2018

Cornerstone MFT Server Clustering & Load Balancing

To configure Cornerstone MFT Server in a clustered or load balanced environment.

QuickStart Guide

Clustering & Load Balancing

Did you know that Amazon.com is a clustered & scalable website? As customers access Amazon's website, the network load balancer at the entrance to the cluster monitors the incoming traffic and either parses out the load of visitors to the available servers or launches additional nodes to share the workload on the website.

By storing configuration information in an external SQLServer Database accessible from one or more Cornerstone nodes in a cluster, **Cornerstone can be scaled and clustered to handle an unlimited number of users**. The User Accounts Database can also be stored remotely in an external SQLServer Database—or, in the case of Active Directory/LDAP-based user authentication, on an external server—which is accessible from multiple nodes. Employing an external database to store configuration and user account information creates a fully scalable system where multiple nodes share the workload and allow system maintenance without creating user access limitations.

The following instructions will help you set up Cornerstone MFT for clustering/load balancing support. For additional assistance, refer to the Cornerstone MFT User Guide available online at **http://webdrive.com/products/cornerstone-mft** or SRT's HelpDesk at **http://srthelpdesk.helpserve.com**.

Cornerstone MFT Clustering/Load Balancing Overview

Clustering support is built into Cornerstone and can be easily configured while creating a new server. Simply decide if you would like to create a stand-alone server—the first or 'master' server in a cluster—or add an additional 'slave' server to the cluster.

Key steps to building a Clustered & Scalable Cornerstone Server:

- Dedicate a separate machine to be used as your SQL Database server. This will allow multiple cornerstone nodes to gain access to the consolidated information.
- Store your user data out on a network drive, accessible through a UNC.
- Store your logfiles and any SSL certificates out on a UNC for shared access across the clustered nodes.

Once the multiple servers have been configured, they will all share the same server, user, and group configuration settings.

NOTE: Using a **Load Balancing Utility**, such as Microsoft Load Balancing, will balance the load across multiple servers.

Create your Database, Security Login, and User Login

These instructions assume you are using SQL Server 2005; please refer to instructions relative to your particular database program if you are not using SQL2005.

1. Run the MS SQL Server Management Studio. Right-click on Database and click New Database.

2. Give your database a name and click OK.
3. Expand Security > Logins.
4. Right-click to display the context menu and click New Login.
5. Type a Login name, then use the radio button to select SQL Server Authentication.
6. Clear Enforce Password Policy, and click the dropdown menu to choose the database for login.
7. Expand your newly created database, expand Security under your database, and right-click New User.
8. Type the User Name and click the Browse button to browse to the Login name you created.
9. Select the Database role memberships, **db_owner** and **db_securityadmin**, and then click OK.
10. Close the MS SQL Server Management Studio.

Create your Data Source on your Primary Cornerstone Server

Use the following steps to create your data source on the primary Cornerstone Server, which will connect to your SQL database. You will repeat this process when you create your secondary/member server.

1. Navigate to Start > Administrative Tools > Data Sources (ODBC).
2. Click the System DSN tab and Add.
3. Select SQL Server and Finish. DO NOT press Enter or click Finish, or you will get a silent fail when you create your server cluster.
4. Type the data source name and a description. Type the SQL Server name and then click Next.
5. Click With SQL Server authentication using a login ID and password to be entered by the user. Type your SQL Login ID and Password and click Next.
6. Select Change the Default Database To and use the dropdown arrow to choose your newly created database.
7. Click Next and Finish.
8. Select Test Data Source. If the test does not complete successfully, begin by creating a new data source.
9. If the test is successful, click OK to finish creating your data source.

Create your Primary Cornerstone Server

When clustering Cornerstone servers, best practices indicate that all information which may be shared between cluster nodes should reside on a UNC share accessible by all nodes. If this Cornerstone server will

be accessible from the Internet, in the WAN Address box, enter the public domain name customers/users will need when accessing this server (ie, cornerstone.mydomain.com).

1. Run the Cornerstone Administrator and click the blue computer in the left-hand tree view; this is the domain icon.
2. Under the Local Administration tab, choose a Data Directory and Logfile Directory location on a UNC.
3. Click the New Server button on the menu bar to launch the Site Profile Wizard. On the first screen of the wizard, select "This server will be the primary server in a clustered environment". **For Subsequent CS nodes**, you will select the third option, "This server will be a new member server in an existing clustered server environment". Click Next.

For Your Information

Cornerstone Service runs at a different permission level than a generic logged in user; this means the NTFS Permissions on the UNC Share must take into account the NT User Account being used by the Cornerstone Service. If you are unsure about this process, please contact your Network System Administrator to ensure that the Cornerstone Service has adequate Read/Write permissions to the UNC Share. Failure to do so will cause problems with the cluster.

4. Enter a name and description for this server. For the Data and Logfile Directories, choose a UNC for the data. The information supplied on this screen will also be shared across all Cornerstone cluster nodes. The UNC specified here will also be used by other nodes.
5. Configure security settings according to preference. When you are finished with FTP Services options below, click Next.
    - ◊ To enable FTP Services, check Enable FTP Services and select the FTP Port number by using the up/down arrows.
    - ◊ To enable anonymous FTP access, select the check box.
    - ◊ If your server is sitting behind a router/firewall, select the appropriate check box and type the external WAN address of the router/firewall.
6. Follow the bulleted steps to enable SSL/TLS access on this server. When you are finished configuring SSL/FTPS Security Settings, click Next.
    - ◊ Select the SSL/TLS check box and choose the appropriate sub-option.
    - ◊ Click the dropdown arrow to choose the certificate and select Certificate Management to configure a certificate for this server.
    - ◊ Enter the password associated with the certificate.
    - ◊ Use the "…" button to browse to the Certificate Store Folder.

7. Follow the bulleted steps to enable SFTP (SSH's Secure File Transfer Protocol). Click Next when you are finished configuring SSH/SFTP Security Settings.
    - Select the SFTP check box and choose the SFTP port (default port 22) using the up/down arrows.
    - Choose the host key set by using the dropdown arrow.
    - Click Host Key Management for host key configuration options, type the password associated with the host key, and click the browse "…" button to browse to the Host Key folder.
8. Type the URL or IP address of the SMTP mail server that will be used to send email notifications to users. When you are finished testing the connection, click Next.
9. Click Finish to create the server.
10. Create a test user on your primary server using the New User Wizard.

Create your Member/Secondary Clustered Server

To create your secondary cluster/member server, repeat the process outlined above on your secondary/member server with one exception: designate this server as a member server. You will need to **point to the data source you just created** instead of creating a new data source.

1. Expand your secondary server domain and select New Server Wizard.
2. Choose "This server will be a new member server in an existing clustered server environment" radio button and click Next.
3. Click Machine Data Source and highlight the data source created for your primary cluster server. Click OK.
4. Type your SQL Login ID and Password.
5. Check your parameters and click Test. Click OK if successful and then click Next.
6. Highlight your primary server and click Next. Click Next again, and then click Finish.
7. Make sure your primary Cornerstone server is running and start your start your secondary/member server.
8. Expand Users and make sure the test user you created on your primary server appears.

If your user appears, you have successfully created a Cornerstone MFT cluster. You can use a NLB (Network Load Balancing) Server on the front end of this cluster if you wish to use Load Balancing.

System Requirements

Supported Operating Systems

- Windows Server 2012, all editions, 32-bit and 64-bit
- Windows Server 2008-R2, all editions, 32-bit and 64-bit
- Windows Server 2008, all editions, 32-bit and 64-bit
- Windows Server 2016, all editions, 32-bit and 64-bit

Minimum Hardware Requirements

- 2 GHz Pentium® class processor
- 4GB of RAM is required; 8GB of RAM is recommended
- Minimum 100MB of free disk space for the application
- Minimum SVGA (800x600) resolution display is required to run the Administration console program.

Minimum Software Requirements

- Microsoft .NET Framework v4.0 is required
- Microsoft SQL Server 2005 or later is required
- Microsoft SQL Server Management Studio Express is recommended

Limitations

- Cornerstone MFT server is a multi-threaded, dynamic server solution for the Microsoft Windows operating system. While designed to handle an unlimited number of user connections and servers, like all software, Cornerstone is limited by the resources of the computer; most notably, those limitations imposed by the Windows Sockets (WINSOCK) Library.

About South River Technologies

South River Technologies (SRT) is an innovator in secure file management software. SRT software allows users to securely access, manage, and collaborate on files over the Internet, streamlining business processes to improve productivity. SRT's products enhance customers' existing applications by instantly enabling secure access and collaboration within those applications. More than 90,000 customers in 140 countries use SRT's software to make remote file access and collaboration more efficient for their customers, partners, and distributed workforce.

For more information, please visit www.southrivertech.com. South River Technologies, Cornerstone MFT, Titan FTP Server, WebDrive, and DMZedge Server are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. Any information in this document about compatible products or services should not be construed in any way to suggest SRT endorsement of that product or service.

Contact Information

South River Technologies, Inc.
1910 Towne Centre Blvd
Suite 250
Annapolis, Maryland 21401
USA

Toll Free: 1-866-861-9483
Main: 443-603-0290
Fax: 410-266-1191
Corporate Web site: www.southrivertech.com
Online Support: www.srthelpdesk.com