Archiving Management

Concepts Overview

This article gives you an overview of the different archiving services and options available in Omnicast. It is an excellent starting point for understanding Archiving Management.

Archiving Services

There are three different types of archiving services (or *archivers*) in Omnicast. The common characteristics of all archivers is that they are all individually responsible for the video archives they manage. The video archives are digitally recorded according to one of the three video compression standards: MPEG-4, MPEG-2 or MJPEG. Each archiving service maintains its own catalog of video archives which enables it to quickly return the desired video sequences when a user issues a query from the Archive Player.

Archiver

The **Archiver** (with a capital “A”) is the main archiving service in Omnicast. This is the only service capable of communicating with the video units. The Archiver sends command and control messages to the units via specific discovery and command ports. Typical commands sent by the Archiver to the units are:

- discovery commands (finding the active units)
- start/stop streaming video
- video stream redirection commands
- video streaming settings (data format, video attributes, etc.)

The Archiver is also responsible to save the live video streams on disks and to create off-line safety copies of the video archive (see Backup). For added security, all commands sent to the units can be encrypted to prevent hacking and the video data can be watermarked to prevent tampering (see Encryption).

There can be as many Archivers as needed on the same system to share the archiving load. The number of encoders that a single Archiver can handle depends on the machine and the desired video quality. The maximum number of Archivers permitted on a system is controlled by the Directory option **Number of Archivers** of your Omnicast license.

See *Config Tool – Archiver* on page 204 to learn more.

Restore Archiver

The **Restore Archiver** is a special type of archiving service used only to restore off-line copies of video archives to full search and playback capabilities for the Archive Player. To use this service, the Directory option **Number of Restore Archivers** must be greater than zero in your Omnicast license.

See *Config Tool – Restore Archiver* on page 390 to learn more.

Auxiliary Archiver

The **Auxiliary Archiver** is a supplemental archiving service. Unlike the Archiver, the Auxiliary Archiver is not bound to any particular discovery port. Therefore, it is free to archive any camera in the system, including the ones that are federated. In addition, the Auxiliary Archiver offers the choice to archive different video streams on different schedules than those followed by the regular Archiver.

The Auxiliary Archiver cannot operate on its own. It relies on the Archiver to communicate with the video units. The Auxiliary Archiver has two distinct purposes:

- to create off-site (outside the LAN) copies of the video archive for selected cameras;
- to create a different version (different quality and different time) of the video archive for specific usage;

To use this service, the Directory option **Number of Auxiliary Archivers** must be greater than zero in your Omnicast license.

See *Config Tool* – *Auxiliary Archiver* on page 223 to learn more.

Archiving Options

Backup

Video archives created by both Archivers and Auxiliary Archivers can be protected through backups. No particular license option is necessary to enable this feature. However, you need to enable Restore Archivers in order to make use of the backups. See *Backup and Restore* on page 20.

Encryption

Encryption occurs at two different levels:

1. Commands sent by Archivers to units can be encrypted using SSL (Secure Sockets Layer) protocol to protect against hackers. The **SSL on Archiver** option needs to be turned on in your Omnicast license in order to use this feature.
2. Archived video data can be watermarked to protect against tampering. This feature is both supported by the Archivers and the Auxiliary Archivers. See *Archiver Security* on page 16.

Standby Archiver

Archivers can be configured to be each other's failover if the Directory option **Standby Archivers** is enabled in your Omnicast license. See *Archiver Availability* on page 17.

Redundant archiving

To protect against accidental data loss, the standby Archivers can be given an optional role of **redundant Archivers** when they are not assuming the primary role of command and control. See *Archiver Availability* on page 17.

Archive Storage Management

Regardless of the types of archiving services you use, they all have the same storage requirements for the same amount of video archives. This article teaches you how to evaluate your archive storage requirements and directs you to the proper section in this user guide for storage configuration and monitoring.

Storage evaluation

The amount of storage space required for archiving video is influenced by the following factors:

1 **The number of cameras that need archiving**

Archiving is enabled on a camera only if the camera is part of an archiving schedule.

To learn how to create an archiving schedule, see *Archiving Schedule* on page 220.

To learn how to enroll a camera on an archiving schedule, see *Camera – Recording* on page 248.

2 **The number of days you need to keep the archive online**

The Archiver uses two methods to free up storage space for new video archives. The first method is to delete the oldest video files when running out of disk space. This is the simplest method if video archives from all cameras are equally important and if you wish to keep as much video as possible (this method maximizes disk usage).

The second method is to specify for each camera the number of days the archives need to be kept online. When the archives become obsolete, they will automatically be deleted, even if the disk space is not running out. This method allows you to keep important video archives longer.

To learn how to set the archive retention period on each camera, see *Config Tool – Archiver – Archiving* on page 205.

The Archiver can also be instructed not to delete any video archive before it is due. In this case, if the Archiver ever runs out of disk space, the archiving will stop.

To learn how to configure this option, see *Server Admin – Archiver –* General archiving options on page 90.

3 **The percentage of recording time**

The percentage of recording time for a given camera depends on the selected archiving mode. You can configure a camera so archiving is (1) disabled, (2) only performed on user requests, (3) performed automatically whenever the motion level is above a certain threshold, or (4) performed continuously. All these modes could be applied to any period of the day and any day of the week.

It is possible to enroll a camera on more than one archiving schedule. To learn how the system sorts out the priorities between conflicting schedules, see *Config Tool – Schedule Priorities and Conflict Resolution* on page 331.

To learn how to configure the motion detection threshold, see *Camera – Motion detection configuration* on page 252.

4 **The selected frame rate**

The higher the frame rate, the more storage space the recording will require. To learn how to configure the recording frame rate, see *Camera – Video Quality* on page 238.

5 **The selected image resolution**

The higher the image resolution, the more storage space the recording will require. The image resolution is determined by the video data format in effect. For a description of the available video data format, see *Camera – Video image resolution* on page 272.

6 **The expected percentage of movement**

MPEG-4 encoding scheme compresses data by storing only the changes in the image between consecutive frames instead of the whole image for every single frame. Therefore, a video containing a lot of movement would require a lot more storage than a still image video. To simplify the movement estimation, we have defined two categories of cameras: the fixed cameras (or cameras with less than 30% of movement) and the PTZ cameras (or cameras with more than 30% of movement).

Archiving Configuration

To store video archives, the archiving service needs a database to store the archives catalog and disk space to store the video files. These configurations are done on the local machine where the archiving service is installed. See *Server Admin – Archiver –* Archiving on page 87.

To learn how to configure the archiving storage space for the Auxiliary Archiver, see *Server Admin – Auxiliary Archiver –* Archiving on page 135.

Storage Usage Monitoring

An estimate, no matter how good it is, remains an estimate. Once the system is in operation, it is always recommended to verify regularly the actual storage consumption of the system.

The Config Tool provides insightful statistics on the actual disk usage for each of the Archivers. The available statistics are:

- The remaining available space on each disk selected for archiving.
- The average disk usage per day for all cameras controlled by the Archiver.
- The average disk usage per day for one camera.
- The estimated remaining recording time left.
- The current online archives span.

To view a sample statistics page for the Archiver, please turn to *Config Tool – Archiver – Statistics* on page 206.

To learn about how much space each restored backup set is using, please turn to *Config Tool – Restore Archiver – Backup Sets* on page 390.

Archiver Security

This section talks about protecting your video archives against tampering and your system against malicious attacks.

Access to the system

The first step to system security is always to prevent illegal access, either physically or through software. Make sure that all privileged accounts are duly protected with passwords and that computer rooms where the Omnicast equipment are installed are not easily accessible to everyone.

Beyond these simple security measures, Omnicast also offer some extra protection against data tampering and hacking.

Protection against hacking

Protection against hacking is achieved by using the SSL (Secure Socket Layer) protocol. All commands sent by the Archiver to the units (PTZ controls, redirection of video streams, etc.) can be encrypted to prevent hackers from remotely taking control of a camera. See *Server Admin – Verint Extension –* SSL settings on page 129.

Each group of units, characterized by one VSIP port, can be protected with a different SSL password.

Protection against data tampering

Protection against tampering is achieved through watermarking. It is the process by which a digital watermark (a digital signature) is added to each recorded video frame to ensure its authenticity. If anyone later tries to make changes to a recorded video sequence by adding, deleting or modifying a video image, the signature will no longer match, thus, showing that the video has been tampered with.

To learn how to setup the Archiver to prevent tampering, see *Server Admin – Archiver –* Security on page 93.

To learn how to validate the authenticity of video files, see *Validate file* in *Omnicast Archive Player User Guide*.

Protection against sabotage and accidents

Other aspects of security management deal with the destruction of the system hardware and data, either by accident or by acts of terrorism. To learn what Omnicast could offer to reduce the vulnerability of the system against such mishaps, see *Archiver Availability* on page 17.

Archiver Availability

This section discusses the different options you have to ensure maximum availability of your surveillance video, either live or archived, in the event of a hardware failure or media loss.

System availability issues

When it comes to the availability of the system, there are three aspects to consider:

1. Protection against service interruptions
2. Protection against data loss
3. Monitoring Archiver events

Protection against service interruptions

The archiving services (Archiver, Auxiliary Archiver and Restore Archiver) must all be running if the users are to be able to access the full range of video archives. And most importantly, the Directory service must be running at all times or nothing will work.

Directory Failover Coordinator

The first step in securing the availability of the system is to ensure the availability of the Directory service. Omnicast offers a safety mechanism by which multiple machines located anywhere on the WAN can be setup to take over the responsibility of the Directory service should the main Directory machine fail. When the main Directory machine is restored, the service will automatically switch back without losing any configuration data. See Directory Failover Configuration on page 170.

Standby Archiver

The Archiver services can also be protected by a failover mechanism. Each Archiver service in the system can be configured to oversee multiple groups of units. Each unit in the system can be configured to have a list of Archivers that it can report to. At any one time, only one Archiver is in charge of any unit. When the primary Archiver fails, the units that are under its care can be automatically handled by the remaining working Archivers, thus ensuring a continuity of service.

Let us consider an example to illustrate how this works. Suppose we have three Archivers and twelve units configured as follow.

Unit	Primary Archiver	Secondary Archiver	Tertiary Archiver
Unit-A1	Archiver-A	Archiver-B	Archiver-C
Unit-A2	Archiver-A	Archiver-B	Archiver-C
Unit-A3	Archiver-A	Archiver-C	Archiver-B
Unit-A4	Archiver-A	Archiver-C	Archiver-B
Unit-B1	Archiver-B	Archiver-A	Archiver-C
Unit-B2	Archiver-B	Archiver-A	Archiver-C
Unit-B3	Archiver-B	Archiver-C	Archiver-A
Unit-B4	Archiver-B	Archiver-C	Archiver-A
Unit-C1	Archiver-C	Archiver-A	Archiver-B
Unit-C2	Archiver-C	Archiver-A	Archiver-B
Unit-C3	Archiver-C	Archiver-B	Archiver-A
Unit-C4	Archiver-C	Archiver-B	Archiver-A

When everything is working fine, each Archiver takes care of four units (see Primary Archiver).

If Archiver-A fails, then the four units under the care of Archiver-A will have to fall back on their secondary Archiver. Units A1 and A2 will be taken care by Archiver-B, while units A3 and A4 will be taken care by Archiver-C (see Secondary Archiver).

If Archiver-B also fails, then the entire load will be assumed by Archiver-C. The same thing is true if Archiver-C fails instead of Archiver-B.

When Archiver-A is restored to service, it will automatically pick up its units and free the load from the other two Archivers.

From this simple example, you can see that the more Archivers you have in the system, the more evenly you can distribute the load when one of them fails so the performance impact felt will be minimal.

To learn how to configure Archivers to handle more than one group of units, see *Server Admin* – Archiver Extensions on page 97.

To learn how to configure a unit so it accepts more than one Archiver, see *Config Tool – Unit – Standby Archivers* on page 416.

Protection against data loss

The failover mechanisms for the Directory and the Archivers can effectively protect against service interruptions, but not necessarily against loss of data. In the previous scenario, if the archiving disks of Archiver-A are damaged, the command and control of the units under Archiver-A would be taken care by the other two Archivers and users would be able to continue to view live videos from them. But the video archives managed by Archiver-A will be lost. Moreover, even if the disks of Archiver-A are not damaged, users would not be able to access the video archives on them if Archiver-A is not running.

Redundant archiving

The solution to the threat of data loss and to the unavailability of the video archives while the Archiver service is down is to create redundant archives.

Redundant archiving can be configured individually for each camera. To enable this feature, go to the **Recording** tab of the camera and select ☑ **Redundant archiving**.

NOTE Once redundant archiving is enabled for a given camera, all standby Archivers for that camera's unit will start archiving. All redundant Archivers follow the same archiving schedules as specified in the **Recording** tab of the camera. See *Camera – Recording* on page 248.

Let us revisit the previous example with twelve units shared between three Archivers. If redundant archiving is turned on for each of the cameras, we will get three copies of video archives for each camera.

Suppose we want to keep all three standby Archivers but only need two copies of video archives. This can be achieved by adopting the following configuration.

Unit	Primary Archiver	Secondary Archiver	Tertiary Archiver
Unit-A1	Archiver-A	Archiver-B	Archiver-C (no archiving)
Unit-A2	Archiver-A	Archiver-B	Archiver-C (no archiving)
Unit-A3	Archiver-A	Archiver-B	Archiver-C (no archiving)
Unit-A4	Archiver-A	Archiver-B	Archiver-C (no archiving)
Unit-B1	Archiver-A	Archiver-B	Archiver-C (no archiving)
Unit-B2	Archiver-A	Archiver-B	Archiver-C (no archiving)
Unit-B3	Archiver-B	Archiver-A	Archiver-C (no archiving)
Unit-B4	Archiver-B	Archiver-A	Archiver-C (no archiving)
Unit-C1	Archiver-B	Archiver-A	Archiver-C (no archiving)
Unit-C2	Archiver-B	Archiver-A	Archiver-C (no archiving)
Unit-C3	Archiver-B	Archiver-A	Archiver-C (no archiving)
Unit-C4	Archiver-B	Archiver-A	Archiver-C (no archiving)

In the above scenario, only Archive-A and Archiver-B are used to create archives. Archiver-C has its archiving option turned off (see *Server Admin – Archiver –* Archiving on page 87).

Archiver-C will become active only if both Archiver-A and Archiver-B have failed. In this case, the users can still view live videos but there will be no archiving.

Auxiliary Archiver

It is sometimes desirable to have a copy of the video archives kept at a remote location (not connected to the same LAN as the core of the system) for safety reasons. In this case, the Auxiliary Archiver should be considered. The Auxiliary Archiver is a better alternative than creating backups because the redundant archives are readily available without the necessity to restore (see *Backup and Restore* on page 20), but it offers no protection against service failures, because it cannot assume the command and control functions of the Archiver.

Monitoring Archiver events

There are many ways to monitor the Archiver events in the system.

1. By defining user notification actions when important Archiver events arise (disk load is over 80%, disks full, application lost, etc.). To learn how to set up the Archiver for automatic notification, see *Config Tool – Archiver – Actions* on page 212.
2. By viewing the **User Tracking Reports** with the Report Viewer, if **Database reporting** is supported by your license. See *Report Viewer* on page 490.
3. By searching the event database for Archiver events with the Config Tool. See *Config Tool – Archiver – Event Search* on page 219.
4. By examining the log files generated by the Archivers. To learn how to configure the Archiver for event logging, please read *Server Admin – Archiver –* Logging on page 95. The Archiver logs are not as easy to use as the Archiver's **Event search** tab in the Config Tool, but it contains more information. All events pertaining to the cameras managed by the Archiver are logged as well.

Backup and Restore

It is not always possible nor necessary to keep weeks or months worth of video archives online. Part of the archiving management strategy is to keep the older video archives offline to achieve a balance between archive availability and storage cost.

In this section, we are going to look at how you can make backup copies of the online video archive and how to restore these backups to full search and playback capabilities should the need arise.

Backup

Backup is the operation that copies a subset of the online video archives, specified by a list of cameras and a date range, to a secondary storage (tape, RW-CD, Zip disk, etc.) for safekeeping.

Backups are handled by Archivers and Auxiliary Archivers in Omnicast. Each archiving service must be configured to backup its own data. Both types of archivers can be configured to perform the backup automatically at regular intervals or on an ad hoc basis.

The data preserved through a single backup operation is called a **backup set**. Backup sets are allowed to overlap each other, providing extra data protection.

Backup not only extends the availability of the video archives beyond the capacity of the online storage, but also protects, to a certain extent, the online data against accidental loss. This is achieved by backing up the data as soon as possible (the earliest is the following day), versus waiting until the last minute. The drawback of such a practice is that any bookmarks generated after a backup will not be included in the backup set.

For the backup operations to take place, the ☑ **Backup** option must be selected on the appropriate archiving service. See *Server Admin – Archiver –* Backup on page 92.

To learn how to set up the Archiver to perform periodic backups, please read *Config Tool – Archiver – Backup* on page 213.

To learn how to check the status of the last backup operation and how to perform unscheduled backups, please read *Config Tool – Archiver – Backup status* on page 214.

The complete backup history of a specific archiver can be viewed by searching the following events with the Config Tool: **Backup started**, **Backup success**, **Backup failed**. For more details about this feature, please read *Config Tool – Archiver – Event Search* on page 219.

Restore

Before the video archive contained in a backup set can be manipulated with the Archive Player, the backup set must first be restored using the Restore Archiver. In order to use this application, the Directory option **Number of Restore Archivers** must be greater than zero in your Omnicast license.

To learn how to restore a backup set, please read *Server Admin – Restore Archiver –* Note If you are using a remote database server and there are multiple archivers on the system, please ensure that the database specified is unique on each archiver on page 143.

You can view the characteristics (size, content description, etc.) of a restored backup set with Config Tool. See *Config Tool – Backup Set – Info* on page 235.

To learn how to delete a restored backup set, please read *Config Tool – Restore Archiver – Backup Sets* on page 390.