Endace Site Survey

Introduction

The purpose of this document is to provide organizations considering, or preparing for, an Endace Site Survey with an overview of the survey process and what needs to be provided in order to enable the Site Survey to be undertaken. It also provides details of the information gathered during the survey process and the output that is generated from the collected survey data.

The purpose of a Site Survey is to understand the state of all the EndaceProbe™ Network Recorders installed in an estate. This information can be used to plan for software upgrades, hardware repairs, resource allocation, and configuration changes. The survey gathers information about each surveyed EndaceProbe's performance, capacity utilization, configuration and health.

Description

The Site Survey is performed by Endace Professional Services staff who will visit the customer site and install a Virtual Machine (VM) with the survey software on an EndaceProbe that has connectivity to the EndaceProbes being surveyed.

Prior to the commencement of a Site Survey, a short interview is conducted with the customer to find out more about the setup of the customer site, use cases and customer expectations and to agree on the plan and schedule for the survey project. During the survey process itself, Endace Professional Services staff will require physical access to the site, information about the EndaceProbes to be surveyed, and network access to those EndaceProbes.

The Site Survey has 2 parts.

The first part is the **Static Survey**. This is used to determine information about the state of each connected EndaceProbe, such as software and firmware versions, hard drive (HDD) health and utilization, VM setup and the amount of storage in the RotationFiles.

The Static Survey establishes a connection via SSH from the VM hosting the survey software to each connected EndaceProbe being surveyed and issues a short SNMP query. During that SSH connection, information is requested via standard CLI (Command-Line Interface) commands. It takes approximately two minutes to run on an estate with 30 EndaceProbes. Only connected EndaceProbes in the estate are contacted.

The second part is the **Polling Survey**. This is used to look at information that changes over time, such as the input bandwidth, number of flows and dropped packets. The Polling Survey periodically establishes a connection via SSH from the VM hosting the survey software to each EndaceProbe and uses the CLI to determine information such as bandwidth and number of flows. The frequency and length of the poll is configurable and normally it is run for 24 hours at five minute intervals. Connected EndaceProbes in the estate are polled directly and there are no connections made to other devices.

Survey output

Endace Professional Services staff collect, collate and analyze the survey data and produce two reports from it.

The first report is an "Initial Findings" report which includes an overview of the state of the EndaceProbes surveyed, the amount of data stored on them and information about the traffic being monitored and recorded. This report highlights any major concerns with the surveyed EndaceProbes.

The second report is a "Comprehensive Report" which contains a full analysis of all the data collected during the survey process and recommendations on next steps.

Details of information collected during the Static Survey

The following information is collected during the Static Survey:

Systems

For each surveyed EndaceProbe, a variety of information is collected, including the EndaceProbe name, IP address, status, model and serial numbers, uptime, OSm™ software version, total RAM and utilization, number of CPUs and utilization, RTT information, BIOS version, SNMP state, IPMI IP address and firmware version, the total RAID size and utilization, and the number, type and size of archives.

DAG information

Information on all installed DAG™ data capture modules is collected, including the types of DAG modules, the serial number and HLB groups, the name of each port, the type, status information (admin, operational, SFP detected, signal), the MAC address, cumulative received and transmitted bytes/packets, temperature, power and voltage information. DAG stream information such as each in and out stream, memory allocated and its status and the cumulative stream drop count are shown also.

Data pipes and RotationFiles

For each data pipe configured on each EndaceProbe, if it is enabled, the survey collects the dropped byte and packet count, the input and output packets and bytes, and what options were configured on the pipe (e.g. sampling, snap length). It shows the source and sink of the pipe. There is also a count of flows, flow fragments and flow errors. For each RotationFile on each EndaceProbe, the survey collects RotationFile (data plus metadata) disk usage and size.

Licenses

Information is collected on the licenses that have been installed on each EndaceProbe, including the start/end date, and whether they are valid and active.

Usernames

The usernames, full names and status of each user on each EndaceProbe is recorded.

Disks

The model, health, status, firmware, serial number, defect list and other information is collected to determine the health of disks (LBA written, wearout level, offline uncorrectable, current pending sector, reallocated sector).

VM Information

The name, capacity, size and type of each VM volume on each EndaceProbe is recorded. For each installed VM, the name, status, memory, CPU count, image name, image size, number of interfaces, number of vDAGs and architecture is shown.

Affinity

How the affinity is set for each EndaceProbe (platform daemons, ERF Stream Manager etc.) is recorded.

Details of information collected during the Polling Survey

The Polling Survey records received DAG Mbps, DAG stream drops, RotationFile disk usage and size, EndaceVision disk size, number of flows, number of data pipe drops (bytes/packets), and the number of data pipe input and output packets/bytes.

The survey process and expected impact

Installation

To perform the site survey installation, a connection to the host EndaceProbe via SSH is required. The compressed site survey image is transferred to the host EndaceProbe, and a VM is set up. A bridge on the host to connect the VM with the internet is created (if it is not already present). This causes a sub-second interruption of the management traffic: running traffic capture and current TCP sessions are not affected by the change.

The deployed VM uses:

- 4GB RAM
- 2GB Disk space (image from above, not additionally)
- 2 CPUs
- One IP address via DHCP (preferred) or static

During deployment/startup some spikes in disk I/O and CPU usage may be seen.

To control the survey, a connection to the VM via SSH is required.

During the Static Survey

The Static Survey requires an input file with host IP addresses, SNMP community string and ‘admin’ credentials (username & password) specified.

The survey script establishes a connection via SSH and issues a short SNMP query to each EndaceProbe; inside the SSH connection, standard CLI commands will be used. The impact on disk I/O, network I/O and CPU usage is minimal and can barely be measured. The query uses a thread pool, which means that many EndaceProbes can be queried simultaneously.

During the Polling Survey

The Polling Survey requires the same input file as the Static Survey, listing host IP addresses, SNMP community string and ‘admin’ credentials (username & password).

A reduced set of SSH connections will be established periodically to all EndaceProbes over a defined time period to poll a few readings only.

The impact is even smaller than with the Static Survey. A thread pool is used here as well.

After Site Survey completion

The collected data has to be retrieved from the VM using SCP (server and client available). This consists of two .xls files. There is an optional dump file, and a log file that is also created.

The Virtual Machine, VM volume and the compressed image can be removed after the Static Survey and Polling Survey has completed, and the data has been retrieved.

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

For further information, email: info@endace.com