THE ARCHITECTURE, SECURITY, AND PERFORMANCE ELEMENTS OF VIAKOO

VIAKOO

Copyright Viakoo ©2023

☎ (650) 263-8225 | ✉ sales@viakoo.com | 🔗 viakoo.com

Table Of Contents

Copyright Viakoo ©2023

Introduction

The Problem: IoT Performance & Cyber

IoT systems (such as video surveillance which we use as an example of IoT throughout this paper) is a significant investment made by organizations to drive their operaitons. It must perform reliably all the time to realize a full return on that investment, and must be cyber-secure. However, in spite of having top-of-the-line technology, first-class networking, continuous IT monitoring, and top-notch people manning and maintaining IoT systems —knowing about failures, how to fix them, and how to maintain cyber hygiene continues to be a problem.

The key question is: **Why?**

First of all, IoT systems are complex. The IP security video application is complicated by heavy bandwidth consumption, extensive storage requirements and a high number of complex configuration requirements. There are a great many variables that create intrinsic technical vulnerabilities that lead to missing video and unnecessary video downtime. Secondly, available IT monitoring tools are agent-based, application-unaware and don't detect many of the causes of IoT failure. There is nothing that provides continuous, end-to-end analysis of the integrity of video streams and accurately measures the retention time and quality of recorded video.

Each vendor or service provider works to support a particular part of the IoT system infrastructure, and has little or no visibility into problems outside of their own area of responsibility. No part of the existing infrastructure is capable of detecting more than a few of the potential problems that result in failures such as missing video.

Lack of integrated diagnostic information leads to inaccurate diagnosis. This is why troubleshooting IoT performance issues are generally an inefficient trial-and-error process that often ends without a conclusive answer. This is also why system failures have remained a problem in spite of the advances of technology.

The Solution: Viakoo

Viakoo is the first solution to directly take aim at performance and security. We do it with advanced Service Assurance and Cyber Hygiene capabilities.

Using patented and agentless technology, Viakoo continuously examines the entirety of the IoT system infrastructure. It does so by tracking a broad range of problem detection points; for video Viakoo goes from the IoT camera devices to the networks to the video application, to the servers and all the way down to the individual recording hard drives. Viakoo analyzes the diagnostic data and sends alerts that include the Problem Location and its Probable Cause. The same mechanisms can be leveraged to perform cyber hygiene, including firmware updates, password rotations, and certificate deployment.

Viakoo provides accurate and actionable information about video stream problems in any portion of the IP video infrastructure. This paper describes the architecture of the Viakoo solution and how Viakoo interacts with the elements of your IoT infrastructure:

- without introducing additional work for Staff,
- without introducing vulnerabilities to computer, network and data,
- without adding any significant load to video server processing,
- without placing more than a nominal amount of data into network traffic,
- and without requiring a VPN connection to Viakoo.

Additionally, it explains the types of diagnostic data collected and the alerts and reports via which the information is presented to desktops and mobile devices.

And it describes the Key Performance Indicators that it measures to detect faults, perform predictive analysis, and help maintain a high-integrity, high-availability IP video infrastructure. These same concepts apply broadly to IoT systems.

The paper also explains the availability and disaster recovery aspects of the solution.

Viakoo Overview

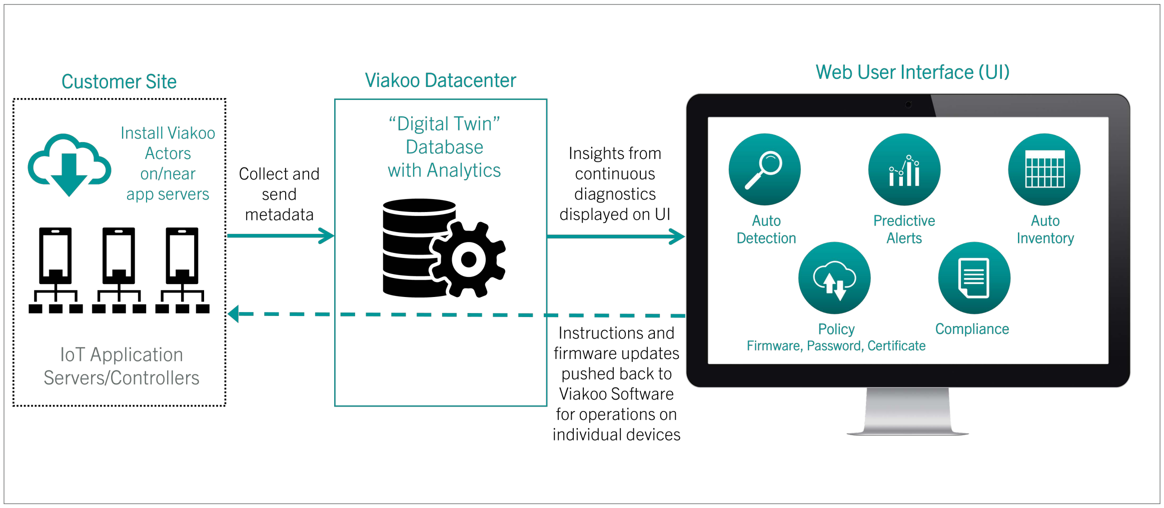
Data Collection and Diagnostics

As shown in **Figure 1** (following page), Viakoo automatically collects diagnostic data from existing IoT infrastructures and sends the data to the cloud-based Viakoo service center, via a secure, outbound-only connection. Viakoo's agentless Actors provide the ability to work across multiple types of IoT.

Once uploaded the diagnostic data is analyzed, looking for anomalies, making correlations, and doing predictive analysis.

The results of the analysis are delivered to the stakeholder’s phone or desktop, using email and a standard browser. Alerts are sent by an automatic Ticket generation capability that tracks activity and corrective actions.

Figure 1. Viakoo Overview


Customer Site
Install Viakoo Actors on/near app servers
IoT Application Servers/Controllers
Collect and send metadata
Viakoo Datacenter
"Digital Twin" Database with Analytics
Insights from continuous diagnostics displayed on UI
Instructions and firmware updates pushed back to Viakoo Software for operations on individual devices
Web User Interface (UI)
Auto Detection
Predictive Alerts
Auto Inventory
Policy
Firmware, Password, Certificate
Compliance

With Viakoo, users can get reports, charts, and graphs of performance status and trends.

To speed problem resolution, Team Viakoo experts can provide additional live, in-depth diagnostic analysis beyond that provided automatically.

Agentless Viakoo implementation is essential to achieving a high-integrity, high-availability IoT and IP video infrastructure.

This document presents key aspects of Viakoo's architecture, security, performance, and diagnostic data collection. It is intended to help in understanding how Viakoo works with existing IoT infrastructure, and understanding how it is designed as a safe solution with no perceptible impact on customer infrastructures.

Key Security Measures

Table 1 (following page) resents the key elements that make Viakoo implementations a safe & secure way to provide a unique set of capabilities that help your IoT infrastructure work properly, fulfilling its mission for systems such as video to provide situational awareness and maintain the video evidence recorded for the full duration intended.

Security Measure	Details	Benefits
No Content Data, Diagnostic Data ONLY	Only diagnostic data are collected to determine Video Path Uptime, Video Stream delivery quality, and Video Retention Compliance.	NO CONTENT or USER DATA is touched by Viakoo.
Outbound-ONLY Connectivity Required	Diagnostic data is automatically transferred every 20 minutes (a user-configurable interval) or upon demand by user.	Limited network connectivity to Viakoo, no persistent connections. **Viakoo requires Outbound-ONLY connections over HTTPS Port 443.** No connection INTO customer premise can be initiated by Viakoo.
No VPN Needed	HTTPS secure connections are used (i.e. connection on standard HTTPS port 443). Secure connection is automatic requiring no manual steps. Standard port usage requires no special port configurations.	Risk due to VPN exposure is eliminated.
Encrypted Diagnostic Data Transport	▸ AES 256-bit encryption authenticated using 2048-bit RSA key ▸ Digitally signed by DigiCert High Assurance Certificate Authority	Encryption means that data cannot be deciphered even if breached.
Viakoo Secure Service Architecture (SaaS)	▸ Role-based access privileges ▸ Multi-tenant data architecture ▸ Multi-layered firewall ▸ Data secured in virtual private cloud with only highly secured external access points.	Data collected by Viakoo is strictly controlled. Only customer-authorized users are able see all or part of the data— depending upon their assigned roles.
Digitally Signed Software Actors	The Actor installation packages and updates for the agentless Viakoo software Actors are digitally signed.	This best practice assures that the software was indeed issued by Viakoo and that it has not been altered or corrupted since it was issued.

Additional details on the above security measures are contained within the remainder of this paper.

Diagnostic Data Collection Architecture

Initiating Viakoo involves a simple, one-time installation of two agentless Viakoo software Actors on your existing IoT system infrastructure.

To collect diagnostic data from your IoT infrastructure and send it securely to Viakoo, two small-footprint software Actors are utilized on the IoT application servers and workstations:

1. The **Viakoo Reader Actor (VRA)** is used on each Windows-based server and workstation utilized to manage, record, and store security video. It collects diagnostic data on the IP video infrastructure only.
2. The **Viakoo Communications Actor (VCA)** is used on one server at each site where video is recorded. It retrieves and consolidates the diagnostic data collected by the RAs; establishes a secure, outbound-only connection to Viakoo, and sends the data.

A VRA defaults to a passive state and waits for its VCA to request data, at which time the VRA obtains diagnostic data and provides it to the VCA. The period of sampling is controlled by each VCA according to the sampling interval set for it. When a VCA has completed its data collection and integrated the information from the VRAs, it establishes an outbound-only connection to Viakoo and sends the collected data.

The VCA must be installed on a server with network connectivity to each server that has an VRA installed. Typically the server hosting the VCA is also hosting an VRA, but there is no reason it couldn't be a separate server.

The network connection to Viakoo that is established by the VCA exists just for the duration of sending the data to Viakoo. It is not a persistent connection. Initiating Viakoo involves a simple, one-time installation of the two Viakoo Actors.

During the installation process each RA will be given administrative privileges so it can utilize standard monitoring tools, such as the **Intelligent Platform Management Interface**[1], which is used to obtain data about the operational status of the server.

Outbound-Only Connectivity

The server with the VCA must also have an outbound-only HTTPS (Port 443) Internet connection. Since this is the same port used for secure connections by Internet browsers, no special network configurations should be required for this port.

The VCA can work through a proxy server. Alternatively, if configured with a proxy server, the VCA only needs an open connection to the proxy server. The proxy server then must have an open outbound HTTPS (port 443) path to Viakoo.

[1] Intelligent Platform Management Interface (IPMI) is a specification for the equipment that monitors the physical environment and behavior of a computer hardware server. The specification was developed jointly by Intel, Hewlett-Packard, Dell, and NEC. It is supported by over 200 computer system vendors. It is intended to cover the regulation of temperature, voltage, and power, and to ensure the proper operation of the firmware.

In either configuration, with proxy or without, all diagnostics sent to Viakoo are securely encrypted to ensure the confidentiality and integrity of the data, as detailed in **Table 1** on page 5.

Performance

Viakoo agentless Actors will not adversely impact the performance of the IoT system or network in general, nor the specific servers on which they run.

Viakoo Actors run at a lower priority than the other software in your IoT system. Viakoo Actors use only idle resources. In this way, key applications will continue to get as many of the CPU cycles as they did before the Viakoo Actor was added to the machine.

If a server is overloaded and runs at over 90% utilization for periods of greater than 15 minutes, its Viakoo Actor may not have enough CPU cycles to do its work and measurements may start falling behind. If this happens, the diagnostic updates may not be performed as frequently as intended.

Flow-Control and Caching

Because of the nature of network connectivity in general, communications between customer-site VCAs and Viakoo could be interrupted temporarily for varying lengths of time.

To prevent losing any of the diagnostic data collected, each VCA maintains a circular buffer file (VCA Cache). If it can't transmit a collection of diagnostics to Viakoo for whatever reason, it simply saves that collected data in its cache until communication is restored.

While communication is disrupted it will continue saving data to the cache, until the end of the available cache file space is reached. At that point, the VCA starts overwriting the oldest diagnostics with the newest diagnostics collected, much in the same way as video management software discards the oldest recorded video to make room for new video recordings.

Each site is different and the amount of space consumed with each collection will vary. The default size of the VCA Cache circular buffer is 100 MB, which should be enough to accommodate a connection outage of up to one week or more.

The VCA Cache Buffer Size and the VCA Send Interval are initially tuned automatically for best performance, but can be adjusted if necessary.

Requirements for Operating On-Premises

Many organizations today have choices when it comes to how to deploy applications, with considerations that will vary from one organization to the next. For a variety of reasons including internal policies, compliance and industry regulations, certain enterprises require that physical security metadata be kept within their own data centers. The Viakoo Action Platform delivers enterprise-wide physical security service assurance while adhering to these requirements while providing easy deployment, increased reliability, and high scalability.

For organizations requiring on-premises deployment the Viakoo Action Platform and licensed modules can be deployed entirely in your own network running VMware ESXi. Please review the Data Center infrastructure requirements listed below.

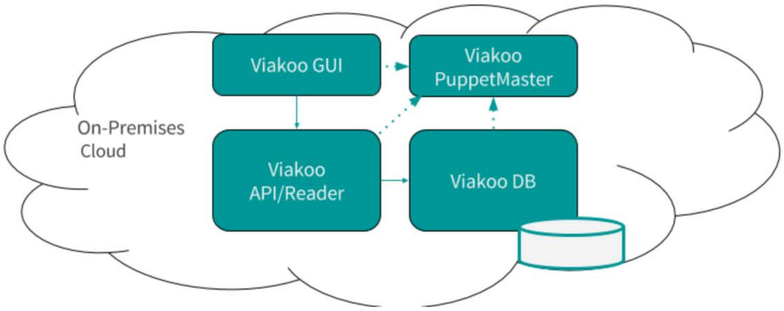
On Premises Installation/Configuration of Viakoo Action Platform

Viakoo provides a version of the Viakoo Action Platform service designed to run within your own Data Center. It is installed within your corporate Data Center running VmWare virtualization VSphere Cluster. There are several Virtual Machines required for running different components of Viakoo.

Viakoo uses two software actors: Communication Actor (CA) and Reader Actor (RA). Below are general requirements; please contact Viakoo Support to discuss your specific infrastructure requirements.

For Viakoo Communications Actor:
OS: Windows XP/7/10, 2003/2008/2012/2016/2019/2022, Linux (Ubuntu)
Memory: 1GB
Disk Space: 1GB
CPU: Any modern hardware with 10% CPU available

For Viakoo Reader Actor:
OS: Windows XP/7/10, 2003/2008/2012/2016/2019/2022, Linux (Ubuntu)
Memory: 1GB
Disk Space: 1GB
CPU: Any modern hardware with 10% CPU available



Data Center Configuration

Viakoo Security Architechure

An effective security architecture establishes layers of defense, creating a sequence of barriers that an attacker must defeat to penetrate a system. A close analogy is one of a castle with a sequence of moats and walls, each with unique and lethal defenses, and with narrow and well-defended entry points, to prevent an invading army from ever reaching the precious assets in the center of the fortress.

Viakoo was built with a secure architecture that establishes layers of defense to safeguard the data it collects and ensure Viakoo's continuous operation. Viakoo maintains SOC-2 Type II certification and can provide current audits, assessments, and penetration testing results.

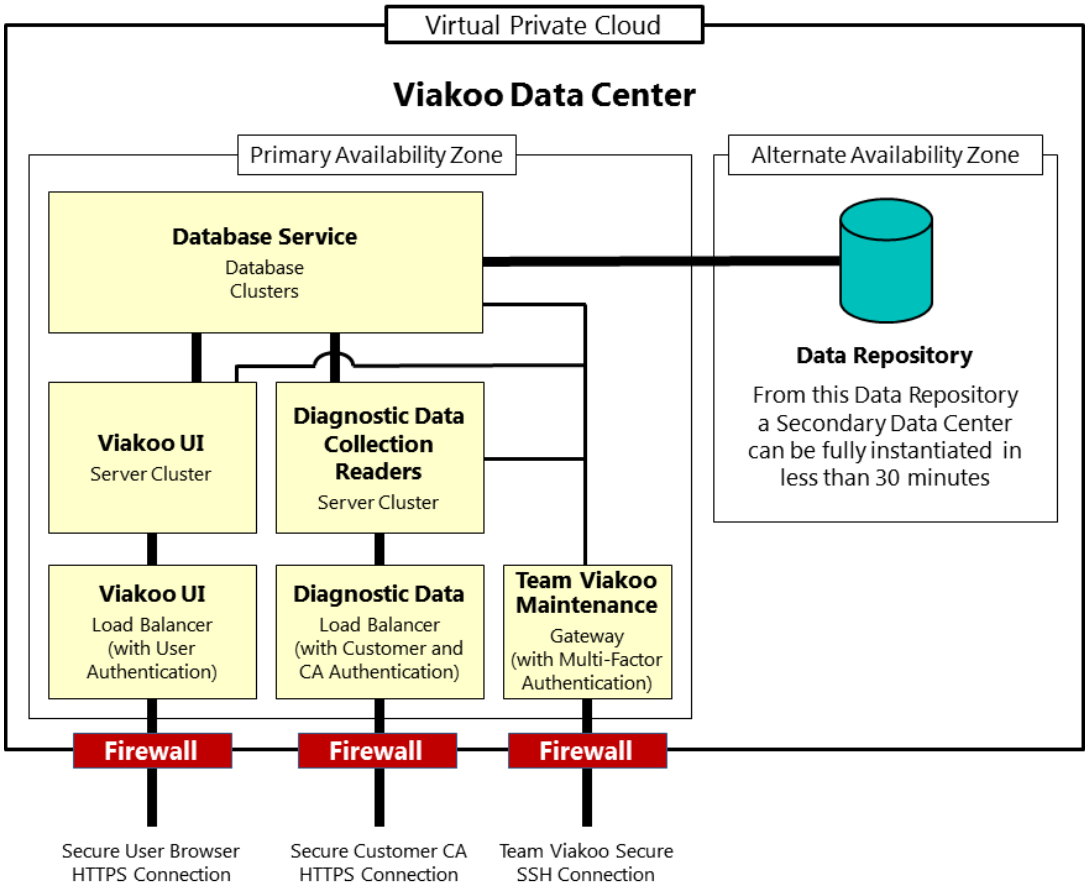
Secure Viakoo Architecture

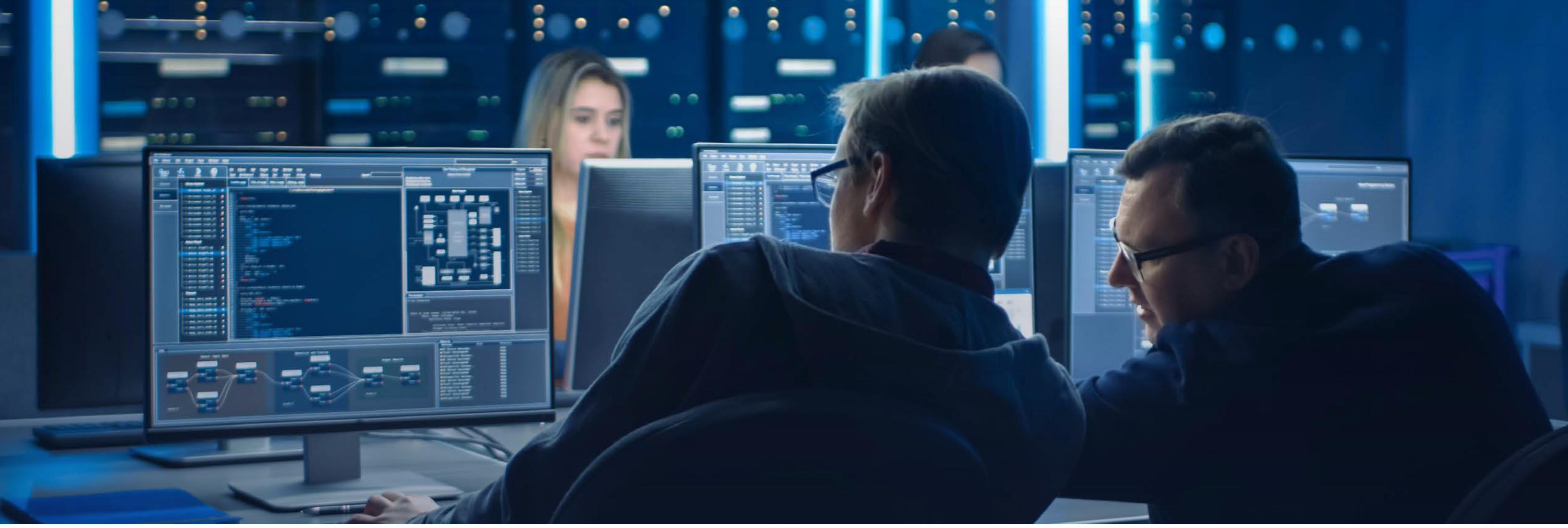
Viakoo leverages the latest architectural disciplines to provide both horizontal scale and security, making sure the service is always available and that customer diagnostics are secure and inaccessible to all but those who have authorized access.

To begin with, Viakoo limits external access points. There are only three network access points to Viakoo, listed below and shown in **Figure 2**:

- **Viakoo UI load-balancer** fronting the Viakoo User Interface servers
- **Diagnostic Data Collection load-balancer** fronting the Viakoo Diagnostic Data Collection Reader servers
- **Maintenance Gateway** server providing secure access to authorized Team Viakoo personnel

Figure 2. The Secure Viakoo Architecture


Virtual Private Cloud
Viakoo Data Center
Primary Availability Zone
Alternate Availability Zone
Database Service
Database Clusters
Data Repository
From this Data Repository a Secondary Data Center can be fully instantiated in less than 30 minutes
Viakoo UI
Server Cluster
Diagnostic Data Collection Readers
Server Cluster
Viakoo UI
Load Balancer (with User Authentication)
Diagnostic Data
Load Balancer (with Customer and CA Authentication)
Team Viakoo Maintenance
Gateway (with Multi-Factor Authentication)
Firewall
Firewall
Firewall
Secure User Browser HTTPS Connection
Secure Customer CA HTTPS Connection
Team Viakoo Secure SSH Connection



EXTERNAL CONNECTIONS

For both of the load-balancer access points, only the HTTPS port is open; both access points have advanced firewalls protecting them. All other entry points are locked down and inaccessible.

The Maintenance Gateway server, also protected by a firewall, has only an SSH port open and requires multi-factor, dynamic key authentication to access.

INTERNAL CONNECTIONS

Within Viakoo, each of the User Interface (UI) servers and the Collection Reader servers have only the HTTPS port and SSH ports open and all other ports locked down.

Furthermore, the Viakoo UI servers will only accept HTTPS connections through the Viakoo User Interface load-balancer, and will only accept SSH connections from the Maintenance Gateway server. Similarly, the Diagnostic Collection Reader servers will only accept connections through the Reader Load-Balancer and only allow SSH connections from the Maintenance Gateway.

The internal Database service is locked down as well. Similar to the Viakoo UI and Collection Reader severs, all Database service ports are closed with the exception of the ports fronting the Database service and the SSH port required for maintenance procedures.

The Database service is specifically restricted to allowing secure connections only from the Reader Servers and the Viakoo UI servers. The Database servers will only accept SSH connections from the Maintenance Gateway.

In this way, it is very difficult for malicious hackers to penetrate the system illegally. Additionally, internal Team Viakoo employees are prevented from having access to the data unless they have been explicitly authorized for access.

SECURE COMMUNICATION

All communications traffic to Viakoo from customer sites and users is encrypted.

Users log in to the Viakoo User Interface with HTTPS, a protocol that encrypts users' login credentials and all session traffic between Viakoo and their browsers.

The Viakoo CAs encrypt all traffic from a customer's infrastructure in a similar way. Additionally, the traffic from Viakoo CAs is unidirectional in that Viakoo only receives information from the VCAs, or responds to requests from the VCAs for updates. Viakoo never penetrates customer firewalls. No Virtual Private Network (VPN) access is required. Nor does Viakoo attempt to initiate any connections into a customer's security video infrastructure.

If a customer wishes to have Team Viakoo engineers help them directly inside the customer-premise security video network, a completely separate session using remote desktop technology would be used and be explicitly initiated by the customer.

SECURE DATA ACCESS

A multi-tenant architecture and customer-managed role-based access control ensure that access to data can be established consistent with the principle of least privilege: users are granted access to only that data they need to perform their job-related duties.

Additionally, access for infrequent users like vendor tech support personnel and contractors can be provided only for the duration that they need it to address an immediate work request.

Availibility and Disaster Recovery

FRONT-END SERVERS

Viakoo runs in a single primary data center with provisions to recover to a remote, secondary data center.

The Viakoo User Interface and the Data Collection Readers are provided high-availability through horizontal scaling (multiple servers in a cluster) behind load-balancers.

If a Viakoo UI server goes down for whatever reason, its load-balancer detects it and routes all subsequent UI traffic away from the affected server. Moreover, the system makes use of auto-scaling mechanisms to not only bring more servers online to accommodate increases in load, but also replace servers that may have failed to restore the server cluster to full capacity.

Similarly, the Data Collection Reader servers are configured in a horizontally scaled cluster. When the Collection Reader load-balancer detects an outage in a server, it routes all subsequent traffic to other servers in the cluster and automatically allocates a replacement reader server.

The database tier provides high-availability through database clustering using multiple replicas for performance and failover recover. In addition, data is replicated continuously to an alternate availability zone within the overall cloud infrastructure.[2]

For most issues affecting a single server, users will not be able to perceive a reduction in service of any kind. At most, a user may be forced to perform a re-login to the Viakoo User Interface.

PRIMARY DATA CENTER RECOVERY

If a disaster befalls the Viakoo primary data center, a fully operational secondary data center can be activated from the replicated data repository maintained in an alternate availability zone, and Viakoo will be up and running again in less than 30 minutes.

Furthermore, because the Viakoo CA Actors have buffering flow control, any diagnostic information collected in that window of time will still be retained and uploaded when Viakoo comes back online. In the event of such an occurrence, the impact on the level of service for most customers would be negligible.

[2] An Availability Zone (AZ) within a cloud infrastructure is a distinct physical location. It has low-latency network connectivity to other AZs and is engineered to be insulated from failures from other AZs. Each Availability Zone is engineered to be highly reliable and runs on its own physically distinct, independent infrastructure. Availability Zones have Independent power, cooling, network and security. Common failure points, such as generators and HVAC equipment, are not shared across zones. Additionally, they are physically separate so that extremely uncommon yet high-impact environmental hazards such as fires, tornados or flooding would affect only a single Availability Zone.

Diagnostic Data Collected

This section summarizes the types of diagnostics that are collected and sent to Viakoo, and which are analyzed and reported in trouble alerts and their related diagnostic data, and then summarized using key performance indicators (KPIs) for individual video streams as well as for the IP video infrastructure overall.

Diagnostic information is can be shared securely with video vendors and contractors, so that all stakeholders can be quickly brought to the same point of understanding with regard to the status of video infrastructure elements both inside and outside of their respective areas of responsibility.

The pages that follow describe specific measurements that are collected, using video surveillance as an example.

Viakoo customers can view these diagnostics in Configuration, Event, Performance, or Topology Views through the Viakoo User Interface.

Not all customer premise video networks serve up all the diagnostics listed below; certain infrastructure elements may be limited by their manufacturer or by the way they are configured during installation.

However, the more diagnostics that can be collected by Viakoo, the more timely the Advisories and Alerts, the more accurately the Probable Cause can be identified automatically, and the more useful Viakoo will be overall.

Infrastructure Performance Measurements

OVERALL IP VIDEO INFRASTRUCTURE PERFORMANCE

Viakoo provides three high-value measures that capture what is important to know about security video streams. These high-level Key Performance Indicators (KPIs) are derived from the diagnostic data Viakoo collects. These KPIs reveal the overall **availability and data integrity** performance of your IP video infrastructure against its design objectives:

- **Video Path Uptime** (VPU)
- **Video Stream Delivery Index** (VSDI)
- **Video Retention Compliance** (VRC)

Video Path Uptime measures the end-to-end stream path availability from camera device to storage media. VPU is defined as the end-to-end uptime percentage of the path through the infrastructure that a video stream takes.

Its goal is to help ensure that camera video streams are being transmitted and recorded as intended. Therefore, based on the aliveness of all components in the system, any component failures in the video stream path will lower the VPU score.

Video Stream Delivery Index measures the performance impact of saturation or decay of a video network on video delivery completeness. VSDI is expressed as a percentage.

This is different from VPU in that VPU reflects video stream paths that are in a fully operational or failed state. VSDI measures the performance of video streams that are still recording data but—due to saturation of networks, load in recording servers or ingestion limitations in storage subsystems—are losing portions of video data along an active video path. This is manifested in video playback as lost frames in seemingly okay video streams.

Video Retention Compliance measures the extent to which a video surveillance recording system meets its video recording retention goals. It is expressed as a percentage, and is calculated for each camera individually and also for the system overall. An individual camera's score can be higher than 100% if the camera is exceeding its retention goals. For example, a stream that is recording for 45 days against a retention requirement of 30 days is 150% in compliance.

[3] A network socket is an endpoint of a communication flow across a computer network. A socket address is the combination of an IP address and a port number, much like one end of a telephone connection is the combination of a phone number and a particular phone extension. Based on the socket address, sockets deliver incoming data packets to the appropriate application.

In the formula for the aggregate score across the entire IP video infrastructure, each stream's score is capped at 100%, so that high-retention streams (over 100%) don't offset and thus mask any low-performing streams.

For detailed information on these performance KPIs, see the white paper titled, **Three Must-Have Measures of IP Security Video Infrastructure.**

The sections that follow present information on the specific categories of diagnostic data collected by Viakoo.

CAMERA DEVICES AND CAMERA NETWORK SWITCH DIAGNOSTICS

The Viakoo Actors collect the following information from Camera Devices and Camera Network Switches:

1. **Configuration Data**
2. **Camera Video Stream Data**
3. **Performance Data**

The Viakoo Actors leverage video-stream socket[3] performance information to understand inflowing and outflowing bitrates from cameras, and SNMP data from Camera Network Switches to get greater details on the topology of the camera network, plus performance and congestion information.

Therefore, to get the best results, Smart Switches or Managed Switches should be configured to support SNMP. In most cases the Viakoo RA Actor needs to be given authenticating information such as the SNMP Community ID to access camera network switch information. The Service will continue to function without this information, but it will lack some key measures that are useful in diagnosing issues that occur in video networks.

Copyright Viakoo ©2023

RECORDING SERVER DIAGNOSTICS

The diagnostics Viakoo collects on each video recording server cover four areas:

1. **Video Recording Server Configuration**
2. **Video Recording Server Environmentals**
3. **Video Recording Server Performance**
4. **Windows Event Log**

This includes servers classified as standby, failover or alternate recording servers.

To collect this information, the Viakoo Reader Actor (RA) uses utilities such as Open Hardware Monitor, Intelligent Platform Management Interface (IPMI), Performance Monitor, and Java SIGAR libraries.

VIDEO MANAGEMENT SERVER DIAGNOSTICS

This is a general category for servers in video systems that perform management of video stream distribution, including authentication servers, configuration servers, and video stream routing servers.

1. **Video Recording Server Configuration**
2. **Video Recording Server Environmentals**
3. **Video Management Server Performance**
4. **Windows Event Log**

STORAGE SERVER AND VIDEO SAN DIAGNOSTICS

In general, the Viakoo Reader Actor collects events, configuration and performance diagnostics. For all systems, we collect the following for all Logical Volumes mounted on a system:

1. **Logical Volume Configuration**
2. **Logical Volume Performance**

For Video Server Storage or SANs (storage area networks) Viakoo collects diagnostic data. They fall into the following categories:

1. **Configuration**
2. **Configuration-Related Conflicts and Issues**
3. **Unannounced Failures**

In addition, some storage systems provide more detailed diagnostic data than is typical. For example, for IntransaBrand™ EnterpriseStorage™ systems with StorStac™ software, the Viakoo RA Actor also collects the system hardware enclosure diagnostics, drive diagnostics and location, RAID disk groups, and iSCSI initiator configuration and performance measurements.

And for certain Windows Operating Systems using Intel Matrix Host Bus Adaptors (HBA) or LSI Logic MegaRAID HBAs, Viakoo RA collects similar drive diagnostics, location, and performance measurements.

VIDEO MANAGEMENT SOFTWARE APPLICATION DIAGNOSTICS

Diagnostics collected from the Video Management Software (VMS) application include data about camera streams and their related names, configurations, target storage locations, and retention goals for each camera. The Viakoo Reader Actor also collects VMS application configuration and logs, useful in diagnosing and resolving issues. Specifically, this includes:

1. VMS Product Data
2. VMS Event Data
3. Key Configuration Data

Read-only integration with either the VMS application or its database is required to obtain all of the above configuration information.

VIDEO STREAM EVENT CORRELATION

Event correlation is a technique for making sense of a number of events and pinpointing the few events or single event that are really important in that mass of information.

This is a proven approach in IT network and systems management, and is well defined in management frameworks and processes such as those found in ITIL. **However, no solutions have previously existed that can specifically and immediately correlate infrastructure events to video stream performance and the risk or realization of missing video conditions.**

Viakoo automated analysis provides the video-stream-specific impact that includes the problem location, affected device, and Probable Cause, instead of providing low-level culled from a log of raw data. This is how Viakoo's diagnostic reports enable **Collaborative Problem Resolution™** with all involved vendors, contractors and customer stakeholders—eliminating unnecessary truck rolls and blind troubleshooting.

This is the whole purpose of Viakoo's diagnostic data collection.

Conclusion

Timely Trouble Detection, Effective Correction Support, and Security

Very different from typical network monitoring applications, Viakoo detects problems along each video stream path and reports their location along with the probable cause. You don't have to waste staff or contractor time trying to correlate network or server events to camera views, or searching for hidden causes of video outages or missing recordings.

You get performance measures for the critical aspects of your IP video infrastructure, so that at any given moment you can see the overall status of your entire video infrastructure, and stay informed about the status of any active problem remediation efforts.

Viakoo customers can grant temporary login access to Viakoo for vendor and contractor troubleshooting personnel, to share diagnostic data about issues affecting the integrity of the video infrastructure. This enables **Collaborative Problem Resolution** with vendors, contractors and customer stakeholders in a secure way, eliminating unnecessary truck rolls, blind troubleshooting and finger-pointing.

A Safe and Secure Solution

As described in this paper, Viakoo provides a secure method to receive timely information about the availability, performance and integrity aspects of your IP video infrastructure, to put an end to the risk and cost of missing video.

The fundamental aspects of Viakoo's safe and secure operation are:

1. Only diagnostic data are collected from a customer's IP video infrastructure by digitally signed Viakoo Actors, and then sent securely via a short-duration outbound-only encrypted connection to Viakoo, which is which is rigorously secured with multi-layered defenses.
2. This diagnostic data can be securely shared with vendors, contractors and customer stakeholders without needing to provide access to the customer's IP video infrastructure.
3. Viakoo's Reader Actors and Communications Actors operate in low-priority mode to eliminate any significant impact on servers. For an entire video network infrastructure, data collections are relatively small and have no perceivable impact on network traffic loads.
4. Timely, accurate, and actionable data about video stream path integrity and video stream delivery quality translates into reduced vulnerabilities, improved availability, and resilience after unplanned disruptions.

These fundamental characteristics combine to assure that Viakoo maximizes customer-premise IP video infrastructure uptime, without introducing additional system risk or infrastructure management burden, while yet reducing the cost and effort expended to achieve high integrity and availability for security video.