CathexisVision Failover Implementation Best Practice Guidelines

Contents

1 Introduction

a. Software

- CathexisVision 2017.1 and above is required for failover.
- Failover only supported for CathexisVision Professional and Premium software packages.

b. Setup Notes

Software Installation

The same software package for a server installation is required for failover. On installation of the server software, select the **Failover Server** option. Refer to CathexisVision setup manual for more detail.

Time Synchronisation

It is imperative to synchronise the operating system times of the failover server with the other servers at the site before installing the failover server software package.

2 Failover Features

a. Failover Roles

The Failover server can take on the following roles:

- User management.
- Site control.
- Licensing.
- Recording for reachable IP cameras.
- Live Viewing for Client PCs.
- Video-wall control.

b. Additional Failover Features

- Statistics can be attained from the Failover server during the failover process
- Client GUI indicators show failover is taking place.
- System indicators show when data is re-inserted back into the main database.
- Technical alarms can be generated (Email, Call Base Station/s) when failover takes place.

3 Licensing

a. CathexisVision Software Packages

Profession Package Sites

In CathexisVision 2018 Professional sites, purchase of a failover base license (CFOR-2001) and the Failover Cameras licenses (CFOR-1001) are required.

Premium Package Sites

From CathexisVision 2018 onwards, a failover base license is included in the purchase of a Premium site. Purchase of failover camera licenses (CFOR-1001) is still required.

b. Failover Camera Licenses

With the 2018 change to overall site licensing (instead of the previous server-by-server licensing model), for failover on the site, all site cameras must have failover camera licenses applied.

A failover camera license (CFOR-1001) is required for every camera on the Professional and Premium sites. These licenses need to be purchased in addition to the Professional and Premium software license.

For example, a site failover license is purchased. If a site has 100 cameras, then 100 failover licenses must be purchased, and a license applied to each camera.

Critical: If number of failover camera licenses does not match number of site cameras, failover will be impaired.

4 Best Practice Implementation

This section provides a best practice guideline to implementing failover.

a. Network Switches

Good quality networks and network switches are imperative to minimise the failover time as well as the time to re-insert the server database and bring the cameras back online. The software cannot compensate for a poor-quality network.

b. CathexisVision Performance Settings

The CathexisVision Performance utility must be run to optimise disk throughput and performance.

Specifically, the following options **must be disabled** to ensure optimal writing performance:

- **Last access timestamp for NTFS partitions,**
- **Search indexing** in Windows based servers.

c. Failover Time

A global time period can be configured (minimum 5 seconds) before the failover server deems a server as failed/down.

The failover server creates an 18 to 30 second gap in recording during failover (assuming 5 seconds to failover is used), and another 18 to 30 second gap when the failed server comes back online.

Failover Time Exceeded

If the times above are exceeded (i.e., in which a server is deemed to be failed and failover starts, and a server restarts and failover stops), the problem may arise from a network hardware configuration issue.

d. Failover Storage

The failover database is configured during the CathexisVision failover setup.

A dedicated storage network for external storage (NAS, etc) is recommended with a sufficient size failover database for the expected down-time in restoring the failed server.

External Storage Write Speed

If the writing speed of the assigned NAS storage to the failover is very low, it is suggested that a local disk of the failover server be assigned to be the failover database, as a local HDD on the failover won't share the writing speed or the storage throughput with any other server. This will enhance the failover recording time dramatically and exclude any network issues.

The size of this local database must be configured to allow recordings for the anticipated downtime in replacing a failed server.

e. Database Recreation

When reinitialising the failover server, it is advisable to re-create the failover database rather than import the old database.

This is because the NVR connects to the failover server to request any new data (i.e. any data recorded for an NVR that the failover server hasn't delivered yet), and if database import is used, the reinitialised (blank) failover server does not receive feedback that the NVR may have already received some (or all) of this data, and it will start uploading all of its data from the beginning. This leads to data duplication problems. Recreating the failover database solves this problem.

f. Database Reinsertion

Priority is placed on the new recordings taking place. The failover database insertions wait until the current database writes have been completed, or when the database system is less busy.

Prevent Database Errors

To prevent errors on the databases on the site and recordings being dropped, check that the sink rate of the iSCSI storage system is sufficient for the expect system data transfer rate.

If the time between the failover server and the failed-over server is not synchronised, then the re-insertion will be based on the failover server time.

g. Restore Point Creation Optimisation

Do not create any large folders (e.g. video, virtual feeds) on the server in the in the **c:\program files\CathexisVision Server\Settings** folder.

This whole folder forms part of the servers' restore points. The failover server during failover needs to extract the failed servers' restore points (stored on the failover server) and the deployment of this restore point file could create a failover delay.

h. Replacing a Server on a Failover Site

For the site master replacement, a restore point needs to be run on the new server which will initialise the system operation on the replaced master server. The failover server will stop failing over the old site master and start monitoring the new server.

For a site slave server replacement, the process is to run the restore point on the new server and then do a 'replace server' operation which inserts the new server into the site as the old server. The new slave server will run and the failover server will relinquish control and dump the recordings from the failover server onto the new server.

i. Changing the IP Address of a Failover Server

The failover server configuration settings that reside on the failover server can only be modified when the failover server is removed in the site failover setup. When settings have been configured accordingly (including changing the IP address of the failover server), the server can then be added back.

j. Client Connection

To enable the client connection during failover, the following CathexisVision setting needs to be configured on the client machine:

File → Enterprise Manager → In connection panel, right-click IP address → Properties → Tick **Use Site Discovery for Connectio**n.

5 Failover Limitations

The following limitations must be taken into consideration when implementing a Failover solution.

a. Master Server

The IP address of the master server will not be retained by the failover server and if there any external site connections directly to this master server they will not be able to connect. An alternative IP address, that of the failover server, will need to be an option for an external connection. This is because duplicate IP addresses cannot exist on the same site, so the Failover server (now the Master) has a different address. If connecting externally into the site, the old Master server IP address is not valid in Failover mode. The Failover (now Master) server IP address will need to be connected.

b. 3rd Party Integrated Devices

3rd party Integrated devices connected directly to the failed server via USB or RS232/485 cannot be failed-over. This includes the USB license dongle required for the ARH ANPR engine. Integrations that have an IP connection (separate from the failed server) will be failed-over, and triggers and events will continue to function. However, metadatabase updates are excluded.

c. Server Clustering

A failover server cannot be assigned to only monitor specified servers or server groups for failover. Any server connected (LAN/WAN) on the same site will be monitored for failover.

Note: For this reason, it is crucial that all site cameras have failover licenses applied.

d. Alarm Gateway

The networks (camera network, storage network) on which failover will take place cannot be specified. In the event that a recording and failover server reside on both a camera and storage network, if the camera network goes down, it will not failover the server as the failover server can still reach the recording server over the storage network.

Another side effect of broadcasting over two networks is that when the failover server fails-over the master server, with both networks intact, the failover server can take on the IP address of the storage network adapter, and this in turn is passed to the video wall units. The video wall units cannot reach the server via the provided storage network address, and this prevents the videowall units from streaming cameras.

6 Conclusion

Please remember that this document was designed to deal specifically with this aspect of the software. For further information about the CathexisVision software please consult the main manual (http://cathexisvideo.com/).

For support please contact support@cat.co.za