Applies to:
SAP NetWeaver 7.00 and higher releases.

Summary
Introduction: SAP has long supported high availability (HA) with Windows Server Failover Clustering (in Windows 2003 it was called Microsoft Cluster Services – MSCS). Virtualization on Windows with Microsoft Hyper-V and VMware is also supported. Both VMware and Microsoft offer technologies to cluster virtual machine. How is this reflected in SAP HA for virtual environments? How is it possible to combine these technologies and achieve even higher levels of SAP System availability and business continuity? This article addresses these issues and also gives a short overview of high availability, business continuity and virtualization.

The technologies used at the time of writing are Microsoft Windows 2008 R2 (used as Hyper-V and Windows Failover Cluster Service), Microsoft System Center 2012, and VMware vSphere 4.1 and 5.0. A short preview of new Windows Server 2012 Hyper-V is also provided.

Authors: Goran Condric
Enterprise Technology Architect
SAP Global IT Enterprise Architecture

Company: SAP AG

Created on: September 2012

Reviewers: Bernhard Steigleider (SAP), Claudia Baur (SAP), Hermann Daeuble (Microsoft), Juergen Thomas (Microsoft), Karl-Heinz Hochmuth (SAP), Matthias Schlarb (VMware), Robert Boban (SAP), Samuel Lang (Connmove GmbH), Sebastian Dusch (Microsoft)

Author Bio
Goran Condric is a Enterprise Technology Architect, responsible for Virtualization and Cloud strategy in SAP Global IT Organization, driving projects related to virtualization and cloud enablement of internal SAP systems. He is an expert in SAP on Microsoft and VMware technologies, and High Availability and Business Continuity of SAP NetWeaver systems.
## Table of Contents

1. **Business Continuity** ................................................................. 3
   1.1 Planned Downtime ................................................................ 3
   1.2 Unplanned Downtime and High Availability .............................. 4
   1.3 Fault Tolerance vs. Failover ....................................................... 4
   1.4 Design of High Availability Solutions ......................................... 4
      1.4.1 HA of Redundant Components ........................................ 4
      1.4.2 HA of Single Point of Failure (SPOF) Components ............... 6

2. **SAP High Availability with Windows Server Failover Clustering in a Physical Environment** .......... 7
   2.1 SAP NetWeaver Architecture – Redundant and SPOFs Components ............................................................. 7
   2.2 6.40 SAP ABAP Cluster Architecture ........................................ 7
   2.3 SAP Cluster Architecture 7.00 (and higher) ............................... 8
   2.4 Utilizing HA to Prevent Unplanned Downtime of an SAP NetWeaver System ....................................................... 10
   2.5 Utilizing HA to Minimize the Planned Downtime of SAP Systems during the OS patching ...................... 10

3. **High Availability in Virtual Environment with Hyper-V and VMware on Microsoft Windows** ........... 12
   3.1 Server Virtualization ............................................................... 12
   3.2 High Availability and Fault Tolerance in Virtual Environment ................................................................. 14
      3.2.1 Technology Overview ..................................................... 14
      3.2.2 Advanced Configurations ................................................. 20

4. **SAP High Availability in a Virtual Environment with Hyper-V and VMware on Microsoft Windows** ...... 28
   4.1 Utilizing Infrastructure Virtualization High Availability Technologies to achieve Higher Availability of SAP Systems ................................................................. 28
      4.1.1 Protecting SAP NetWeaver with VM HA ................................ 28
      4.1.2 Utilizing VM Migration to Move an SAP System from One Hypervisor to Another ................................. 29
      4.1.3 Protecting ASCS/SCS Instance with VMware FT ................................................................. 30
   4.2 Achieving SAP Application High Availability and Business Continuity ............................................................. 31
      4.2.1 High Availability and Business Continuity of Application Servers - AS (PAS and AAS, or CI and DI) ............ 31
      4.2.2 High Availability and Business Continuity of SAP SPOFs – (A)SCS and DB Instances) .......................... 34
      4.2.3 Examples of HA and Business Continuity of SAP Systems in a Virtual Environment – Complete Picture ... 38

5. **Sneak Preview of new Windows Server 2012 OS and Hyper-V** ................................................................. 40

6. **SAP High Availability and Business Continuity in Virtual Environment vs. Physical Environment** .... 44

7. **Related Content** ......................................................................... 46

8. **Copyright** .................................................................................. 47
1 Business Continuity

Business continuity (BC) means how to keep your systems and services available, e.g. how to prevent downtime for your business system. It is the essence of mission-critical applications being provided quickly and reliably to clients expecting your services to be continuously available. A business IT system is the heart of a company. Every minute of unavailability or downtime, for whatever reason, can cause hundreds of thousands of dollars in lost income. For example, if you have an online shop, unavailability means that you cannot sell your product. If your IT system controls production, downtime means production is stopped! Therefore, it is a must to ensure business continuity and availability of an IT system.

The reasons for downtime and unavailability can be generally divided into two groups:

- Planned downtime
- Unplanned downtime

![Figure 1: Business Continuity covers both planned and unplanned downtime.](image)

1.1 Planned Downtime

Planned downtime can be controlled. Reasons for planned downtime include hardware maintenance, operating system maintenance (installing patches or upgrading OS), hypervisor maintenance (installing patches or upgrading hypervisor) and application maintenance such as an SAP system kernel patch, or upgrade of an SAP system. All these activities can cause downtime of your system. However, you yourself can plan when to perform these activities, that is, you can choose the most appropriate time.

To minimize the planned downtime of SAP Systems, SAP is addressing this issue with the following technologies:

- **Rolling kernel switch** – used for the SAP kernel patch (see SAP Note [953653](https://support.sap.com)). To patch the SAP Kernel there is no need to completely shut down SAP Systems. SAP Instances are assigned new kernel patches in sequence rather than simultaneously.
• **Near Zero Downtime** – used to minimize downtime during an SAP upgrade or Enhancement Package Installation.

In this document we do not discuss planned downtime of the SAP software itself.

### 1.2 Unplanned Downtime and High Availability

Unplanned downtime cannot be controlled. There are different reasons for it – hardware failure, software failure, disaster of a site etc. **High Availability** (HA) is a term often used in connection with unplanned downtime. HA is a complex topic. It does not only cover making your software highly available, but the whole IT infrastructure (networks, routers, power supply, storage etc.) must be designed with HA in view.

This document is restricted to SAP software HA and failover solutions in physical and virtual environments.

### 1.3 Fault Tolerance vs. Failover

Fault tolerance indicates no downtime at all. Usually, failover is associated with some downtime, but it is usually short.

Many fault tolerant solutions are hardware-based, where the crash of a physical machine does not cause the crash of the OS; OS and applications continue to run without interruption. Still direct application protection and monitoring is usually not covered by such solutions – an aspect that must be dealt separately. What is most important is that end user service is not interrupted, and this is often achieved through monitoring and protection of critical applications.

### 1.4 Design of High Availability Solutions

When we design an HA solution, we try to make sure that unavailability of one component does not cause unavailability of the whole system. A system can have different components. Some of those components are redundant, and some are unique.

#### 1.4.1 HA of Redundant Components

One way to achieve HA is to make components redundant, e.g. to have more than one and to use some kind of load balancing to distribute the load between them. In this setup, unavailability of one component does not cause unavailability of the whole system, since other component(s) of the same system continue working.

For example in an SAP system, SAP application servers are redundant components (it is assumed here that we have a separate (A)SCS instance). If we install two (or more) SAP application servers on two (or more) different physical machines and we use load balancing, HA of the SAP application server can be achieved.

If one physical machine where an SAP application server is installed goes down (for any reason), another SAP application server on another machine can continue running and providing services to the SAP users. The new users then connect through load balancing to the available SAP app servers.
Three SAP application servers (AS) are installed on three OS one primary (PAS) and two additional (AAS) application servers. Load balancing distributes user requests evenly.

Hardware failure on first machine: this causes OS 1 and all applications on it to crash, e.g. primary application server (PAS). All user connections to PAS are lost, and all open transactions are rolled back.

First machine is down and all new user request are distributed by load balancing to the two remaining AAS running on OS 2 and OS 3

**Figure 2: Redundancy of SAP Application Servers**
1.4.2 HA of Single Point of Failure (SPOF) Components

However, it is not always possible to make all components redundant – for example, because there are components which are unique to one system. These components are called Single Points of Failure (SPOFs) and they must be protected with some kind of HA failover solution. Windows Server Failover Clustering – WSFC (in Windows 2003 it was called Microsoft Cluster Services – MSCS) is one such technology that offers a mechanism to protect SPOFs.

A failover cluster is a group of independent computers, or nodes that are physically connected by a local-area network (LAN) or a wide-area network (WAN) and that are logically connected by cluster software. Normally, if a server that is running a particular application crashes, the application remains unavailable until the server is fixed. Failover clustering addresses this situation by detecting hardware or software faults and immediately performing a pre-configured action, which can be restarting the application on the same or another server node without requiring administrative intervention — a process known as failover. Failover also implies short downtime of a HA service while the service or application is moved from one machine to another. The service needs to be stopped on one machine and started on another one.

For example, the database management system (DBMS) is an application that is SPOF and has to be protected with a failover cluster solution or different database mirroring solution.

**Figure 3:** Protection of SPOF (DBMS) with Windows Server Failover Clustering Solution
2 SAP High Availability with Windows Server Failover Clustering in a Physical Environment

Understanding SAP HA in a physical environment is a prerequisite for extending it to operate in a virtual environment. Therefore this section discusses this briefly.

2.1 SAP NetWeaver Architecture – Redundant and SPOFs Components

To correctly design an SAP HA solution, it is important to identify redundant as well as SPOF components.

In an SAP system on Windows, SPOFs are:

- SAP message server process
- SAP enqueue server process
- SAP global host name and IP address
- SAPMNT share
- SAP global files
- Database management system (DBMS)

**Note:** The SAP enqueue server process is used to manage logical locks of the SAP transactions in the lock table. The lock table contains the logical database locks of the ABAP or Java runtime environment of the SAP System. This table is stored in the main memory. If the enqueue server process stops or crash, the enqueue lock table is lost and all open transactions are therefore lost – that is, the SAP system performs a rollback.

Windows Server Failover Clustering is used to protect these SPOFs.

2.2 6.40 SAP ABAP Cluster Architecture

SAP NetWeaver 6.40 ABAP has the following instances:

- **Central instance (CI),** which consists of dialog work process (which forms an application server) and SPOFs components like message server process, enqueue server process, SAPMNT share and global files
- **DBMS instance**
- One or more **dialog instances** (which consist of dialog work processes)

Although the CI is an application server (and application server are redundant components), the fact that SPOF components such as the message and enqueue server processes etc. are part of the CI is the reason that the CI is now clustered. Another SPOF is the DBMS. Until 6.40 the SAP central instance (CI) and DBMS were clustered.
2.3 SAP Cluster Architecture 7.00 (and higher)

As of SAP NetWeaver 7.00 SAP (and for Java-only SAP systems, as of 6.40), the ASCS instance for ABAP systems and the SCS instance for Java systems was introduced. This contains only SPOF components e.g. message server process, enqueue server Process, SAPMNT share, SAP global host name with IP address and global files.

**Note:** SCS stands for SAP Central Services

The CI contains only application server work processes. Work processes are redundant components. Therefore, by installing two app servers on two different machines solved the problem of HA for application work processes: one CI and at least one DI.

**Note:** As of 7.10 (and higher), the terms central instance (CI) and dialog instance (DI) have been changed to primary application server (PAS) and additional application server (AAS).

Therefore, only the ASCS/SCS and DBMS were clustered, not the CI.

**Note:** For backward compatibility, the instance name of PAS - for example, CI - is still the same as in 640 (for example, DVEBMGS<InstanceNumber>), although it no longer contains message (M) and enqueue (E) processes.

ASCS for an SAP NetWeaver 7.0 ABAP system is currently available only in...
an HA installation and is not part of a non-HA installation. As of SAP NetWeaver 7.3, the ASCS is also part of the standard (non-HA) installation.

It is planned to offer an ASCS instance installation for a non-HA installation for all SAP NetWeaver 7.0 and higher products (most probably beginning of 2013 – this is still not officially confirmed).

SCS for a Java system is available as of the 640 kernel and is always installed.

Figure 5: New 7.00 SAP High Availability Architecture with Clustered (A)SCS and DBMS Instances

There are many benefits of this new HA architecture:

- Failover of an ASCS/SCS instance is much faster than failover of a CI as it contains only two lightweight processes (failover takes approximately 15 to 20 sec).
- The SAP user connected to an SAP application server is not disconnected during the failover of the ASCS/SCS instance, because the CI is no longer clustered. Therefore, the end user does not notice the failover.
- With the ASCS/SCS instance it is possible to install the enqueue replication server (ERS) instance and save the replicated enqueue table (which holds all opened DB transactions) during the failover process, e.g. a rollback of opened transactions does not happen. This means we have achieved a type of fault tolerance for the enqueue server.
Note: Although the Microsoft Windows Failover Cluster supports more than two cluster nodes, SAP only supports the installation of an ASCS or SCS instance on two cluster nodes due to the locally installed Enqueue Replication Server (ERS) instances. The reason is that local ERS instance replicates the lock table from one host to one other host only. It is currently only possible to replicate to one other ERS instance. However, there are several scenarios where it might be useful to fail over an ASCS or SCS instance to a third or fourth cluster node, even if the lock table cannot be replicated to these Cluster nodes.

For more information, see:
SAP Note 1634991 - How to install an ASCS or SCS instance on more than 2 cluster nodes?

Note: The prerequisite for enqueue replication is the (A)SCS instance - ERS is not supported for the "old"-style HA architecture where CI (PAS) which contains message and enqueue process is clustered.

As of 70 SR3 installations, the ERS is always installed in a WSFC HA installation.

- Users can choose if they want to install application servers locally on MSCS nodes and in this way better utilize the hardware resources of cluster machines.

This is the reason that SAP is strongly recommending migrating to the new SAP HA architecture.

To simplify the migration procedure, SAP is offering an migration procedure for existing 7.0 and higher SAP Systems that have the old cluster architecture (clustered ABAP CI or ABAP+Java CI), where you can split old CI on ASCS Instance and the new PAS (SAP Note 1011190 - MSCS:Splitting the Central Instance After Upgrade to 7.0/7.1)

For more information about SAP HA with Windows Failover Cluster architecture, see the white paper "SAP Applications on Windows Server 2008 R2 - High Availability Reference Guide.

2.4 Utilizing HA to Prevent Unplanned Downtime of an SAP NetWeaver System

As already mentioned, high availability of the SAP system is fully realized when you cluster SAP SPOFs ((A)SCS and DB Instance) utilizing the WSFC cluster solution and installing at least two application servers on two different server, using load balancing to distribute user load between application servers.

2.5 Utilizing HA to Minimize the Planned Downtime of SAP Systems during the OS patching

From time to time we need to patch Windows OS, which might require a reboot of the OS. Or we need to do hardware maintenance and shut down the OS. Shutting down and rebooting of OS would cause downtime of SAP components and potentially whole SAP systems.
To patch the Windows OS where the SAP application servers are running we can apply the following procedure:

- Remove the SAP application server from load balancing - this prevents the new SAP user logging on to it.
- Execute a soft shutdown of SAP application server – notify logged on users that the AS is going to be shut down after some time, wait for the jobs to be finished, etc.
- When the SAP application server is stopped, patch the OS and reboot if necessary
- When the OS patching has finished, start SAP AS and join SAP load balancing
- Repeat the procedure for all other SAP application servers

This procedure for patching SAP application servers applies independently if SAP SPOFs (e.g. DBMS, (A)SCS instance and CI) are clustered or not.

If SAP SPOFs are not clustered, the main downtime of SAP SPOF is caused by the Windows server reboot time.

Failover clusters are primarily used as an HA solution to protect SPOFs from unplanned downtime of hardware, OS, or applications. However, failover clusters can also help to reduce the planned downtime of SAP SPOFs during the maintenance of the hardware and Windows cluster nodes operating system maintenance.

To minimize downtime of clustered SAP SPOFs (and the whole SAP system) prior to patching of a clustered Windows OS node where SPOFs are running, we can move (fail over) SPOFs to another node and then patch that Windows cluster node. When the reboot is finished, we can fail over the SPOF back to that patched windows cluster node, and then patch the second, third etc. Windows cluster nodes.

For more information about how to automate the whole Windows patch procedure for clustered SAP systems, see the following blog: [Automated Windows Patching in a Microsoft Private Cloud for SAP](https://scn.sap.com)

**Note:** Failover of clustered DBMS cause a short downtime of DBMS.

<table>
<thead>
<tr>
<th>Cluster Protection</th>
<th>Unplanned Downtime (Failure)</th>
<th>Planned Downtime (Maintenance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Table 1:** Utilizing Failover Cluster to Minimize Unplanned and Planned Downtime of Hardware, OS and Applications
3  High Availability in Virtual Environment with Hyper-V and VMware on Microsoft Windows

3.1  Server Virtualization

Server virtualization is the ability to virtualize server workloads. Server virtualization can save businesses money and simplify management overhead by allowing a reduction in the number of required physical servers due to server consolidation.

Server virtualization lets you virtualize entire computers by running multiple operating systems on a single physical computer (typically server-class hardware). Each guest operating system thinks (if operating systems could think) that it owns the computer and has exclusive use of the computer's hardware resources (or to whatever subset of the total machine resources that have been allocated to the virtual machine). Each operating system is therefore said to be running in a separate virtual machine (VM), with these multiple virtual machines running on the same physical computer. In a typical non-virtualized environment, only one operating system can run on a computer at the same time.

Virtual Machines (VM)

A virtual machine is a computing environment that is implemented in software and that abstracts the hardware resources of the physical computer so that multiple operating systems can run simultaneously on a single computer. Each operating system runs in its own virtual machine and is allocated logical instances of the computer's processors, hard disks, network cards, and other hardware resources. A fully virtualized operating system behaves as if it exclusively controls the underlying physical computer's hardware. A para virtualized operating system, respectively para virtualized components like device drivers, are aware of the own state of virtualization and therefore are able to directly communicate with the hypervisor. An operating system running inside of virtual machine is often called Guest Operating System (Guest OS).

Hypervisors

A hypervisor is a virtualization platform that enables you to run multiple operating systems on a single physical computer called the virtualization host. The main function of the hypervisor is to provide isolated execution environments for each virtual machine and to manage access between the guest operating systems running in virtual machines and the underlying hardware resources on the physical computer.
SAP supports Hyper-V and VMware ESX Server to run SAP systems inside a Microsoft Windows guest OS.

More info: [SAP Community Network - Virtualization on Windows](https://scn.sap.com)

**Figure 6:** Hypervisor Supporting Guest OSs Running as VMs
3.2 High Availability and Fault Tolerance in Virtual Environment

3.2.1 Technology Overview

The following technologies are applied in the virtual environment:

- Virtual machine high availability (VM HA) – sometimes referred to as host clustering
- Guest clustering
- Virtual machine migration (VM migration)
- Fault tolerance (FT)

Virtual Machine High Availability (Host Clustering) with Hyper-V and VMware

Host clustering is used to protect your guest VMs. As the cluster software that controls a VM is installed on a hypervisor running on physical host machine, this type of clustering is often called "host clustering".

Host clustering offers us following benefits in unplanned downtime of hardware, hypervisor, or guest OS (VM).

If the host fails due to hardware or hypervisor software problems, all VMs running on that machine also crash. Host clustering offers automatic recovery, and VMs are cold restarted on a surviving server.

Figure 7: VM High Availability - Protection from Unplanned Downtime of Hardware or Hypervisor
In addition, host clustering offers health monitoring of the VM – if the VM crashes or becomes unresponsive, the VM health monitoring detects this and executes predefined actuation (restart the VM on the same physical machine or failover and start on another machine).

**Figure 8: VM High Availability - VM Guest OS Monitoring**

Microsoft Hyper-V
Host clustering with Hyper-V is implemented using existing cluster technology called Windows Server Failover Clustering which is installed inside the parent partition of Windows Server 2008 (R2) x64.

**Note:** With Windows Server Failover Clustering installed on the physical machine, you can cluster not only VMs but also other resources types like database software, file shares etc. or you can also install some other software on the parent partition. However, if the host is promoted to a Hyper-V host, Microsoft does not recommend running any software on the parent partition except VMs – that is, it is not recommended to cluster and protect anything other than VMs.

It is strongly recommended to run all applications inside VMs.

Microsoft TechNet article: [Hyper-V: Hyper-V should be the only enabled role](https://technet.microsoft.com/en-us/library/hh831894.aspx)

VMware
Host clustering with VMware is implemented with VMware’s own cluster technology called VMware HA (which is not related to Windows Server Failover Clustering)
**Guest Clustering**

To protect applications themselves (e.g. SPOFs), you have to use cluster software that protects the respective applications and that is installed inside the VMs. Windows Server Failover Clustering is one solution which is used to protect applications and which is supported by SAP.

In a guest cluster implementation, the Windows Server Failover Clustering service runs on the Windows guest operating system in the virtual machine, which is why this type of clustering is often called “guest clustering”. This type of clustering provides high availability for applications that are hosted within the virtual machines, e.g. applications and services move (e.g. failover) from one VM to another VM.

Below is an example of a guest cluster where MSCS is installed in two VMs, both of them are running on different physical hypervisors, and DBMS is a protected application which can fail over from one VM to another:

The guest clustering offers:

- **Application health monitoring**
  If an application or service crashes or hangs, it is restarted or moved to another VM.

- **Application mobility**
  An application or service can be moved to another VM, which is useful to prevent application downtime when doing guest OS maintenance or patching.
Both Microsoft and VMware support guest clustering with Windows Server Failover Clustering.

**Note:** For Microsoft Failover Guest Cluster you have to use shared disks.

WSFC Guest Cluster on Windows 2008 R2 Hyper-V is currently leveraging iSCSI. On VMware, consult VMware [KB 1037959: Microsoft Clustering on VMware vSphere: Guidelines for Supported Configurations](https://scn.sap.com)

---

**Virtual Machine Migration**

Microsoft and VMware offer technologies where VMs can seamlessly move from one server to another without affecting the network connectivity. All client connections to VM (like RDP) or to any software running inside of VM are not lost. Of course, this is only possible in planned downtime, where both source and target physical machines are up and running.

![VM Migration Diagram](image)

VM is running on hypervisor 1. Users are connected to it.

VM migration is started. Users are connected to VM.

VM migration is finished. VM is running on hypervisor 1. No user connection to VM or applications was lost.

**Figure 10:** VM Migration
Hyper-V has two technologies which enables us to move VM from one server to another:

- Live Migration – No downtime of VM, e.g. with no client downtime
  Live Migration is supported on Windows 2008 R2 and higher
- Quick Migration – Session state saved to disk, client loses connection
  Quick Migration is supported on Windows 2008 and higher.

Customers should use Live Migration as it offers more benefits than Quick Migration.

VMware has also a technology for moving VM from one server to another with no client downtime:

- vMotion

This technology is useful, when we want to do:

- Hypervisor or host maintenance – for example we need to do hardware maintenance where we have to shut down the hypervisor machine, or we need to do hypervisor software patching and machine reboot is required.
- Scaling and load balancing the physical hypervisor machine – sometimes hypervisors reach their limit in RAM and CPU utilization and we want to move VMs from a heavily loaded hypervisor machine to another hypervisor physical machine with more free resources.

**Note:** For load balancing you have to use additional products in addition to migration.

VMware Distributed Resource Scheduler (DRS) is a VMware product.
Microsoft System Center Virtual Machine Manager (SCVMM) 2012 is a Microsoft product.

*Figure 11: Load Balancing of Hypervisor Host Cluster*
VM migration is NOT applicable for:

- Unplanned downtime of the infrastructure
- Application-level HA

**Fault Tolerance (FT)**

Fault tolerance means no downtime at all. Failover is always associated with some downtime (usually a short one).

VMware has a **hardware** fault-tolerant solution that delivers no downtime for VMs in an unplanned environment. When VMware FT is enabled on a virtual machine (called the Primary VM), a copy of the Primary VM (called the Secondary VM) is automatically created on another host (with identical amount of RAM and CPU as in the Primary VM). In the event of a hardware failure that causes the Primary VM to fail, the Secondary VM immediately picks up where the Primary VM left off, and continues to run without any loss of network connections, transactions, applications or data. The Secondary VM becomes Primary VM; a new Secondary VM is created and fault tolerance is re-established in a short period of time.

It is a better solution to VM HA, where a crash of the hypervisor host causes the VMs to crash (and the applications running inside), resulting in a restart of the VM on another cluster host.

However, the FT solution is not monitoring the health of the VMs itself, but you can combine it with VMware features called VM Monitoring and VM HA. VM Monitoring will detect VM unresponsiveness (“blue screen” on the Windows guest OS) and the VM HA will automatically restart the failed VM.

FT does not protect the application running inside of VM.

**Note:** If you run a VM as fault tolerant VM, there is a VM limitation in vSphere 5.0 with a maximum of 1 CPU and 64 GB RAM.
3.2.2 Advanced Configurations

To implement solutions which require high level of availability and flexibility, it is possible to combine some of above mentioned technologies.

Combining Guest Clustering and Host Clustering (VM HA), VM Migration

It is possible to combine guest clustering with:

- VM HA (host clustering)
- VM migration

This provides a higher level of flexibility and availability. The downside is that such solutions are more complex.

Figure 12: Combining Guest Clustering with VM HA (Host Clustering) and VM Migration
Combining Guest Clustering with Host Clustering (VM HA) to Reduce Unplanned Downtime

If we only use guest clustering without host clustering, downtime of the hypervisor means downtime of the VMs – that is, downtime of the guest cluster node. Let’s take an example where we have 3 hypervisors (no host cluster configured) and two guest clusters.

VM A and B are configured as two guest cluster nodes and are running on hypervisor 1 and 2. The DBMS is clustered application running inside of VM A.

Failure of hypervisor 1 causes failure of VM A, and the DBMS. The guest cluster automatically executes failover of the DBMS to VM B.

DBMS is up and running on VM B. The guest cluster consists now of only one node with VM B.

In the event of hypervisor 2 failure, VM B is down, as well as DBMS and the whole guest cluster.

Figure 13: Using Guest Clustering without a Host Cluster
The ability to combine a host cluster (VM HA) with guest clustering gives us the possibility to stretch the nodes of the guest cluster across more nodes of the host cluster. Guest clustering protects clustered services between WSFC nodes, and host clustering protects VMs against host failures.

Below is an example of a host cluster consisting of 4 hypervisor hosts. We have a guest cluster with 2 VMs, VM A and VM B. The DBMS application is protected with a guest cluster.

VM A is running on hypervisor 1, and VM B is running on hypervisor 2. DB cluster group is running on VM A node.

Hypervisor 1 failure occurs. This causes failure of VM A and all the software running on it, e.g. also the DB software. The guest cluster recognizes failure of the DBMS and executes failover of the DB group to VM B. The host cluster also executes VM A failover to hypervisor 3.

VM A is started and joins the guest cluster, which is now complete.

Hypervisor 2 failure occurs. This causes failure of VM A and all the software running on it, including the DB software. The guest cluster recognizes failure of the DBMS and executes failover of the DB group to VM A. The host cluster also executes VM B failover to hypervisor 4.
VM B is started and joins the guest cluster. The guest cluster is now complete.

**Figure 14:** Combining Gust Clustering (DBMS is a Clustered Application) with VM HA (Host Clustering)

**Note:** For productive usage, it is very important that guest cluster VMs do NOT run on the same physical hypervisor machine.

If all of the guest clusters VMs are running on one hypervisor and this hypervisor crashes, it brings down all guest cluster VMs. This means it brings down the whole guest cluster and all protected cluster applications.

On the other hand, if you run guest cluster VMs on different physical machines, the unplanned downtime of one hypervisor server only causes one guest cluster VM to fail – the remaining VM continues to run with a protected clustered application.

If VM HA and VM Migration are used for guest cluster VMs, it is important to set so called anti-affinity rules, which define that VMs which are part of the same guest cluster must NOT run on the same hypervisors. These rules policies are automatically deployed, without user intervention.

You can find more details on setting anti-affinity rules for VMs on Hyper-V and VMware in Related Content.

For testing purposes you can run both VMs on the same physical machine.

Both Microsoft and VMware support Windows Server Guest Clustering in combination with their own VM HA technologies.
Combining Guest Clustering (WSFC) and VM Migration to Eliminate Planned Downtime

Sometimes we have to do hardware maintenance or hypervisor maintenance. This requires downtime or reboot of the hypervisor. Migration of guest cluster VMs to another hypervisor can be done without any downtime of guest VMs, including all applications running inside. This also includes clustered software. Migration of the clustered VM from one hypervisor to another on which a clustered group is running does not cause any downtime of that clustered software (the VM migrates and the cluster group continues to run on it). This means that there is no need to perform failover of the clustered group in order to move clustered application from one host (hypervisor) to another.
VM A is running on hypervisor 2 and VM B is running on hypervisor 3. DB cluster group is running on VM A.

Migration of VM A from hypervisor 2 to hypervisor 1 is initiated.

At the end, VM A is migrated without downtime to hypervisor 1. The clustered DB group also has no downtime, and it continues to run on VM A, as before.

**Figure 15:** Combining Guest Clustering (DBMS in a Clustered Application) with VM Migration
Microsoft supports VM Migration (Live Migration) where VMs are nodes of a guest cluster.

VMware does not support VM Migration (vMotion) where VMs are nodes of Guest Cluster.
For more information, check the VMware Knowledge Base: Microsoft Clustering on VMware vSphere: Guidelines for Supported Configurations.

**Combining Guest Clustering (WSFC) and Hypervisor Load Balancing**
Microsoft supports load balancing of the hypervisor cluster (using SCVMM and Live Migration), where VMs are nodes of the guest cluster.

VMware has limited support for load balancing of hypervisor clusters with DRS where VMs are configured as guest clusters. DRS can be activated only while initially starting and placing a VM on a hypervisor host. vMotion cannot be used to migrate VMs from one host to another.

For more information, check the VMware document Setup for Failover Clustering and Microsoft Cluster Service (ESXi 5.0, vCenter Server 5.0).

**Combining Guest Clustering (WSFC) and VMware Fault Tolerance**
VMware does not support combining guest clustering with VMware Fault Tolerance.

For more information, check the VMware document Setup for Failover Clustering and Microsoft Cluster Service (ESXi 5.0, vCenter Server 5.0).
Tables 2 and 3 give an overview of application and virtualization HA technologies and how they can be used for both preventing unplanned and planned downtime, and increasing overall business continuity.

<table>
<thead>
<tr>
<th>Failure Type</th>
<th>Host Cluster VM HA (VMware &amp; Hyper-V)</th>
<th>Guest Cluster Microsoft WSFC</th>
<th>VMware FT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Failover Protection</td>
<td>FT Protection</td>
<td>Failover Protection</td>
</tr>
<tr>
<td>Host Hardware Failure</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Hypervisor Failure</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Guest OS VM Failure</td>
<td>✔️</td>
<td>(in combination with VM HA &amp; VM Monitoring)</td>
<td>✔️</td>
</tr>
<tr>
<td>Application Failure</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Table 2:** Virtualization and Application HA technologies for Preventing **Unplanned Downtime**

<table>
<thead>
<tr>
<th>Maintenance Type</th>
<th>Host Cluster VM Migration (VMware &amp; Hyper-V)</th>
<th>Guest Cluster Microsoft WSFC</th>
<th>VMware FT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Failover Mode</td>
<td>Zero Downtime</td>
<td>Failover Mode</td>
</tr>
<tr>
<td>Host Hardware Maintenance</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Hypervisor Maintenance</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Guest OS VM Maintenance</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Application Maintenance</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Table 3:** Virtualization and Application HA technologies for Eliminating **Planned downtime**, e.g. to achieve zero downtime
4 SAP High Availability in a Virtual Environment with Hyper-V and VMware on Microsoft Windows

4.1 Utilizing Infrastructure Virtualization High Availability Technologies to achieve Higher Availability of SAP Systems

4.1.1 Protecting SAP NetWeaver with VM HA

You can utilize VM HA to protect an SAP System. Here is an example of a central SAP system protected with VM HA:

A central SAP System is installed on a protected VM.

Hypervisor 2 and the VM crash, together with all SAP processes. End users lose connection to the application server. The host cluster executes the VM failover process.

The VM is restarted on hypervisor 1. After SAP system start (manually or automatically), end users can reconnect to the SAP system.

**Figure 16:** Protection of an SAP System with a VM HA

Of course you can distribute SAP instances across multiple VMs and protect them with VM HA.

**Note:** It is important to mention that VM HA primarily protects VMs and NOT applications. VM HA does not offer high availability for SAP applications, but it does offer infrastructure HA and therefore indirectly “higher availability” of SAP systems.
To ensure automatic start of the SAP System, you have to add the following parameter to the start profile of all instances:

\[\text{Autostart} = 1\]

This virtualization feature gives higher availability for SAP systems compared to SAP systems installed on physical hardware without a HA cluster, since VMs and all software running inside are decoupled from the physical hardware.

### 4.1.2 Utilizing VM Migration to Move an SAP System from One Hypervisor to Another

VM migration is fully transparent to an SAP System. You can fully migrate a VM with a SAP application from one hypervisor to another. End users do not lose connections (like SAP GUI or web browser). In this way you can achieve **zero downtime** for your SAP system.

Here is an example of the migration of a central SAP System.

![Diagram of VM migration](image)

**Figure 17:** Moving SAP Systems with VM Migration from One Physical Machine to Another with Zero Downtime.

You can distribute SAP instances across multiple VMs.

As mentioned earlier, you can use this in a **planned downtime environment**, where both hypervisors are up and running.

This virtualization feature gives us zero downtime for SAP systems, which does not exist in a physical environment.
4.1.3 Protecting ASCS/SCS Instance with VMware FT

As FT is supported for VMs with 1 CPU and 64 GB of RAM, it is appropriate for smaller application loads like ASCS/SCS instance.

As already mentioned, VMware FT solution is a hardware FT solution, which enables VM fault tolerant protection from hardware and hypervisor unplanned downtime. FT in combination with VM Monitoring and VM HA, will protect Windows VM from "blue screen" crash. More availability of VM would reflect itself on more availability for application, e.g. ASCS/SCS instance.

Still, FT is not covering application monitoring – in the case of an ASCS/SCS crash (due to ASCS/SCS process crash or OS crash); no action for ASC/SCS recovery will be taken. An ASCS/SCS crash would cause the loss of the enqueue lock table, and the rollback of all open transactions.

For planned downtime and patching of Windows OS, which may require a Windows OS reboot, the ASCS/SCS will be down during the OS reboot process. This will also cause loss of enqueue lock table, and rollback of all open transactions.
4.2 Achieving SAP Application High Availability and Business Continuity

Utilizing virtualization HA technologies like VM HA and VM Migration, we can achieve higher availability for SAP systems as well. However, as mentioned before, these solutions do not protect SAP applications.

As mentioned before, SAP NetWeaver 7.0 (and higher) ABAP, Java and ABAP+Java have the following components/instances:

- One or more AS Instances (redundant components)
- ASCS/SCS instance (SPOF)
- DB instance (SPOF)

To achieve application HA, all SAP System components must be protected. We will discuss separately how to achieve HA for each of the SAP instances.

4.2.1 High Availability and Business Continuity of Application Servers - AS (PAS and AAS, or CI and DI)

The SAP AS is not a SPOF. As mentioned previously, in non-virtual environments it is necessary to have at least two ASs on two different OS hosts. If one host crashes, the SAP AS on that host also crash whereas another AS on another host continues running.

The approach to provide AS HA in virtual environments is similar to that in physical environments – we need to install at least two ASs in two different VMs. The two VMs must run on different hypervisors, as a crash of one hypervisor causes all VMS to crash, together with the software running inside.

Three SAP application servers are installed on three VMs. VMs are running on different hypervisors. User requests are load-balanced.

The first hardware box crashes, which also crash hypervisor 1, VM1 and all applications on it, include the primary application server (PAS). All user connections to PAS are lost and all open transactions are rolled back.

The first hardware box is down and all new user requests are load-balanced between the two remaining AASs running on VM2 and VM3.

Figure 18: Distributing redundant SAP Application Servers across multiple hypervisor hardware boxes.
As you can see, approach is similar like in physical environment described on Figure 2.

**Using VM HA to reduce Unplanned Downtime of Application Servers**

Distributing applications servers across the different hypervisors is enough to achieve application servers HA.

Still we can leverage VM HA feature for the VM running application servers as described in Figure 19:

**Figure 19:** Utilizing VM HA to Protect SAP Application Servers from Unplanned Downtime of Hardware and Hypervisors

With VM HA we can additionally protect application servers from unplanned downtime of hardware and hypervisor, and get them up and running on another physical box much faster. This feature increases overall availability of application servers, as well as the complete system. This advantage is not possible in the physical world where the OS is bound to the hardware.

**Note:** Set anti-affinity rules to keep (at least) two VMs with two ASs running on separate hypervisor hosts.

To ensure automatic start of the AS, add start profile `Autostart = 1` parameter to the AS.
Using VM Migration to Eliminate Planned Downtime of Hardware and Hypervisor

In a planned downtime environment, VM migration (vMotion and Live Migration) can be used to move VMs from one host to another without any downtime of the OS and AS. All SAP users connected to the AS retain their connections.

This feature can be used to avoid downtime for maintenance work on the hardware or hypervisor (like installing new patches), which often requires shutting down or rebooting the hypervisor. In the physical world, if we need to do hardware maintenance, this often causes downtime of the OS and application server. With VM migration, we can achieve zero downtime of the SAP system for the hardware maintenance.

Note: VM Migration does not help us maintain the guest OS or SAP AS, which might require a reboot of the guest OS or a restart of the SAP AS.

Using Load Balancing to Scale Hypervisor Load

Both on Hyper-V and VMware you can activate automate load balancing of the hypervisor cluster (which leverages VM migration) for the VMs where the AS is installed without any limitations.
4.2.2 High Availability and Business Continuity of SAP SPOFs – (A)SCS and DB Instances

Guest Clustering

SCS/ASCS and DB instances are two SPOFs of SAP NetWeaver. Using just VM HA only gives us protection of the guest OS VMs against hardware, hypervisor, or guest OS failures, which offers advantages in comparison to running ASCS/SCS in physical non-HA environments. It is important to mention that VM HA does not offer protection against application failures of ASC/SCS nor does it save the enqueue table. In addition, VMware FT offers fault-tolerance protection in the event of hardware or hypervisor problems, but it does not protect us at all against application failures, and it does not protect the enqueue table.

To fully protect the ASCS/SCS against hardware, hypervisor, guest OS, and application failures, it is necessary to use Windows Sever Failover Cluster (WSFC) installed inside VMs in a guest cluster. Using WSFC also automatically protects the enqueue tables through the ERS instance.

Figure 21: Guest cluster – WSFC installed on 2 VMs. VMs runs on different hypervisors. Guest cluster protects SAP SPOFs (A)SCS and DB instance. The ERS is installed locally on 2 VMs and used to protect the enqueue lock table.
Combining Guest Clustering with VM HA (Host Clustering) and VM Migration to protect SAP SPOFs

Using only guest clustering provides a similar setup to that in physical clustering (compare Figure 5) – each one of two VM runs on two separate hypervisor hosts. Currently SAP supports a two-node WSFC cluster for (A)SCS. One reason for this limitation is that an ASC/SCS instance that is combined with ERS instances must be configured on a two-node cluster, even if we want a Microsoft WSFC cluster with more than two nodes.

![Graph of WSFC](image)

**Figure 22:** Three-Node Windows Server Failover Cluster in Physical Setup where (A)SCS Must be Configured on Two Nodes

Generally, the ability to run clustered services on a higher number of cluster nodes increase overall availability.

The ability to combine guest clustering with VM HA and VM Migration enables us to stretch a two-node guest cluster across multiple hypervisor host clusters.
Combining Guest Clustering with VM HA (Host Clustering) to Reduce Unplanned Downtime of SAP SPOFs

The ability to combine host cluster (VM HA) together with guest clustering means that we can stretch 2-node guest clusters across a multiple-node host cluster. Guest clustering protects clustered services between a 2-node WSFC, and host clustering is protecting both VMs against host unplanned downtime failures.

**Note:** Set anti-affinity rules to keep all VMs in a guest cluster off the same host!
Combining Guest Clustering (WSFC) and VM Migration to Eliminate Planned Downtime of SAP SPOFs

The ability to migrate VMs that are nodes of a guest cluster enables us to stretch the guest cluster across more hosts and eliminate downtime in a planned downtime environment.

The migration of a clustered VM from one hypervisor to another on which a clustered group is running does not cause any downtime of that clustered software. This means that there is no need to perform a failover of the clustered group to move clustered application from one host to another.

In a physical environment, the only way to move the load of a cluster instance from one physical machine to another is to execute a failover. For a clustered DBMS, if there are some open transactions at DBMS level, failover (e.g. restart on another machine) causes rollback of all opened transactions.

With VM migration, we can move the clustered DBMS load from one physical box to another with zero downtime!

The (A)SCS instance also benefits from this feature, through no downtime of message server, and no downtime of sapmnt share. The enqueue server is already protected by the enqueue replication server (ERS) instance.

**Note:** Check database vendor support for running in a virtual environment, running in a guest cluster, and combining a guest cluster with a host cluster.

Combining Guest Clustering (WSFC) and Load Balancing to Better Scale Hypervisor the Load of Guest-Clustered VMs

Load balancing of guest-clustered VMs can be activated to better utilize hypervisor hardware resources.

As mentioned before, Microsoft fully supports this load balancing feature although VMware has some limitations.

**Note:** For the latest support updates on high availability in a virtual environment on Windows, check SAP Note 1374671.
4.2.3 Examples of HA and Business Continuity of SAP Systems in a Virtual Environment – Complete Picture

Two hypervisors are used. A guest cluster (VM1 and VM2) is used to cluster the (A)SCS instance and DBMS. PAS is running on VM3, and AASs are running on VM4. Here we have an analogous setup to a physical cluster (check Figure 5)
Host clustering (VM HA and VM migration) is used to increase availability of application servers. The guest cluster nodes are additionally protected and secured with VM HA for the unplanned downtime, and with VM migration to achieve zero downtime.

**Figure 25**: Combination of Host Cluster and Guest Clustering for SAP Instances - ASs, (A)SCS and DB.
5 Sneak Preview of new Windows Server 2012 OS and Hyper-V

At the time of writing this white paper, Microsoft released new version of Windows Server 2012 OS and new version of Windows Server 2012 OS Hyper-V 3.0.

SAP and Microsoft are working on releasing SAP NetWeaver software on this new platform, which is expected to happen soon in the future. For more information, see SAP Notes: Note 1752767 - Release planning for Windows Server 2012 and Note 1753578 - Windows Server 2012 in Virtual Environments.

New Windows Server 2012 OS and Hyper-V are coming with new features that increase not only scalability but also high availability and business continuity of deployed SAP systems.

From a scalability perspective, the new Windows Server 2012 Hyper-V enables now to virtualize complete enterprise application like SAP.

Here are listed just a few scalability improvements:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM</td>
<td></td>
</tr>
<tr>
<td>Virtual CPU per VM</td>
<td>64</td>
</tr>
<tr>
<td>Memory per VM</td>
<td>1 TB</td>
</tr>
<tr>
<td>IOPS inside of VM</td>
<td>&gt; 1 million</td>
</tr>
<tr>
<td>Hyper-V Host</td>
<td></td>
</tr>
<tr>
<td>Logical Processors</td>
<td>320</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>4 TB</td>
</tr>
<tr>
<td>Virtual CPUs per Host</td>
<td>2048</td>
</tr>
<tr>
<td>Hyper-V Cluster</td>
<td></td>
</tr>
<tr>
<td>Maximum Nodes</td>
<td>64</td>
</tr>
<tr>
<td>Maximum VMs</td>
<td>8000</td>
</tr>
<tr>
<td>Parallel Live Migrations</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

Table 4: Windows Server 2012 Hyper-V and clustering scalability improvements
From high availability and business continuity perspective, a lot of improvements are done as well, here are few of them:

- **Guest Clustering via Fibre Channel**
  Prior to Windows Server 2012, shared storage for guest Windows Server Failover Cluster on Hyper-V could only be accessed through iSCSI. With Windows Server 2012 guest WSFC in addition to iSCSI, you can use access shared storage through Fibre Channel, or Fibre Channel over Ethernet (FCoE) fabrics.

  **Note:** To use virtual SAN adapters in Windows Server 2012 guests, the SAN must support the NPIV feature enabled.

- **Hyper-V Cluster-Aware Updating (CAU)**
  CAU patches all Hyper-V hosts that are part of Hyper-V cluster. It moves all VMs from a node in the cluster, using VM Migration (Live Migration), and then places the nodes in maintenance mode so that workloads are not moved to it during the update. It then downloads and installs updates and reboots the node if required. When the update process is complete, it takes the node out of Maintenance Mode and migrates the workload to the updated node. The process repeats itself until all nodes in the cluster have been updated.

  This process is without any downtime for VMs and SAP applications, as Live Migration is used to move VMs from one hypervisor host to another one.

- **Continuously Available File Server (SMB 3.0) storage for Hyper-V**
  The Server Message Block (SMB) Protocol is the file sharing protocol used by default on Windows computers. Windows Server 2012 provides a vast set of new SMB features, with an updated SMB protocol that greatly enhance reliability, availability, manageability, and performance of file servers. New SMB features are specifically designed for server applications like Hyper-V that store the data on file shares (include VM configuration, VHD files, snapshots).

  Supporting business critical server application workloads like Hyper-V requires the connection to the storage back end to be continuously available. The new SMB server and client cooperate to provide transparent failover with zero downtime to an alternative cluster node for all SMB operations for planned moves and unplanned failures.

- **Enhanced Virtual Machine Mobility**
  Windows Server 2008 R2 introduced VM Migration (live migration), which made it possible to move a running virtual machine from one physical computer to another with no downtime and no service interruption. Prerequisite is that the virtual hard disk for the virtual machine remained consistent on a shared storage device such as a Fibre Channel or iSCSI SAN, attached to Hyper-V cluster. Therefore, migrating of VMs was possible only between hypervisor hosts that are part of one Hyper-V cluster.
In Windows Server 2012, live migrations are no longer limited to a cluster, and virtual machines can be migrated across cluster and network boundaries.

The following scenarios for this are:

- **SMB-based live migration**: In this instance, each virtual machine’s hard disk is stored on a central SMB file share. You then perform a live migration of the virtual machines from one server to another while their storage remains on the central SMB share.

- **“Shared-nothing” live migration**: you can move VMs between standalone Hyper-V hosts, including moving the VM’s virtual hard disks (VHDs), memory content, processor, and device state with no downtime to the VM and application running inside. The only prerequisite is two standalone Server 2012 Hyper-V hosts with a Gigabit Ethernet connection between them. There is no need for shared storage nor Hyper-V host cluster.

- **Storage live migration**: Through this feature, you can transfer virtual hard disks, with no downtime, to a new location for upgrading or migrating storage, performing backend storage maintenance, or redistributing your storage load.

- **Hyper-V Replica**: Hyper-V Replica provides asynchronous replication of virtual machines for the purposes of business continuity and disaster recovery. In the event of failure (such as a power failure, fire, or natural disaster) at the primary site, an administrator can manually fail over the production virtual machines to the Hyper-V server at the recovery site. During failover, the virtual machines are brought back to a consistent point in time.

- **Network Virtualization**: Network Virtualization is a new technology to virtualize and abstract network used by VMs from underlining physical hypervisor network. The concept is similar to server virtualization of physical compute resource like RAM and CPU – server virtualization enables us to run multiple virtual servers (VMs) on a physical server and Hyper-V network virtualization enables us to run multiple virtual networks on a physical network. Hyper-V Network Virtualization decouples the VMs virtual networks from the physical network infrastructure of the hosters, providing freedom for workload placements inside the datacenters.

  Currently, VLANs are the mechanism that most organizations use to support address space reuse and tenant isolation. One disadvantage with VLANs are constraints within a single IP subnet, which limits the number of nodes within a single VLAN and restricts the placement of virtual machines based on physical locations. Even though VLANs can be expanded across sites, the entire VLAN must be on the same subnet. Another limitation is limited in scalability because typical switches support no more than 1000 VLAN IDs out of a maximum of 4094.
Live migration of virtual machine workloads traditionally has been limited to the same IP subnet or VLAN because crossing subnets required the virtual machine’s guest operating system to change its IP address.

Virtual machine workload placement is no longer limited by the IP address assignment or VLAN isolation requirements of the physical network because it is enforced within Hyper-V hosts based on software-defined, multitenant virtualization policies.

This enables us not only scalable multi-tenant network isolation, but also live migration across physical subnets.
Virtualization provides the following advantages in the area of high availability compared to running in a physical environment:

- Virtualization HA technologies such as VM HA and VM migration can be used to protect an SAP system. Although these technologies do not offer application but rather infrastructure high availability, with high availability of infrastructure we can indirectly also achieve “higher availability” of SAP systems.

- Through virtualization of an SAP application server using:
  - VM HA – we can reduce unplanned downtime of hardware, hypervisor or guest OS
  - VM migration – we can eliminate planned downtime of hardware and hypervisor for SAP AS

In the physical environment we do not have this opportunity.

It is important to notice that when increasing the availability of just one SAP component – in this case of the application servers – increases the availability of the whole SAP system.

- Using guest clustering in a virtual environment achieves application HA. Here we have the same situation as in a physical environment. Virtualization gives us the ability to consolidate hardware, which is especially useful for SAP instances such as the (A)SCS, which has low CPU and RAM consumption.

- Windows Server Failover Clustering used for ASCS/SCS instance in combination with integrated enqueue replication is offering highest HA features, and for enqueue work process and enqueue replication table basically a fault tolerance protection, in unplanned downtime scenarios (like crash of enqueue work process, crash of OS) as well as in planned downtime scenarios (patching of Windows OS, patching of SAP kernel of ASCS/SCS).

- Using guest clustering in combination with VM HA (host clustering), we can stretch two-node guest clusters across more hypervisor hosts, and get more availability compared to a physical unplanned downtime environment.

- Using guest clustering in combination with VM Migration, we can stretch two-node guest clusters across more hypervisor hosts in a planned downtime environment. Migration of guest-clustered VM nodes where SPOFs are running does not cause any downtime of clustered SPOFs. This is not possible in a physical environment.
The DBMS benefits with from this feature (as we can move clustered DBMS form one host to another with zero Downtime), and a few components of the (A)SCS instance, such as message server and SAPMNT share this. E.g. there is no need to perform failover which cause a short downtime.

- Dynamic load balancing of the hypervisor host can be used to better use hardware resource. This is not possible in a physical environment.

- The downside of combining guest clustering with VM HA and VM migration is higher complexity.
7 Related Content

SAP Community Network (SCN):
Virtualization and Cloud Infrastructure
Business ContinuitySAP on Microsoft Windows
Virtualization on Windows
SAP Applications on Windows Server 2008 R2 - High Availability Reference Guide
SAP on VMware
VMware documents regarding SAP products
Best Practices for SAP on Hyper-V
Support for SAP Components in Virtual and Cloud EnvironmentsNew Installation Options for a High-Availability SAP System Based on SAP NetWeaver 7.1 Including EHP1 (7.11) in a Microsoft Cluster

SAP Notes:
(SMP login required)
SAP Notes Related to Virtualization on Windows
SAP Note 1634991 - How to install an ASCS or SCS instance on more than 2 cluster nodes?
SAP Note 953653 - Rolling kernel switch

Microsoft:
Microsoft TechNet Blog: Hyper-V Guest Clustering Step-by-Step Guide
Microsoft TechNet: Hyper-V
MSDN: VM-VM Affinity Rules on Hyper-V
Automated Windows Patching in a Microsoft Private Cloud for SAP
Server Virtualization - Windows Server 2012
Windows Server 2012 Cluster-Aware Updating Overview
Storage Windows Server 2012
Hyper-V Network Virtualization Overview

VMware:
VMware Knowledge Base: Microsoft Cluster Service (MSCS) support on ESX/ESXi
VMware Knowledge Base : Microsoft Clustering on VMware vSphere: Guidelines for Supported Configurations
Setup for Failover Clustering and Microsoft Cluster Service and vSphere 5.0
VM-VM Affinity Rules on VMware
MSDN Blog: Guest Failover Clustering with VMware
VMware® Fault Tolerance Recommendations and Considerations on VMware vSphere™ 4
vSphere Availability - ESXi 5.0, vCenter Server 5.0
vSphere Availability Guide - ESX 4.1, ESXi 4.1, vCenter Server 4.1
8 Copyright

© Copyright 2013 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Oracle Corporation.

JavaScript is a registered trademark of Oracle Corporation, used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.