CINOS.net

Archived resources

For further resources and
documentation please visit us:
www.cinos.net

Nextiva Video Management Software: Protecting Mission Critical Operations

A Verint Technical Brief

November 2011

VERINT

POWERING ACTIONABLE INTELLIGENCE®

Table of Contents

Mission Critical Operations ... 1

Network Availability ... 2

Operational Site Availability ... 2

Protecting Nextiva Configuration Data ... 2

Ensuring Multi-site Availability ... 2

Protecting Nextiva Using Fault Tolerant, High Availability or Disaster Recovery Solutions ... 3

Video Recording Availability ... 3

Dual Recording ... 3

Recorder Failover Groups ... 4

Video Stream Availability in Client Applications ... 4

What’s Your Nextiva Solution? ... 5

Transforming Video into *Value*™

Verint® Video Intelligence Solutions™ is the leading global provider of networked video solutions designed to enhance the security of people, property and assets. Its award-winning Nextiva® portfolio features IP video and physical security information management software, integrated analytics, encoders, cameras, wireless devices and intelligent NVRs for use across a variety of environments. Open, standards-based and IT friendly, Verint solutions help organizations realize the benefits of IP video and to leverage their legacy video investments.

About Verint Systems Inc.

Verint® Systems Inc. is a global leader in Actionable Intelligence® solutions and value-added services. Our solutions enable organizations of all sizes to make timely and effective decisions to improve enterprise performance and make the world a safer place. More than 10,000 organizations in over 150 countries—including over 85 percent of the Fortune 100—use Verint solutions to capture, distill, and analyze complex and underused information sources, such as voice, video and unstructured text. Headquartered in Melville, New York, we support our customers around the globe directly and with an extensive network of selling and support partners. Verint is listed on the NASDAQ Stock Market under the symbol “VRNT.” Visit us at our website www.verint.com.

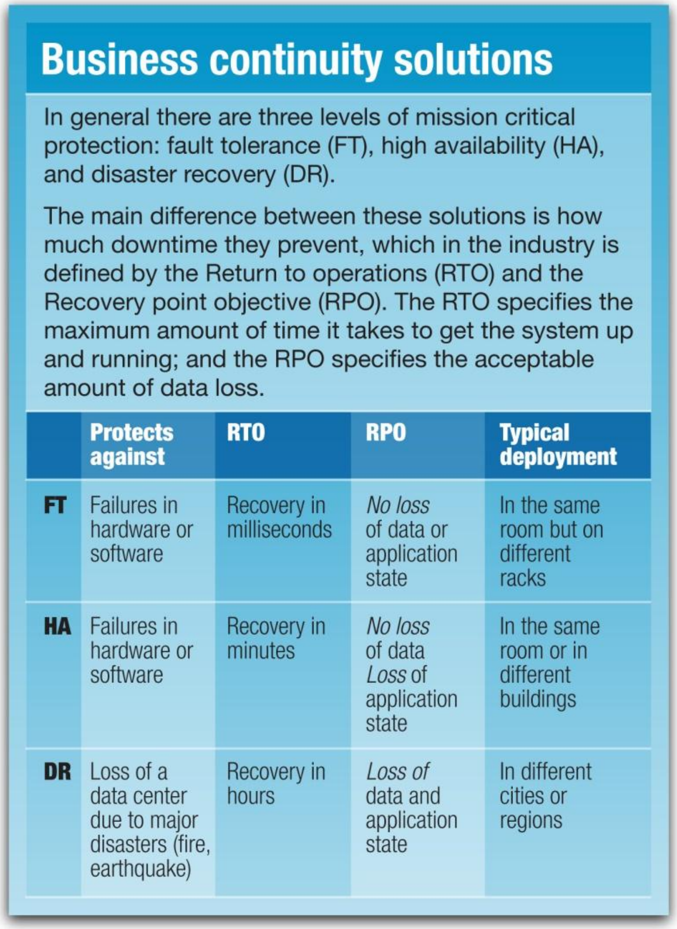
Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited.

By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice.

Features listed in this document are subject to change. Please contact Verint for current product features and specifications.

Mission Critical Operations

Today, video security systems are increasingly important in mission critical environments, such as those found in airports, seaports and railway stations, banks and financial institutions, cities and metropolitan areas, government institutions, hospitals, large corporations, petrochemical and utility companies, and schools, colleges and universities. These organizations need robust and resilient video management software (VMS) to ensure that video is available for viewing, event identification and verification, multi-agency collaboration and investigation at all times. The VMS must ensure maximum system uptime for increased situational awareness and compliance.



Business continuity solutions

In general there are three levels of mission critical protection: fault tolerance (FT), high availability (HA), and disaster recovery (DR).

The main difference between these solutions is how much downtime they prevent, which in the industry is defined by the Return to operations (RTO) and the Recovery point objective (RPO). The RTO specifies the maximum amount of time it takes to get the system up and running; and the RPO specifies the acceptable amount of data loss.

	Protects against	RTO	RPO	Typical deployment
FT	Failures in hardware or software	Recovery in milliseconds	*No loss* of data or application state	In the same room but on different racks
HA	Failures in hardware or software	Recovery in minutes	*No loss* of data *Loss* of application state	In the same room or in different buildings
DR	Loss of a data center due to major disasters (fire, earthquake)	Recovery in hours	*Loss of* data and application state	In different cities or regions

Below are some key examples on when mission critical capabilities are needed:

- In *a hospital*, a chipset fails in the primary server of the VMS. The VMS has a fault tolerant configuration to immediately overcome the hardware failure and maintain operations.
- An *airport* datacenter experiences a complete power outage. The VMS must be able to operate from two locations, geographically dispersed to avoid similar failure situations and to provide application availability until the primary server is restored.
- A fire occurs at a *utility company* that disables the security operations center. The VMS must have a geographically remote server that can take over operations in the wake of a disaster and ensure that video is always recorded for post-incident investigation.

In all of the above scenarios, the VMS is instrumental in helping these organizations respond to an emergency and later investigate its causes. Consequently, the VMS is expected to continue operating normally, even if some components fail.

This technical brief explores how Nextiva® Video Management Software (VMS) can help ensure the efficient operation and up-time of the system, uninterrupted access to recorded video, and the continuity of live and recorded video distribution to client applications. Although mentioned briefly, network planning is considered an IT-centric activity and falls outside the scope of this document. Actual resiliency of any VMS is dependent in large part on the actual design, deployment and maintenance of the VMS system.

Network Availability

Nextiva VMS consists of several server machines, client workstations, and cameras; it may also include encoders, decoders, external monitors and CCTV keyboards. All of these machines and devices connect together over an IP network. Security and network professionals must plan for events, such as power outages and surges, by implementing standard IT practices – the use of generators, power surge protectors, multiple IP switches, routers, and IP routes – to the various machines on the network. For example, IT designers and integrators need to plan for storage redundancy, which could include dual storage paths, switches, and controllers, and also RAID configurations.

Operational Site Availability

Nextiva VMS is a highly reliable system of client and server applications that interact with edge devices over an IP Ethernet network. Verint® provides several methods to help ensure the availability of the Nextiva components on video surveillance networks.

Protecting Nextiva Configuration Data

The Nextiva database stores configuration data for all of the servers and devices, user management information, event management rules, and networking information. It also stores alarms, events, bookmarks and investigations. If the entire Nextiva database becomes unavailable, the Nextiva site is no longer operational. Protecting the Nextiva database ensures operational continuity.

To protect this key component, Nextiva can be configured to automatically performs a full backup of the Nextiva database every day and a backup of the transaction log every hour; creating both a duplicate file of all the information in the database and a record of database modifications, updates and deletions. By default, the backups are stored on the Master Server. It is recommended to store the backup files on a separate disk or other medium, preferably in a separate building in case of fire or other disaster.

Ensuring Multi-site Availability

The distributed architecture of the Nextiva Multisite feature enables each Nextiva site to operate independently of other Nextiva sites and the Multisite Server. As a result, there is no single point of failure within a multi-site deployment.

Each Nextiva site stores and manages its own multisite configuration and user information. The Multisite Server stores the site IP and user information of each site in its database. This distributed architecture ensures that if the Multisite Server fails or loses its network connection, the Nextiva sites are unaffected. And since a copy of the Multisite directory is on each Nextiva site, even if the Multisite Server loses its connection, the individual sites remain connected, allowing operators to perform their duties undisturbed. Most importantly, Nextiva Review™ users continue to have access to the Nextiva sites. Similarly, if a Nextiva site loses connection or fails, the other Nextiva sites continue to function. Nextiva Review users lose access only to the failed Nextiva site.

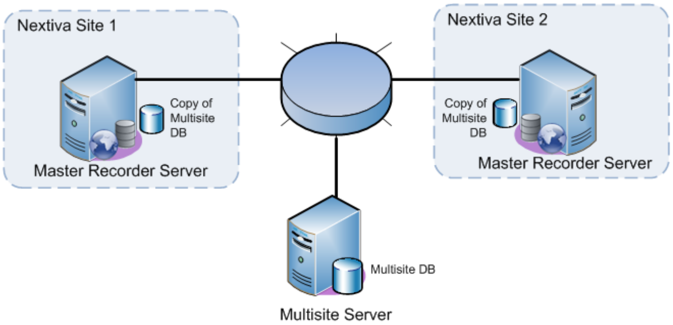


Figure 1 Multisite data copied in every site

Protecting Nextiva Using Fault Tolerant, High Availability or Disaster Recovery Solutions

When the Master Server is unreachable, users cannot establish a new client session. For client sessions that were running prior to loss of communication with the Master, a user cannot playback recorded video. For many operators, these losses are acceptable. However, mission critical operations require more protection for the Nextiva VMS. In these cases, Verint recommends using one of the availability solutions that have been fully certified and tested for use with Nextiva.

Fault Tolerant (FT) and High Availability (HA) solutions protect against unplanned downtime from common failures, such as network and storage interface failures, and server failures; while the Disaster Recovery (DR) solutions protect against disasters (such as fire, earthquakes, and floods) that affect a particular location. All of these solutions offer rapid recovery by eliminating many of the manual steps of a traditional recovery solution. In FT or HA solutions, specialized software automatically puts standby services online. The DR solutions offer the option of either manual or automatic recovery.

Video Recording Availability

The video surveillance systems found in mission critical operations, such as security in an airport or seaport, cannot afford to lose any recorded video. Nextiva's distributed architecture helps ensure that if a site's Master Server becomes unavailable, the Recorder Servers continue to capture video and audio. In addition, Nextiva VMS includes two methods for protecting recorded video in the event that a Recorder Server becomes unavailable: ***Dual Recording*** and ***Recorder Failover Groups***.

Dual Recording

The ***dual recording*** feature in Nextiva VMS refers to the simultaneous recording of camera video by two Nextiva Recorder Servers. Using dual recording, organizations help ensure that if a Recorder Server becomes unavailable, recording continues and users continue to have access to live and recorded video.

Dual recording enables the availability of video when a Recorder Server becomes unavailable as a result of failures on the network, server machine, or storage devices. As part of the dual recording feature, the Nextiva streaming infrastructure provides uninterrupted live streaming of video to consumers. Consumers of video include the Review and WebReview™ clients, applications that connect through the Nextiva Client SDK, and virtual matrix monitors that connect to HDR or S1801e-R decoders.

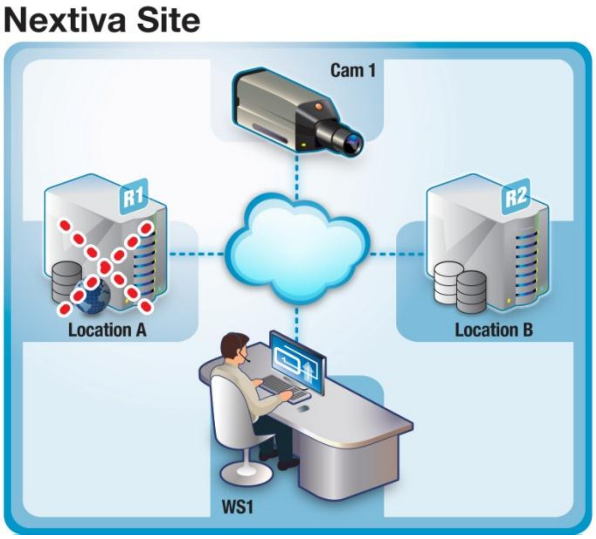


Figure 2 No Gaps in Recorded Video: Although Recorder1 is unavailable, Recorder2 continues to capture camera video

Recorder Failover Groups

In a Nextiva Master Server deployment that has multiple Recorder Servers, you can create ***failover groups*** to provide a backup mechanism for the Recorder Servers. Each failover recorder acts as a hot standby, ready to take over the functions of another recorder automatically in the event of a Recorder Server failure.

In the event of a Recorder Server failure, its cameras are reassigned by the Master Server to the other Recorder Server(s) in the failover group. Nextiva recording operations continue with only a brief interruption until the failover servers take over. The transferred cameras record on the failover Recorder Servers until the original Recorder Server comes back online.

For the failover function to operate as intended, each failover Recorder Server or group must have sufficient resources to support the extra cameras that will be moved there in the event of a server failure. If a Recorder Server fails, its cameras are reassigned by the Master Server to the other Recorder Servers in the failover group.

In the image provided, all four Recorder Servers are members of the same failover group. Recorder R1 has failed. All of its cameras are reassigned intelligently to the Recorders R2, R3, and R4.

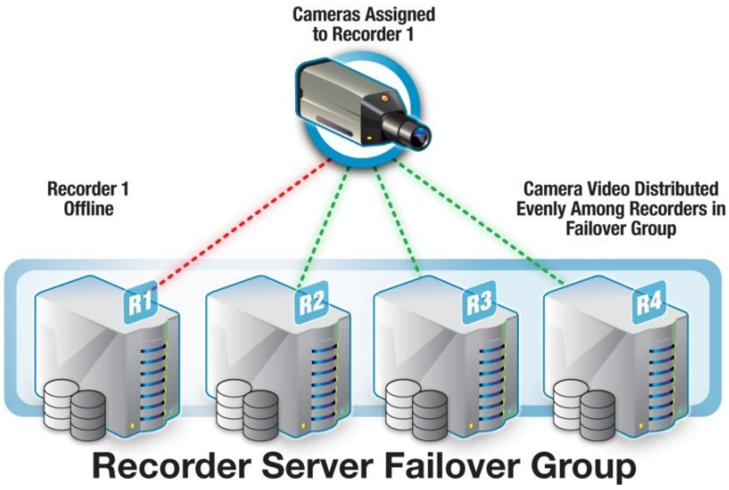

Cameras Assigned to Recorder 1
Recorder 1 Offline
Camera Video Distributed Evenly Among Recorders in Failover Group
R1
R2
R3
R4
Recorder Server Failover Group

Figure 3 Cameras from R1 reassigned R2, R3, and R4

Video Stream Availability in Client Applications

In Nextiva VMS, there are several methods for ensuring the continuity of live and recorded video viewing in a Nextiva client application (Review, WebReview, and application that use the Nextiva Client SDK).

- ***High Availability Streaming*** in a multicast network helps ensure that live video streams are uninterrupted by server failures.

  In Nextiva VMS, video streams to Nextiva client applications are more resilient as a result of the High Stream Availability feature. If a Master Server or a Recorder Server becomes unavailable, live video that is playing in the client application is uninterrupted. However, new requests for live or recorded video streams cannot be completed until the Master Server is restored. *Available in multicast networks only.*

- ***Dual Recording*** helps ensure that recorded video is available.

  If a Master Server becomes unreachable, not only does camera video continue to be recorded by the Nextiva VMS Recorder Server or Servers in the network, but the Nextiva clients continue to display playback video. If the Recorder Server that provides the playback video stream to the Nextiva client becomes unavailable, users simply request the video again.

- ***Media Gateway Redundancy*** helps ensure that requests for video streams are always answered.

  By deploying several Media Gateway Servers in a Nextiva site, if a single Media Gateway goes down or reaches full capacity, subsequent media streams requests are delivered through one of the remaining Media Gateways.

- ***Camera Service Mobility*** helps ensure the availability of camera services in the Nextiva Virtual Matrix.

  The services provided by cameras and encoders may include PTZ control, camera tampering, dry contacts and output relays, motion detection, status monitoring and analytics. If a Recorder Server that controls a camera goes down, Nextiva moves the cameras services to another Recorder. As a result, operators regain control of the PTZ cameras and all of its services.

What's Your Nextiva Solution?

In a mission critical environment, the video management system is essential for responding to an emergency, and later investigating its causes. Consequently, the VMS needs to be reliable and available at all times. Nextiva VMS includes several methods to help ensure the availability of the Nextiva components on the video surveillance network; thus ensuring that mission critical operations are better protected. Specifically, Nextiva VMS can provide automatic data backups to safeguard the system configuration information, event, alarm and investigation; several video recording solutions that safeguard video clips; and robust distributed architecture for multi-site networks so there is no single point of failure. Moreover, if a video recorder fails, *High Availability Streaming* ensures live video is not interrupted if a recorder fails, and *Service Mobility* ensures that PTZ cameras in the Virtual Matrix continue to be available.

Find out how Nextiva VMS can help *your* organization improve security and operational effectiveness.

Call Verint at **1-866-NEXTIVA** or visit us on the web at www.verint.com/videosolutions.

For further resources and
documentation please visit us:

www.cinos.net