Disaster Recovery Recommendations and Best Practices

THE INFORMATION IN THIS ARTICLE APPLIES TO:

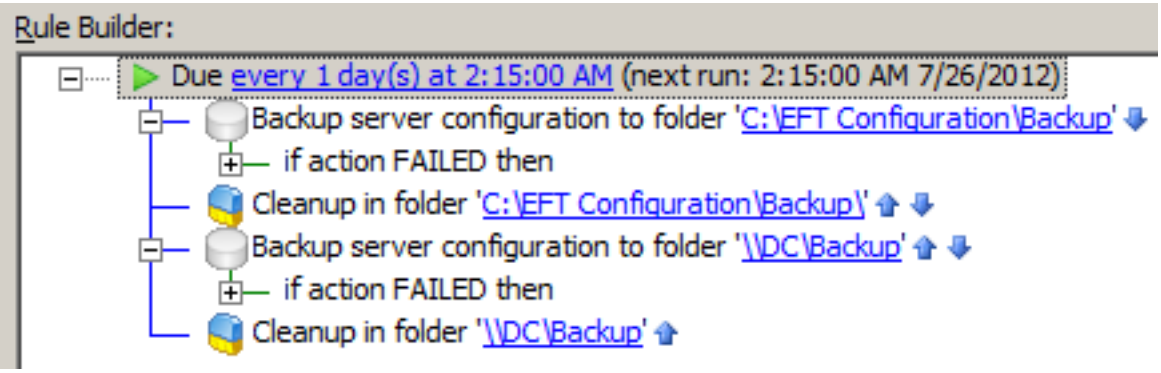
- EFT all versions

DISCUSSION

The EFT User Guide provides guidelines for installing, configuring, and deploying EFT Server in a production environment, including best practices for configuration and security. A checklist for EFT is available at https://kb.globalscape.com/KnowledgebaseArticle11312.aspx. Other disaster recovery recommendations and best practices are described below.

EFT Configuration:

EFT Enterprise has the built-in ability to automatically back up its configuration to a single backup file that can be saved anywhere. For example, here's a simple scheduled task in EFT Enterprise to back up its configuration both locally and to a remote server that is accessible through a UNC path (to which the EFT service account has access).



The Cleanup actions are there to remove old configuration backups that are no longer necessary (perhaps they're considered obsolete after 7 days, 30 days, whatever period of time is desired) so that you avoid accumulating a large number of old files and waste space. Backups can be taken manually if desired by clicking **File > Backup Server Configuration**. In the DR environment, you can restore the configuration from the latest backup either manually by clicking **File > Restore Server Configuration** or automatically using the COM API to assist in the disaster recovery process and help reduce the chance of human error.

Disaster Recovery Recommendations and Best Practices

General recommendations are universal, not necessarily specific to EFT. For example, use host names whenever possible in the configuration, NOT an IP address, as the IP addresses in the DR environment will not generally be the same. If you need to address a SQL Server, for example, do so by name, not IP address. If an EFT Site is configured to connect to a DMZ Gateway, address DMZ Gateway by name. Using the host name allows the local DNS at any Site to point to the appropriate local IP address, requiring minimal (if any) changes to the EFT configuration. If for some reason DNS is too difficult to manage, the option of using the "hosts" file on the EFT computers remains an option.

Databases: EFT does not do any database server backup or restoration. A proper database replication solution is recommended. As long as EFT has the appropriate configuration and access to working database servers, and as long as the database servers in the DR environment are configured correctly with the same database name and tables, starting up the EFT service in the DR environment will not encounter problems. It will simply begin writing to the configured database as usual. It does not care whether old data is present, though of course you cannot report on data that doesn't exist in the database. If data is replicated to the DR, reports will continue to be generated as usual and contain the desired information.

User Data: EFT does not replicate or keep current any backup directories for user data. A proper file replication solution is recommended. As noted in the above referenced documentation, when restoring a Site, EFT can optionally recreate the directory structure, if necessary, but the files that existed within the users' directories will not be backed up or restored by EFT. Remember that if you have any Virtual Folders created in the Virtual File System (VFS) that are using UNC paths to shares on the network, those shares must exist and be available in the DR environment. If they are not, those Virtual Folders will not work correctly; the client will receive a failure if they try to browse to them, or if the user's home folder is a Virtual Folder or within a Virtual Folder that is inaccessible, they may encounter an error when logging in.

Refer to "Backing Up or Restoring Server Configuration" in the online help for your version of EFT.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11100/Disaster-Recovery-Recommenda...