Bosch Video Management System

High Availability with Hyper-V

BOSCH

en Configuration Manual

Table of contents

1	**Introduction**	**4**
1.1	General Requirements	4
2	**Hyper-V architectures**	**5**
2.1	Low effort: Replication	5
2.2	Medium effort: Cluster	6
3	**Preparing the operating system for replication and cluster**	**7**
4	**Configuring DSA E-Series 2600**	**15**
4.1	Installing SANtricity on client computer	15
4.2	Assigning static IP addresses (part 1)	15
4.3	Installing the firmware on a DSA E-Series	15
4.4	Assigning static IP addresses (part 2)	17
4.5	Configuring storage for Hyper-V or VMware	18
4.6	Configuring iSCSI targets on Windows host	19
5	**Performance tips**	**26**
6	**Example System Dimensions**	**27**
6.1	Sizing	27
6.2	Network segments	27
6.3	Server configuration	27
6.3.1	Replication	27
6.3.2	Cluster	27
6.3.3	Cluster using Starwind solution	28
	Glossary	**30**

1 Introduction

The need for high-availability systems

Software systems that provide security for lives and property need themselves to be secure from threats such as hardware failure, software failure, sabotage and natural disasters. Hence it is desirable for security management systems to be installed on some form of high-availability (HA) platform. The choice of platform depends on a number of limiting factors, including:

- Cost of downtime of the system
- Maximum tolerable downtime of the system
- Cost of the high-availability platform (usually per server)

Scope of this document

This document describes installations that Bosch has tested in-house. It does not describe the implementation of Hyper-V systems in general, but rather helps those planning and commissioning Bosch Security Management systems on high-availability systems to avoid common misconceptions and mistakes.

As IT infrastructures differ widely, Bosch strongly recommends that those with little experience in the area of HA obtain the assistance of consultants with suitable Microsoft qualifications.

Required hardware

See the datasheet of Bosch VMS or BIS for hardware requirements.

Notice!

Prerequisite for Microsoft support

Microsoft supports a failover cluster or replica solution only if all the hardware features are marked as "Certified for Windows Server 2012 R2." In addition, the complete configuration (servers, network, and storage) must pass all tests in the **Validate a Configuration** Wizard, which is included in the Failover Cluster Manager snap-in.

Documentation and software for Bosch Security Systems products can be found in the online product catalogue as follows:

- Open any browser > enter www.boschsecurity.com > select your region and your country > start a search for your product > select the product in the search results to show the existing files.

1.1 General Requirements

Goals of the high availability platform:

- Near zero downtime of the security management system, e.g. BIS, Bosch VMS
- Availability as a pre-configured bundle
- Familiarity to customers and IT departments
- Cost-effectiveness
- Ease of deployment
- Upward scalability
- Ease of support

2 Hyper-V architectures

You can achieve two different architectures for high availability using Hyper-V from Microsoft:

– Replication
– Cluster

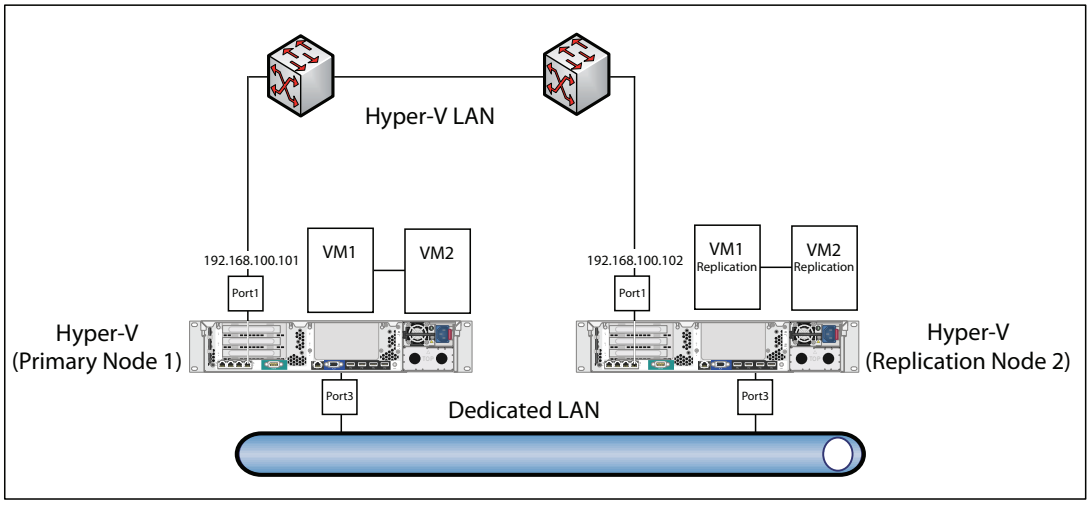
2.1 Low effort: Replication

Advantages:

– Short downtime, low budget, low effort, widespread standard solution

Overview

The easiest way to ensure high availability of an application using virtual machines (VMs) is to set up asynchronous replication between two Hyper-V hosts. In this scenario you replicate a virtual machine from your primary site to another site using snapshot technology. A short replication interval is around 30 seconds, and you can use Kerberos authentication or (self-signed) certificates. Information arising during the replication interval is lost. To set up VM replication you need only Windows Server 2012 R2 with Hyper-V. No domain or cluster services are necessary.



2.2 Medium effort: Cluster

Advantages:

– Near zero downtime, cost-effectiveness, small central storage, easy to implement with tested standard components

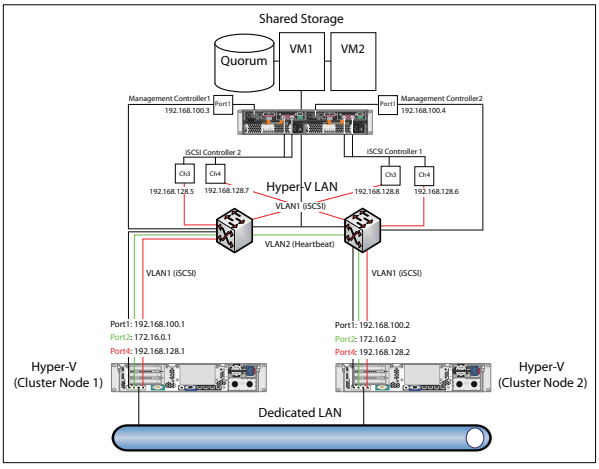
Overview

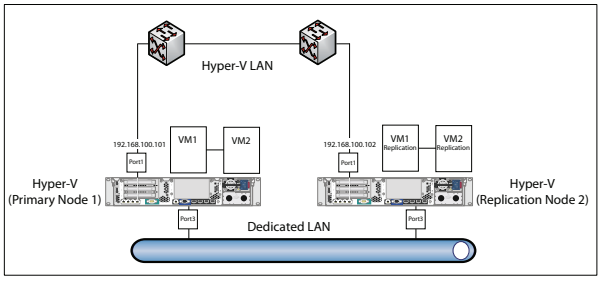
A more secure way to ensure business continuity of a virtual machine is to create a Hyper-V cluster. In this scenario a Domain Controller, at least two Hyper-V nodes and a shared storage are required. The VMs are located on the shared storage to which all Hyper-V cluster nodes have access.

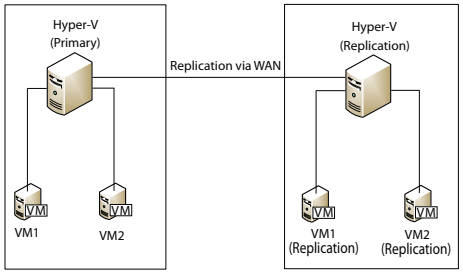
To ensure high availability of an application, all cluster nodes listen to each other's "heartbeat" signal. If a cluster node's heartbeat is missing then that node is assumed to have crashed, and another cluster node will pick up the failed node's VMs with minimal downtime and information loss.

The information loss consists of the data residing in the RAM of the affected cluster node, and some events that occur during the downtime of the cluster node.

The shared storage is a single point of failure. If it fails, the VMs can no longer run. To avoid such a single point of failure, the DSA E-Series storage device provides additional redundancy. We recommend purchasing a shared storage with dual controller.







VM1 can for example host the Bosch VMS server, VM2 can host a Primary Domain Controller (PDC).

Instead of using a dedicated server for the shared storage, you can also use the Starwind solution to create a virtual shared storage on the 2 cluster nodes.

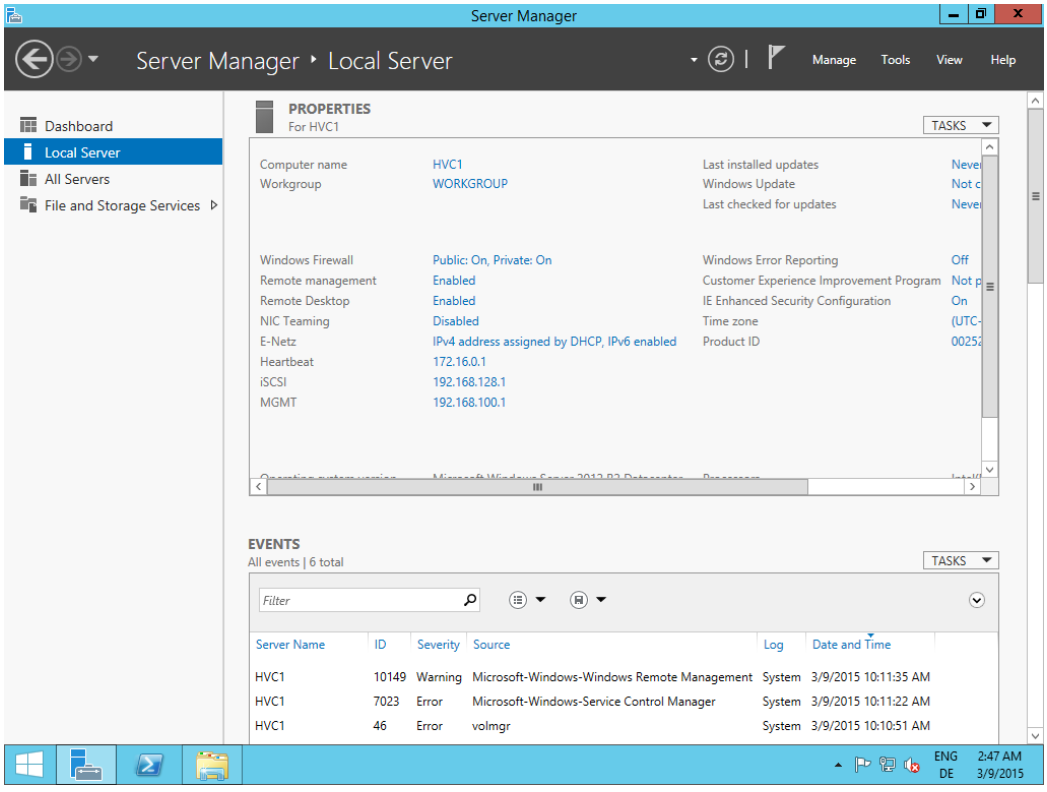
See the *Cluster using Starwind solution, page 28* chapter for details.

3 Preparing the operating system for replication and cluster

Configuring network cards

Perform this procedure on both hosts.

1. Start **Server Manager > Local Server**.
2. Click the computer name to rename the server.
3. Click **Disabled** right by **Remote Desktop** to enable Remote Desktop.
4. Click **IPv4 address assigned by DHCP** to configure the ports of the network card.



Network card port #1: Management (mandatory)

Network card port #2: Heartbeat (mandatory for cluster architecture)

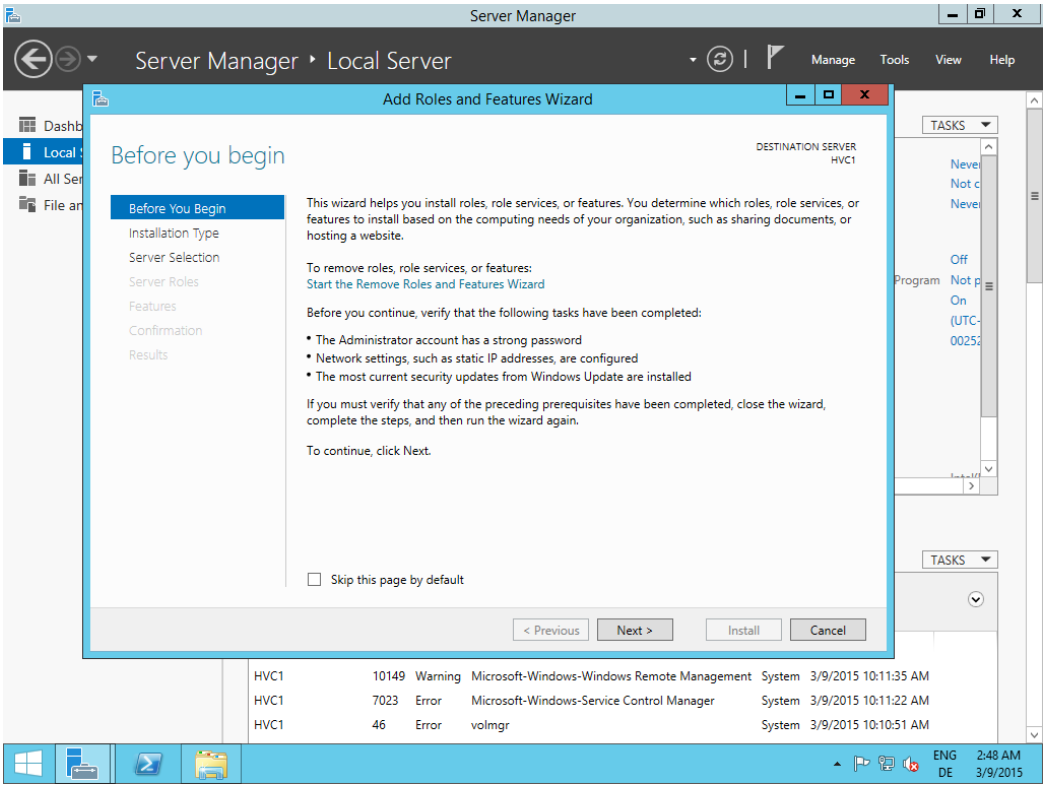
Network card port #3: Business network (optional)

Network card port #4: iSCSI (mandatory for cluster architecture)

5. Restart the computer.

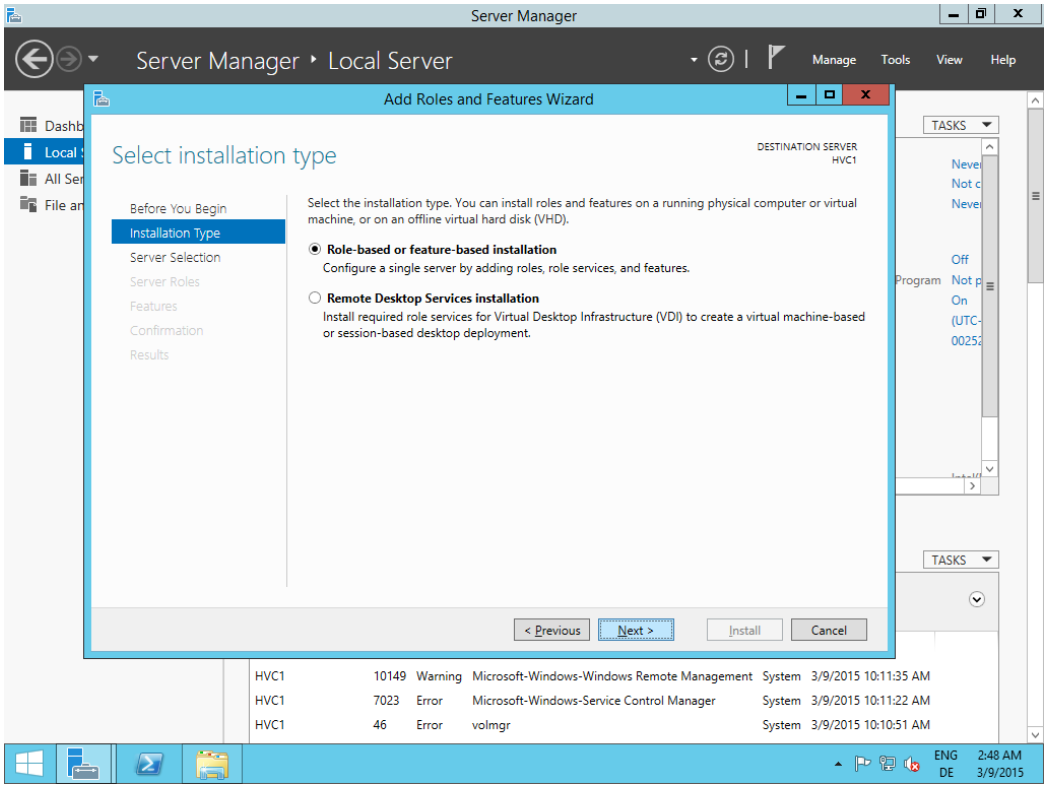
Adding roles and features

1. Start **Server Manager** and click **Manage** > **Add Roles and Features**.
   The **Before You Begin** page of the **Add Roles and Features Wizard** dialog box is displayed.

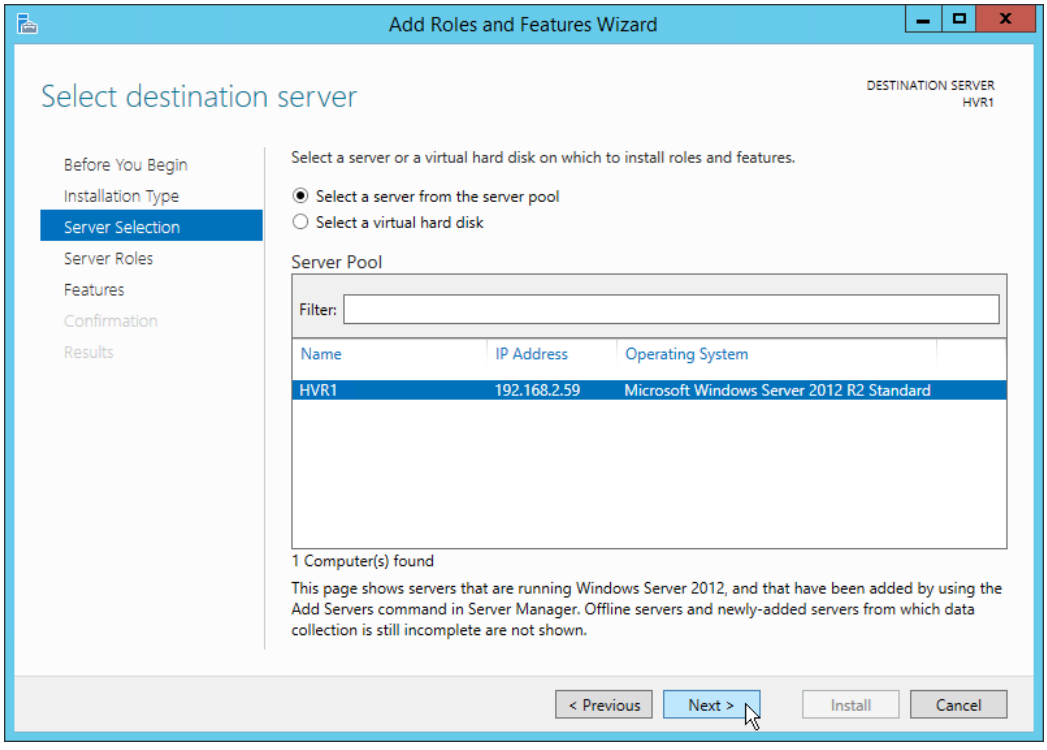


2. Click **Next**.
   The **Select installation type** page is displayed.

3. Click **Role-based or feature-based installation**.

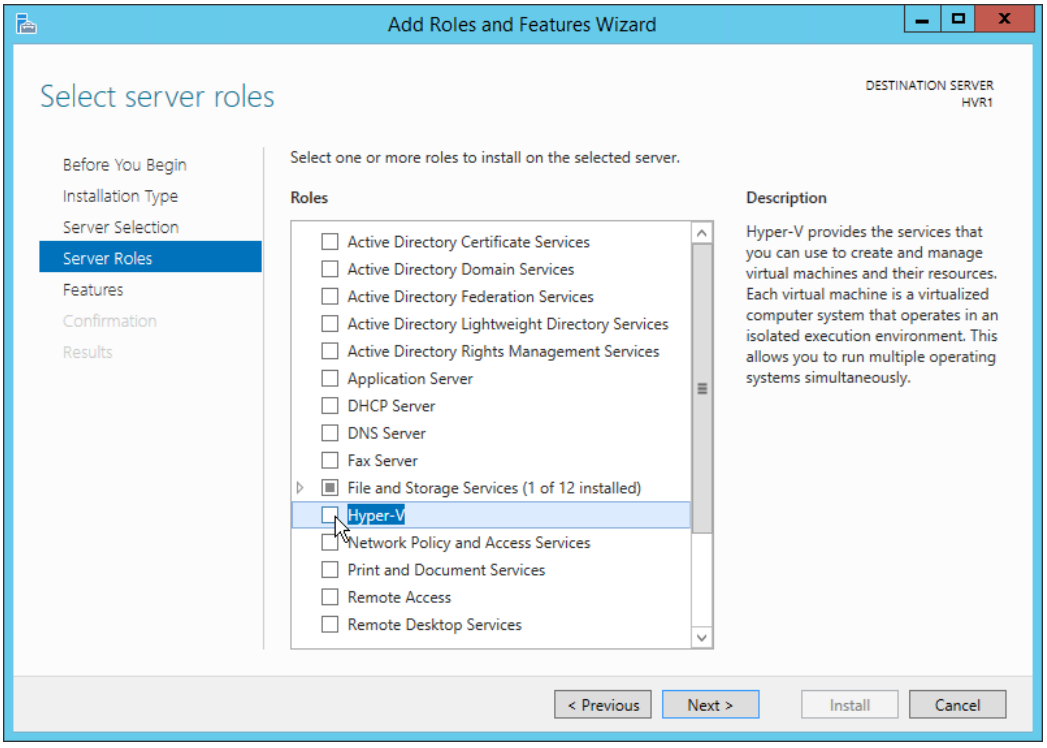


4. Click **Next**.
   The **Select destination server** page is displayed.
5. Click **Select a server from the server pool**.
   Your server is displayed in the **Server Pool** list.

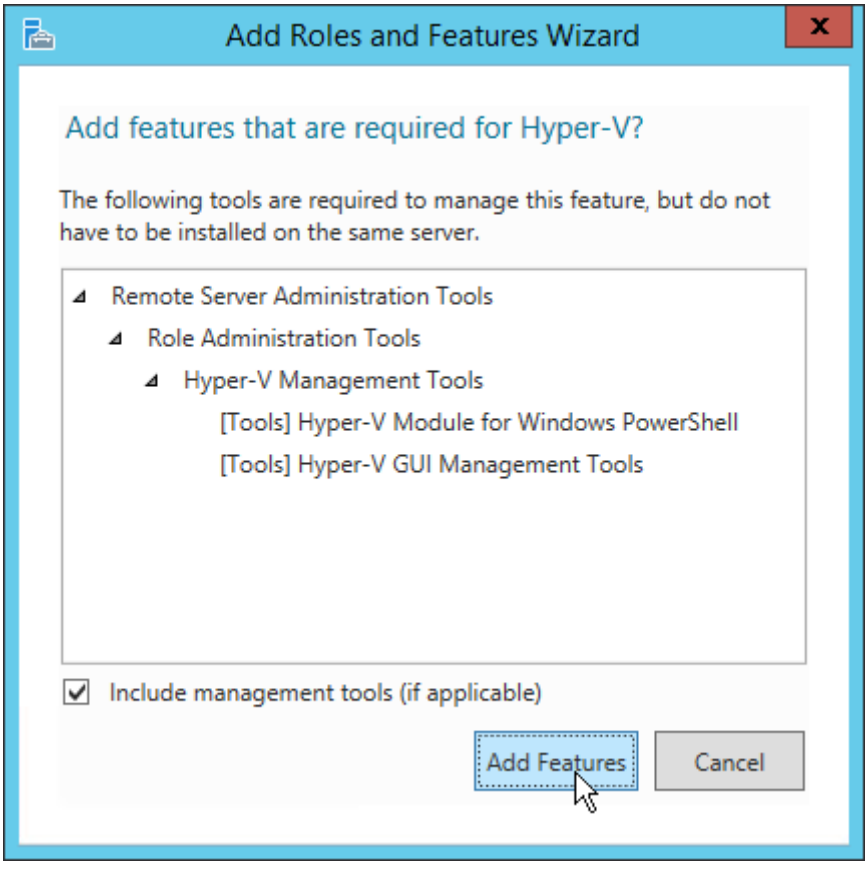


6. Select your server and click **Next**.
   The **Select server roles** page is displayed.

7. Click to enable **Hyper-V**.

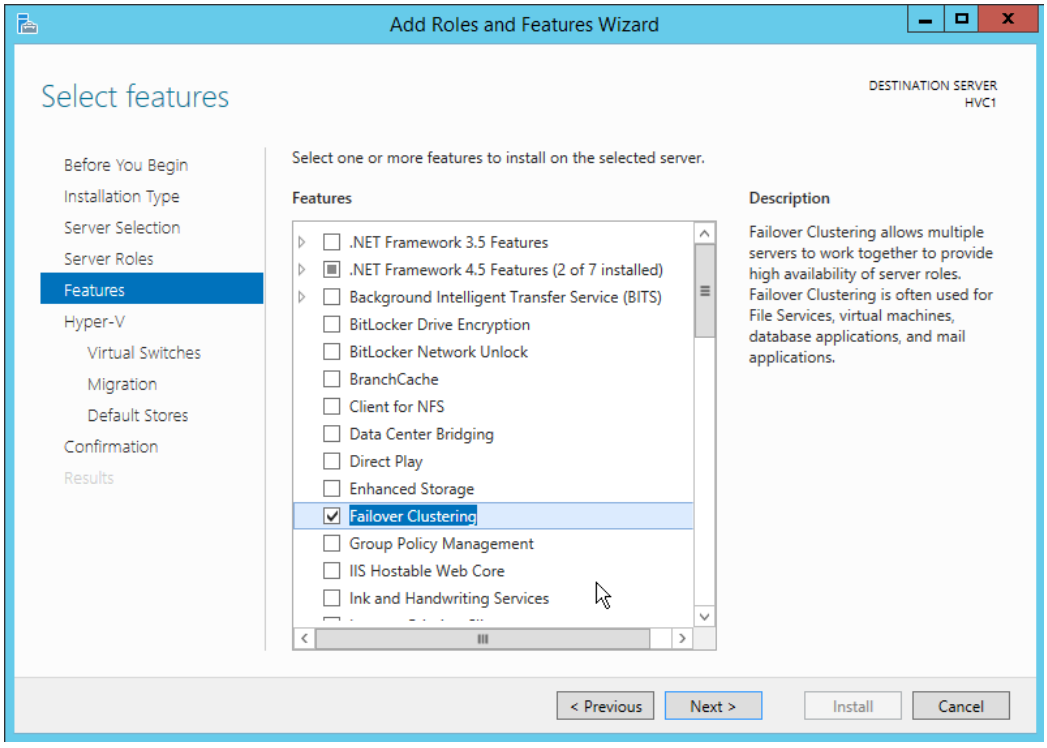


8. Click **Next**.
The **Add features that are required for Hyper-V** page is displayed.

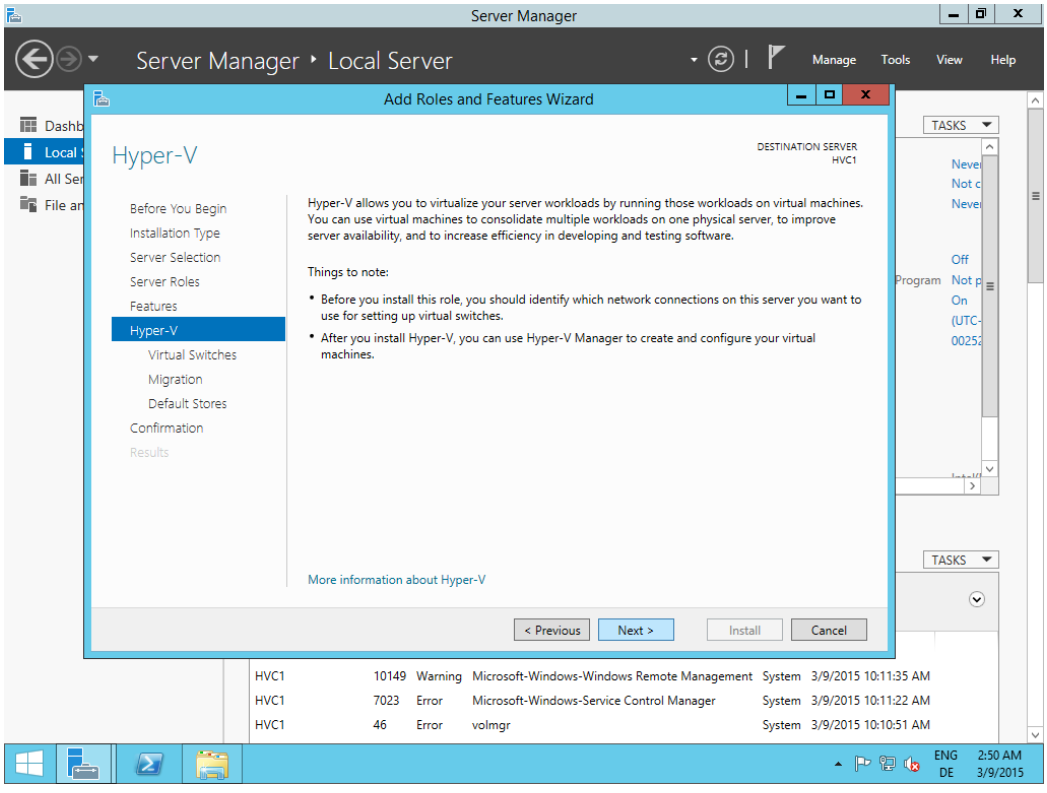


9. Click **Add Features**.
The **Select features** page is displayed.

10. Only on Hyper-V Cluster installations: Click to enable **Failover Clustering**.

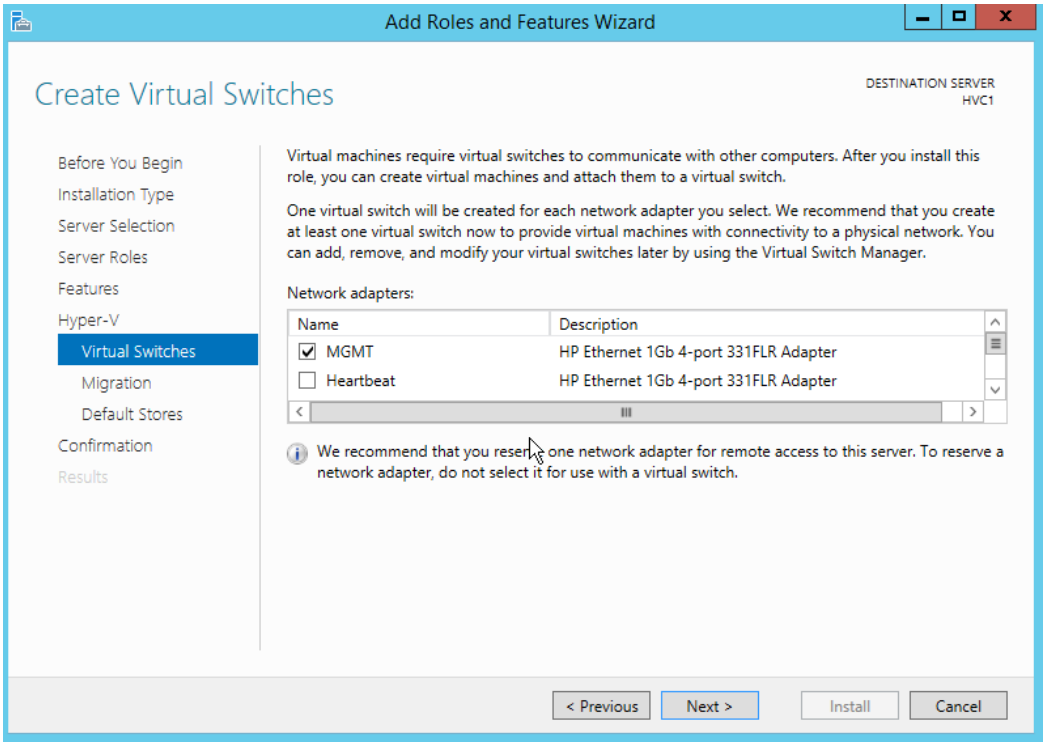


11. Click **Next**.
The **Hyper-V** page is displayed.

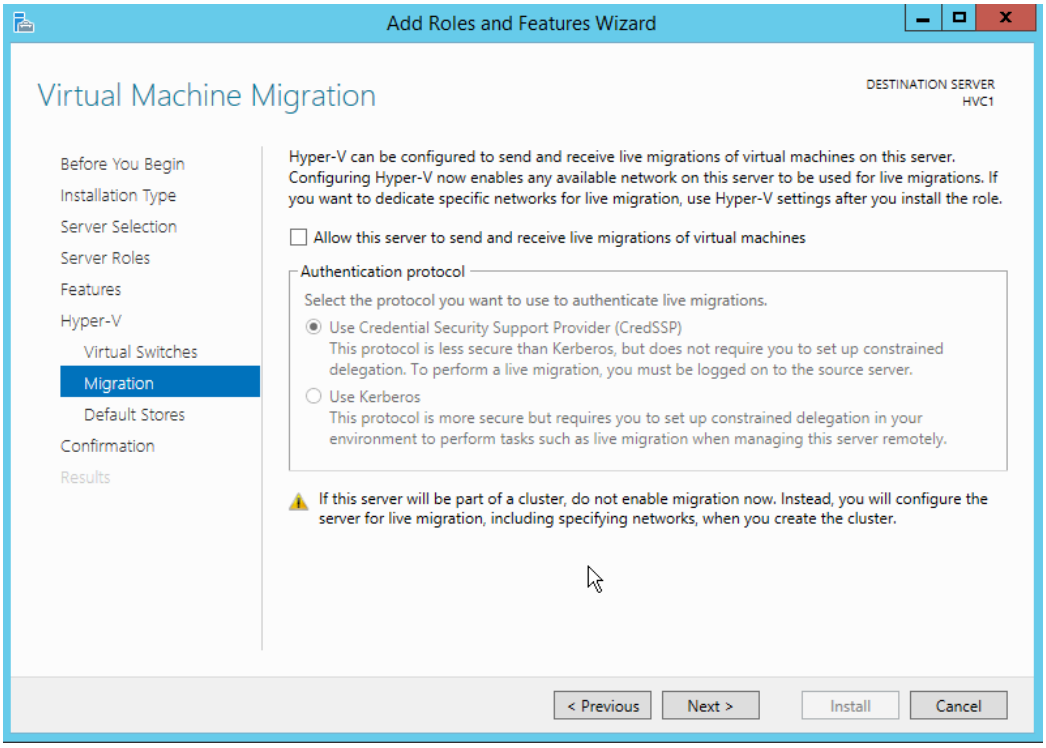


12. Click **Next**.
The **Create Virtual Switches** page is displayed.

13. Click to enable **MGMT**.

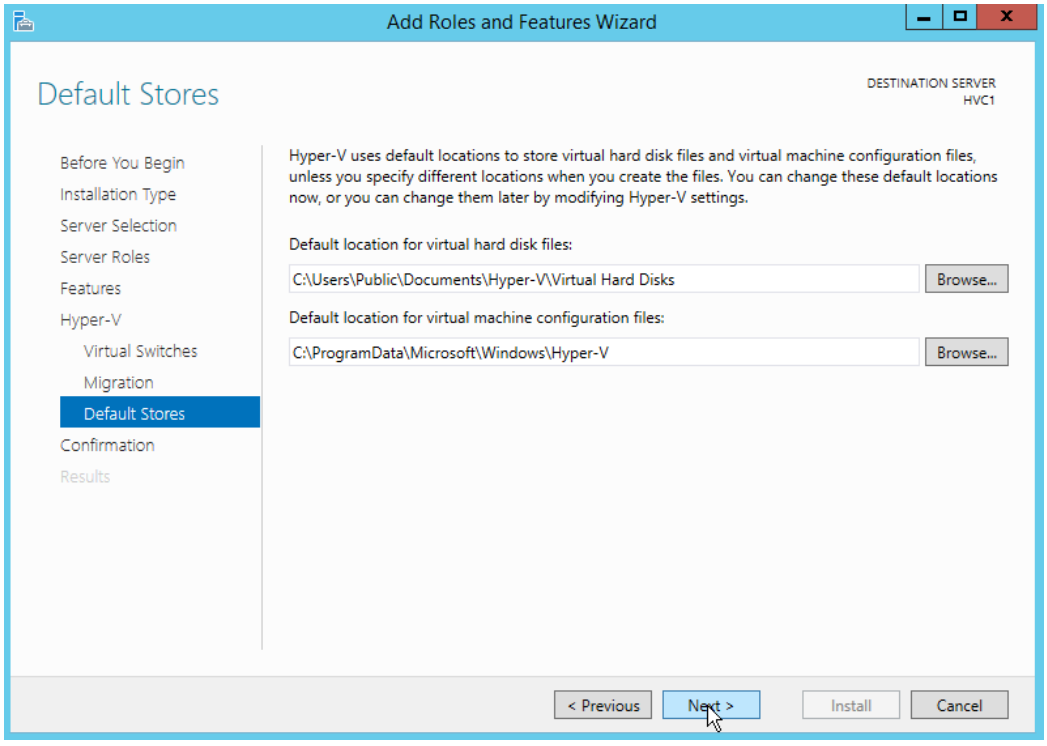


14. Click **Next**.
The **Virtual Machine Migration** page is displayed.

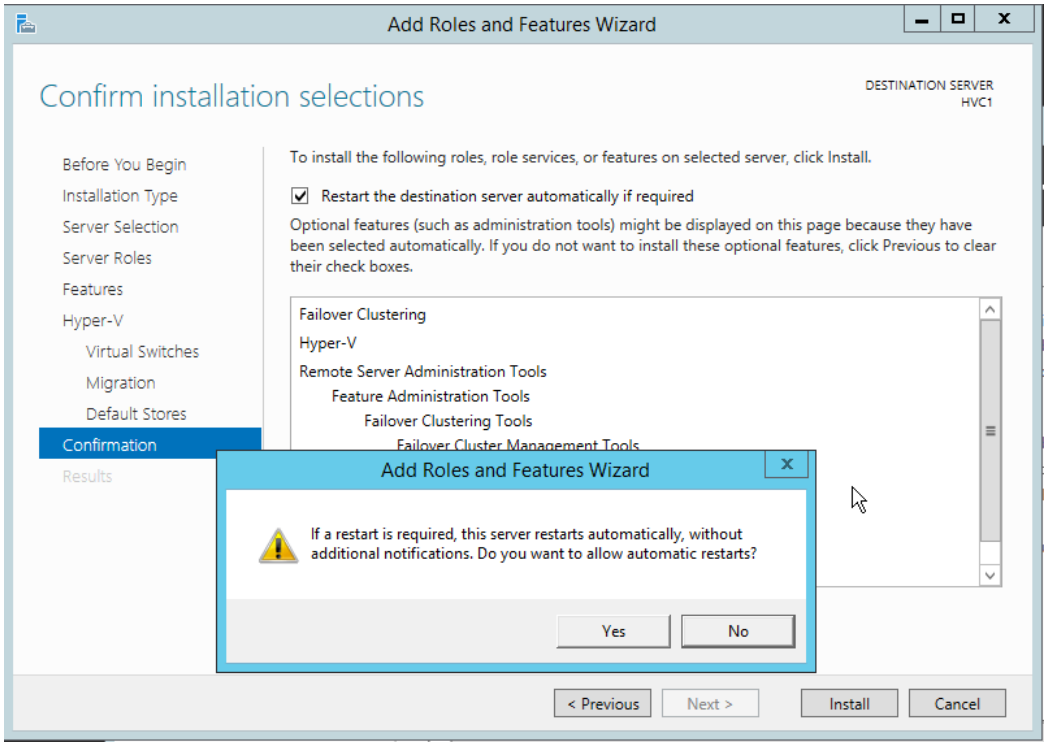


15. Click **Next**.
The **Default Stores** page is displayed.

16. Change the default locations.



17. Click **Next**.
    The **Confirm installation selections** page is displayed.
18. Click to enable **Restart the destination server automatically if required**.



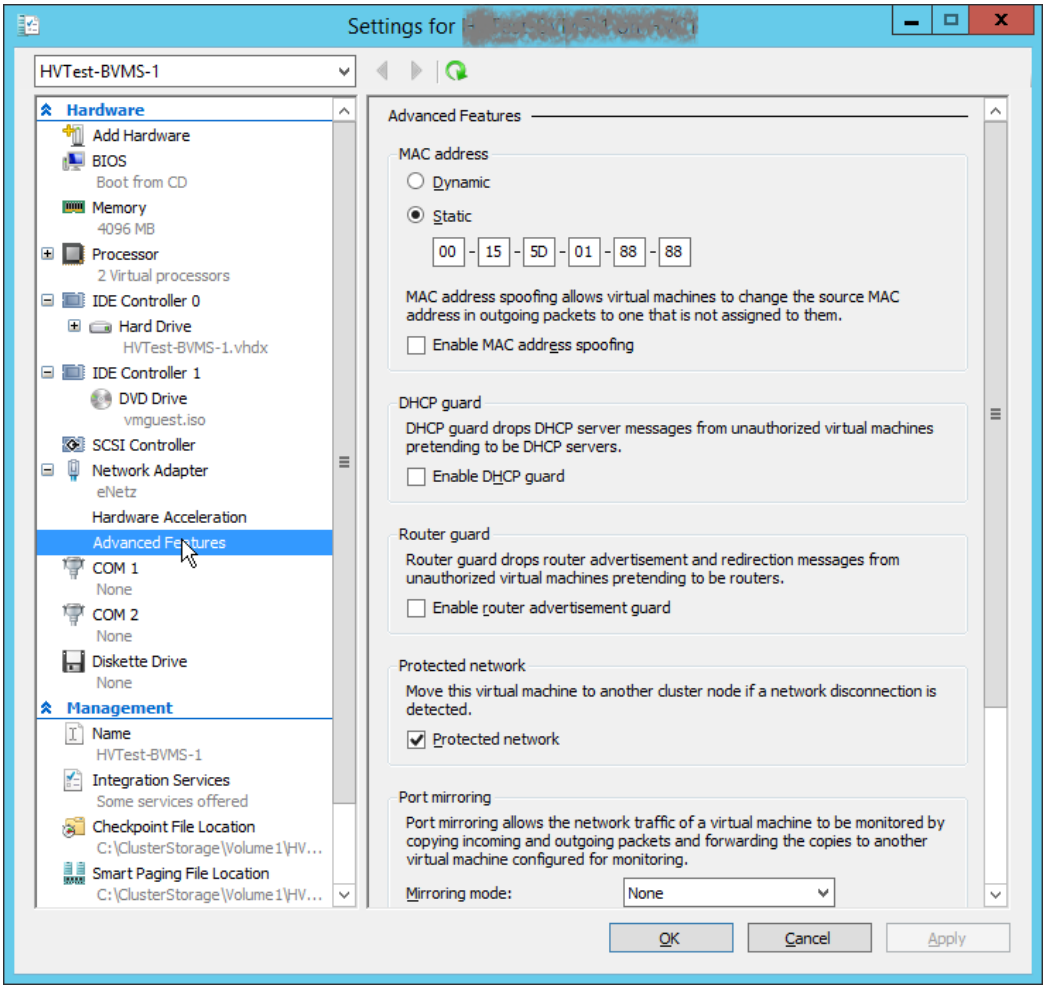
19. Click **Yes**.
20. Click **Install**.
    The server is restarted.

Fixing MAC addresses

To avoid that the MAC address of the network adapter of the Bosch VMS virtual machine is automatically changed, perform this procedure.

You need the MAC address of the affected network adapter.

1. Start **Hyper-V Manager**.
2. Right-click a virtual machine entry and click **Settings...**
   The Settings dialog box is displayed.
3. In the Hardware list, click **Advanced Features**.



4. In the MAC address field, click **Static**.
5. Type in the valid MAC address.
6. Click **OK**.

4 Configuring DSA E-Series 2600

For installing the firmware and assigning static IP addresses, install SANtricity ES Storage Manager software.
You need the default NetAppp firmware to install it on your DSA E-Series device. This firmware is available on the Bosch VMS product catalog page.
Contact Bosch Technical Support for these software packages.

Notice!
For more detailed and up-to-date information refer to the SANtricity installation manual available on http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=61197.

See also
- *Installing SANtricity on client computer, page 15*
- *Assigning static IP addresses (part 1), page 15*
- *Installing the firmware on a DSA E-Series, page 15*
- *Assigning static IP addresses (part 2), page 17*
- *Configuring storage for Hyper-V or VMware, page 18*

4.1 Installing SANtricity on client computer

- Start `Setup.exe` and follow the instructions on the screen.

4.2 Assigning static IP addresses (part 1)

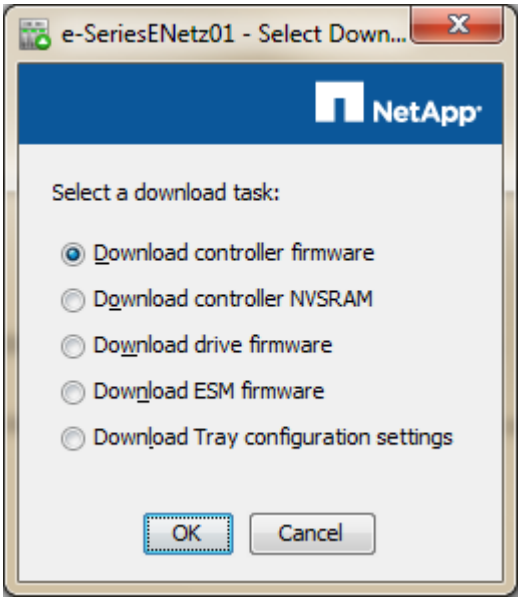
Refer to the SANtricity manual for performing the following tasks.
Switch on the DSA E-Series device. The device waits several minutes for a DHCP server assigning IP addresses. If no DHCP server is available or the DHCP does not assign IP addresses, default IP addresses are automatically assigned for both the iSCSI Controller and the Management Controller. SANtricity can only detect devices in the same subnet. If DHCP server is available, this is not a problem. Otherwise you must configure an alternative IP address for your network adapter so that you can reach iSCSI storage devices in other subnets.
Assign the static IP addresses for the iSCSI controller after you installed the NetApp firmware on your DSA E-Series device.

Assign IP addresses:
1. After this automatic assignment, start SANtricity to configure static IP addresses.
2. For the Management Controller configure port 1.
   For better network redundancy, you can also configure port 2.
3. Exit SANtricity and restart it.
4. Remove the old array entry and rescan.

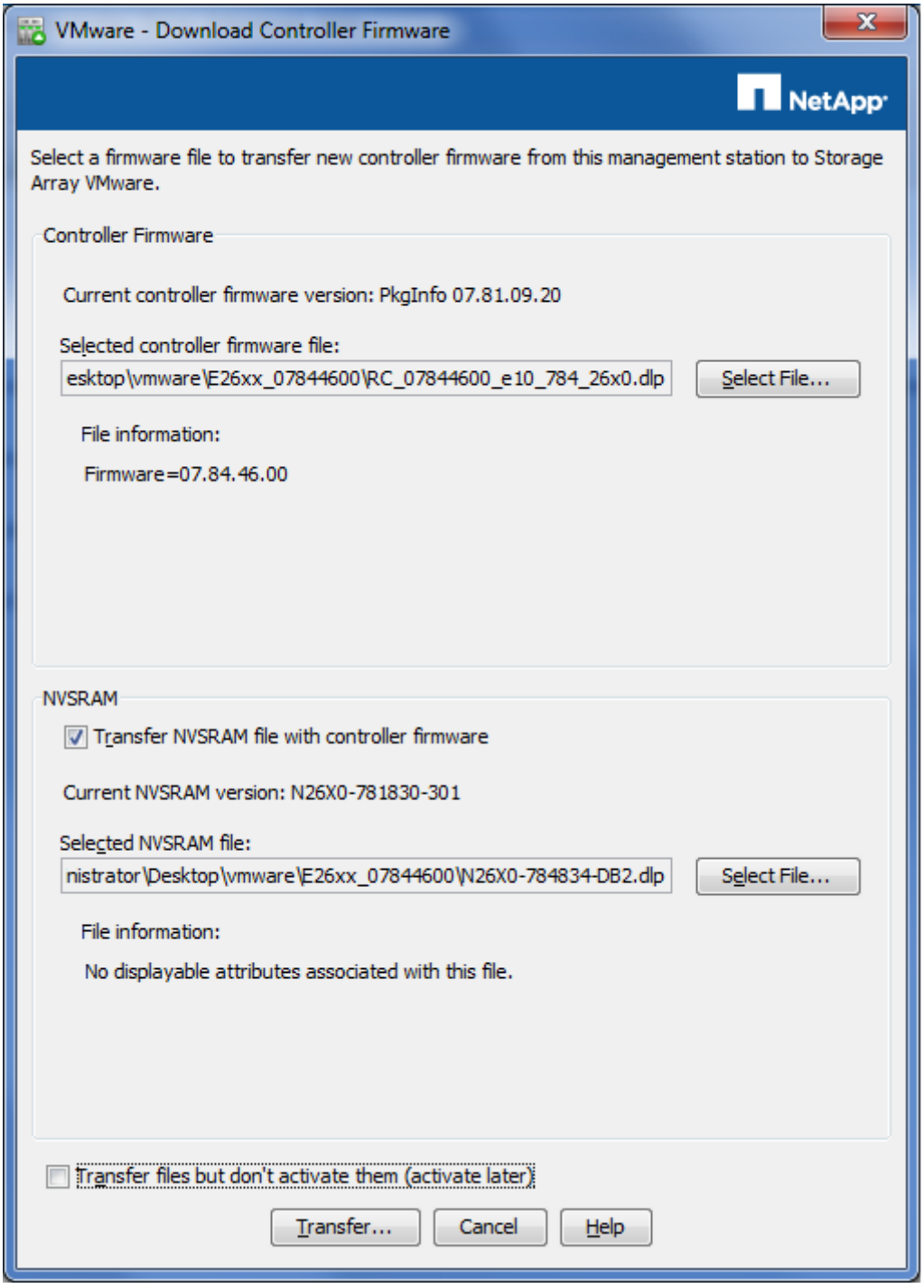
4.3 Installing the firmware on a DSA E-Series

To install:
1. Start **SANtricity ES Storage Manager**.
2. Click the **Support** tab.
3. Click **View Event Log**.
   The Event Log dialog box is displayed.
4. Click **Clear All...**.

5. In the next dialog box, type in `yes` and click **OK**.
   Old event logs are removed. This is a prerequisite for installing the firmware.
6. Click **Download Firmware**.
   The following dialog box is displayed.



7. Select **Download controller firmware** and click **OK**.
   The following dialog box is displayed.



8. Select check box **Transfer NVSRAM file with controller firmware**.
9. In both selection fields, enter the appropriate path and filenames.
10. Click **Transfer...**
    The firmware is transferred and installed on your device.
    This process can last 10 minutes or longer.

4.4 Assigning static IP addresses (part 2)

Refer to the SANtricity manual for performing the following task.
Assign static IP addresses for the iSCSI controllers.

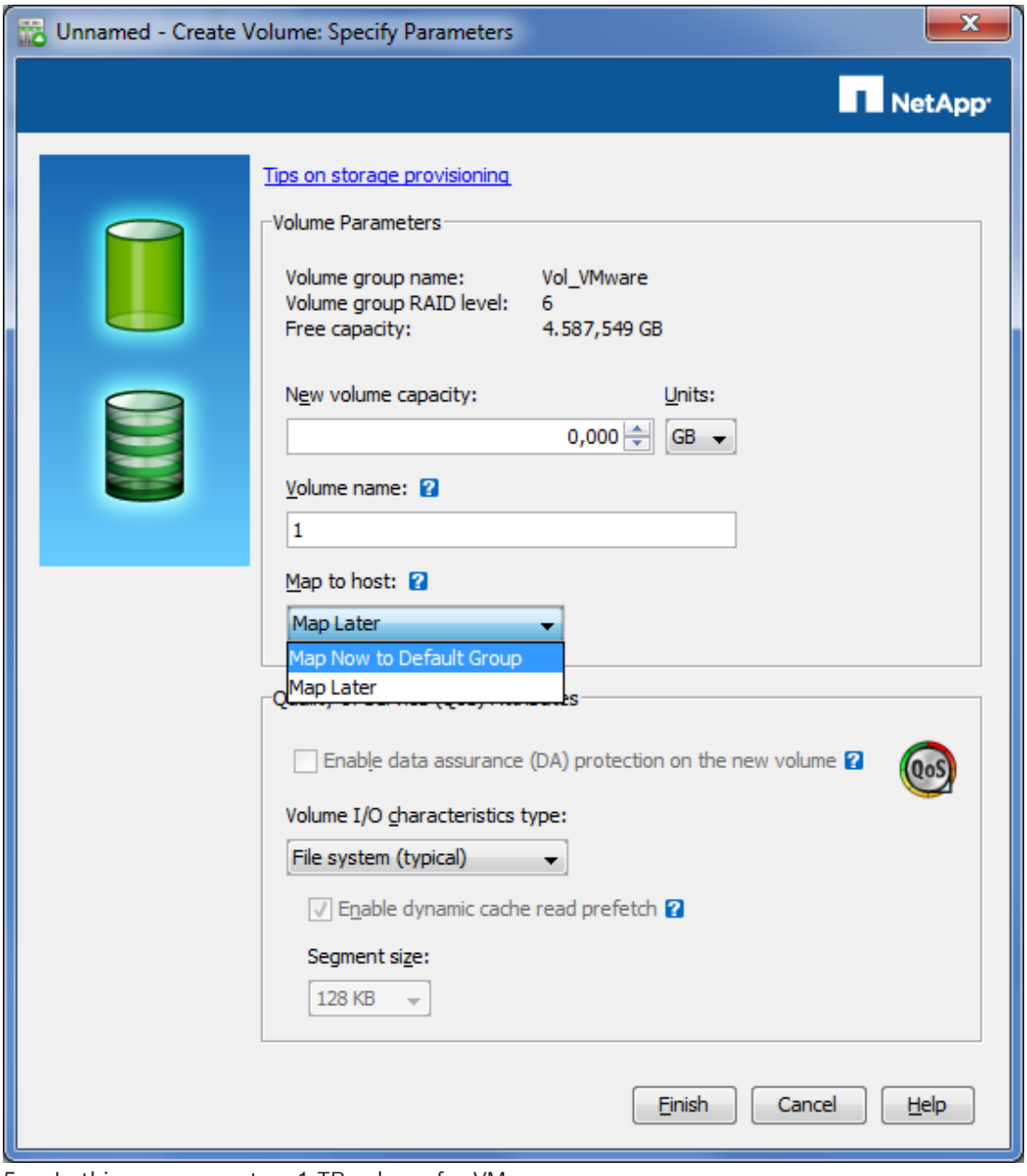
Assign IP addresses:

- For each iSCSI controller configure 2 iSCSI ports with static IP addresses. Configure the correct port speed used in your network.

4.5 Configuring storage for Hyper-V or VMware

Create volume group with volume:

1. Click the **Storage & Copy Services** tab.
2. Create a volume group.
3. For this group configure **Automatic** and **RAID 6**.
4. In the **Map to host:** list, select **Map Now to Default Group**.



5. In this group, create a 1 TB volume for VMware.
   For Hyper-V, create 3 volumes:
   1x 100GB Quorum
   2x 1TB as Cluster Shared Volumes

For VMware: Change the default host operating system type:

1. Click the **Host Mappings** tab.
2. Right-click **Default Group** and click **Change Default Host Operating System**.
3. As the new host type configure **VMWare**.

For Hyper-V: Change the default host operating system type:

1. Click the **Host Mappings** tab.
2. Right-click **Default Group** and click **Change Default Host Operating System**.
3. As the new host type configure **Windows Server 2003/Server 2008 Clustered (Supports DMP)** for a dual controller device.
   For a single controller device select the **Windows Server 2003/Server 2008 Non-Clustered (Supports DMP)** option.

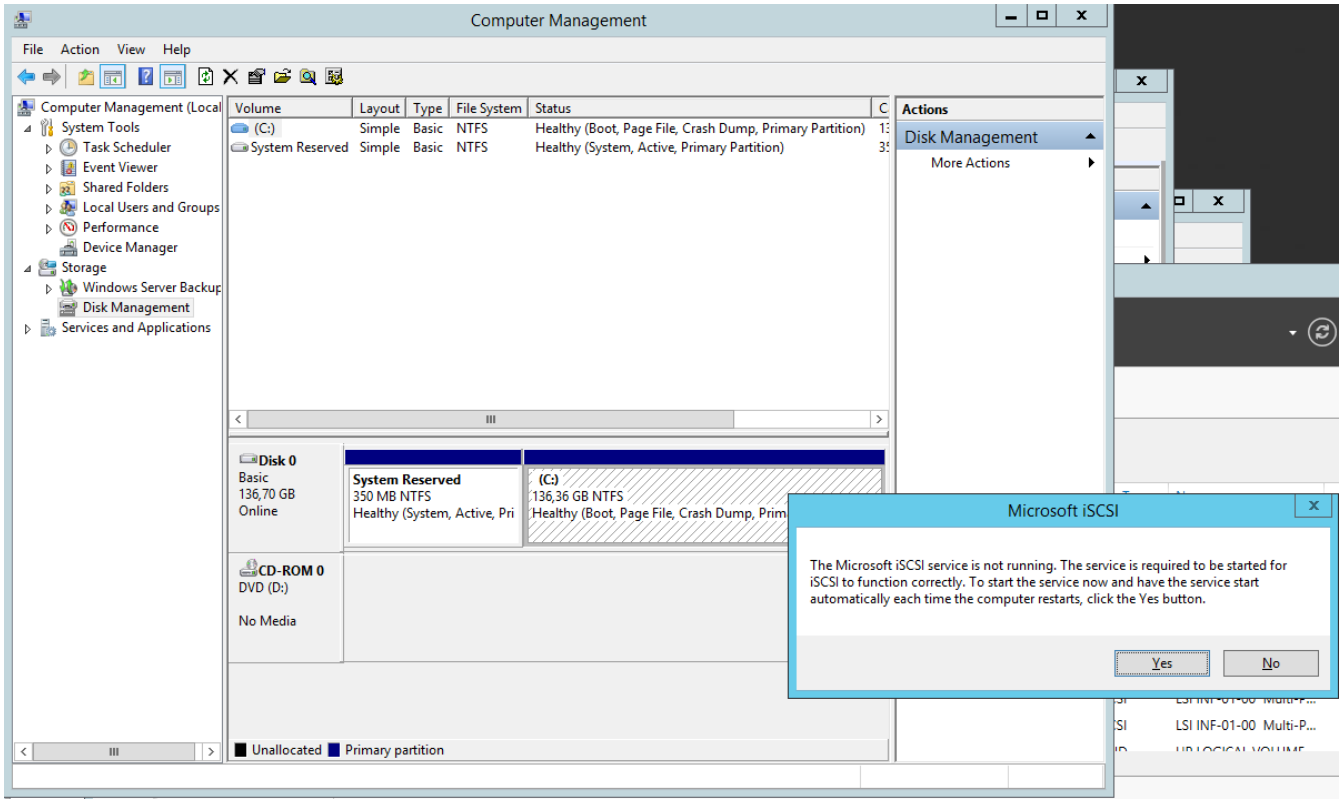
4.6 Configuring iSCSI targets on Windows host

For preparing the storage you must perform the following tasks:

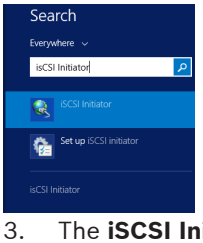
– Adding the iSCSI target
– Initializing the disks of the iSCSI target

Adding the iSCSI target

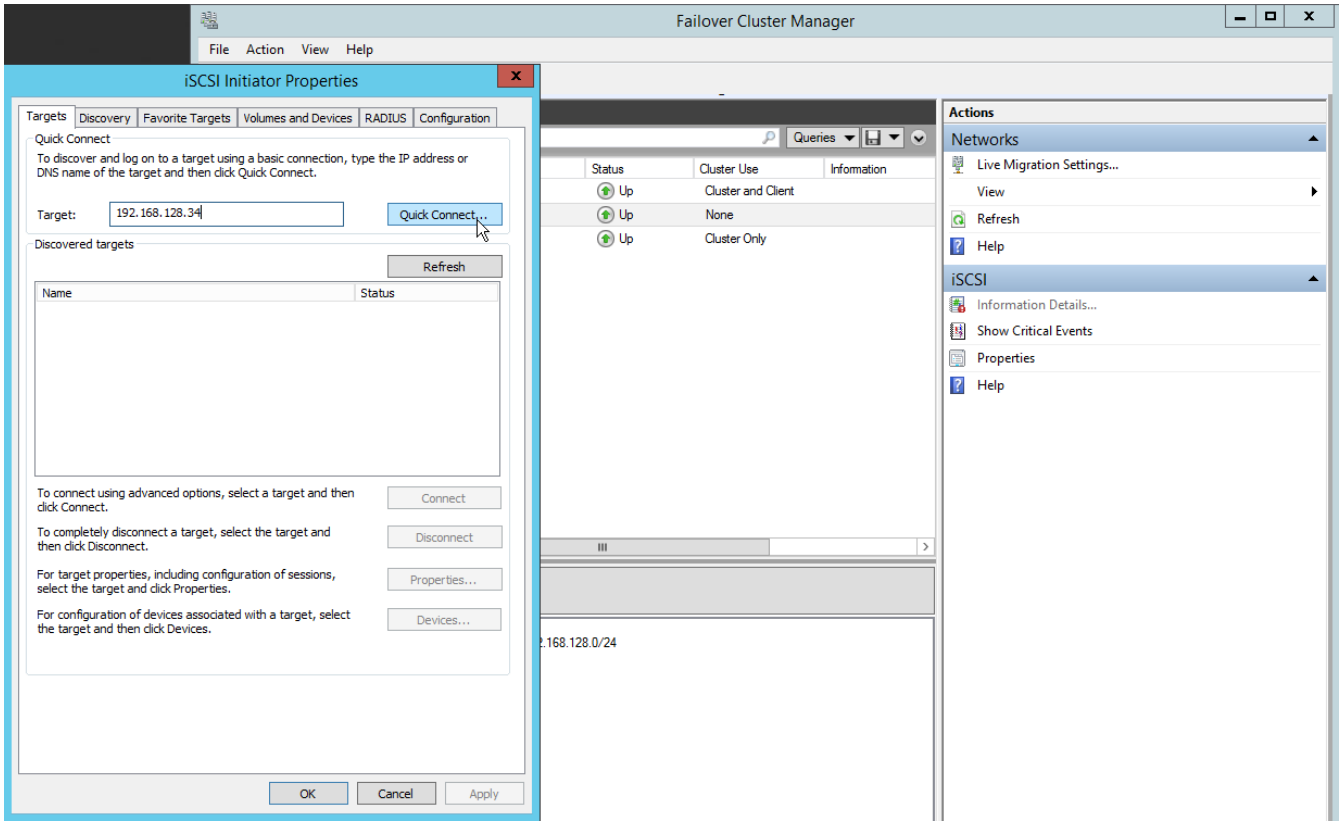
1. Start the iSCSI service.



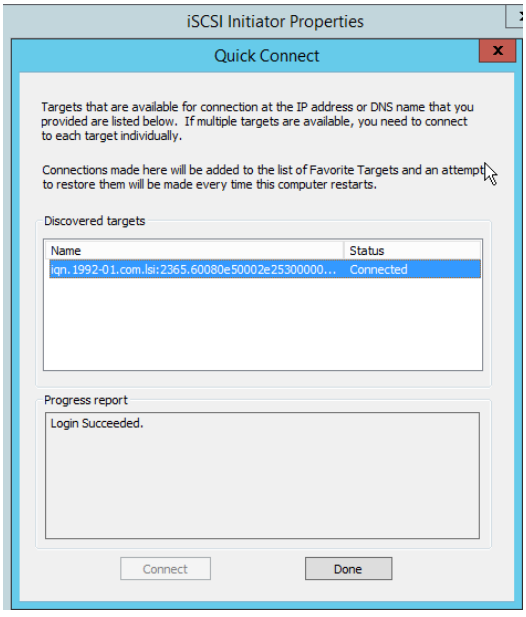
2. Find and start the iSCSI initiator using the Windows search function.



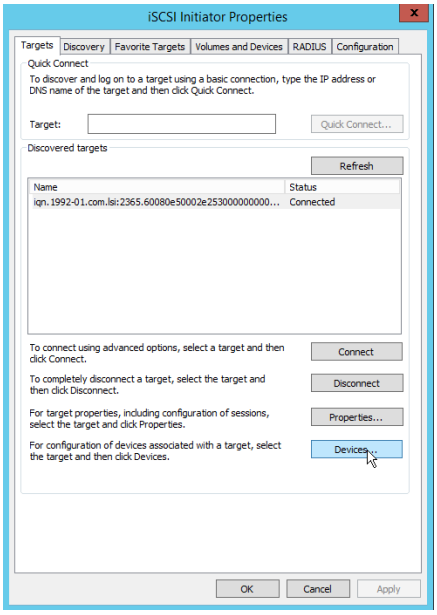
3. The **iSCSI Initiator Properties** dialog box is displayed.
4. Type in the IP address of your iSCSI target and click **Quick Connect...**



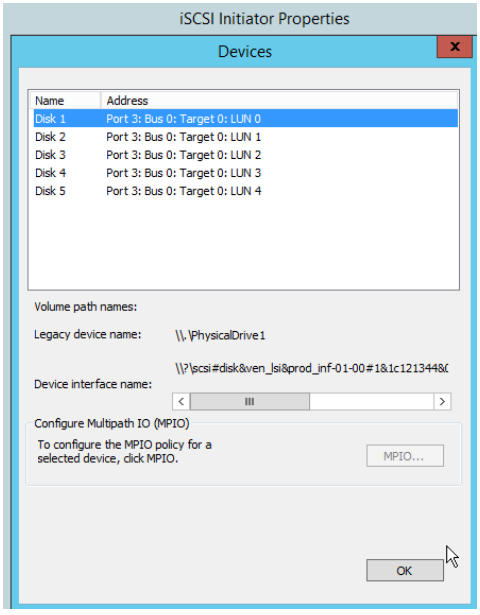
5. The **Quick Connect** dialog box is displayed.
   The successfully connected iSCSI target is displayed in the **Discovered targets** field.



6. Click **Done**.
   The **iSCSI Initiator Properties** dialog box with the connected iSCSI target is displayed.



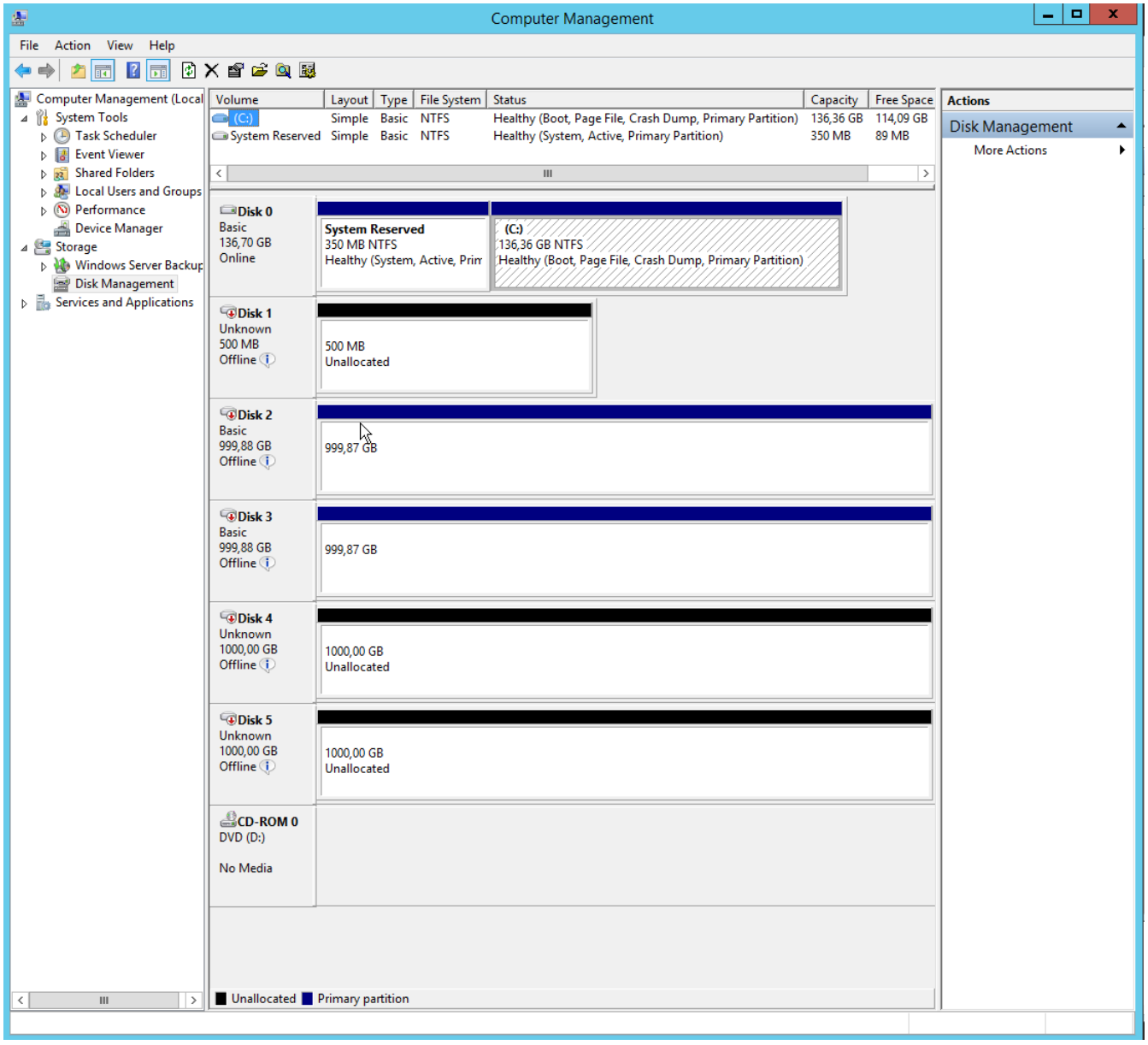
7. Click **Devices...**
   The **Devices** dialog box with all disks assigned to your target are displayed.



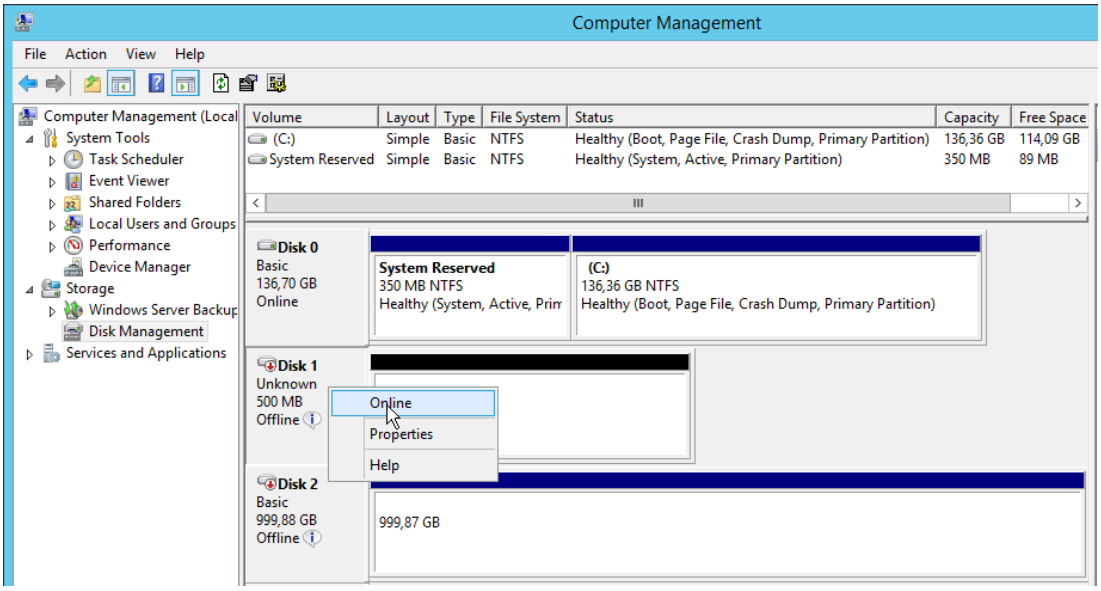
8. Click **OK**.
   The iSCSI target is successfully added.

Initializing the disks of the iSCSI target

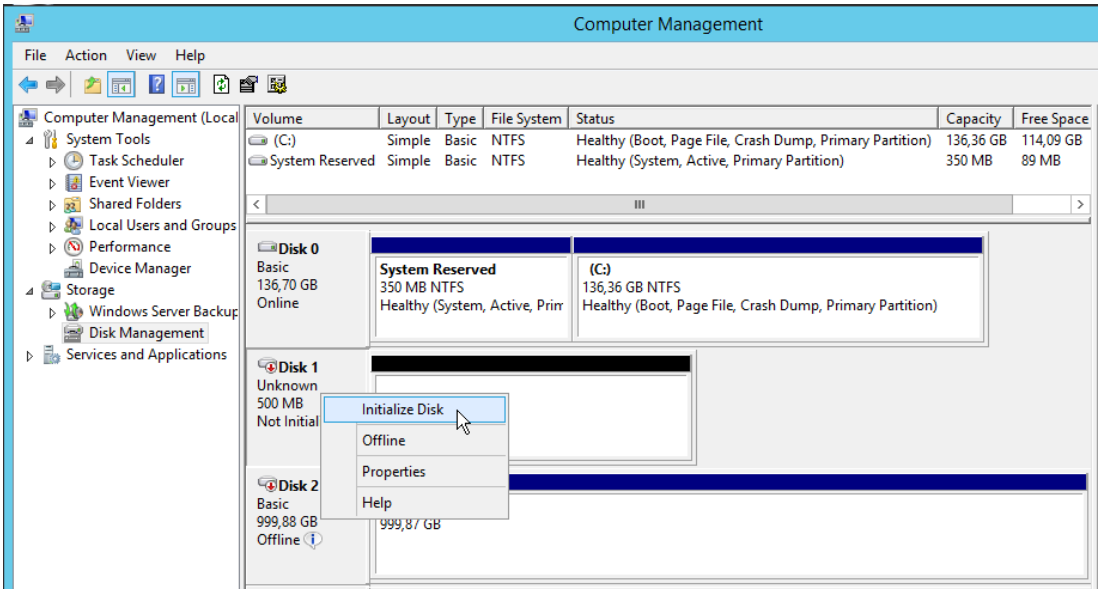
1. Start **Disk Management**.



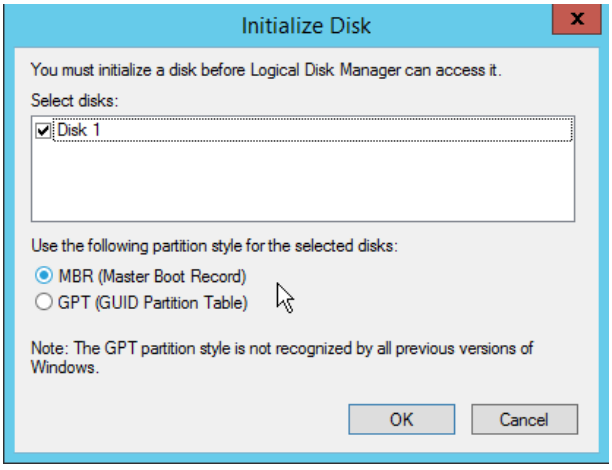
2. Right-click **Disk1** and click **Online**



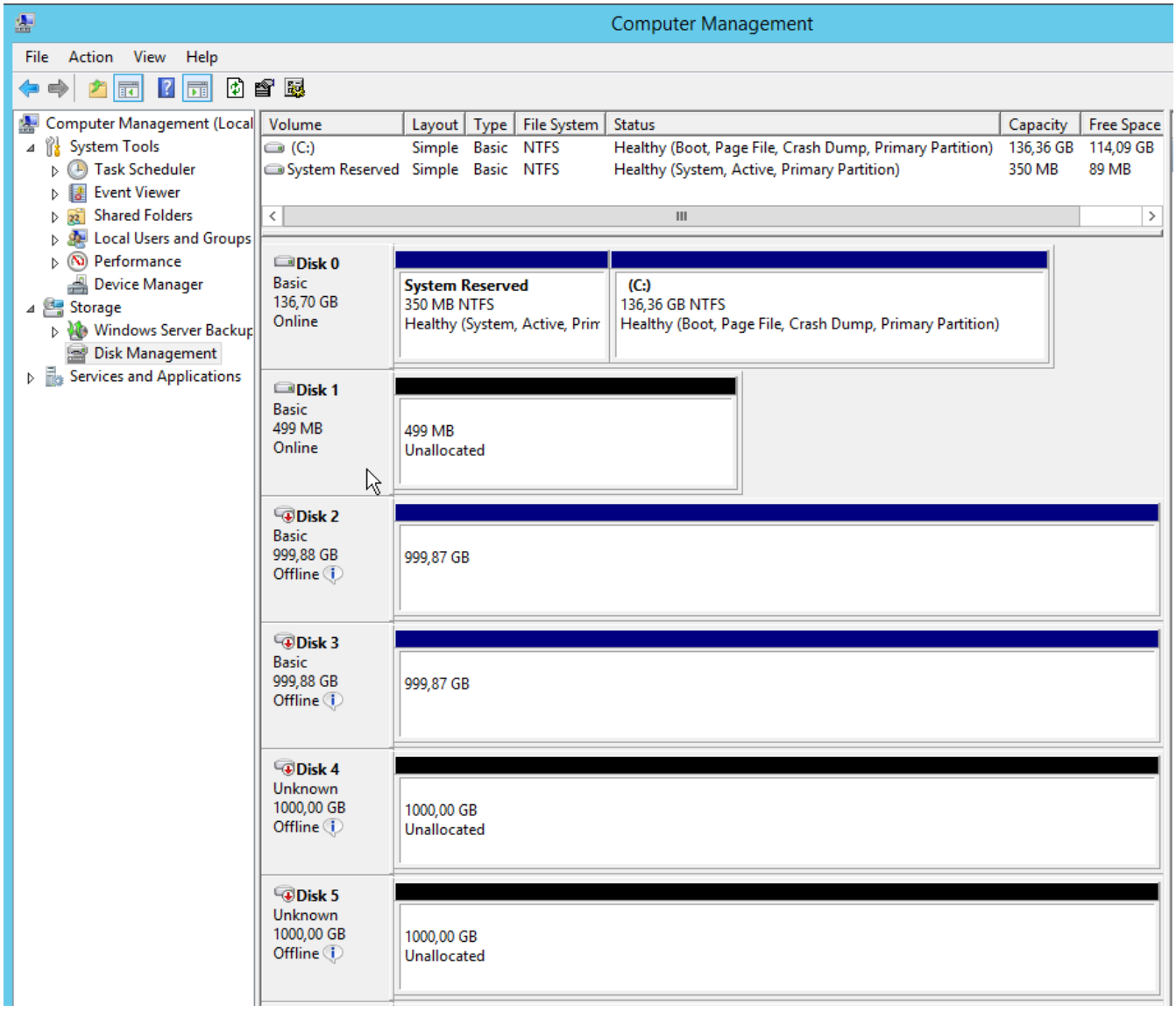
3. Right-click **Disk 1** and click **Initialize Disk**.



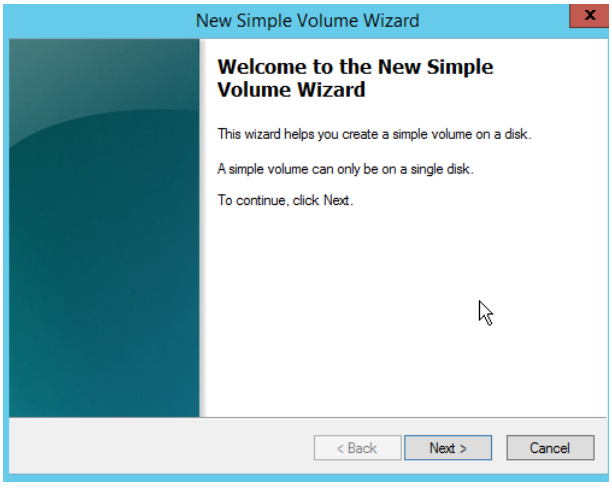
4. The **Initialize Disk** dialog box is displayed.



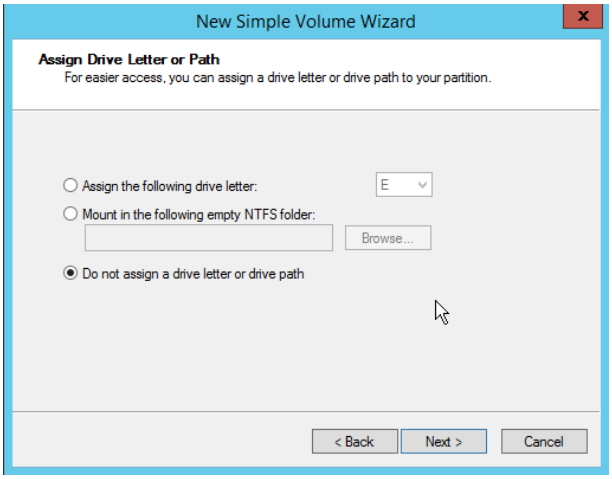
5. Click **OK**
   Disk 1 is online and unallocated.



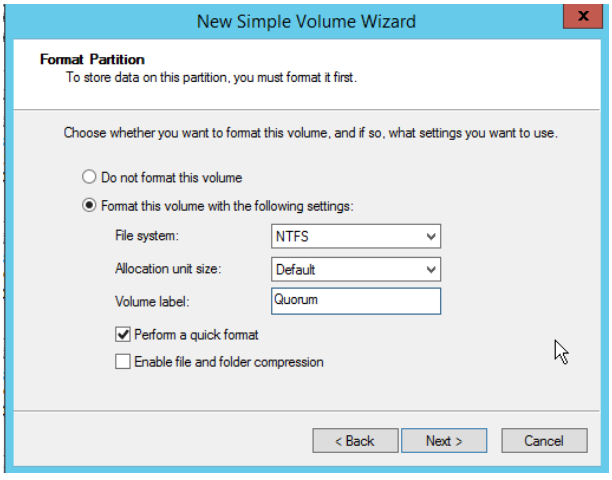
6. Right-click **Disk 1** and click **New Simple Volume**.
   The **New Simple Volume Wizard** is displayed.



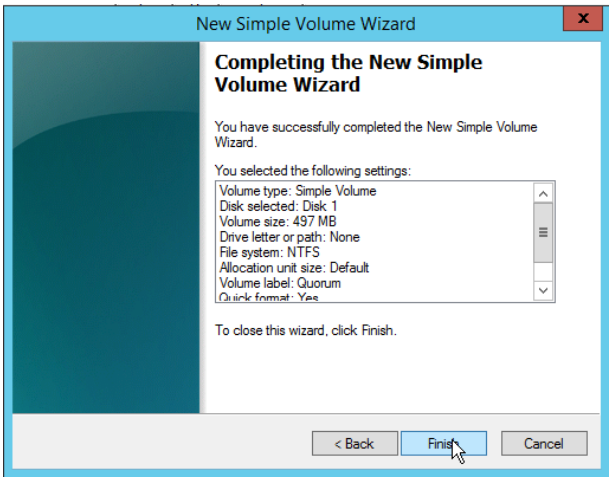
7. Click **Next**.
8. Type in the desired disk size and click **Next**.
9. Click to select **Do not assign a drive letter or drive path**.



10. Click **Next**.
11. Click to select **Format this volume with the following settings**.



12. Click **Next**.



13. Click **Finish**.
14. Repeat the above steps for all disk drives that are not yet included.

5 Performance tips

The following practices help optimize Hyper-V performance

1. Since MS Server 2012 the default **Power Options** for the virtual machines and hosts is **Balanced**. Reset this to **High Performance**.
2. Ensure that the number of virtual CPUs assigned is not higher than the number of physical CPUs available.
3. Install the latest versions of Guest Tools appropriate to your version of the Hypervisor.
4. The virtual hard disks (VHDs) of the virtual machines (VMs) should be deployed on logical unit numbers (LUNs) that suit the demands of the application. For example:
   - Put the operating system (OS) and the application on separate VHDs.
   - Format the VHD for the OS with an allocation unit (cluster size) of 4096
   - (Profitable for BIS, not Bosch VMS) format the VHD where an MS SQL database resides with a cluster size of 64K
   - Format the VHD where the error log resides with a cluster size of 1024
5. If possible, do not run the Hyper-V Manager on the Hyper-V host. Run it from a client instead.
6. Use **Checkpoints** (Snapshots) of virtual machines only temporarily for updates, not for backups, because Checkpoints lead to increased I/O.
7. Always prefer synthetic over emulated hardware (for background information see https://support.microsoft.com/en-us/kb/2844106). Do not activate hardware compatibilities in the devices of the virtual machine, even though this is allowed, for example for the CPU.

6 Example System Dimensions

6.1 Sizing

Sizing			
SCx	**HDD Size**	**Memory Size**	**Network**
HVC1	146 GB	16 GB	4x 1 Gbit/s
HVC2	146 GB	16 GB	4x 1 Gbit/s
HVR1	146 GB	16 GB	4x 1 Gbit/s
HVR2	146 GB	16 GB	4x 1 Gbit/s

6.2 Network segments

Network configuration						
Name	**Named in OS**	**Network mask**	**IP-Address range**	**DNS**	**DHCP**	**Gateway**
Management	MGMT	/24	192.168.100	192.168.0.10	Yes	192.168.0.254
Heartbeat	Heartbeat	/16	172.16	NA	No	NA
Production	E-Netz	DHCP	DHCP	DHCP	Yes	DHCP
Storage	iSCSI	/24	192.168.128	NA	No	NA

6.3 Server configuration

6.3.1 Replication

Server configuration: Physical server (Replication)		
Server name	**HVR1**	**HVR2**
Usage	MS Windows Hyper-V	MS Windows Hyper-V
Server type	HP Proliant DL380	HP Proliant DL380
Network configuration		
NIC1 (MGMT)	192.168.100.101	192.168.100.102
HDD		
C Partition	136 GB	136 GB
Type		
Cluster	No	No
Physical / Virtual	Physical	Physical
OS	Windows Server 2012 R2	Windows Server 2012 R2

6.3.2 Cluster

Server configuration: Physical server (Failover Cluster)			
Server name	**HVC1**	**HVC2**	**HVPDC**
Usage	MS Windows Hyper-V	MS Windows Hyper-V	Domain Controller

Server configuration: Physical server (Failover Cluster)			
Server name	**HVC1**	**HVC2**	**HVPDC**
Server type	HP Proliant DL380	HP Proliant DL380	Hyper-V Virtual Machine
Network configuration			
NIC1 Port1 (MGMT)	192.168.100.1	192.168.100.2	192.168.100.10
NIC1 Port2 (Heartbeat)	172.16.0.1	172.16.0.2	
NIC1 Port3 (E-Netz)	Over DHCP	Over DHCP	
NIC1 Port4 (iSCSI)	192.168.128.1	192.168.128.2	
HDD			
C Partition	136 GB	136 GB	50 GB
Storage			
Volume 1 (Quorum)	500 MB		
Volume 2 (CSV1)	1 TB		
Volume 3 (CSV2)	1 TB		
Type			
Cluster	Management Cluster	Management Cluster	NA
Physical / Virtual	Physical	Physical	Virtual
OS	Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2

6.3.3 Cluster using Starwind solution

Tested with:

- StarWind Virtual SAN V8 Build 8198
- Microsoft Server 2012 R2 as Host System
- Microsoft Server 2008 R2 as Client System
- Bosch VMS 5.5.5.258

Server Name	HVC 1	HVC 2
Usage	Windows Hyper-V	Windows Hyper-V
Server Type	HP Proliant DL 380	HP Proliant DL 380
Network Configuration		
Nic 1 Port 1 Mgmt	192.168.*.*	192.168.*.*
Nic 1 Port 2 Heartbeat / Sync 1	172.16.110.* / 172.16.210.*	172.16.110.* / 172.16.210.*
Nic 2 Port 1 Heartbeat / Sync 2	172.16.111.* / 172.16.211.*	172.16.111.* / 172.16.211.*

Server Name	HVC 1	HVC 2
HDD		
HDD 1 (136GB)	Raid Group 1 C Partition	Raid Group 1 C Partition
HDD 2 (136GB)		
HDD 3 (136GB)	Raid Group 2 StarWind Partition	Raid Group 2 StarWind Partition
HDD 4 (136GB)		
Storage		
Volume 1 (Quorum)	500 MB	500 MB
Volume 2 (CSV1)	100GB	100GB
Type		
Cluster	Management Cluster	Management Cluster
Physical/Virtual	Physical	Physical
OS	Windows Server 2012 R2	Windows Server 2012 R2

Glossary

Emulated device

[Context: Microsoft Hyper-V] Software that emulates a legacy device within a virtual machine. Advantage: availabilitiy of drivers. Disadvantage: sub-optimal performance.

High availability (HA)

Technology to keep a system available for use despite threats such as HW or SW failures, sabotage or natural disasters.

Host

In the context of high availability a host is the physical computer on which hypervisor software creates and runs virtual machines.

Hyper-V

Hyper-V is Microsoft's standard native hypervisor. A hypervisor or virtual machine monitor creates and runs virtual machines.

Logical unit number

a unique identifier to designate an individual or collection of physical or virtual storage devices to a SCSI system

Synthetic device

[Context: Microsoft Hyper-V] A new kind of high-performance virtual device available with Hyper-V. Advantage: better performance than emulated devices.

Virtual hard disk

A software file that emlates a hard disk in high availability technology

Virtual machine

The emulation of a physical computer in software. The VM has its own operating system and uses the physical resources of the physical computer that hosts it. See Host.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com
© Bosch Sicherheitssysteme GmbH, 2016