EndaceProbe vProbe

The EndaceProbe™ vProbe is a virtual machine (VM) implementation of the EndaceProbe network recorder designed to complement hardware-based EndaceProbes in a network-wide, monitoring fabric.

The vProbe integrates transparently with physical EndaceProbe deployments to expand visibility across the network. It is ideally suited for monitoring performance and diagnosing issues within virtualized applications, providing east-west traffic monitoring from within the virtual infrastructure without requiring physical appliances.

The vProbe collects data by tapping virtual switches or collecting packets from a dedicated host Network Interface Card (NIC). Because the vProbe uses standard NIC or virtual switch capture, it does not provide the same guaranteed 100% packet capture as physical EndaceProbe appliances which leverage DAG™ capture card technology. Nevertheless, the vProbe can be useful for extending network visibility - particularly into virtualized environments or low-speed network links that otherwise cannot be, or are not, monitored using a physical appliance.

The vProbe allows EndaceProbe users to economically expand their coverage horizontally across their network. As a virtual appliance, the vProbe can be run on a variety of different hardware platforms, such as ruggedized chassis or luggable devices, making it also suitable for deployment in unusual environments or as a portable solution for monitoring low speed links where 100% guaranteed packet capture is not a requirement.

The EndaceProbe family

EndaceProbes are a range of high-fidelity network recorders. With 100% accurate network data capture, EndaceProbes deliver network-wide visibility for security and network event investigation including centralized search and retrieval of recorded traffic. They are available in a range of configurations for monitoring, capturing, analyzing and visualizing traffic from the edge to the core of the network. The virtual EndaceProbe vProbe™ also provides visibility into virtualized environments.

EndaceProbes are uniquely multi-functional, combining network recording with an integrated VM hosting environment that gives hosted third-party applications real-time access to recorded traffic. An open, RESTful API allows external applications to search for and retrieve packets from packet storage and enables applications to be tightly integrated. The API and VM hosting make it easy for your chosen applications – from open-source or custom-developed tools to commercial solutions – to leverage a single, authoritative and accurate source of captured traffic.

The power and flexibility of EndaceProbes enables SecOps and NetOps teams to monitor and analyze network behavior more effectively and identify and resolve security events and network issues faster. They gain access to the full, rich data they need and can deliver it to their chosen tools quickly and efficiently.

THE vPROBE AT A GLANCE

- Designed for pervasive monitoring in virtualized environments or for monitoring low speed edge links where 100% packet capture is not a requirement
- VMware vSphere ESXI 5.5 or 6.0 based
- Minimum VM requirements: 4x virtual CPUs, 2TB storage, 12GB RAM, 1x virtual NIC or 1x 1GbE NIC with PCI passthrough for monitoring
- Capture inter-VM traffic via access to vSwitch or vSphere Distributed Switch (VDS)
- Up to 1Gbps capture rate

BENEFITS

Accurate

- Network packet capture on links up to 1Gbps

Powerful

- Back-in-time incident investigation and troubleshooting
- Analyze network traffic before, during and after a specific period of interest, such as an outage or traffic microburst
- Drill down to packet level on locally stored trace files and export traffic easily to desktop or other servers via bundled EndaceVision and EndacePackets applications
- DPI-based application detection identifies applications based on packet payload rather than limited port based identification
- Integration with in-house or third-party network monitoring and security applications via RESTful API
- Up to 2TB onboard packet storage

Flexible

- Economical option for expanding coverage horizontally across the network to increase traffic visibility
- Integrates seamlessly with other EndaceProbes in a monitoring fabric
- Monitor performance and diagnose issues with virtualized applications
- Monitor dynamic virtualized environments without requiring physical appliances and virtual taps
- Delivers east west traffic monitoring in virtualized environments via vSwitch integration
- EndaceVision provides rapid search, visualization, analysis and retrieval of archived traffic
- Run on any specialized hardware, such as ruggedized chassis or luggable probes, for monitoring physical networks in unusual environments

Secure and Reliable

- Hardened Endace OSm™ operating system

EndaceProbes come bundled with EndaceVision™, a network history search and visualization tool, and EndacePackets™, a packet-analysis tool with support for Wireshark™ display filters. Efficient access to packets and seamless integration between EndaceProbes, EndaceVision and existing tools maximizes tool utility and streamlines work-flows.

An Integrated Monitoring Fabric

The vProbe integrates seamlessly with Endace's hardware-based EndaceProbe family. Multiple EndaceProbes can be combined into a high-performance, monitoring fabric able to accurately capture and monitor traffic across the entire network – including complex, geographically distributed infrastructures – right up to 100GbE.

EndaceProbes support centralized deployment and management – via EndaceCMS™ (Central Management Server), ensuring efficient management and reducing the overall cost of deploying and managing a monitoring fabric. The EndaceProbe's multi-functional capability means your monitoring fabric can also host your chosen network applications – allowing you to consolidate hardware and reduce costs.

The 100% packet capture and nanosecond-level accurate synchronization and time stamping delivered by EndaceProbes ensures you have the richest, most reliable source of captured traffic data from across your entire network available for the applications that need it.

Virtual Machine Settings (common to both options)

Minimum VM resources required by vProbe	
CPU cores	4
Memory	12GB
Storage	2TB

Performance

Performance of the vProbe is highly dependent on the capability of the hardware the vProbe's VM is deployed on. The tables below show representative performance for vProbe deployed on two different sorts of hardware platforms.

- Commodity Hardware represents performance where the vProbe's VM is hosted on a low-end server with a single SATA drive hosting the storage volume.
- High Performance Hardware represents performance when the vProbe's VM is hosted on a higher-end system with a large number of disks in a RAID array, for increased storage performance, and using PCI pass-through on the network interface.

In general, due to the software nature of the product, CPU resources remain the key bottleneck.

Performance comparison

	Commodity Hardware	High-Performance Hardware
Host hardware attributes		
Storage bandwidth (MB per second)	165 MBps	1975 MBps
IOPs (transactions/sec)	IOPS 4k write 208 IOPS 4k read 139	IOPS 4k write 4200 IOPS 4k read 7980
CPU cores	2 x Intel E5-2680 v2 @ 2.8 GHz 40 core	2 x Intel E5-2680 v2 @ 2.8 GHz 40 core
Memory DIMM speed (GHz)	1600	1600
Network interface	1x virtual NIC	1 x 1GbE pass-through
Performance		
Max packet capture performance	250 Mbps	1 Gbps

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

For further information, email: info@endace.com