GlobalSCAPE® DMZ Gateway v2:

Installing in a Cluster

globalSCAPE®

GlobalSCAPE, Inc. (GSB)

Address:	4500 Lockhill-Selma Road, Suite 150 San Antonio, TX (USA) 78249
Sales:	(210) 308-8267
Sales (Toll Free):	(800) 290-5054
Technical Support:	(210) 366-3993

Web Support: *http://www.globalscape.com/support/*

October 3, 2008

Table of Contents

Installing GlobalSCAPE® DMZ Gateway in a Cluster

The topics below provide the procedures for installing GlobalSCAPE DMZ Gateway in a configuration with Microsoft Clustering Services.

Configuring Clustering with DMZ Gateway

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 at: https://winqual.microsoft.com/default.aspx
- To learn more about MSCS, search for "clustering" on the Microsoft Developer Network Library at: http://msdn2.microsoft.com/en-us/library/default.aspx
- For information about clustering on Windows 2003 Server, review the article "Introducing Microsoft Cluster Service (MSCS) in the Windows Server 2003 Family" at: http://msdn2.microsoft.com/en-us/library/ms952401.aspx
- 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.
- The procedures for configuring EFT Server in a cluster is available in the *online help file*.

Prerequisites for DMZ Gateway in a Clustered Setup

Operating System requirements

Microsoft Clustering Service as available on:

- Windows 2000 Advanced Server name service
- Windows Server 2003 R2 Enterprise Edition
- Windows Server 2003 Datacenter Edition

Hardware and resource requirements

- A complete system for each node of the cluster (minimum of two)
- A shared disk resource such as DAS, or SANS, preferably configured as a RAID-redundant array
- A disk quorum for disk and resource management; a minimum of two adapters per system (one for internal cluster communications, and another for public access)

Skill Set

A systems or network administrator familiar with the organization's structure and skilled in networking, Active Directory (AD), and cluster administration.

First Step: Configure the DMZ Gateway Cluster

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. If available, give Internet access to each system because you will need to activate DMZ Gateway on each node. If you cannot provide Internet access, you will have to activate the product manually (see Activating the Software).
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 as another domain controller. Both nodes must be domain controllers.
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 adaptor 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. Select the **Resources** folder in the left pane, right-click, click **New > Resource**, then create 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.

Next Step: Set Up DMZ Gateway to Run in a Clustered Environment

Set Up DMZ Gateway to Run in a Clustered Environment

*If you are upgrading DMZ Gateway in a cluster, you **MUST** bring down **BOTH** nodes **BEFORE** performing the upgrade. Refer to Upgrading DMZ Gateway in a Cluster instead of this topic.*

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. Select the shared disk drive as the installation directory.
3. When the install completes, launch the product. Connect to DMZ Gateway using the Administrator account that you created during installation.
4. Activate the software in Full or Trial mode. Use your primary serial number if activating the primary node and your backup serial number if activating the backup node.

5. Once activated, exit the Administrator.
6. 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**.
7. Stop the DMZ Gateway service, close the **Services** dialog box, and launch the Cluster Administrator.
8. 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.
9. 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.
10. Launch the Administrator, connect to the DMZ Gateway service on the second node, and configure DMZ Gateway.

Next Step: Integrate DMZ Gateway into the Cluster

Integrate DMZ Gateway into the Cluster

After you have Set Up DMZ Gateway Cluster and Set Up 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, are saving data to the same place, and share the same outside-facing IP.

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 (**GlobalSCAPE EFT Gateway**; It must be exact, including case.) Do not choose to replicate the registry settings.
3. Click **Finish** to add the service as a resource.

Next Step: Complete Configuration and Test

Complete Cluster Configuration and Test

After you Set Up the Cluster, Set Up DMZ Gateway 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 Gateway. Perform tests to ensure the system was correctly configured.

1. In the Cluster Manager, right-click the "GlobalSCAPE EFT Gateway" service, then click **Bring online**.
2. Open the DMZ Gateway Administrator. Verify that it is online.
3. In the Cluster Manager, right-click "GlobalSCAPE EFT Gateway service" then click **Bring Offline**.
4. Verify in DMZ Gateway Administrator that the service is stopped (the play button for the service will become available).
5. Cause a failover to confirm the service can be started on each node automatically.
6. Configure EFT Server to connect to DMZ Gateway using the cluster IP address (IP address that the cluster shares).
7. Verify that the DMZ Gateway Administrator has a green light (to show that EFT Server is connected).
8. Verify that the failover allows EFT 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

If you are upgrading a DMZ Gateway that is part of a cluster, follow the procedures below.

To upgrade DMZ Gateway in a cluster

1. Obtain new installation file(s)
2. Bring down the cluster (from within the cluster manager).
3. It is critically important that DMZ Gateway service is STOPPED on both nodes! 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 8 below.)
4. Run the installer on the first node and select **Repair** when prompted. (Do NOT click **Modify**.)
5. Run the installer on the second node and select **Repair** when prompted. (Do NOT click **Modify**.)
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 Administrator interface and verify that the version number is the same on both nodes (click **Help**, then click **About**).