High Availability Clustering in a Microsoft Windows Environment

VERITAS Cluster Server™ for Microsoft® Windows NT®
Table of Contents

High Availability Solutions for Applications and Data ................................................. 1
A Brief Guide to Clustering .............................................................................................. 2
The Evolution of Clustered Systems ................................................................................ 3
VERITAS Cluster Server ................................................................................................. 4
Configuring VERITAS Cluster Server Clusters and Applications for High Availability ... 4
  Configuring the Network and Storage – Cluster Server Hardware Requirements ...... 4
  VERITAS Cluster Server Communication Channels ................................................. 6
Configuring Cluster Server Components ................................................................. 8
Resources ......................................................................................................................... 8
Service Groups ................................................................................................................ 9
Dependencies ................................................................................................................... 9
Controlling and Monitoring Resources ....................................................................... 10
The Cluster Manager Console ....................................................................................... 13
Monitoring Clusters ....................................................................................................... 13
Resource View ............................................................................................................... 15
Service Group View ....................................................................................................... 15
Heartbeat View .............................................................................................................. 15
Complementary Products ............................................................................................ 16
Summary ......................................................................................................................... 17
High Availability Solutions for Applications and Data

A constant requirement in today’s dynamic computing environments is the need for continual access to applications and data. Customers, partners, suppliers, and employees expect databases, mission critical applications and other resources to be available 24x7. The demand on system, network, application and database administrators to deliver high availability (HA) solutions has never been greater.

Successful organizations today need high availability solutions because downtime – when applications and data are unavailable to users – is extremely costly. A 1999 study by IDC (International Data Corporation) estimates that lost revenue associated with an application outage averages $1,000 per minute for a typical messaging system. Internet banking and e-commerce application outages can cost $7,000 to $10,000 per minute. Regardless of the application (Microsoft Exchange, Microsoft SQL Server, Oracle, etc.) or the environment (Windows, UNIX or other), the cost of downtime is significant.

Downtime is classified as either planned or unplanned. A significant percentage of system downtime is planned downtime – the time the system is taken down by administrators to perform regular system maintenance, backups, etc. Unplanned downtime is caused by many factors: applications, hardware, or errors introduced by people using the systems can cause systems to unexpectedly fail. Creating HA systems to suit the business requirements of an individual organization requires reducing both planned and unplanned downtime. This requires careful planning, as well as both hardware and software elements selected to meet the specific needs of an HA plan.

The purpose of this white paper is to provide an overview of VERITAS Cluster Server™ for the Microsoft® Windows NT® operating system – application availability management software that, as a stand-alone solution, protects against application downtime and also functions as a critical part of an overall HA plan. VERITAS Cluster Server is a highly scalable clustering solution that monitors and controls the availability of applications running in a cluster, and restarts applications in response to a variety of hardware or software faults. A highly scalable solution – allowing up to 32 nodes within a single cluster – VERITAS Cluster Server is currently available for Windows NT, as well as Solaris and HP-UX platforms.
A Brief Guide to Clustering

Achieving high availability in a Windows environment today involves many areas, or layers, in the data center. Storage, storage infrastructure, servers, networking components and applications all need to be available so end users can access required applications and data. Clustering is a critical piece in the overall HA strategy. Through clustering, organizations can achieve high levels of system reliability (availability), increased processing power (scalability), and simplified administration of IT assets (manageability). In addition, clustering can reduce the cost of ownership based on server consolidation and use of virtual servers.

Clustering comes in many forms, including:

- **Failover clusters**, like VERITAS Cluster Server, contain multiple servers connected to each other and storage devices. Servers, or nodes, in the cluster, communicate with each other, and if one node fails, applications running on that node fail over to run on healthy nodes.

- **Parallel processing** (also called distributed processing) can provide high availability and increased performance for applications, but in a different way than failover. Parallel processing divides a large task into many smaller tasks, and executes the smaller tasks concurrently on several nodes. As a result, the larger task completes more quickly.

- **Load-balancing clusters** can be either software- or hardware-based. In a software-based “load-balancing” cluster, incoming requests are distributed among multiple nodes running the same programs. Each server in the cluster is able to handle requests, and if a server or component fails, requests can be redistributed between remaining servers. Load-balancing hardware distributes traffic to multiple servers in a similar fashion.

Clustering and high availability are occasionally confused with *fault tolerance*. A fault-tolerant system contains replacement (spare) hardware components that are always online and running in conjunction with the primary system. In the event of a failure on the primary system, the replacement system can immediately take over. While fault tolerance does provide a high availability solution, it does so at considerable cost and requires a specially modified operating environment.
The Evolution of Clustered Systems

Clustering is an evolving discipline. Traditional failover systems allow for two servers (or nodes) in a cluster. A primary node hosts a highly available application like Exchange or SQL Server, and a secondary node (a “hot standby”) only takes over running the application when a failure on the primary node occurs. While this scenario does provide HA, these traditional systems have limited scalability, and the required 100 percent hardware redundancy for the secondary system is costly.

VERITAS Cluster Server provides next-generation failover technology, where multiple nodes (up to 32 in a Cluster Server cluster) communicate together to ensure that clients maintain continual access to applications and data. Because Cluster Server allows many systems to monitor each other simultaneously, if any one system goes down, there are multiple systems available that can take over the applications and services that were running on the failed system. Finally, for easy administration, the Cluster Server management graphical user interface (GUI) provides a central, cross-platform interface from which administrators can monitor and manage multiple clusters. Cluster Server is also tightly integrated with other VERITAS online storage management products, such as VERITAS Volume Manager™, which is described later in this paper.

High Availability Definitions

**Failover:** The process by which services that were running on one node are moved to another node or nodes in a cluster.

**Heartbeat network:** In a failover configuration, the heartbeat network allows two systems to communicate privately with each other. Heartbeats are signals that are sent periodically from one system to another to verify the systems are active.

**Private disks:** The private disks contain a system's operating system and other unshared files.

**Public disks:** Also known as shared disks. Public disks are switched from one server to another during a failover.

**Public network:** The network over which a server contacts its clients.

**SAN:** Storage area network. A modern, high-speed model for connecting storage devices (disks and tape drives) to the systems that need their resources.

VERITAS Cluster Server

VERITAS Cluster Server provides high availability through automated or manual failover of applications and services. Key features of VERITAS Cluster Server include:

- Extreme scalability (up to 32 nodes in a cluster). A single standby system can protect the availability of dozens of servers in a cluster. This scalability and flexibility reduces the cost of high availability to as low as three to five percent of total system cost, and ensures business continuity at a significantly reduced cost compared to traditional two or four node static failover solutions.

- Support for mixed environments. Windows NT, Solaris and HP-UX are supported today. Support for additional operating systems is planned. Because Cluster Server is a cross-platform solution, administrators only need to learn one clustering technology to support multiple environments.

- A new approach to managing large server clusters. Through its Java-based graphical management interface, administrators can manage large clusters on multiple platforms automatically or manually, and migrate applications and services among them.

- Supports for all major third-party storage providers and works in both traditional client/server and SAN environments. VERITAS provides ongoing testing of storage devices through its own Interoperability Lab (iLab) and Storage Certification Suite – a self-certifying test for third-party vendors to qualify their arrays.

- Flexible failover possibilities. 1:1, Any:1, 1:Any and cascading failovers are possible. Various failover policies are available and can be configured per service group.

- Seamless integration with other VERITAS products (including VERITAS Volume Manager for Windows NT) to increase availability, reliability, and performance.

- Simplified disaster recovery by a small sized, redundant configuration.

- Support for all applications. Cluster resources are extremely customizable, and versatile enough to cluster almost any non cluster-aware application. An open API is available for customer agent development and agents can be developed in a variety of languages including C, C++ and Perl.

Configuring VERITAS Cluster Server Clusters and Applications for High Availability

The basic steps for setting up a VERITAS Cluster Server cluster are below. The subsequent sections provide detail about the components and processes involved at each step.

- Configuring the network and storage — Cluster Server hardware requirements
- Configuring Cluster Server communication channels
- Configuring VERITAS Cluster Server components
- Controlling and monitoring resources

Configuring the Network and Storage – Cluster Server Hardware Requirements

Today, VERITAS Cluster Server supports applications running in a Windows NT 4.0 environment. The product is being extended to support Windows 2000. Cluster Server requires the standard Server version of Windows NT 4.0, instead of the more costly Enterprise Edition version (though Cluster Server will also run on Windows NT 4.0 EE).

A Cluster Server cluster requires a minimum of two nodes, and can scale up to as many as 32 nodes. At the storage layer, VERITAS supports all major storage vendors through its ongoing test programs. At the storage connectivity layer, Cluster Server supports both traditional client/server environments such as SCSI, as well as fibre channel-based SANs.
Each node in the cluster requires three network interface cards (NICs). One is used to connect to the public network (through which clients connect to the cluster). The remaining NICs are for private network connections used by Cluster Server to monitor nodes and exchange cluster status information. Nodes communicate via heartbeats, which enables them to recognize which are active members of the cluster, which are joining or leaving the cluster, and which have failed. The next section includes information about how nodes in the cluster communicate.

![Figure 2: Example of a four-node VERITAS Cluster Server cluster](image)

**Clustering in a SAN Environment**

VERITAS Cluster Server works in both traditional client/server and SAN environments. The scalable nature of Cluster Server (up to 32 nodes) makes it effective in a SAN, because SANs provide many paths to the same data. In addition, using Cluster Server in a SAN environment lets customers enjoy benefits that a SAN itself provides, including an enhanced ability to handle storage growth.

To implement a Cluster Server SAN installation, the application must be able to configure paths to all storage devices on the SAN. To accomplish this, Cluster Server is used with VERITAS Volume Manager. Volume Manager allows for online storage management for Windows environments, and includes the functionality to organize multiple physical disk objects into logical volume entities. Using Volume Manager with Cluster Server permits all servers to see the storage on the SAN, but the storage is not explicitly mapped to the server application unless it has ownership of the data. Tight integration between Cluster Server and Volume Manager allows Cluster Server to quickly remap the failed server storage to the new server and provide continuous access to data.
VERITAS Cluster Server Communication Channels

In a clustered environment, each node in the cluster must know the status of other nodes, so a reliable communication mechanism is important.

VERITAS Cluster Server has its own communication mechanism that the cluster uses to determine cluster status (called Global Atomic Broadcast or GAB). This protocol ensures that clustered nodes stay in sync and communicate accurate status throughout the cluster almost instantaneously.

The Cluster Server communication protocol performs three major functions:

• **Manages cluster memberships** — All nodes in the cluster have constant communication with each other so that they are always aware of changes in resource status, cluster membership, and configuration. The protocol also maintains a synchronized state in the cluster membership and configuration files for all cluster systems. If a failure occurs while transmitting status changes, GAB ensures that, upon recovery, all systems will have the same information regarding the status of any monitored resource in the cluster.

• **Monitors heartbeat communication** — GAB monitors heartbeat communication between systems. Both the heartbeat interval and the number of consecutive heartbeats a system can miss before it determines that another system has failed are configurable. When a system suspects another system has failed, the system in question is probed by other systems in the cluster to verify the failure. If the system remains unresponsive, it is marked DOWN and excluded from the cluster. Its applications are then migrated to the other systems.

• **Distributes information throughout the cluster** — GAB distributes information to all systems throughout the cluster regarding the system loads, agent reports, and administration commands.

GAB operates on top of Low Latency Transport (LLT), which provides kernel-to-kernel communications and monitors network communications. LLT runs directly on top of the Network Driver Interface Specification (NDIS) on Windows NT. This ensures events, such as state changes, are quickly reflected, which in turn enable faster responses. LLT can also be configured to run as “low priority.” This prevents Cluster Server communication on the public network until the public network is the final link, thereby reducing the rate of heartbeat broadcasts.
**Split-Brain**

Split-brain refers to a state where nodes in a cluster lose contact with each other across the network, but shared disks continue to operate (also known as “network partitioning”). The secondary server in the cluster, believing the primary server has failed because it no longer hears its heartbeat, takes over the disk. The primary server, which no longer receives a heartbeat from the backup server, but knows that it (the primary) is still operating properly, continues to write to disk. Windows NT (as well as other operating systems and file systems today) cannot support multiple systems writing to the same disk at the same time, so some data may be lost.

Because split-brain is a situation that must be avoided, Cluster Server uses multiple mechanisms to keep split-brain from happening to the cluster, including:

- **Multiple communication channels** — The second communication channel (NIC) employed by Cluster Server allows it to distinguish between network and system failures. If all but one network channel fails, Cluster Server enters a degraded mode that disables automatic application failover caused by system failure. If the last network channel fails, Cluster Server partitions into multiple “mini-clusters” without failing over or shutting down applications.

- **SCSI reservation** — SCSI reservation is the process used to control a hard disk, or in an array, multiple hard disks, so that only the server with the reservation can access the drive(s). Through SCSI reserve and release commands, Cluster Server is able to maintain control of the shared disks so that only the server that has control of the drives has access.

To protect the cluster from a pre-existing network partition, Cluster Server uses a technique called “seeding.” Cluster Server requires you to declare the number of systems that will participate in the cluster. When the last system is booted, the cluster will seed and start Cluster Server on all systems. Systems can then be brought down and restarted in any combination. Seeding is automatic as long as at least one instance of Cluster Server is running somewhere in the cluster.
Configuring Cluster Server Components

A single Cluster Server cluster consists of multiple systems connected in various combinations to shared storage devices. The Cluster Server engine (consisting of a number of processes) monitors and controls applications running in the cluster, and restarts applications in response to hardware or service faults. Information about how applications and services should be handled in the cluster is configurable. This configuration information is set for Cluster Server components, including resources (for example, hardware or software entities, such as disks, NICs, applications, and databases), resource types (for example, disk resources), and service groups (related resources, for example, an application).

For out-of-the-box supported applications like Microsoft Exchange, VERITAS Cluster Server includes templates that identify resources and resource types that can quickly be tailored for each unique cluster by VERITAS Cluster Server configuration tools.

![Diagram of sample resources and attributes for Microsoft SQL Server](image)

**Figure 3: Sample resources and attributes for Microsoft SQL Server**

**Resources**

Resources are hardware or software entities, such as disks, NICs, IP addresses, applications, and databases that work together to provide a service to clients in a client/server environment. They are identified by unique names within the cluster. Available resources can be displayed in the Cluster Server manager GUI or accessed from the Cluster Server command line interface.

There are different types of resources and multiple resources can be of a single type. For example, two disk resources within a service group are both classified as a type of Disk. A set of predefined resource types are provided with Cluster Server and users can also define and create unique resource types.

Resource attributes can be one of three types:

- **Type-independent attributes** are applicable to resources of all types. For example, Auto-start, Critical, and Enabled apply to all resource types.
- **Type-specific attributes** are applicable to resources of a specific type. For example, the Mount resource has attributes for partition, autoFSclean, forceunmount, drive letter, and file system type.
- **Static attributes** are attributes that have the same value for all resources of a specific type.
Service Groups

Service groups consist of related resources that work together to deliver application service to clients. When a service group is brought online, all the resources within the group are brought online. There are two types of service groups: failover and parallel.

- **A failover group** is a service group that can be fully or partially online on only one system at a time. Most application services, such as virtual file shares, are configured as failover groups.

- **A parallel group** is a service group that can be fully or partially online on more than one system at a time. An example is a web server.

Dependencies

Typically, resources are dependent upon each other or related resources, meaning that they operate in a particular order as established in the configuration file. This is most important during failover, when resources must be brought online or taken offline in the correct order so they can migrate to another system in the cluster. Cluster Server provides a number of templates for easy management of dependencies.

![Figure 4: Template view showing dependency information for Microsoft Exchange resources](image)

From the Cluster Server console window that contains a selected template, the administrator can view resource dependencies and attributes in that template. The templates can also be used to add service groups to the cluster, or to copy the resources within the templates to existing service groups.
Controlling and Monitoring Resources

VERITAS Cluster Server has defined procedures to bring applications and their associated resources online or take them offline to ensure that when a failover occurs, the shutdown of resources is controlled, the change of ownership to another server is managed, and resources are brought online on the second system in proper order. Cluster Server knows how different types of resources are brought online (for example, an IP resource is started by configuring the IP address on a NIC).

Agents are the Cluster Server processes that bring resources online and take them offline. They also monitor resources and report any state changes to Cluster Server. Agents that are packaged with Cluster Server are referred to as bundled agents. Examples of bundled agents include fileshare, IP, and NIC agents. The agents that are packaged separately for use with Cluster Server are referred to as enterprise agents (for example, Exchange, Oracle). New agents are always being developed; custom agents can be developed by end users or by working with VERITAS Consulting Services. VERITAS Cluster Server comes with its own API, templates, and manual that details how to develop custom agents.

<table>
<thead>
<tr>
<th>VERITAS Cluster Server for Windows NT Bundled Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Composite FileShare</td>
</tr>
<tr>
<td>Disk</td>
</tr>
<tr>
<td>ElifNone</td>
</tr>
<tr>
<td>FileNone</td>
</tr>
<tr>
<td>FileOnOff</td>
</tr>
<tr>
<td>FileOnOnly</td>
</tr>
</tbody>
</table>

The Generic Services Agent is an important bundled agent that can be used by generic applications and services. It can monitor multiple resources and services.

<table>
<thead>
<tr>
<th>VERITAS Cluster Server for Windows NT Enterprise Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange</td>
</tr>
<tr>
<td>Lotus Domino</td>
</tr>
</tbody>
</table>

The Cluster Server approach to managing applications through agents is different than other clustering technologies that require a special version of the application designed to run in the cluster. The agents approach supplies communication, translation, or the “glue” between the Cluster Server engine and the managed application in the cluster. The agents also provide a more flexible approach to clustering applications, since custom applications can be developed to make virtually any application cluster-aware, without needing a specific version (e.g., Exchange Server Enterprise Edition) of the application.
Figure 5: Cluster Server agents provide communication between the Cluster Server engine and the clustered applications. A number of Enterprise Agents are available to support popular Windows applications, and custom agents can be developed.

Configuring a Clustered File Share with VERITAS Cluster Server

To illustrate how resources and service groups are configured, the following example outlines the steps for setting up a file share Service Group in a two-node VERITAS Cluster Server cluster.

Before working with the file share in Cluster Server, disk resources must be set up. Use Disk Administrator to assign the drive letter on the shared disk for the file share, and then use My Computer to open the shared disk and create the directory to be used as a file share.

Once this is complete, the administrator is ready to begin creating and configuring the file share using VERITAS Cluster Server.

- The easiest way to set up a file share (or any other application) is to use the Service Group Configuration Wizard. The wizard guides the administrator through the steps needed to set up a service or application, including naming the Group, selecting nodes on which to configure the file share, and the priority order for each of the nodes.

- Select the FileShareGroup Service Group template and Cluster Server will create the resources needed by the file share. These resources will be listed on the Cluster Server GUI.

- Select each resource (for example, disk resource, NIC, VirtualName, etc.), and view and configure its attributes (for example, select the NIC resource and verify that the name of the adapter is correct).

Once all attribute values are assigned and verified, the wizard will finalize the file share configuration. To enable the file share (bring it online), the administrator simply needs to select the file share from the GUI and select the Enable resource command from the menu items.

Creating a file share is a simple example of setting up a clustered resource. The steps are the same for other applications and services.
Responding to Faults and Failovers

Once an application or service like a file share is set up and configured in the Cluster Server environment, it can then be set to automatically fail over in the event of unexpected failure, or manually failed over using the Cluster Server GUI.

In the event of an unexpected resource fault, Cluster Server ensures successful failover of the application or service by performing the following actions:

• All resources in the path of the fault are taken offline, starting from the faulted resource to the top of the dependency tree.

• If an online critical resource is part of the path that was faulted or taken offline, Cluster Server takes the entire group offline in preparation for failover, skipping all faulted resources.

• Cluster Server starts the group on another system.

Avoiding Planned Downtime Using Manual Failover

To avoid downtime of applications and data for a normal maintenance activity like an operating system service pack update, administrators can use Cluster Server manual failover capabilities. During the manual failover, Cluster Server performs the same actions as it would during an automated failover, but at the request of the administrator executing a command from the Cluster Server GUI.

For example, to install an operating system Service Pack update on a two-node Exchange cluster, the Cluster Server administrator can do the following to perform the upgrade on both nodes while keeping Exchange online:

• Install the operating system Service Pack update on the node in the cluster that is not actively running Exchange.

• Thoroughly test the node on which the upgrade was just installed.

• Manually fail over Exchange to the upgraded server. If Exchange does not run on the upgraded server, immediately fail it back.

• If Exchange runs without a problem on the upgraded node, perform the same maintenance on the node where Exchange was originally running (and again, test thoroughly).

By using manual failover with Cluster Server, maintenance activities that used to cause several hours of application downtime can be reduced to the few minutes needed to fail over an application between nodes in the cluster.
The Cluster Manager Console

The Cluster Server GUI is the console that allows users to configure and administer clusters. The GUI is Java-based, and a single console can be used to manage and administer cross-platform clusters.

From the console, the administrator configures the properties of resources and service groups to ensure successful and efficient failover in the case of an unplanned outage. Wizards provided with the console make it easy to set up popular applications and services. The console can also be used to perform manual failovers and execute other commands on the cluster, such as freezing a node to prevent failover.

Users receive different levels of access to the Cluster Server console, depending on their category:

- **Guests** — can view and monitor the cluster, but not modify the configuration or perform administrative tasks.
- **Operators** — can view the cluster and perform basic administrative tasks, such as bringing service groups online and taking them offline, but cannot modify the configuration.
- **Superusers** — have full permission to view the cluster, perform administrative tasks, and modify the configuration.

Monitoring Clusters

The Cluster Server console consists of several windows through which the administrator can access a variety of information about the state of a cluster. The main window for cluster administration is the Cluster Explorer window, which allows the administrator to view the status of cluster objects and perform various operations. Other windows are:

- **Cluster Monitor** — enables the administrator to log on to and off of a cluster, view summary information about cluster objects, customize the display and exit the Cluster Manager.
- **Command Center** — where Cluster Server commands can be built and executed.
- **Command Shell** — where non-interactive shell commands can be launched on cluster systems and the results are displayed on a per system basis.
- **Template View** — allows the administrator to view resource dependencies and attributes.
The Cluster Explorer window has three sections, or “panes.” The top pane includes a toolbar, which gives quick access to frequently used operations. The left pane contains the configuration tree, a hierarchical display of all cluster objects. The right pane contains a view panel, which displays details of the object selected in the configuration tree. The right pane also includes five tabs (attributes, resources, service groups, heartbeats, and SNMP), which the administrator can use to monitor and administer various cluster objects.

Figure 6 shows the Cluster Server Attributes View. The attributes of the cluster object selected in the configuration tree are displayed in a tabular format consisting of five columns: Name, Scope, Dimension, Value, and Edit. The Edit column denotes attributes that can be modified.
Resource View

The Resource View displays resource dependencies.

![Resource View Diagram](image)

Figure 7: Sample Cluster Server resources and dependencies for Oracle.

A dependency graph is displayed, showing the resource dependencies within the service group. Resources are arranged according to their distance from the root resources. Root resources (resources without parents) are displayed in the top row. The line between the two resources represents a dependency, or "parent-child" relationship.

Service Group View

The Service Group View displays service groups and their dependencies. This graph is similar to that of the Resource View, except in this view each icon represents a service group instead of a resource. The graphic overlay and color scheme for each service group icon represents the state of the service group. The color of the link indicates the type of the dependency. For example, a red link indicates a firm dependency while a blue link indicates a soft dependency.

Heartbeat View

In this view, the system heartbeat graph is displayed with systems arranged as nodes. If a system in the cluster is having difficulty connecting to other systems, it appears with an error icon indicating that the link or disk heartbeat is down.
Complementary Products

A high availability solution is more than just clustering software – it should be a total approach involving every layer in today’s data center: applications, storage management, storage infrastructure (for example, switches), and data storage itself. VERITAS Software, The Data Availability Company, is unique in that it provides solutions for improving availability at every layer in the data center.

To protect valuable data, VERITAS delivers backup and recovery solutions for any size system ranging from mobile computers to large data centers. With the VERITAS NetBackup™ and VERITAS Backup Exec™ product families, VERITAS solutions protect data in Windows, Novell and UNIX environments.

For managing storage devices and infrastructure in a SAN environment, VERITAS recently introduced SANPoint Control. VERITAS SANPoint Control™ is an easy to use, centralized management tool for automatic discovery, visualization, and zoning administration of SAN-connected devices.

To promote availability at the storage management layer, VERITAS Volume Manager™ provides online storage management functionality. Volume Manager provides disk-usage analysis, RAID techniques, and the dynamic reconfiguration of disk storage while a system is online. This ensures continuous data availability and data protection, and also eliminates the need for servers to be taken offline for administrative and maintenance tasks, allowing administrators to keep data available to users.

Replication technologies promote high availability over a wide area. VERITAS Storage Replicator™ creates continuous remote updates of critical files and is a natural complement to VERITAS Cluster Server. Another wide-area high availability solution from VERITAS that will soon support VERITAS Cluster Server for Windows clusters is VERITAS Global Cluster Manager™. Global Cluster Manager monitors multiple geographically distributed Cluster Server clusters and manages failover of an entire cluster from one site to another. Global Cluster Manager supports Cluster Server in UNIX environments today, and is being extended to also support Windows environments.
Summary

Ensuring high availability of applications and data in today's rapidly growing Windows environments is a challenge. Many factors can cause downtime – planned downtime to perform system maintenance and necessary upgrades, as well as unexpected faults with software and hardware.

VERITAS Cluster Server is a high availability clustering solution for mixed computing environments, supporting Windows, Solaris and HP-UX today with additional operating system support planned. Cluster Server is highly scalable (supporting 2-32 nodes in a cluster), flexible (supporting 1:1, 1:N, N:1, and cascading failovers), and supports today's most popular Windows applications including Exchange, SQL Server, IIS, and Oracle.

Clustering is one technique for improving availability for applications and data, and availability can be further enhanced using additional solutions for managing other components in the data center. For example, using Cluster Server with VERITAS Volume Manager enables administrators to ensure high application availability (through Cluster Server), and through Volume Manager, be able to manage storage online without having to bring applications down.

To learn more about VERITAS Cluster Server and other VERITAS high availability clustering and replication solutions, visit http://www.veritas.com/us/products/clustering.