Large surveillance systems
An Axis, HP and Milestone joint solution guide.
Table of contents

Overview 3
1. Purpose and motivation 4
2. System overview 4
3. Specification of the outdoor surveillance system 4
   3.1 Cameras 5
   3.2 Axis Virtual Camera 5
   3.3 HP 3800 series core switch 5
   3.4 HP c7000 blade servers 5
   3.5 HP 3par SS7400 storage system 6
   3.6 Viewing client – HP z 420 workstation 6
   3.7 Video management – Milestone Xprotect® Corporate 6
4. Physical installation of surveillance system 7
5. Logical installation 8
6. Milestone Xprotect® Corporate 9
   6.1 Multi-stage archiving 9
   6.2 Video grooming 10
   6.3 RAID configuration 10
7. Best practices – HP 11
Overview

Today, large IP Video Surveillance Systems (VSS) consisting of over 1000 cameras are becoming more common. Such a network, supporting a significant number of end-users, needs to be very reliable, manageable, and scalable. Such applications are often found in several facilities:

- City or municipal street and public surveillance networks
- City or municipal traffic monitoring networks
- Transportation and transit line networks
- Large education campuses (college, university)
- Large business parks
- Large retail malls
- Airports
- Other high security installations

Recognizing the interest and importance of experience with large VSS, Axis hosted a global technical conference in corporation with global partners to setup two large VSS’s, using different state-of-art technologies, with the aim to test and identify critical components, establish a set of best practices for network design, configuration, reliability, scalability, and troubleshooting. Together with the partners the finding are presented in a set of white papers solution guidelines for system integrator and engineers.

The two VSS setups vary in both hardware and software. Each network consists of 1000 cameras. Due to logistics limitations we have decided to seperate the two VSS as indoor and outdoor setups. It is important to know that the naming of the 2 systems depends only on the cameras. In the outdoor system both indoor and outdoor Axis cameras are used, whereas in the indoor system only indoor cameras were used. The other components in the VSS works well with both indoor and outdoor installations.

This paper describes the outdoor surveillance system that was setup during the conference. The outdoor surveillance system is a joint solution deploying hardware from multiple partners consists of HP VMware server and network solution, with Milestone VMS on top. In this paper we will present the actual configuration implemented by each partner. We will also bring up basic concepts and best practices provided by the partners within networking, storage and VMS.

---

1 Including HP, NetApp, Allied Telesis, Genetec, Milestone, ABB, Weidmuller, Microsemi, Moodifier, Veracity, Firetide and Raytec
1. **Purpose and motivation**

The purpose of this paper is to provide a reference for large surveillance systems in the 1000 camera range. As details related to these types of projects are often kept secret, a case neutral setup and configuration involving some of the biggest manufacturers in the surveillance/IT industry will give insight to setup/configuration as well as best practices.

2. **System overview**

- The system was set up and built into a 40ft shipping container command center.
- An important goal was to ensure performance, reliability, all while saving on space, power and need for cooling.
- The HP 1000 camera solution was an HP Converged Infrastructure including a c7000 blade system using the latest BL460c Gen 8 server blades and the virtual connect flex fabric interconnects.
- The storage was the 3Par SS7200 using 144, 2.5", 900GB 10k RPM disks in RAID 5, configured as pass thru drives for the HyperV Virtual Machines (VM’s) located on the server blades and containing two VM’s per server to run the Milestone Xprotect Corporate version 6 software.
- The network was built as a core and edge configuration with the core being an HP 3800 switch and the edges being 2530 POE+ switches. These are all 1Gb connections with the HP 3800 having an additional 4 ports used as 10Gb uplinks into the c7000.
- The video management software was Milestone Xprotect Corporate version 6 and it was configured to have 10 active recording servers and 2 failovers as well as a separate management and SQL server, all located in the VM’s.
- The cameras were 50 various Axis cameras, using the Axis Virtual Camera software to simulate a total of 1000 camera streams into the Milestone software to load the system. The goal of the conference was to have 1000 cameras running into the VMS by the end of the conference.

3. **Specification of the outdoor surveillance system**

On the first day of the conference the cameras, edge networks and cabling was installed by the participants and connected into the core switch. The container and the racked components had been installed within the previous week, including the operating systems and the video management system.

---

**Figure 1.** Overview of the outdoor network
3.1 Cameras

The cameras were a selection of Axis models allowing participants to be able to explore fixed, PTZ's, and thermal cameras in action in order to get a better understanding of the product line. The cameras were mounted inside the container, or on scaffolding, and connected to the HP 2530 POE+, gigabit edge switches for network connectivity and power. The cameras used a variety of POE and POE+ connections, but only required a single CAT5e or higher performance cable to run the video stream and the various features of the cameras.

3.2 Axis Virtual Camera

Axis Virtual Camera (AVC) was installed inside nine different VM's on the three DL360s, 1U rack servers to simulate video streams from live cameras at a ratio of about 20:1 to arrive at the 1000 camera goal for the conference.

3.3 HP 3800 series core switch

The network solution used a small, but adequate, core switch. The perfect choice was the HP 3800 series layer 3 stackable, with over 2000 multicast groups, IGMP v3, VLAN capability as well as many other features.

The key to this core switch was the ability to run four, 10Gb SFP+ uplinks, into the HP c7000 blade servers to provide the ability for future testing and to increase the camera counts to several times the initial 1000 camera limit. The switch has 48 GigE POE+ ports that were used for local camera connections in the container.

Additionally, there were three HP 2530 edge switches, also with POE+, but only 24 GigE ports for the edge cameras on the scaffolding and the other external cameras.

In the design of the network, an averaging stream of about 5Mb/s per camera, including the simulated streams, were assumed in an attempt to create a load on the VMS that would be realistic in a production system.

For the demo solution no activate any extra features, such as VLANs or port intrusion protection was activated, as this would have taken too long to implement for the class. However, in a production environment, at least VLANs would be recommended for this number of cameras. Protection of a network will vary in production from simple, wide open access, to restricted VLANs or even a separate, independent network from production in high security installations.

See: http://hp.com/go/networking for more information.

3.4 HP c7000 blade servers

The HP c7000 blade system was chosen for the 1000 camera solution. This conserved space, required less power, was less complex, and provided a bonus of about $100k (USD) saving compared to a rack server equivalent.

The actual servers in this solution were the BL460c Gen8 blades with a pair of E5-2620 (6 core) Intel processors and 96GB of memory with a pair of 450GB 6Gb/s SAS 10k RPM disks in RAID1 behind a P220i controller with 512MB cache.

Each blade contained a 554FLB Flexible LOM for its networking and storage connectivity. This is a pair of 10Gb/s network connections that are divided into 8 logical networks through a programmable interface. For the large system setup, the interface was set up as a 4Gb/s storage connection and a 6Gb/s network connection.
The c7000 chassis is a powerful solution. With capacity for up to 16 blades in a single chassis, it can contain over 4000 VLANs at up to 480Gb/s across the backplane. When compared to 16 rack servers, this setup only needs 6 power supplies and 10 fans to run.

Another advantage of this blade system and the HP servers is the ability to monitor and configure the chassis from a remote location. Monitoring includes the bandwidth of the LOM ports, the input and output temperatures, instantaneous power being consumed, as well as power up.

The blades each contained a pair of HyperV, virtualized operating systems, explained in more detail later. See: http://hp.com/go/servers for more information.

3.5 HP 3Par SS7400 storage system

The storage used was an HP 3Par SS7400 storage system. It was chosen to be able to sustain the performance demand of high performance video surveillance, as well as for its enterprise reliability. The system contained only 900GB 10k RPM disk drives for the pass thru drive of the HyperV VM’s which contained the LiveDB of the Milestone Xprotect Corporate software. In a production implementation, there would also be near line 3 or 4 TB drives to contain the archive video for longer term retention.

A operational system may have up to a week of video stored on the higher performance disk before being archived for typically 30 days (With anything between 14 to 60 days would be normal). This 3par array contained many additional features were however, not required in this particular video surveillance system.
See: http://hp.com/go/storage for more information.

3.6 Viewing client - HP z 420 workstation

The viewing client for the HP 1000 camera system was also part of the HP Converged Infrastructure. This was an HP z420 workstation, running Windows 7 and Milestone Xprotect viewing station software. The workstation included a 6core Intel CPU and 16GB of memory to drive the pair of 4 port video cards that displayed live or recalled video from the Milestone VMS on the five 47” monitors located on the video wall of command central container. As most video streams today are using h.264 compression from the cameras, a high power, reliable workstation equipped with high-end graphics cards is required to decompress the video streams and display them clearly.

3.7 Video Management System – Milestone Xprotect® Corporate

For high-end and large installations such as the 1000 camera solution set up at the Axis Technical conference, the Milestone XProtect® Corporate 2013, in version 6 was recommended and used to manage and operate the 1000+ cameras as described in the following sections. Milestone XProtect® Corporate offers surveillance system architects, designers and administrators the architecture to implement large-scale surveillance systems spanning multiple physical locations, as well as legal and government entities.

To demonstrate the options for centralized solutions Milestone’s versatile video wall solution, the XProtect® Smart-Wall, that addresses the market for tactical/situation rooms, monitoring centers etc. was installed. Furthermore, a Mobile Server was configured on the same machine as the Fail-over Server. The aim here was to demonstrate the possibility to have clients connecting to the Mobile Server from tablets and mobile phones.
Once operational, features demonstrated included, but was not limited to:

- How 1000+ cameras easily could be configured and managed
- Easy to use, daily operation using XProtect® Smart Client and Smart Wall
- Scenarios for using SD card in cameras
- Secure connections and exports using HTTPS
- How to change settings for multiple cameras in one operation!
- Cost efficient solutions using 64-bit technology and multi-stage storage
- Alarm management
- System management with a minimum of configuration using Milestone’s centralized management client, demonstrating how to easily deploy and maintain a multi-site scenario

4. **Physical installation of Surveillance System**

![Rack view](image)

*Figure 2. The Physical setup of the Outdoor 1000 camera network*

All network equipment is mounted inside a 19" rack. Starting at the top, there is the network core switch, a HP 3800, more specifically the model J9574A.

Moving down, the HP c7000 contains the seven BL460c Gen8 blades. The rear view shows the fans, interconnects, as well as the six power connectors. Note the simple connections to the core switch and storage unit. All connections required by the rack server are software configured within the chassis, limiting cabling mistakes and complex troubleshooting issues.

The HP 3par array has a very simple and cost effective connection to the blade system. There are only four fiber cables and no switches required for the 1000 cameras. For further expansion it’s possible to rearrange the rack for additional storage needed in a larger system or for longer retention periods.

The workstation for viewing was mounted in the container’s second rack, providing video to the five 47" LCD displays that were located on the container walls.
5. **Logical Installation**

The network switches were left in their default, non-secured configuration as they were shipped in order to avoid the complexity of having to create VLAN and add items like port security for the limited use during the conference. Normally, this would be planned and implemented in a production system.

The seven servers were installed with the 'full' version of Windows Server 2008 R2, (hereafter named 2008 R2). The Hyper-V service was then activated and finally 2 VM’s were created with 2008 R2 for the Milestone Software components. (Later referred to as the hypervisor)

In a production environment, the “core” version of 2008 R2 would most likely be used as it is free, whereas the full version has a licensing cost. However, the full version was used as it is easier to troubleshoot in a learning situation. Details are included below as Hyper-V is new to most people.

For each Virtual Machine (VM), the operating system was located on the local, 450GB hypervisor drive of each server. The additional drives were located on the hypervisor, but not mounted to the hypervisor. These will be referred to as pass through drives. The pass through drives were owned and formatted by each VM for dedicated performance required by the LiveDB or other uses.

In the configuration for the conference, there were two pass through drives per VM, as shown in figure three. The 500GB Logical Unit Number/disks (LUN) were for the LiveDB while the 7TB LUN was used for archive storage and to illustrate how video were moved from the LiveDB to the archiving tier.

In the 1000 camera outdoor solution, the seven server blades containing the seven hypervisors are shown in Figure 3 as hosts 1-7. The first hosts, 1-5 were set up as 10 live recording servers. Host 6 was a pair of VM’s used for recording server failovers, allowing for 2 VM’s or 1 complete blade to fail in...
production. The 7th blade contained the management server and the SQL database server for the Milestone Xprotect Corporate version 6 software. These could have had additional VM’s for their failover as well, as these don’t failover into the recording server failover VM’s.

The HP z420 workstation running Windows 7 with Milestone viewing station software was used to display the video feeds to the LCD displays in the container. In a production environment there would be at least one viewing station, but more stations for additional security personal, management, or other persons requiring access could be utilized. These stations could be using a single display, multiples or whole video walls, depending on the graphic cards, processor and memory configured into each workstation.

50 actual cameras were used for the system during the conference. In order to replicate and generate the load for 1000 camera streams, three DL360 servers running VMware were set up with three VM’s each for a total of nine VM’s. Each of the VM’s was using the Axis Virtual Camera, running on 2008R2 to simulate the load for the system. These servers would obviously not be required in a production system as the 1000 cameras would all be real cameras.

6. Milestone XProtect® Corporate

As seen in the previous hardware description, the solution was configured to suit the Milestone approach to storage with one cluster of disks for immediate recording and one for archiving. This multi-stage storage was configured to demonstrate how to make best use of storage and design cost-efficient solutions in respect to storage. Furthermore, XProtect® Corporate introduces a number of features and technologies in the storage architecture aimed to benefit large scale project by lowering the TCO and improve system performance.

6.1 Multi-stage archiving

XProtect® Corporate supports a multi-stage storage architecture where the recordings can be archived again and again to new storage areas. Combined with the grooming feature, (see grooming section below) multi-stage storage architecture greatly reduces the storage cost for systems that require recordings to be stored for a long time. The feature allows the recorded frame rate and thus data amount to be reduced over time.

The definition and configuration of 'Live' databases and archives are defined as part of a concept called a 'Storage container'. Cameras that should store video or audio recordings are simply set to use one of the defined Storage containers. This makes the storage configuration of the individual devices very simple as all settings are made and configured through the storage container.

![Figure 4 - The Storage container with a live database and 3 archives](image-url)
6.2 Video grooming

XProtect® Corporate has the possibility to groom the video recorded in the surveillance databases each time the recordings are archived.

Grooming is a method to decrease the frame rate of the recorded video over time in order to save space on the storage system. Through grooming, past recordings are kept, albeit at lower frame rate, keeping a record throughout the required retention time. The typical argument for using grooming is that the older the video are, the less likely it is that something important is recorded on it as important things most often are discovered and investigated quickly.

XProtect® Corporate can groom video recordings each time they are archived. Grooming is enabled and the specific frame rate of the groomed recording is setup in the same dialog as archiving is configured. As XProtect® Corporate supports multi-stage archives the grooming can be done as many times as there are archives, reducing the frame rate again and again over time.

For M-JPEG recordings, it is possible to groom to any frame rate lower than the native frame rate recorded in the database. Please note however, that for Inter frame encoding, such as MPEG-4 and H.264 recordings, grooming can only be done to key-frames (I-Frames) or slower frame rates. For Axis cameras, where GOV length is set at 32 as default, the implication is that the grooming would render a first level grooming at about 1 fps, whereas the following grooming’s would exclude I-frames and provide 2fps, 4 fps, and so on.

6.3 RAID configuration

Typically the disks, both Live and Archive, are configured to use RAID in order for them to be large enough. In this case it is recommended to only use RAID 0, 1 or 1+0 for the ‘Live’ disks and then RAID 5 or 6 for the archive disks.

The reason for only recommending RAID 0, 1 & 1+0 for the live disks is that there is a large overhead on the RAID controller to calculate the parity and writing the data at a high rate in parallel across all the disks in a RAID 5 or 6 disk system.

Normally it is not a problem or challenge to use RAID 5 or 6 in a normal IT environment, as buffers in both ends holds the data until it is written to the disk. In a video surveillance system there are no buffers as data (video) are received in real-time. So the disks and controllers continuously need to be able to handle the data in real-time. This often proves to be more than most RAID controllers can handle in RAID 5 or 6, even on more expensive disk systems.

The recommendation for the drive type usage and RAID configuration is also the same when the drives are used in a storage box like a SAN, DAS, NAS etc.
7. **Best practices - HP**

This is a description of suggestions to do in a real world production environment.

> Encryption through IPSec may be implemented between video endpoints to ensure data privacy, integrity, and authentication, mostly used in a very secure site.

> VLANs, and other network virtualization techniques may be used to segment the video endpoints and servers, this is recommended to isolate video and other IP traffic so they don’t interact or affect each other’s operation. In the simple, very small system, a customer would be able to put everything in the site on a single switch. As systems grow, or security concerns and networks ownership become an issue, this is where VLANs or independent switches may be used to segregate the traffic and isolate types of traffic and security levels to different, at least, VLANs. This can be taken as far as color coding cables for video, VOIP, data or other traffic, down to cable colors like “the RED cables can’t be touch”, “BLUE for data”, “YELLOW for video”, etc. A good rule for VLANs is to keep them “class C”.

> Port security or intrusion protection should be considered as the sites become larger or security more sensitive.

> Deploying a video surveillance solution through a WAN environment presents challenges that are not typically seen in a LAN, the WAN bandwidth is costly and the available transport types and performance depend on the service provider offerings.

> Network Time Protocol (NTP) must be configured for an accurate and consistent time for all video surveillance devices in the network, even to the cameras.

> Small systems don’t require failover, but as systems grow suggest this to a customer for their protection.

> Cat5e cabling at a minimum is required today, Cat7 and fibre are available for distance and performance, but remember that most cameras today still only run at 100Mb/s.

> Virtualization is great today, but as with a single server, the aggregate performance of the VM’s must not exceed the server’s capability or the requirements of the video or storage being used, be careful to not oversubscribe.

> If multicast is used, the number of multicast groups and IGMPv3 must be available in the switches.

> Different VMS ISV’s have different requirements make sure the ISV are involved.
About Axis Communications

Axis offers intelligent security solutions that enable a smarter, safer world. As the global market leader in network video, Axis is driving the industry by continually launching innovative network products based on an open platform - delivering high value to customers through a global partner network. Axis has long-term relationships with partners and provides them with knowledge and ground-breaking network products in existing and new markets.

Axis has more than 1,600 dedicated employees in more than 40 countries around the world, supported by a network of over 65,000 partners across 179 countries. Founded in 1984, Axis is a Sweden-based company listed on NASDAQ OMX Stockholm under the ticker AXIS.

For more information about Axis, please visit our website www.axis.com.