MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS

Failover clustering guide

milestone

Contents

Overview

High availability of the management server with Windows Server Failover Clustering (WSFC)

WSFC is a feature of the Microsoft Windows Server operating system for fault tolerance and high availability (HA) of applications and services. It enables several computers to host shared services, and if the services fail on one node, the remaining nodes automatically take over the hosting of the services.

You can install the management server a minimum of two nodes within a cluster. One node runs the Management Server and Data Collector Server and exchanges heartbeats with the other cluster nodes. If the active management server and its related services stop running on a node or run very slowly, the VMS services start running on another node in the cluster.

For more information about WSFC, refer to the Microsoft documentation (https://msdn.microsoft.com/en-us/library/hh270278).

Requirements and considerations

Before you configure the management server failover cluster

Make sure your system meets the clustering requirements below.

Network and host prerequisites

To configure the failover cluster, you must prepare a minimum of two hosts with an identical configuration.

As the failover cluster relies on a quorum which generally requires more than half the nodes to be running, consider configuring an odd number of nodes.

Make sure that each of the hosts meets the prerequisites below:

- **Operating system.** Use a Windows Server version that is compatible with your XProtect VMS. See https://www.milestonesys.com/systemrequirements/. Install the same Windows Server version and edition on all hosts that you plan to add to the cluster.
- **Domain**. Make sure that all hosts belong to the same Active Directory domain and can reach each other.
- **Windows account**. Use a single account with administrator permissions to log in to all hosts.
- **Windows server features**. Install the **Failover Clustering** feature on all hosts. See Install the Failover Clustering feature on page 7.

Refer to the Microsoft documentation (https://msdn.microsoft.com/en-us/library/ms189910.aspx) for more detailed information on installation requirements for failover clustering.

XProtect VMS prerequisites

Install identical VMS products under a common user account with administrator permissions. You can use any XProtect VMS variant. To learn more about the general prerequisites for installing XProtect VMS, see the XProtect VMS administrator manual.

On all hosts, install the following system components:

- XProtect Management Server
- XProtect API Gateway
- (Optional) XProtect Log Server

To make sure that the Management Server and Log Server components on all cluster nodes connect to one SQL Server database, during your XProtect VMS installation, you must select the following options:

- When you install the XProtect VMS on the first host, select **Let the installer create or recreate a database** for the Management Server and Log Server services.
- On the second, and all additional hosts that you want to add to the failover cluster, use the database you created on the first host. On the **Select Database** page in the XProtect installation wizard select to use an existing database and point to that database and select to keep the existing data.

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

Microsoft SQL Server prerequisites

You can use a SQL Server instance that is hosted elsewhere in your network.

Prerequisite	Description
Connection	Verify that the VMS installations on all hosts can connect to the external SQL Server instance.

Encryption considerations

To encrypt the connection to and from the failover cluster, you must install the CA certificate and SSL certificates on all cluster nodes. The certificates must contain the hostname IP address of the node and the cluster name.

Use a certificate for an external IDP in a cluster environment

When you install XProtect in a single-server environment, the Identity Provider configuration data is protected using the 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.

Before you start, you must complete the following configuration:

- Import your server certificate to the **Personal** store for the user running the Management Server service.
- Give the server certificate **Read** permissions.
- Ensure that the root certificate that you used to create the server certificate is imported to the **User certificates' Trusted Root Certification Authorities** store.
- If you use a self-signed certificate, you must add it to the **Trusted Root Certificates Authorities** store on your local computer.

To set up data protection for the certificate that runs the VMS services on the nodes, go to a node and complete the following steps:

1. Retrieve the thumbprint of the certificate that the IDP application pools and the Management Server service use. See How to: Retrieve the Thumbprint of a Certificate.
2. Locate the `appsettings.json` file in the installation path of the Identity Provider (`[Install path]\Milestone\XProtectManagement Server\IIS\IDP`).
3. In the **DataProtectionSettings** section, set the thumbprint of the certificate that the IDP application pools and the Management Server service use.

```
"DataProtectionSettings": {
 "ProtectKeysWithCertificate": {
  "Thumbprint": "[thumbprint]"
 }
},
```

4. Repeat step 2 on the remaining management server nodes.
5. Trigger a node failover to ensure that the certificate setup is correct.
6. Log in again to XProtect Management Client and apply the external provider configuration. If the configuration has already been applied, you must re-enter the client secret from the external IDP in XProtect Management Client.

If you encounter any issues, check the Identity Provider log file for more information. The system stores the file at `C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`.

Encrypting the connection to the failover cluster

To connect securely to the running management server, the remote servers must trust all nodes.

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

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

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

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 the hosts where you have installed a VMS client component.
3. Create an SSL certificate for the failover cluster that includes the node name and the address of the cluster.
4. Install the SSL certificate for the failover cluster on the nodes.

5. Enable encryption for the Management Server service on the nodes.
6. Create and install certificates on the hosts where you installed a VMS server component.
7. Enable encryption on the hosts where you installed a VMS server component.

Install the Failover Clustering feature

To add your hosts to the failover cluster, you must install the Failover Clustering feature on all host.

1. Log in to the Windows Server as Administrator and open **Server Manager**.
2. Click Manage and select **Add roles and features**.
3. Follow the steps in the wizard to install the **Failover Clustering** feature.

After you have prepared the operating system on all nodes, you are ready to create the failover cluster.

Deployment

Configuring high availability of the management server

To make sure that the management server can start running on another node when the active node fails, you must configure a failover cluster and update your VMS configuration.

1. Create the failover cluster on page 8.
2. Create a cluster role for the VMS services on page 9.
3. Register the management server on the cluster nodes on page 11.
4. Configure the Data Collector Server service to run in a cluster environment on page 10.
5. Connect the server VMS components to the system on page 12.
6. Connect to the VMS system from the clients on page 13.
7. Verify that the failover cluster is working on page 13.

Create the failover cluster

You can create the cluster from the **Failover Cluster Manager**. The wizard validates your configuration and creates the cluster from your selected hosts.

You can create the failover cluster from any Windows Server host in your domain that has the following Windows Server features installed:

- **Failover Cluster Management Tools**
- **Failover Cluster Module for Windows PowerShell**

You can install these features from the Server Manager's **Add Roles and Features** wizard under **Features** > **Remote Server Administration Tools** > **Failover Clustering Tools**.

To create the cluster:

1. On a host in your domain, open **Failover Cluster Manager** from the Windows Start menu and select **Create Cluster...**
2. In the **Select Servers** window, click **Browse** and add the names of the nodes in the cluster.
3. In the **Validation Warning** window, select **Yes** to run all validation tests before configuration.
4. On the **Summary** page, you see a report of the tests. Review and fix all warnings on the hosts to continue with the cluster configuration. If the test validation is successful, select **Finish** to return to the cluster configuration.
5. In the **Access Point for Administering the Cluster** window, specify a name for your cluster.

6. In the **Confirmation** window, review your selections and ensure that the **Add all eligible storage to the cluster** option is selected.

   The wizard creates the failover cluster. Once the configuration is complete, the wizard displays the **Summary** window.

7. In **Failover Cluster Manager**, go to your cluster and select **Nodes** to make sure that all nodes are up and running.

You can now create a role for the VMS services.

Create a cluster role for the VMS services

To make sure the node monitors the management server and its related services, you must create a role for the VMS services and add them as generic services.

Create a role and add the Management Server service to that role

A cluster role represents an application, service, or workload that the cluster manages to ensure high availability. It allows the cluster to detect failures and move the workload between nodes as needed. To create a role:

1. On a node in the failover cluster, go to **Failover Cluster Management**. In the **Failover Cluster Management** window, expand your cluster, right-click **Roles**, and click **Configure Role...**
2. In the **Select Role** window, select **Generic Service**.
3. In the **Select Service** window, select the **Milestone XProtect Management Server** service.
4. In the **Client Access Point** window, specify a name that will serve as the management server hostname. Clients will use this name to access the management server.

   The hostname must be different from the name of the cluster.

5. In the **Select Storage** window, you do not need to make any changes, as the service does not require any storage.
6. In the **Replicate Registry Settings** window, you do not need to make any changes, as no registry settings will be replicated.
7. In the **Confirmation** window, verify that the cluster service can be configured according to your requirements.

   The wizard configures the high availability for the selected role.

8. In the **Summary page** window, you can review the configuration.

   On the **Roles** page, the role status changes from **Pending** to **Running**. You can see the node that runs the Management Server service in the **Owner node** column.

Add related services to the role

To ensure the Management Server service runs smoothly in the cluster:

1. On the **Roles** page, right-click the role you just created and click **Add resource** > **Generic Service**. Select the **Milestone XProtect Data Collector Server** service.
2. (Optional) Repeat Step 1 to add the **Milestone XProtect Log Server** service.

All added services are displayed in the bottom pane of the **Role** window on the **Resources** tab. Verify that all the services are running on the owner node.

If a service is not running, you can start it from the **Failover Cluster Manager** by selecting the service and then clicking **Bring Service** from the panel on the right.

Verify that the information from the **Failover Cluster Manager** matches the actual status of the services by checking the services status on the owner node.

Configure the Data Collector Server service to run in a cluster environment

The Data Collector Server is an XProtect service that collects and manages the performance statistics for devices and services.

To make the management server on all nodes behave as one system, you must update the Data Collector Server configuration files on all cluster nodes.

Step 1: Obtain the cluster ID

To make sure that all nodes share the same cluster ID, you must obtain the ID from the system:

1. On a cluster node, open Windows PowerShell as administrator and type the following command:

   ```
   Get-Cluster -Name '[name]' | format-list -Property *
   ```

   where [name] is the name of the role you have defined for the cluster.
2. Copy the value for the **Id** property.

Step 2: Update the configuration file

You must update all Data Collector Server configuration files on all cluster nodes with the cluster ID.

Before you make any changes to the configuration on a node, stop the XProtect Data Collector Server service on that node.

1. On a node, go to `C:\Program Files\Milestone\XProtect Data Collector Server\` and open the `appsettings.json` file in a text editor as an administrator.
2. Update the lines with your cluster details:
   - `CLUSTER ADDRESS` contains the full address of the cluster in the format *[protocol]://[role name].[domain name],* for example, *https://ms-cluster.company.com*
   - `[CLUSTER ID]` contains the alpha-numeric value of the cluster ID that you obtained.

   Using the cluster address and ID, update the fields in the .json files as follows:

   ```
   "ClusterSettings": {
   "ClusterAddress": "[CLUSTER ADDRESS]",
   "ClusterApplicationId": "[CLUSTER ID]"
   },
   ```
3. Restart the role from **Failover Cluster Manager**.
4. Repeat steps 1-3 on all nodes.
5. Verify that the Data Collector Server service is running only on the owner node.

All the data you receive from and send to the remote servers will go to the running management server.

Register the management server on the cluster nodes

To ensure your clients can always connect to the running management server, on all cluster nodes and clients, you must replace the hostname of the management server with the role name followed by the domain name.

> To avoid conflicts between the failover cluster and VMS Server Configurator, pause the cluster before you start tasks in the Server Configurator. The Server Configurator may need to stop services while applying changes, and the failover cluster environment may interfere with this operation.

On the cluster nodes:

1. Right-click on the management server tray icon and select Server Configurator.
2. Go to the **Registration** page and click the pencil ( ) symbol to make the management server address editable.
3. Change the management server address to the cluster address by replacing the management server address with the role name followed by the domain name, for example, `https://role.company.com`.
4. Click **Register**.

   The wizard updates your VMS configuration and starts the Management Server, Data Collector Server,

and Log Server services on that node.

5. To verify that the failover works as expected, restart the node owner.

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
- Milestone 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 XProtect DLNA 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 XProtect DLNA Server service restarts and the tray icon turns green.

Change the management server address for Milestone Open Network Bridge

1. On the computer that runs Milestone Open Network Bridge, right-click the Milestone 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:

- XProtect Management Client
- XProtect Smart Client
- XProtect Mobile client
- XProtect 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.

Verify that the failover cluster is working

Before deploying your failover cluster to production, you can validate your configuration with some simple steps.

Check the service startup type

Verify that the **Failover Cluster Manager** can control the VMS services by checking the service startup type.

1. On a node that belongs to the failover cluster, go to Windows **Services**.
2. Verify that the startup type for the Management Server, Data Collector Server, and Log Server services is set to **Manual**.
3. Repeat the same steps on the remaining failover cluster nodes.

Check service status

Make sure that the **Failover Cluster Manager** shows the actual status of the nodes.

1. In **Failover Cluster Manager**, expand your node and go to roles. Then, click your node.
2. In the Resource tab, check the status of the Management Server, Data Collector Server, and Log Server services.

3. Go to the owner node, open **Services**, and compare the service status of the three VMS services.

If the statuses do not match, start and stop the role. Then, repeat the steps above.

Trigger a failover

After ensuring that the configuration is set up correctly, you can trigger a failover manually.

1. Restart the node that runs the VMS services.
2. From the **Failover Cluster Manager**, see which node has become the new owner node.
3. Go to the new owner node and verify that the Management Server, Data Collector Server, and Log Server services are running on that node.
4. Go to the other node members and verify that the services are stopped.

Log in

Try logging in to XProtect Management Client or XProtect Smart Client using the cluster address.

If the configuration is working properly, you should be able to connect seamlessly to the running management server using the cluster address.

Copyright, trademarks, and disclaimer

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file `3rd_party_software_terms_and_conditions.txt` located in your Milestone system installation folder.

helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.