Security Overview

Briefing to understand security implemented while collecting and processing performance metrics **2018**

The integrity of the Live Optics collector, security of the customer environment, and protection of customer data are issues of paramount concern in all elements of design of the Live Optics application. Security overrides all other concerns. As an example, many frequently-requested usability features have been rejected, as such features would compromise our strict security requirements.

Live Optics security areas can be divided into the following categories:

- Collector Integrity
- Collector Information-Gathering Protocols
- Collector Live Optics Web Service Security
- SIOKIT file security
- Live Optics Web Application Security
- Collector Security

Security begins with the Live Optics collectors. This section covers security issues pertaining directly to the Live Optics collectors.

Collector Integrity

The Live Optics collectors are native binary executables for the Windows and Linux platforms. These executables run in customer environments, often at elevated privilege levels. Guaranteeing the integrity of these collectors is of critical concern.

With the introduction of Live Optics, Dell has moved the Live Optics collector download to a login-protected, HTTPS (SSL) download link. By downloading the collectors directly, users know they are getting the collector directly from Dell. The Windows collector is digitally signed by Dell. The collector's internal meta-data is also signed to guarantee that the collector and the End User meta-data identifying the collector has not been altered.

Collector Information-Gathering Protocols

As the collector gathers information from the target servers or hardware appliance, the security ramifications of the underlying protocols are scrutinized.

First, any credentials provided to the collector for remote server access are never persisted in any kind of file or sent back to Dell in any format. Credentials are encrypted in memory using OS-defined methods, in the event that the collector's memory is paged to disk, or if the collector memory should otherwise be accessed.

For local Windows collection, the collector uses the PDH protocol and other Windows system API calls. The PDH protocol also could be used for remote collection. However, this protocol is not sufficiently secure when used remotely. So, for remote collection, the collector uses the remote WMI protocols. These protocols use the Windows remote Kerberos authentication to securely access the remote systems. Passwords are never transmitted in plain text.

In This Briefing

- Collector Security
- Protocols Used
- Securing the Online Analytics Portal

Security: continued

For remote Linux collection, the collector uses SSH to establish an encrypted secure shell with the target Unix system. The Windows collector only supports the latest SSH 2.0 key exchange methods.

The Linux collector uses the SSH module installed on the system where the collector runs. We advise users to update their SSH and underlying OpenSSL libraries to the most recent libraries.

For VMware collection, Live Optics uses VMware's SOAP based HTTPS API. This method uses HTTPS/SSL which is an encrypted communication stream. Live Optics uses the OpenSSL library for SSL communication. The library is updated routinely with the most recent updates from the OpenSSL development team.

Live Optics Web Service API Communication

Live Optics communicates (optionally) with Live Optics analytics servers using a SOAP based HTTPS protocol. The SSL stream is encrypted using the OpenSSL library. Again, the SSL libraries are updated to have the latest security patches from the SSL team. Additionally, the Live Optics Web Service API requires SSL Client Certificate Authentication. The SSL Client Certificate is embedded into the Live Optics collector as a part of the signed meta-data including the collector build.

Live Optics SIOKIT File Security

Live Optics SIOKIT files are encrypted with 2048 bit RSA and 256-AES keys. The key pairs are generated per collector. The private keys are secured within the Dell EMC Live Optics datacenter. The public keys are embedded into the collector.

Live Optics Web Application Security

The Live Optics web application was designed following the strict Dell EMC guidelines and has been scrutinized by both the internal Dell EMC Security Team as well as outside security experts.

Access to the site is via the secure and encrypted HTTPS framework. Latest security patches are routinely applied to all Live Optics servers.

While we do not disclose the design of our environment, the Live Optics datacenter consists of multiple layers of firewalled servers and communication frameworks. Data is securely stored behind numerous firewalled networks.

Dell Security policy prevents us from listing the exact methods we use to secure the site, but we can disclose that the Dell Security team routinely runs numerous leading 3rd party security applications that scan both the site and source code for vulnerabilities.

Anonymizing Data At the Source

The design of the Live Optics program allows each End User to own their own data, yet share it to trusted technical consultants to collaborate in infrastructure decision making processes or support cases. Most often the data is sent "as is", however, if one feels the need to mask server names by providing an alias then this can be accomplished in the collector itself prior to starting any data collection process.

To accomplish this you would use the /anon switch and start the collector from the command line. Similarly, in Linux/Unix variants you would use -- anon.

This will provide source side randomization of all server name, LUNs, or any other information that might be unique to internal naming conventions.

Security: continued

Collection and Web Service Protocols

Live Optics uses the following protocols to gather information from the supported target platforms and communicate with Live Optics Web Services:

Microsoft Windows PDH performance counter API

Only used for local Windows system collection

Microsoft Windows Registry APIs and other local system calls

Only used for local Windows system collection

Microsoft Windows Remote WMI

SSH

On Linux, the local ssh client is used

On Windows, a proprietary SSH stack implementation is used.

Used for remote Linux (and Solaris/HP-UX) collection

Uses bash shell commands on the target system to collect data (screen scraping)

VMware vSphere SDK API

HTTPS/SOAP XML protocol for communicating with vCenter servers

Live Optics Web Services API Client

HTTP/SOAL XML protocol compatible with Microsoft WCF Web Services that communicates with the Live Optics Web Services.

Linux Collection Details

Wherever possible, Live Optics tries to read the kernel sysfs files directly to get information rather than relying on the user-space tools. This is because the kernel file formats rarely change, while the user tools change frequently, making screen scraping difficult.

Such kernel files include:

- /proc/net/dev
- /sys/block/*
- /dev/*

/dev/mapper/*
Whenever possible, Live Optics tries to use tools that typically do not require root privileges.

Live Optics uses a variety of bash and sh commands too numerous to list here.

Security: continued

Data Gathered by Live Optics during a Host or OS level scan

The collectors gather information about each host system that they monitor:

- Operating System and version
- Hostname
- Domain Name of the server
- Date and time
- List of Installed Applications (optional)
- List of physical block devices (disks)
  - Advertised Capacity
  - Used Capacity
  - Serial Numbers (Shared Cluster Disk Information)
- List of network interfaces
  - Negotiated Speed
- CPU Configuration
  - Number of sockets
  - Number of cores
  - Clock speed
  - Model
- Server Model

During the monitoring session, Live Optics collects stats for the following:

- Disk performance
  - IOPS (reads/writes)
  - MB/s Throughput (read/write)
  - Avg. IO Size (reads/writes)
  - Avg. Latency (reads/writes)
  - Avg. Queue Depth
- Server performance
  - Memory usage
  - Virtual Memory Hard Page Faults per sec
  - CPU usage
- Network performance
  - Bytes received
  - Bytes sent

Windows PDH Collection Details

For Windows local collection, Live Optics uses the Microsoft PDH API. This API accesses the system performance counters. These are the same performance counters that PerfMon accesses. The following counters are used by Live Optics:

- PhysicalDisk/Disk Reads/sec
- PhysicalDisk/Disk Writes/sec
- PhysicalDisk/Disk Read Bytes/sec
- PhysicalDisk/Avg. Disk sec/Read
- PhysicalDisk/Avg. Disk sec/Write
- PhysicalDisk/Current Disk Queue Length
- Processor/% Processor Time
- Memory/Page Faults/sec
- Memory/Available Kbytes
- Network Interface/Bytes Received/sec
- Network Interface Bytes Sent/sec
- Hyper-V Hypervisor Logical Processor/Guest Run Time

Windows Remote WMI Collection Details

For remote Windows collection, Live Optics uses Microsoft WMI. WMI is notoriously unreliable. In many cases, we have to run Live Optics locally in order to bypass firewall and configuration issues associated with WMI. Live Optics uses the following WMI classes:

- Win32_ComputerSystem
- Win32_DiskDrivePhysicalMedia
- Win32_DiskDriveToDiskPartition
- Win32_DiskPartition
- Win32_LogicalDisk
- Win32_LogicalDiskToPartition
- Win32_NetworkAdapter
- Win32_NetworkAdpaterConfiguration
- Win32_OperatingSystem
- Win32_PerfRawData_PerfOS_Processor
- Win32_PerfRawData_Tcpip_NetworkInterface
- Win32_PhysicalMedia
- Win32_Processor
- Win32_SystemEnclosure
- Win32_PerfRawData_HvStats_HyperVHypervisorLogicalProcessor
- Win32_PerfRawData_PerfDisk_PhysicalDisk
- Win32_PerfFormattedData_PerfDisk_PhysicalDisk
- MSCluster_Disk
- MSCluster_DiskPartition
- MSCluster_DiskToDiskPartition
- StdRegProv

Understanding more about Live Optics

The Live Optics team is happy to conduct local or online training.

Our contact information can be found on the right in the blue area below!

The Live Optics site is located at https://LiveOptics.com

The Live Optics support site is located at https://support.liveoptics.com or by emailing support@LiveOptics.com

The Live Optics support site also has a vast library of other insightful attributes of Live Optics and can be located here:

https://support.liveoptics.com/forums

Contact Us

The Live Optics team can be contacted at the following address:

General Manager:
Sam Kirchoff
@SJKirchoff
Samuel.Kirchoff@Dell.com

Social Media
@runLiveOptics
#LiveOptics

live optics