live optics

RAPID Discovery

Inventory your network for enhanced business insights

live optics

Contents

live optics

Live Optics Overview

Live Optics is an industry-standard method of impartially documenting configuration and performance as well as observing file characteristics of unstructured data. It is free, online software you can use to collect, visualize, and share data about your IT environment and workloads, to help you make real-world IT decisions. Live Optics offers solutions such as:

Server and Cloud: **View live inventory and performance insight of hosts and VMs, regardless of platform or vendor. View inventories and basic performance statistics, dive into deeper performance metrics over time, and examine individual servers, disk, and virtual machines.**

Workloads: **Generate summaries of SQL Server and Oracle databases, in addition to capacities and critical and performance metrics.**

Storage: **View detailed breakdowns at the hardware appliance level of configuration and performance.**

Data Protection: **Produce insights into platform-specific backup and protection cycles as well as protected capacity.**

File: **Characterize storage growth, file types and potentials for archiving, compression, or deduplication.**

live optics

RAPID Discovery Overview and Security

Purpose

RAPID Discovery is designed to easily generate a holistic view of an environment or specified range to reveal insights that might be difficult to identify in large deployments. It is a feature of the Live Optics Collector that scans an environment to identify network devices (servers, laptops, switches, printers, storage arrays, etc.) and represents them as a set of objects that can be manipulated by filtering and sorting.

Discovery Mechanisms

RAPID Discovery performs scans using Active Directory and network port scanning techniques. These techniques can be classified as *mandatory* and *elective*.

Mandatory methods:

Mandatory methods are used in the core discovery operations and include the following:

- **DNS (Domain Name System), a service/protocol that translates host names to IP addresses and vice versa.**
- **ICMP (Internet Control Message Protocol), used to ping remote hosts.**
- **ARP (Address Resolution Protocol), used to find network card's MAC address for a given IP address, and vice versa.**

Elective methods:

Elective methods are optional methods by which additional details about the discovered network objects can be obtained. These methods include the following:

- **LDAP (Lightweight Directory Access Protocol) used to access distributed directory services.**
- **Kerberos is a computer-network authentication protocol that allows nodes to prove their identity to one another in a secure manner.**
- **WMI (Windows Management Instrumentation) Remote Protocol, used to query remote Windows devices.**
- **SSH (Secure Shell) used to securely execute remote commands.**

Security Considerations

Credential Manager and Credential Groups

RAPID Discovery allows you to create multiple Credential Groups. A Credential Group can contain one or more credentials. A credential consists of a username and password pair, requested via a native Windows Security dialog. Credentials are kept encrypted in memory and discarded when the software is closed. See Appendix A: Usage Guide for more detail on the Credential Manager.

Notes on security events

During execution, multiple authentication attempts and port scans can be performed. Security mechanisms and intrusion detection systems might create security events. For more detail, see the Operational and Protocol Details section of this document.

Please consult with your security administrators before running RAPID Discovery.

Features

Import/Export Configuration

The Live Optics Collector generates (and can import) a user readable JSON (Java Script Object Notation) file containing states and information gathered for all discovered devices.

Report Generation

RAPID Discovery includes the ability to produce a report (Microsoft Excel format) of discovered network objects.

Notes on privacy implications

Host names, usernames, IP addresses and operating systems can appear in the reports. Appropriate information security measures should be taken with these reports.

Operation and Protocols

Network Scan

From a user-specified IP range, the collector pings (via the IMCP protocol) each IP address. For each success, a DNS lookup is performed to retrieve the hostname and MAC address

via ARP (Reverse Address Resolution Protocol). The NIC (network interface cards) vendor is derived from a lookup table embedded in the Live Optics Collector.

Active Directory Scan

A query for Computers against the given LDAP address path is performed. Currently, only Windows Servers and Linux entries are selected. For each result, a DNS lookup is performed to retrieve its IP address.

SSH Scan

An SSH scan leverages the Secure Shell protocol 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 succeeds. Then a set of SSH commands is executed and the results are parsed. The gathered data can be seen in the exported configuration file.

Examples of commands executed:

- `hostname`
- `uname -s`
- `cat /proc/version`
- `df -lPaT`
- `dmidecode -t 1`

WMI Scan

A WMI scan employs the Windows Management Instrumentation protocol using credentials specified in Credential Groups and retrieves management data. Using the IP address and selected Credential Groups, an authentication attempt is made for each selected device with each credential pair until authentication succeeds. Then a set of WMI commands (see examples below) is executed and the results are parsed. The gathered data can be seen in the exported configuration file.

Examples of commands executed:

- `SELECT * FROM Win32_OperatingSystem WHERE Primary=true`
- `SELECT * FROM Win32_Processor`
- `SELECT * FROM Win32_DiskDrive`
- `SELECT Domain, Name, Model, Manufacturer FROM Win32_ComputerSystem`

live optics

Conclusion

The RAPID Discovery feature is an ideal complement to the existing solutions in the Live Optics Collector. It extends the perspective of network administrators and can be used as input into refresh cycles, business decisions and considerations for other Live Optics scans.

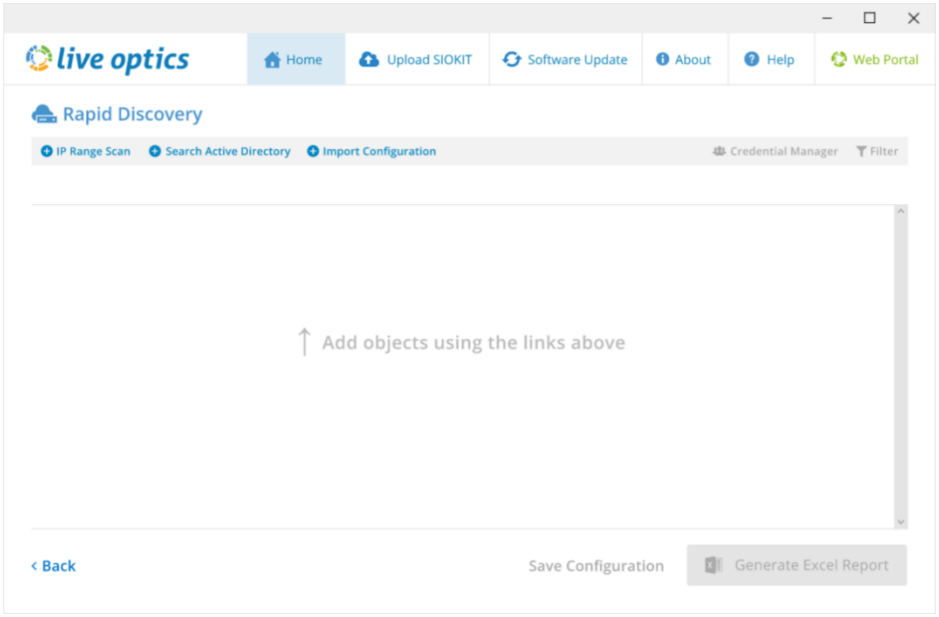
Appendix

Appendix A: Usage Guide

This appendix provides step-by-step instructions to perform RAPID Discovery scans.

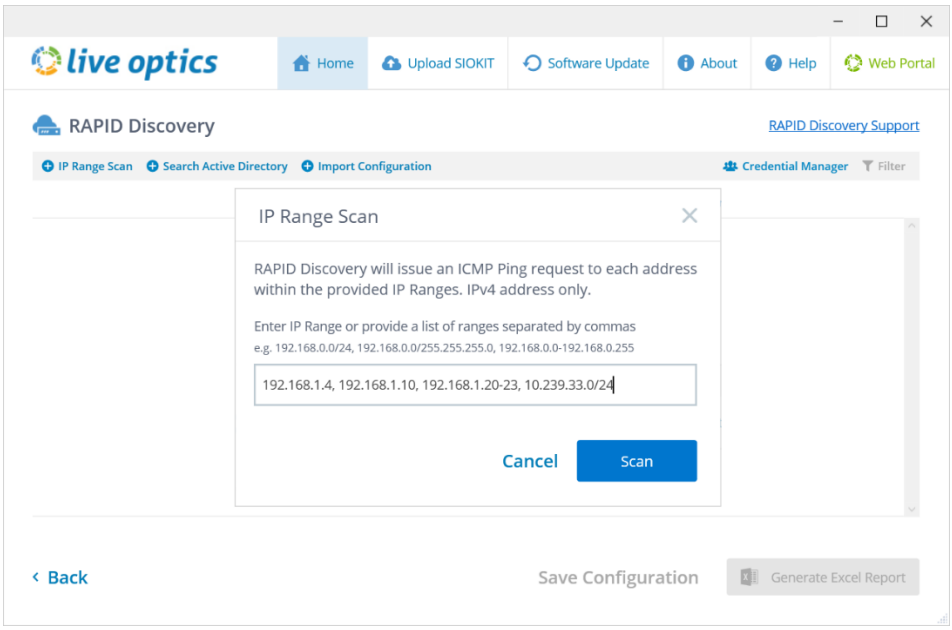
1. **To run RAPID Discovery, download the Live Optics Collector. The Live Optics Collector is updated frequently, so please ensure you are running the latest version.**

2. **Click through the introductory screens of the Live Optics Collector application and navigate to the main screen for RAPID Discovery:**

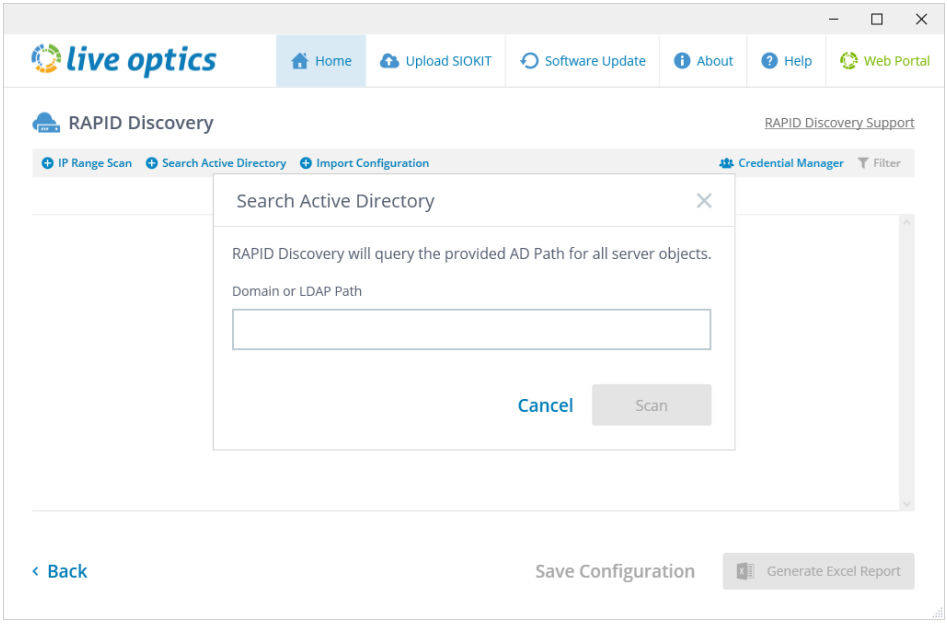


3. **From this screen, initiate either IP Range Scan or Active Directory Scan.**

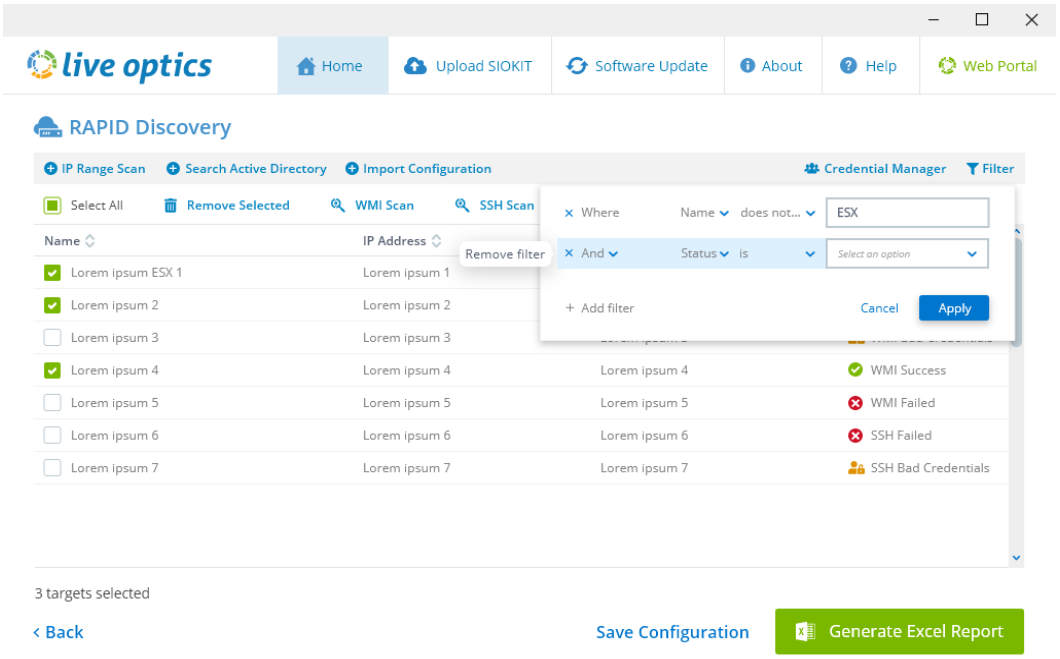
    a. **For an IP Range Scan, enter the corresponding IP Range to scan:**



b. **For an Active Directory Scan, provide an AD Path that contains all server objects:**

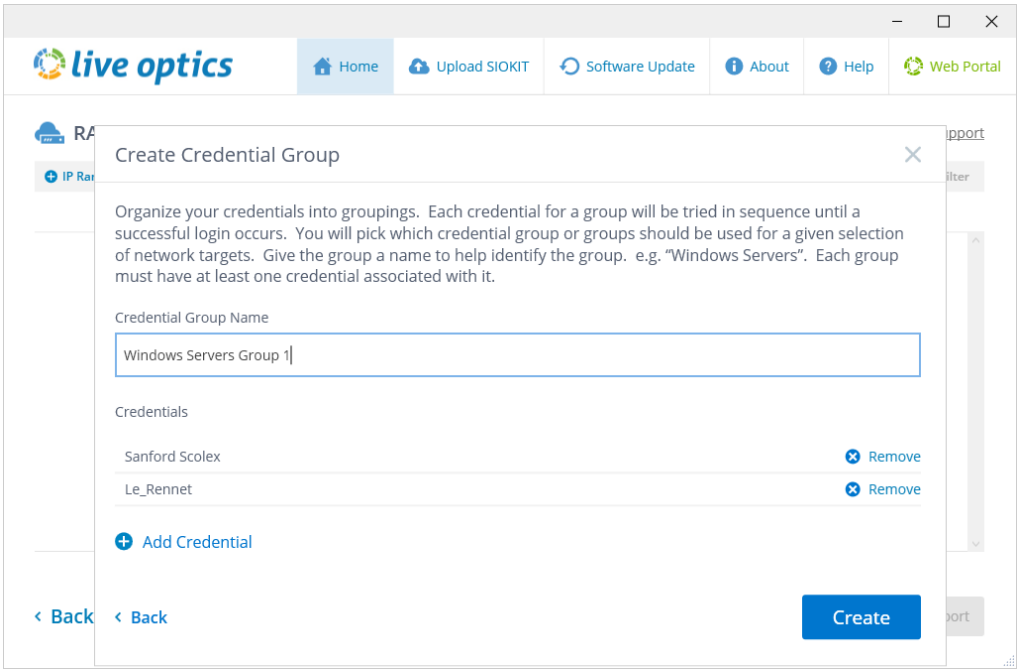


4. **Optionally sort, filter and select objects from the list (multiple filters are allowed):**



5. **If needed, run additional, deeper scans of either WMI or SSH types.**

   a. **For these scans you must provide credentials (username and password) using the Credential Manager:**



6. **Once the collection is completed, click the Generate Excel Report button.**

a. **For definitions of the fields in the Excel report, click here.**

7. **Additionally, you can Save Configurations and Import Configurations.**

   a. **This saves the data to a JSON format file which you can import into the RAPID Discovery feature. The file is created in the folder that contains the Live Optics Collector.**