EMC²
where information lives®

EMC Virtual Infrastructure for Physical Security

Enabled by EMC CLARiiON, VMware vSphere 4, and Verint Nextiva

Reference Architecture

EMC Global Solutions

EMC² PROVEN SOLUTIONS

vmware® TECHNOLOGY ALLIANCE PARTNER

Published May, 2010

Part number: H7125

Contents

Reference architecture overview

Document purpose

This document provides an architectural overview of the EMC Virtual Infrastructure for Physical Security solution enabled by EMC® CLARiiON®, EMC Celerra®, VMware vSphere 4, and Verint Nextiva.

This document also includes configuration guidelines and resource specifications for the solution components and storage arrays. For detailed information regarding installation and implementation, please consult the Proven Solution Guide for the EMC Virtual Infrastructure for Physical Security.

Solution purpose

The purpose of this solution is to present a reference architecture that provides a platform for integrating legacy and state-of-the-art physical security and surveillance infrastructures, while using virtualization technology to:

- Increase resource utilization
- Decrease the number of servers and their associated costs
- Maximize server manageability

Using the EMC and Verint integrated solution, a security team can view realtime video while also receiving policy-based and anomaly-based alerts generated from sophisticated software analysis of the data from remote locations and historical archives.

The business challenge

Private businesses and public entities have responded to rising concerns about theft, fraud, and terrorism by sharpening their focus on physical security and surveillance systems. These organizations face two key challenges:

- Managing and protecting their ever-growing volume of physical security information
- Maximizing the performance and utilization of their network and storage infrastructure

The ability to access the right data at the right time from anywhere is crucial to supporting physical security and surveillance needs. But comprehensive solutions may be hindered by:

- Proprietary software and closed hardware platforms
- Lack of archive management capabilities
- Data retrieval wait times or lost data
- Content authenticity

These limitations are amplified by the high expansion costs of legacy video surveillance systems based on CCTV, digital video recorders (DVRs) or networked video recorder (NVR) technologies; and non-integrated IT and physical security systems.

The technology solution

The EMC Virtual Infrastructure for Physical Security solution provides the ability to control video surveillance and analyze security incidents in real time from anywhere, while monitoring and collecting evidence faster through realtime data and active archiving capabilities.

This solution integrates EMC and Verint technology in a virtualized architecture to help meet the challenges of video surveillance information convergence and management.

Verint Nextiva software aggregates physical security content from multiple sources, integrating IP networking and a full range of physical security systems, including:

- Video surveillance cameras
- Access control devices and intrusion detection systems
- Information security applications
- Visitor management and identity recognition
- Asset management
- Sensors and alarms
- RFID, biometrics, plus future enhancements and analytics

Verint's Review application is compatible with RSA's SecurID Windows Authentication agent, providing multiple layers of secure access to the physical security infrastructure and authenticated tamper-proof video data for increased conviction rates.

The core storage architecture is based on enterprise-class EMC CLARiiON storage systems to cost-effectively scale the solution as security requirements grow with industry-leading reliability, availability, scalability, and storage-based functionality.

To reduce the footprint of a Nextiva installation, the servers and recorder can be run on virtual machines using VMware vSphere 4, including the Nextiva master server, Nextiva recorder server, Nextiva ESM server, and the Nextiva master recorder.

The virtualized architecture uses VMware vSphere 4 and includes fault-tolerance high-availability (FT/HA) functionality to provide:

- Zero downtime
- Zero data loss
- Continuous availability

Key components

Solution architecture

The physical security components are typically comprised of legacy analog monitoring capabilities, analog cameras, and IP cameras.

Nextiva encoders are employed to convert standard NTSC/PAL video from analog cameras to a digital video stream over TCP/IP. Nextiva IP cameras or customer-furnished IP cameras can also be deployed. Each camera is capable of producing a digital video stream over TCP/IP.

EMC's storage platforms are used to provide single- or multi-tiered storage architectures for centralized or decentralized enterprise requirements.

To optimize hardware costs, reduce the data center footprint, and reduce greenhouse gas, Nextiva servers may be virtualized, running on virtual machines enabled by VMware vSphere 4.

Digital video streams

Digital video streams over TCP/IP are captured by the Nextiva recorder server application and written to CLARiiON storage.

Note: Only the EMC E-Lab™ Interoperability Navigator SAN and DAS configurations are supported with the Nextiva recorder application.

Master server

The Nextiva master server application provides an index of the video captured by the Nextiva recorders as well as user authorization and event management.

The master and recorder server applications can be installed on a single server depending on configuration requirements. This configuration is considered a master recorder server.

Recorder server

The Nextiva recorder server application captures live video streams to storage volumes for archiving. The recorder application keeps a separate index for all video captured and acts as the source for video playback and review requests.

VMware vSphere 4

VMware vSphere 4 is the market-leading virtualization solution that allows you to turn your infrastructure into an efficient and flexible internal cloud, enabling you to:

- decrease your capital and operating costs,
- run a greener data center and reduce energy costs,
- control your application service levels with advanced availability and security features, and
- streamline IT operations and improve flexibility.

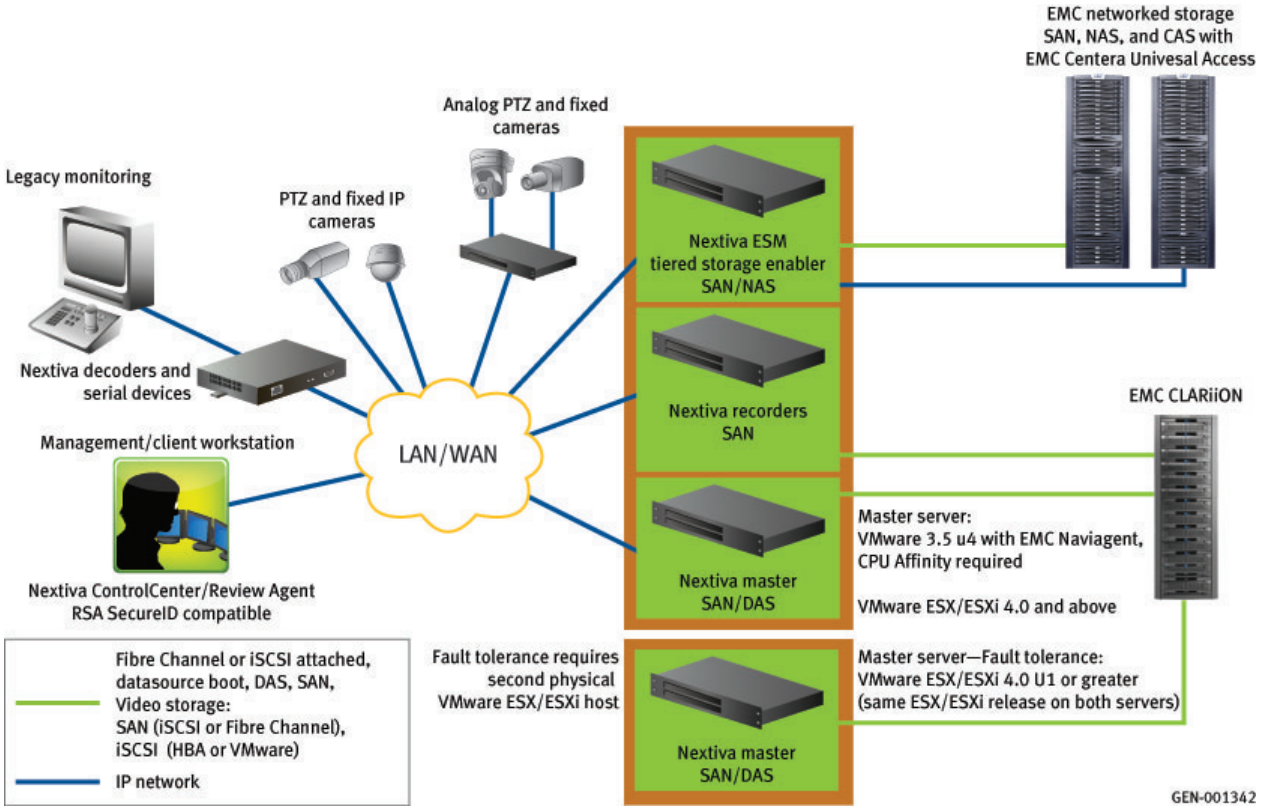
Fault tolerance

VMware vSphere 4.0 with ESX 4.0 provides hardware component failure protection for up to 500 cameras with event-based recording enabled or up to 700 cameras without event-based recording enabled.

Physical architecture

Reference architecture diagram

The following illustration depicts the overall physical architecture of the solution.



Virtualized Nextiva servers

The reference architecture diagram illustrates the virtualization of Nextiva servers using VMware vSphere 4.

The virtualized infrastructure must use server and storage adapter hardware that is officially validated by VMware as well as validated by EMC.

VMware FT relies on a single processor for all activity such as operating system functions, a SQL database, and Nextiva software. It can support up to 500 cameras with event-based recording enabled. The normal boundary of 700 cameras is maintained when event-based recording is not enabled. VMware FT provides a full nondisruptive transition where no data is lost during a failover or noticeable by the client.

VMware HA is not restricted to any hardware limitation. Therefore it is treated as a real physical server and can follow the Boundaries and Limitation by Nextiva. VMware HA allows more hardware resources used per virtual machine then FT, but is considered to be a disruptive failover where the virtual machine will reboot on the secondary server. Expected time for a full Nextiva recovery depends on the scale of the system and may reach up to 8 minutes.

The database of supported hardware, including fault tolerance, for VMware can be found at:
http://www.vmware.com/resources/compatibility/search.php

Validated environment profile

Profile characteristics

The solution was validated with the following environment profile.

Profile characteristic	Value
Nextiva application software	Windows Server 2003 SP2/R2 on local server disk or boot from CLARiiON
Storage topology	SAN, iSCSI, and NAS
Number of recorder servers per master recorder	22 – Windows Server 2003 75 – Windows Server 2008 without R2 (Verint tested)
Number of cameras per recorder server	Varies based on total VMware load and server class of VMware platform 96 @ CIF 30 FPS 48 @ 2 CIF 30 FPS 32 @ 4 CIF 30 FPS
Total bandwidth per recorder server	19.5 MB/s
Total bandwidth per ESM server	19.5 MB/s
Total bandwidth per CUA	31 MB/s

Verint minimum requirements for ESX

Verint recommends the following minimum requirements. These minimum requirements were derived during validation testing.

Processor minimum

At least a quad-core processor of the following is required.

Number of hosts	Processors	Processor Type
2	Single (1)	Xeon 54xx, 55xx, or 74xx
4	Dual (2)	Xeon 54xx, 55xx, or 74xx
8	Quad (4)	Xeon 54xx, 55xx, or 74xx

Memory

Number of hosts	Memory Requirement
2	4 GB
2+*n*	2 GB per additional host

Networking

Number of hosts	GigE NIC Requirement
n/a	Dedicated NIC ESX Console
2	Minimum: 1 NIC
2+*n*	Dedicated NIC per host (recommended)

Storage adapter

- All storage adapters must be VMware certified.
- Fibre Channel adapters must be VMware- and EMC-certified.

Storage

- Datastore
  - Direct attached or SAM devices with unpartitioned space
  - A minimum of 80 GB per VM is required
- Video storage
  - SAN devices with unpartitioned space (that is, VMware RAW attach)

CLARiiON configuration

The following table lists the CLARiiON configuration guidelines for the solution. See the *CLARiiON Configuration Guidelines for Verint's Nextiva Technical Note* for more information.

Parameter	Value
RAID type	5 and 6
Size (no. of disks) per RAID group	4-9
Disk types	320 GB, 5400 rpm 500 GB, 7200 rpm SATA 750 GB, 7200 rpm SATA 1 TB, 7200 rpm SATA 1 TB, 5400 rpm SATA (additional cache may be required)
RAID group configuration	Multi-Disk Array Expansion (DAE) LUNs (bus-spanning) and single DAE RAID groups are acceptable.
LUN configuration	Single LUN RAID groups only See *CLARiiON Configuration Guidelines for Verint's Nextiva Technical Note* for additional details (restricted to employees only)
Bandwidth per LUN	See *CLARiiON Configuration Guidelines for Verint's Nextiva Technical Note*
Bandwidth per array	See *CLARiiON Configuration Guidelines for Verint's Nextiva Technical Note*
Cache/memory settings	See *CLARiiON Configuration Guidelines for Verint's Nextiva Technical Note*

Hardware and software resources

Hardware The following table lists the hardware used to validate the solution.

Equipment	Quantity	Configuration
Any 1U, 2U, or blade server on Verint and EMC's supported hardware listing	1	Per master server application Per recorder server application Per Enterprise Storage Manager application
AX4-5/5i, CX3-XX, CX4-XXX, NS-XX, and NX4	Based on solution requirements	See *CLARiiON Configuration Guidelines for Verint's Nextiva Technical Note* for additional information (restricted to employees only)
NS-XX, NX4, CLARiiON NAS arrays	Based on solution requirements	Tiered storage architectures only. For use with ESM and Nextiva Review bookmarks
EMC Centera Universal Adapter (CUA) Server	Based on solution requirements	Standard CUA configuration
EMC Centera (with CUA)	Based on solution requirements	Generation 4 only Tiered storage architectures only. For use with ESM and Nextiva Review bookmarks See *CLARiiON Configuration Guidelines for Verint's Nextiva Technical Note* for additional details (Please contact the Physical Security development team)
Nextiva Review and Nextiva Control Center workstations	Minimum of 1; Maximum – Unlimited	Specified in Verint's Nextiva documentation

Software

The following table lists the software used to validate the solution.

Software	Version	Configuration
VMware ESX 3.5, VMware ESX/ESXi	3.5 Update 4, 4.0 Update 1	As described in the "Virtual Hardware Requirements" section.
Windows Server 2003	SP2/R2	Operating system for Nextiva servers and workstation(s)
Windows Server 2008	None	Operating system for Nextiva servers and workstation(s)
Nextiva master server	6.0 R1 6.1	Windows Server 2003 R2 Windows 2008 32-bit and 64-bit Local disk drive installation for all non-boot from SAN configurations
Nextiva recorder server	6.0 R1, 6.1	Windows Server 2003 R2 Windows 2008 32-bit and 64-bit Local disk drive installation for all non-boot from SAN configurations.
Nextiva Control Center	6.0 R1, 6.1	Administrator interface
Nextiva Review	6.0 R1, 6.1	User interface
EMC Naviagent	Latest GA version	Installed on ESX 3.5 prior to installing virtualized servers

Virtual hardware requirements

The following table lists the virtualized hardware requirements for the solution.

Virtual element	Description
vCPU	Two vCPUs per virtualized Nextiva server
Memory	2 GB memory per virtualized Nextiva server plus 2 GB for ESX
Configuration	• Set the affinity manually for each virtualized Nextiva server – Set affinity to all CPU other then 0 • Reserve 1200 MHz for each virtualized Nextiva server • Smaller environments on ESXi 4.0 CPU affinity was not set during lab testing
Runtime	• To ensure a smooth execution of each virtualized Nextiva server, the average CPU utilization of the host should be kept below 55 percent (total CPU usage)

Conclusion

Summary

The EMC Virtual Infrastructure for Physical Security solution enabled by Verint Nextiva products represents an ideal solution for surveillance management and IT infrastructure, and incorporates virtualization technology that allows you to increase system performance and maximize resource utilization.

The solution provides a flexible and highly scalable virtualized infrastructure that can meet a broad range of today's demanding physical security requirements. By leveraging the best-in-breed surveillance management software from Verint and advanced IT infrastructure components from EMC, customers can maximize the return on their investment in these crucial platforms, and optimize the use of their system infrastructure.

In addition, the solution provides seamless integration with new and legacy infrastructures while reducing the total number of physical servers, reducing greenhouse gas, and more effectively utilizing a physical server's processing capabilities. EMC storage-based functionality also allows customers to nondisruptively back up their primary servers while the system remains online and available to users. As requirements change and become more sophisticated, customers can be assured that the EMC Physical Security Solution's flexibility and modular architecture can be designed to meet their needs.

Next steps

EMC can help to accelerate assessment, design, implementation, and management while lowering the implementation risks and costs of a physical security solution for a VMware environment.

To learn more about this and other solutions contact an EMC representative or visit www.emc.com/solutions/business-need/information-security/physical-security.htm.