Keep Your Business Running with High Availability and Disaster Recovery for SAP Applications

Who should read this paper

This whitepaper is aimed at technical architects and IT decision-makers at customer companies as well as architects and consultants involved in the design and planning of technical solution architectures for SAP-centric business solutions.
# Keep Your Business Running with High Availability and Disaster Recovery for SAP Applications

## Content

**Executive Summary** ................................................................. 1

**The Challenges of SAP Application Availability** ........................................... 2

**Symantec High Availability and Disaster Recovery Solutions** .............................. 14

**Conclusion** ............................................................................. 26

**Appendix** ................................................................................. 27
Executive Summary

Many organizations rely on SAP applications to support vital business processes. Any disruption of these services translates directly into bottom-line losses. As organization's information systems become increasingly integrated and interdependent, the potential impact of failures and outages grows to enormous proportions.

The challenge for IT organizations is to maintain continuous SAP application availability in a complex, interconnected, and heterogeneous application environment. The difficulties are significant:

• there are many potential points of failure or disruption
• the interdependencies between components complicates administration
• the infrastructure itself undergoes constant change

To gain additional competitive advantage, enterprises must now work more closely together and integrate their SAP environment with those of other organizations, such as partners, customers, or suppliers. The availability of these applications is therefore essential.

There are three main availability classes, depending on the degree of availability required:

• Standard Availability – achievable availability without additional measures
• High Availability – increased availability after elimination of single points of failure within the local datacenter
• Disaster Recovery – highest availability, which even overcomes the failure of an entire production site

Symantec helps the organizations that rely on SAP applications with an integrated, out-of-the-box solution for SAP availability. Symantec’s High Availability and Disaster Recovery solutions for SAP enhance both local and global availability for business critical SAP applications.

• Local high availability: By clustering critical application components with application-specific monitoring and failover, Symantec’s solutions simplify the management of complex environments. Administrators can manually move services for preventative and proactive maintenance, and the software automatically migrates and restarts applications in case of failures.

• Global availability/disaster recovery: By replicating data across geographically dispersed data centers and using global failover capabilities, companies can provide access to essential services in the event of major site disruptions. Using Symantec’s solutions, administrators can migrate applications or an entire data center within minutes, with a single click through a central console. Symantec’s flexible, hardware independent solutions support a variety of cost-effective strategies for leveraging your investment in disaster recovery resources.

Symantec provides High Availability and Disaster Recovery solutions for SAP, utilizing Symantec™ Storage Foundation, powered by Veritas, Symantec™ Replicator Option, Symantec™ Cluster Server, powered by Veritas, and Cluster Server agents that are designed specifically for SAP applications. The result is an out-of-the-box solution that you can quickly deploy to protect critical SAP applications immediately from either planned or unplanned downtime.
The Challenges of SAP Application Availability

As customers increasingly deploy SAP systems for their global operations to support mission-critical business functions, the need for maximized SAP system availability becomes crucial.

Maintaining optimal performance and availability for critical SAP applications is increasingly difficult for many IT departments, because the IT environment itself is complex, dynamic, and inherently unstable. Several factors combine to make the availability of SAP applications both costly and challenging.

The SAP application environment is complex and heterogeneous

An SAP application environment may include the following services: a database server, a central services instance with a message server and an enqueue server, an enqueue replication server, and one or more dialog instances. It is essential that the operations team understand the dependencies among these application services. For example, the database must be running before the central services instance can be started. Between the application and the end user, however, there are several other application services, such as web servers, load balancers, and the logical IP address infrastructure. These services may use different operating systems and equipment from multiple vendors.

Because application availability depends on the availability of the total environment, the operations team must be able to manage and maintain, or at least troubleshoot, application servers, operating systems, storage systems, network infrastructure, and databases. Most often these skills are distributed through a number of different people, possibly in different organizational units, and requires manual coordination. To reduce the administrative costs while improving availability, IT organizations need a single interface for managing all services of the application environment, across different platforms and databases.

Downtime is not an option

With SAP applications being critical to an organization's daily operations, taking the whole application offline for hours or days to fix any problems is not an option.

• With global operations, the few hours that operations staff once had in the middle of the night are now business hours somewhere around the globe, making planned downtime increasingly scarce and expensive.
• Unplanned downtime may interrupt critical business processes and cost companies thousands of dollars or more per hour.

In an inherently volatile environment, IT organizations need the ability to upgrade, test, maintain and deploy infrastructure components without disrupting operations. The need to maintain applications and infrastructure, and correct problems as they occur, is inevitable, and these activities should be able to be performed without interrupting application access.

Multi-tier applications have many potential points of failure

To access the application, the user needs the entire application infrastructure to be working. As the number of tiers within an application’s architecture increase, the number of points of failure that must be either eliminated or mitigated also increases.

IT organizations typically focus on protecting specific, essential components of the infrastructure, such as the database. But protecting the database alone is not effective if the network router fails. Applications depend not only on the other application services (such as the database and application servers), but also on the infrastructure components, such as the disks and volumes, NFS shared mounts, virtual IP addresses, network cards, and so on. Building redundancy at a component level at each layer increases the complexity of the IT environment – and hence the cost of managing that environment.
IT organizations need an end-to-end approach in protecting SAP application availability that incorporates all of the essential application tiers, services, and components.

**Growing interdependence of business systems expands the risk**

Even more complex than a single multi-tier application are several interconnected applications. With the increasing adoption of enterprise application integration (EAI) initiatives, companies are linking vital business applications together with middleware to create a service-oriented architecture (SOA). Modern business processes require running multiple applications in an interconnected and performing manner. For instance, in a Customer Relationship Management environment there is a data feed coming from a SAP ERP system into SAP CRM. Ensuring the availability of such a business process requires the availability of both SAP applications. Each SAP application consists of several components and some of them are single points of failure. This results in multi-tiered environments with complex dependencies residing inside the single SAP systems and between multiple SAP systems likewise. The unintended effect of this architecture is the increased risk of an outage in case of an application failure. When a critical application is tightly linked with other applications in a composite architecture, the loss of the application affects wider service availability.

**Virtualization of SAP Applications**

There are a number of motivations for using virtualization. The primary focus for all of the motivations is reduction of complexity and the total cost of ownership of the IT landscape:

- **Landscape consolidation:** Reduction of physical servers by combining multiple SAP systems while keeping the isolation level.
- **Load shifting:** Move SAP systems between physical hosts to accommodate changes in resource utilization.
- **Optimized Application Availability:** Free physical servers for maintenance, or quick restart of services after hardware failure.
- **Rapid Provisioning:** Easy duplication of virtual containers, compared to a physical server.

These possibilities, provided by virtualization, help to increase server use and application availability and provide a high degree of flexibility.

As server virtualization adoption increases, IT needs to leverage the benefits of virtualization for business-critical applications. However, there are challenges with minimizing downtime associated with application failures within virtual machines or virtual containers. While the virtualization layer might be able to detect and mitigate failures on the container or operating system level, the applications running inside the containers are not protected from failure.

**Protect your SAP environment with Symantec HA/DR Solutions.**

Symantec's suite of High Availability and Disaster Recovery (HA/DR) products provide a simple and cost-effective solution to overcome the availability challenges, outlined above, and ensure 24x7 availability of your SAP applications.

**Symantec Cluster Server** eliminates planned and unplanned downtime by clustering critical applications and the resources they require. Cluster Server can monitor and centrally manage all of the critical components of an SAP environment, including the SAP application, the underlying database, and the file server, to ensure maximum application availability. By monitoring the status of applications and automatically moving them to another server in the event of a fault, Cluster Server can dramatically increase the availability of an application or database. Cluster Server can detect faults in an application and all its dependent components, including the associated database, operating system, network, and storage resources. When a failure is detected, Cluster Server gracefully shuts down the application, restarts it on an available server, connects it to the appropriate storage device, and resumes normal operations. Cluster Server can temporarily move applications to a standby server when routine maintenance such as upgrades or patches requires that the primary server be taken offline.
Cluster Server uses high-availability agents to guarantee application compatibility, reduce time to deployment, and cut consulting costs. Several agents for SAP applications are available, which start the SAP application during online, stop the SAP application during offline, monitors the SAP applications for critical processes, and cleans the environment for SAP applications in case of any issue. Agents for databases are available for most of the databases relevant for deployment with SAP applications. They support enterprise-class databases such as Oracle, SQL Server, DB2, Informix and Sybase. The Cluster Server agent for DNS updates the Domain Name Server with the virtual hostname and IP for SAP applications for DNS based SAP configurations for local or remote cluster failover. All of these agents come with the Cluster Server license. An overview of available application and database agents relevant to SAP NetWeaver based business applications is available in the appendix.

Symantec Storage Foundation High Availability, provides a highly available, local data and application availability environment that helps you do the following:

- Manage complexity by providing a single interface for starting, stopping, monitoring and maintaining SAP application services.
- Manage change by proactively moving application services to enable dynamic maintenance and testing. Improve availability with automated, application-specific monitoring and failover when problems do occur, and fast reconfiguration when the problem is resolved.
- Consolidate servers and make better use of resources through local clustering and the virtualization of critical services. Improve storage utilization and administrator productivity through policy-based storage management.

Symantec Cluster Server HA/DR is a Cluster Server extension that monitors and controls multiple, geographically-distributed Cluster Server (VCS) clusters as well as replication occurring with Symantec Replicator Option or third-party replication technologies. Cluster Server HA/DR lets administrators migrate all of the applications in a data center with a single click, enabling companies to survive serious local disruptions without significant interruptions to critical services. With agents for managing all leading replication technologies, Cluster Server HA/DR makes it simple to fully automate the disaster recovery of your SAP applications.

Symantec Replicator Option delivers reliable, storage-independent replication over any IP network, providing a critical component of a rapid disaster recovery configuration. The product replicates data at the logical volume level, as well as on the file system level (Linux only), while ensuring data integrity and reliability during replication.

Symantec™ Disaster Recovery Advisor automatically detects and reports on risks in high availability and disaster recovery infrastructure. By scanning systems across the data center to ensure that existing HA/DR plans are applied seamlessly, Disaster Recovery Advisor helps limit the risk of infrastructure and application downtime by ensuring data center recoverability.

Symantec™ ApplicationHA provides added protection and visibility for SAP applications running in virtualized environments including: VMware®, Microsoft® Hyper-V, Red Hat® Kernel VM (KVM), IBM® AIX® Logical Partitions (LPAR), and Oracle® VM on Solaris Sparc (formerly Solaris Logical Domains or LDOM). ApplicationHA enables administrators to safely virtualize business-critical applications like SAP with confidence by dramatically improving application availability. Through integration with VMware vCenter and Veritas Operations Manager, ApplicationHA significantly enhances application visibility and manageability in VMware virtual environments and helps reduce operations and training costs.

Before we analyze how each of these products contribute to a highly available SAP ecosystem, let us look at the key components that constitute a typical SAP application.
SAP System Components

Any availability solution for SAP must address the specific availability requirements and constraints of the SAP system environment. This section describes the architecture of the SAP NetWeaver Application Server, which provides the platform for most SAP business applications, outlining a few of the SAP-specific issues affecting application availability.

An SAP application instance has multiple services which are typically deployed across multiple servers. An SAP system consists of SAP instances. An SAP instance is a group of processes that are started and stopped at the same time. These instances are as follows:

- Primary Application Server instance: Each SAP system has a primary application server instance with the following components:
  - Usage type AS ABAP
    - Dispatcher
    - Work processes (dialog, batch, spool, or update)
    - Gateway
    - Internet Communication Manager (ICM)
    - Internet Graphics Service (IGS)
  - Usage type AS Java™
    - Java dispatcher
    - Server processes
    - Software Deployment Manager (SDM)
    - Internet Graphics Service (IGS)
- The Application Server Instance is also known as the Central Instance.
  - Central Services instance: In this instance, we have the Java central services instance (SCS) or ABAP central services instance (ASCS). These instances form the basis of communication and synchronization for the Java or ABAP clusters. This instance, existing only once in an SAP system, consists of the message server and the Enqueue Server. The message server is the central message hub for technical, non-application information, such as information about the technical SAP system layout. The enqueue server manages the locking information for all business objects.
  - Database instance: This instance is a mandatory installation component for the installation of an SAP system and holds all of the business data and a lot of technical data as well.
  - Additional Application Server instance or Dialog instance: This optional instance is used to add more resources in an SAP System. There can be multiple Application Server instances in an SAP system.
  - Enqueue Replication Server instance: This optional instance is used to provide a replica of the data held by the Enqueue Server for high availability purposes.

To understand these core components of an SAP NetWeaver System, we need to take a closer look at some of them.

Message Server

The Message Service keeps a list of dispatchers and server processes. It represents the infrastructure for data exchange (small datasets only) between the participating nodes. The message service also supplies information to the SAP Web Dispatcher about Load Balancing between many ABAP and Java Instances.
The following diagram shows how the message server helps the SAP Web Dispatcher with load balancing information:

![Figure 1 - SAP Message Server architecture](image)

To avoid the single point of failure with the message server, the message server must be restarted along with the Enqueue Server quickly. Both can be restarted automatically using cluster software, such as Symantec's Cluster Server.

**Enqueue Server**

The Enqueue service is a critical component of the SAP system. It administers locking using objects within SAP transactions that can be requested by applications to ensure consistency within the SAP system.

Since the lock table is held in the main memory of the Enqueue Server, server failure without additional backup measures results in loss of the locks held. To maintain consistency, all open transactions are rolled back after the Enqueue Server is restarted.

An Enqueue Server failure has significant implications on the SAP systems. The enqueue table contains only locks on business objects, locks are session bound. A loss of the enqueue service, and therefore the enqueue table, requires the concerned sessions to be rolled back (done automatically by SAP).

Similarly, for a JAVA stack, the Enqueue table contains business object locks plus infrastructure locks (system, not session bound). A loss of the enqueue service, and therefore the enqueue table, requires the concerned sessions to be rolled back. Additionally a restart of all J2EE instances is required due to the infrastructure locks being in an ambiguous state.

The Enqueue Replication Server resolves this challenge.

**Enqueue Replication Server**

The Enqueue Replication service enables the lock table to be replicated on a second server, the replication server. A copy of the lock table is maintained on this server. If the Enqueue service fails, a new Enqueue service is started on the Replication Server using a failover solution (clustering software from a partner like Symantec) and this replication service creates a new lock table from the copy of the lock table. This
enables the Enqueue service, and therefore the whole SAP component, to continue operating almost without interruption. If the Enqueue service fails, transactions are no longer terminated, so that work can be continued transparently.

Symantec Cluster Server provides the cluster technology for the Enqueue Server and its Replication Server, which is required for the Enqueue service to operate without interruption.

**Application Server Instances**

The Application Server instances play the main role in execution of ABAP or JAVA applications. In medium to large SAP systems as well as for highly available systems, there are multiple Application Server instances. Each instance can run on a separate server, but it is also possible to operate multiple instances on one host. An SAP instance can provide different service types. The standard SAP services that can be configured on all instances of the SAP component are dialog, batch, update, and spool. The failure of an SAP instance on which only these standard services are configured causes all the transactions processed on it to be terminated and rolled back. Database consistency is guaranteed at all times. Terminated transactions can be repeated on one of the instances still available.

**Database Instance**

SAP environments may use any of the relational database management systems as the database server. Administering the database itself requires experience in the specific database used, such as Oracle, Microsoft SQL Server, IBM DB2, IBM Informix, SAP MaxDB or SAP/Sybase ASE.

The database represents a single point of failure for the SAP system, unless the database itself is clustered.

Apart from the core components of an SAP NetWeaver system, additional components can be used.
**SAP Web Dispatcher**

The SAP Web dispatcher is recommended when you use an SAP system with several SAP Web Application Servers for Web applications. The SAP Web dispatcher is a program that you can run on the computer that is connected directly to the Internet.

The SAP Web dispatcher lies between the Internet and your SAP System. It is the entry point for HTTP(s) requests into your system, which consists of one or more Web application servers. As a "software web switch", the SAP Web dispatcher can reject or accept connections. When it accepts a connection, it balances the load to ensure an even distribution across the servers.

You can use the SAP Web dispatcher in Add-In systems and in pure Java systems, as well as in pure ABAP systems. It is also beneficial to use the SAP Web dispatcher, if you do not need security functions (entry point in the DMZ, SSL, URL filtering), but you simply want to balance the load between several SAP Web AS instances.

If multiple Application Servers are available in the SAP system, the SAP Web Dispatcher provides load balancing for HTTP(S)-based requests to the SAP system. This can be replaced with other HTTP load balancers including hardware-based solutions.

**Internet Communication Manager**

The Internet Communication Manager (ICM) enables communication between the SAP Web AS and external partners using Internet standard protocols, such as HTTP, HTTPS, SMTP, SOAP, and the Java communication services. The SAP Java Connector (SAP JCo) enables method calls between Java applications and ABAP applications.

The following diagram shows how SAP JCo connects an ABAP system and a Java system:
High Availability of SAP NetWeaver systems

For SAP NetWeaver systems, the following single-point-of-failures need to be protected in a high availability setup:

- Database instance
- Central Services (SCS or ASCS)
  - Message Server Enqueue Server
  - Enqueue Replication Server instance
- Network File System (NFS) or Common Internet File System (CIFS) services, used to provide shared file systems used across the SAP system (Central file share /sapmnt/...)

In traditional setups, both the Enqueue and Message service reside in the SAP Central Instance (CI). In more advanced configurations, the Enqueue Server runs independently and is backed up by a separately operating Enqueue Replication Server (ERS). In most large SAP installations, the database uses a separate server for performance purposes. The file server is typically separate as well.

The following figures depict the Single Point of Failures (SPOFs) for SAP NetWeaver based systems:

In a traditional SAP NetWeaver Application Server ABAP system, the database, the global file system, and the ABAP Central Instance represent single points of failure, as shown in Figure 4 below.

![Figure 4](image)

**Figure 4 – Single points of failure in a traditional SAP NetWeaver Application Server ABAP system with a central instance**

In a more modern SAP NetWeaver Application Server ABAP system, the Enqueue Server and Message Server are separated out from the Central Instance into a small ABAP SAP Central Services (ASCS) instance, which now represents a single point of failure instead of the Central Instance. Figure 5 below illustrates this.
In an SAP NetWeaver Application Server ABAP system with a central services instance, the database, the global file system, and the JAVA Central Services (SCS) Instance (hosting Enqueue Server and Message Server) represent single points of failure, a very similar concept to a modern ABAP system. The Software Deployment Manager (SDM) in an SAP NetWeaver JAVA system is existing only once in a system, but due to its non-critical nature it is not considered a single point of failure. Figure 6 below illustrates the single points of failure in an SAP NetWeaver Application Server JAVA system.

An SAP NetWeaver Application Server Add-In system, also referred to as a dual-stack system, combines both the ABAP execution environment and the JAVA execution environment into one SAP System. Figure 7 below illustrates this and points out the single points of failures in such a system: The ASCS and SCS instances, the global file system and the database.
SAP applications typically have more application server instances in addition to the primary application server instance. Because the application server instances are redundant, they do not present a potential single point of failure. However, the loss of a dialog instance in a heavily-loaded system can significantly degrade performance, and the application server instances are a key part of a global failover scenario.

SAP recommends the following HA setups for SAP NetWeaver applications:

<table>
<thead>
<tr>
<th>HA Setup</th>
<th>SAP Rating SAP NetWeaver AS Java</th>
<th>SAP Rating SAP NetWeaver AS Add-In</th>
<th>SAP Rating SAP NetWeaver AS ABAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB only in switch-over group</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
</tr>
<tr>
<td>CI, ASCS/SCS and DB in one switch-over group</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
</tr>
<tr>
<td>CI, ASCS/SCS in one switch-over group, DB in another</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
</tr>
<tr>
<td>DB and ASCS/SCS in one switch-over group</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
</tr>
<tr>
<td>DB and ASCS/SCS each in its own switch-over group</td>
<td>RECOMMENDED</td>
<td>RECOMMENDED</td>
<td>RECOMMENDED</td>
</tr>
</tbody>
</table>

* Prerequisite: Separation of SCS for ABAP and JAVA
  * Each HA Setup should be extended by the Enqueue Replication Server
  * In an ABAP only or Add-In Installation, it is recommended to separate an ASCS instance

Taking the previously described single-points of failures and SAP's recommendations into account, a highly available SAP system could be achieved with a configuration as shown in Figure 9 below:
The different components of SAP have strict dependencies in the order in which they are restarted in case of a failure.

For example:

- In most cases, the NFS/CIFS server should be available before the database and the Central Services and Application Server instances start.
- The database server must be available before the Central Services and Application Server instances start.
- The Central Services Instance must be online before Application Server instances are brought online.

The Symantec solution can help address the single points of failure and manage the dependencies. The different components of the Symantec solution work together and help IT organizations improve SAP application availability on a daily basis while offering significant protection from the loss of service and data in the case of a disaster or regional disruption.

**Storage Availability and Performance**

The storage subsystem is one of the most critical components of an SAP system landscape, playing a key role in availability of the entire system, protection of data and delivery of expected performance to the end user. No matter whether the customer uses Fibre Channel (FC), SCSI over IP (iSCSI), Network Attached Storage (NAS) or Direct Attached Storage (DAS), some basic principles regarding storage apply:

- Data should be distributed across the highest number of disk spindles possible to ensure that requests – for example from the database – are not slowed down due to hotspots on single disks. Alternatively, new technologies like Flash Storage can be used to ensure performance.
- Storage protection mechanisms are required, such as RAID, to protect from single disk failures.
- Throughout the entire SAN, components such as host bus adapters (HBA) or switches should be redundant to protect from single component failures and to enable load balancing.
Symantec Storage Foundation combines Symantec's industry-leading file system and volume management solutions to create a highly available, robust foundation for SAP data. The journal file system restarts in seconds for fast failovers. Logical volumes support highly available, high performance storage configurations. Database-specific components such as direct I/O accelerate database read and write performance while simplifying the manageability of database data. Storage Foundation provides database-specific optimizations for Oracle, DB/2, Sybase, Microsoft SQL Server, and Oracle RAC databases. Storage Foundation enables a flexible and agile infrastructure with features such as SmartIO and Flexible Storage Sharing while reducing storage costs with features such as deduplication, compression, thin provisioning, and storage tiering. With Storage Foundation, you can adopt Solid State Drive (SSD) technology and implement any changes to your storage infrastructure, including operating system or array migrations, without impacting application availability.

The SmartIO feature enables data efficiency on your SSDs through I/O caching. Using SmartIO to improve efficiency, you can optimize the cost per IOPS. SmartIO uses advanced, customizable heuristics to determine what data to cache and how that data gets removed from the cache. The heuristics take advantage of Storage Foundation’s knowledge of the characteristics of the workload.

For example, for a database, the index volumes may have different caching policies from the data volumes. SmartIO uses templates to apply policies to particular types of volumes in the database to optimize caching for those databases. SmartIO provides application templates for Oracle and Sybase databases.

Flexible Storage Sharing (FSS) within Storage Foundation Cluster File System enables network sharing of local storage across a global namespace to provide data redundancy, high availability, and disaster recovery without the need of shared storage. FSS enables operating a highly available SAP NetWeaver system (including the database) entirely on local storage.

Optimizing Resource Utilization

Most clustering solutions recommend using active/passive two-node clustering configurations, which means that backup servers remain idle, wasting computing resources and decreasing server utilization. On the other hand, Cluster Server allows true N+1 "roaming spare" or N+M "active/active" capability for maximum availability without the cost of a dedicated spare per application.

Cluster Server uses dynamic selection of target system to failover an application to the biggest available system. It monitors the available capacity of systems in the cluster in terms of CPU, memory, and swap to select the biggest available system based on application needs. When a failure occurs, Cluster Server can automatically choose the least utilized server to failover to, as well as add repaired servers back into the selection pool when they rejoin the cluster. AdaptiveHA in Cluster Server ensures that application uptime is maximized and server resources are utilized most efficiently for Linux and UNIX environments. AdaptiveHA enables VCS to make dynamic decisions about selecting the cluster node with maximum available resources to fail over an application. VCS dynamically monitors the available unused capacity of systems in terms of CPU, Memory, and Swap to select the most resourceful system. Cluster Server provides immediate detection of application faults with the Intelligent Monitoring Framework (IMF) feature. By removing the constant monitoring cycle needed in legacy clustering products, there is no additional CPU overhead. In addition, this framework provides instant notification to VCS when a resource goes offline. As a result, action is taken immediately instead of any delay caused by the timing of the monitoring process.

In addition to the moment-to-moment and day-to-day availability concerns, IT organizations have to also find ways to provide continued access to critical applications in the case of a disaster. Most critical applications must have the ability to run at an alternate, geographically-separate location from the primary production environment.

Alternate data centers are costly. The money spent on disaster recovery facilities comes from a fixed pool of resources available for IT and infrastructure. For many companies, disaster recovery planning entails identifying a "cold" recovery site that requires an initial investment
and ongoing maintenance to remain current. In the case of a disaster, recovery may require significant time and manual intervention. By taking advantage of existing resources and multi-purposing equipment, Symantec technology enables companies to build “hot” recovery sites that can provide nearly instant recovery without manual intervention.

**Symantec High Availability and Disaster Recovery Solutions**

Symantec's High Availability and Disaster Recovery solutions for SAP enhance both local and global availability for business critical SAP applications. The following sections describe how to protect an SAP NetWeaver environment for local high-availability and disaster recovery.

**Local failover with Symantec Cluster Server**

This section describes how you can configure an SAP system for local high availability.

**Setting up the cluster**

Symantec Cluster Server allows for highly flexible, scalable clustering configurations. For an SAP environment, you will probably want to include the following system components in a cluster configuration:

- SAP central services instance
- Enqueue Replication Service
- Any application server instances
- The server running the database
- The file system server

Although the application server instances do not represent single points of failure, the loss of an instance can degrade application performance. If you plan to implement global failover for disaster recovery, you will likely need to include the application instances in the cluster configuration even if they do not necessarily failover. Finally, including application server instances in the local cluster simplifies application server administration, allowing operators to use the same interface to start, stop, monitor and manage these additional SAP services.

Symantec strongly recommends configuring the application server instances under the cluster software for better manageability and performance. Customers can cluster as many application server instances as needed to service the basic functions after failover and the necessary application server instances (not so important) for additional connections.

To provide transparent failover, you will need to implement shared data between the cluster nodes. Typically this is achieved using SAN-based storage, or alternatively use Symantec Storage Foundation’s Flexible Storage Sharing feature to seamlessly combine shared and direct-attached storage under a common storage virtualization solution. The cluster configuration requires redundant private Ethernet connections between nodes to support cluster heartbeat communications.

You can add other servers as well, to consolidate management of a high availability environment and provide spare capacity for critical applications. Clusters managed by Cluster Server can support up to 64 nodes, allowing the clusters to be expanded for maximum server efficiency.

Cluster Server supports both active/passive and active/active configurations, meaning that you do not need to dedicate spare, unused processing capacity for each critical server. Many customer sites maintain an n+1 clustering environment, with one spare or a little-used server providing failover capacity for other servers in the cluster.

---

It is also possible to have an entirely active/active (n-to-m) cluster, using multiple application groups on multiple servers, each group capable of being failed over to different servers in the cluster. The cluster only needs sufficient spare capacity available on production servers to absorb the applications of a failed system.

**Configuring the high availability agent for SAP NetWeaver**

Cluster Server uses application-specific agents to start, stop, monitor, and switch over different applications and infrastructure components. A Cluster Server environment running SAP uses Cluster Server high-availability agents to monitor and track the SAP system, the database, and the file server.

The Cluster Server agents for SAP NetWeaver starts, stops, and monitors essential SAP application services, including the:

- Enqueue Service (running within a Central Instance or within a Central Services Instance (SCS))
- Message Service (running within a Central Instance or within a Central Services Instance (SCS))
- Enqueue Replication Service (ERS)
- Dispatcher and Worker Processes in Application Server Instances
- Collector and Sender (CO & SE) processes in both Dialog and Central Instances
- Gateway processes in both Dialog and Central Instances
- Internet Graphics Service (IGS) process in both Dialog and Central Instances
- SAP OS Collector process

The agent provides the ability to start, stop, and monitor each of these SAP services. Additionally, if a service fails, the agent will clean the node for any remaining system processes and shared resources.

Symantec Cluster Server provides multiple levels of monitoring for SAP services:

- The first (default) level confirms the existence of essential processes in the process table.
- The second level, which is optional and additional to the first, runs SAP supplied tools to check the health of the SAP systems.
- The third level, which is also optional, invokes an external monitoring program, allowing the user to provide custom scripts for application monitoring.

**Creating service groups**

Symantec Cluster Server provides application failover by encapsulating the resources required for each application into a service group – creating virtualized application services that can be moved among cluster nodes. Operations staff can operate on the cluster itself, on the service group (starting, stopping, switching over, etc.), or on the specific resources within the service group. A Cluster Server service group is the smallest unit of failover.

Each SAP service group contains a set of dependent resources – the lower-level components that an application requires to operate successfully. Resources include disk groups, disk volumes, file systems, IP addresses, and dependent application processes. The resources within a service group have dependencies which define the start and stop order that Cluster Server uses to bring the service group online and offline, respectively.

---

2. The SAP OS Collector process (saposcol) is only started if not already started by an OS init script, but not monitored and never stopped.
Cluster Server starts, stops, monitors and switches service groups on any server in the cluster in response to server or resource faults. In addition, an administrator can proactively move a service group between cluster nodes to perform preventative maintenance or apply patches. The service group includes logic about the dependencies between application components.

For example, the following figure illustrates the relationship between the Cluster Server resources required to support a SAP central services instance:

![General Cluster Server Service Group diagram for SAP](image)

The resource for the SAP Central Services instance depends on the Virtual IP address and the file system mounted by the mount agent. The mounted file system is shared to allow access by other SAP application servers running on different systems.

**Disk Groups**

Each service group requires a dedicated file system, volume and disk group to store the service group’s data and programs. By importing and deporting this set of storage objects on different servers in the cluster without affecting other service groups, Cluster Server allows the service groups themselves to be independent of the underlying architecture and mobile across the cluster.

For example, when Cluster Server shuts down a service group, the resources are shutdown in the following hierarchy:

- As the file system resource is shutdown, the file system is un-mounted
- As the volume is shutdown, the volume is stopped
- As the disk group is shutdown, the disk group is deported.

Cluster Server initiates startup of the service group on another system in the cluster where each resource is started in dependent order. On the new system, the disk group will be imported, the volume started and the file system will be mounted. This entire process happens automatically in the event of a failure, significantly reducing the downtime associated with a failure or outage. This sequence could not be accomplished if the SAP application component was installed on a local system disk on one node in the cluster.
Network Resources

In addition to disk groups, applications also require specific network resources, such as Network Interface Cards (NICs) and IP addresses.

The service group definition for a SAP Central Services service group in a Cluster Server configuration includes a Cluster Server resource for the Network Interface (NIC). It also includes a resource for the IP. This resource plumbs an IP address to the host when the resource is brought online and un-plumbs the IP when the resource is taken offline.

The service group also includes a resource to manage the Disk Group and another resource to mount the file system (Mount) for the SAP application. And, finally the service group includes a resource to manage the SAP application. This resource starts the SAP application when it is brought online and shuts down the SAP application when it is taken offline.

To support automated failover, SAP application components should be configured with virtual IP addresses. If a service group becomes unavailable, Cluster Server frees the virtual IP address so it can be reconfigured on the failover host. In this way, users connect to the application without regard for its physical location.

Example Local Failover Scenario

The Symantec solution works in an SAP environment as illustrated in the following scenario.

The sample environment is a four-node cluster, with an NFS server, two application instances, the Central Services Instance, an Enqueue Replication Server and a database instance. All the four nodes of the cluster access storage from a shared disk array.

Cluster Server monitors each component with application-specific agents, and maintains "heartbeat" connections between cluster nodes to determine system availability. With this infrastructure in place, Cluster Server supports both proactive application switchover and automated failover processes.

Figure 11: Sample local cluster environment for SAP
Proactive switchover for planned downtime purposes

In a planned downtime scenario, the administrator initiates the switch of the service group to another node in the cluster. When this happens, the following processes occur:

- Appropriate application services are stopped in a clean and orderly manner.
- The virtual IP address is unconfigured and the file systems are unmounted on the current node.
- The virtual IP address is reconfigured and the file systems are remounted on the new node.
- The application services are started on the new node.

The shutdown and startup processes follow a given order.

In the first example, Server 3 (which runs both the Central Services instance and the database instance) needs preventative maintenance. There is no "spare" server in the cluster, so the application services on Server 3 need to be switched to servers performing other tasks.

The administrator first switches the Oracle database server to Server 1, which is also running the NFS server. The SAP DB Reconnect feature ensures that application servers reconnect to the relocated database instance transparently, without interruption of the current user sessions. Nevertheless, open transactions are rolled back in the DB restart phase and need to be reapplied by the user.

Next, the administrator chooses to switch the Central Services instance to Server 4. The Central Services instance will be shut down on server 3 and started on server 4 where the corresponding Enqueue Replication Server is running. If needed, the application server instances cache transactions while waiting for the Central Services instance to return. The Enqueue server reads the Enqueue Replication Server’s shared memory copy of the lock table and reinitializes the locks from this table. Once fully restored, the Enqueue server accepts connections from the application server instances, which could resume normal operations and re-acquire locks without having to redo transactions in process. The Enqueue Replication Server is stopped after successful Enqueue replica failover, Cluster Server recognizes this failure and initiates a failover to a different server (here: Server 2) in order to restore redundancy.
At this point, Server 3 is available for maintenance. When the maintenance is complete, the administrator uses Cluster Server to switch the applications back to their original configuration on the newly updated Server 3.

**Automatic failover in response to unplanned downtime**

The primary difference between a switchover and a failover is that in a failover, Cluster Server detects the failure and initiates the switch. If an orderly shutdown is not possible (i.e. in the case of a kernel panic, memory fault, or operating system anomaly) then the agent performs a more aggressive and immediate shutdown of the application. Once the application is shut down, the agent completes the process by “cleaning” the SAP instance environment, which includes removing SAP IPC resources (shared memory segments, semaphores and message queues), removing lock files, and removing the kill.sap program. At this point, the SAP instance can safely migrate to an alternate cluster node or can restart on the same node depending on the desired behavior.

Cluster Server automatically restarts the service group on other nodes of the cluster. Cluster Server uses a workload management feature to make intelligent decisions about system capacity and resource availability so that applications are hosted on the best server available within the cluster. You can also design failover policies to determine where applications are restarted.

**Site Migration for Disaster Recovery**

Creating a highly available local clustering environment protects critical SAP applications from a wide range of component failures as well as supporting preventative and proactive maintenance without service disruption. However, it still leaves companies vulnerable to site-wide disruptions. Many companies are giving their business continuity planning efforts renewed emphasis in recent years, and critical SAP applications are a logical place to start planning.

By adding data replication and global clustering to your highly available SAP environment, you gain the ability to switch over an entire SAP application between geographically-distributed data centers, quickly and accurately.

---

3 A kernel panic is an action taken by an operating system upon detecting an internal fatal error from which it cannot recover.
Primary and Secondary sites

As discussed in previous sections, global clustering depends on the existence of one or more alternate computing sites.

- The primary site is the site where the application usually runs, during normal operations.
- The secondary site is the site where the application fails over to in the event of a disaster at the primary site.

The secondary site does not need to be identical in computing resources to the primary site, provided degraded performance is acceptable. Also the secondary site might host non-productive applications which can be shut down to free up resources in case of a disaster at the primary site.

The definitions of primary and secondary site can differ between applications. While one application might have site A as its primary site, and site B as its secondary, another application might have site B as its primary and site A as its secondary site.

In any case, to support site migration at the click of a button, the production data from the primary site must already be resident, and up-to-date, at the secondary site.

Symantec Replicator Option

Storage Foundation's Volume Manager, can be used to synchronously mirror data over an extended SAN infrastructure (up to 100km, depending on the network's latency) to provide protection for metropolitan area networks. Replicator Option, the IP replication option to Storage Foundation's Volume Manager, offers the ability to consistently and reliably replicate data across IP networks.

Replicator Option replicates the contents of each volume across a wide area network to the secondary site. It is completely transparent to the application components. Unlike database-oriented solutions that replicate transactions or database blocks across distances, Replicator Option can also manage other, essential file-based data, such as database configuration files, necessary for a complete site migration. And, unlike traditional block-based approaches, Replicator Option replicates write I/O's instead of disk tracks to ensure the data is always replicated in a consistent fashion thereby guaranteeing the recoverability of the SAP application.

Replicator Option supports both synchronous and asynchronous replication.

- Using synchronous replication, the initial write is not committed until the data has been replicated successfully. This solution guarantees that there is no data loss in case of a site failure, but there will be an application performance impact because the application at the primary site is waiting for the transaction to travel to the secondary site and back before the transaction is committed at the primary site. Over long distances synchronous replication may introduce unacceptable write delays in production systems.
- Using asynchronous replication, Replicator Option commits the data at the primary site immediately and then queues replication operations for network availability. Asynchronous replication does not impact the application performance at the primary site but there may be some potential for data loss. Typical data loss between sites over long distance can be measured in milliseconds. Replicator Option is unique in the market because it enforces write order on the replicated site, ensuring data integrity and consistency, thereby guaranteeing the data will be recoverable at the secondary site.

Most organizations select asynchronous replication for long-distance, global failover scenarios.
Hardware Based Replication

As discussed in the Replicator Option section to support the site migration, the production data must already be resident and up-to-date at the secondary site. The Cluster Server agents for hardware based replication offer the ability to support failover and recovery in environments where array based replication is used to replicate the data between arrays.

The following diagram shows a typical hardware based replication set-up. The set-up has a total of four servers out of which two servers are connected to a source array at the primary site and the remaining two servers are connected to a target array at the remote or secondary site.

![Figure 14: Hardware based replication](image)

Clustering in a hardware replication environment typically consists of the following hardware infrastructure:

- The primary array, comprising one or more hosts directly attached by SCSI or Fibre Channel to a primary array containing source volumes/devices.
- The secondary array, comprising one or more hosts directly attached by SCSI or Fibre Channel to a second array containing target volumes/devices. These devices pair with the source devices in the primary array. These hosts and the array must be at a significant distance from the primary site to survive a potential disaster.
- Network heartbeats, Low Latency Transport (LLT) or TCP/IP between the two data centers to determine the health of the other site.
- In a replicated data cluster environment, all hosts are part of the same cluster. You must connect them with dual dedicated networks that support Low Latency Transport (LLT) or LLT over User Datagram Protocol (UDP).
- In a global cluster environment, you must attach all hosts in a cluster to the same array.

The Cluster Server agent for array based replication starts the replication, stops the replication, turns the replication direction when necessary, and monitors the replication link between the source and destination arrays. Symantec supports various hardware based replication technologies; however, the actual functionality depends on the specific replication technology used.

---

4 Actual functionality depends on replication technology used.
replication technologies. Some of the hardware based replication solutions that Symantec supports includes Hitachi True Copy, EMC MirrorView, and IBM MetroMirror, among others.

**Global Clusters for SAP**

Symantec Cluster Server HA/DR enables the linking of clusters from separate locations together and connecting SAP applications across clusters. This connection provides complete service level protection against an entire site failure by providing SAP application failover to the remote site.

Cluster Server HA/DR continuously monitors and communicates relevant SAP application events between clusters. Inter-cluster communication ensures that the remote cluster is aware of the state of the SAP application at all times. In the event of a system or application service failure, Cluster Server HA/DR fails over the affected services to another system in the same cluster. If the entire cluster or a site fails, Cluster Server HA/DR fails the complete SAP application over to the remote cluster at the DR site. Cluster Server HA/DR also redirects clients once the application is online to the new location.

Note that the Cluster Server service groups must include all of the components necessary to run the SAP application – not just those that represent a single point of failure in a local clustering environment. For example, you might choose to not cluster application server instances for local failover if you already run redundant dialog servers in your environment, but if you are implementing global failover you likely need to include all SAP components in the cluster, including application server instances, web servers, etc.

Here is an example of Cluster Server service group diagram which shows the resource dependencies for a SAP application with global clustering.

---

**Figure 15: Resource dependencies for a SAP disaster recovery environment**

---

5 Symantec strongly recommends clustering application server instances for local as well as global availability for easier management and operation of SAP applications.
The service group includes a Cluster Server resource for a Network Interface Card (NIC). The service group includes a resource to update the Domain Name Server (DNS) with a hostname and Virtual IP for the SAP application during global failover. It also includes a resource for IP. This resource plumbs the IP address to the host when the resource is brought online and un-plumbs the IP when the resource is taken offline.

The service group includes a resource for Hitachi True Copy (HTC) for data replication across sites for the SAP application. The service group also includes a resource to manage the Disk Group and another resource to mount the file system (Mount) for the SAP application. Finally, the Service group includes a resource to manage the SAP application. This resource starts the SAP application when it is brought online and shuts down the SAP application when it is taken offline.

The Cluster Server service group should be configured as a Global Service Group (GSG). A global service group can be brought online on any node in the global cluster (listed in the ClusterList attribute). The GSG can also failover to any node in any cluster, even across sites.

The following screenshot shows the status of the SAP Central Services global service group in the local cluster, Boston, and the remote cluster, Chicago.

The SAP Central Services failover service group is online on system vcsaix12 in the local cluster, Boston, and offline on all the nodes in the remote cluster, Chicago.
Example Disaster Recovery Scenario

To understand how the integrated Symantec solution can switch a critical SAP application environment across sites for disaster recovery, it's worth walking through a disaster recovery scenario. As with local clustering, the difference between a planned switchover and a failover is whether or not you can shut down the production instances gracefully and initiate the switchover yourself, or whether a hard failure causes the automated failover.

Even in some "disaster" situations, you may have time to perform the switchover proactively, ensuring a smoother transition. For example, in the case of a power failure you may have a short period of time in which power is available from the Uninterruptible Power Supply system, which should be more than adequate to perform the site switch. Weather disasters often come with some advanced warning as well. Validation tests performed by Symantec show that application switchover can occur in only minutes. Actual switchover time largely depends on how long the critical applications take to start.

Consider the case of a company with a production facility running a SAP application in Chicago and a DR/failover site in Boston. The Boston site could be running other services, which would then be shut down in case of a DR event. For the purposes of this example, we'll only look at the SAP application.

If the Chicago site experiences a failure, such as a power failure or flooding, an operator would be notified that the site in Chicago was down. He would then log on to the Cluster Server console from anywhere in the world to verify the site is actually not available. At that point the operator initiates switching the SAP application to the Boston data center through a series of quick and easy point-and-click operations.

After Symantec Cluster Server stops any remaining SAP application services, it would perform the following steps:
1. Stop replication: First, Cluster Server will stop any replication between the primary (Chicago) and secondary (Boston) sites. (If the primary site has experienced a dramatic failure, then replication has already stopped.)
2. Reconfigure the network: Next, Cluster Server updates the Domain Name Server (DNS) so that client network traffic is routed to the secondary site in Boston.
3. Promote the replicated data: Then, Cluster Server promotes the secondary data to primary status. If another secondary site is still available, the agent for hardware based replication or Replicator Option can replicate to another site to maintain data availability.
4. Restart services: Finally, Cluster Server starts the SAP application services in the appropriate order, bringing the SAP instance back online.

At this point, the SAP application is now running successfully at the Boston data center – typically in a matter of minutes. All SAP instances would be restarted, without maintaining their transaction state. As a result, users would have to re-establish and re-authenticate their connections by refreshing the IP address, and restart all transactions not completed during the time of the switch. Otherwise, users would try to access the application in Chicago without being aware that the application was running in a secondary site, Boston.

When the disaster has passed and the primary data center is running again, you can update the Chicago storage, restart replication, and then switch the application back to its original location, using the Cluster Server Management Console or Veritas Operations Manager. The only data sent back to the Chicago site is the data that changed while operations were occurring in Boston, so that a complete re-initialization does not have to occur between the sites.

Compare this to the processes most companies manage today. First, companies need to maintain the disaster recovery site at the same update and patch levels as the primary site – difficult when the site is physically removed from the primary data center. Coordinating change control for multiple sites for each production application presents a significant challenge. Then, when it’s time to switch an application to the disaster recovery site, IT has to replicate their data and applications at the disaster recovery site, and have no automated start-up of the
applications. Application start-up has to be done in a manual way, without the documentation being used has every item in the correct order. The process can be very time consuming and expensive, and subject to possible human error.

Symantec’s High Availability and Disaster Recovery solutions eliminate these change control problems, as all changes to the primary application (and its subsidiary components) are replicated to the disaster recovery site automatically. The failover is automated, reducing risks while improving application availability.

**Conclusion**

In many ways, the problems faced by IT organizations to maintain SAP application availability are endemic to all kinds of enterprise applications. Application complexity, high service level expectations, and constant change are factors nearly universal in today’s IT environments.

These challenges have given rise to the concept of utility computing (or cloud computing, real-time infrastructure, on-demand computing or other like terms). Utility computing is all about reducing complexity, freeing applications from physical resource dependencies and creating a dynamic IT infrastructure that aligns with IT needs. Most vendors, however, support utility computing with inflexible, incomplete point solutions, or only a blueprint, and a map to future architectures.

In contrast, Symantec’s High Availability and Disaster Recovery Solutions for SAP provide tangible, demonstrable results in a matter of days, helping reduce the complexity of the SAP application environment while improving service level delivery.

Using Symantec solutions, the SAP application is not tied to a specific server or set of hardware components – it can be relocated manually or automatically when needed. Administrators gain time to do preventative maintenance and infrastructure work, and time to respond to crises appropriately while users continue to access the critical application. Companies gain improved service levels and reduced risk from outages. IT departments can better leverage resources, consolidating capacity in clusters and multi-purposing equipment used in disaster recovery facilities.

Symantec offers a real-world solution that solves immediate needs while supporting the long-term objectives of utility computing.

---

6- This is true for applications that are replicated. This is not true for system level, Q/S level patches and firmware, which are generally not replicated. You can use Symantec Disaster Recovery Advisor to keep track of the changes to the applications and use the Fire Drill feature in Cluster Server HA/DR to simulate the DR failover scenario before performing the actual failover.
# Appendix

## Symantec Cluster Server High-Availability Agents for SAP Application

The following table gives an overview of the Symantec Cluster Server high-availability agents for SAP NetWeaver based SAP applications.

<table>
<thead>
<tr>
<th>Agent</th>
<th>Application</th>
<th>Application version</th>
<th>Availability Notes (for details please refer to SORT)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAPComponents</strong></td>
<td>SAP Components – Gateway, Webdispatcher, MDM</td>
<td>NetWeaver 04, NetWeaver 2004s, NetWeaver 7.1 / 7.3, NetWeaver MDM 7.1</td>
<td>Not available on Windows</td>
</tr>
<tr>
<td><strong>SAPContentServer</strong></td>
<td>SAP Content Server</td>
<td>6.30 and 6.40</td>
<td>Not available on Windows</td>
</tr>
<tr>
<td><strong>SAPLiveCache</strong></td>
<td>SAP LiveCache</td>
<td>7.5, 7.6, 7.7, 7.9 and all intermediate versions</td>
<td>Not available on Windows</td>
</tr>
<tr>
<td><strong>SAPNW04</strong></td>
<td>SAP NetWeaver</td>
<td>SAP R/3 4.6, R/3 Enterprise 4.7, NW04, NW04s, ERP/ECC 5.0/6.0, SCM/APO 4.1/5.0/5.1/7.0, SRM 4.0/5.0/7.0, CRM 4.0/5.0/7.0, MDM 5.5/7.0 (MDM on Windows only)</td>
<td>Available on all platforms</td>
</tr>
<tr>
<td><strong>SAPWebAS</strong></td>
<td>SAP NetWeaver</td>
<td>Process Integration (PI), Composition Environment (CE), Mobile</td>
<td>Windows only</td>
</tr>
<tr>
<td><strong>SAPNW</strong></td>
<td>SAP NetWeaver with HA-API support</td>
<td>PI, CE, Mobile, ERP, SCM with SAP Kernel 7.20 DCK or higher</td>
<td>Not available on Windows / HP-UX</td>
</tr>
<tr>
<td><strong>SybaseRS / SybaseRMA</strong></td>
<td>SAP Sybase Replication Server</td>
<td>15.7.1.x</td>
<td>Linux on x86_64 only</td>
</tr>
<tr>
<td><strong>SAPHotStandby</strong></td>
<td>SAP liveCache Hot Standby</td>
<td>7.6, 7.7, 7.9</td>
<td>Linux on x86_64, AIX 5.2/5.3</td>
</tr>
</tbody>
</table>

For details and up-to-date information about availability of these agents, please refer to the Symantec Operations Readiness Tool (SORT) at [http://sort.symantec.com/agents](http://sort.symantec.com/agents).

SAP NetWeaver with HA-API Support: The SAPNW agent is certified by SAP according to the SAP NetWeaver High Availability Cluster (NW-HA-CLU 7.30) integration certification (see [http://scn.sap.com/docs/DOC-31701](http://scn.sap.com/docs/DOC-31701))
Symantec Cluster Server High-Availability Agents for Databases Relevant for SAP Applications

The following table gives an overview of the Symantec Cluster Server high-availability agents for database relevant for use with SAP NetWeaver based SAP applications.

<table>
<thead>
<tr>
<th>Agent</th>
<th>Application</th>
<th>Application version</th>
<th>Availability (for details please refer to SORT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2UDB</td>
<td>IBM DB2</td>
<td>(9.1, 9.5), 9.7, 10.1, 10.5</td>
<td>Not available on Windows</td>
</tr>
<tr>
<td>Informix</td>
<td>IBM Informix Dynamic Server</td>
<td>7.31, 9.21, 9.30, 9.40, 10.0, 11.10, 11.50, 11.70, 12.0</td>
<td>Not available on Windows</td>
</tr>
<tr>
<td>SQLServer</td>
<td>Microsoft SQL Server</td>
<td>2012</td>
<td>Windows 2008 / 2008R2 only</td>
</tr>
<tr>
<td>Oracle, Netlsnr, ASMInst, ASMDG</td>
<td>Oracle Database with ASM</td>
<td>(10gR2, 11gR1), 11gR2</td>
<td>Not available on Windows</td>
</tr>
<tr>
<td>SAPMaxDB</td>
<td>SAP MaxDB</td>
<td>7.5, 7.6, 7.7, 7.8, 7.9 and all intermediate versions</td>
<td>Not available on Windows</td>
</tr>
<tr>
<td>Sybase,</td>
<td>Sybase ASE Database (incl. Backup Server), Sybase ASE Cluster Edition (CE)</td>
<td>Sybase ASE: 12.5.x, 15.x; Sybase ASE CE: 15.x</td>
<td>Not available on Windows (ASE CE only on Solaris SPARC and SUSE Linux)</td>
</tr>
<tr>
<td>SybaseBk</td>
<td>Sybase IQ</td>
<td>15.1, 15.2, 15.3, 15.4, 16.0</td>
<td>Linux on x86_64 and Solaris/SPARC only</td>
</tr>
<tr>
<td>SybaseRS / SybaseRMA</td>
<td>SAP Sybase Replication Server</td>
<td>15.7.1.x</td>
<td>Linux on x86_64 only</td>
</tr>
</tbody>
</table>

For details and up-to-date information about availability of these agents, please refer to the Symantec Operations Readiness Tool (SORT) at [http://sort.symantec.com/agents](http://sort.symantec.com/agents).
About Symantec
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com