Installing or Upgrading DMZ Gateway in a Failover (ACTIVE/PASSIVE) Cluster

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- DMZ Gateway, version v3.0 and later
- For other versions of DMZ Gateway, contact Globalscape Customer Support.

DISCUSSION

This article discusses installing DMZ Gateway in a failover cluster and upgrading DMZ Gateway in a failover cluster. This article **DOES NOT** detail configuration for a High Availability (Active/Active) cluster scenario.

Set up DMZ Gateway in a clustered environment using Microsoft Clustering Services or Globalscape's monitoring utilities and achieve high availability through failover clustering.

If you have Microsoft Clustering Service (MSCS) deployed, you can use its built-in Resource Monitor to manage the availability of DMZ Gateway. MSCS can manage DMZ Gateway as a generic service.

Clustering setups vary between operating systems, hardware resources used, and various other factors. If you have never set up a server cluster before, please consult your Windows documentation or the Cluster Administrator help file for detailed instructions on setting up a server cluster prior to proceeding. The focus of these instructions is for setting up DMZ Gateway ***in a pre-existing clustered environment***.

- To find out which hardware is compatible with MSCS, refer to Microsoft's hardware compatibility list.
- To learn more about MSCS, search for "clustering" on the Microsoft Developer Network Library.

Deploying DMZ Gateway in a clustered environment as described in this document is typically the most reliable method to achieve high availability and mitigate down time. For more information specific to clustering with DMZ Gateway, contact Globalscape Customer Support.

Configure the DMZ Gateway Cluster

Perform the steps below to configure clustering *before* setting up DMZ Gateway on

the system.

1. Make sure the hardware is set up correctly and there is a shared disk resource, disk quorum, hub, or switch with Ethernet hookups between the two DMZ Gateways, as well as adapters for the crossover and for outside access, an adequate uninterruptible power supply (UPS) support for each device, and so on.
2. Make sure you install an operating system that supports clustering on each system.
3. Install Active Directory (AD) and configure the domain name service (DNS) on the first node. Choose one of DMZ Gateways to be node 1. The administrator password cannot be left blank.
4. Create an account for the cluster in AD with a non-blank password and assign the account to the Administrators group.
5. Join the second node to the AD domain.
6. Reboot, then log in to the first node with the cluster account.
7. Launch the Cluster Configuration Manager from the **Add/ Remove Windows components** dialog box and create a new cluster.
8. Complete the new cluster creation wizard, providing a name for the cluster and cluster account credentials. Allow it to manage the disk, quorum, and other shared resources. Verify the quorum drive is correct, and select the private network option. Use one adapter for the cluster nodes and the other for the public network. Specify the IP address for managing the cluster.
9. Run the cluster configuration tool on the second node and configure it to be an additional node in the cluster. You will need to provide the cluster name and appropriate cluster account credentials.
10. After you have completed the cluster configuration wizard, verify that the two nodes are set up properly from the cluster administrator dialog box. (To access the cluster administrator, click **Start > Programs > Administrative Tools > Cluster Administrator**.)
11. In the left pane, right-click the **Resources** folder, click **New > Resource**, then specify the shared IP address on which the DMZ Gateways will listen. Note that DMZ Gateway captures the IP address when the DMZ Gateway service starts, so if the IP address is changed after that, the service must be restarted to capture it.

Configure DMZ Gateway to Run in a Clustered Environment

After you install and configure clustering on the system, perform the following procedure to configure DMZ Gateway in the cluster.

1. Install DMZ Gateway on the active node.
2. Specify the installation directory for DMZ Gateway:
   - For **DMZ Gateway 3.0-3.2.x,** select the shared disk drive as the installation directory.
   - For **DMZ Gateway 3.3.x and later**:
     - For the installation files, specify a location local to the server.
     - For the configuration files, specify a shared disk location.
3. When the install completes, launch the product. Connect to DMZ Gateway using the administrator account that you created during installation.
4. Open the **Services** dialog box (in Windows **Administrative Tools**), open the DMZ Gateway service **Properties** dialog box, then switch the startup mode from **Automatically** to **Manual**.
5. Stop the DMZ Gateway service, close the **Services** dialog box, and launch the Cluster Administrator.
6. In the Cluster Administrator, make the second node active: In the left pane, click **Groups**, right-click the appropriate cluster and disk groups, then click **Move Group**. All resources should move from the first node over to the second node so that the second DMZ Gateway installation succeeds. If not, the shared disk will lock for the second node. It may take a few moments for the resources to switch over.
7. Install DMZ Gateway on the second node once it is active (also to the shared directory), following steps above, and then exit the **Services** dialog box without stopping the DMZ Gateway service.
8. Launch the administration interface, connect to the DMZ Gateway service on the second node, and configure DMZ Gateway.

Integrate DMZ Gateway into the Cluster

After you have set up the DMZ Gateway cluster and configured DMZ Gateway to run in a clustered environment, DMZ Gateway configuration is identical for both DMZ Gateways because both are using the same configuration file stored on the shared disk, saving data to the same place, and sharing the same outside-facing IP address.

To integrate DMZ Gateway into the cluster

1. Open the cluster administrator. In the left pane, right-click the **Resources** folder, click **New Resource**, expand the **Create New Resource** list, then click **Generic Services**.
2. Choose both nodes, select all resources as dependencies, then type the exact service name as displayed in the Windows **Services** dialog box (e.g., "DMZ Gateway Server"; it must be exact, including case.) Do not choose to replicate the registry settings.

3. Click **Finish** to add the service as a resource.

Complete Cluster Configuration and Test

After you set up the DMZ Gateway cluster, configured DMZ Gateway to run in a clustered environment, and integrated DMZ Gateway into the cluster, you should have both nodes configured with shared resources, including a shared IP address, disk array, quorum, and two DMZ Gateways.

Perform tests to ensure the system was correctly configured.

1. In the Cluster Manager, right-click the DMZ Gateway Server service, then click **Bring Online**.
2. Open the DMZ Gateway administration interface and verify that it is online.
3. In the Cluster Manager, right-click the DMZ Gateway Server service then click **Bring Offline**.
4. In the DMZ Gateway administration interface, verify that the service has stopped.
5. Cause a failover to confirm the service can be started on each node automatically.
6. Configure the remote server to connect to DMZ Gateway using the cluster IP address (IP address that the cluster shares).
7. Verify that the DMZ Gateway administration interface has a green light (to show that the server has connected).
8. Verify that the failover allows the server to continue to be connected to a DMZ Gateway in the cluster.

Your cluster setup is now complete.



If one DMZ Gateway goes down, you lose any transactions in progress until the failover goes online.

Upgrading DMZ Gateway in a Cluster

To upgrade DMZ Gateway in a cluster

1. Obtain the new installation file(s).
2. Bring down the cluster (from within the cluster manager). It is critically important that

DMZ Gateway service is STOPPED on both nodes!

3. Verify that the DMZ Gateway service is stopped by logging in to each node and inspecting the service control panel. For extra assurance you can change the startup type to **Manual** from **Automatic**. (Make sure to switch it back before you bring the cluster back up in step 7 below.)
4. Run the installer on the first node and select **Upgrade** when prompted.
5. Run the installer on the second node and select **Upgrade** when prompted.
6. If you changed DMZ Gateway service startup to **Manual** in step 4, change it back to **Automatic**
7. Bring the cluster back up.
8. Verify the upgrade was successful:
   a. Verify that DMZ Gateway is running on the primary node.
   b. Disable the primary node and verify secondary node starts up.
   c. Open the DMZ Gateway administration interface and verify that the version number is the same on both nodes (click **Help > About**).

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11114/Installing-or-Upgrading-DMZ-...