Improving Fault Tolerance in BizTalk Server by Using a Windows Server Cluster

Microsoft Corporation

Published: May 2009

Author: Trace Young

Summary

Microsoft BizTalk Server inherently provides high availability for the BizTalk application service when a BizTalk group is configured with multiple BizTalk servers. If a BizTalk group is configured with multiple BizTalk servers, high availability for the BizTalk application service is achieved by creating an instance of a BizTalk Host on multiple servers. In this scenario, if one of the host instances fails, host instances on other servers will take over processing duties for the failed host instance. Although this functionality provides high availability for the BizTalk application service, it does not provide high availability for BizTalk Server dependencies and is subject to certain limitations. Windows Server 2008 failover cluster and Windows Server 2003 server cluster provide high availability for services and applications by enabling fault tolerance.

This white paper provides guidance for information technology (IT) professionals on how to use a Windows Server 2008 failover cluster or Windows Server 2003 server cluster to provide high availability for key BizTalk Server components and dependencies.

Microsoft

Copyright

Contents

Improving Fault Tolerance in BizTalk Server by Using a Windows Server Cluster

Product(s): BizTalk Server 2006 and later, Windows Server 2008 (for failover clustering), Windows Server 2003 (for server clustering).

Microsoft BizTalk Server inherently provides high availability for the BizTalk application service when a BizTalk group is configured with multiple BizTalk servers. If a BizTalk group is configured with multiple BizTalk servers, high availability for the BizTalk application service is achieved by creating an instance of a BizTalk Host on multiple servers. In this scenario, if one of the host instances fails, host instances on other servers will take over processing duties for the failed host instance. Although this functionality provides high availability for the BizTalk application service, it does not provide high availability for BizTalk Server dependencies and is subject to certain limitations.

Windows Server 2008 failover cluster and Windows Server 2003 server cluster provide high availability for services and applications by enabling fault tolerance. This white paper describes how to use a Windows Server 2008 failover cluster or Windows Server 2003 server cluster to provide high availability for key BizTalk Server components and dependencies.

This white paper is intended to provide guidance to information technology (IT) professionals on configuring various BizTalk Server components and dependencies in a Windows Server cluster environment. It does not describe how to set up a cluster.

In This White Paper

BizTalk Server Clustering Overview

A Windows Server failover cluster / server cluster consists of two or more computers, each of which houses an identical copy of an application or service to be managed as a Windows Server cluster resource. Each computer configured in the cluster is referred to as a cluster node. Once an application or service is configured as a Windows Server cluster resource, the Cluster service monitors the availability of the resource. If a cluster resource fails on one of the cluster nodes, the Cluster service can start an instance of the resource on another cluster node. This functionality is commonly referred to "failing over" the resource, and provides high availability through fault tolerance.

BizTalk Server supports the use of a Windows Server cluster to configure a BizTalk Host as a Windows Server cluster resource. A Windows Server cluster can also be used to provide high availability for the BizTalk Server Enterprise Single Sign-On (SSO) service and the following BizTalk Server dependencies:

- Microsoft SQL Server 2008, 2005, or 2000

  Note

  Different versions of BizTalk Server support running databases on different versions of SQL Server. For more information see the BizTalk Server 2009 installation and upgrade guides at BizTalk Server 2009 Installation and Upgrade Guides (http://go.microsoft.com/fwlink/?LinkID=128383) and the BizTalk Server 2006 R2 installation and upgrade guides at BizTalk Server 2006 R2 Installation and Upgrade Guides (http://go.microsoft.com/fwlink/?LinkID=81041).
- Microsoft Distributed Transaction Coordinator (MSDTC)
- Message Queuing (MSMQ)
- Windows file system

Planning for Fault Tolerance

The following table lists the components and dependencies of a BizTalk Server environment that can be clustered and the impact on the BizTalk Server environment if the component or dependency fails. You should consider the scope of a potential failure when deciding whether to cluster a component or dependency.

Component or dependency	Scope of failure
SQL Server	**Systemwide** - If SQL Server fails, BizTalk Server will be unable to process documents.
Master secret server	**Systemwide** - If the master secret server fails, BizTalk Server will be unable to process documents.

Component or dependency	Scope of failure
	Note If the master secret server fails, each BizTalk Server computer in the BizTalk group will continue to use a cached in-memory copy of the master secret until the SSO service on that BizTalk Server computer is restarted. If the SSO service is restarted on the BizTalk Server computers, the cached copy of the master secret is released from memory, and the BizTalk Server computers must be able to contact the master secret server to obtain another copy of the master secret. Do not restart the SSO service on the BizTalk Server computer(s) in a group if the master secret server fails, and you want the BizTalk Server computer to continue processing documents.
MSDTC	**Server** - If MSDTC fails, any component on the server that requires transaction support will fail. **Note** Because SQL Server and the master secret server are dependent on MSDTC for transaction support, the scope of the failure will become system wide if the MSDTC on SQL Server or on the master secret server fails. BizTalk Server requires transaction support when communicating with SQL Server and the master secret server during run-time operations.
BizTalk host instance	**Server** - Any components housed in a BizTalk host instance will be unable to participate in document processing if the host instance fails.
Message Queuing (MSMQ)	**Server** - If MSMQ fails, any document processing that is dependent on the MSMQ service, such as the MSMQ adapter, will be halted on the server.

Component or dependency	Scope of failure
File System	**Server** - If the file system fails, any document processing that is dependent on the file system, such as the File adapter, will be halted on the server.

Because a failure of SQL Server or the master secret server can cause a system wide failure, these components are commonly configured as cluster resources to provide fault tolerance.

The following table describes the number of computers that can be used to achieve specific levels of fault tolerance with a Windows Server cluster and BizTalk Server:

Total number of computers	Number of cluster nodes	Level of fault tolerance
2	2 (one Windows Server cluster)	This configuration can provide fault tolerance for all BizTalk Server components and dependencies that can be clustered by creating a two-node cluster that uses an Active/Active model. One or more BizTalk Hosts and the SSO master secret server are configured as cluster resources in the same group on one node. SQL Server is configured as a cluster resource in a different group on the other node. **Note** • This approach is not recommended for the following reasons:
3	2 (one Windows Server cluster)	This configuration is used to provide fault tolerance for SQL Server and the SSO master secret server. SQL Server and the SSO master secret server are configured as cluster resources on a two-node cluster that uses an Active/Passive model. BizTalk Server is installed and configured on a stand-alone computer. This

Total number of computers	Number of cluster nodes	Level of fault tolerance
		configuration is recommended as the minimum number of computers to provide fault tolerance in a BizTalk Server environment. This configuration does not provide fault tolerance for the BizTalk Hosts.
4 or more	4 or more (two Windows Server clusters)	This configuration can provide fault tolerance for all BizTalk components and dependencies that can be clustered by creating two multiple-node clusters and using an Active/Passive model for each cluster. SQL Server and the SSO master secret server are run on one cluster. BizTalk Server is run on the other cluster. This configuration is recommended as the minimum number of computers to provide fault tolerance for SQL Server, SSO, and BizTalk Hosts in a BizTalk Server environment.

For an overview of Windows Server 2008 failover clustering see Failover Clustering (http://go.microsoft.com/fwlink/?LinkId=135623).

For more information about Windows Server 2003 clustering technologies, see Windows Server 2003 R2 Enterprise Edition – Server Cluster (http://go.microsoft.com/fwlink/?LinkId=65096).

For information about the new functionality provided with Windows Server 2008 failover clustering, see Introducing Windows Server 2008 Failover Clustering (http://go.microsoft.com/fwlink/?LinkId=135622).

Using a Windows Server Cluster to Provide High Availability for BizTalk Server Dependencies

You can use Windows Server clustering to provide high availability for BizTalk Hosts and several BizTalk Server dependencies. This section discusses the BizTalk Server dependencies that can

be clustered and the steps that you can follow to configure the dependencies as cluster resources.

How to Create a Cluster Group with a Disk, IP Address, and Name Resource

For clustered BizTalk Server components and dependencies to be accessible over the network via NetBIOS, a clustered **Network Name** resource must be created in same cluster group. For a clustered Network Name resource to be accessible via the TCP/IP protocol, an **IP Address** resource must be created in the same cluster group as well. Some BizTalk Server dependencies also require the use of a clustered **Physical Disk** resource to function correctly. To create a cluster group with a **Physical Disk**, **IP Address** and **Network Name** resource follow these steps:

Procedures

To create a service or application with a Physical Disk, IP Address, and Network Name resource (Windows Server 2008)

1. In Windows Server 2008, click **Start**, **Programs**, **Administrative Tools**, and then **Failover Cluster Management** to start the Failover Cluster Management program.
2. Fail over all services and applications to the cluster node that you are running Failover Cluster Management on. To fail over a service or application, right click the service or application in the left pane of Failover Cluster Management, point to **Move this service or application to another node** and click to select the destination node.

   Note

   The cluster node that hosts running cluster resources is also known as the **active** node. The cluster node that hosts non-running cluster resources is also known as the **passive** node.
3. In the left-hand pane, right-click **Services and Applications**, click **Configure a Service or Application** to launch the High Availability Wizard, and then click **Next**.
4. Click to select **File Server** and click **Next**.

   Note

   Selecting **File Server** at this point is done as a straightforward way to create a cluster group with a disk resource.
5. On the **Client Access Point** page of the High Availability Wizard enter a unique network name into the **Name** box, for example *BizTalkCluster*, enter an available IP address under **Address**, and then click **Next**.
6. On the **Select Storage** page, click to select an available disk resource and then click **Next**.

7. On the **Confirmation** page click **Next** to create the cluster group.
8. On the **Summary** page click **Finish**.

To create a cluster group with a Physical Disk, IP Address, and Network Name resource (Windows Server 2003)

1. In Windows Server 2003 click **Start**, **Programs**, **Administrative Tools**, and then **Cluster Administrator** to start the Cluster Administrator program.
2. Fail over all cluster groups to the cluster node that you are running the Cluster Administrator on. To fail over a cluster group, right click the group in the left pane of the Cluster Administrator and select **Move Group**.

   Note

   The cluster node that hosts running cluster resources is also known as the **active** node. The cluster node that hosts non-running cluster resources is also known as the **passive** node.
3. On the **File** menu, point to **New**, and then click **Group**.
4. Enter a value for the **Name** field of the **New Group** dialog, for example, **BizTalkClusterGroup** and click **Next**.
5. In the **Preferred Owners** dialog include each cluster node as a possible owner of the group and click **Finish**.
6. Click **OK** on the dialog box that indicates that the cluster group was created successfully.
7. Click to select the new cluster group in the left pane of the Cluster Administrator.
8. Add a **Physical Disk** resource to the group by following these steps:
   a. On the **File** menu, point to **New** and then click **Resource**.
   b. Enter a value for the **Name** field of the **New Resource** dialog, for example, **BizTalkDisk**.
   c. In the **Resource type** dropdown, click **Physical Disk** and click **Next**.
   d. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the Physical Disk resource and click **Next**.
   e. In the **Dependencies** dialog box click **Next**.
   f. Select an available disk from the **Disk** dropdown and click **Finish**.
9. Add an **IP Address** resource to the group by following these steps:
   a. On the **File** menu, point to **New** and then click **Resource**.
   b. Enter a value for the **Name** field of the **New Resource** dialog, for example, **BizTalkIPAddress**.
   c. In the **Resource type** dropdown, click **IP Address** and click **Next**.
   d. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the IP Address resource and click **Next**.
   e. In the **Dependencies** dialog box click **Next**.

f. In the **TCP/IP Address Parameters** dialog enter a valid IP address and subnet mask. For a valid IP address to use for the new IP address resource, contact your network administrator.

g. In the **Network** dropdown select the Public network assigned to the cluster.

h. Check the box to **Enable NetBIOS for the address** and click **Finish**.

i. Click **OK** on the dialog box that indicates that the cluster resource was created successfully.

10. Add a **Network Name** resource to the group by following these steps:

a. On the **File** menu, point to **New**, and then click **Resource**.

b. Enter a value for the **Name** field of the **New Resource** dialog, for example, **BizTalkNetworkName**.

c. In the **Resource type** dropdown, click **Network Name** and click **Next**.

d. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the IP Address resource and click **Next**.

e. In the **Dependencies** dialog box add the IP address resource that you created earlier and click **Next**.

f. Enter a unique network name into the **Name** box, for example *BizTalkCluster*.

g. Click **Finish** and click **OK** on the dialog box that indicates that the cluster resource was created successfully.

How to Cluster MSDTC

Many BizTalk Server operations are performed within the scope of a Microsoft Distributed Transaction Coordinator (MSDTC) transaction.

A clustered MSDTC resource must be available on the Windows Server cluster to provide transaction services for any clustered BizTalk Server components or dependencies. BizTalk Server components or dependencies that can be configured as Windows Server cluster resources include the following:

- BizTalk Host
- Enterprise Single Sign-On (SSO) service
- SQL Server instance
- Message Queuing (MSMQ) service
- Windows File system

Windows Server 2003 only supports running MSDTC on cluster nodes as a clustered resource. For more information see Microsoft Knowledge Base article 305742 "You may receive error messages when you start MSDTC on a node of a cluster server" (http://go.microsoft.com/fwlink/?LinkId=152648).

Windows Server 2008 supports running a local DTC on any server node in the failover cluster; even if a default clustered DTC resource is configured. For more information about implementing MS DTC resources in Windows Server 2008 failover clusters see Understanding MS DTC Resources in Windows Server 2008 Failover Clusters (http://go.microsoft.com/fwlink/?LinkId=152901).

Procedures

To configure the Distributed Transaction Coordinator (DTC) for high availability (Windows Server 2008)

1. To start the Failover Cluster Management program, click **Start**, **Programs**, **Administrative Tools**, and then click **Failover Cluster Management**.
2. In the left hand pane, right-click **Failover Cluster Management**, and then click **Manage a Cluster**.
3. In the **Select a cluster to manage** dialog box, enter the cluster to be managed, and then click **OK**.
4. To start the High Availability Wizard, in the left pane click to expand the cluster, right-click **Services and Applications**, and then click **Configure a Service or Application**.
5. If the **Before You Begin** page of the High Availability Wizard is displayed, click **Next**.
6. On the **Select Service or Application** page, click **Distributed Transaction Coordinator**, and then click **Next**.
7. On the **Client Access Point** page, enter a value for **Name**, enter an available IP address under **Address**, and then click **Next**.
8. On the **Select Storage** page, click to select a disk resource and then click **Next**.
9. On the **Confirmation** page, click **Next**.
10. On the **Summary** page, click **Finish**.

To add an MSDTC resource to an existing cluster group (Windows Server 2003)

1. To start the Cluster Administrator program, click **Start**, **Programs**, **Administrative Tools**, and then click **Cluster Administrator**.
2. Click to select a cluster group other than the quorum group that contains a Physical Disk, IP Address, and Network Name resource. To create a group with a Physical Disk, IP Address, and Network Name resource if one does not already exist, follow the steps in How to Create a Cluster Group with a Disk, IP Address, and Name Resource.
3. On the **File** menu, point to **New**, and then click **Resource**.
4. Enter a value for the **Name** field of the **New Resource** dialog box, for example, **MSDTC**.
5. In the **Resource type** drop-down list, click **Distributed Transaction Coordinator**, and then click **Next**.
6. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the

distributed transaction coordinator resource, and then click **Next**.

7. In the **Dependencies** dialog box, add a dependency to a network name resource and the disk resource associated with this group, and then click **Finish**.
8. In the dialog box that indicates that the resource was created successfully, click **OK**.

To configure the MSDTC transaction mode as Incoming Caller Authentication Required (Windows Server 2008)

1. To open the **Component Services** management console, click **Start**, **Programs**, **Administrative Tools**, and then click **Component Services**.
2. Click to expand **Component Services**, click to expand **Computers**, click to expand **My Computer**, click to expand **Distributed Transaction Coordinator**, click to expand **Clustered DTCs**, right-click the clustered DTC resource, and then click **Properties**.
3. Click the **Security** tab.
4. If network DTC access is not already enabled, click to enable the **Network DTC Access** option. Network DTC access must be enabled to accommodate transactional support for BizTalk Server.
5. Under Transaction Manager Communication, enable the following options:
   - **Allow Inbound**
   - **Allow Outbound**
   - **Incoming Caller Authentication Required**
6. After changing security settings for the clustered distributed transaction coordinator resource, the resource will be restarted. Click **Yes** and **OK** when prompted.
7. Close the **Component Services** management console.

Note

The MSDTC transaction mode must be set to either **No Authentication Required** or **Incoming Caller Authentication Required** to function correctly on a Windows Server 2008-based failover cluster. **Incoming Caller Authentication Required** is the recommended option because this option is more secure.

To configure the MSDTC transaction mode as Incoming Caller Authentication Required (Windows Server 2003)

1. To open the **Component Services** management console, click **Start**, **Programs**, **Administrative Tools**, and then **Component Services**.
2. Click to expand **Component Services**, and then click to expand **Computer**.
3. Right-click **My Computer**, and then select the **Properties** menu item to display the **My Computer Properties** dialog box.
4. Click the **MSDTC** tab.
5. To display the **Security Configuration** dialog box, click **Security Configuration** .

6. If network DTC access is not already enabled, click to enable the **Network DTC Access** option. Network DTC access must be enabled to accommodate transactional support for BizTalk Server.
7. Under Transaction Manager Communication, enable the following options:
   - **Allow Inbound**
   - **Allow Outbound**
   - **Incoming Caller Authentication Required**
8. Stop and restart the Distributed Transaction Coordinator service.

Note

The MSDTC transaction mode must be set to either **No Authentication Required** or **Incoming Caller Authentication Required** to function correctly on a Windows Server 2003-based server cluster. **Incoming Caller Authentication Required** is the recommended option because this option is more secure.

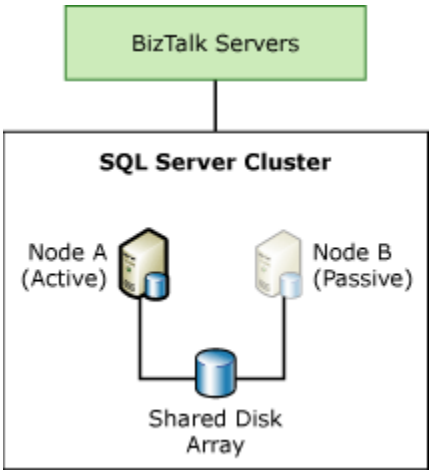
For more information about security functionality in the Distributed Transaction Coordinator service in Windows Server 2003 SP1 and later, see Microsoft Knowledge Base article 899191 "New functionality in the Distributed Transaction Coordinator service in Windows Server 2003 Service Pack 1 and in Windows XP Service Pack 2" (http://go.microsoft.com/fwlink/?LinkId=64887).

For more information about how to configure MSDTC on a Windows Server 2003 cluster, see Microsoft Knowledge Base article 301600 "How to configure Microsoft Distributed Transaction Coordinator on a Windows Server 2003 cluster" (http://go.microsoft.com/fwlink/?LinkId=62730).

Clustering SQL Server

BizTalk Server relies heavily on SQL Server for data persistence. To provide high availability for the BizTalk Server databases, create a server cluster by using Windows Server Clustering to configure two database computers that are running SQL Server. This server clustering provides redundancy and fault tolerance for the BizTalk Server databases. Unlike load-balanced clustering, where a group of computers function together to increase availability and scalability, server clustering typically involves a pair of database computers in an active/passive configuration so that one computer provides backup resources for the other.

The following figure shows a BizTalk Server database tier with high availability through active/passive server clustering.



If the active database computer encounters errors or fails, the passive computer becomes active and assumes control over the database resources until the failed computer is repaired. The database service fails over and restores data connections to the new active computer and enables the BizTalk application to continue functioning.

For information about clustering SQL Server, see your SQL Server documentation.

How to Cluster Message Queuing

Cluster support is provided for the BizTalk Server MSMQ adapter by running the MSMQ adapter handlers in a clustered instance of a BizTalk Host. If the BizTalk Server MSMQ adapter handlers are run in a clustered instance of a BizTalk Host, a clustered Message Queuing (MSMQ) resource should also be configured to run in the same cluster group as the clustered BizTalk Host when using the Send adapter or the Receive adapter for BizTalk Server 2006 R2 and earlier. This should be done for the following reasons:

- **MSMQ adapter receive handler** – The MSMQ adapter receive handler for BizTalk Server 2006 R2 and earlier does not support remote transactional reads; only local transactional reads are supported. The MSMQ adapter receive handler on BizTalk Server 2006 R2 and earlier must run in a host instance that is local to the clustered MSMQ service in order to complete local transactional reads with the MSMQ adapter.
- **MSMQ adapter send handler** - To ensure the consistency of transactional sends made by the MSMQ adapter, the outgoing queue used by the MSMQ adapter send handler should be highly available, so that if the MSMQ service for the outgoing queue fails, it can be resumed. Configuring a clustered MSMQ resource and the MSMQ adapter send handlers in the same cluster group will ensure that the outgoing queue used by the MSMQ adapter send handler will be highly available. This will mitigate the possibility of message loss in the event that the MSMQ service fails.

Procedures

To configure Message Queuing for high availability (Windows Server 2008)

1. To start the Failover Cluster Management program, click **Start**, **Programs**, **Administrative Tools**, and then click **Failover Cluster Management**.
2. In the left pane, right-click **Failover Cluster Management**, and then click **Manage a Cluster**.
3. In the **Select a cluster to manage** dialog box, enter the cluster to be managed, and then click **OK**.
4. To start the High Availability Wizard, i the left pane, click to expand the cluster, right-click **Services and Applications**, and then click **Configure a Service or Application**.
5. If the **Before You Begin** page of the High Availability Wizard is displayed, click **Next**.
6. On the **Select Service or Application** page, click **Message Queuing**, and then click **Next**.
7. On the **Client Access Point** page, enter a value for **Name**, enter an available IP address under **Address**, and then click **Next**.
8. On the **Select Storage** page, click a disk resource, and then click **Next**.
9. On the **Confirmation** page, click **Next**.
10. On the **Summary** page, click **Finish**.
11. To create a clustered MSDTC resource on the cluster so that there is transaction support for the clustered MSMQ resource, follow the steps in How to Cluster MSDTC.

    Note

    The clustered MSDTC resource does not have to exist in the same cluster group as the clustered MSMQ resource to provide transaction support. If the clustered MSDTC resource exists in a different cluster group, the Windows Server cluster uses the DTC proxy to handle requests for transaction services.

To add an MSMQ resource to an existing cluster group (Windows Server 2003)

1. To start the Cluster Administrator program, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Cluster Administrator**.
2. Click to select a cluster group other than the quorum group that contains a Name and Disk resource.
3. On the **File** menu, point to **New**, and then click **Resource**.
4. Enter a value for the **Name** field of the **New Resource** dialog box, for example, **MSMQ**.
5. In the **Resource type** drop-down list, click **Message Queuing**, and then click **Next**.
6. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the message queuing resource, and then click **Next**.
7. In the **Dependencies** dialog box, add a dependency to a network name resource and the

disk resource associated with this group, and then click **Finish**.

Note

The specified network name resource must have the option for **Enable Kerberos Authentication** enabled.

8. Click **OK** in the dialog box that indicates that the resource was created successfully.
9. To create a clustered MSDTC resource on the cluster so that there is transaction support for the clustered MSMQ resource, follow the steps in How to Cluster MSDTC.

Note

The clustered MSDTC resource does not have to exist in the same cluster group as the clustered MSMQ resource to provide transaction support. If the clustered MSDTC resource exists in a different cluster group, the Windows Server cluster uses the DTC proxy to handle requests for transaction services.

See Also

Considerations for Running Adapter Handlers within a Clustered Host

How to Cluster the File System

You can create a clustered file share resource to ensure high availability for BizTalk Server operations that require the use of the file system at run time. The File adapter and Base EDI adapter explicitly require the use of the Windows file system for the following:

- File adapter receive locations and send ports.
- Base EDI adapter receive handlers, send ports, and the Base EDI Subsystem [documentshome] directory.

Note

The Base EDI adapter is deprecated in BizTalk Server 2006 R2 and removed from BizTalk Server 2009. The Base EDI adapter is only available with BizTalk Server 2006 R2 when upgrading from BizTalk Server 2006.

Procedures

To add a file share resource to an existing cluster group (Windows Server 2008)

1. To start the Failover Cluster Management program in Windows Server 2008, click **Start**, **Programs**, **Administrative Tools**, and then click **Failover Cluster Management**.
2. In the left pane, right-click **Failover Cluster Management**, and then click **Manage a Cluster**.

3. In the **Select a cluster to manage** dialog box, enter the cluster to be managed, and then click **OK**.
4. In the left pane, click the cluster, click **Services and Applications**, and then click an existing clustered service or application that contains a Physical Disk, IP Address, and Network Name resource. To create a clustered service or application with a Physical Disk, IP Address, and Network Name resource if one does not already exist, follow the steps in How to Create a Cluster Group with a Disk, IP Address, and Name Resource.

   Note

   A Network Name and IP Address are used to create a **Client Access Point** in Windows Server 2008 Failover Clustering.
5. To start the **Provision a Shared Folder Wizard**, right-click the clustered service or application, and then click **Add a shared folder**.
6. To add the file share resource to the cluster group, follow the steps in the **Provision a Shared Folder Wizard**.
   - If the clustered file share resource is going to be used with the File adapter, grant full control permissions to the account used by the BizTalk Host for the File adapter send and receive handlers. This should be done for both NTFS and share level (SMB) permissions.
   - If the clustered file share resource is going to be used with the Base EDI adapter, grant full control permissions to the account used by the BizTalk Host for the Base EDI adapter send and receive handlers and the account used by the BizTalk Base EDI Service. This should be done for both NTFS and share level (SMB) permissions.

To add a file share resource to an existing cluster group (Windows Server 2003)

1. To start the Cluster Administrator program, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Cluster Administrator**.
2. Click to select a cluster group other than the quorum group that contains a Physical Disk, IP Address, and Network Name resource. To create a group with a Physical Disk, IP Address, and Network Name resource if one does not already exist, follow the steps in How to Create a Cluster Group with a Disk, IP Address, and Name Resource.
3. On the **File** menu, point to **New**, and then click **Resource**.
4. In the **New Resource** dialog box, enter a value for the **Name** field, for example **FileShareCluster**.
5. In the **Resource type** drop-down list, click **File Share**, and then click **Next**.
6. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the file share resource, and then click **Next**.
7. In the **Dependencies** dialog box, add a dependency to a name resource and the disk resource associated with this group, and then click **Next**.
8. Create a folder on the disk that is used by the cluster disk resource. This will be the

physical location used by the clustered file share resource.

9. In the **File Share Parameters** dialog box, enter a value for the **Share name** and the **Path** text boxes. The **Path** should point to the folder that was created on the disk used by the disk resource.
10. Set the appropriate share level permissions, and then click **Finish**.
    - If the clustered file share resource is going to be used with the File adapter, grant full control permissions to the account used by the BizTalk Host for the File adapter send and receive handlers.
    - If the clustered file share resource is going to be used with the Base EDI adapter, grant full control permissions to the account used by the BizTalk Host for the Base EDI adapter send and receive handlers and the account used by the BizTalk Base EDI Service.

Clustering Enterprise Single Sign-On

The BizTalk application service maintains a hard-coded dependency on the Enterprise Single Sign-On (SSO) service that is installed with BizTalk Server. The SSO service must be able to communicate with the master secret server to start. Configure the SSO service on the master secret server as a Windows Server cluster resource to make the master secret server highly available.

Note

- If the master secret server becomes unavailable, BizTalk Server host instances can still perform run-time operations by using the in-memory cached copy of the master secret until:
- If the SSO service is restarted on the BizTalk Server computers or if the SSO master secret is changed, the cached copy of the master secret is released from memory. The BizTalk Server computer must be able to contact the master secret server to obtain another copy of the master secret.
- If the master secret server is unavailable, any administrative operations that require access to the master secret server for purposes of encryption will fail.

How to Cluster the Master Secret Server

We recommended that you follow the instructions in this section to cluster the Enterprise Single Sign-On (SSO) service on the master secret server successfully.

When you cluster the master secret server, the Single Sign-On servers communicate with the active clustered instance of the master secret server. Similarly, the active clustered instance of the master secret server communicates with the SSO database.

You must be an SSO administrator to perform this procedure.

Caution

You cannot install the master secret server on a Network Load Balancing (NLB) cluster.

Procedures

To install and configure Enterprise SSO on the cluster nodes (Windows Server 2008)

1. Install BizTalk Server 2009 on each cluster node. In the **Component Installation** dialog box of the **Microsoft BizTalk Server Installation Wizard**, elect to install the **Enterprise Single Sign-On Administration Module** and **Enterprise Single Sign-On Master Secret Server** components. After installation has completed successfully you have the option to run the BizTalk Server 2009 Configuration program but do not do so at this time.
2. Create domain groups with the names **SSO Administrators** and **SSO Affiliate Administrators**. To create a clustered instance of the Enterprise SSO service, you must create the **SSO Administrators** and **SSO Affiliate Administrators** groups as domain groups.
3. Create or designate a domain account that is a member of the **SSO Administrators** domain group. The Enterprise SSO service on each node will be configured to log on as this domain account. This account must have the **Log on as a service** right on each node in the cluster.
4. Add the account that you are using to log on during the configuration process to the domain **SSO Administrators** group.

   Important

   Configuration of the Enterprise SSO service will fail if steps 3 and 4 are not completed.
5. Start the BizTalk Server 2009 Configuration program. Click **Start**, point to **Programs**, point to **Microsoft BizTalk Server 2009**, and then click **BizTalk Server Configuration** to display the Microsoft BizTalk Server 2009 Configuration dialog box.
6. Choose the **Custom Configuration** option and enter the appropriate values for the **Database server name**, **User name** and **Password** fields. After entering these values click the **Configure** button to continue.

   Note

   Since you will only be configuring the Enterprise SSO service at this time you can just enter the domain account that you created earlier here.
7. Select the **Enterprise SSO** option from the left pane of the Microsoft BizTalk Server 2009

Configuration dialog box and set the following options for the Enterprise SSO feature:

a. Select the check the box next to **Enable Enterprise Single Sign-On on this computer**.
b. Click the option to **Create a new SSO system**.
c. Enter the appropriate values under **Data stores** for **Server Name** and **Database Name**.
d. Verify that the domain account that you created earlier is the account that is associated with the Enterprise SSO service.
e. Specify the domain SSO Administrators group that you created earlier as the group associated with the SSO Administrator(s) role.
f. Specify the domain SSO Affiliate Administrators group that you created earlier as the group associated with the SSO Affiliate Administrator(s) role.

8. Select the **Enterprise SSO Secret Backup** option from the left pane of the Microsoft BizTalk Server 2009 Configuration dialog box and provide the appropriate parameters for backing up the Enterprise SSO secret. By default the Enterprise SSO secret is backed up to <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On*SSOxxxx*.bak.
9. Click the **Apply Configuration** option to display the Microsoft BizTalk Server 2009 Configuration Wizard Summary dialog box.
10. Click **Next** to apply the configuration.
11. Click **Finish** to close the Microsoft BizTalk Server 2009 Configuration Wizard.
12. Close the Microsoft BizTalk Server 2009 Configuration program.
13. Log on to the passive cluster node and start the BizTalk Server 2009 Configuration program.
14. Choose the **Custom Configuration** option and enter the same values for the **Database server name**, **User name**, and **Password** fields that you entered when configuring the first cluster node. After entering these values click the **Configure** button to continue.
15. Select the **Enterprise SSO** option from the left pane of the Microsoft BizTalk Server 2009 Configuration dialog box and set the following options for the Enterprise SSO feature:
    a. Check the box next to **Enable Enterprise Single Sign-On on this computer**.
    b. Click the option to **Join an existing SSO system**.
    c. Enter the same values for the SSO Database **Server Name** and **Database Name** that you entered when configuring the first cluster node.
    d. Enter the same value for the domain account that you entered when configuring the first cluster node.
16. Click the **Apply Configuration** option to display the Microsoft BizTalk Server 2009 Configuration Wizard Summary dialog box.
17. Click **Next** to apply the configuration.
18. Click **Finish** to close the Microsoft BizTalk Server 2009 Configuration Wizard.

19. Close the Microsoft BizTalk Server 2009 Configuration program.

To install and configure Enterprise SSO on the cluster nodes (Windows Server 2003)

1. Install BizTalk Server 2006 or BizTalk Server 2006 R2 on each cluster node. In the **Component Installation** dialog box of the **Microsoft BizTalk Server Installation Wizard**, elect to install the **Enterprise Single Sign-On Administration Module** and **Enterprise Single Sign-On Master Secret Server** components. After installation has completed successfully you have the option to run the BizTalk Server Configuration program but do not do so at this time.
2. Create domain groups with the names **SSO Administrators** and **SSO Affiliate Administrators**. To create a clustered instance of the Enterprise SSO service, you must create the **SSO Administrators** and **SSO Affiliate Administrators** groups as domain groups.
3. Create or designate a domain account that is a member of the **SSO Administrators** domain group. The Enterprise SSO service on each node will be configured to log on as this domain account. This account must have the **Log on as a service** right on each node in the cluster. This account must also be granted **Full Control** access to the cluster. To grant **Full Control** access to the cluster for this account, follow these steps:
   a. Start the Cluster Administrator. To do this, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Cluster Administrator**.
   b. Select the cluster.
   c. On the **File** menu, click **Properties**.
   d. On the **Security** tab, grant the domain account **Full Control** access to the cluster.
4. Add the account that you are using to log on during the configuration process to the domain **SSO Administrators** group.

   Important

   Configuration of the Enterprise SSO service will fail if steps 3 and 4 are not completed.
5. Start the BizTalk Server Configuration program. Click **Start**, point to **Programs**, point to **Microsoft BizTalk Server 2009**, and then click **BizTalk Server Configuration** to display the Microsoft BizTalk Server Configuration dialog.
6. Choose the **Custom Configuration** option and enter the appropriate values for the **Database server name**, **User name** and **Password** fields. After entering these values click the **Configure** button to continue.

   Note

   Since you will only be configuring the Enterprise SSO service at this time you can just enter the domain account that you created earlier here.
7. Select the **Enterprise SSO** option from the left pane of the Microsoft BizTalk Server Configuration dialog box and set the following options for the Enterprise SSO feature:

a. Select the check the box next to **Enable Enterprise Single Sign-On on this computer**.
b. Click the option to **Create a new SSO system**.
c. Enter the appropriate values for the **SSO Database Server Name** and **Database Name**.
d. Verify that the domain account that you created earlier is the account that is associated with the Enterprise SSO service.
e. Specify the domain SSO Administrators group that you created earlier as the group associated with the SSO Administrator(s) role.
f. Specify the domain SSO Affiliate Administrators group that you created earlier as the group associated with the SSO Affiliate Administrator(s) role.

8. Select the **Enterprise SSO Secret Backup** option from the left pane of the Microsoft BizTalk Server Configuration dialog box and provide the appropriate parameters for backing up the Enterprise SSO secret. By default the Enterprise SSO secret is backed up to <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On*SSOxxxx*.bak.
9. Click the **Apply Configuration** option to display the Microsoft BizTalk Server Configuration Wizard Summary dialog box.
10. Click **Next** to apply the configuration.
11. Click **Finish** to close the Microsoft BizTalk Server Configuration Wizard.
12. Close the Microsoft BizTalk Server Configuration program.
13. Log on to the passive cluster node and start the BizTalk Server Configuration program.
14. Choose the **Custom Configuration** option and enter the same values for the **Database server name**, **User name**, and **Password** fields that you entered when configuring the first cluster node. After entering these values click the **Configure** button to continue.
15. Select the **Enterprise SSO** option from the left pane of the Microsoft BizTalk Server Configuration dialog box and set the following options for the Enterprise SSO feature:
    a. Check the box next to **Enable Enterprise Single Sign-On on this computer**.
    b. Click the option to **Join an existing SSO system**.
    c. Enter the same values for the SSO Database **Server Name** and **Database Name** that you entered when configuring the first cluster node.
    d. Enter the same value for the domain account that you entered when configuring the first cluster node.
16. Click the **Apply Configuration** option to display the Microsoft BizTalk Server Configuration Wizard Summary dialog box.
17. Click **Next** to apply the configuration.
18. Click **Finish** to close the Microsoft BizTalk Server Configuration Wizard.
19. Close the Microsoft BizTalk Server Configuration program.

To update the master secret server name in the SSO database

1. Type the following commands from a command prompt on the active cluster node to stop and restart the Enterprise SSO service:

   ```
   net stop entsso
   ```

   and

   ```
   net start entsso
   ```

2. Change the master secret server name in the SSO database to the cluster name by following these steps:

   Note

   The cluster name is the name defined for the network name resource that you have created in the cluster group / clustered service or application that will contain the clustered Enterprise SSO service. For example, the name may be *BIZTALKCLUSTER*.

   a. Paste the following code in a text editor:

   ```
   <sso>
     <globalInfo>
       <secretServer>BIZTALKCLUSTER</secretServer>
     </globalInfo>
   </sso>
   ```

   Note

   BIZTALKCLUSTER is a placeholder for the actual network name resource that is created in the cluster group / clustered service or application.

   b. Save the file as an .xml file. For example, save the file as SSOCLUSTER.xml.

   c. At a command prompt, change to the Enterprise SSO installation folder. By default, the installation folder is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

   d. Type the following command at the command prompt to update the master secret server name in the database:

   ```
   ssomanage -updatedb XMLFile
   ```

   Note

   XMLFile is a placeholder for the name of the .xml file that you saved earlier.

To create the clustered Enterprise SSO resource (Windows Server 2008)

1. If the cluster is not configured with a clustered Distributed Transaction Coordinator (MSDTC) resource then follow the steps in the "Improving Fault Tolerance in BizTalk Server by Using a Windows Server Cluster" white paper at

http://go.microsoft.com/fwlink/?LinkId=69207 to create a clustered MSDTC resource.

2. Click **Start**, **Programs**, **Administrative Tools**, and then **Failover Cluster Management** to start the Failover Cluster Management program.
3. In the left hand pane, right-click **Failover Cluster Management** and click **Manage a Cluster**.
4. On the **Select a cluster to manage** dialog box, enter the cluster to be managed and click **OK**.
5. In the left hand pane click to select a clustered service or application that contains an IP Address and Network Name resource. Follow the steps in How to Create a Cluster Group with a Disk, IP Address, and Name Resource to create a group with an IP Address and Network Name resource if one does not already exist.

   Note

   A clustered Enterprise SSO service does not explicitly require the use of a clustered Physical Disk resource in the same group.
6. Right-click the clustered service or application, point to **Add a resource**, and click **Generic Service** to display the **New Resource Wizard** dialog.
7. On the **Select Service** page of the **New Resource Wizard**, click to select **Enterprise Single Sign-On Service** and click **Next**.
8. On the **Confirmation** page click **Next**.
9. On the **Summary** page click **Finish**. A clustered instance of the Enterprise Single Sign-On Service will appear under **Other Resources** in the center pane of the **Failover Cluster Management** interface.
10. Right-click the clustered instance of the Enterprise Single Sign-On Service and select **Properties** to display the **Enterprise Single Sign-On Service Properties** dialog box.
11. Click the **Dependencies** tab of the properties dialog box and click **Insert**.
12. Click the drop down box under **Resource**, select the **Name:** resource and click **OK**.

To create the clustered Enterprise SSO resource (Windows Server 2003)

1. If the cluster is not configured with a clustered Distributed Transaction Coordinator (MSDTC) resource then follow the steps in the "Improving Fault Tolerance in BizTalk Server by Using a Windows Server Cluster" white paper at http://go.microsoft.com/fwlink/?LinkId=69207 to create a clustered MSDTC resource.
2. In Windows Server 2003, click **Start**, **Programs**, **Administrative Tools**, and then **Cluster Administrator** to start the Cluster Administrator program.
3. Click to select a cluster group other than the quorum group that contains an IP Address and Network Name resource. Follow the steps in How to Create a Cluster Group with a Disk, IP Address, and Name Resource to create a group with an IP Address and Network Name resource if one does not already exist.

   Note

A clustered Enterprise SSO service does not explicitly require the use of a clustered Physical Disk resource in the same group.

4. On the **File** menu, point to **New**, and then click **Resource**.
5. In the **New Resource** window, follow these steps:
   a. In the **Name** box, type the name of the SSO resource. For example, *ENTSSO*.
   b. In the **Resource type** dropdown, click **Generic Service**.
   c. Click **Next**.
   d. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the *ENTSSO* resource and click **Next**.
   e. In the **Dependencies** dialog box, add a dependency to the Network Name resource that you created for this group, and then click **Next**.
   f. In the **Generic Service Parameters** dialog box, type **entsso** for the **Service name**, leave **Start parameters** blank, click to select the **Use Network Name for computer name** check box, and click **Next.**
   g. In the **Registry Replication** dialog box click **Finish**.

      Note

      Do not configure any registry keys for replication in the Registry Replication dialog box. Replication of registry keys is not a requirement when creating a clustered Enterprise SSO resource and in fact may cause problems when failover of this cluster resource is attempted.

   h. Click **OK** on the dialog box that indicates that the resource was created successfully.

Important

- If you do not click to select the **Use Network Name for computer name** check box, SSO client computers will generate an error similar to the following when they try to contact this clustered instance of the Enterprise SSO service:
- Failed to retrieve master secrets.
- Verify that the master secret server name is correct and that it is available. Secret Server Name: ENTSSO Error Code: 0x800706D9, there are no more endpoints available from the endpoint mapper.

To restore the master secret on the second cluster node (Windows Server 2008)

1. In Failover Cluster Management, right click the clustered service or application that contains the clustered Enterprise Single Sign-On service and then click **Bring this service or application online** to start all of the resources in the clustered service or application.
2. Right-click the clustered service or application, point to **Move this service or application to another node**, and click the second node. This step moves the clustered service or application that contains the clustered Enterprise Single Sign-On service from the first

node to the second node.

3. Right-click the clustered Enterprise Single Sign-On service and click **Take this service or application offline**, then right-click the clustered instance of the Enterprise SSO service and click **Bring this service or application online**.

   Note

   If this step is not completed the attempt to restore the master secret may not succeed.

4. Copy the master secret backup file from the first node to the \Enterprise Single Sign-On installation folder on the second node. By default, the installation folder is *<drive>*:\Program Files\Common Files\Enterprise Single Sign-On.
5. Log on to the second node and at a command prompt, change to the Enterprise SSO installation folder.
6. Type the following command from the command prompt to restore the master secret to the second node:

   ```
   ssoconfig -restoresecret RestoreFile
   ```

   Note

   Replace *RestoreFile* with the path of and the name of the backup file that contains the master secret.

   The master secret is stored in the registry at the following location:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ENTSSO\SSOSS
7. Move the clustered service or application that contains the clustered Enterprise Single Sign-On service from this cluster node to other cluster node to ensure failover functionality. Then move the cluster group back to verify fail-back functionality.

To restore the master secret on the second cluster node (Windows Server 2003)

1. In Cluster Administrator, right-click the cluster group that contains the clustered Enterprise SSO service resource, and then click **Bring Online** to start all of the resources in the cluster group.
2. Right-click the cluster group and click **Move group**. This step moves the cluster group that contains the clustered Enterprise SSO service resource from the first node to the second node.
3. Right-click the clustered instance of the Enterprise SSO service and click **Take Offline**, then right-click the clustered instance of the Enterprise SSO service and click **Bring Online**.

   Note

   If this step is not completed the attempt to restore the master secret may not succeed.

4. Copy the master secret backup file from the first node to the \Enterprise Single Sign-On

installation folder on the second node. By default, the installation folder is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

5. Log on to the second node and at a command prompt, change to the Enterprise SSO installation folder.
6. Type the following command from the command prompt to restore the master secret to the second node:

   ```
   ssoconfig -restoresecret RestoreFile
   ```

   Note

   Replace *RestoreFile* with the path of and the name of the backup file that contains the master secret.

   The master secret is stored in the registry at the following location:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ENTSSO\SSOSS
7. Move the cluster group that contains the clustered Enterprise SSO service from this cluster node to other cluster node to ensure failover functionality. Then move the cluster group back to verify fail-back functionality.

See Also

How to Create a Cluster Group with a Disk, IP Address, and Name Resource

How to Cluster SSO and a BizTalk Host in the Same Cluster Group

With BizTalk Server you can cluster one or more BizTalk hosts and the Enterprise Single Sign-On (SSO) service on the same Windows Server cluster.

Note

Correct implementation of this strategy requires that you create any BizTalk host instances and the SSO service as cluster resources in the same cluster group.

The use of Windows Clustering with one or more BizTalk hosts and SSO typically falls into one of these categories:

1. Clustering the SSO master secret server and one or more BizTalk hosts in the same cluster group.

   In this scenario, the dependency between the clustered BizTalk hosts and the clustered SSO service is maintained so that if the cluster group is failed over, all resources move with the group.

   If the SSO service is configured as a clustered resource on a BizTalk Server computer, you must create a clustered IIS web service in the same cluster group. This must be done to ensure that all isolated host instances will run on the cluster node that the SSO service is

running on. This ensures that any adapters that run in an isolated host instance will have access to the SSO service since isolated host instances run in IIS.

Note

If an unclustered instance of a BizTalk host is running on the same cluster node that a clustered instance of the SSO service is running, the clustered instance of the SSO service cannot be failed over unless the unclustered instance of the BizTalk host is stopped. An unclustered instance of the BizTalk host maintains a dependency upon the clustered instance of the SSO service running on the cluster node and prevents the clustered instance of the SSO service from failing over. For this reason, it is recommended that you do not create an unclustered instance of a BizTalk host to run on the same cluster node that is running a clustered instance of the SSO service.

2. Clustering the SSO service (non master secret server) and one or more BizTalk hosts in the same cluster group. This scenario requires that a remote master secret server be available. In this scenario, the dependency between the clustered BizTalk hosts and the clustered SSO service is maintained so if the cluster group is failed over, all resources move with the group.

   If the SSO service is configured as a clustered resource on a BizTalk Server computer, you must create a clustered IIS web service in the same cluster group. This must be done to ensure that all isolated host instances will run on the cluster node that the SSO service is running on. This ensures that any adapters that run in an isolated host instance will have access to the SSO service since isolated host instances run in IIS.

   Note

   If an unclustered instance of a BizTalk host is running on the same cluster node that a clustered instance of the SSO service is running then the clustered instance of the SSO service cannot be failed over unless the unclustered instance of the BizTalk host is stopped. An un-clustered instance of the BizTalk host maintains a dependency upon the clustered instance of the SSO service running on the cluster node and prevents the clustered instance of the SSO service from failing over. For this reason, it is recommended that you not create a unclustered instance of a BizTalk host to run on the same cluster node that is running a clustered instance of the SSO service.

3. Clustering one or more BizTalk hosts on a Windows Server cluster without clustering the SSO service. In this scenario, one or more BizTalk hosts are configured as cluster resources but the SSO service is not configured as a clustered resource. This design provides high availability for the clustered BizTalk hosts but does not provide high availability for the SSO service. In this scenario, if the SSO service on a node fails then BizTalk Server components that depend on SSO on that node will also fail. For more information about how to configure a BizTalk Server host as a cluster resource see How to Configure a BizTalk Host as a Cluster Resource.

The following procedures describe the steps that you should follow to cluster a BizTalk host and the SSO service on the same Windows Server cluster.

Procedures

To cluster a BizTalk host and the SSO master secret server on the same Windows Server cluster (Windows Server 2008)

1. If the cluster is not configured with a clustered Distributed Transaction Coordinator (MSDTC) resource, cluster MSDTC on a Windows Server 2008 failover cluster by following the steps in Checklist: Creating an MS DTC Resource in a Windows Server 2008 Failover Cluster (http://go.microsoft.com/fwlink/?LinkID=129677).
2. Install and configure the SSO service on the Windows Server cluster by following the steps in How to Cluster the Master Secret Server. Since you will be running BizTalk Server on the Windows Server cluster, install all required BizTalk Server components even though you will only be configuring the SSO components at this time.
3. Cluster IIS on the BizTalk Server computer by following the steps documented in Microsoft Knowledge Base article 970759 "Configuring IIS 7.0 in a Microsoft Windows Server 2008 failover cluster" (http://go.microsoft.com/fwlink/?LinkId=152793). Create the clustered IIS Web service in the same cluster group as the clustered SSO service.
4. Move the cluster group that contains the clustered SSO service to one of the cluster nodes, and log on to this cluster node.
5. Start the BizTalk Server Configuration program, and complete the configuration of BizTalk Server on this cluster node. Since this is the first BizTalk Server computer in the group, click **Create a new BizTalk Group** when configuring the BizTalk Group.
6. Once the BizTalk Server configuration has completed successfully, move the cluster group that contains the clustered SSO service to the other cluster node, and log on to this cluster node.
7. Start the BizTalk Server Configuration program, and complete the configuration of BizTalk Server on this cluster node. Click **Join an existing BizTalk Group** when configuring the BizTalk Group component on this cluster node, and specify the BizTalk group that you created on the first node.
8. Once the BizTalk Server configuration has completed successfully, create one or more clustered BizTalk hosts by following the steps in How to Configure a BizTalk Host as a Cluster Resource.

   Note

   In this scenario, all BizTalk hosts must be created as cluster resources in the same cluster group as the clustered SSO service resource. Running a unclustered BizTalk host instance on a Windows Server Cluster node where the SSO service is clustered is not a supported configuration. This is because the unclustered BizTalk host instance will fail when the clustered SSO service is failed over to another node due to the dependency of a BizTalk host instance on the SSO service.

To cluster a BizTalk host and the SSO master secret server on the same Windows Server cluster (Windows Server 2003)

1. If the cluster is not configured with a clustered Distributed Transaction Coordinator (MSDTC) resource, create a clustered MSDTC resource by following the steps in the Microsoft Knowledge Base article 301600 “How to configure Microsoft Distributed Transaction Coordinator on a Windows Server 2003 cluster” (http://go.microsoft.com/fwlink/?LinkID=55136).
2. Install and configure the SSO service on the Windows Server cluster by following the steps in How to Cluster the Master Secret Server. Since you will be running BizTalk Server on the Windows Server cluster, install all required BizTalk Server components even though you will only be configuring the SSO components at this time.
3. To cluster IIS on the BizTalk Server computer Follow the steps documented in Checklist: Creating a clustered IIS Web or FTP service (http://go.microsoft.com/fwlink/?LinkId=75278). Create the clustered IIS Web service in the same cluster group as the clustered SSO service. The script file that is referenced in this topic (clusweb.vbs) does not contain code to take the clustered IIS resource offline. Modify the Offline() function in the script with the following code:

```
Function Offline( )

    Dim objWmiProvider
    Dim objService
    Dim strServiceState

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

    If ucase(strServiceState) = "STOPPED" Then
        Offline = True
    Else

    ' If the service is running, try to stop it.  If it won't stop, log an
error
        response = objService.StopService()

        ' response = 0  or 10 indicates that the request to stop was
```

```
accepted
        If ( response <> 0 ) and ( response <> 10 ) Then
            Resource.LogInformation "The resource failed to go offline
because the W3SVC service is still running."
            Offline = False
        Else
            Offline = True
        End If
    End If

End Function
```

Important

After making this change you must save the updated clusweb.vbs file with a different name (for example, clusIIS.vbs) and then reference the new file when you create the Generic Script Resource for the IIS Service. A new file name must be used because Windows File Protection will take any changes that you make to the clusweb.vbs file and revert them to the original file.

4. Move the cluster group that contains the clustered SSO service to one of the cluster nodes and log on to this cluster node.
5. Start the BizTalk Server Configuration program, and complete the configuration of BizTalk Server on this cluster node. Since this is the first BizTalk Server computer in the group, click **Create a new BizTalk Group** when configuring the BizTalk Group component.
6. Once the BizTalk Server configuration has completed successfully, move the cluster group that contains the clustered SSO service to the other cluster node, and log on to this cluster node.
7. Start the BizTalk Server Configuration program, and complete the configuration of BizTalk Server on this cluster node. Click **Join an existing BizTalk Group** when configuring the BizTalk Group component on this cluster node and specify the BizTalk group that you created on the first node.
8. Once the BizTalk Server configuration has completed successfully, follow the steps in How to Configure a BizTalk Host as a Cluster Resource to create one or more clustered BizTalk host instances.

Note

In this scenario, all BizTalk hosts must be created as cluster resources in the same cluster group as the clustered SSO service resource. Running an unclustered BizTalk host instance on a Windows Server Cluster node where the SSO service is clustered is not a supported configuration. This is because the

unclustered BizTalk host instance will fail when the clustered SSO service is failed over to another node due to the dependency of a BizTalk host instance on the SSO service.

To cluster a BizTalk host and SSO (non master secret server) on the same Windows Server cluster when the SSO master secret server is remote (Windows Server 2008)

1. If the cluster is not configured with a clustered Distributed Transaction Coordinator (MSDTC) resource, cluster MSDTC on a Windows Server 2008 failover cluster by following the steps in Checklist: Creating an MS DTC Resource in a Windows Server 2008 Failover Cluster (http://go.microsoft.com/fwlink/?LinkID=129677).
2. Create domain groups with the names **SSO Administrators** and **SSO Affiliate Administrators**. To create a clustered instance of the SSO service, you must create the **SSO Administrators** and **SSO Affiliate Administrators** groups as domain groups.
3. Create or designate a domain account that is a member of the **SSO Administrators** domain group. The SSO service on each node will be configured to log on as this domain account. This account must have the **Log on as a service** right on each node in the cluster.
4. Add the account that you are using to log on during the installation and configuration process to the domain **SSO Administrators** group.

   Important

   Configuration of the SSO service will fail if steps 3 and 4 are not completed.
5. Log on to one of the cluster nodes and install BizTalk Server 2009. Select the option to start the configuration program when installation has completed successfully.
6. Choose the **Custom Configuration** option and enter the appropriate values for the **Database server name**, **User name** and **Password** fields. After entering these values click the **Configure** button to continue.
7. Set the following options for the SSO feature:
   a. Select the check the box next to **Enable Enterprise Single Sign-On on this computer**.
   b. Click the option to **Join an existing SSO system**.
   c. Enter values for the existing SSO Database Server Name and Database Name.
   d. Enter the existing SSO service account when specifying the account to use for the Enterprise Single Sign-On service.
8. Since this is the first BizTalk Server in the group choose the option to **Create a new BizTalk Group** when configuring the BizTalk Group component.
9. Specify the remaining configuration options as needed and apply the BizTalk Server configuration to this node.
10. Once the BizTalk Server configuration has completed successfully on the first node, log on to the second node and install BizTalk Server 2009. Select the option to start the

configuration program when installation has completed successfully.

11. Choose the **Custom Configuration** option, and then enter the appropriate values for the **Database server name**, **User name** and **Password** fields. After entering these values, click the **Configure** button to continue.
12. Set the following options for the SSO feature:
    a. Select the check the box next to **Enable Enterprise Single Sign-On on this computer**.
    b. Click **Join an existing SSO system**.
    c. Enter values for the existing SSO Database Server Name and Database Name.
    d. Enter the existing SSO service account when specifying the account to use for the Enterprise Single Sign-On service.
13. Choose the option to **Join an existing BizTalk Group** when configuring the BizTalk Group component on this cluster node, and specify the BizTalk group that you created on the first node.
14. Specify the remaining configuration options as needed and apply the BizTalk Server configuration to this node.
15. After the BizTalk Server configuration has completed successfully, follow these steps to cluster the SSO service:
    a. Stop the SSO service on each of the cluster nodes by typing the following command from a command:

       ```
       net stop entsso
       ```

    b. In Failover Cluster Management, move all cluster groups to one node and log on to this node.
    c. In the left hand pane click to select a clustered service or application that contains an IP Address and Network Name resource. This clustered service or application will contain the clustered SSO service and the clustered BizTalk host.

       Note

       A clustered SSO service does not explicitly require the use of a clustered Physical Disk resource in the same group.

    d. Right-click the clustered service or application, point to **Add a resource**, and click **Generic Service** to display the **New Resource Wizard** dialog box.
    e. On the **Select Service** page of the **New Resource Wizard**, select **Enterprise Single Sign-On Service**, and then click **Next**.
    f. On the **Confirmation** page click **Next**.
    g. On the **Summary** page click **Finish**. A clustered instance of the Enterprise Single Sign-On Service will appear under **Other Resources** in the center pane of the **Failover Cluster Management** interface.
    h. Right-click the clustered instance of the Enterprise Single Sign-On Service and select **Properties** to display the **Enterprise Single Sign-On Service Properties** dialog

box.

i. Click the **Dependencies** tab of the properties dialog box and click **Insert**.

j. Click the drop down box under **Resource**, select the **Name:** resource and click **OK**.

Important

If you do not add the dependency to the **Name:** resource, SSO client computers will generate an error similar to the following when they try to contact this clustered instance of the SSO service:

Failed to retrieve master secrets.

Verify that the master secret server name is correct and that it is available. Secret Server Name: ENTSSO Error Code: 0x800706D9, there are no more endpoints available from the endpoint mapper.

16. Cluster IIS on the BizTalk Server computer by following the steps documented in Microsoft Knowledge Base article 970759 "Configuring IIS 7.0 in a Microsoft Windows Server 2008 failover cluster" (http://go.microsoft.com/fwlink/?LinkId=152793). Create the clustered IIS web service in the same cluster group as the clustered SSO service.
17. In Failover Cluster Management, right click the clustered service or application that contains the clustered Enterprise Single Sign-On service and then click **Bring this service or application online** to start all of the resources in the clustered service or application.
18. Right-click the clustered service or application, point to **Move this service or application to another node**, and click the second node. This step moves the clustered service or application that contains the clustered Enterprise Single Sign-On service from the first node to the second node.
19. Right-click the clustered Enterprise Single Sign-On service and click **Take this service or application offline**, then right-click the clustered instance of the SSO service and click **Bring this service or application online**.
20. Set the SSO server name for all users to the clustered SSO service with the ssomanage command line utility. This command should be run from the SSO installation folder on each BizTalk server in the group. For example, the following command line will set the SSO server name for all users to the clustered SSO service:

```
ssomanage -serverall SSOCLUSTER
```

Note

SSOCLUSTER is a placeholder for the actual network name resource that is created in the cluster group that contains the clustered SSO service.

21. Update the SSO Server name accessible in the **BizTalk Group Properties** page to reference the clustered SSO service. Open **BizTalk Server Administration**, right-click the BizTalk Group, select the **Properties** menu item, update the entry for SSO Server name, and then click **OK**.
22. Follow the steps in How to Configure a BizTalk Host as a Cluster Resource to create one

or more clustered BizTalk host instances in the same cluster group that you have created the clustered SSO service.

Note

In this scenario, all BizTalk hosts must be created as cluster resources in the same cluster group as the clustered SSO service resource. Running an unclustered BizTalk host instance on a Windows Server Cluster node where the SSO service is clustered is not a supported configuration. This is because the unclustered BizTalk host instance will fail when the clustered SSO service is failed over to another node due to the dependency of a BizTalk host instance on the SSO service.

To cluster a BizTalk host and SSO (non master secret server) on the same Windows Server cluster when the SSO master secret server is remote (Windows Server 2003)

1. If the cluster is not configured with a clustered Distributed Transaction Coordinator (MSDTC) resource then create a clustered MSDTC resource.by following the steps in the Microsoft Knowledge Base article 301600 "How to configure Microsoft Distributed Transaction Coordinator on a Windows Server 2003 cluster" (http://go.microsoft.com/fwlink/?LinkID=55136).
2. Create domain groups with the names **SSO Administrators** and **SSO Affiliate Administrators**. To create a clustered instance of the SSO service, you must create the **SSO Administrators** and **SSO Affiliate Administrators** groups as domain groups.
3. Create or designate a domain account that is a member of the **SSO Administrators** domain group. The SSO service on each node will be configured to log on as this domain account. This account must have the **Log on as a service** right on each node in the cluster. This account must also be granted **Full Control** access to the cluster. To grant **Full Control** access to the cluster for this account, follow these steps:
   a. Start the Cluster Administrator. To do this, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Cluster Administrator**.
   b. Select the cluster.
   c. On the **File** menu, click **Properties**.
   d. On the **Security** tab, grant the domain account **Full Control** access to the cluster.
4. Add the account that you are using to log on during the installation and configuration process to the domain **SSO Administrators** group.

   Important

   Configuration of the SSO service will fail if steps 3 and 4 are not completed.
5. Log on to one of the cluster nodes and install BizTalk Server. Select the option to start the configuration program when installation has completed successfully.
6. Choose the **Custom Configuration** option and enter the appropriate values for the **Database server name**, **User name** and **Password** fields. After entering these values

click the **Configure** button to continue.

7. Set the following options for the SSO feature:
   a. Select the check the box next to **Enable Enterprise Single Sign-On on this computer**.
   b. Click the option to **Join an existing SSO system**.
   c. Enter values for the existing SSO Database Server Name and Database Name.
   d. Enter the existing SSO service account when specifying the account to use for the Enterprise Single Sign-On service.
8. Since this is the first BizTalk Server in the group choose the option to **Create a new BizTalk Group** when configuring the BizTalk Group component.
9. Specify the remaining configuration options as needed and apply the BizTalk Server configuration to this node.
10. Once the BizTalk Server configuration has completed successfully on the first node, log on to the second node and install BizTalk Server. Select the option to start the configuration program when installation has completed successfully.
11. Choose the **Custom Configuration** option and enter the appropriate values for the **Database server name**, **User name** and **Password** fields. After entering these values, click the **Configure** button to continue.
12. Set the following options for the SSO feature:
    a. Select the check the box next to **Enable Enterprise Single Sign-On on this computer**.
    b. Click the option to **Join an existing SSO system**.
    c. Enter values for the existing SSO Database Server Name and Database Name.
    d. Enter the existing SSO service account when specifying the account to use for the Enterprise Single Sign-On service.
13. Choose the option to **Join an existing BizTalk Group** when configuring the BizTalk Group component on this cluster node and specify the BizTalk group that you created on the first node.
14. Specify the remaining configuration options as needed and apply the BizTalk Server configuration to this node.
15. After the BizTalk Server configuration has completed successfully, follow these steps to cluster the SSO service:
    a. Stop the SSO service on each of the cluster nodes by typing the following command from a command:

       ```
       net stop entsso
       ```

    b. In the Cluster Administrator, move all cluster groups to one node and log on to this node.
    c. Click to select a cluster group other than the quorum group that contains an IP Address and Network Name resource. This group will contain the clustered SSO

service and the clustered BizTalk host.

Note

A clustered SSO service does not explicitly require the use of a clustered Physical Disk resource in the same group.

d. On the **File** menu, point to **New**, and then click **Resource**.

e. Enter a value for the **Name** field of the **New Resource** dialog box, for example, *ENTSSO*.

f. In the **Resource type** drop-down list, click **Generic Service**.

g. Click **Next**.

h. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the *ENTSSO* resource, and then click **Next**.

i. In the **Dependencies** dialog box, add a dependency to a Network Name resource that is created in this group, and then click **Next**.

j. In the **Generic Service Parameters** dialog box, type **entsso** for the **Service name**, leave **Start parameters** blank, click to select the **Use Network Name for computer name** check box, and then click **Next.**

k. In the **Registry Replication** dialog box, click **Finish**.

l. Click **OK** in the dialog box that indicates that the resource was created successfully.

Important

If you do not click to select the **Use Network Name for computer name** check box, SSO client computers will generate an error similar to the following when they try to contact this clustered instance of the SSO service:

Failed to retrieve master secrets.

Verify that the master secret server name is correct and that it is available. Secret Server Name: ENTSSO Error Code: 0x800706D9, there are no more endpoints available from the endpoint mapper.

16. Cluster IIS on the BizTalk Server computer by following the steps documented at Checklist: Creating a clustered IIS Web or FTP service (http://go.microsoft.com/fwlink/?LinkId=75278). Create the clustered IIS web service in the same cluster group as the clustered SSO service. The script file that is referenced in this topic (clusweb.vbs) does not contain code to take the clustered IIS resource offline. Modify the Offline() function in the script with the following code:

```
Function Offline( )


    Dim objWmiProvider

    Dim objService

    Dim strServiceState
```

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

    If ucase(strServiceState) = "STOPPED" Then
        Offline = True
    Else

    ' If the service is running, try to stop it.  If it won't stop, log an
error
        response = objService.StopService()

        ' response = 0  or 10 indicates that the request to stop was
accepted
        If ( response <> 0 ) and ( response <> 10 ) Then
            Resource.LogInformation "The resource failed to go offline
because the W3SVC service is still running."
            Offline = False
        Else
            Offline = True
        End If
    End If

End Function
```

Important

After making this change you must save the updated clusweb.vbs file with a different name (for example, clusIIS.vbs) and then reference the new file when you create the Generic Script Resource for the IIS Service. A new file name must be used because Windows File Protection will take any changes that you make to the clusweb.vbs file and revert them to the original file.

17. In Cluster Administrator, right-click the cluster group that contains the clustered SSO service resource, and then click **Bring Online** to start all of the resources in the cluster group.
18. Move the cluster group that contains the clustered SSO service from the active cluster

node to the other cluster node to ensure failover functionality. Then move the cluster group back to verify fail-back functionality.

19. Set the SSO server name for all users to the clustered SSO service with the ssomanage command line utility. This command should be run from the SSO installation folder on each BizTalk server in the group. For example, the following command line will set the SSO server name for all users to the clustered SSO service:

    ```
    ssomanage -serverall SSOCLUSTER
    ```

    Note

    SSOCLUSTER is a placeholder for the actual network name resource that is created in the cluster group that contains the clustered SSO service.

20. Update the SSO Server name accessible in the **BizTalk Group Properties** page to reference the clustered SSO service. Open **BizTalk Server Administration**, right-click the BizTalk Group, select the **Properties** menu item, update the entry for SSO Server name, and then click **OK**.
21. Follow the steps in How to Configure a BizTalk Host as a Cluster Resource to create one or more clustered BizTalk host instances in the same cluster group that you have created the clustered SSO service.

    Note

    In this scenario, all BizTalk hosts must be created as cluster resources in the same cluster group as the clustered SSO service resource. Running an unclustered BizTalk host instance on a Windows Server Cluster node where the SSO service is clustered is not a supported configuration. This is because the unclustered BizTalk host instance will fail when the clustered SSO service is failed over to another node due to the dependency of a BizTalk host instance on the SSO service.

Using Windows Server Cluster to Provide High Availability for BizTalk Server Hosts

BizTalk Server 2006 and later provide functionality that allows you to configure a BizTalk Host as a clustered resource within a Windows Server cluster. Host cluster support is provided to support high availability for integrated BizTalk adapters that should not be run in multiple host instances simultaneously, such as the FTP adapter receive handler or, under certain circumstances, the POP3 adapter receive handler. Host cluster support is also provided to ensure transactional consistency for messages sent or received by the MSMQ adapter in scenarios that require that the MSMQ service be clustered.

Note

Host clustering is only available with the Enterprise Edition of BizTalk Server.

Note

Before you can cluster a BizTalk Host, you must have configured at least two BizTalk Server computers in a BizTalk Server group as members of a Windows Server cluster. For more information about configuring a Windows Server Cluster, see the Windows Server online Help.

Considerations for Installing BizTalk Server on a Windows Server Cluster

Special considerations must be made when installing BizTalk Server on a Windows Server cluster. This topic lists these considerations.

A non-clustered BizTalk host instance should not be run on a Windows Server cluster where the Enterprise SSO service is clustered

It is a recommended practice to cluster the Enterprise Single Sign-On Master Secret Server in an active/passive configuration to provide high availability for the master secret server. If a non-clustered BizTalk host instance and a clustered instance of the Enterprise SSO service are running on the same cluster node, the BizTalk host instance will fail if the clustered Enterprise SSO service is moved to a different node in the cluster. BizTalk Hosts maintain a dependency on a locally running instance of the Enterprise SSO service. Therefore if the Enterprise SSO service is configured as a clustered resource, then any BizTalk Hosts running on the cluster nodes must be configured as a clustered resource in the same cluster group.

Configure the Microsoft Distributed Transaction Coordinator (MSDTC) as a clustered resource before installing BizTalk Server on a cluster

If you plan to install BizTalk Server on a Windows Server cluster, you must cluster the Microsoft Distributed Transaction Coordinator first.

To cluster MSDTC on a Windows Server 2008 failover cluster, follow the steps outlined in Checklist: Creating an MS DTC Resource in a Windows Server 2008 Failover Cluster

To cluster MSDTC on a Windows Server 2003 cluster, follow the steps outlined in the Microsoft Knowledge Base article 301600 at http://go.microsoft.com/fwlink/?LinkId=62730.

Network DTC access must be enabled on all BizTalk Servers and on the SQL Server before installing or configuring BizTalk Server

To enable network DTC access on each cluster node as well as on the SQL server that will host the BizTalk Server databases, follow the steps outlined in Microsoft Knowledge Base article 817064, available at http://go.microsoft.com/fwlink/?LinkId=55137. Network DTC access must be enabled to accommodate transactional support for BizTalk Server. We recommend that you restart each server after completing the steps in this Knowledge Base article.

The Configure Your Server Wizard is not available on a Windows Server 2003 cluster

Since the **Configure Your Server Wizard** is not available on a Windows Server 2003 cluster, you must manually complete the following steps when installing BizTalk Server on a Windows Server 2003 cluster:

- Install Internet Information Services (IIS).
- Enable COM+ for remote transactions.
- Enable the ASP.Net Web Service extension.

Note

- Windows Server 2008 does not provide a **Configure Your Server Wizard**. Complete the following steps when installing BizTalk Server on a Windows Server 2008 failover cluster:

You must manually create domain groups in Active Directory before you configure BizTalk Server

If you install BizTalk Server on multiple computers, you must specify domain groups and user accounts in the BizTalk Server Configuration Wizard. If you use domain groups for your BizTalk Server configuration, you must manually create the groups before you configure BizTalk Server.

How to Configure a BizTalk Host as a Cluster Resource

This topic discusses the steps that you must follow to configure a BizTalk host as a cluster resource. To complete the steps in this topic, you must have already configured at least two BizTalk Servers in a BizTalk group as members of a Windows Server cluster. For more information about configuring a Windows Server cluster, see the Windows Server online Help.

Prerequisites

You must be logged on as a member of the BizTalk Administrators group to cluster or uncluster a host.

Considerations and Known Issues

- A BizTalk Server must be configured as a node in a Windows Server 2003 server cluster or Windows Server 2008 failover cluster before you can run an instance of a clustered BizTalk host on the BizTalk Server. For more information about configuring a cluster node in a server cluster, see the Windows Server online Help.
- You cannot fail over a clustered BizTalk host to a host instance that has the option **Disable host instance from starting** set. Ensure that all host instances for the clustered BizTalk host do not have this option enabled. This option is set in the BizTalk Server Administration console on the **Host Instance Properties** page.
- When you cluster a BizTalk host, a corresponding cluster resource is created in the specified cluster resource group. When the cluster resource is created, each available node of the cluster is added as a possible owner of the cluster resource. Since a cluster resource can be failed over to any node in the list of possible owners, you should add an instance of the host to all available nodes of a cluster before clustering a BizTalk host. Attempts to fail over a clustered BizTalk host to a BizTalk Server computer that does not contain an instance of the host will fail.

  Note

  If you want to prevent a clustered BizTalk host from running on or failing over to a particular cluster node, remove the node from the list of possible owners of the clustered resource that is created when you cluster the BizTalk host. You can modify the list of possible owners of a cluster resource using the Windows Server 2008 Failover Cluster Management interface or the Windows Server 2003 Cluster Administrator.
- When clustering a BizTalk host, ensure that the cluster group (Windows Server 2003) or clustered service or application (Windows Server 2008) that you are adding the host to contains a Network Name and IP Address resource. If the target cluster group contains a Network Name and IP Address resource, then the Network Name resource is added as a dependency to the clustered BizTalk host. If these resources are not available, then the BizTalk host will not function correctly as a clustered resource.
- If you unconfigure a BizTalk server/cluster node that is listed as a possible owner of a clustered BizTalk host, the cluster resource for the host instance is taken offline in Windows Cluster. If you need to unconfigure a BizTalk Server computer that is listed as a possible owner of a clustered BizTalk host without taking the cluster resource for the host instance offline, follow these steps:

- In the Windows Server 2008 Failover Cluster Management interface or the Windows Server 2003 Cluster Administrator, fail over the clustered host to a BizTalk Server computer other than the BizTalk Server computer that you will unconfigure.
- In the BizTalk Server Administration console, select the instance of the clustered BizTalk host that corresponds to the BizTalk Server computer which is to be unconfigured.
- Delete the host instance. If prompted with an error choose the option to forcefully delete the host instance.
- Unconfigure BizTalk Server.

- When a BizTalk host is configured as a clustered host, a corresponding cluster resource is created in the specified cluster resource group on the Windows Server 2008 failover cluster or Windows Server 2003 server cluster.

  By default, a clustered BizTalk host resource is configured with the following restart values on a Windows Server 2008 failover cluster which are available on the **Policies** tab of the **Properties** dialog box for the cluster resource:

Option	Value
If resource fails, attempt restart on current node.	**True** The Cluster service will attempt to restart the resource if it fails.
Period for restarts (mm:ss):	**15:00** Specifies the time period during which restart attempts are counted.
Maximum restarts in the specified period:	**1** Specifies the maximum number of restart attempts allowed during the **Period for restarts (mm:ss)** .
If restart is unsuccessful, fail over all resources in this service or application.	**True** The Cluster service will attempt to restart the resource by failing over the entire resource group to another cluster node.
If all the restart attempts fail, begin restarting again after the specified period (hh:mm):	**1:00** Specifies an extended waiting period after which the Cluster service will begin another series of restart attempts.
Pending timeout (mm:ss):	**3:00** Specifies the length of time the resource can take to change states between Online and Offline before the Cluster service puts the resource in the Failed state.

The default restart values dictate that the Windows Server 2008 failover cluster will attempt to restart a failed instance of a clustered BizTalk host instance up to 1 time within a time span of 15 minutes. Since the **If restart is unsuccessful, fail over all resources in this service or application** value is set to **True**, any restart attempts will also fail over the cluster resource group to another cluster node. If a failed instance of a clustered BizTalk host cannot be restarted in the specified number of attempts during the specified time period then the clustered BizTalk host will assume a state of **Failed** in the Failover Cluster Management interface. If a clustered BizTalk host assumes a state of **Failed** then it must be manually started in the Failover Cluster Management.

By default, a clustered BizTalk host resource is configured with the following restart values on a Windows Server 2003 server cluster which are available on the **Advanced** tab of the **Properties** dialog box for the cluster resource:

Option	Value
Restart	**True** The Cluster service will attempt to restart the resource if it fails.
Affect the group	**True** The Cluster service will attempt to restart the resource by failing over the entire resource group to another cluster node.
Restart Threshold	**3** Specifies the maximum number of restart attempts allowed during the **Restart Period**. If the number of restart attempts exceeds the **Restart Threshold** during the **Restart Period** then the cluster resource assumes a state of **Failed** and the Cluster service does not attempt any more restarts.
Restart Period	**900 seconds** Specifies the time period during which restart attempts are counted. The **Restart Period** is initialized upon the first restart attempt. The restart attempt count is reset to zero if the **Restart Threshold** is not exceeded for the duration of the **Restart Period**.

The default restart values dictate that Windows Server cluster will attempt to restart a failed instance of a clustered BizTalk host instance up to 3 times within a time span of 900 seconds. Since the **Affect the group** value is set to **True**, any restart attempts will also fail over the cluster resource group to another cluster node. If a failed instance of a clustered BizTalk host cannot be restarted in the specified number of attempts during the specified time period, then the clustered BizTalk host will assume a state of **Failed** in Cluster Administrator. If a clustered BizTalk host assumes a state of **Failed**, then it must be manually started in Cluster Administrator.

Procedures

To configure a BizTalk host as a cluster resource

1. In the BizTalk Server Administration console, click to expand **BizTalk Server Administration**, click to expand **BizTalk Group [<servername>:<management database>]**, click to expand **Platform Settings**, and then click to expand **Hosts**. The list

of hosts appears under the folder.

2. Right-click the host that you would like to cluster, and then select **Cluster**.

   Note

   Ensure that you have created an instance of the host on all member nodes that are possible owners of a cluster group before adding the BizTalk host to that cluster group.

3. Select the cluster group that you would like to run the host in from the drop-down list of available cluster groups.

   Note

   As soon as a host is clustered, it is brought online and will begin processing documents for any adapter handlers or orchestrations that are configured to run in the host.

To uncluster a clustered BizTalk host

1. In the BizTalk Server Administration console, click to expand **BizTalk Server Administration**, click to expand **BizTalk Group [<servername>:<management database>]**, click to expand **Platform Settings**, and then click to expand **Hosts**. The list of hosts appears under the folder.
2. Right-click the clustered host that you would like to uncluster, and then select **Un-Cluster**.

   Note

   When a clustered host is unclustered, any host instances associated with the clustered host are stopped and the host will stop processing documents for any adapter handlers or orchestrations that are configured to run in the host.

Considerations for Running Adapter Handlers within a Clustered Host

BizTalk host cluster support is available to provide high availability for three of the integrated BizTalk adapters: the FTP adapter, the MSMQ adapter, and the POP3 adapter. Host cluster support is also provided so that there is high availability for running a single instance of an adapter for purposes of ordered delivery.

All of the BizTalk adapter handlers can be run in a clustered host but there is no benefit derived for running adapter handlers in a clustered host except as described below. If your processing requirements do not include any of the scenarios described below, then you should not run adapter handlers in a clustered host.

Running the FTP adapter receive handler within a clustered BizTalk host

For most of the BizTalk Server integrated adapters, high availability can be achieved by creating multiple adapter handlers to run on BizTalk host instances on different BizTalk Server servers within a BizTalk group. FTP adapter receive handlers should not, however, be configured to run in multiple BizTalk host instances simultaneously. This recommendation is made because the FTP receive adapter uses the FTP protocol to retrieve files from the target system and the FTP protocol does not lock files to ensure that multiple copies of the same file are not retrieved simultaneously when running multiple instances of the FTP receive adapter.

To provide high availability for the FTP receive adapter, you should configure the FTP receive adapter to run in a BizTalk host instance that has been clustered.

Running MSMQ adapter handlers within a clustered BizTalk host

To ensure high availability for the MSMQ adapter and to ensure transactional consistency for messages sent or received by the MSMQ adapter, you should do the following:

1. Configure Message Queuing (MSMQ) as a clustered resource in a Windows Server cluster group on your BizTalk Server computers.
2. Add the clustered MSMQ service to the list of Resource dependencies for the clustered BizTalk host. This will ensure that the clustered BizTalk host will always start after the clustered MSMQ service in failover scenarios.
3. Configure the MSMQ adapter send and receive handlers in a BizTalk host instance that has been configured as a cluster resource in the same cluster group as the clustered MSMQ resource.

These steps are recommended for the following reasons:

MSMQ adapter receive handler – MSMQ versions prior to MSMQ 4.0 do not support remote transactional reads, only local transactional reads are supported. In this case, the MSMQ adapter receive handler must run in a host instance that is local to the clustered Message Queuing service in order to complete local transactional reads with the MSMQ adapter.

Important

The MSMQ adapter receive handler requires that a local non-clustered instance of the Message Queuing service is running on the same computer that the receive handler host instance is running on.

MSMQ adapter send handler - To ensure the consistency of transactional sends made by the MSMQ adapter, the outgoing queue used by the MSMQ adapter send handler should be highly available so that if the MSMQ service for the outgoing queue fails it can be resumed. Configuring a clustered Message Queuing resource and the MSMQ adapter handlers in a cluster group will ensure that the outgoing queue used by the MSMQ adapter send handler will be highly available.

This will mitigate the possibility of message loss in the event that the Message Queuing service fails.

Running the POP3 adapter receive handler within a clustered BizTalk host

The POP3 adapter receive handler does not need to be configured to run in a clustered BizTalk host unless the POP3 server that the adapter is reading from allows multiple concurrent connections to be made to the same mailbox. If the POP3 server that the POP3 adapter is connected to permits multiple concurrent connections to its mailboxes, then we recommend that you ensure high availability for the POP3 adapter by configuring a single POP3 adapter receive handler to run in a BizTalk host instance that has been clustered. This recommendation is made to ensure that multiple copies of the same e-mail message are not retrieved simultaneously when running multiple instances of the POP3 receive adapter.

Running a receive adapter that supports ordered delivery with a clustered BizTalk host

The MSMQ and MQSeries integrated adapters provide the ability to submit documents to BizTalk Server in the order that they were received. Correct implementation of this functionality requires that only a single instance of these receive adapters be running at any given time. To provide high availability for a single instance of these adapters, they should be configured to run in a clustered BizTalk host instance.