globalscape
by HelpSystems

Globalscape EFT System Architecture Guide

Table of Contents

Introduction

Globalscape EFT is a managed file transfer solution that streamlines the exchange of data between your systems, employees, customers, and trading partners. It provides a single point of control with extensive security settings, workflow management, detailed audit trails, and reports.

The intuitive EFT interface and comprehensive workflow features help to eliminate the need for custom programs/scripts, single-function tools, and manual processes. This innovative solution reduces costs, improves the quality of your file transfers, and helps your organization comply with data security policies and regulations.

EFT can be installed as a standalone deployment with one server (which can have multiple sites/IP addresses) or in a variety of more complex options, including cloud deployments, depending what you need to accomplish.

With integrated support for clustering, EFT can process high volumes of file transfers for enterprises by load balancing processes across multiple nodes. The clustering technology in EFT also provides active-active automatic failover for disaster recovery.

EFT can be scaled horizontally by adding additional systems to the cluster. When paired with a load balancer, inbound connections to file servers can be distributed to the available systems in the cluster. As your business and transfer requirements grow, EFT can easily grow with it by adding additional servers to the cluster.

This guide includes several EFT different architectures, including support for high availability (clustering) and load balancing, and summarizes the advantages of each configuration.

Standalone EFT Server

In this architecture, a single EFT server instance is installed behind the front-end firewall. If file transfer services are enabled, ports to the HTTP/S, FTP, FTPS, SFTP, and AS2 protocols are opened on the firewall to allow all inbound connections to EFT.

Figure 1 Standalone EFT Server

The default standalone system uses the installed EFT database files and (optionally) SQL or Oracle database inside the private network. EFT includes an automated backup and cleanup event rule in case of application failure.

Figure 2 Standalone EFT Server with DMZ Gateway

An optional DMZ Gateway® can be installed in the demilitarized zone (DMZ) to provide secure communication with EFT behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ.

Requisites

- 1 EFT
- Database server (optional)
- 1 DMZ (optional)

Benefits

- Ideal for small organization where high availability is not needed

Development & Test

HelpSystems recommends that customers purchase an additional Globalscape EFT license for development and/or testing purposes. This extra license is helpful for providing change control and quality assurance of new workflows that you build in Globalscape EFT. It will also allow you to test new releases/patches provided by HelpSystems in an isolated environment.

Globalscape EFT allows authorized administrative users to export workflows, schedules, and other items from a development/test environment and import them into production. EFT server and site configuration, stored in .db files, can be exported and imported using a tool such as SQLite.

HelpSystems recommends load testing in staging environments for definitive settings that meet your organization's requirements.
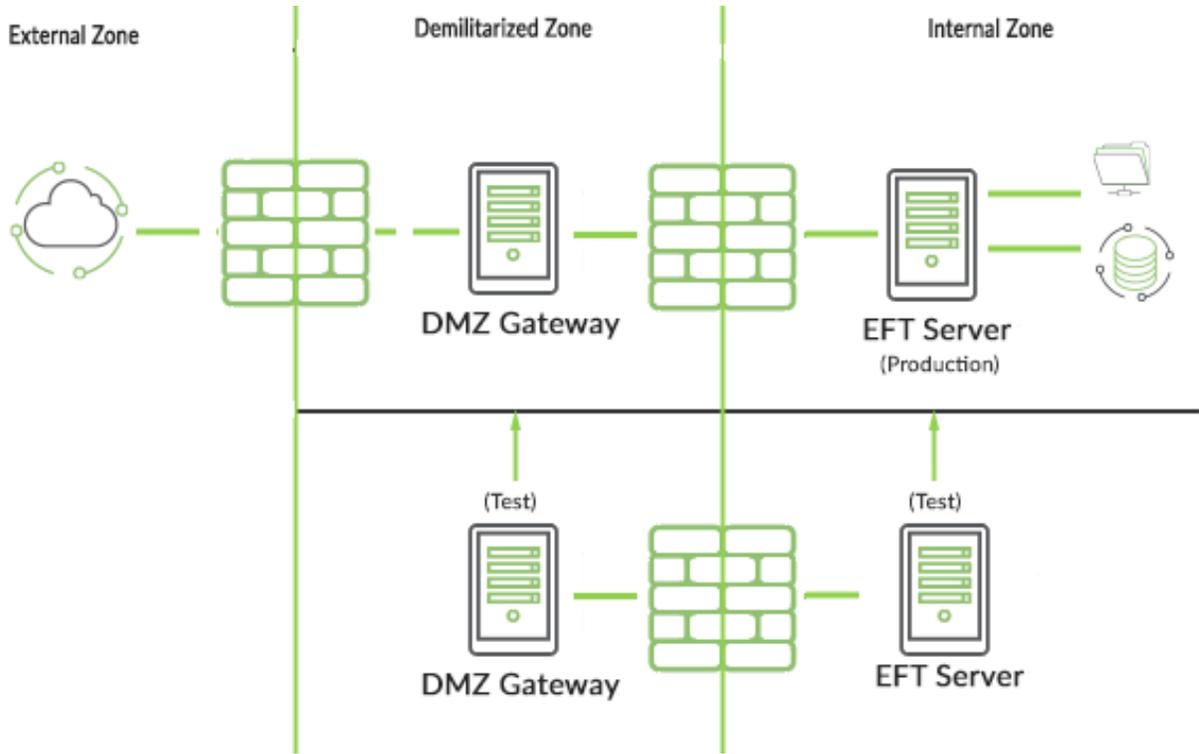

Figure 3 Development & Test environment

High Availability Environments (Clustering)

A group of tightly coupled computers that work together closely so that they can be viewed as though they are a single computer is a "cluster." A failover cluster has redundant nodes that are used to provide service when redundant system components fail.

EFT High Availability (HA) solution can protect your critical business processes and ensure that crucial file transfer systems are always on, and that employees, customers, and business partners experience seamless availability of critical applications and information.

EFT with HA can:

- Maintain availability through any planned or unplanned outage

- Increase stability and flexibility by implementing multiple nodes of EFT for load balancing

- Enhance throughput and better meet important SLAs by deploying multiple nodes of EFT to allow the collective environment to use more available resources

- Improve scalability with the ability to share common configurations across nodes, eliminating the challenge of having multiple servers set up with different configurations

In a clustered environment, two or more EFT servers within a cluster can access the same product database and user files at the same time. Clustering allows these systems to share security settings, user accounts, configurations, audit logs, and other product tables. If one EFT node fails, the remaining nodes in the cluster will automatically continue to process workloads and file transfer requests.

What's the difference between active-active and active-passive load balancing?

- An active-active cluster is typically made up of at least two nodes, both actively running the same kind of service simultaneously. The main purpose of an active-active cluster is to achieve load balancing. Load balancing distributes workloads across all nodes to prevent any single node from getting overloaded. Because there are more nodes available to serve, there will also be a marked improvement in throughput and response times.

- Like the active-active configuration, active-passive also consists of at least two nodes. However, as the name "active-passive" implies, not all nodes are going to be active. In the case of two nodes, for example, if the first node is already active, the second node must be passive or on standby. The passive (a.k.a. failover) server serves as a backup that's ready to take over as soon as the active (a.k.a. primary) server gets disconnected or is unable to serve.

The clustering configurations described below include Active-Passive, Active-Active, and Active-Active for Disaster Recovery.

EFT Active-Passive Cluster

EFT Active-Passive Cluster is a high availability solution that provides very fast automatic failover in a case of application failure or node failure.

Requisites for EFT Cluster Mode (Active-Passive)

- Load Balancer (if using DMZ Gateway)
- MSMQ Multicast (configuration coherence, heartbeat, event rules coordination)
- Highly Available File Storage (NAS) (same datacenter)
- Database Server (Optional)
- EFT is configured for Active/Passive using failover in Event Rules
- 1 EFT Production license
- 1 EFT Standby license
- 1 DMZ Production license
- 1 DMZ Standby license

Benefits

- Highly Available End points (Inbound/outbound) and automation
- No downtime for OS patching and rebooting
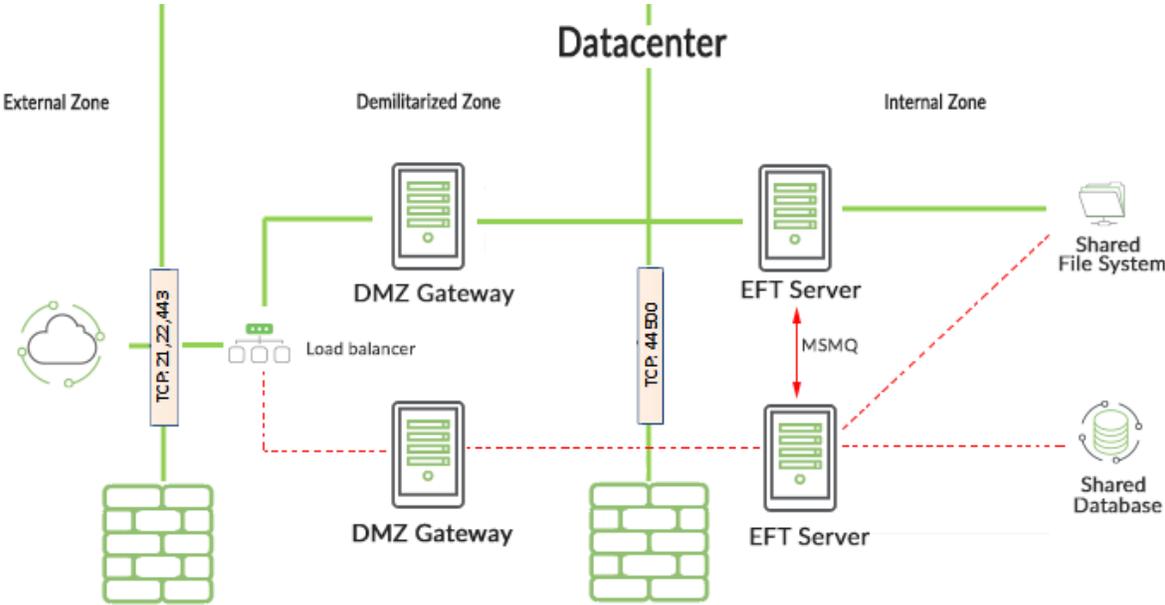- Automatic failover

Figure 4 EFT Active-Passive Cluster

EFT Active-Active Cluster

EFT's active-active deployments provide HA using multiple instances of EFT and a load balancer for non-stop availability of your network. And unlike active-passive failover clusters, all of the nodes in EFT's active-active deployment are put to work in production—with no standby hardware, and no clustering software. In this architecture, EFT is clustered with 2 or more servers for high availability, and the systems are installed in the private network. Associated DMZ Gateways are installed in the DMZ and no inbound ports are opened to the private network. The product and user files share configuration across each system/node in the cluster. A load balancer provides load balancing for incoming connections to DMZ Gateway, and the clustered EFT servers distribute the project workloads evenly across each node in the cluster.

Requisites for EFT Cluster Mode (Active-Active)

- Load Balancer (if using DMZ Gateway)
- MSMQ Multicast (configuration coherence, heartbeat, event rules coordination)
- Highly Available File Storage (NAS) (same datacenter)
- Database Server (Optional)
- 2 EFT Production licenses
- 2 DMZ Gateway Production licenses (if using DMZ Gateway)

Benefits

- Highly Available End points (Inbound/outbound) and automation
- Scale out with load balancing traffic and automation processing
- Scale out up to 16 nodes (usually in the same datacenter)
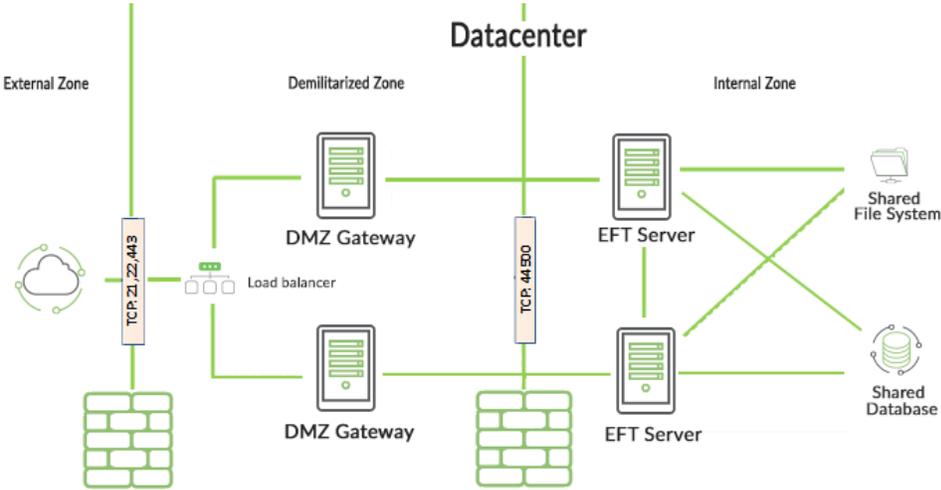- No downtime for OS patching and rebooting

Figure 5 EFT Active-Active cluster

EFT Active-Active Cluster HA + Disaster Recovery

EFT's active-active deployments provide HA using multiple instances of EFT and a load balancer for non-stop availability of your network. Unlike active-passive failover clusters, all of the nodes in EFT's active-active deployment are put to work in production—with no standby hardware, and no clustering software.

In this architecture, EFT is clustered with two or more servers for high availability, and the systems are installed in the private network. Associated DMZ Gateways are installed in the DMZ, and no inbound ports are opened to the private network. The product and user files share configuration across each system/node in the cluster. A load balancer provides load balancing for incoming connections, and the clustered EFT servers distribute the project workloads evenly across each node in the cluster.

Benefits

- Highly Available Endpoints (Inbound/outbound) and automation
- Scale out with load balancing traffic and automation processing
- Disaster Recovery
- Scale-up to 16 nodes on each data center
- No downtime for OS patching and rebooting
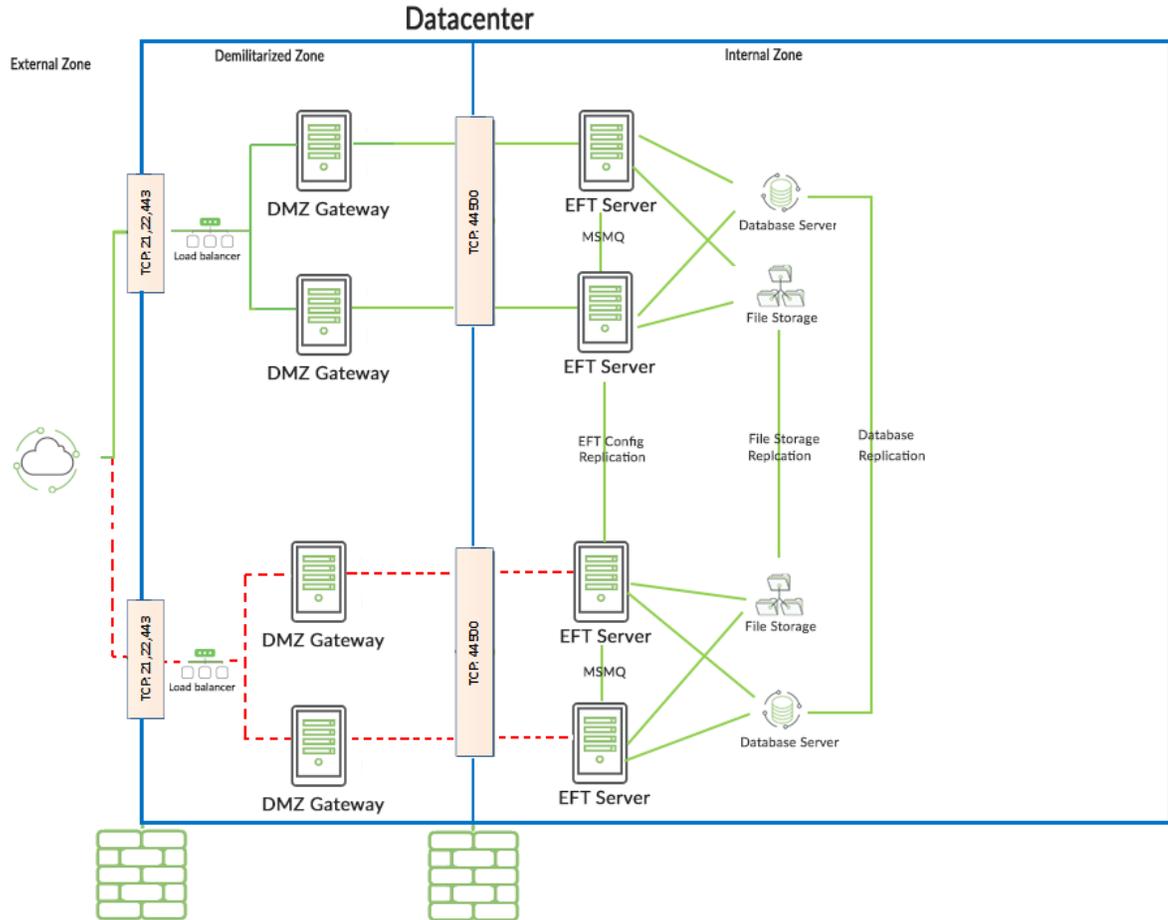
EFT Active-Active Cluster HA + DR

Figure 6 EFT Active-Active Cluster Disaster Recovery

Requisites for EFT Cluster HA Mode (Active-Active) + DR

- Global Load Balancer or DNS manager for failover
- Load Balancer
- MSMQ Unicast (configuration coherence, heartbeat, event rules coordination) between all nodes in both data centers
- Highly Available File Storage (NAS) with synchronous file replication across data centers among all nodes of each cluster for EFT HA Share Config and EFT share users' home folders is required
- Database HA Server Cluster across data centers
- 2 EFT and 2 DMZ Production licenses
- 2 EFT and 2 DMZ Standby licenses
- DR Failover is achievable by manual failover procedure on EFT and its dependencies

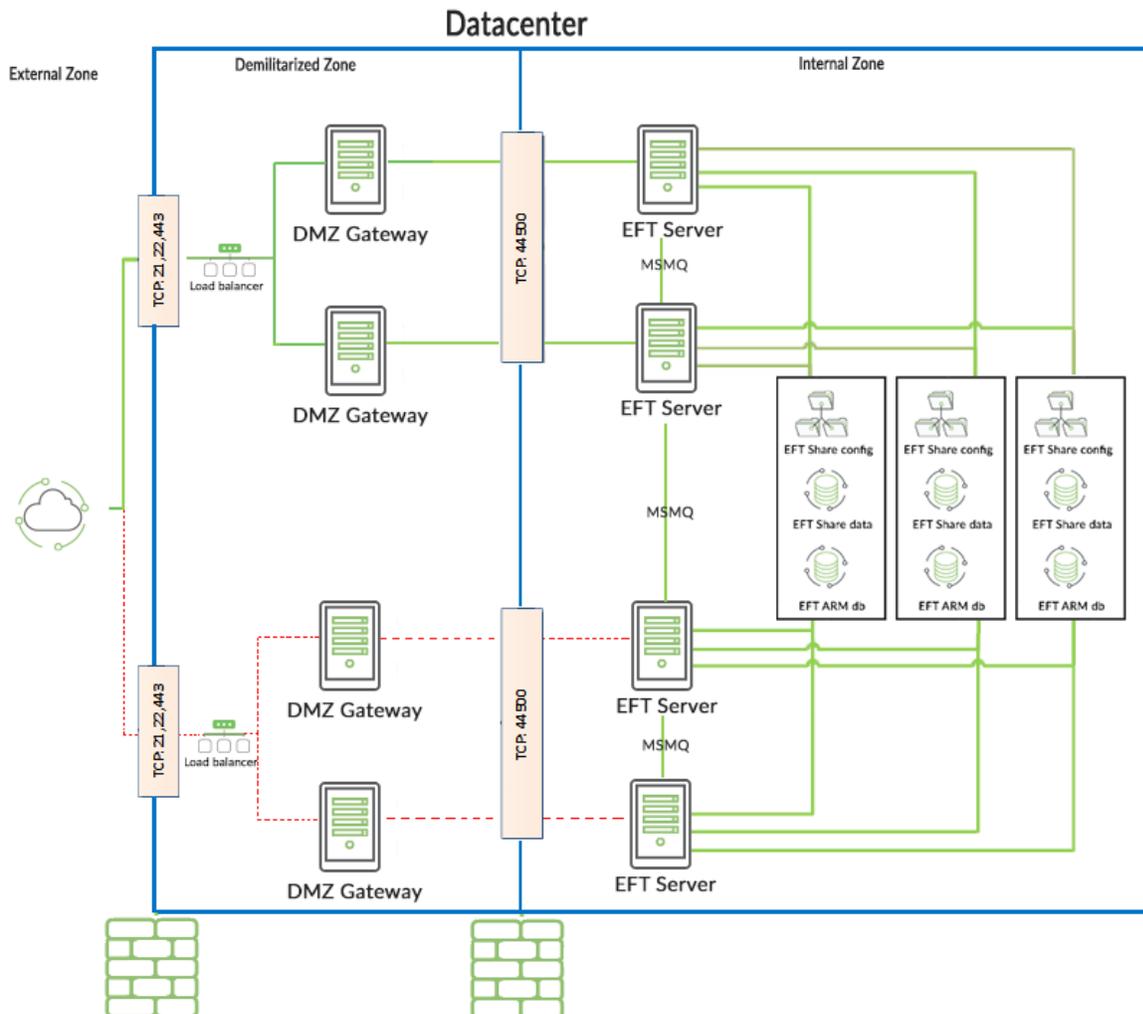# EFT Active-Active Cluster HA Mode + DR (Mission Critical)

Figure 7 EFT Active-Active Cluster Disaster Recovery Mission Critical

Requisites for EFT Cluster HA Mode (Active-Active) + DR (Mission Critical):

- Global Load Balancer or DNS manager for failover
- Load Balancer
- MSMQ Unicast (configuration coherence, heartbeat, event rules coordination) across each data center
- Enterprise Highly Available File Storage (NAS) with synchronous file and locks replication between data centers for EFT HA share config and EFT share users' home folders among all nodes of are required
- Database Server (Optional) with database replication technologies
- 2 EFT and 2 DMZ Production licenses
- 2 EFT and 2 DMZ Standby licenses
- DR Failover is achievable automatically if all EFT dependencies support it (database, storage, and Load Balancer)

EFT in the Cloud

With a self-managed cloud deployment of Globalscape EFT, companies can enjoy the benefits of the cloud, including scalability, flexibility, and affordability, while reducing the size of their own data centers. By minimizing their software costs, number of data servers, and other related resources, organizations can significantly decrease IT expenses without reducing IT capabilities.

Deploying EFT through a cloud platform allows you to securely transfer data to and from the cloud. Deploying EFT in cloud platorm requires that you buy an EFT license and then install it on your own cloud instance (e.g., in Google Cloud Platform, Microsoft Azure, or Amazon Web Services), designed however you need it. You install it, you manage it, and you are in control of your data.

Businesses that use the cloud benefit from high utilization and smooth transactions, ready to handle operational workload peaks and valleys. These companies also see improvements with operational efficiency, reduced overhead costs, enhanced agility, and rapid deployment readiness.

Additionally, if you already have an on-premises installation of EFT and the Cloud Connector module, you can configure automated cloud storage monitoring for Google Drive, AWS S3 buckets, and Azure Blobs, and support for automation processes such as uploading or downloading files to/from that cloud storage.

Globalscape's "Bring Your Own License" (BYOL) model allows you to pay once to purchase licenses that include all of the EFT features you want. You can deploy the license on-premises, in a private cloud, or any public cloud of your choice. Globalscape also offers a subscription license which would ensure that your EFT installation is always the most up-to-date version with the latest security updates.

A cloud MFT deployment supplements your EFT platform with:

- Easy trial experience
- Extensive global footprint with multiple regions around the world
- Strong service-level agreements
- Automate data exchanges between people and systems
- Gain visibility into the movement of files
- Replace legacy, or homegrown file sharing systems
- Securely share files internally or externally
- Enable compliance with corporate, industry, and government mandates
- Ensure uptime of your mission-critical infrastructure
- Additional cloud-service tools and services such as load balancing, storage redundancy, replication to a second region, site recovery, automatic OS image upgrade, security patching, and others

The cloud services are described below.

Microsoft Azure:

Globalscape EFT is certified compatible with Microsoft Azure. In Azure, you can configure a virtual machine (VM) with the latest Windows operating system, then install and configure EFT (as a single server) and any EFT modules that you have licensed. After EFT is installed and configured, you can connect to it as you would any other EFT installation. During the Azure setup, you configure the DNS location to which users and other servers can connect, such as myeftserveronazure.com.

Availability zones expands the level of control you have to maintain the availability of the applications and data on your VMs. An Availability Zone is a physically separate zone, within an Azure region. There are three Availability Zones per supported Azure region. Each Availability Zone has a distinct power source, network, and cooling. By designing your solutions to use replicated VMs in zones, you can protect your apps and data from the loss of a data center. If one zone is compromised, then replicated apps and data are instantly available in another zone.

Microsoft recommends that two or more VMs are created within an availability set to provide for a highly available application and to meet the 99.95% Azure SLA. Combine the Azure Load Balancer with an availability zone or availability set to get the most application resiliency. The Azure Load Balancer distributes traffic between multiple virtual machines.
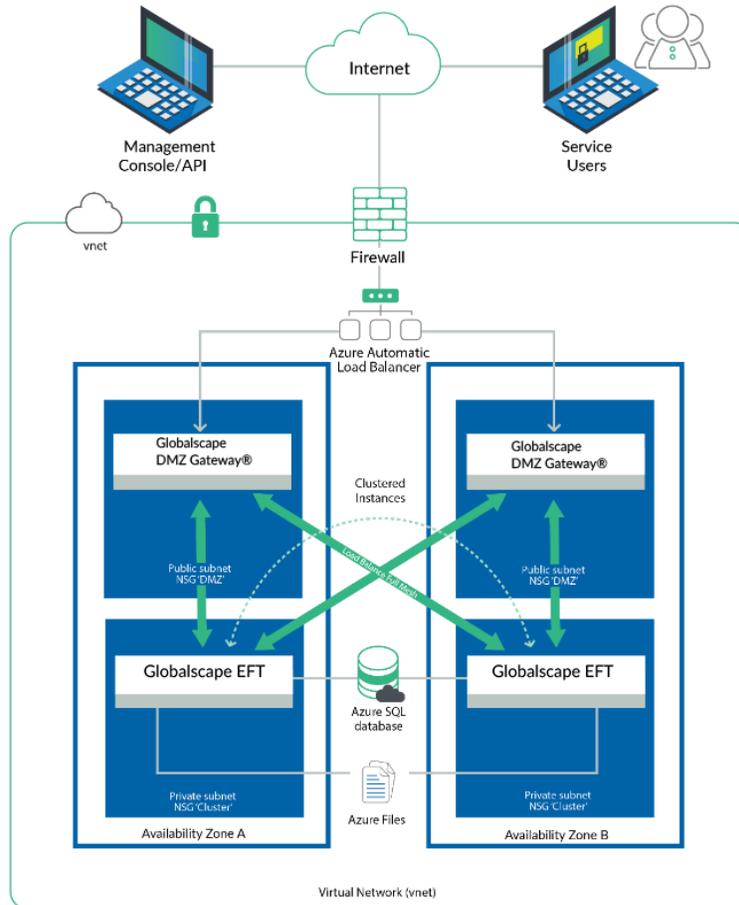
Figure 8 EFT in Microsoft Azure

Amazon AWS:

Leverage the Amazon AWS infrastructure to power your managed file transfer system, Globalscape EFT. With Globalscape EFT deployed in AWS, IT teams can use the industry-leading services and tools available in AWS.

With a self-managed deployment model, you can leverage your own resources to manage your infrastructure. The EFT BYOL license can be installed on an Amazon Machine Image (AMI) in the Amazon Marketplace. With this deployment model you can decide which AWS instance size to run the AWS AMI based on the demands of your business. EFT will be able to provide intra- and inter-region high availability when deployed across multiple Availability Zones (AZ), thus providing more protection against failures in case of a single zone outage.
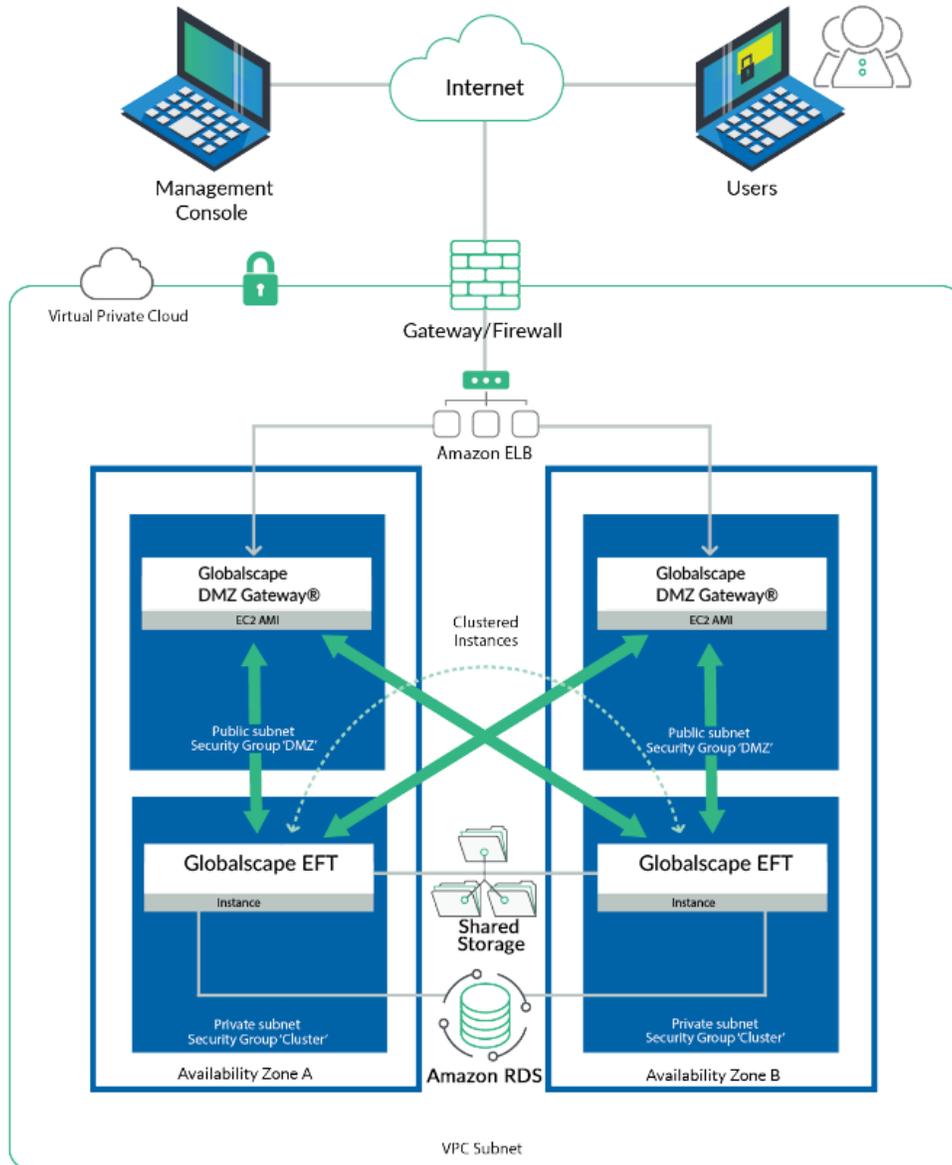
Figure 9 EFT in Amazon AWS

Google Cloud Platform (GCP)

You can install EFT on the Google Cloud Platform Compute Engine and manage it with the Google Cloud console. Google's "Confidential Computing" provides protection of data in use with secure isolated environments that prevent unauthorized access or modification of applications and data while they are in use. Google's end-to-end encryption, that is, encryption at rest, encryption in transit, and encryption in use, protects your data while being stored, moving, and processing.

Like AWS and Azure, Google has multiple, world-wide activity zones to keep you connected against failures in case of a single zone outage. Load balancing, a fully managed SQL server database, and numerous monitoring and management tools can complete the perfect GCP solution for your organization.

Note: Windows Server images on GCP are premium images; using them results in additional charges, not included with the GCP Free Trial.

References

For assistance installing and configuring your self-managed EFT installation in the cloud, refer to the following articles or ask your account manager about Professional Services.

- [EFT Running on Azure in the Cloud](#)
- [Enable Azure AD SSO with EFT Arcus and the Web Transfer Client](#)
- [Amazon EC2 Instance Deployment Guide for Standalone EFT POC](#)
- [AWS EFT Usage Instructions](#)
- [Google Cloud Platform (GCP)](#)
- [Google Cloud Official Icons and Solution Architectures](#)