EndaceConsole

With EndaceConsole™ you can investigate quickly by conducting packet searches across an entire network. EndaceConsole rapidly locates and retrieves packets of interest from Petabytes of stored data distributed across a network-wide EndaceFabric of interconnected EndaceProbes.

EndaceConsole's key features are:

- Easy-to-use, browser-based interface for searching and retrieving Network History.
- Find packets of interest quickly by searching multiple EndaceProbes simultaneously.
- Archive results from packet searches off-probe to secure storage for analysis at a later time.
- An API proxy that supports all REST API versions when querying multiple EndaceProbes.

Fabric-wide search and retrieval

EndaceConsole can search one or more EndaceProbes simultaneously, making locating specific traffic of interest a simple and efficient process. It enables analysts to focus investigations on specific groups of EndaceProbes and gives administrators the ability to control access to EndaceProbes that are capturing particularly sensitive or confidential information.

EndaceConsole has an easy-to-use GUI interface to streamline the process and allows you to:

- Create data-mining sessions
- Search multiple EndaceProbes at once
- Download packet captures from multiple probes at once
- Archive packet trace files to SAN, NAS or local storage in pcap or ERF format.

BENEFITS

Scalable

- Multiple instances of EndaceConsole can be deployed to provide scalable search and retrieval of Network History from across an EndaceFabric. Search up to 100 EndaceProbes simultaneously from each EndaceConsole instance.

Easy-to-Deploy, Easy-to-use

- Deployable as a virtual machine (VM) compatible with VMware vSphere EXSi 5.5 or 6. EndaceConsole may also be deployed in Application Dock™ on EndaceProbes.
- EndaceConsole's browser-based GUI interface makes it easy for analysts to search for and retrieve packets of interest from across the network. Packet trace files can be saved to NAS, SAN or local storage.

Secure

- Comply with data privacy requirements with fine-grained control over who in your organization can search, who can download packets, and where they can download packet trace files to.

Secure Access

EndaceConsole offers complete control over access to Network History, allowing you to select which EndaceProbes are analyzed and whether the packet data or results are stored on NAS, SAN or local storage.

Administrators can define which EndaceProbes a user can search and which users are restricted from downloading packet traces. Restricted SAN or NAS storage can be created for secure storage of sensitive trace files. Fine-grained user access control over who can search for, and who can download, packets helps teams operate efficiently at scale without compromising data privacy.

In environments where sensitive data is captured, such as PCI data, administrators can restrict viewing of packet data to staff with appropriate security clearance, while still allowing staff with lower level clearance to perform search and archival functions. This means they can do much of the investigation legwork by gathering relevant packet evidence before handing off to analysts with sufficient security clearance to inspect the packet data.

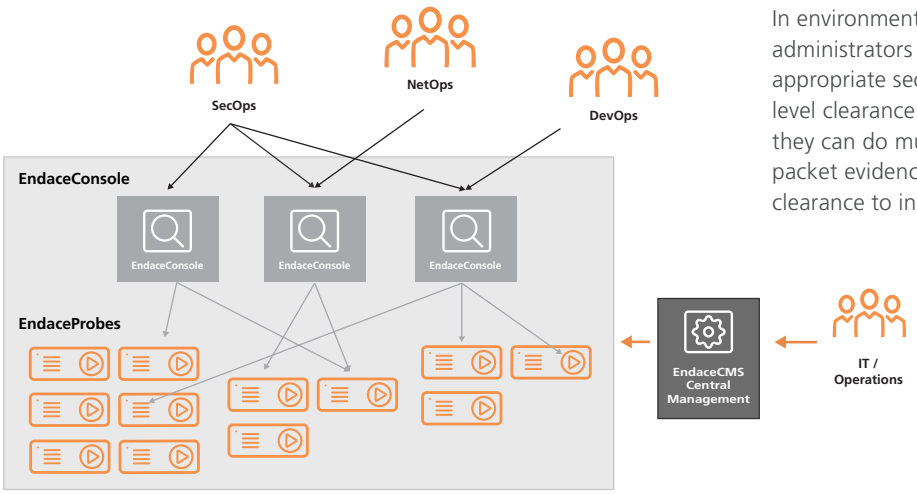

Figure 1: Multiple EndaceConsole instances can be deployed to provide scalability and allow access control to specific data

© Copyright Endace Technology Limited, 2018. All rights reserved. Information in this data sheet may be subject to change.

END_ds_endace_console_1.0_0518

API Proxy

Upgrade your EndaceProbes to the latest version without fear of breaking custom API integrations. The API proxy translates API versions, which lets applications continue to run unchanged just by pointing them at the EndaceConsole instance.

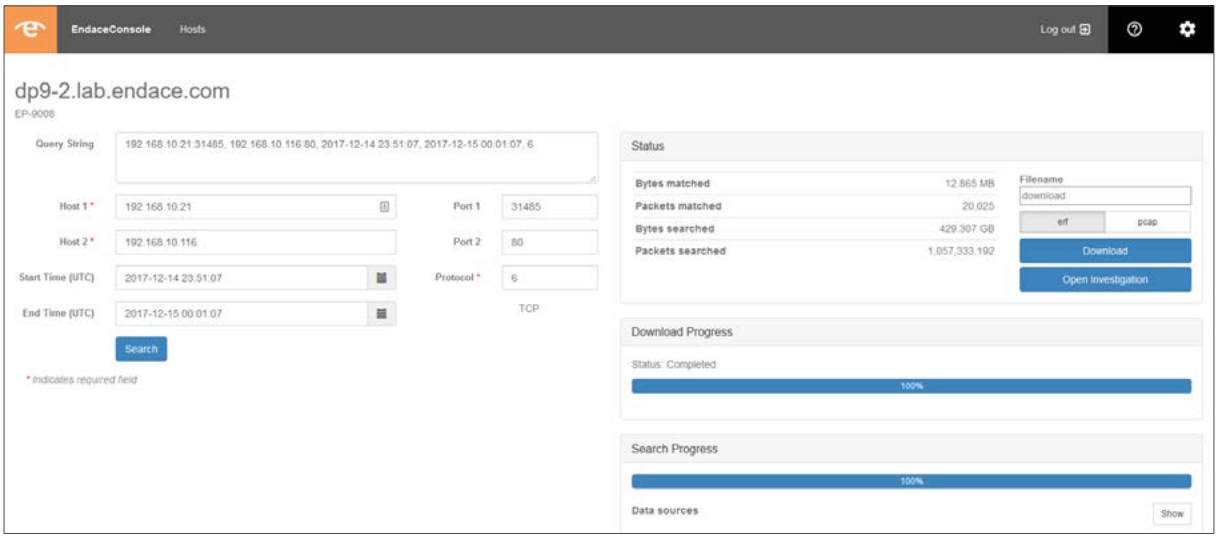

Figure 2: EndaceConsole can be used to search multiple EndaceProbes simultaneously. Each EndaceProbe in the collection is searched individually and results are aggregated.

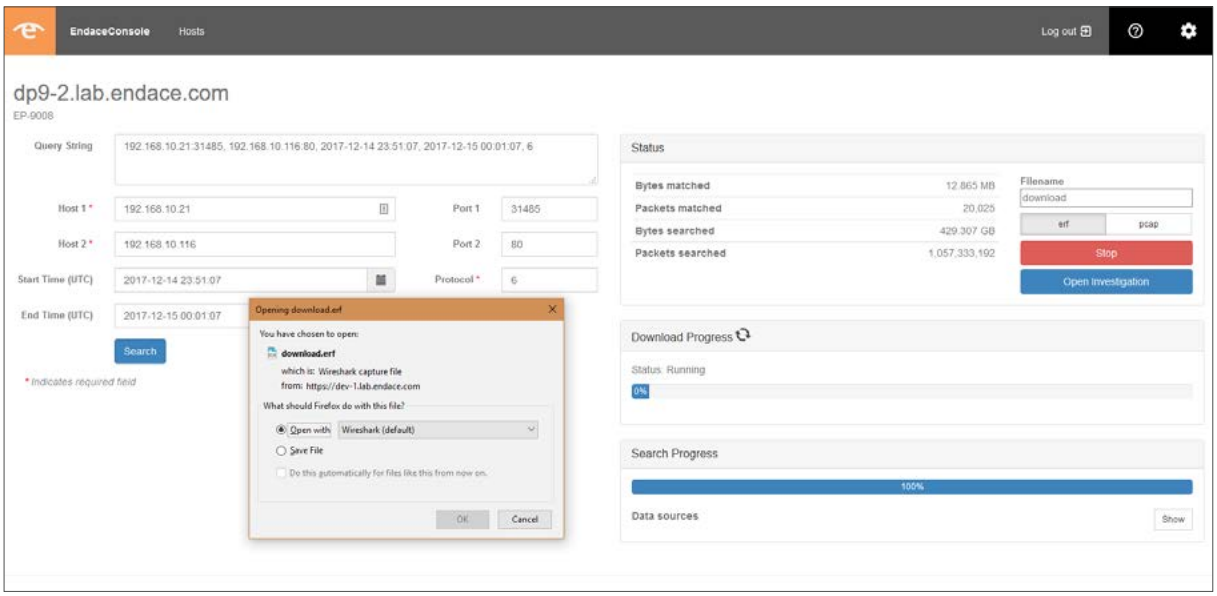

Figure 3 - Once the search has completed, the resulting packet trace file can be downloaded to local or attached network storage (assuming the user has sufficient permissions) or analyzed using EndaceVision and EndacePackets

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.

Endace™, the Endace logo and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com

© Copyright Endace Technology Limited, 2018. All rights reserved. Information in this data sheet may be subject to change.