **Internet Information Services (IIS) Manager**.

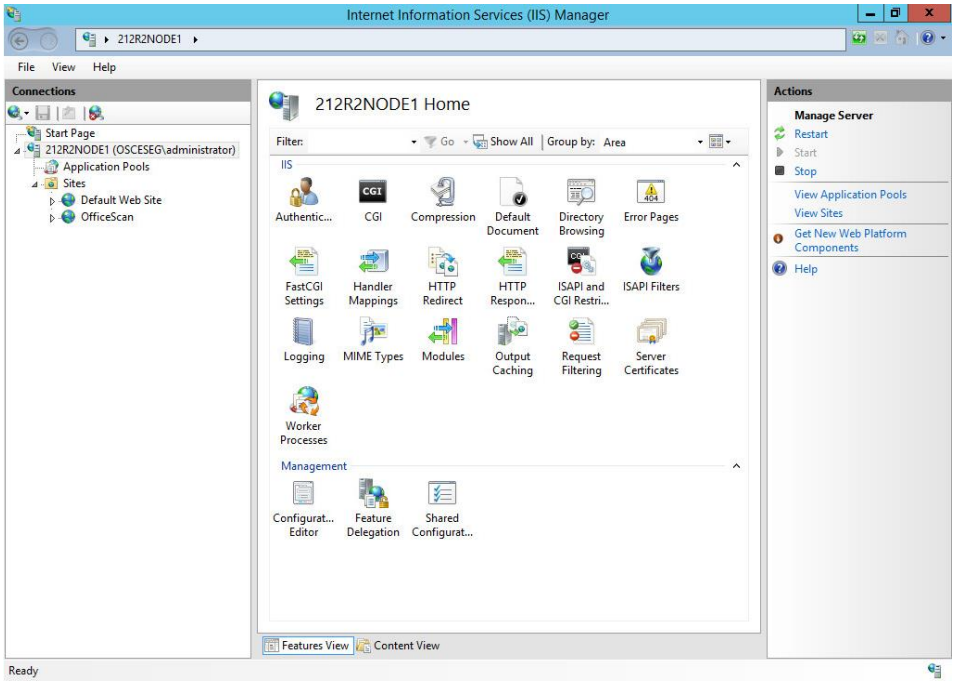

Figure 18. Internet Information Services (IIS) Management

2. In the connections panel, click **Node1 IIS Server**.
3. In the central panel, click **Authentication**.
4. Click **Anonymous Authentication**, and click **Edit** in right panel.

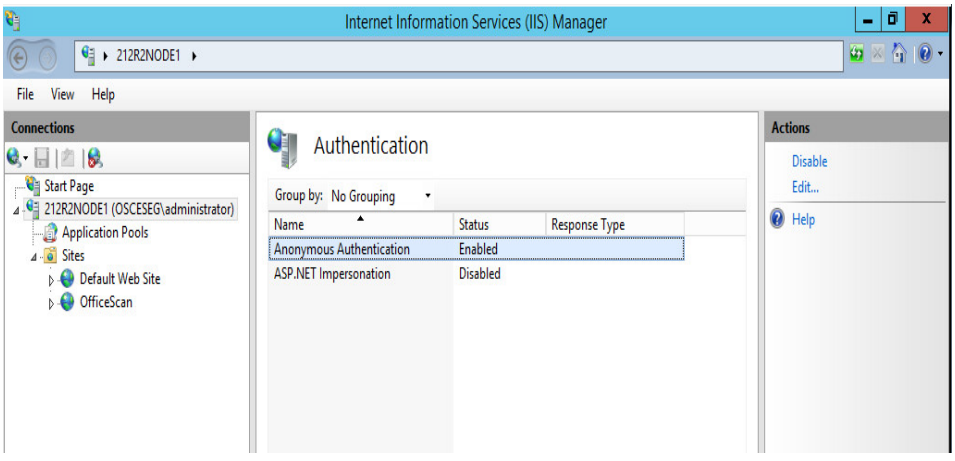

Figure 19. Anonymous Authentication

5. After the **Edit Anonymous Authentication Credentials** window popup, Click **Set** in **Specific user**.

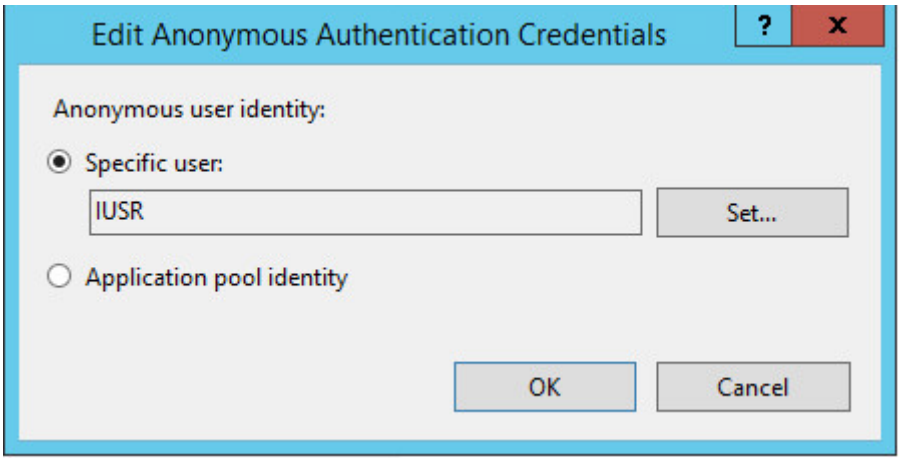

Figure 20. Edit Anonymous Authentication Credential screen

6. Enter domain account and password.

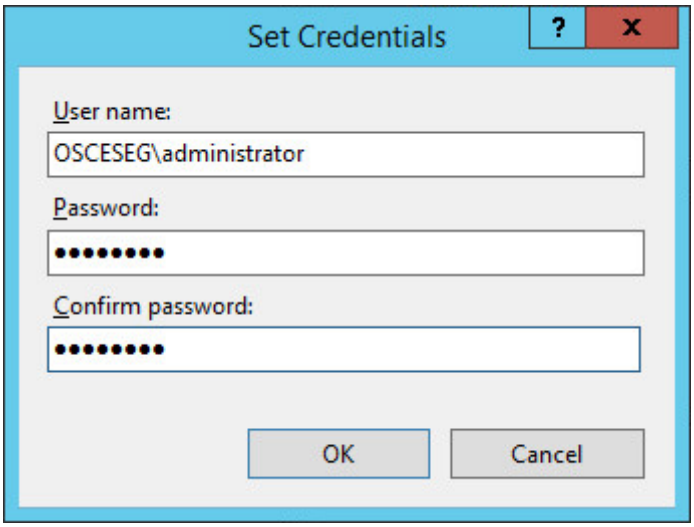

Figure 21. Set Credentials screen

7. Click **Ok**.

4 OfficeScan services startup type

This process must be followed on each node. To configure service startup type：

1. Start Services management from the **Start** screen → **Administrative Tools** → **Services.**

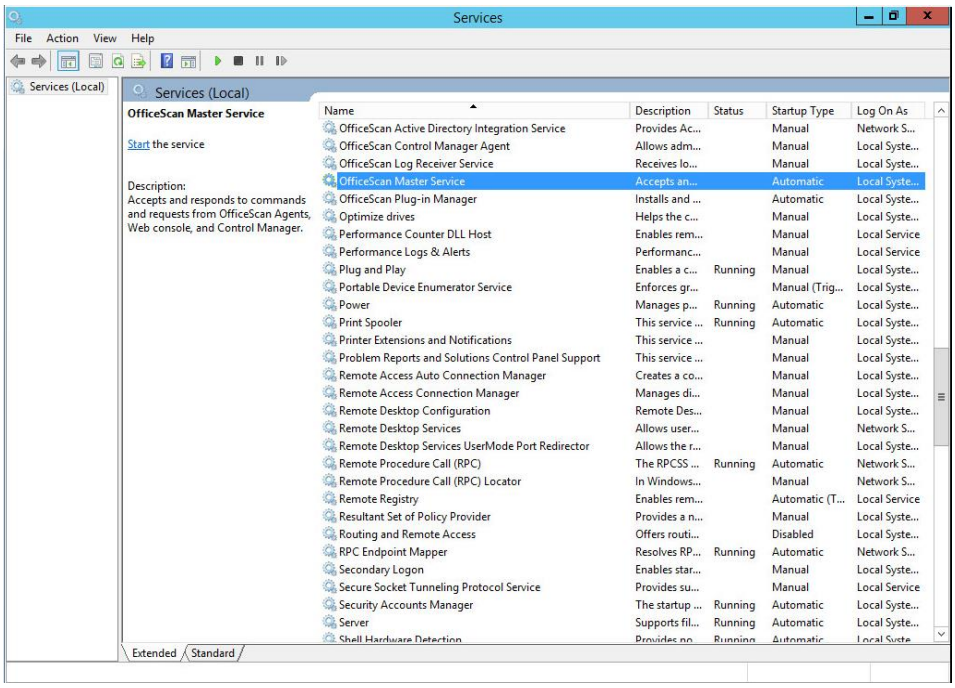

Figure 22. Services Manager

2. Right-click **OfficeScan Master Service**.
3. Click **Properties.**
4. Change **Startup type** to **Manual.**

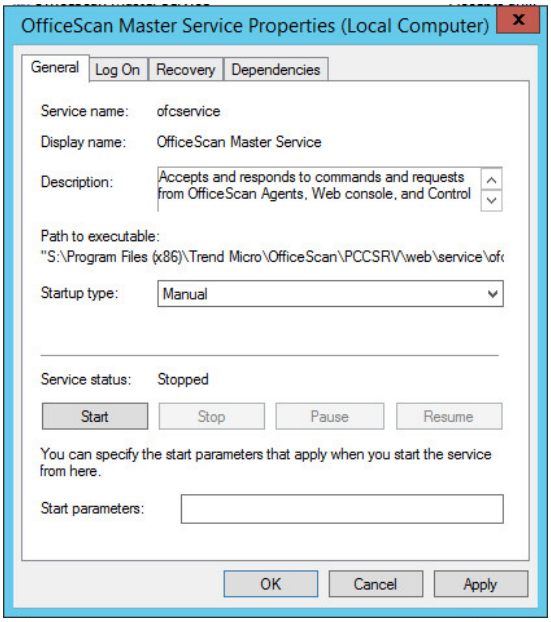

Figure 23. OfficeScan Master Service Properties

5. Click **Apply**, and click **OK.**

5 Creating cluster generic script

This process must be followed on each node. To creating a generic script：

1. Copy the generic script to **C:\Windows\System32\inetsrv**

Note：The script compress with this document, Clusweb7.vbs.

Note：The **site name** and **app pool name** in generic script should be the same with OfficeScan used in IIS manager.

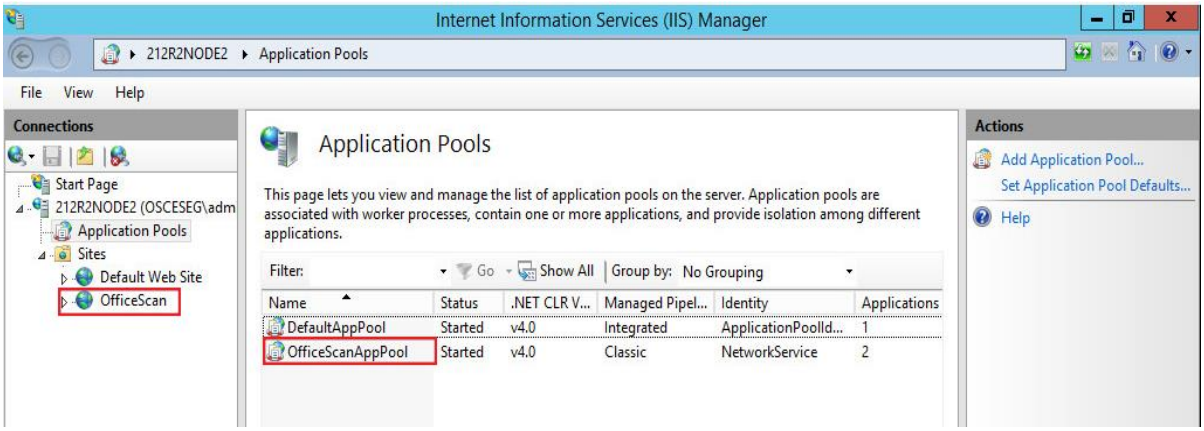

Figure 24. OfficeScan AppPool and web site name in IIS

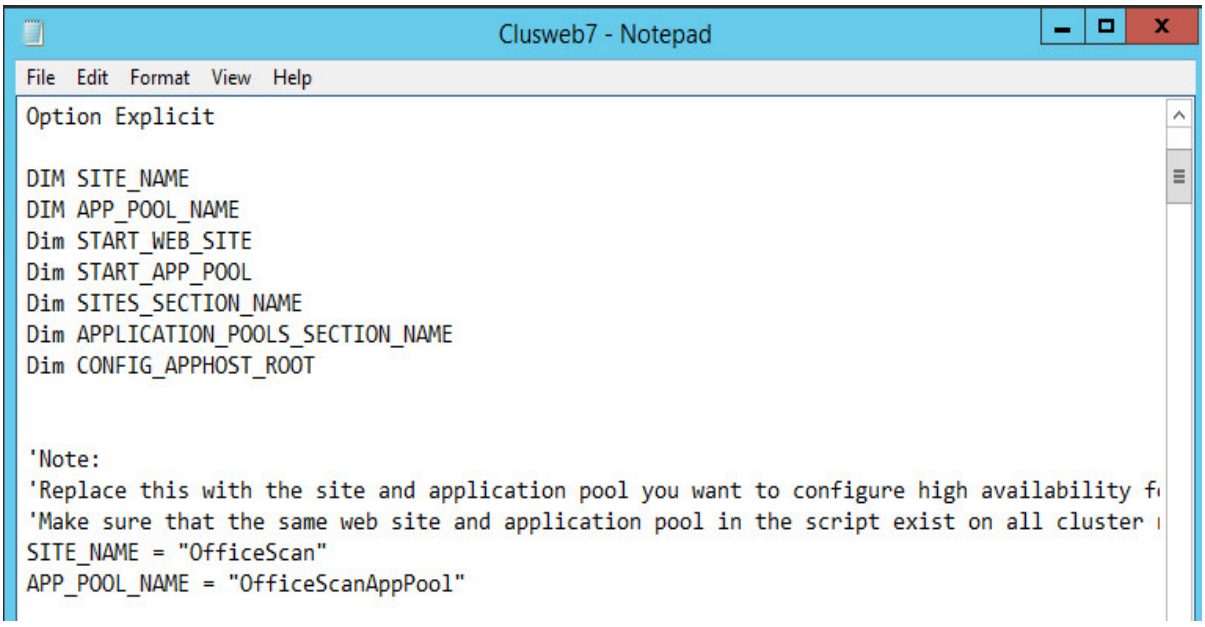

Figure 25. Site name and app pool name in generic script

6 Creating a high availability cluster generic script

1. Start Failover Cluster Manager from the **Start** screen → **Administrative Tools** → **Failover Cluster Manager.**

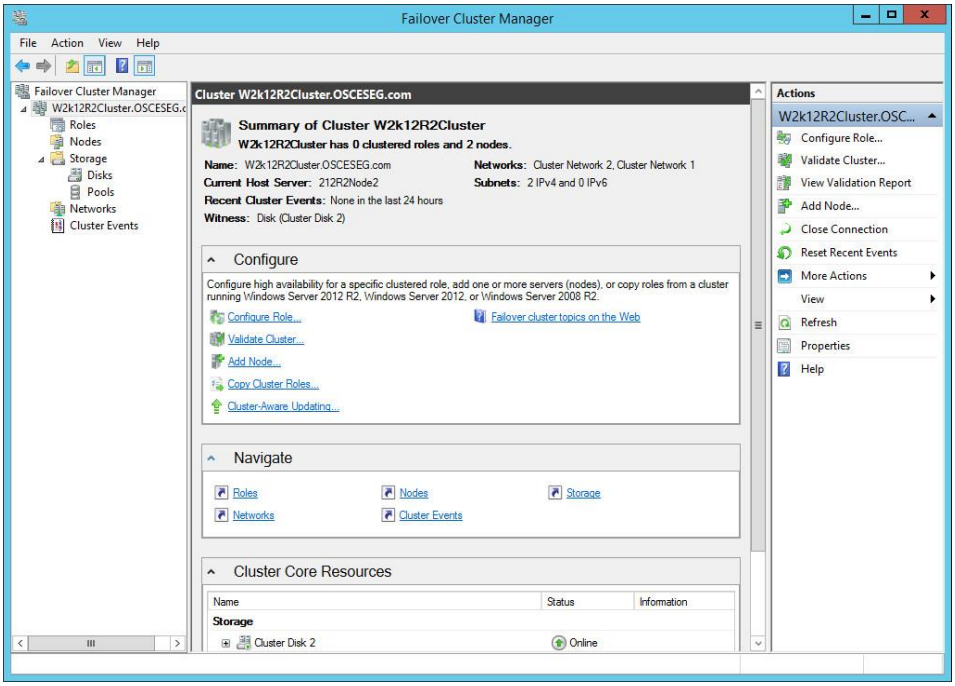

Figure 26. Failover Cluster Manager

2. From **Failover Cluster Manager**, right-click the cluster name, and choose **Configure Role**

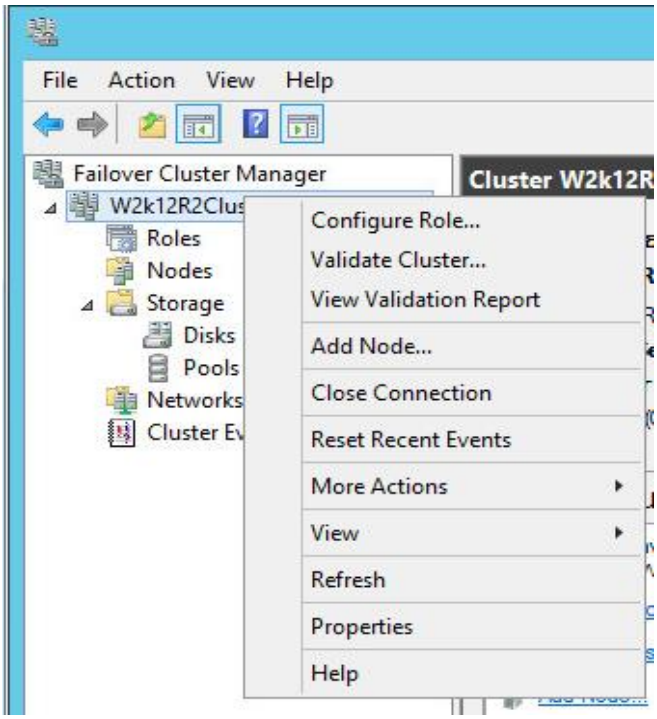

Figure 27. Configure Role

3. Click **Next** on the **Before You Begin** dialog screen of the **High Availability Wizard**.

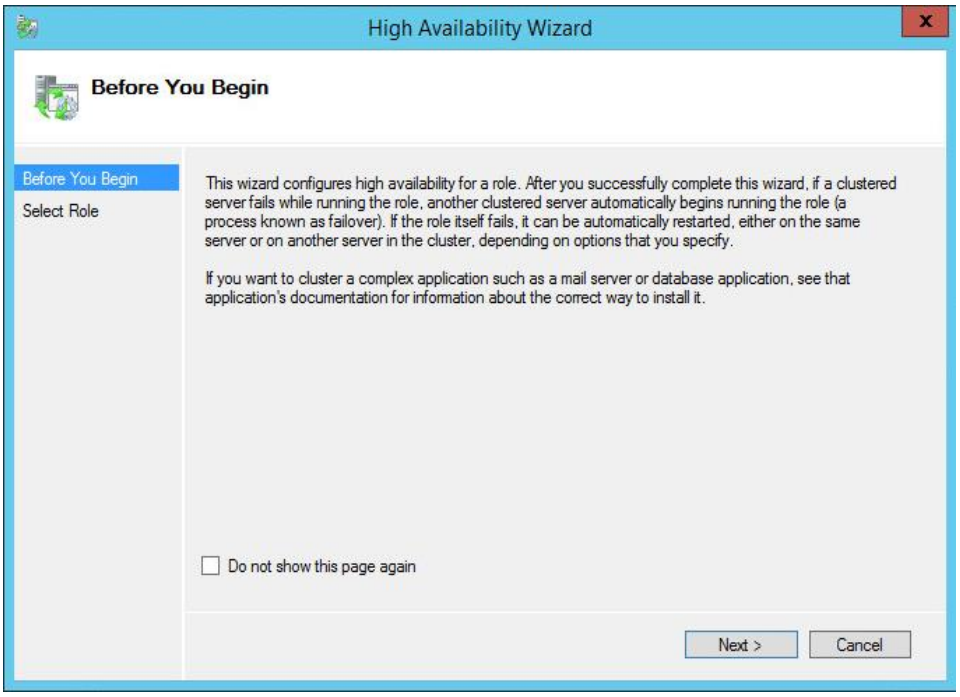

Figure 28. High Available Wizard

4. Select **Generic Script** from the list of available roles. Click **Next**.

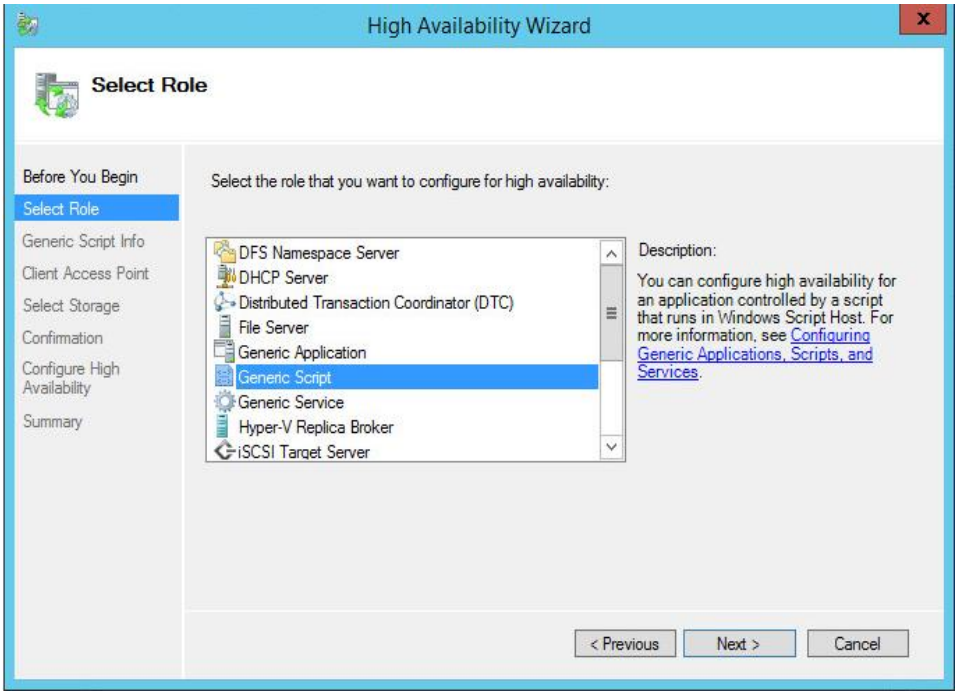

Figure 29. Select Role

5. Enter the generic script path, and click **Next**.

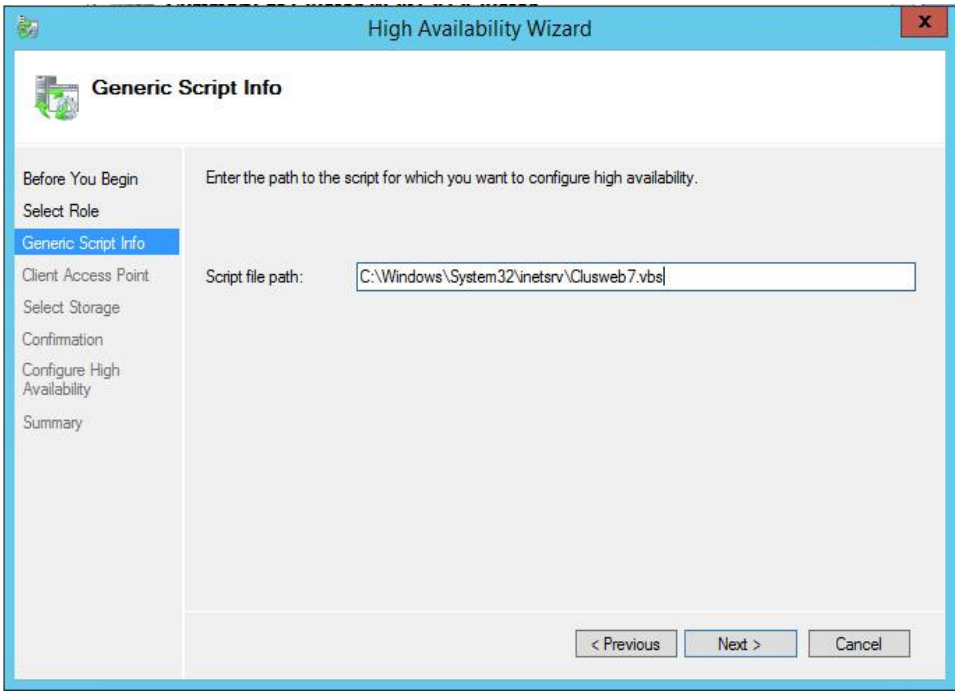

Figure 30. Generic Script Path

6. Enter a name that clients will use to access the cluster role. Enter a unique IP address for the file server. Click **Next**.

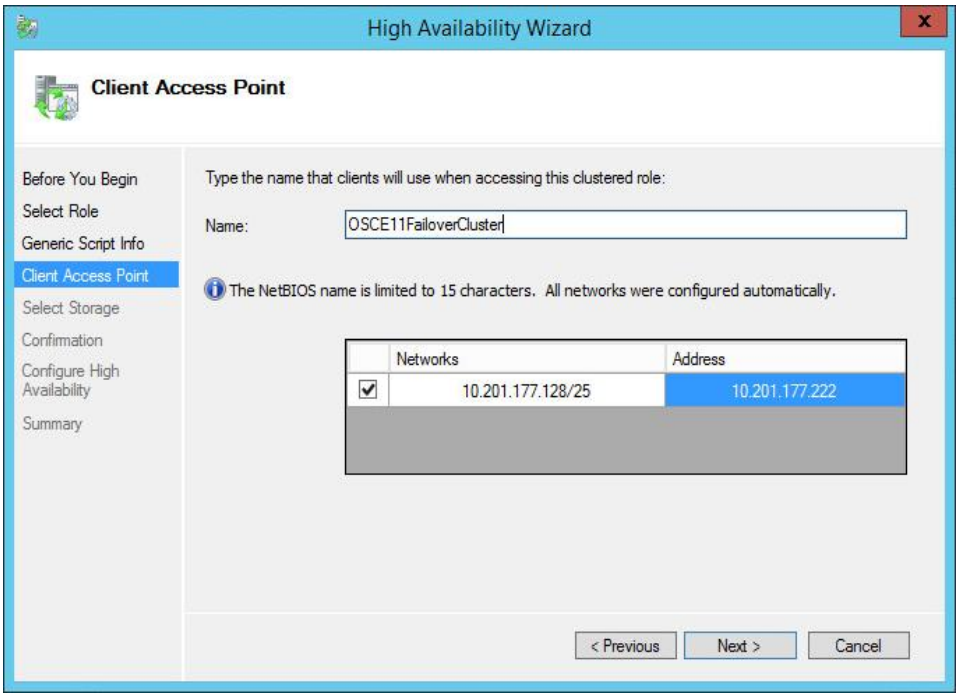

Figure 31. Client Access Point

7. Select the storage volume to assign to the clustered role. Click **Next**.

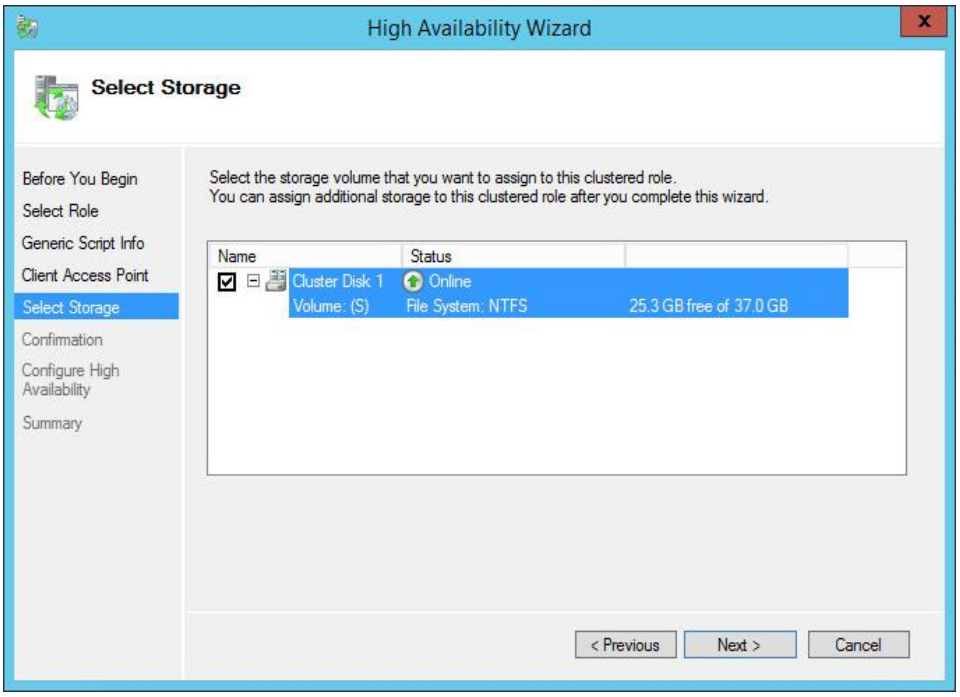

Figure 32. Select Storage

8. Confirm settings and click **Next**.

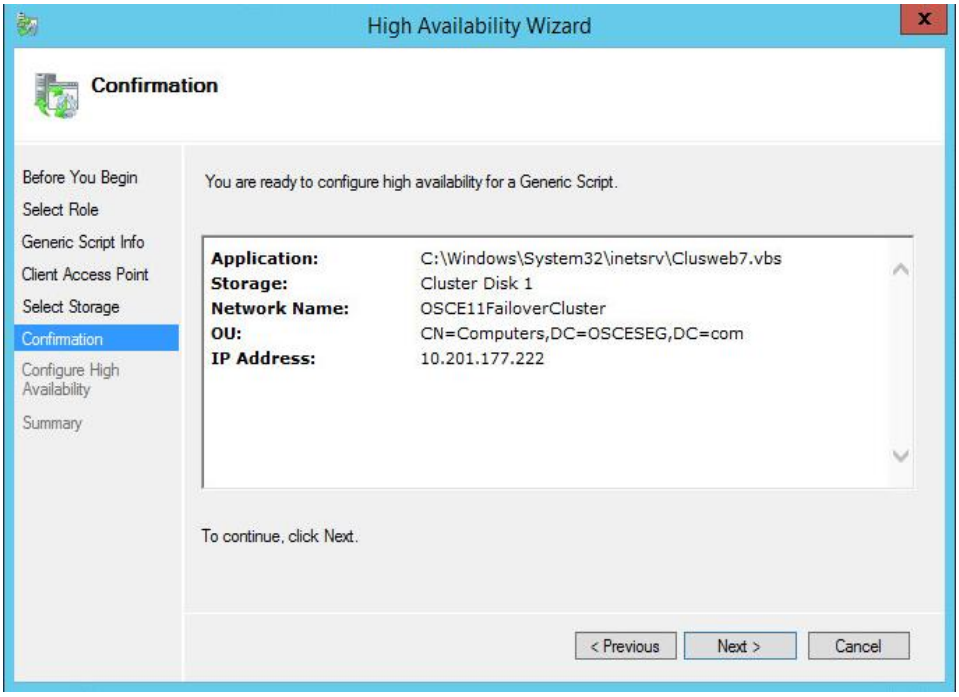

Figure 33. Confirm Settings

9. Click **Finish** on the Summary screen.

7 OfficeScan service role

1. From the **Failover Cluster Manager**, click **Roles**.
2. In the central penal, right-click the role name, and choose **Add Resource** → **Generic Service**.

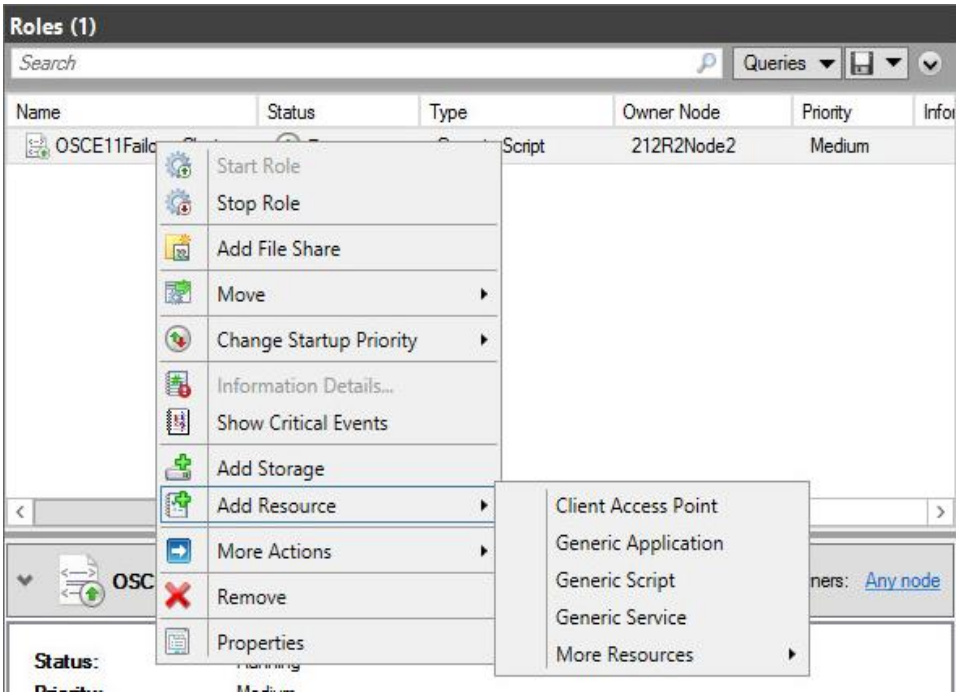

Figure 34. Context Window

3. Select **OfficeScan Master Service**, and click **Next**.

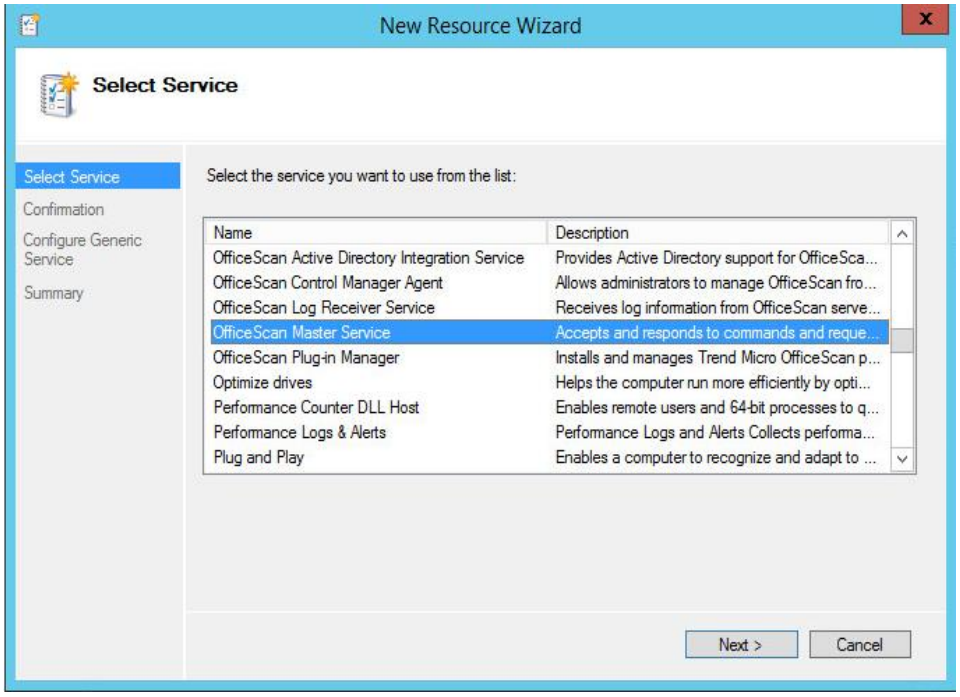

Figure 35. Select Service

4. Confirm the information, and click **Next**.

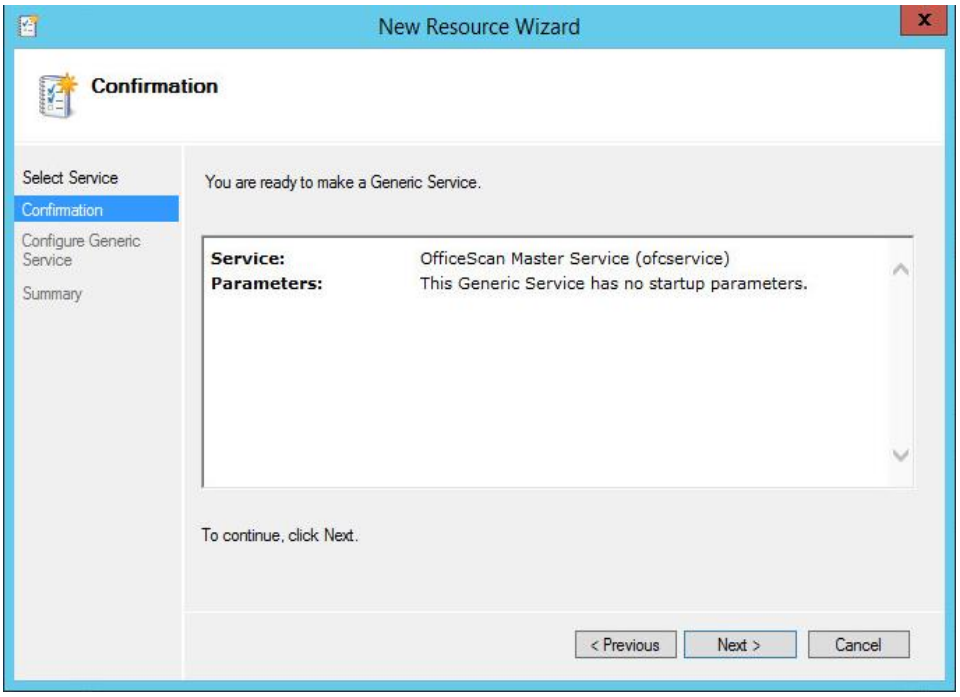

Figure 36. Confirmation Window

5. Click **Finish** on the Summary screen.

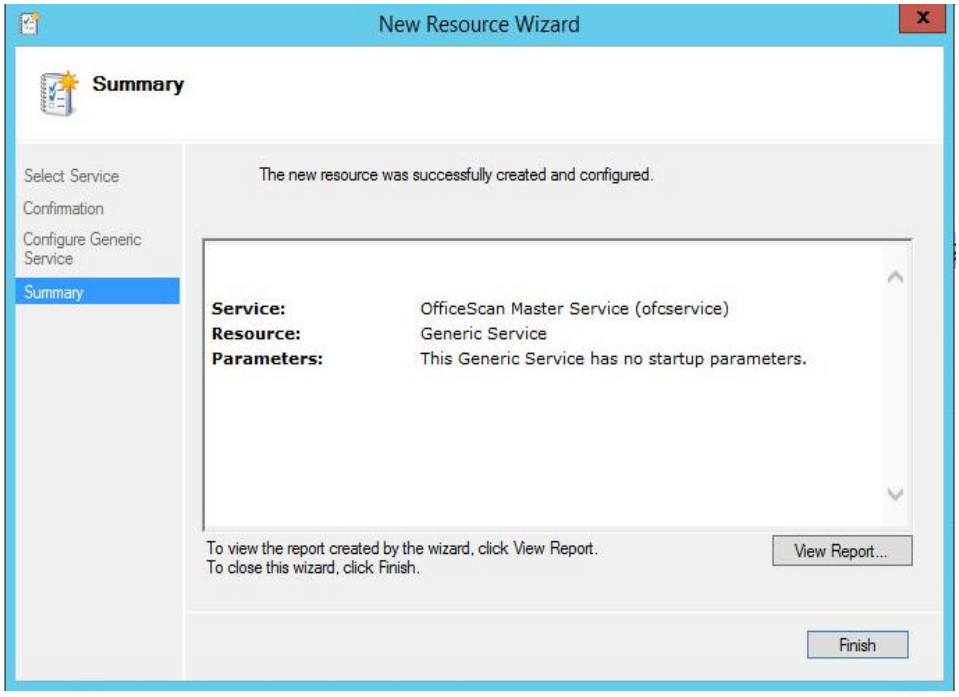

Figure 37. Summary

6. Repeat Step 1 - 5, and add following OfficeScan services.

- OfficeScan Active Directory Integration Service
- OfficeScan Log Receiver Service
- OfficeScan Plug-in Manager

7. Once the service role configuration has completed, the roles will be visible in Failover Cluster Manager.

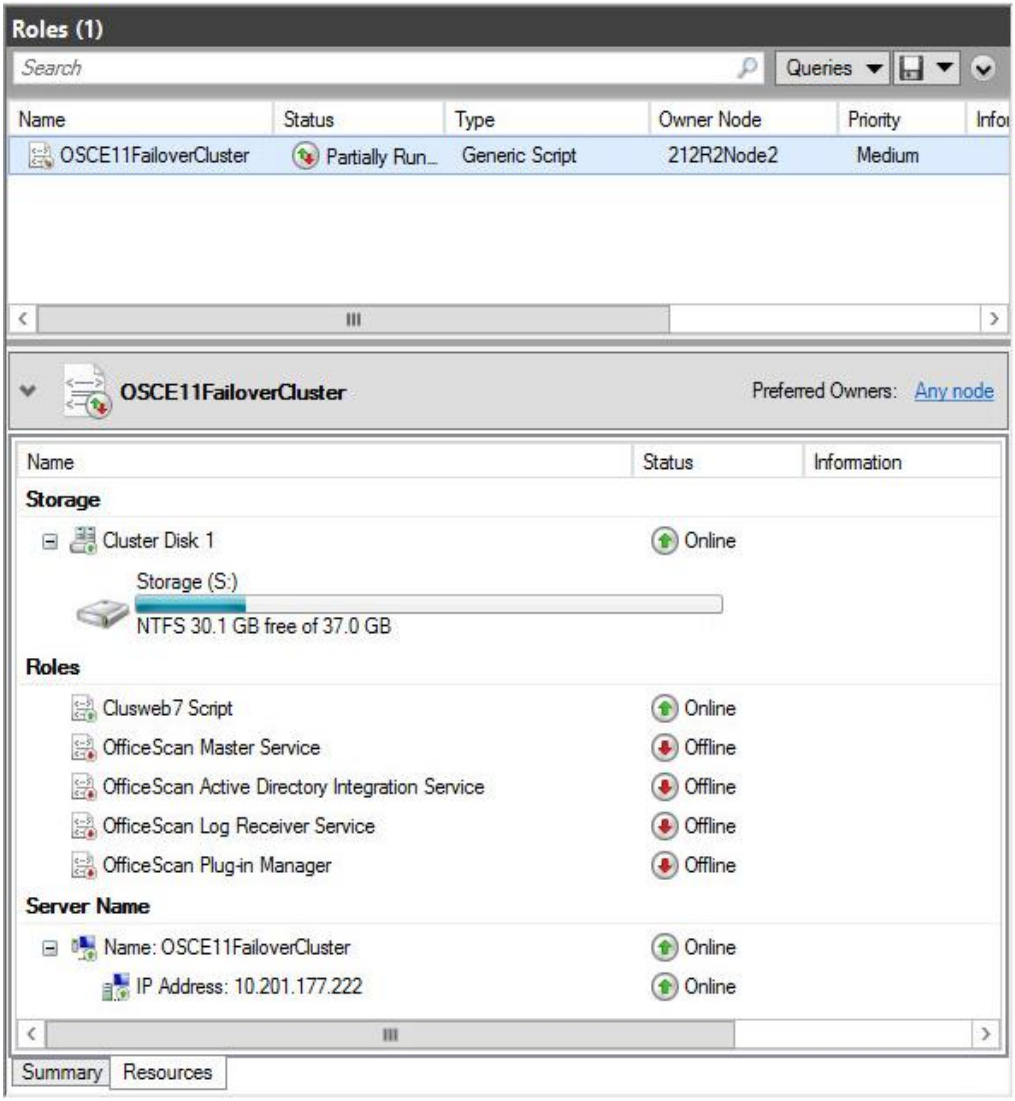

Figure 38. Failover Cluster Roles

7.1 Configuring service role dependencies

1. Right-click **OfficeScan Active Directory Integration Service role**, and choose **Properties**

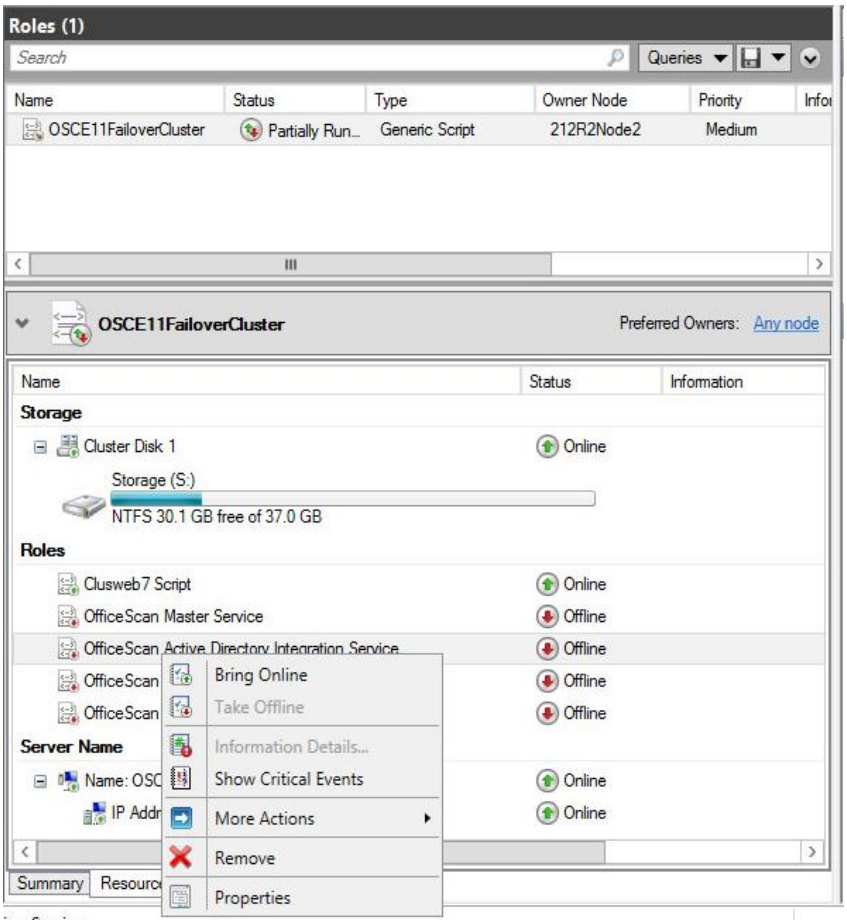

Figure 39. Context Window

2. Click **Dependencies** tab.

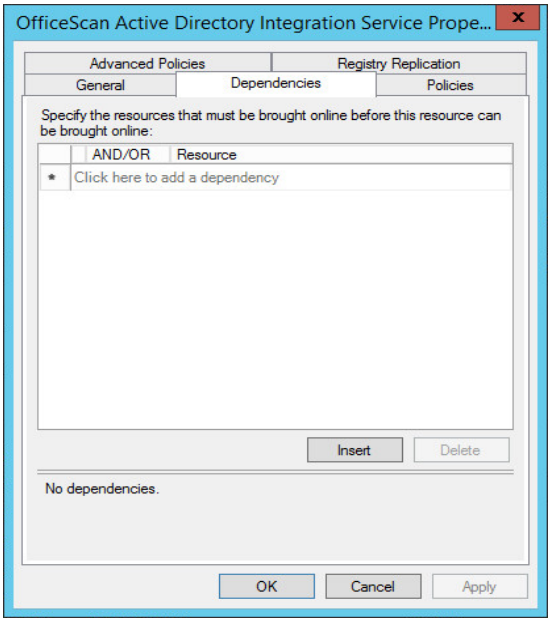

Figure 40. Dependencies Tab

3. Click **Insert**.
4. In the **Resource** column, drop down the option list, and choose **OfficeScan Master Service**.

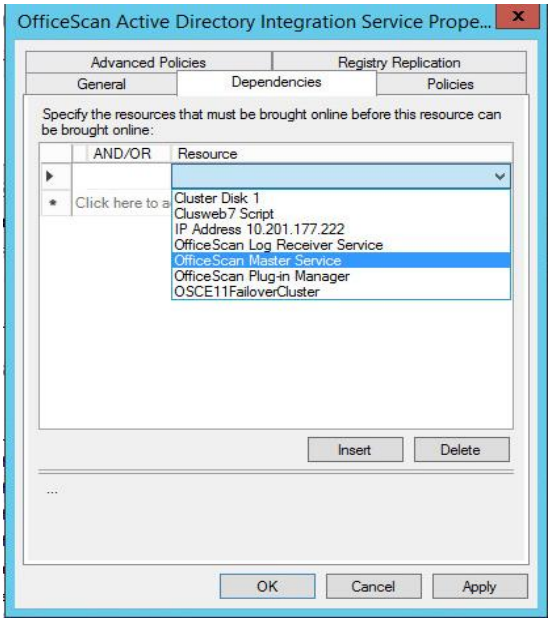

Figure 41. Resource Drop down List

5. Repeat Step 1-4 for following OfficeScan service role.
   - OfficeScan log Receiver Service
   - OfficeScan Plug-in Service

6. Right-click **OfficeScan Master Service role**, and choose **Properties.**
7. Click **Dependencies** tab.
8. Click **Insert**, and insert two column.
9. In the **Resource** column, drop down the first option list, and choose Cluster Storage
10. Drop down the second option list, and choose the cluster name.

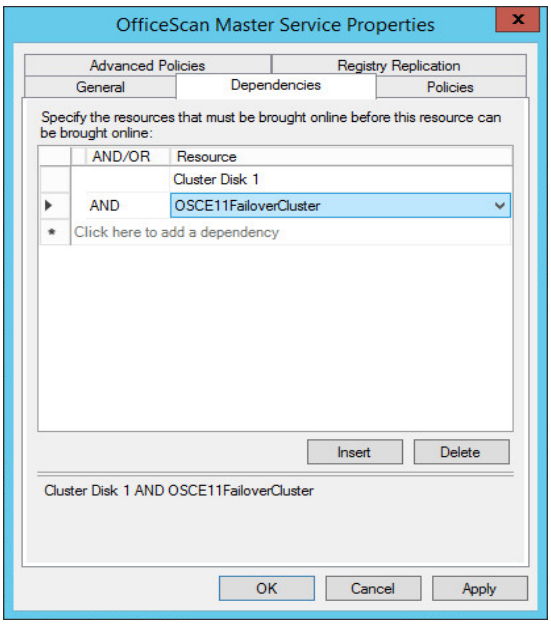

Figure 42. OfficeScan Master Service Dependencies

7.2 OfficeScan server registry replication in cluster

1. Start Windows PowerShell from the **Start** screen → **Administrative Tools** → **Windows PowerShell**
2. Enter following registry replication command
   - Add-ClusterCheckpoint -Cluster <Cluster Name> -RegistryCheckpoint "SOFTWARE\Wow6432Node\TrendMicro\Database Backup" -ResourceName "OfficeScan Master Service"
   - Add-ClusterCheckpoint -Cluster <Cluster Name> -RegistryCheckpoint "SOFTWARE\Wow6432Node\TrendMicro\OfficeScan" -ResourceName "OfficeScan Master Service"
   - Add-ClusterCheckpoint -Cluster <Cluster Name> -RegistryCheckpoint "SOFTWARE\Wow6432Node\TrendMicro\Solar" -ResourceName "OfficeScan Master Service"

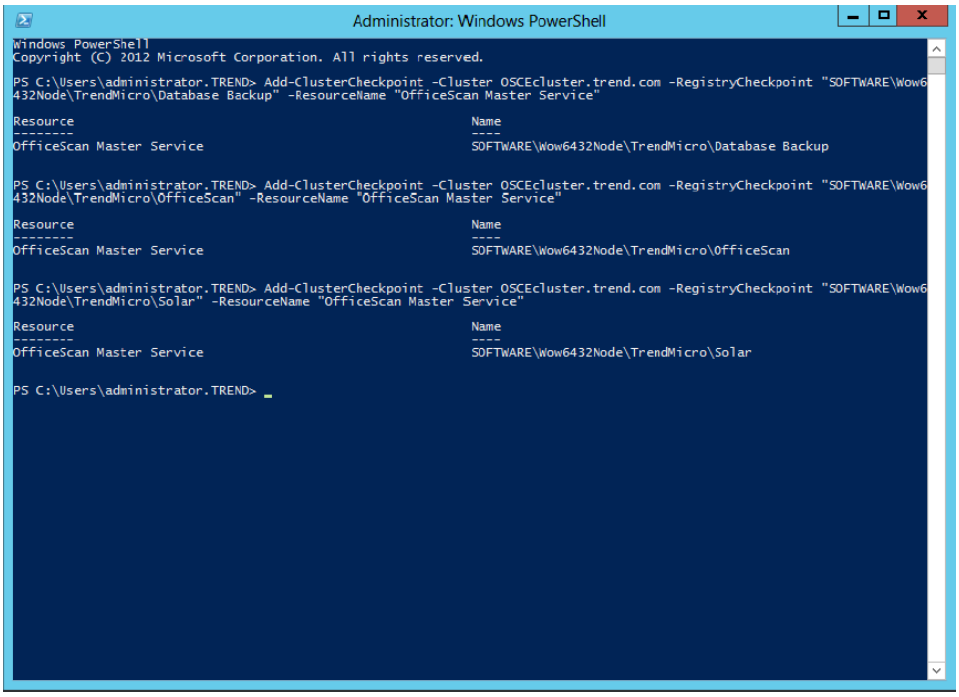

Figure 43. Registry Replication Commands

7.3 Bring OfficeScan service roles online

1. Right-click **OfficeScan Master Service role**, and choose **Bring Online**.
2. Right-click **OfficeScan Active Directory Integration Service role**, and choose **Bring Online**.
3. Right-click **OfficeScan Log Receiver Service role**, and choose **Bring Online**.
4. Right-click **OfficeScan Plug-in Manager role**, and choose **Bring Online**.

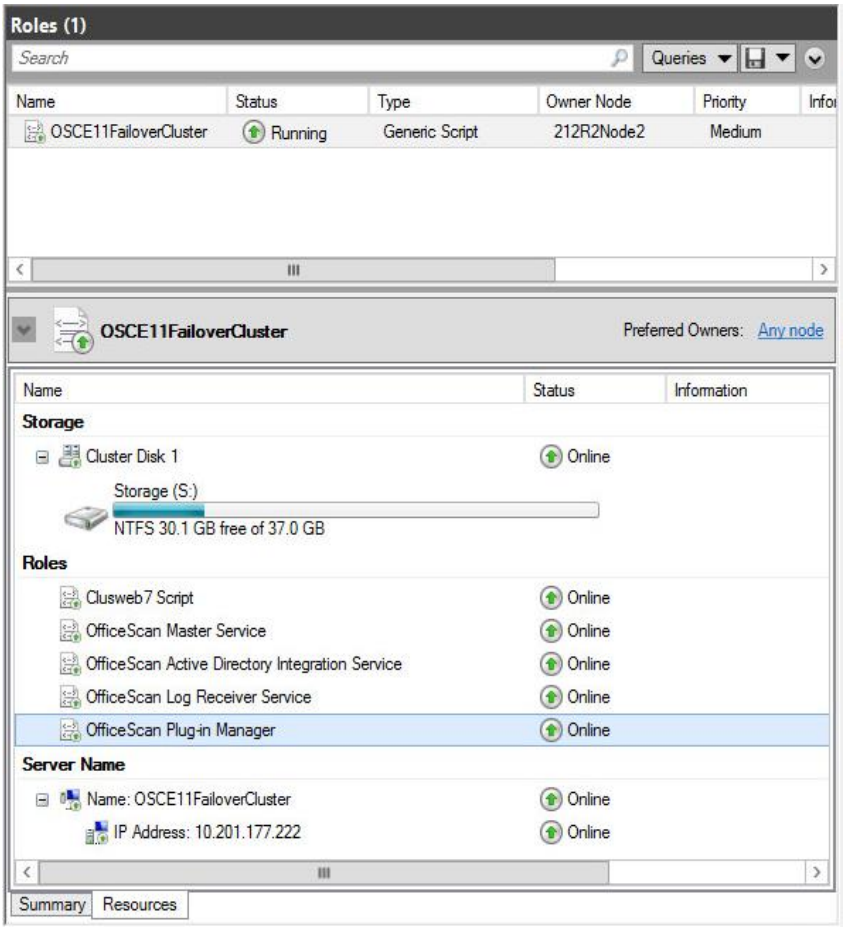

Figure 44. Role Window

8 Provision a shared folder for the OfficeScan cluster role

Note: Cluster nodes must have file server role. You can enable file server role on server manager.

1. Navigate to OfficeScan installation folder
2. Right-click **PCCSRV** folder, and choose **Properties**.
3. Click **Sharing** tab, and click **Advanced Sharing**.
4. Click Add, and enter ofcscan as share name.

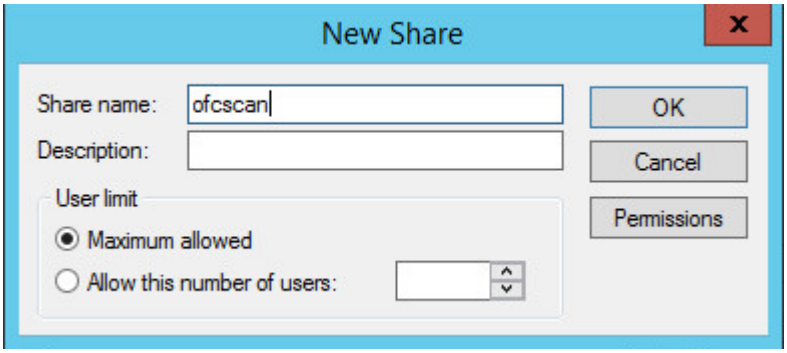

Figure 45. New Share Folder

5. Click **Permissions**.
6. Set permissions for everyone is **Read**

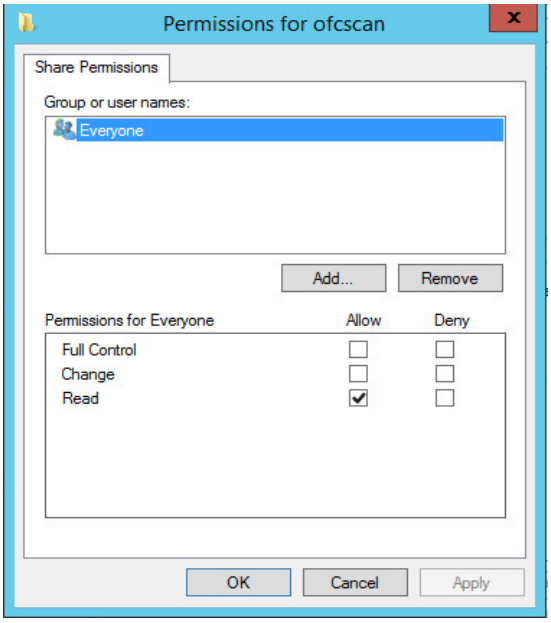

Figure 46. Everyone Permissions

7. Click Add, and add domain administrator account.

8. Set permissions for administrator is **Full Control**.

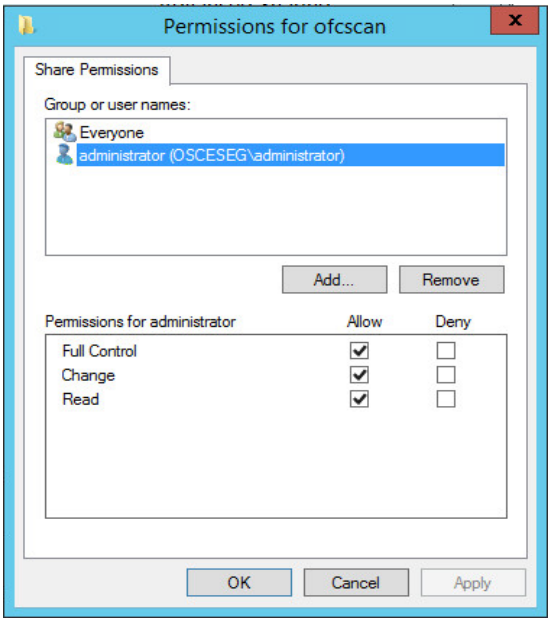

Figure 47. Administrator Permissions

9. Click Apply, and share the folder.
10. From the Failover Cluster Manager, click **Roles**.
11. Click **Shares** tab.
12. Right-click pccsrv share folder, and select **Stop Sharing**.
13. Right-click ofcscan share folder, and select **Properties**.

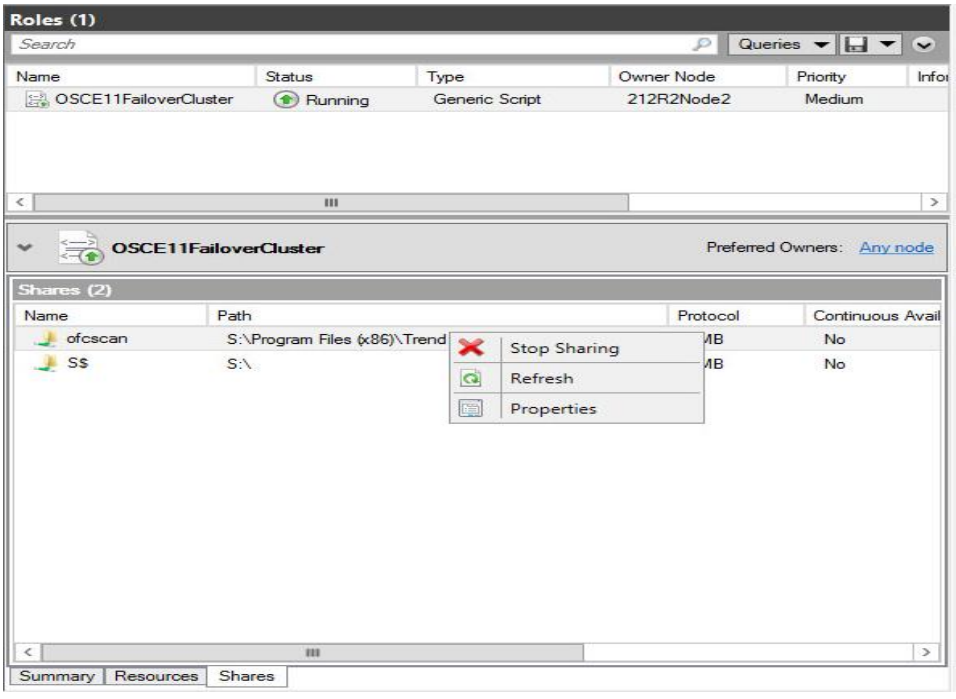

Figure 48. Share Folder Context Window

14. In the left panel, click **Permissions**.

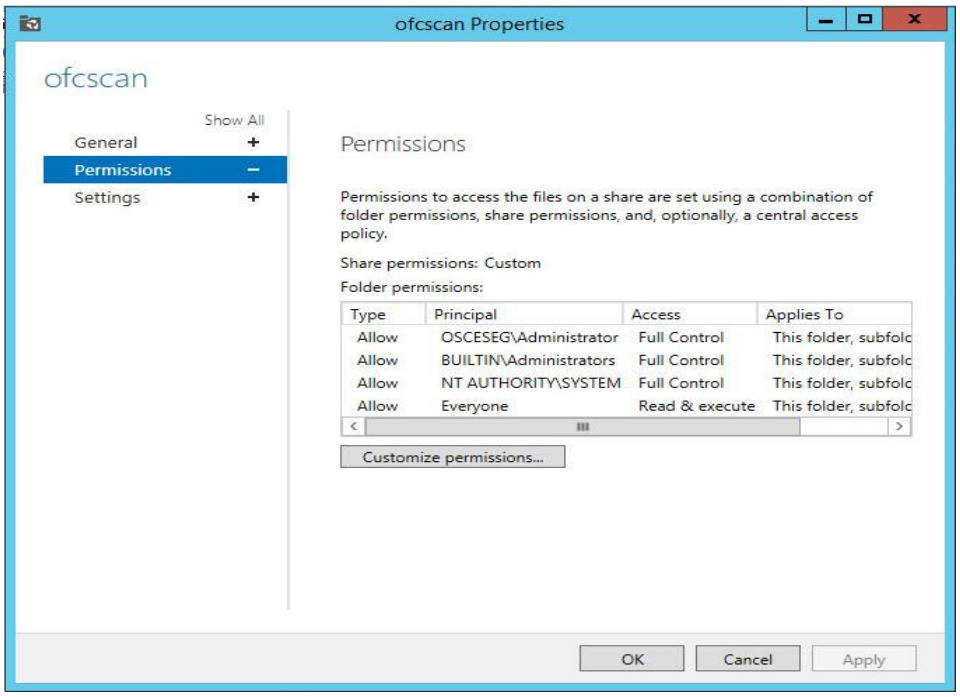

Figure 49. ofcscan share folder properties

15. Click **Customize permissions**.
16. Select Everyone permission, and click **Edit**.

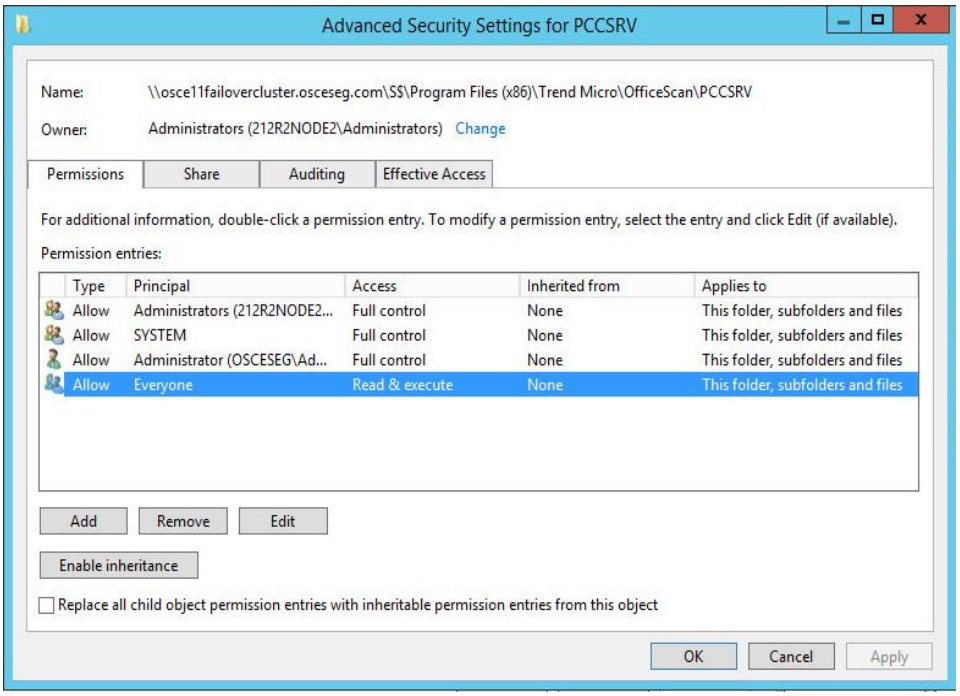

Figure 50. Advanced Security Settings

17. Set only **Read** permission.

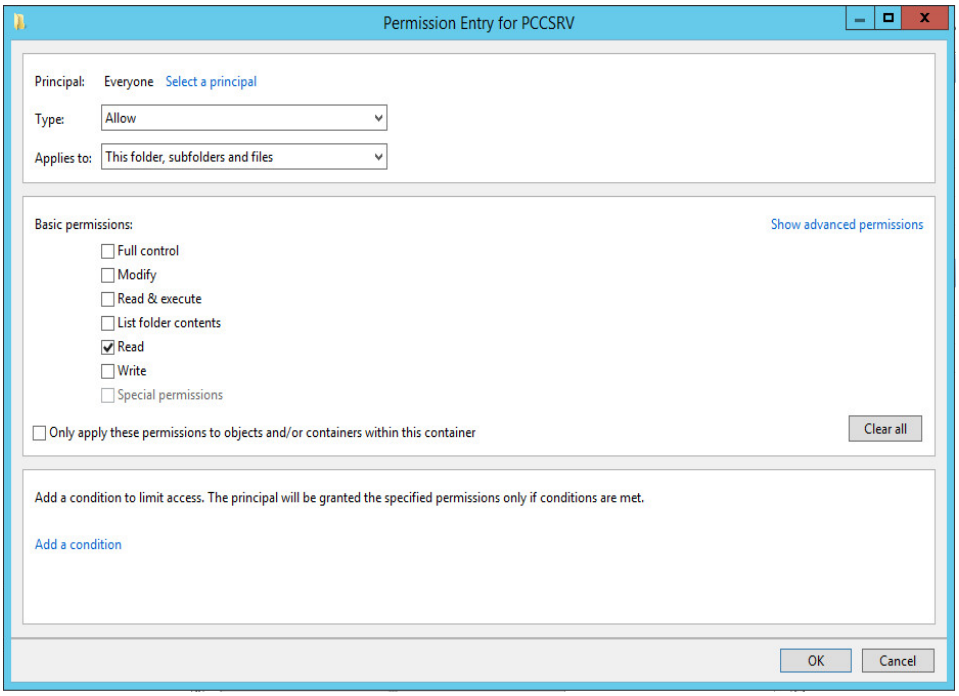

Figure 51. Everyone Permissions

18. Click **OK**.
19. In the Advanced Security Settings page, click **Apply**, and **OK**.
20. In the left penal, click **Settings**.

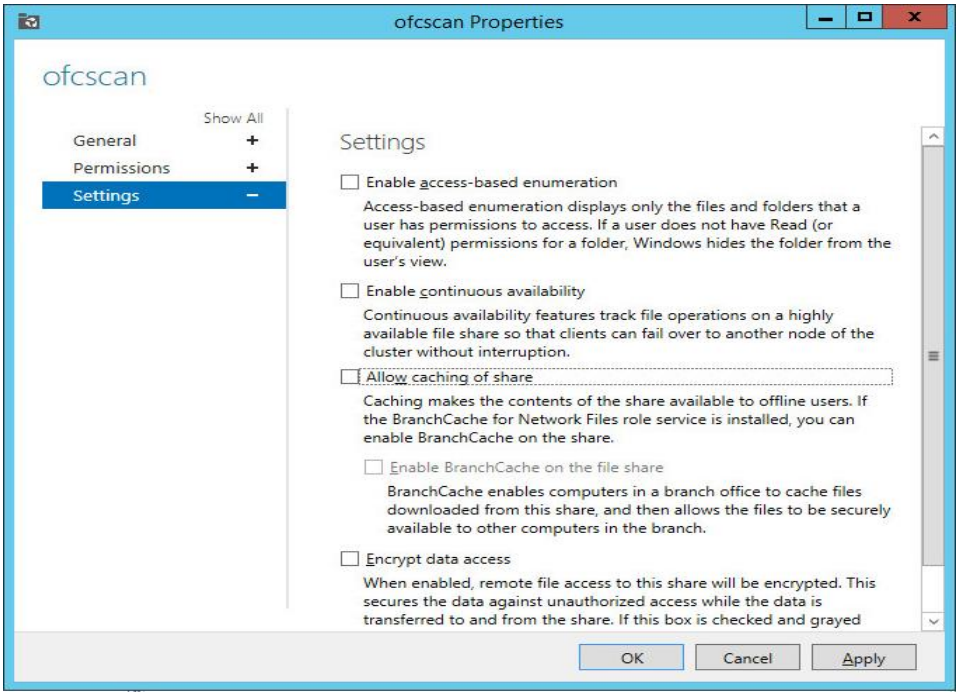

Figure 52. ofcscan Share Folder Settings

21. Disable **Allow caching of share** option.

22. Click **Apply**, and **OK**.

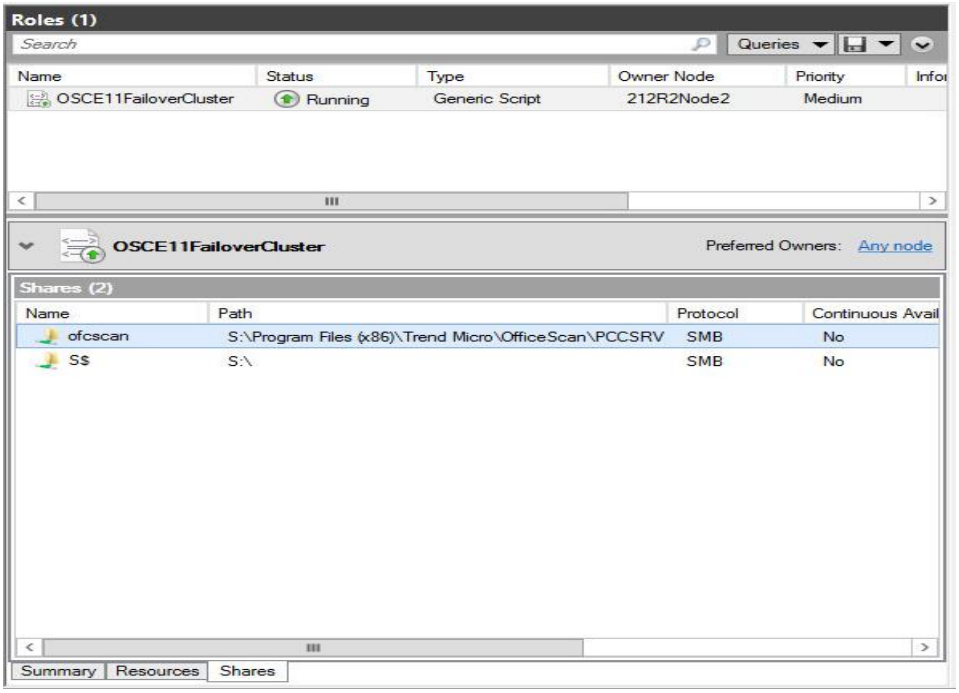

Figure 53. Roles Window

9 OfficeScan Agent configuration for cluster node

In the cluster environment, there will be multiple NICs in each node. There will be a primary cluster NIC for the application communication. The OfficeScan agent is designed to acquire the IP address from the primary NIC for registration to the OfficeScan server. When the node is inactive, the primary IP address will be a private address. In this scenario, the OfficeScan server lose the communication with the agents and the client will go offline.

1. On the OfficeScan server, navigate to installation path.
2. Open and edit ofcscan.ini.
3. Under the [Global Setting] section, add the following keys and assign the valid IP address for the Officescan server.

   IPTemplateDeployEnable=1
   IPTemplateDeploy=<assign_a_valid_IP_address_range_used_to_connect_to_the_officescan_server>

   For example:

   [Global Setting]
   IPTemplateDeployEnable=1
   IPTemplateDeploy0=10.200.10.x
   Note: If some of your agents have 2 or more network cards, set the range to the ones you will be using to connect
   IPTemplateDeploy1=10.210.x.x
   Note: Same for a different range on a different agent
   IPTemplateDeploy2=10.211.10.*
   IPTemplateDeploy3=10.211.30.*
   IPTemplateDeploy4=172.18.x.x
   IPTemplateDeploy5=172.17.x.x
   IPTemplateDeploy6=172.16.x.x
   IPTemplateDeploy7=192.168.50.*
   IPTemplateDeploy8=192.168.30.*
   IPTemplateDeploy9=192.168.10.*

   Note: The x and * symbols are interchangeable. This will deploy the settings on the officescan.ini file to agents within the range defined by those symbols.

4. Save and close the file.
5. Log on to the OfficeScan server management console.

6. Go to **Agents** tab → **Global Agent Settings** and then click **Save** to deploy the settings to the agents. The OfficeScan agent program automatically installs the following registry keys:

   Key: HKLM\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion
   Name: IPTemplateDeployEnable
   Type: REG_DWORD
   Data: 1

   Key: HKLM\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion
   Name: IPTemplateDeploy0 to IPTemplateDeploy9
   Type: REG_SZ
   Data: the assigned IP address