Trend Micro™ OfficeScan (OSCE) 11.0 and XG with Windows 2016

Failover Clustering Guide
and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Copyright © 2017 Trend Micro Incorporated. All rights reserved.

No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations

Released: 28 November 2017
Contents

Chapter 1: Preface ......................................................................................... 7
  1.1 > Audience ....................................................................................... 7
  1.2 > Purpose ......................................................................................... 7

Chapter 2: Installing OfficeScan on Windows Server 2016 Failover Clustering ........................................................................... 8

Chapter 3: Authenticating the IIS server .............................................. 19

Chapter 4: Configuring OfficeScan service startup type .................... 22

Chapter 5: Creating cluster generic script .......................................... 24

Chapter 6: Creating a high availability cluster generic script .............. 25

Chapter 7: Configuring OfficeScan service roles ................................ 30
  7.1 > Configuring service role dependencies ....................................... 34
  7.2 > OfficeScan server registry replication in cluster ............................ 37
  7.3 > Configure OfficeScan server IP ....................................................... 38
  7.4 > Bring OfficeScan service roles online ........................................... 39

Chapter 8: Provisioning a shared folder .............................................. 40

Chapter 9: Configuring OfficeScan agent for cluster node ............... 44
Chapter 1: Preface

1.1 > Audience

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

1.2 > Purpose

This document provides the information and guidelines for OfficeScan 11.0/XG server installation on Windows 2016 Failover Clustering. This document uses OfficeScan XG to demonstrate.
Chapter 2: Installing OfficeScan on Windows Server 2016 Failover Clustering

NOTE † The OfficeScan server only supports Active/Passive clusters.

The following process must be followed on each node.

To install OfficeScan XG on Windows Server 2016 Failover Clustering:

1. Execute the OfficeScan XG installer on Node 1, then click Next.

Figure 1. OfficeScan Setup Program
2. Read the license agreement carefully and accept the license agreement terms to proceed with installation, then click **Next**.

![License Agreement](image1.png)

**Figure 2. License Agreement**

3. Run the setup and install the OfficeScan server on the current endpoint, then click **Next**.

![Installation Destination](image2.png)

**Figure 3. Installation Destination**
4. Choose whether to scan or not to scan the target endpoint, then click **Next**.

![Endpoint Prescan](image)

**Figure 4. Endpoint Prescan**

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

![Installation Path](image)

**Figure 5. Installation Path**
6. You can enable proxy settings on this page and click **Next**.

![Proxy Server](image1)

**Figure 6. Proxy Server**

7. Choose IIS web server and click **Next**.

![Web Server](image2)

**Figure 7. Web Server**
8. Enter a name or IP address that agents use to access the OfficeScan server. Please select arbitrary one and click **Next**. It still has to be reconfigured in later procedure.

![Trend Micro OfficeScan Setup Program](image1)

**Server Identification**

Specify whether OfficeScan agents identify the server by domain name or IP address.

Trend Micro recommends using the IP address when the server uses multiple network cards and using the fully qualified domain name (FQDN) or host name when the IP address is subject to change.

- **Fully qualified domain name (FQDN) or host name:** Win-node1.failover.com
  - Tip: Before proceeding, verify that the domain name is resolvable.
- **IP address:**
  - 192.168.64.52
  - 192.168.64.60
  - fe80::c0f8:b0e8:dc92:6b5e

![InstallShield](image2)

**Figure 8. Server Identification**

**NOTE** Do not use the host name for the server-agent connection.

9. Click **Next** again.
10. Enter the OfficeScan activation code (AC) and click **Next**.

![Trend Micro OfficeScan Setup Program](image)

**Figure 9. Product Activation**

11. Click **Next**.

12. Choose whether to install Integrated Smart Scan Protection Server or not and click **Next**.

![Trend Micro OfficeScan Setup Program](image)

**Figure 10. Install Integrated Smart Protection Server**
13. Choose whether to install the OfficeScan agent on the target endpoint and click **Next**.

![Trend Micro OfficeScan Setup Program](image)

**Figure 11. Install OfficeScan Agent**

**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** again.
15. Choose whether to enable TrendMicro Smart Feedback or not and click Next.

![Smart Protection Network](image)

*The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to deliver proactive protection against the latest threats.*

- **Enable Trend Micro Smart Feedback (recommended)**
  - When enabled, Smart Feedback shares anonymous threat information to the Smart Protection Network for analysis. It is possible to disable Smart Feedback anytime through the product console.
  - Your industry (optional): Not specified

![Administrator Account Password](image)

Specify the passwords for opening the web console or uploading/uninstalling the OfficeScan agent. Passwords prevent unauthorized modification of web console settings or removal of the OfficeScan agent.

- **Web console password:**
  - Account: root
  - Password: [ ]
  - Confirm password: [ ]

- **OfficeScan agent upload and uninstall password:**
  - Password: [ ]
  - Confirm password: [ ]

16. Enter the OfficeScan web console password as well as agents’ unload and uninstall password and click Next.
17. Please input arbitrary port number. The port number will be replaced by last installed node. Click **Next**.

![OfficeScan Agent Installation](image1.png)

**Figure 14. OfficeScan Agent Installation**

18. Click **Next**.

19. Choose whether to enable assessment mode or not and click **Next**.

![Anti-spyware Feature](image2.png)

**Figure 15. Anti-spyware Feature**
20. Click **Next**.

21. Generate a new authentication certificate and enter the password, then click **Next**.

![Server Authentication Certificate](image)

**Figure 16. Server Authentication Certificate**

22. Make sure that the shortcut folder name should be the same on each node, then click **Next**.

![OfficeScan Program Shortcuts](image)

**Figure 17. OfficeScan Program Shortcuts**
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 the following OfficeScan installation folder: Cluster storage disk\Trend Micro\OfficeScan\PCCSRV.

27. Repeat steps 1 to 20 on Node 2.

28. On the Server Authentication Certificate screen, browse and import the existing certificate in cluster storage disk \Trend Micro\OfficeScan\AuthCertBAckup, then enter the password that you set on Node 1. Afterwards, click **Next**.

![Server Authentication Certificate](image)

**Figure 18. Server Authentication Certificate**

29. Click **Next** and process the OfficeScan installation on Node 2.
Chapter 3: Authenticating the IIS server

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

1. Start Internet Information Services (IIS) Manager from the Start > Windows Administrative Tools > Internet Information Services (IIS) Manager.

2. In the Connections panel, click Node 1 IIS Server.

3. In the Central panel, click Authentication.

Figure 19. Internet Information Services (IIS) Management
4. Click **Anonymous Authentication** and then click **Edit** in the right panel.

![Figure 20. Anonymous Authentication](image)

5. After the Edit Anonymous Authentication Credentials window pops up, click **Set** for Specific user.

![Figure 21. Edit Anonymous Authentication Credentials](image)
6. Enter the domain account and password.

![Set Credentials dialog box](image)

Figure 22. Set Credential

7. Click Ok.
Chapter 4: Configuring OfficeScan service startup type

The following process must be followed on each node to configure the service startup type:


   ![Services](image)

   Figure 23. Services

   2. Right-click on OfficeScan Master Service.

   3. Click Properties.
4. Change Startup type to “Manual”.

![OfficeScan Master Service Properties](image)

Figure 24. OfficeScan Master Service Properties

5. Click **Apply**, and then click **OK**.
Chapter 5: Creating cluster generic script

This process must be followed on each node. To create a generic script, save the generic script in Appendix I to Clusweb7.vbs and copy it to C:\Windows\System32\inetsrv.

**NOTE** The site name and AppPool name in generic script should be the same with OfficeScan

---

**Figure 25. OfficeScan AppPool**
Chapter 6: Creating a high availability cluster generic script

To create a high availability cluster generic script:

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

![Configure Role](image)

Figure 27. Configure Role

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

![High Availability Wizard](image)

Figure 28. High Availability Wizard screen
4. Select Generic Script from the list of available roles and click **Next**.

![Select Role]

**Figure 29. Select Role**

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

![Generic Script Info]

**Figure 30. Generic Script Info**
6. Enter the name that clients will use to access the cluster role. Enter a unique IP address, and then click **Next**. It will become OfficeScan server IP.

![Client Access Point](image1)

**Figure 31. Client Access Point**

7. Assign a storage volume to the clustered role and click **Next**.

![Select Storage](image2)

**Figure 32. Select Storage**
8. Confirm the settings and click **Next**.

![High Availability Wizard Confirmation](image)

**Figure 33. Confirm Settings**

9. Click **Finish** on the Summary screen.
Chapter 7: Configuring OfficeScan service roles

To configure OfficeScan service roles:

1. From the Failover Cluster Manager, click Roles.

2. In the Central panel, right-click the role name and choose Add Resource > Generic Service.

Figure 34. Add Resource
3. Select OfficeScan Master Service and click **Next**.

![Select Service](image)

**Figure 35. Select Service**

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

![Confirmation](image)

**Figure 36. Confirmation**
5. Click **Finish** on the Summary screen.

![Summary screen](image)

**Figure 37. Summary**

6. Repeat Steps 1 to 5 and add the 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 the Failover Cluster Manager.

Figure 38. Failover Cluster Roles
7.1 Configuring service role dependencies

To configure service role dependencies:

1. Right-click on the OfficeScan Active Directory Integration Service role and choose Properties.

Figure 39. Properties
2. Go to the Dependencies tab.

![OfficeScan Active Directory Integration Service Properties](image)

**Figure 40. Dependencies**

3. Click **Insert**.

4. In the Resource column, choose OfficeScan Master Service from the dropdown list.

![OfficeScan Active Directory Integration Service Properties](image)

**Figure 41. Resource**
5. Repeat Steps 1 to 4 for following OfficeScan service roles:
   - OfficeScan log Receiver Service
   - OfficeScan Plug-in Service
6. Right-click on the OfficeScan Master Service role and choose Properties.
7. Go to the Dependencies tab.
8. Click Insert and insert two columns.
9. In the Resource column, choose Cluster Storage from the first dropdown list.
10. Choose the cluster name from the second dropdown list.

![OfficeScan Master Service Properties](image)

Figure 42. OfficeScan Master Service Dependencies
7.2 > OfficeScan server registry replication in cluster

To replicate the OfficeScan server registry:


2. Enter following registry replication commands:

   - 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. Windows PowerShell](image.png)
7.3 Configure OfficeScan server IP

The OfficeScan server IP should be the IP setting up from Chapter 6. To configure OfficeScan IP, please follow procedure below:

1. Open the ofcscan.ini under <Server installation folder>\PCCSRV\ using text editor and modify the values of the following lines:

   [INI_SERVER_SECTION]
   MasterDirectory=\%Cluster IP%
   Master_DomainName=\%Cluster IP%

   [Scan Now Configuration]
   MoveDir =HTTP://\%Cluster IP%
   CleanFailedMoveDir =HTTP:// \%Cluster IP%

   [Real Time Scan Configuration]
   MoveDir =HTTP://\%Cluster IP%
   CleanFailedMoveDir =HTTP:// \%Cluster IP%

   [Manual Scan Configuration]
   MoveDir =HTTP://\%Cluster IP%
   CleanFailedMoveDir =HTTP:// \%Cluster IP%

   [Prescheduled Scan Configuration]
   MoveDir =HTTP://\%Cluster IP%
   CleanFailedMoveDir =HTTP:// \%Cluster IP%

2. Open the OfUninst.ini under <Server installation folder>\PCCSRV\ using text editor and modify the values of the following lines:

   [INI_SERVER_UNINST]
   InstallServer=\%Cluster IP%
   MasterDirectory=\%Cluster IP%\ofcscan
   InstallWorkStation=\%Cluster IP%

3. Open the ofcserven.ini under <Server installation folder>\PCCSRV\private\ using text editor and modify the values of the following lines:

   [PRODUCT_INFO]
   OSCE_URL=https://\%Cluster IP%:4343/officescan/default.htm

   [TMCS]
   WSS_URL=https://\%Cluster IP%:4343/tmcss/
   WSS_HTTP_URL=http://\%Cluster IP%:8080/tmcss/

   [LWCS]
   LWCS_HTTP_URL=http://\%Cluster IP%:8080/

4. Open the apricot_config.xml under <Server installation folder>\PCCSRV\SRS\ using text editor and modify the values of the following lines:

   <cert cn>%Cluster IP%</cert cn>
7.4 Bring OfficeScan service roles online

To bring OfficeScan service roles online:

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

Figure 44. Roles
To provision a shared folder for the OfficeScan cluster role:
1. Navigate to OfficeScan installation folder
2. Right-click on the PCCSRV folder and choose Properties.
3. Go to the Sharing tab and click Advanced Sharing.
4. Enable Share this folder.
5. Input “ofcscan” as the Share name.
6. Click Permissions.
7. Set the permissions for everyone to “Read”.

![Figure 46. Everyone Share Permissions](image1)

8. Click **Add** and add a domain administrator account.

9. Set the permissions for administrator to “Full Control”.

![Figure 47. Administrator Share Permissions](image2)
10. Click **Apply** and share the folder.

11. From the Failover Cluster Manager, click **Roles**.

12. Go to the Shares tab.

13. Right-click on the ofcscan share folder and select Properties.

![Failover Cluster Manager](image)

**Figure 48. Share Folder**
14. In the left panel, click **Settings**.

![Settings](image)

**Figure 49. Share Folder Settings**

15. Disable the “Allow caching of share” option.

**NOTE** If an error message shows “The specified object cannot be updated either because the server is not available”, please wait for a while until the service up.

16. Click **Apply** and **OK**.

![Roles](image)

**Figure 50. Roles**
Chapter 9: Configuring OfficeScan agent 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 will lose the communication with the agents and the client will go offline.

To configure the OfficeScan agent for cluster node:

1. On the OfficeScan server, navigate to the installation path.
2. Open and edit ofcscan.ini.
3. Under the [Global Setting] section, add the following keys and assign a 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
   IPTemplateDeploy1=10.210.x.x
   IPTemplateDeploy2=10.211.10.*
   IPTemplateDeploy3=10.211.30.*

**NOTE** If some of your agents have two or more network cards, set the range to the ones you will be using to connect.

   IPTemplateDeploy1=10.210.x.x

**NOTE** It’s the 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 > Global Agent Settings** and click Save to deploy the settings to the agents.

   The OfficeScan agent program will automatically install 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
Appendix I: Clustweb7.vbs

' <begin script sample>

'This script provides high availability for IIS websites
' By default, it monitors the "Default Web Site" and "DefaultAppPool"
' To monitor another web site, change the SITE_NAME below
' To monitor another application pool, change the APP_POOL_NAME below
' More thorough and application-specific health monitoring logic can be added to the script if needed

Option Explicit

Dim SITE_NAME
Dim APP_POOL_NAME
Dim START_WEB_SITE
Dim START_APP_POOL
Dim SITES_SECTION_NAME
Dim APPLICATION_POOLS_SECTION_NAME
Dim CONFIG_APPHOST_ROOT

' Note:
' Replace this with the site and application pool you want to configure high availability for
' Make sure that the same web site and application pool in the script exist on all cluster nodes. Note that the names are case-sensitive.
SITE_NAME = "OfficeScan"
APP_POOL_NAME = "OfficeScanAppPool"

START_WEB_SITE = 0
START_APP_POOL = 0
SITES_SECTION_NAME = "system.applicationHost/sites"
APPLICATION_POOLS_SECTION_NAME = "system.applicationHost/applicationPools"
CONFIG_APPHOST_ROOT = "MACHINE/WEBROOT/APPHOST"

' Helper script functions

' Find the index of the website on this node
Function FindSiteIndex(collection, siteName)
    Dim i
    FindSiteIndex = -1
    For i = 0 To CInt(collection.Count) - 1
        If collection(i).Name = siteName Then
            FindSiteIndex = i
            Exit For
        End If
    Next i
End Function
If collection.Item(i).GetPropertyByName("name").Value = siteName Then
    FindSiteIndex = i
    Exit For
End If
Next
End Function

'Find the index of the application pool on this node
Function FindAppPoolIndex(collection, appPoolName)

    Dim i

    FindAppPoolIndex = -1

    For i = 0 To (CInt(collection.Count) - 1)
        If collection.Item(i).GetPropertyByName("name").Value = appPoolName Then
            FindAppPoolIndex = i
            Exit For
        End If
    Next
End Function

'Get the state of the website
Function GetWebSiteState(adminManager, siteName)

    Dim sitesSection, sitesSectionCollection, siteSection, index, siteMethods, startMethod, executeMethod
    Set sitesSection = adminManager.GetAdminSection(SITES_SECTION_NAME, CONFIG_APPHOST_ROOT)
    Set sitesSectionCollection = sitesSection.Collection

    index = FindSiteIndex(sitesSectionCollection, siteName)
    If index = -1 Then
        GetWebSiteState = -1
    End If

    Set siteSection = sitesSectionCollection(index)

    GetWebSiteState = siteSection.GetPropertyByName("state").Value
End Function

'Get the state of the ApplicationPool
Function GetAppPoolState(adminManager, appPool)

    Dim configSection, index, appPoolState

    set configSection = adminManager.GetAdminSection(APPLICATION_POOLS_SECTION_NAME, CONFIG_APPHOST_ROOT)
    index = FindAppPoolIndex(configSection.Collection, appPool)
If index = -1 Then
    GetAppPoolState = -1
End If

GetAppPoolState = configSection.Collection.Item(index).GetPropertyByName("state").Value
End Function

' Start the w3svc service on this node
Function StartW3SVC()

    Dim objWmiProvider
    Dim objService
    Dim strServiceState

    ' Check to see if the service is running
    set objWmiProvider = GetObject("winmgts:/root/cimv2")
    set objService = objWmiProvider.get("win32_service='w3svc'")
    strServiceState = objService.state

    If ucase(strServiceState) = "RUNNING" Then
        StartW3SVC = True
    Else
        ' If the service is not running, try to start it
        response = objService.StartService()

        ' response = 0 or 10 indicates that the request to start was accepted
        If ( response <> 0 ) and ( response <> 10 ) Then
            StartW3SVC = False
        Else
            StartW3SVC = True
        End If
    End If
End Function

' Start the application pool for the website
Function StartAppPool()

    Dim ahwriter, appPoolsSection, appPoolsCollection, index, appPool, appPoolMethods, startMethod, callStartMethod
    Set ahwriter = CreateObject("Microsoft.ApplicationHost.WritableAdminManager")

    Set appPoolsSection = ahwriter.GetAdminSection(APPLICATION_POOLS_SECTION_NAME, CONFIG_APPHOST_ROOT)
    Set appPoolsCollection = appPoolsSection.Collection

    index = FindAppPoolIndex(appPoolsCollection, APP_POOL_NAME)
    Set appPool = appPoolsCollection.Item(index)

    ' See if it is already started
    If appPool.GetPropertyByName("state").Value = 1 Then
StartAppPool = True
Exit Function
End If

'Try To start the application pool
Set appPoolMethods = appPool.Methods
Set startMethod = appPoolMethods.Item("START_APP_POOL")
Set callStartMethod = startMethod.CreateInstance()
callStartMethod.Execute()

'If started return true, otherwise return false
If appPool.GetPropertyByName("state").Value = 1 Then
  StartAppPool = True
Else
  StartAppPool = False
End If

End Function

'Start the website
Function StartWebSite()

  Dim ahwriter, sitesSection, sitesSectionCollection, siteSection, index, siteMethods, startMethod, executeMethod
  Set ahwriter = CreateObject("Microsoft.ApplicationHost.WritableAdminManager")
  Set sitesSection = ahwriter.GetAdminSection(SITES_SECTION_NAME, CONFIG_APPHOST_ROOT)
  Set sitesSectionCollection = sitesSection.Collection

  index = FindSiteIndex(sitesSectionCollection, SITE_NAME)
  Set siteSection = sitesSectionCollection(index)

  if siteSection.GetPropertyByName("state").Value = 1 Then
    'Site is already started
    StartWebSite = True
    Exit Function
  End If

  'Try to start site
  Set siteMethods = siteSection.Methods
  Set startMethod = siteMethods.Item("START_WEB_SITE")
  Set executeMethod = startMethod.CreateInstance()
  executeMethod.Execute()

  'Check to see if the site started, if not return false
  If siteSection.GetPropertyByName("state").Value = 1 Then
    StartWebSite = True
  Else
    StartWebSite = False
  End If

End Function
'Cluster resource entry points. More details here:  

'Cluster resource Online entry point  
'Make sure the website and the application pool are started  
Function Online()  
  Dim bOnline  
  'Make sure w3svc is started  
  bOnline = StartW3SVC()  
  If bOnline <> True Then  
    Resource.LogInformation "The resource failed to come online 
    because w3svc could not be started."  
    Online = False  
    Exit Function  
  End If  
  'Make sure the application pool is started  
  bOnline = StartAppPool()  
  If bOnline <> True Then  
    Resource.LogInformation "The resource failed to come online 
    because the application pool could not be started."  
    Online = False  
    Exit Function  
  End If  
  'Make sure the website is started  
  bOnline = StartWebSite()  
  If bOnline <> True Then  
    Resource.LogInformation "The resource failed to come online 
    because the web site could not be started."  
    Online = False  
    Exit Function  
  End If  
  Online = true  
End Function  

'Cluster resource offline entry point  
'On offline, do nothing.  
Function Offline()  
  Offline = true  
End Function  

'Cluster resource LooksAlive entry point  
'Check for the health of the website and the application pool  
Function LooksAlive()  
  Dim adminManager, appPoolState, configSection, i, appPoolName,
appPool, index

i = 0
Set adminManager = CreateObject("Microsoft.ApplicationHost.AdminManager")
appPoolState = -1

'Get the state of the website
if GetWebSiteState(adminManager, SITE_NAME) <> 1 Then
    Resource.LogInformation "The resource failed because the " & SITE_NAME & " web site is not started."
    LooksAlive = false
    Exit Function
End If

'Get the state of the Application Pool
if GetAppPoolState(adminManager, APP_POOL_NAME) <> 1 Then
    Resource.LogInformation "The resource failed because Application Pool " & APP_POOL_NAME & " is not started."
    LooksAlive = false
    Exit Function
    end if

' Web site and Application Pool state are valid return true
LooksAlive = true
End Function

'Cluster resource IsAlive entry point
'Do the same health checks as LooksAlive
'If a more thorough than what we do in LooksAlive is required, this should be performed here
Function IsAlive()
    IsAlive = LooksAlive
End Function

'Cluster resource Open entry point
Function Open()
    Open = true
End Function

'Cluster resource Close entry point
Function Close()
    Close = true
End Function

'Cluster resource Terminate entry point
Function Terminate()
    Terminate = true
End Function

'<end script sample>