

Dynatrace and Endace

Deliver unrivalled digital experiences

Wire based, real-user monitoring and 100% accurate network packet recording combine to ensure great performance and user experience for all your enterprise applications.

Dynatrace Data Center Real User Monitoring (DC RUM) delivers deep visibility into enterprise applications, allowing you to see what's going on inside 'black box' applications including SAP, Oracle, Exchange and Citrix. DC RUM applies powerful, real-time analysis to provide full visibility into customer experience from the front-end to the back-end.

The EndaceProbe™ Network Analytics Platform captures, indexes and stores network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. The built-in Application Dock™ virtual machine hosting environment extends security and performance monitoring by allowing third party monitoring solutions like a virtual instance of DC RUM Agentless Monitoring Device™ (vAMD) to be hosted on the open EndaceProbe platform.

Identify and Resolve Application Issues Rapidly

Integration between Dynatrace's DC RUM Central Analysis Server (CAS) and EndaceProbes gives analysts streamlined access to network history for fast, conclusive investigations. Clicking on an event in the CAS lets analysts quickly drill-down, retrieve and view specific packets relative to the interaction from the Network History stored on one or more EndaceProbes.

Using the EndaceProbe's built-in EndaceVision™ investigation tool, you can search and filter packet history and download packets for analysis in Dynatrace Network Analyzer™ (DNA). Packets can also be analyzed directly on the EndaceProbe using EndacePackets™, removing the need to download large trace files across the network.

Increased Monitoring with Lower Cost of Ownership

Deploy virtual instances of DC RUM vAMD in Application Dock on EndaceProbes for real-time monitoring anywhere. No hardware installs and no truck rolls. Flexible licensing of the vAMD allows you to deploy everywhere, license only what you need, and choose what to monitor on-demand.

Application Dock allows you to run multiple applications simultaneously on a single EndaceProbe. In addition to hosting vAMD, you can run other tools such as an Intrusion Detection System (IDS) to boost your security posture and leverage your investment even further.



PRODUCTS

Dynatrace Data Center Real User Monitoring (DC-RUM)
EndaceProbes with Application Dock

BENEFITS

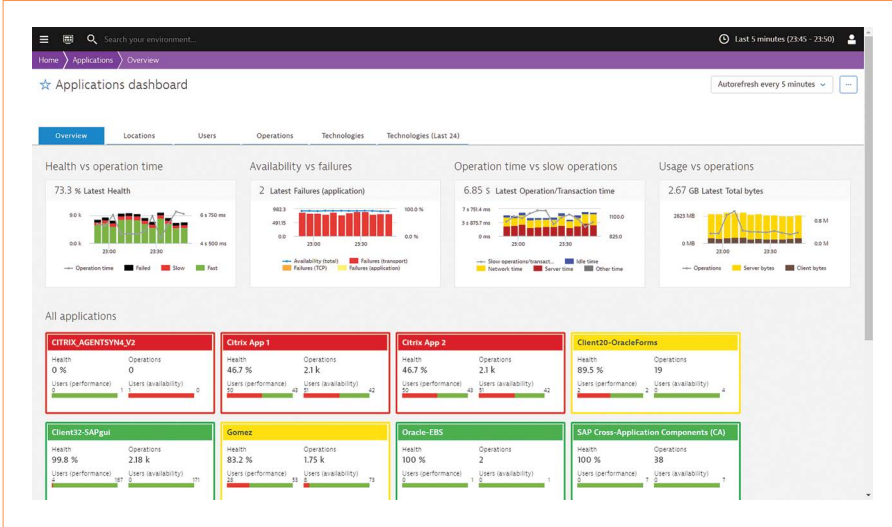
- 100% visibility into user experience across every transaction. No sampling.
- Accelerate performance improvements and issue resolution with integrated drill-down to packet-level detail.
- See inside enterprise applications including SAP, Oracle, Citrix and Exchange.
- Flexible deployment and lower cost-of-ownership by deploying Dynatrace software on EndaceProbes.

Use Playback to Analyze Historical Events

With a virtual instance of the DC RUM Agentless Monitoring Device deployed in Application Dock™, archived packet history can be replayed to the hosted vAMD to analyze past history.

Conclusion

Leveraging EndaceProbes to host DC RUM vAMD significantly lowers cost of ownership, expands coverage and enables flexible deployment on-demand without truck rolls or hardware installs. The integrated solution provides deep visibility into real user experience, ensuring you can discover and resolve performance issues before they impact on business productivity.



Monitor Performance in Dynatrace DC RUM CAS

Pivot-To-Packets integration provides fast search and retrieval of the packet history relating performance issues



Capture packets

The selected time range extends into the past. The AMD does not support back-in-time captures, so all AMD data sources will be ignored.

Task name: Task 20170127031102
 Description: Created from 'Application respons'

Traffic Filters | Data Sources | Advanced Options

Time range

Fixed date and time

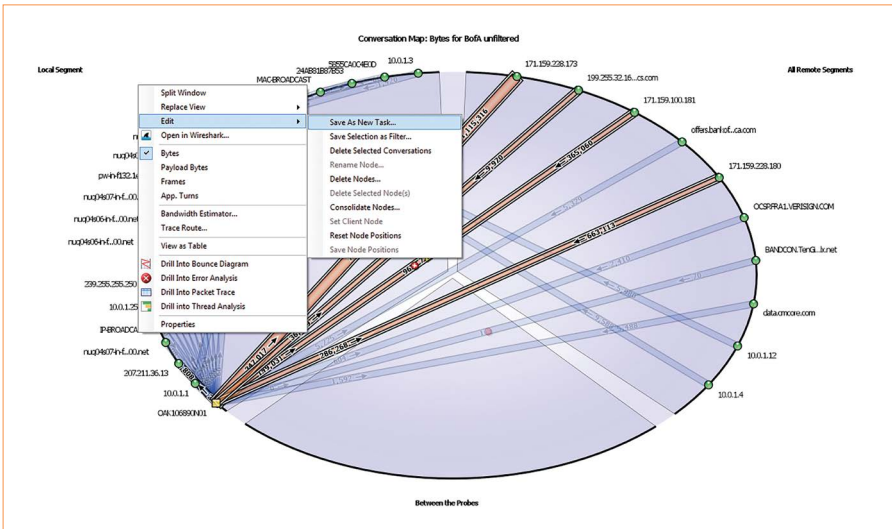
Start time: 01/27/2017 00:00:00
 Stop time: 01/27/2017 15:10:00

TCPDUMP filter

```
1 (host 10.245.7.198 and host 10.242.68.48 and port 53) or
2 (host 10.245.7.198 and host 192.168.32.2 and port 53)
```

Estimated task size: 0.00 B
 Free space: 167 TB

OK CANCEL



Packet traces can be downloaded for analysis in Dynatrace DNA or other packet analysis tools



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