HIRSCH

HIGH SECURITY MADE SIMPLE

VELOCITY VISION

Velocity Vision Management Server Failover 6.2

Administrator Manual

Contents

Overview

Vision Management Server Failover

If a standalone computer running the management server or SQL Server has a hardware failure, it does not affect recordings or the recording server. However, these hardware failures can result in downtime for operators and administrators who have not logged in to the clients.

Vision Management Server Failover is a Velocity Vision VMS extension that can help you when:

- A server fails – you can run the system components from another computer while you resolve the problems.
- You need to apply system updates and security patches – applying security patches on a standalone management server can be time-consuming, resulting in extended periods of downtime. When you have a failover cluster, you can apply system updates and security patches with minimal downtime.
- You need seamless connection – users get continuous access to live and playback video, and to the system's configuration at all times.

To configure Vision Management Server Failover, you install the management server, log server, and event server on two computers. If the first computer stops working, the VMS components start running on the second computer. Additionally, you can benefit from a secure real-time replication of the VMS databases when SQL Server runs in the failover cluster.

What's new?

In Vision Management Server Failover 6.1

External Public Key Infrastructure (PKI) certificates

- You can now use your certificates to connect to the failover web console. See Use custom server certificates for communication with the failover web console on page 27

SQL Server

- You can use custom locations for the data and log files of the SQL Server databases. See Configure the failover cluster on page 22

In Vision Management Server Failover 4.3

Failover recording server:

- You can now configure Vision Management Server Failover and a failover recording server in a workgroup environment. See Prerequisites for running a recording server or failover recording server on the cluster nodes on page 13.

Troubleshooting:

- To see a list of the most common issues with Vision Management Server Failover, go to Troubleshooting Vision Management Server Failover on page 40.

Compatibility

Vision Management Server Failover is compatible with:

- Velocity Vision Enterprise 3.0 and later
- Velocity Vision Pro 2022 3.0 and later

Vision Management Server Failover elements

Vision Management Server Failover consists of the following elements:

Failover cluster - It consists of two independent computers that work together to maintain high availability of the management server, log server, event server, and SQL Server. If one of the computers fails, the other computer in the cluster takes over the workload of running the VMS server components.

Primary and secondary computers - Typically, the primary computer is the computer you have a running VMS installation on. To configure the failover cluster, you install a VMS product on the secondary computer that mirrors the one on the primary computer.

Nodes - The failover cluster consists of two computers called nodes. The primary computer is referred to as Node 1, and the secondary computer is referred to as Node 2. The names of the nodes do not change but they can have different states. During normal operation, the node the VMS servers run on is in PRIM state and the standby node is in SECOND state.

Virtual IP - The virtual IP serves as a cluster address and allows the remote servers to connect seamlessly to the running management server. The virtual IP is an address you define during the configuration of the failover cluster.

Related topics:

- Failover steps on page 6
- The failover web console on page 31
- Node states on page 33

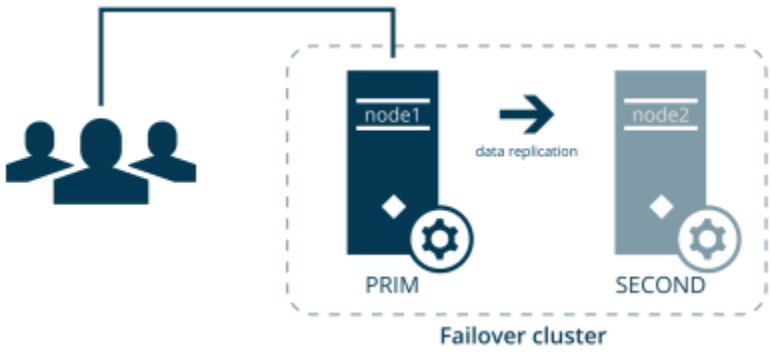
Failover steps

In a typical scenario, you install these components on both nodes:

- Velocity Vision Management Server
- Velocity Vision Log Server
- Velocity Vision Event Server
- SQL Server

The failover steps in a typical scenario are:

I. The management server, event server, log server, and SQL Server run on Node 1 (in PRIM state). If you have installed SQL Server on the nodes, Vision Management Server Failover replicates the data from these system components on Node 2 (in SECOND state).

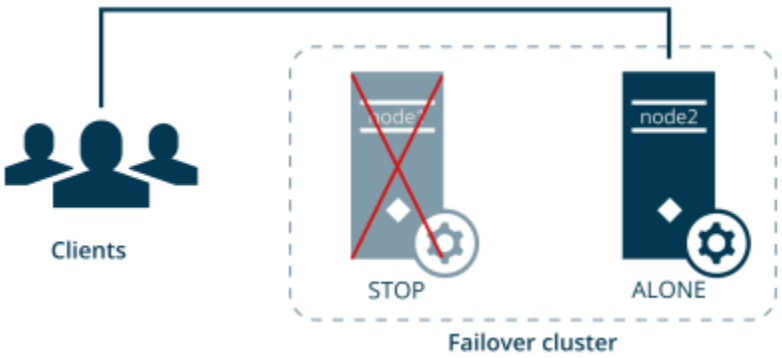


Every second, the nodes exchange heartbeats.

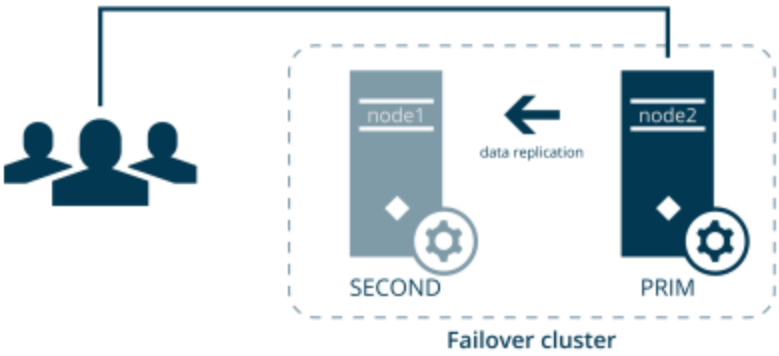
II. If the management server on Node 1 becomes unavailable for 30 seconds, Node 2 takes over.

The failover time depends on the startup time of the Management Server service.

1. Node 2 comes into ALONE state, and the data replication stops.
2. The management server, event server, log server, and SQL Server start running on Node 2.
3. The management server, event server, and log server store data on the SQL Server on Node 2.



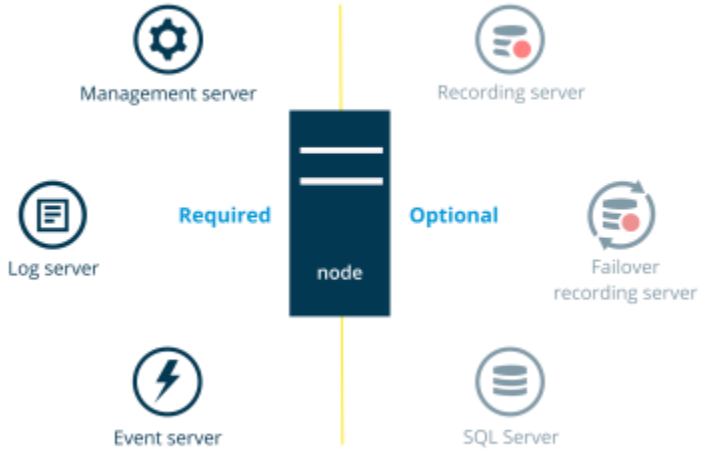
III. You identify and fix the issue that caused the failover and start Node 1 from the failover web console. The data that was modified on Node 2 replicates to Node 1.



The VMS system components still run on Node 2 (in PRIM state), and the data replicates on Node 1 (in SECOND state). If needed, you can swap the states of the nodes from the failover web console.

Required and optional Velocity Vision VMS components

Depending on the size of your VMS installation and resources, you can configure Vision Management Server Failover in different ways. You can install the following system components on Node 1 and Node 2 in a domain or workgroup environment:



On the failover cluster nodes, you must install:

- Velocity Vision Management Server
- Velocity Vision Event Server
- Velocity Vision Log Server

Additionally, you can install the following system components:

SQL Server

You can use internal or external SQL Server instances.

To use an internal SQL Server instance, you must install SQL Server on both nodes. When using an internal SQL Server instance, Vision Management Server Failover replicates the contents of the SQL Server databases and triggers failover if the SQL Server instance fails.

If you have a large VMS installation, you can use an external SQL Server instance and exclude SQL Server from the failover cluster. In this scenario, the Vision Management Server Failover solution does not monitor and replicate the SQL Server databases. Hirsch recommends regular backups of the SQL Server databases as a disaster recovery measure.

See SQL Server prerequisites on page 10.

Recording Server

You can install a recording server on one or both nodes.

Vision Management Server Failover does not provide failover for the recording server. You must configure the failover recording server yourself.

See Prerequisites for running a recording server or failover recording server on the cluster nodes on page 13.

Failover Recording Server

You can install a failover recording server on one or both nodes.

If you have limited resources, you can use the failover cluster nodes to host a recording server and a failover recording server. You configure the failover recording server from Velocity Vision Management Client.

For system resiliency, Hirsch recommends installing the recording server on Node 2 and the failover recording server on the Node 1.

When part of the failover cluster, the failover recording server can work only in a Hot standby setup.

Licensing

Vision Management Server Failover licenses

Vision Management Server Failover comes with a three-day demo license.

To use the failover cluster for an unlimited period, register the host names of the nodes and add your Vision Management Server Failover license.

If you do not add your Vision Management Server Failover license, the Management Server service will stop after three days.

To obtain a license for Vision Management Server Failover, contact your reseller.

You can add the license during the failover cluster configuration or afterward. See Add a license for Vision Management Server Failover on page 27.

Requirements and considerations

Network and computer prerequisites

Before you can start using Vision Management Server Failover, you must make sure that you go through the following network and computer prerequisites:

- Operating system - Install two identical operating systems on Node 1 and Node 2. To see a list of supported operating systems, go to https://portal.hirschsecure.com/aspx/login..
- Addresses - In the same subnet, assign static IPv4 addresses to the nodes and reserve an IPv4 address for the virtual IP. The virtual IP allows the remote servers to connect seamlessly to the running management server.

  If the host name and address of a node does not resolve as expected by the system, the configuration might fail. See DNS lookups on page 17.

  Do not assign IPv6 addresses to the computers that run the management server and external SQL Server. Vision Management Server Failover does not support the IPv6 protocol.

- Domain or workgroup environment - Configure the failover cluster in an Active Directory (AD) domain or workgroup environment.

  Domain

  Use the same AD domain on both nodes.

  Workgroup

Prerequisite	Description
Workgroup membership	Add Node 1 and Node 2 to the same workgroup.
(When without DNS server) Host name mapping	Map the host names of the nodes to their IP addresses. See Map the host names of the nodes on page 19.
Windows group	You must add a new Windows group in Velocity Vision Management Client on both nodes. Go to **Roles** and add the BUILTIN/Administrators Windows group to the **Administrators** role.
Basic user	To make sure you can always log in, add a basic user to the Administrators role in Velocity Vision Management Client for the VMS installations on both nodes. Go to **Roles** and add an existing basic user or create a new one.

- Time - Synchronize the time and time zones between the nodes.
- ICMP traffic - Allow inbound ICMP traffic through Windows Defender Firewall.
- PowerShell execution policy - Set your PowerShell execution policy to Unrestricted. This allows the configuration wizard to run PowerShell scripts on both nodes. See about_Execution_Policies.
- Windows Defender Advanced Thread Protection Service - You must disable Windows Defender Advanced Thread Protection Service. See Disable Windows Defender Advanced Thread Protection Service on page 16.

SQL Server prerequisites

When using an internal SQL Server instance, Vision Management Server Failover replicates the contents of the SQL Server databases and triggers failover if the SQL Server instance fails.

For large VMS installations, you can connect the management server to an external SQL Server instance.

Internal SQL Server instance

The SQL Server installations must be identical on both nodes. To see a list of supported SQL Server editions for your VMS product, go to https://portal.hirschsecure.com/aspx/login.

Also, consider the following:

Prerequisite	Description
Database backup	Back up any existing databases to avoid loss of data. During the failover cluster configuration, the wizard replicates the SQL Server databases on Node 1 to the SQL Server databases on Node 2. All data on the SQL Server databases on Node 2 is overwritten.
SQL Server service account	The SQL Server service must run under the same user account as the Velocity Vision services. To change a service account for the Velocity Vision VMS, see Changing the service account that runs a VMS service on page 18
Database location	You can use the default or custom location for the VMS databases data and log files. The default configuration is as follows: • The VMS databases data and log files are stored in the DATA folder. • The SQL Server error logs, trace log files, and log events are stored in the Log folder.

	• The DATA and Log folders belong to the same parent folder. The default locations are: • `C:\Program Files\Microsoft SQL Server\MSSQL{nn}.MSSQLSERVER\MSSQL\DATA` • `C:\Program Files\Microsoft SQL Server\MSSQL{nn}.MSSQLSERVER\MSSQL\Log` {nn} is the version number. If you use custom locations for the data and log files, you can select them during the configuration of the failover cluster
Virus scanning exclusions	In your antivirus program, exclude the locations of the DATA and Log folders from virus scanning.
Instance name	Verify that the instance name of your SQL Server is MSSQLSERVER. See View the SQL Server instance name on page 17.

External SQL Server instance

You can use a SQL Server instance that is hosted elsewhere in your network. Vision Management Server Failover does not monitor the SQL Server databases when the SQL Server instance is hosted on a separate server.

The failover server configuration with external SQL Server does not work in a workgroup environment.

Prerequisite	Description
Permissions for the SQL Server user	In Microsoft SQL Server Management Studio, add a Windows user to the public role and map the user to the db_owner database role for the following databases: • Surveillance • Surveillance_IDP • Surveillance_IM • LogserverV2
Connection	Verify that the VMS installations on both nodes: • Are connected to the external SQL Server instance.

	• The VideoOS IIS application pools on Node 1 are running. • The VMS services on Node 1 are running.
Service account	Make sure that the Management Server service on both nodes runs under the Windows user you added on the SQL Server computer. If your SQL Server runs under a different user, you can change the account that runs the Management Server service. See Changing the service account that runs a VMS service on page 18.
Database conflicts	If you have two or more running management servers that are connected to the same SQL Server databases, your data might be corrupted. To avoid potential database conflicts, before you start the configuration, go to Node 1 and: • Stop all VMS services. You can start the services after you have configured the failover cluster. See Start or stop a VMS service on page 19. • Stop all Internet Information Services (IIS) application pools for the VMS. You can start the application pools after you have configured the failover cluster. See Start or stop an Internet Information Services (IIS) application pool on page 19.

Velocity Vision VMS prerequisites

Install two identical VMS products under a common user account with administrator permissions. To learn more about the general prerequisites for installing Velocity Vision VMS, see the Velocity Vision VMS administrator manual.

When working in a domain environment, select AD users for the service accounts and only give them the permissions required to run the relevant services.

On both nodes, install the following system components:

- Velocity Vision Management Server
- Velocity Vision Event Server
- Velocity Vision Log Server
- Vision Management Server Failover
- Velocity Vision Recording Server (optional), see Prerequisites for running a recording server or failover recording server on the cluster nodes on page 13.

Hirsch recommends that you install all other server components not mentioned above on different computers.

Depending on your system configuration, consider the following:

- System configuration password - To assign a system configuration password, use the same password for the VMS installations on both nodes.

Encryption considerations

If you want to encrypt the connection between the failover cluster nodes and other VMS components, you must consider the following:

- VMS certificates - To encrypt the connection to and from the running management server, you must install the CA certificate and an SSL certificate on both nodes. See Encrypting the connection to the failover cluster on page 15.
- Failover certificates - The failover cluster communicates with the failover web console through HTTP or HTTPS. During the failover cluster configuration, you select the connection protocol. If you select HTTPS, the wizard generates a server certificate that encrypts the connection to the failover web console. See Server certificate for the failover web console on page 13.
- Identity Provider - To ensure that users can log in to the running management server, you must set up data protection and update the data protection keys. See Update the data protection settings for Identity Provider on page 15.

Prerequisites for running a recording server or failover recording server on the cluster nodes

Installing the recording server or failover recording server on the cluster nodes requires additional steps.

You can install a recording server or failover recording server on one or both nodes. For example, you can install:

- A recording server on Node 1.
- A recording server on Node 1 and a failover recording server on Node 2.
- A recording server on Node 1 and Node 2.

Before you configure the management server failover, consider the following:

- Environment - The nodes can run in a domain or workgroup environment.
- Failover recording server setup - If you configure a failover recording server on any of the nodes, you must use it in a hot standby setup.
- Encryption (optional)- To encrypt the connection between the VMS components, you must install the SSL certificate for the recording server on the recording server computer. Then, you must enable encryption for the recording server from the recording server's Server Configurator.
- Services - The Velocity Vision Recording Server service and the configuration wizard for Vision Management Server Failover need port 9001 to operate. To avoid conflicts, you must either use another port for the Hirsch Velocity Vision Recording Server service or stop the service when you configure or remove the configuration from the failover cluster.

To learn more about the configuration of the recording server and the failover recording server, see the Velocity Vision VMS administrator manual.

Server certificate for the failover web console

You can connect to the failover web console over an HTTP or HTTPS connection. This section is only relevant if you want to use an HTTPS connection.

To secure the communication with the failover web console, you need a server certificate, see The failover web console on page 31.

The wizard downloads a server certificate from a local web service while configuring the failover cluster on Node 1.

The server certificate is a .crt file that you install on your computer. You must add the certificate to the computer's "Trusted Root Certification Authorities" store so that your computer trusts that certificate. If you do not install the certificate, your connection will remain secure, but:

- You will get a security warning the first time you open the failover web console.
- The system will not trigger an event in case of failover.

Install the server certificate on all computers from which you want to access the failover web console, see Install the server certificate on a computer on page 26.

The wizard downloads a new server certificate whenever you configure the failover cluster. You can remove the previous certificates from the "Trusted Root Certification Authorities" store.

The wizard stores the certificate on Node 1. If you lose the server certificate, you can download it again from the **Manage your configuration** page on Node 1. See Download the server certificate to access the failover web console on page 29.

The server certificate is valid for five years. You will not receive a warning when a certificate is about to expire. If a certificate expires, your browser will no longer trust that certificate. To renew the server certificate, you must configure a new failover cluster.

Browser requirements for the failover web console

Use the failover web console to manage the failover cluster. To learn more, see The failover web console on page 31.

To make sure that the contents of the failover web console are correctly displayed:

- Network, firewall, and proxy configuration must allow access to the administration network of all the servers that are administered with the web console.
- JavaScript must be available and enabled in the web browser.
- To avoid security popups in Internet Explorer, you may add the addresses of the primary and the secondary computer into the Intranet or Trusted zone.
- The messages in the failover web console are displayed in French, English, Japanese languages, according to the preferred language configured into the web browser (for not supported languages, English is displayed).
- To see the list of supported browsers, go to the Hirsch website (https://portal.hirschsecure.com/user/login)
- After every VMS upgrade, clear the browser's cache. To clear the cache only for the failover web console page, press **Ctrl**+**F5**.

Additional configuration

Encrypting the connection to the failover cluster

To connect securely to the running management server, the remote servers must trust both Node 1 and Node 2.

To learn how to generate and install certificates, see the Velocity Vision VMS certificates guide.

To enable encryption between the management servers and the remote servers, you must install on both nodes:

- The public CA certificate
- The SSL certificate for the failover cluster

Do not enable encryption on the management server if you have already configured the failover cluster.

If you want to enable encryption for a new VMS installation, you must:

1. Create a private and a public CA certificate.
2. Install the public certificate on all client computers.
3. Create an SSL certificate for the failover cluster.
4. Install the SSL certificate for the failover cluster on Node 1 and Node 2.
5. Enable encryption for the Management Server service on both nodes.
6. Create and install certificates on the remote servers.
7. Enable encryption on the remote servers.

Update the data protection settings for Identity Provider

When you install Velocity Vision in a single-server environment, the Identity Provider configuration data is protected using Data Protection API (DPAPI). If you set up the management server in a cluster, you must update the Identity Provider configuration data to make it identical on both nodes.

To ensure fluent node failover, you must set up data protection and update the data protection keys for the user running the VideoOS IDP AppPool application pool.

You must have imported your certificate to the Personal store for the user running **VideoOS IDP AppPool** and given it Read permissions. Also, if you use a self-signed certificate, you must add it to the Trusted Root Certificates Authorities store on your local computer.

On Node 1:

1. Locate the `appsettings.json` file in the installation path of the Identity Provider (`[Install path]\Hirsch\Velocity VisionManagement Server\IIS\IDP`).
2. In the DataProtectionSettings section, make the following changes:
    - To set up data protection, set the thumbprint of the certificate that's used by the IDP application pools and the Management Server service. See How to: Retrieve the Thumbprint of a Certificate.

- To remove the old certificate key, set **CleanUpNonCertificateKeys** to **true**.

```
"DataProtectionSettings": { "ProtectKeysWithCertificate": { "Thumbprint": ""
"CleanUpNonCertificateKeys": true } },
```

3. Repeat steps 1-2 on Node 2.

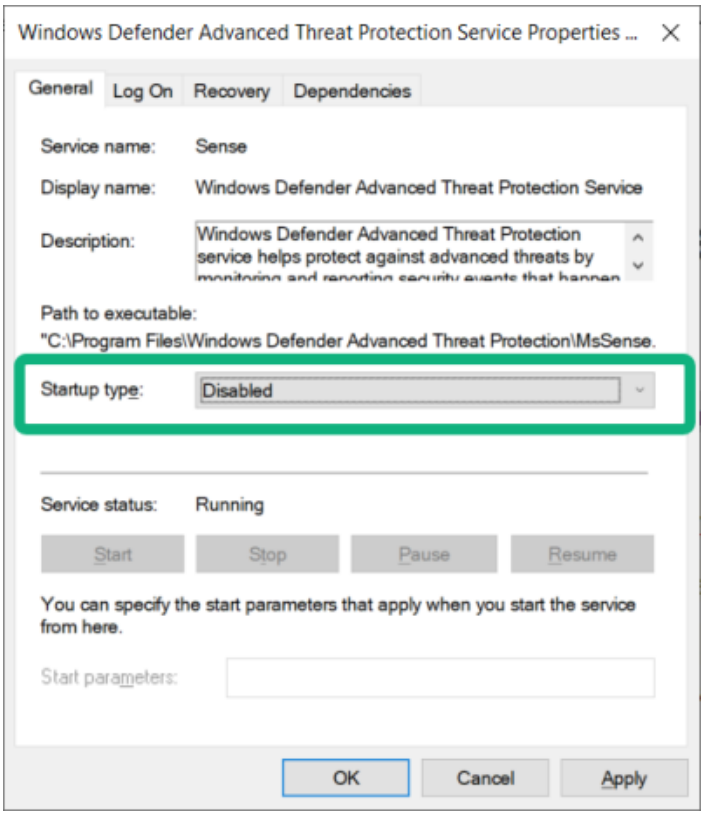
Disable Windows Defender Advanced Thread Protection Service

The configuration of the Vision Management Server Failover will fail if the Windows Defender Advanced Thread Protection Service is enabled.

1. On Node 1, open the **Start** menu, and enter **services.msc** to open **Services**.
2. Scroll down to **Windows Defender Advanced Threat Protection Service**.
3. Check the status of the service. If the status field is blank, this means that the service is not running.
4. To prevent the service from starting at system startup, right-click the service and select **Properties**. On the **General** tab, change the **Startup type** to:
   - **Disabled** if the service is running.
   - **Manual** is the service is stopped.

   Then, select **OK** to save your changes.

   You must have the necessary user permissions in Windows to perform this operation.



5. Repeat steps 1-4 on Node 2.

DNS lookups

For successful failover cluster configuration, Hirsch recommends that you run DNS queries in Windows PowerShell:

- Use forward DNS lookup to obtain an IP address by searching the domain
- Use reverse DNS lookup to obtain the host name that is related to an IP address

To make sure that the IP addresses and the host names of the nodes are resolved as expected, you must perform the queries on Node 1 and Node 2:

Query name	Command	Perform on	Expected result
Forward DNS lookup	Resolve-DnsName [Node 2 host name]	Node 1	The host name of Node 2 corresponds to the first IP address on the list.
Forward DNS lookup	Resolve-DnsName [Node 1 host name]	Node 2	The host name of Node 1 corresponds to the first IP address on the list.
Reverse DNS lookup	Resolve-DnsName [Node 2 IP address]	Node 1	The IP address of Node 2 corresponds to the first host name on the list.
Reverse DNS lookup	Resolve-DnsName [Node 1 IP address]	Node 2	The IP address of Node 1 corresponds to the first host name on the list.

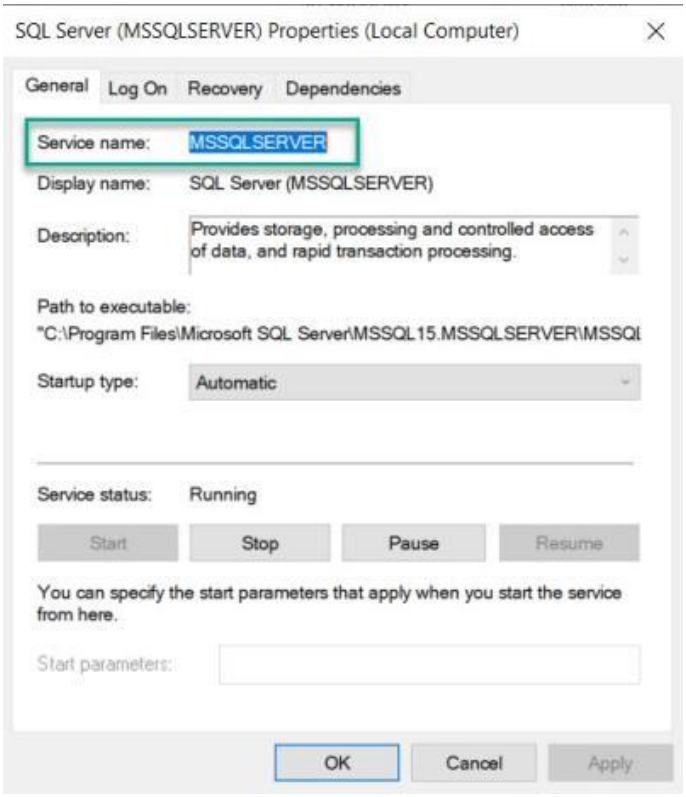
View the SQL Server instance name

This section is only relevant if you want to use an internal SQL Server instance.

Vision Management Server Failover uses a hardcoded name for the SQL Server instance name **MSSQLSERVER** and, If the instance name differs, the configuration will fail.

You must check the SQL Server instance name on both nodes.

1. Open the **Start** menu, and enter **services.msc** to open **Services**.
2. Scroll down to **SQL Server [Display name]**.
3. Right-click the service and select **Properties**. On the **General** tab, the value in the **Service name** field is the instance name.



Changing the service account that runs a VMS service

A Microsoft service account is an account used to run one or more services or applications in a Windows environment. The VMS services use the service accounts to register and communicate with the other VMS components. You select the service account for the VMS during the installation of the Velocity Vision VMS, such as **Network Service**, but you can change the service account afterward.

To make sure that the different VMS components can communicate with each other after you have changed the service account, you must do the following:

1. Add the selected Windows user to the Administrator role in Velocity Vision Management Client.
2. In Microsoft SQL Server Management Studio, add a Windows user to the **public** role and map the user to the **db_owner** database role for the following databases:
   - **Surveillance: Management and event server**
   - **Surveillance_IDP: IDP**
   - **Surveillance_IM: Incident Manager**
   - **LogserverV2: LogServer**
3. Stop the VMS services, see Start or stop a VMS service on page 19.
4. Stop the IIS application pools for the VMS, see Start or stop an Internet Information Services (IIS) application pool on page 19.
5. Change the identity of an IIS application pool, see Change the identity of an IIS application pool for Velocity Vision on page 20.
6. Change the service accounts for the VMS, see Change the service account for a Windows service on page 20.

7. Register the management server from the Server Configurator.

   The registration triggers a restart of the server services. Once the services start, a confirmation appears, stating that registration on the management server has succeeded. If the services did not start automatically, you can start them from the Windows Services Manager, see Start or stop a VMS service on page 19.

Start or stop a VMS service

The VMS services use the service accounts to register and communicate with the other VMS components. To start or stop a VMS service:

1. Open the Start menu, and enter **services.msc** to open **Services**.
2. Right-click a **Hirsch Velocity Vision** service and select **Start** or **Stop**.

   The VMS services for Vision Management Server Failover are:

   - The **Hirsch Velocity Vision Management Server** service
   - The **Hirsch Velocity Vision Log Server** service
   - The **Hirsch Velocity Vision Event Server** service
   - The **Hirsch Velocity Vision Data Collector** service
   - (Optional) The **Hirsch Velocity Vision Recording Server** service

Start or stop an Internet Information Services (IIS) application pool

The management server communicates with the remote servers through IIS.

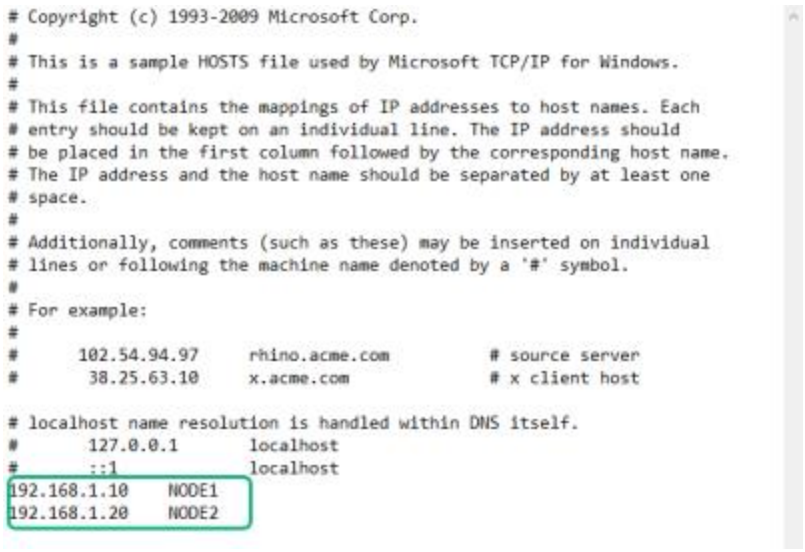
To start or stop an IIS application pool:

1. Open the Start menu, and enter **inetmgrc** to open **Internet Information Services (IIS) Manager**.
2. On the **Connections** pane, double-click on your server to expand the list menu, then select **Application Pools**.
3. Right-click an application pool that starts with **VideoOS** and select **Start** or **Stop**.
4. Repeat step 3 for all **VideoOS** application pools.

Map the host names of the nodes

If you do not have a DNS server to resolve the host names of Node 1 and Node 2, you must map their IP address to host names manually.

1. On Node 1, go to **`C:\Windows\System32\drivers\etc`** and open the **hosts** file as administrator with a text editor such as Notepad.
2. Under the section **`localhost name resolution is handled within DNS itself`**, specify the IP address of Node 1 and its host name. On a new line, add the IP address of Node 2 and its host name.



Repeat the same steps on Node 2.

Change the identity of an IIS application pool for Velocity Vision

To change the identity of an IIS application pool:

1. Open the Start menu, and enter **inetmgrc** to open **Internet Information Services (IIS) Manager**.
2. On the **Connections** pane, double-click your server to expand the list menu, then select **Application Pools**.
3. Right-click an application pool that starts with **VideoOS** and select **Advanced settings...**
4. Under **Process Model**, change the **Identity** with the selected Windows account.
5. Repeat steps 3-4 for all **VideoOS** application pools.
6. Start all **VideoOS** application pools.

Change the service account for a Windows service

To change the service account for a Windows service:

1. Open the Start menu, and enter **services.msc** to open **Services**.
2. Right-click on the service you want to change the service account for and select **Properties**. The Windows services used by Velocity Vision are:
    - The **Hirsch Velocity Vision Management Server** service
    - The **Hirsch Velocity Vision Log Server** service
    - The **Hirsch Velocity Vision Event Server** service
    - The **Hirsch Velocity Vision Data Collector** service
3. On the **Log On** tab, select **This account** and specify or browse for your account.
4. Enter the password and select **OK** to save your changes.

Installation

Install Vision Management Server Failover

The Vision Management Server Failover component is part of the Velocity Vision installer. You can install it with a new VMS installation or add it later.

To set up a failover cluster, you must install the Vision Management Server Failover component on two separate computers, referred to as nodes.

Install Vision Management Server Failover with a new VMS installation

Follow the steps for **Custom** installation and select Vision Management Server Failover as a component you want to install.

Add the Vision Management Server Failover component to an existing VMS installation

1. Open **Add or remove programs** on Windows and select Hirsch.
2. Select **Modify** to launch the Hirsch Velocity Vision VMS wizard.
3. On the **Uninstall or change Hirsch Velocity Vision VMS components**, select **Change one or more Hirsch Velocity Vision VMS components**. Select **Continue**.
4. Select Vision Management Server Failover. Select **Continue** to install the component.
5. When the installation is complete, the list displays the installed components.

To continue with the cluster configuration, see Configure the failover cluster on page 22

Configuration

Configure Vision Management Server Failover (wizard)

When you select **Configure Vision Management Server Failover** from the Management Server Manager tray icon, you get one of the following messages:

Your Velocity Vision **product does not support** Vision Management Server Failover

To learn more about the supported products, see Compatibility on page 5.

No failover management server installed on this computer

Make sure that you have installed the Vision Management Server Failover component on the computer, see Install Vision Management Server Failover on page 21.

Select the step in your configuration flow

You have started the configuration process, see Configure the failover cluster on page 22.

Manage your configuration

From this page you can:

- **Apply failover license**, see Add a license for Vision Management Server Failover on page 27.
- **Download server certificate on your computer**, see Download the server certificate to access the failover web console on page 29.
- **Change current password for authentication**, see Change the password for authentication on page 31.
- **Remove existing configuration**, see Remove the existing failover cluster configuration on page 30.

Configure the failover cluster

During the configuration process, you switch between Node 1 and Node 2. To configure the failover cluster successfully:

I. Start the configuration on Node 2. Once you prepare Node 2, move to Node 1.

II. Continue the configuration on Node 1. Once done, move to Node 2.

III. Finish the configuration on Node 2.

During the configuration, the Velocity Vision VMS users won't be able to log in to any Velocity Vision client during configuration.

I. Start the configuration on Node 2

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Configure the secondary computer** and select **Continue**.
3. Make sure that you have installed the required system components and scheduled downtime. Select **Confirm** to continue.
4. On the **Select connection protocol** page, select a protocol for communication with the failover web console.
   - To use a system-generated certificate, select **HTTPS** to secure your connection. During configuration, the wizard takes the first DNS entry from your DNS servers list to generate the certificate. If the DNS server is down, the failover cluster configuration might fail.
   - If you want to use a custom certificate for encryption or you do not want to encrypt your connection, select **HTTP**.

   Select **Continue**
5. On the **Set a password for authentication** page, specify a password for login to the failover web console. You need to set the same password on Node 1.

   Select **Continue**.

The wizard prepares the node and informs when successfully completed.

(For HTTPS only) Save the security code. To establish a secure connection between the nodes, you must specify the security code on the Node 1.

You are now ready to continue on Node 1.

II. Continue the configuration on Node 1

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. In the **Failover management server** wizard, select **Configure the primary computer**.

   If you want to exclude SQL Server from the failover cluster, select **Use an external SQL Server**.

   If you select to use external SQL Server, Vision Management Server Failover will not replicate the data on the SQL Server databases. To keep your SQL Server databases safe, you must configure a backup solution yourself.

   Then, select **Continue**.
3. If you have prepared Node 2, select **Confirm** to continue.
4. On the **Select connection protocol** page, select the same connection protocol you selected on Node 2. Select **Continue**.
5. On the **Specify locations of the SQL Server data and log files** page, click the check box to browse for your SQL Server data and log files if you use custom locations. If you use the default locations, you can skip this step. Select **Continue**
6. On the **Connect to the secondary computer** page, specify the required system information.

Name	Description
Secondary computer's FQDN (recommended), host name, or IPv4 address	Specify the address of Node 2. • When in an AD domain, you must specify the Fully Qualified Domain Name (FQDN) of Node 2. • If it is a workgroup environment, specify the host name (recommended) or IP address of Node 2.
Failover license	If you have purchased an Vision Management Server Failover license, you can add it now on this node. If you do not add a license within three days, the Management Server service will stop. You must add the same Vision Management Server Failover license on both nodes.
Virtual IPv4 address	The remote servers will communicate with this IPv4 address instead of the management server address. Specify an available IPv4 address in your network to replace the actual address of the management server.
Security code (for HTTPS only)	To establish a secure connection between the nodes, specify the security code you got from Node 2.

Then, select **Continue**. If you have not added a license, a message informs you that the management server becomes unavailable after three days.

7. On the **Set a password for authentication** page, enter the password that you set on Node 2 in step 5, then select **Continue**.

   The wizard configures the failover cluster. The wizard configures the failover cluster. The time may vary depending on the system load, connection speed and the size of the SQL Server databases that are replicated.

8. (For HTTPS only) On the **Select destination folder for the server certificate** page, specify a destination folder. If you do not select a destination folder, the wizard will export the certificate to `C:\Users\{user}\Documents`.

   Select **Continue**. The wizard saves the certificate to the selected folder.

When the configuration of Node 1 succeeds, go to Node 2 to finish the configuration.

III. Finish the configuration on Node 2

1. Confirm that you have completed the configuration on Node 1, and then select **Continue**.
2. On the **Add a failover license on this computer** page, you can add your failover license.

   Select **Continue**.

3. When the configuration is successful, the failover web console opens automatically on Node 2. Node 1 comes into the PRIM state, and Node 2 comes into the SECOND state.

   The wizard adds a shortcut to the failover web console to your desktop on both nodes.

You can enforce a node failover to ensure that the setup is correct. You can then swap the nodes again to revert to the original state of the nodes.

If the configuration fails, remove the current configuration and start the process again, see Remove the existing failover cluster configuration on page **Error! Bookmark not defined.**.

To continue with the setup, see After you configure the failover cluster on page 24.

After you configure the failover cluster

To make sure your VMS system can connect to the running management server seamlessly, you must make some addition configuration steps.

Connection

The remote servers and clients use the management server address to connect to the VMS system. To update the management server address on all components, you must:

- Connect the server VMS components to the system on page 25.
- Connect to the VMS system from the clients on page 26.

Encryption

Depending on the certificate you want to use to encrypt the connection to the failover web console, you must do one of the following actions:

- Install the failover certificate that the wizard generated during the configuration of the failover cluster. See Install the server certificate on a computer on page 26..
- Install your custom certificate. See Use custom server certificates for communication with the failover web console on page 27.

Connect the server VMS components to the system

To connect a server component to the failover cluster, you must register the following server components with the cluster address.

- Recording Server service
- Mobile Server service
- DLNA Server service
- Hirsch Open Network Bridge
- API Gateway

Change the management server address on the recording server

1. On the recording server computer, right-click the server manager tray icon and click **Server Configurator**.
2. In Server Configurator, click **Registering servers**.
3. Specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **Register**.

If the change is successful, a confirmation window appears.

Change the management server address on the mobile server

1. On the mobile server computer, right-click the Mobile Server Manager tray icon and click **Management server address**.
2. Specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **OK**.

   The Mobile Server service restarts and the tray icon turns green.

Change the management server address on the DLNA server

1. On the DLNA Server computer, right-click the Velocity Vision Server Manager tray icon and click **Management server address**.
2. Specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **OK**.

   The Velocity Vision DLNA Server service restarts and the tray icon turns green.

Change the management server address for Hirsch Open Network Bridge

1. On the computer that runs Hirsch Open Network Bridge, right-click the Hirsch ONVIF Bridge tray icon and click **Configuration**.
2. On the **Surveillance Server Credentials** page, in the **Management server** field, specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **OK**.

If the change is successful, a confirmation window appears.

Connect to the VMS system from the clients

Replace the hostname of the management server with the cluster address when logging in from the following clients:

- Velocity Vision Management Client
- Velocity Vision Client
- Velocity Vision Mobile client
- Velocity Vision Web Client.

You replace the hostname on the clients mentioned above to ensure your users always connect to the running management server and your system remains operational when a failure on the management server host occurs.

Install the server certificate on a computer

Install the server certificate on all computers that will access the failover web console.

1. Copy the `serverCert.crt` file from Node 1 to the computer that needs to access the failover web console.
2. Right-click the server certificate and select **Install Certificate**.
3. In the **Certificate Import wizard**, choose the **Store Location**:
   - For Node 1 and Node 2, select **Local Machine**
   - For all other computers, select **Current User**

   Select **Next** to continue.
4. Select **Place all certificates in the following store** and specify a folder.
5. Select **Browse**, and then **Trusted Root Certification Authorities**.
6. Select **OK** and **Next**.
7. On the **Completing the Certificate Import Wizard** dialog, select **Finish**.

   If you receive a security warning that you are about to install a root certificate, select **Yes** to continue.

   If the import has succeeded, a confirmation dialogue box appears.
8. Verify that the server certificate is listed in the center view of the **Trusted Root Certification Authorities** subtree.

Use custom server certificates for communication with the failover web console

When setting up secure communication between the nodes in your cluster, each node will need a certificate that proves its identity. These certificates are created using PKI (Public Key Infrastructure), a system that uses public and private keys to establish trust and security.

Without certificates that are trusted by both nodes, your connection is not secure.

During configuration, the wizard generates a server certificate that encrypts the communication with the failover web console. If you want to encrypt the connection to the failover web console with a custom certificate (your enterprise PKI or commercial PKI), you can do that after you have configured the failover cluster with HTTP.

Requirements

You need the following files:

File	Description
Server certificates	You need a server certificate for each node in the .crt format signed by the root or intermediate CA certificate. Make sure each client certificate contains the following Subject Alternative Name (SAN) details: • The hostnames and FQDNs of both nodes as **DNS** values. • The virtual IP of the failover cluster as an **IP address** value.
Private keys	You need the private unencrypted keys of the server certificates.
Client certificates	Client certificates signed by the same root or intermediate CA that you used to sign the server certificates. You can use client certificates in the .pfx or .p12 format that are issued to a specific Windows user. Make sure the client certificates have the following properties: • The **Key Usage** field is set to **Client Authentication**. • The name of the Windows user in the **Common Name** subfield under the **Subject** field.
A CA certificate	You need the root or intermediate CA certificate for signing the server and client certificates. It must be an X.509 certificate in the .pem format.

Install the CA certificates

You need a CA certificate that signs the server certificates.

1. On Node 1, rename the CA certificate for the servers to `cacert.crt`.
2. Rename the CA certificate for the clients to `clcacert.crt`.
3. Copy the `cacert.crt` certificate file and paste it to `C:\Program Files\Hirsch\Vision Management Server Failover\safekit\conf`.
4. Copy the `clcacert.crt` certificate file and paste it to `C:\Program Files\Hirsch\Vision Management Server Failover\safekit\web\conf`.
5. Repeat steps 1-4 on Node 2.

Install the server certificates

To make sure the failover web console knows which certificate to use, you must copy the certificate and its private key to the configuration folder:

1. On Node 1, rename the server certificate to `server.crt` and the private key file to `server.key`.
2. Copy the certificate and key files and paste them to `C:\Program Files\Hirsch\Vision Management Server Failover\safekit\conf`
3. Repeat step 1 and 2 on Node 2.

Install the client certificates

To connect to the failover console from a computer that is not part of the failover cluster, you need a client certificate.

1. Double-click on the certificate to start the installation wizard.
2. Select to import the certificate in the store of the Current User and click Next.
3. Specify the password for the certificate and click Next.
4. Select Place all certificates in the following store and click Browse. Then, select the Personal store.
5. On the Completing the Certificate Import Wizard dialog, select Finish.
6. Verify that the server certificate is listed in the center view of the Personal subtree.

After you have completed these steps, try logging in to the failover web console.

If you are not able to log in to the console, verify that you have added the necessary exceptions to your Windows Firewall. See Ports used by Vision Management Server Failover services and modules on page 38.

Maintenance

Add a license for Vision Management Server Failover

You receive the Vision Management Server Failover license in your email.

You have the option for when to add the license:

- During the failover cluster configuration, see Configure Vision Management Server Failover (wizard) on page 21.
- After the failover cluster configuration, from the **Manage your configuration** page.

Add a license from the Manage your configuration page

You must add the same license on both nodes.

1. On Node 1, in the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Apply failover license** and select **Continue**.
3. On the **Add a failover license on this computer** page, select **Browse** and select your Vision Management Server Failover license. Select **OK**, then **Continue**. A message informs you that the configuration of the failover management server is successful.
4. Repeat steps 1 to 4 on Node 2.

Download the server certificate to access the failover web console

To establish a secure connection with the failover web console, you need a certificate that your browser trusts. To learn more about the server certificate, see Server certificate for the failover web console on page 13.

You must install the server certificate on every computer that needs access to the failover web console.

If you have a running recording server on Node 1, you must stop the Velocity Vision Recording Server service on that node until you have completed the steps. Then, you must manually start the service. See Start or stop a VMS service on page 19.

You can only download the server certificate from Node 1.

To download the server certificate after you have configured the failover cluster:

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Download server certificate on your computer** and then select **Continue**.
3. On the **Select a destination folder for the server certificate** page, select a destination folder. If you do not select a destination folder, the wizard will export the certificate to `C:\Users\{user}\Documents`.
4. Select **Continue**. The wizard downloads the server certificate to the selected destination.

You can now install the server certificate, see Install the server certificate on a computer on page 26.

Remove the existing failover cluster configuration

Remove your failover cluster configuration when you make changes in your VMS configuration, for example when you change the location of a SQL Server database or the system configuration password.

To remove the failover cluster configuration successfully and make sure the work of the VMS users is restored:

- Use a Windows user that has administrative permissions for Velocity Vision.
- Replace the virtual IP address with the address of the running management server on all clients and remote servers.
- If the Velocity Vision Recording Server or Velocity Vision Failover Recording Server services run on any of the nodes using port 9001, you must stop the service on that node.
- If you use external SQL Server and want to remove your configuration, see Removing the failover cluster configuration when connected to an external SQL Server instance on page 30.

The wizard does not remove the Vision Management Server Failover license, the SQL Server databases, and the server certificate.

To remove the existing failover cluster configuration:

1. On Node 2, in the notification area, right-click the Management Server Manager tray icon.
2. Select **Configure Failover Management Server**.
3. Select **Remove existing configuration** and then **Continue**. The wizard removes the failover management server configuration from the computer.
4. Select **Close** to exit the wizard. Wait for the Management Server service to start.

   (When in a workgroup environment) If the Management Server service does not start automatically, register the management server with the local address from the management server's Server Configurator.

5. Repeat steps 1-4 on Node 1.

Removing the failover cluster configuration when connected to an external SQL Server instance

To avoid any potential issues with your external SQL Server, you must take extra steps when you remove the existing failover configuration:

1. Backup your existing SQL Server.
2. Stop Node 1 and Node 2 from the failover web console. See Start or stop a node on page 35
3. Remove the existing failover cluster configuration from Node 2. See Remove the existing failover cluster configuration on page 30.
4. Stop the VMS services on Node 2 or change the address of SQL Server. See Start or stop a VMS service on page 19.
5. Remove the existing failover cluster configuration from Node 1. See Remove the existing failover cluster configuration on page 30.

Change the password for authentication

To log in to the failover web console, you need to authenticate using a user name and a password.

You cannot change the predefined user name **admin**. During the configuration of the failover cluster, you must set a password for authentication.

To change the password for authentication:

1. On Node 1, in the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Change password for authentication** and then select **Continue**.
3. On the **Change password for authentication** page, specify and confirm a new password. Your password must be between 6 and 32 characters in length. You can use a combination of letters, numbers, and the following characters **( ) * _ - .**
4. Select **Continue** to set a new password.
5. Repeat steps 1-4 on Node 2.

Uninstall Vision Management Server Failover

Before you uninstall Vision Management Server Failover, you must remove the failover management server configuration from both nodes.

1. Open the Windows **Control Panel**. Then double-click **Add or remove programs** and select **Hirsch**.
2. Select **Modify** to launch the Hirsch Velocity Vision VMS wizard.
3. On the **Uninstall or change Hirsch Velocity Vision VMS components** page, select **Change one or more Hirsch Velocity Vision VMS components**. Select **Continue**.
4. Clear the check box for the Vision Management Server Failover component and select **Continue**.
5. When the installation completes, a list shows the components that you have installed on the computer.

The failover web console

Use the failover web console to manage the failover cluster. You can access the failover web console from any computer that can connect to Node 1 and Node 2.

How you open the failover web console depends on the computer:

- On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.
- On all other computers, type the URL of the failover web console in your browser: http://[computername.domainname]:9010 or https://[computername.domainname]:9453.

  [computername.domainname] is the FQDN of either Node 1 or Node 2.

To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.

From the failover web console, you can, for example:

- View the status of the nodes on page 35
- Swap the state of the nodes on page 36
- Start or stop a node on page 35
- Identify the host name of a node on page 36
- Change the behavior of a node after restart on page 37
- See your license information
- View logs entries

User interface details

The failover web console consists of two main tabs:

Control

On the **Control** tab, you can view the following:

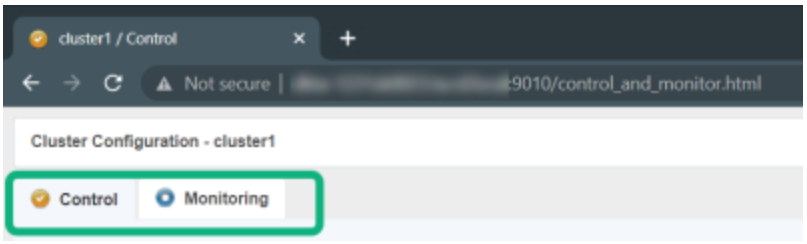
Tab	Description
Resources	View the resources status of the module. Place the mouse cursor over the resource name to get the internal name of the resource.
Module Log	Read the execution log of the module. Set or clear the verbose log's checkbox to display the short log (with only E messages) or the verbose log (all messages including debug ones).
Application Log	Read application output messages of start and stop scripts. These messages are saved on the server side in SAFEVAR/modules/AM/userlog.ulog (where AM is the module name).
Commands Log	Display the commands that have been executed on the node (commands applied on the module and all global commands).
Information	Check the server level and the module configuration.

On the **Module Log**, **Application Log**, and **Commands Log** tabs, click on the refresh button to get the last messages or on the save button to save the log locally.

Monitoring

The **Monitoring** tab presents a simplified view of the current state of the module instances.

You can view and manage the nodes on both tabs from the **Cluster Configuration** panel.



Cluster options

The control panel consists of four columns:

Node actions

Node actions menu ❶ shows the options to change the state of a node:

Option	Description
Start	Start a node.
Stop	Stop a node.
Restart	Restart a node.
Swap	Swap the states of the nodes.
Expert	Stop and start a node, swap without data sync, force start or estimate the data sync.
Admin	Configure boot start, suspend or resume the error detection of module processes, start or stop all checkers, and set failover to on or off.
Support	Save logs, dumps, or snapshots for troubleshooting.

Nodes

Nodes ❷ are the members of the failover cluster. node1 corresponds to the computer you selected as the primary computer, while node2 corresponds to the computer you selected as the secondary computer.

Node states

The node state ❸ column shows the current state of a node:

Tab	Description
PRIM	The data replicates from this node.
SECOND	The data replicates to this node.
ALONE	No data replication. The node acts as a single unit.
STOP	The node stopped, and no redundancy is available.
WAIT	(Transient) The node is starting up (magenta) or waiting for the availability of a resource (red).

Color

A color indicates if the node is available:

Tab	Description
Green	The node is available.
Magenta	The node status is transient.
Red	The node is unavailable.

Data synchronization status

The node data synchronization status ❹ column shows the current data synchronization status of a node. The column is not available when the failover cluster is connected to external SQL Server.

Tab	Description
uptodate	The replicated files are up-to-date.
not uptodate	The replicated files are not up-to-date.
connection error	Cannot connect to the node.
not configured	The configuration is missing from the node.

Open the failover web console

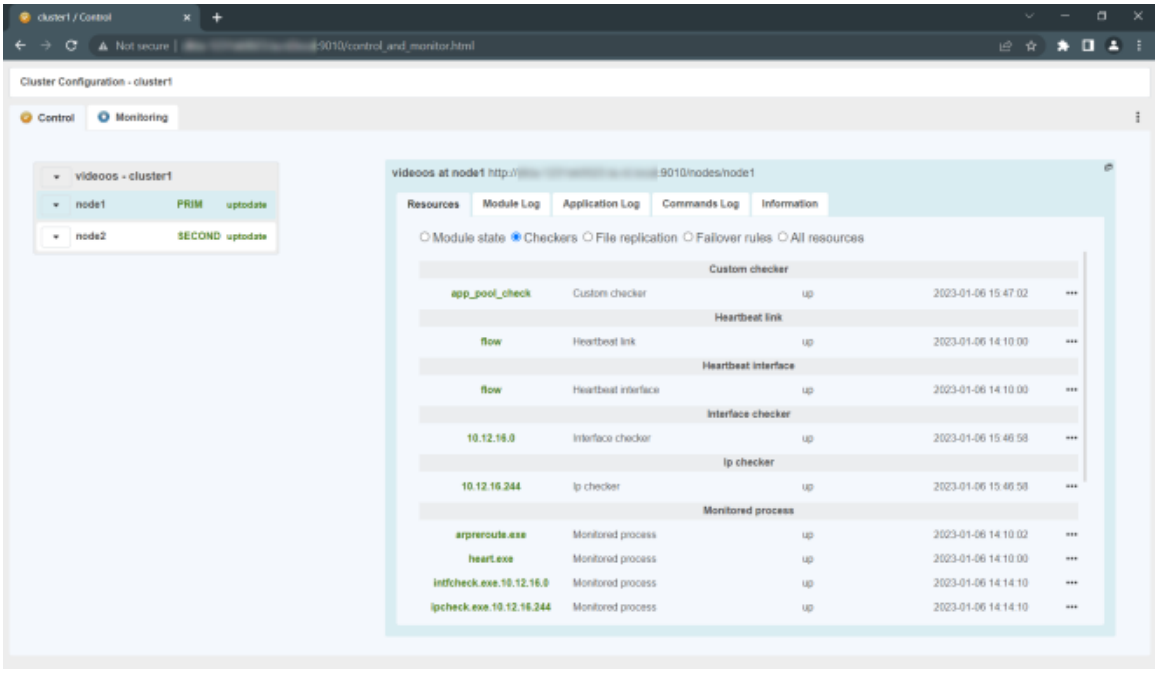
1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: http://[computername.domainname]:9010 or https://[computername.domainname]:9453.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.

The failover web console opens:



View the status of the nodes

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **http://[computername.domainname]:9010** or **https://[computername.domainname]:9453**.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.

3. On the left-hand side of the failover web console, select the **Monitoring** tab to view the current state of the nodes. To learn more about node statuses, see User interface details on page 32.

Start or stop a node

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **http://[computername.domainname]:9010** or **https://[computername.domainname]:9453**.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.

3. On the left-hand side of the failover web console, select the arrow next to a node.

   You can select the arrow next to **videoos-cluster1** to trigger an action on both nodes.

   Select **Start** or **Stop**. The console refreshes with the expected state.

Swap the state of the nodes

By default, after a failback, the failed node is stopped. If you decide to start the node, it comes into SECOND state.

To swap the state of the nodes:

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **http://[computername.domainname]:9010** or **https://[computername.domainname]:9453**.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.

3. Select the arrow next to the node in **PRIM** state and select **Swap**. A window appears. Select **Confirm** to swap the states of the nodes.

   The Management Server, Log Server, Event Server, and the SQL Server services stop, and there is no data replication. Once the roles are swapped, and the services start on the other node. The data replication between the nodes is restored.

Identify the host name of a node

The failover web console represents the primary computer as node1 and the secondary computer as node2. To see the host name that corresponds to a node:

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **http://[computername.domainname]:9010** or **https://[computername.domainname]:9453**.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.
3. Select one of the nodes.
4. Select the **Information** tab.
5. In the **Server information** area, you can see the host name of the computer.

Change the behavior of a node after restart

By default, if a node restarts, it keeps its previous state. You can change that behavior and make a node to always start or stop after restart.

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **http://[computername.domainname]:9010** or **https://[computername.domainname]:9453**.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.
3. Select the arrow next to a node and select **Admin** > **Configure boot start**.
4. From the **Module start at boot time** window, select:
   - **enabled** - the node starts automatically after restart and comes into SECOND state.
   - **disabled** - the node comes into STOP state after restart. You can start the node manually from the failover web console.

To revert to the default behavior and set the node to keep the state from before the restart, you need to remove the existing failover configuration and configure the failover cluster again.

Create snapshots of a module for support

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **http://[computername.domainname]:9010** or **https://[computername.domainname]:9453**.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the Vision Management Server Failover web console on your desktop.

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 31.
3. In **Control** tab, click on the button of the node. It opens a menu with all actions that can be executed on the selected node.

4. Select the Support submenu, then Snapshot command. The web console relies on the web browser download settings for saving the snapshot file on your workstation.
5. Repeat this operation for the other node in the cluster.
6. Send snapshots to support.

The module snapshot action for a node is available in Control and Monitoring tabs.

A snapshot command creates a dump and gathers under SAFEVAR/snapshot/modules/AM the last 3 dumps and last 3 configurations to archive them in a ZIP file.

A dump command creates a directory `dump_<date>_<hour>` on the server side under `SAFEVAR/snapshot/modules/AM. The dump_<date>_<hour>` directory contains the module logs (verbose and not verbose) and information on the system state and processes of the failover cluster at the time of the dump.

Ports used by Vision Management Server Failover services and modules

Vision Management Server Failover services

Service	Default ports	Purpose
safeadmin	Remote access on UDP port 4800 and local access on UDP port 6259	Communicate with other safeadmin instances on other computers. The main and mandatory administration service that is started at boot.
safewebserver	Local and remote TCP access on port 9010 for the HTTP web console or port 9453 for the HTTPS web console	The safewebserver service is a standard Apache web service that is mandatory for running the web console, the distributed comman-line interface, and the <module> checkers.
safecaserv (optional)	Local and remote access on TCP port 9001	The safecaserv service is a web service for securing the web console with the SafeKit PKI.
safeagent (optional)	Local and remote access on UDP port 3600	The safeagent service for SNMP v2.

Failover cluster modules

The ports values of one module are automatically computed depending on its module ID.

Module	Ports	Purpose
heart	port=8888 +(id-1)	UDP port used for sending heartbeats between the servers.
rfs	safenfs_port=5600 +(id-1)x4	TCP port used for replications requests between the servers.

Upgrade

Vision Management Server Failover upgrade

Vision Management Server Failover is part of the VMS, so you do not have to download additional files. To upgrade Vision Management Server Failover, you must upgrade your Velocity Vision VMS. See Upgrade best practices.

Before you upgrade, you must remove the existing failover cluster configuration. See Remove the existing failover cluster configuration on page 30.

After you upgrade your Velocity Vision VMS, Hirsch recommends that you restart the nodes.

If you want to configure the failover cluster afterward, you do not need to add the Vision Management Server Failover license or install the certificates again.

FAQ

Vision Management Server Failover FAQ

What happens if a node restarts unexpectedly?

By default, when a node restarts, it keeps the state from before the restart.

What happens when the three-day demo license expires?

The Management Server service stops every day and you have to start the service manually.

How can I determine if a node has failed?

You can view the states of the nodes from the failover web console or create an event in Velocity Vision Management Client.

Does Velocity Vision supports events from the failover cluster?

Yes, you can configure an event in Velocity Vision Management Client when a failover occurs.

What editions of SQL Server does Vision Management Server Failover support?

Vision Management Server Failover supports all editions of SQL Server.

Do I have to remove my existing VMS configuration before I can configure a failover cluster?

You can configure a failover cluster with an existing VMS configuration. Before you start the configuration, backup the existing SQL Server databases and the Velocity Vision system configuration.

Which Windows users can see the desktop icon for the Vision Management Server Failover web console?

All users of Node 1 and Node 2 can see the desktop icon for the Vision Management Server Failover web console.

I upgraded my VMS and tried to configure the failover cluster, but my configuration failed. What can I do?

Before you start the configuration process again, remove the existing failover cluster configuration, then restart the nodes..

I have configured the failover cluster and I want to change or add a system configuration password. What should I do?

You must remove the failover cluster configuration on both nodes every time you want to:

- Assign a password
- Change a password
- Remove a password

You must use one system configuration password for the VMS installations on both nodes. Once you have applied your password changes, you can configure the failover cluster again.

I have an external SQL Server installation connected to the failover cluster. What should I do to update my SQL Server?

Before you start, you must stop the nodes from the failover web console. Once you have updated your external SQL Server, you can start the nodes.

Troubleshooting

Troubleshooting Vision Management Server Failover

System log file

To troubleshoot system errors, you can find the `ManagementServerFailover.log` file on the computer where you have installed Vision Management Server Failover at `C:\ProgramData\Hirsch\Velocity Vision Management Server\Logs`.

The configuration of the failover cluster has failed
Error: <primary machine fqdn> not in server certificate

If you have multiple network adapters on Node 1 or Node 2, the wizard might not resolve their IP addresses or host names.

Solution: Check the address resolution on the nodes using DNS lookups on page 17. If the IP address or host name of a node does not resolve as expected, disable all network adapters except the one you use for the failover cluster. You can re-enable the network adapters after you configure the failover cluster.

Error: Cannot find any service with service name 'MSSQLServer'. Service MSSQLServer was not found on computer.

The failover cluster configuration fails because the SQL Server instance name does not match the name in the configuration files.

Solution: Check the SQL Server instance names on Node 1 and Node 2. See View the SQL Server instance name on page 17. If the instance name of your SQL Server is not MSSQLServer, you need to update the contents of the configuration files.

Before you make any changes, make a backup of the configuration files.

You can find the configuration files at `C:\Program Files\Hirsch\Vision Management Server Failover\scripts`. You must replace MSSQLServer with the name of your SQL Server instance:

- ConfigureServices.ps1 - you can open the file with a text editor.
- videoos.safe - open the file with a file archiver such as 7zip and go to the bin folder. Edit the start_prim.cmd and stop_prim.cmd files.

Error: StartCertificateServerException occured during RunConfigurationStepsAsync: No connection to certificate authority service.

The system uses port 9001 to connect to the safecaserv service and generate a server certificate. If the port is in use by another service, for example the Recording Server service, the configuration fails.

Solution: Stop all services that use port 9001 on Node 1 and Node 2. Then, configure the failover cluster. The safecaserv service is necessary only during configuration.

Error: PSSecurityException occured during RunConfigurationStepsAsync: File C:\Program Files\Velocity Vision\Vision Management Server Failover\scripts\ConfigureNativeFailoverServices.ps1 cannot be loaded because running scripts is disabled on this system

During the configuration of the failover cluster, the wizard runs PowerShell scripts in the background. Your PowerShell execution policy might block the scripts from running.

Solution: Set your PowerShell execution policy to Unrestricted and configure the failover cluster again. See Execution Policies.

The failover cluster does not function properly

Failover events are not triggered

When you log in to Velocity Vision clients and services as a basic user, your request goes to the Identity Provider. The Identity Provider keeps the certificate keys that were generated during the initial VMS configuration. To ensure the users have access to the resources you have allowed them to, you must remove the certificate keys before you configure the failover cluster.

Solution: Remove the failover cluster configuration, then set up data protection and remove the existing certificate private keys for the Identity Prover, then configure the failover cluster again. See Update the data protection settings for Identity Provider on page 15.

Cannot remove configuration

Error: StartCertificateServerException occured during RunConfigurationStepsAsync: No connection to certificate authority service.

The system uses port 9001 to connect to the safecaserv service to remove the stored server certificate. If the port is in use by another service, for example the Recording Server service, the configuration fails.

Solution: Remove the existing failover cluster configuration, then stop all services that use port 9001 on Node 1 and Node 2. After you have removed the configuration, you can start the services that use port 9001.

The VMS services do not start after removing the configuration

The Management Server and Event Server services will not start (when in a domain environment)

If you have removed the configuration and you have logged in as a standard user in Windows or administrator user that is not added to administrator role in Velocity Vision, the services may fail to register.

Solution: Log in to the computer with an AD user that has administrative permissions in Velocity Vision and remove the configuration.

The Management Server and Event Server services will not start (when in a workgroup environment)

The services fail to register as the configuration still keeps the virtual IP of the failover cluster.

Solution: From the Server Configurator, register the management server and event server with the address of the management server computer.