DELL Technologies

live optics

Security Technical Brief

Contents

Copyright Statement

Revision History

Date	Document Revision	Description of Changes
September 2024	1.2	Added SSL certificate notes to *Optical Prime*, *Nutanix*, *Kubernetes*, *RVTools*, *PowerScale/Isilon*, *NetApp*, *PowerStore*, *Pure*, *SC*, *Unity*, *XtremIO*, *NetWorker*, and *PowerProtect DM*.
August 2024	1.1	• Added Kubernetes and RVTools sections under *Server and Cloud* • Added *FAQ* section
March 2024	1.0	Initial version

About This Document

This document is intended to provide Live Optics users with information about security measures employed during collections using the Live Optics collector. For more information contact security.and.customer.trust@dell.com.

Live Optics Overview

Live Optics is a free software tool that inventories and analyzes your current IT environment for the purpose of infrastructure planning activities. It automatically collects real-time metrics on storage, servers, and data protection. Using an intuitive dashboard and detailed graphs, it delivers a holistic view of your IT environment. It helps to better understand your environment, optimize your IT investments, and improve your overall system capacity and performance.

Live Optics collects information from all vendors, hardware types, operating systems, and platforms, making it especially useful in multi-vendor and multi-cloud environments. It also provides pricing comparisons for public cloud solutions, including Amazon AWS, Google Cloud, and Microsoft Azure.

Server and Cloud
View live bare-metal server and virtual machine inventory, configuration, and performance telemetry.

File
Insight into unstructured data through rapid characterization of storage growth, file types, and predictive potential for archive, compression, and reducibility.

Storage
View detailed vendor and model specific storage hardware, including inventory, configuration, and performance history.

Data Protection
Insight into vendor specific backup software and appliances, data protection configuration, cycles and policies, and the front-end capacity of protected systems.

Workloads
Generate summaries of supported databases, capacity reports, and performance metrics.

There are two Live Optics collector download options available:

- **Corporate Edition** - This version requires registration with a corporate email address for access to all Live Optics configuration and performance data collection options.
  See Download the Live Optics collector or Download the Live Optics collector (Linux) to get started.

- **Personal Edition** - This version does not require registration with an email address but offers only a limited selection of data collection options. See Download the Live Optics Personal Edition collector for more information.

Live Optics Security Overview

What information does Live Optics collect?

Live Optics collects metadata information only. Metadata provides contextual information which is used to classify, organize, and understand data, and helps to provide meaningful insights into user environments. Live Optics does not read or collect personal information or read application data or user files (see Dossier exception below).

For example, during a storage array collection, Live Optics gathers information including the number of volumes, volume names, and volume properties including capacity, but never reads the actual information stored on the volumes.

NOTE: Dossier reads application information (for example, file names and, optionally, file content) in certain circumstances as part of its scanning operation. See Dossier for further information.

Collection Types

Live Optics collects information using two methods:

- **API Based Collection** - connects to a system (for example, a storage array or data protection appliance) using a network protocol, such as REST API.
- **File Based Collection** - uses files manually retrieved from systems which are then uploaded to the Live Optics collector.

It is recommended that API based collection is used where possible. APIs are the most secure method of gathering information. Generally, only necessary information and metrics are gathered when using APIs, and the overall user experience is more streamlined.

Live Optics Collector Security

The Live Optics collector is downloaded using a login-protected HTTPS (SSL) link. The collector and its respective metadata are digitally signed by Dell to guarantee that it, and any user metadata identifying the collector, has not been altered. The Live Optics collector application is developed under strict Dell DevSecOps security guidelines and is continuously updated with the latest security patches and best practices for secure SSL connections.

Web Service API Communication

The Live Optics collector communicates (optionally) with Live Optics analytics servers over the internet using a secure HTTPS/SSL protocol.

Web Portal Security

The Live Optics web portal was designed following strict Dell security guidelines. It is accessed using a secure and encrypted HTTPS framework. Live Optics servers are routinely updated with the latest security patches. The Live Optics datacenter consists of multiple layers of firewalled servers and communication frameworks. Collections are securely stored behind firewalled networks and are encrypted at rest. The Dell security team routinely scan both the site and source code for vulnerabilities.

Live Optics SIOKIT File Security

An SIOKIT file is an encrypted file the Live Optics collector creates if you choose to store your collection information on your local system. This option is typically used when an internet connection is not available to automatically transmit collected information directly to the Live Optics datacenter for processing. Instead, an SIOKIT file must be manually uploaded to the Live Optics datacenter where it is converted into a project for viewing.

When you download the Live Optics collector it is linked to your account with an embedded RSA key. This public key is used to encrypt and sign SIOKIT files, so that Live Optics can identify the source of an SIOKIT file and associate it with a specific user account. Live Optics SIOKIT files are encrypted with 2048-bit RSA and 256-AES keys. The private key is securely stored in the Live Optics datacenter, so the SIOKIT file cannot be decrypted outside of Live Optics. Key pairs are generated on a per-collector basis for each download.

For information on uploading SIOKIT files after a Live Optics collection, see:

- Upload an SIOKIT file from the Live Optics collector
- Upload an SIOKIT file from the Live Optics web portal

Anonymizing Collections

Live Optics users own their information and can share it with trusted Live Optics technical consultants to collaborate on IT infrastructure decision making processes or support cases. Typically, collection information is sent in its raw format. However, if required, resource names (for example, servers, disks, and LUNs) can be obfuscated prior to running a collection.

NOTE: The option to anonymize collection information is available for Optical Prime project reports only.

Starting Live Optics from the command prompt using */anon* (Windows) or -- *anon* (Linux/Unix) provides source-side randomization of all server, disk, and LUNs identities, and any other information that might be unique to internal naming conventions. Additionally, when a project is shared, there is an option to anonymize the project information for the recipient.

Server and Cloud

Optical Prime

Optical Prime gathers inventory, configuration, and performance metrics for physical and virtual servers, desktops, and hypervisors. The Live Optics collector connects to local and remote hosts running operating systems including Windows, Linux, and hypervisors including VMware vCenter, Microsoft Hyper-V, KVM, and Xen.

Information types collected include hostnames, operating systems, CPU and memory configurations, storage and disk configurations, hypervisor information such as guest virtual machines, network configurations, IP addresses, and lists of installed applications.

Optical Prime collections can be run from 10 minutes to 7 days and gather information from host systems. The application runs in system memory only and does not make any modifications to your system or the system from which information is collected.

NOTE: As Optical Prime runs in system memory only, its collections are session sensitive. Logging out or rebooting your host system will terminate an Optical Prime collection in progress.

Optical Prime scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.
- **Written to a local Microsoft Excel spreadsheet** – *Inventory Mode* creates a summary of hardware, operating systems, and virtual machines hosted by hypervisors. No performance information is collected.

Windows Collection

Optical Prime uses the Microsoft WMI (Windows Management Instrumentation) protocol to collect information from Windows systems. This protocol uses TCP port 135 for the initial connection, before switching to a randomly selected TCP port between 49152 and 65535 for collection. Some environments with more recent Windows Server operating system versions can be configured to use a fixed TCP port. WMI is encrypted and secure.

Linux Collection

Optical Prime uses the SSH (Secure Shell) protocol to remotely connect to Linux systems. By default, SSH uses TCP port 22. Once the shell is established, Optical Prime runs several commands to collect information. SSH is encrypted and secure.

VMware Collection

Optical Prime can scan entire VMware deployments by connecting to a VMware vCenter system. It uses the VMware vSphere SOAP API which runs over the encrypted and secure HTTPS/SSL protocol

and is typically configured over TCP port 443. However, in cases where the deployment is using a custom override port, you may specify a custom port number instead.

Optical Prime establishes a connection to the VMware vCenter system only and does not directly communicate with any ESXi hosts.

NOTE: Optical Prime supports VMware collections by connecting to VMware vCenter only. VMware deployments without vCenter are not supported.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on VMware vCenter server and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the vCenter server. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

RAPID Discovery

RAPID Discovery scans host environments to identify network objects including servers, laptops, switches, printers, and storage arrays. It is designed to easily generate a holistic view of an environment to reveal insights that may be difficult to identify particularly in large deployments.

RAPID Discovery performs scans using Active Directory and network port scanning techniques. WMI and SSH protocols are used to obtain additional detail about the discovered network objects.

NOTE: The Live Optics collector does not transmit information during or after a RAPID Discovery session.

Active Directory Scan

A query is completed for the Secure LDAP (SLDAP) addresses provided. Currently, only Windows Servers and Linux entries are selected. For each result, a DNS lookup is performed to retrieve its IP address. SLDAP is encrypted and secure.

Network Scan

The Live Optics collector pings each IP address from a user-specified IP range. A DNS lookup is performed to retrieve hostnames and MAC addresses. The NIC vendor is obtained from a lookup table.

WMI

WMI scans use credentials specified in credential groups and retrieves management information. Using the IP address and selected credential groups, an authentication attempt is made for each selected device with each credential pair until authentication is successful. A set of WMI commands are executed and the results are displayed in a downloadable Microsoft Excel file containing information and states collected for all discovered devices.

WMI uses TCP port 135 for the initial connection, before switching to a randomly selected TCP port between 49152 and 65535 for collection. Some environments with more recent Windows Server

operating system versions can be configured to use a fixed TCP port. WMI is encrypted and secure.

SSH

SSH scans leverage the Secure Shell protocol over TCP port 22 using credentials specified in credential groups. Using the IP address and selected credential groups, an authentication attempt is made for each selected device with each credential pair until authentication is successful. A set of SSH commands are executed and the results are displayed in a downloadable Microsoft Excel file (for the host on which the scan was performed) containing information and states collected for all discovered devices.

Amazon Web Services (AWS)

AWS scans gather inventory details for EC2, S3, Glacier, EFS, RDS, ECS, and EKS services.

To begin an AWS scan, enter your *Access Key ID* and *Secret Access Key* credentials. *Secret Access Keys* are used with the *Access Key ID* to cryptographically sign AWS requests. This process identifies the sender and prevents a request from being altered. You can generate Secret Access Keys for your AWS account, individual IAM users, and temporary sessions.

For information on creating a temporary user account with relevant permissions for a Live Optics collection, see Create a temporary AWS IAM user for Live Optics collection.

Once your credentials are authenticated, a HTTPS connection to AWS is established and information is collected.

AWS scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.
- **Written to a local Microsoft Excel file** – *Inventory Mode* collects configuration and status information for all EC2 instances, S3 buckets, EFS, and RDS instances across multiple regions. No performance information is collected.

Microsoft Azure

Microsoft Azure scans gather inventory details for Azure VMs, Scale Sets, Storage Accounts, and Azure SQL Database services.

To begin an Azure scan, enter your *Client ID*, *Client Secret*, *Tenant ID*, and *Subscription ID* credentials. Once your credentials are authenticated, a HTTPS connection to Azure is established and information is collected.

Azure scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over port 443 with Dell servers and information is transmitted when the collection is complete.

- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.
- **Written to a local Microsoft Excel spreadsheet** – *Inventory Mode* collects configuration and status information. No performance information is collected.

Nutanix

Nutanix collections provide inventory and performance information for clusters, hosts, VMs, and vDisks. Collection details represents the past 7 days of use.

NOTE: Only one Nutanix cluster can be scanned at a time. Nutanix Prism Central is not currently supported.

To begin a Nutanix scan, enter your *Prism Element IP address* and credentials. Authentication against Nutanix REST APIs uses HTTP Basic Authentication. Requests on HTTP TCP port 80 are automatically redirected to HTTPS on TCP port 9440.

Nutanix scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the Nutanix Prism Element and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the Nutanix Prism Element. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

Kubernetes

Kubernetes collections provide inventory information for multiple clusters.

NOTE: You must have a valid *kubeconfig* file before beginning a Kubernetes scan. You can use an existing *kubeconfig* file or create a temporary service account to generate a new one. See Create a service account with Kubectl or Create a service account for a Red Hat OpenShift environment for more information.

By default, the Kubernetes API server listens on port 6443 on the first non-localhost network interface, protected by TLS. In a typical production cluster, the API uses port 443, however, custom ports can be specified. Contact your system administrator for more information.

To begin a Kubernetes scan, upload a *kubeconfig* file in the Live Optics collector.

Kubernetes scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.
- **Written to a local Microsoft Excel spreadsheet** – *Inventory Mode* collects configuration and status information and saves it locally. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the Kubernetes API service and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the Kubernetes API service. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

RVTools

RVTools collections provide inventory, configuration, and status information for VMware deployments. It is run against VMware vCenter servers or can directly target ESXi hosts.

NOTE: To complete an RVTools collection, visit www.robware.net/download to download and install the free RVTools application (you do not need to register for an account). For more information see the RVTools User Guide.

To begin an RVTools scan, you can:

- Launch the installed application and run the collector against your selected targets (vCenter servers or ESXi host)
- Run the application using the command line against your selected targets
- Run scheduled scripts (non-interactive mode) to scan your selected targets

RVTools scans VMware deployments by connecting to a VMware vCenter system or an ESXi host. It uses the VMware vSphere SOAP API which runs over the encrypted and secure HTTPS/SSL protocol and is typically configured over TCP port 443. However, in cases where the deployment is using a custom override port, you may specify a custom port number instead.

All credentials used to communicate with the VMware vCenter or ESXi host are encrypted using Windows Data Protection API. If you use either the command line or scheduled scripts options to run RVTools, you must use the encryption tool provided to protect your passwords before you proceed.

RVTools scan results can be exported to a Microsoft Excel spreadsheet or CSV file. The Excel file can be uploaded to the Live Optics web portal to generate an AIR report. This output provides easy to read results which are displayed in insightful graphs and tables.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on VMware vCenter server and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the vCenter server. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

File

Dossier

Dossier scans unstructured file system information using file characterization techniques and provides useful insights into capacity utilization and compression of your file systems and directories.

NOTE: Dossier *always* reads file names during a scan regardless of which scan options are selected.

A *.dossier* file is downloaded to your computer when a scan is completed. This file contains summary information which is used to generate the final Dossier PowerPoint report. This information includes the names of the file systems (or file shares) scanned, file extensions observed most frequently, number of files by category, and other summary metrics.

NOTE: Dossier only reads file information if the **Test for Compressibility** option is selected before a scan. Sections of some files are read to determine how the data can be compressed, and only a selection of larger files are tested for a more accurate compressibility estimation. If compressibility testing is not selected before a scan, no file information, apart from files names, is read.

The *.dossier* file must be manually uploaded to the Live Optics dashboard to view the results. For information on completing a Dossier scan and uploading a *.dossier* file, see:

- Complete a Windows Dossier scan
- Complete a Linux Dossier scan

Dossier collections are completed on the host machine running the Live Optics collector. No information is transmitted during a Dossier session.

Storage

API Based Collection

IBM Storwize

The Live Optics collector gathers configuration and performance information for IBM Storwize storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration from 10 minutes to 3 days for which the Live Optics collector will run and gather real-time performance details.

NOTE: Only one IBM Storwize storage array can be scanned at a time.

To begin an IBM Storwize storage array scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A secure SSH connection is established between the Live Optics collector and the IBM Storwize array over TCP port 22.

IBM Storwize scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

PowerScale/Isilon

The Live Optics collector gathers configuration and performance information for PowerScale/Isilon storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration from 10 minutes to 24 hours for which the Live Optics collector will run and gather real-time performance details.

NOTE: Only one PowerScale/Isilon array can be scanned at a time.

To begin an PowerScale/Isilon scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A HTTPS connection is established between the Live Optics collector and the PowerScale/Isilon array over TCP port 8080.

PowerScale/Isilon scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the PowerScale/Isilon cluster and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the PowerScale/Isilon cluster. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

NetApp

The Live Optics collector gathers configuration and performance information for NetApp storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration from 10 minutes to 3 days for which the Live Optics collector will run and gather real-time performance details.

NOTE: Only one NetApp storage array can be scanned at a time.

To begin a NetApp storage array scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A secure SSH connection is established between the Live Optics collector and the NetApp array over TCP port 22, and HTTPS/SSL over port 443. For custom SSH ports, use the format *address:port*.

NetApp scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the NetApp appliance and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the NetApp appliance. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

PowerStore

The Live Optics collector gathers configuration and performance information for PowerStore storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration for which the Live Optics collector will run and gather real-time performance details (the default selection is 48 hours).

NOTE: Only one PowerStore array can be scanned at a time.

To begin a PowerStore scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A HTTPS connection is established between the Live Optics collector and the Isilon/PowerScale array over TCP port 443.

PowerStore scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the PowerStore appliance and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the PowerStore appliance. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

Pure

The Live Optics collector gathers configuration and performance information for Pure storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration from 1 hour to 7 days for which the Live Optics collector will run and gather real-time performance details.

NOTE: Only one Pure storage array can be scanned at a time.

To begin a Pure scan, chose a collection method:

- **FlashArray (REST API 2.x)** for Purity firmware 5.3 and above. This option uses RSA SSL key based authentication. Enter a *DNS Name* or *IP Address*, *Issuer*, *Client ID*, and *Key ID*. A secure HTTPS/SSL connection is established between the Live Optics collector and the Pure array over TCP port 443 by default. For custom TCP ports, use the format *address:port*.

- **FlashArray (REST API 1.x)** for Purity firmware 5.2.6 and older. This option uses username/password-based authentication. Enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A secure HTTPS/SSL connection is established between the Live Optics collector and the Pure array over TCP port 443 by default. For custom TCP ports, use the format *address:port*.

Pure scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.

- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the Pure appliance and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the Pure appliance. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

SC

The Live Optics collector gathers configuration and performance information for SC storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration for which the Live Optics collector will run and gather real-time performance details.

To begin an SC scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A HTTPS connection is established between the Live Optics collector and the SC array over TCP port 3033.

SC scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the DSM server and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the DSM server. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

Unity

The Live Optics collector gathers configuration and performance information for Unity storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration for which the Live Optics collector will run and gather real-time performance details.

To begin a Unity scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A secure HTTPS/SSL connection is established between the Live Optics collector and the Unity array over TCP port 443 by default. Users can also specify a custom port.

Unity scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the Unity appliance and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the Unity appliance. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

XtremIO

The Live Optics collector gathers configuration and performance information for XtremIO storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration for which the Live Optics collector will run and gather real-time performance details.

To begin an XtremIO scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A secure HTTPS/SSL connection is established between the Live Optics collector and the XtremIO array over TCP port 443 by default. Users can also specify a custom port.

XtremIO scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the XtremIO XMS server and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the XtremIO XMS server. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

HPE 3PAR

The Live Optics collector gathers configuration and performance information for HPE 3PAR storage arrays. You can choose to collect configuration information only, or configuration and performance information together. For configuration and performance collections, select the duration between 3 and 7 days for which the Live Optics collector will run and gather real-time performance details.

NOTE: Only one HPE 3PAR storage array can be scanned at a time.

To begin a HPE 3PAR storage array scan, enter a *DNS Name* or *IP Address*, *Username*, and *Password*. A secure SSH connection is established between the Live Optics collector and the 3PAR array over TCP port 22.

HPE 3PAR scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

File Based Collection

VNX/CLARiiON

The Live Optics collector gathers configuration and performance information for up to 7 days for VNX/CLARiiON storage arrays. You can choose to collect configuration information only, or configuration and performance information together.

To begin a VNX/CLARiiON scan, select a *.NAR (or .NAZ)* file for performance information, and an *SPCollect.zip* file for additional configuration information.

VNX/CLARiiON scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** - collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

VMAX/PowerMax

The Live Optics collector gathers configuration and performance information for up to 7 days for VMAX/PowerMax storage arrays. You can choose to collect configuration information only, or configuration and performance information together.

To begin a VMAX/PowerMax scan, select a *.symapi_db.bin* file for configuration information, and a *.BPT* or *.TTP* file (for legacy VMAX arrays) or a *.DCF* file (for PowerMax version 3 and 4 arrays) for performance information.

VMAX/PowerMax scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

Data Protection

API Based Collection

NetWorker API

The Live Optics collector gathers configuration and performance information for NetWorker (v19.1 and above).

To begin a NetWorker scan, enter an *IP Address*, *Username*, and *Password*. A HTTPS/SSL connection is established between the Live Optics collector and NetWorker over TCP port 9090.

NetWorker scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the NetWorker server and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the NetWorker server. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

PowerProtect DM

The Live Optics collector gathers configuration and performance information for PowerProtect DM.

To begin a PowerProtect DM scan, enter an *IP Address*, *Username*, and *Password*. A HTTPS/SSL connection is established between the Live Optics collector and PowerProtect DM over TCP port 8443.

PowerProtect DM scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

NOTE: Currently, the Live Optics collector ignores invalid or self-signed SSL certificates on the NetWorker server and a warning message is not displayed to users. This may put users at risk of potential man-in-the-middle attacks where an adversary gains control of the network between the Live Optics collector and the NetWorker server. In this scenario, usernames and passwords may become compromised. In future, Live Optics will display a warning message to users where invalid or self-signed SSL certificates are detected.

File Based Collection

Avamar

The Live Optics collector gathers configuration and performance information for Avamar.

To begin an Avamar scan, select an *sql.gz* file to upload to the Live Optics collector. This file contains a backup of your selected database. A small subsection is scanned to produce a viewable Live Optics project. No database information is read or transmitted to Live Optics servers during or after the collection is complete.

Avamar scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

PowerProtect Data Domain

The Live Optics collector gathers configuration and performance information for PowerProtect Data Domain.

To begin a PowerProtect Data Domain scan, either:

- Browse for an Auto-support (ASUP) file to upload to Live Optics from an existing folder.

- Scan for an ASUP file by entering a PowerProtect Data Domain system *IP Address*, and your *Username* and *Password*. The ASUP file is automatically retrieved from PowerProtect Data Domain using a secure SSH connection over TCP port 22.

No database information is read or transmitted to Live Optics servers during or after the collection is complete.

PowerProtect Data Domain scan results can be:

- **Uploaded to the Live Optics datacenter** - a secure HTTPS/SSL connection is established over TCP port 443 with Dell servers and information is transmitted when the collection is complete.
- **Saved to an SIOKIT file** – collection details are saved to a local SIOKIT file which must be manually uploaded to the Live Optics portal before collection results can be viewed. No outbound connection is made by the Live Optics collector.

Workloads

Microsoft SQL Server

Live Optics supports two information collection methods for Microsoft SQL Server:

- Remote WMI using Optical Prime
- Remote SQL Connection

Remote WMI using Optical Prime

When targeting Microsoft Windows servers with Optical Prime, the Live Optics collector automatically detects Microsoft SQL Server installations and issues a series of SQL specific WMI queries. These calls use the same WMI protocol as described in the Optical Prime section. For more information see Windows Collection.

Remote SQL Connection

This method establishes an SQL database connection over a secure and encrypted channel. By default, TCP port 1433 is used, however, custom ports can be specified.

Dark Sites

For environments where Internet usage may pose a security risk, offline and inventory collections are recommended. For configuration information, Optical Prime and RAPID Discovery offer inventory mode collections which are saved locally only.

FAQ

About Live Optics

What is Live Optics?
Live Optics is free, remote, agentless software provided by Dell Technologies that collects configuration and performance data from your IT environment. It streams workload data from storage, data protection, servers, and file systems to an online analytics engine, analyses your workload characteristics, and offers valuable performance information in insightful graphs and reports.

How is Live Optics software used in the industry?
Live Optics is available in 160 countries, and approximately 15,000 datacenter scans are completed each month. Live Optics is also used by almost all Dell Technologies channel partners to gather and communicate requirements.

Is Live Optics complicated?
Live Optics is a simple point and click application that does not require installation on your system.

Does Live Optics require an agent?
The Live Optics collector runs in memory, does not need to be installed, and communicates with all endpoints without an agent. Windows, Linux, VMware, Hyper-V, Linux, HPUX, and Solaris are all supported natively.

Does Live Optics create a workload and/or consume resource?
Servers are constantly logging performance activity. Live Optics simply collects and analyzes this data. Even in large scale collections a workload on the target is almost untraceable. The Live Optics collector then streams the data to the Live Optics servers for analysis. This data is highly compressed and minimally traceable on the network.

Does Live Optics do more than just server/virtualization assessments?
Yes, Live Optics can also complete data protection, file, storage, workload, and cloud assessments.

What data is collected by Live Optics?
Live Optics collects telemetry data (performance data) and configuration data of the hardware supporting the OS. For virtual environments, a full analysis of the VMs and hypervisor performance is completed.

What is the Live Optics privacy policy?
Live Optics does not have a privacy policy. Live Optics is a Dell Technologies product and follows the Dell Technologies Privacy Policy.

What if I am a Federal or DoD entity?
For configuration data use Inventory mode. For performance data, contact support@liveoptics.com and request an *offline Federal/DoD license* to open an .SIOKIT file. This is only issued to customers where data cannot be transmitted back to Live Optics servers, or where other business exceptions exist. This service is not available for data protection or storage.

Access Privileges and Controls

Who can see or have access to customer data via the Live Optics application?
Customer data can only be viewed by registered users from the customer's organization. A customer may elect to share this data with Live Optics users. Live Optics application administrators also have access to this data.

What actions and internal controls are in place to prevent unauthorized viewing of customer information?
At an application-level, Role Based Access Control (RBAC) is implemented. Access to the Live Optics infrastructure is limited to Live Optics Site Reliability Engineers (SREs). Live Optics also utilizes a feature called "Teams" to ensure customer data is visible to that customer alone.

What audit log is available for customers and what is the retention period?
No audit log is available for customers to manage.

Is an IAM solution integration for automated provisioning/de-provisioning customer user accounts supported?
There is no automated process, however customer user accounts can be removed by Live Optics support. Customer team administrators may also remove users from teams.

What policies are implemented for any third party hosted applications?
Live Optics complies with Dell's public cloud and cybersecurity policies in relation to using third party cloud platform and services.

Business Continuity

What is the disaster recovery process?
Databases are running in multi-datacenters with built in redundancy. Our application servers are automated with one-click deployment and can be deployed in any datacenter within a few minutes.

Data Backup and Recovery

How is the data backed up?
Backups of data are carried out as per internal Live Optics policy.

How many copies of the data are stored, and where are they stored?
Multiple copies of backups are stored for 90 days in a backup vault.

How often are backups tested?
As per internal policy.

What is the retention period for backups?
90 days.

Data Remanence

How is the data purged, so that the data is deleted completely, and there are no remnants of deleted data, therefore, not subject to attack or e-discovery?
An automated deletion process is in place to delete data after 7 years.

In case of termination of the contract, will the data be provided back to the customer?
Raw data is not returned to the customer; however, reports may be downloaded by the customer for all projects owned in Excel and PowerPoint format.

Encryption Requirements

How is 'Data in Transit' encrypted?
Data communications are encrypted using industry approved protocols, protecting data in transit.

How is the data encrypted at rest? What type of encryption is used?
All Live Optics data technologies automatically apply encryption for data at rest.

What technology is used to encrypt data backups and how are those keys managed?
Data backups are encrypted and stored using a backup vault.

Are all client-to-server data transmissions also encrypted?
Data transmitted over public networks is encrypted using industry standard protocols.

How are the encryption keys managed?
Certificates used in Live Optics are stored within the organization vault utilizing IAM controls. A certificate rotation policy is in place.

Incident Management and Response

How are incidents handled?
Dell has multiple teams handling incidents depending on the type of incident. Robust processes are in place.

Would a customer receive a notification if a data breach is detected?
Yes.

What access is provided to logs? Would a customer be provided with logs from an incident?
Live Optics logs are not provided to customers.

Network and Application Security

Do you perform vulnerability scans on the application?
All Dell networked systems are scanned periodically. Additionally, vendor and industry sites are monitored for vulnerability announcements, patch, and non-patch remediations, and any emerging threats on a periodic basis. Frequency of these scans depends on asset type and criticality. Live Optics undergoes routine application vulnerability scans.

Do you have an internal, external, or red team performing annual penetration tests of your IT environment?
Penetration tests on external and internal networked systems are performed periodically by Dell's internal Red/penetration testing team. Also, if required by compliance requirements, Dell uses third-party vendors (S3Security for PCI, and Whitehat for penetration testing). The Red Team is part of the Security and Resiliency Organization (SRO). The SRO has defined roles and responsibilities for security

and resiliency management, which includes vulnerability management and penetration testing. Dell's Chief Security Officer (CSO), authorized by Dell executive management, reports directly to the General Counsel, and oversees and directs a comprehensive security and resiliency program. This includes cybersecurity for all systems, data and networks, product security, physical security, supply chain security, and enterprise resiliency.

What steps have been taken to ensure the applications are secured from application-level attacks like XSS and SQL injection?
Dell's Secure Development Lifecycle integrates standards from a variety of data sources. A primary consideration is data from both internally discovered and externally reported issues. This awareness allows us to focus on the issues that are most prevalent in our technology space.
A second major consideration is industry practices. Dell collaborates through many industry-standard venues such as SAFECode, BSIMM, and IEEE Center for Secure Design to ensure that we follow industry practices. Lastly, Dell's Secure Development Lifecycle is aligned with the principles outlined in ISO/IEC 27034 information technology, security techniques, and application security.

Do you regularly perform vulnerability threat assessments, penetration testing, and code reviews? Are these performed by an independent third party?
Yes. Penetration testing is performed by a third party.

What measures are in place to mitigate Denial of Service (DDoS) attacks?
All public endpoints are behind a gateway which implements firewall rules protecting against such attacks as DDoS.

Software Development

What is the development lifecycle process?
Live Optics follows a Secure development Lifecyle aligning to ISO/IEC 27034 principles, including, but not limited to, code reviews, security scans, testing, logging, and automated pipelines.