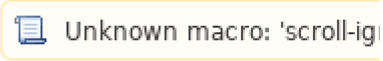
CAS and reporting

Unknown macro: 'scroll-ig


Unknown macro: 'scroll-ig

The Central Analysis Server (CAS) provides real-time access to information about performance and usage of your key business applications. It monitors user session performance, application performance, and server performance in different configurations, with the purpose of identifying when and where problems occur and how to address them.

Why CAS?

With CAS, you have an insight into business application performance on the transaction and operation level. The information is aligned with the business structure of the organization (such as branches, working groups, and business units) and is not dependent on the infrastructure components. It is delivered via comprehensive, interactive, service-oriented reports, and via event-driven alerts that inform you about important events such as performance degradation or traffic pattern anomalies.

With CAS reports, you see a complete view of your application performance. The report structure reflects business organization priorities and allows for quick identification of the root causes of problems. The CAS is equipped with powerful data mining and report building tools for creating new or customized reports quickly and easily.

The Smart Packet Capture functionality enables you to analyze and diagnose the cause of a known and observed network problem by examining detailed packet trace data. Once a monitoring system has detected a network problem, the Smart Packet Capture process can then take over to drill down to the root cause of the issue.

How it all works

The CAS uses the measurement data provided by the passive network monitoring devices referred to as Agentless Monitoring Devices or Network Monitoring Probes, and by synthetic network monitoring agents referred to as Enterprise Synthetic Agents.

In real-user monitoring, one or more AMDs or Network Monitoring Probes are attached to the monitored network near the core switch of the data center or near VPN access switches. The AMDs and Network Monitoring Probes collect the data from the monitored network, preprocess it, and deliver it to the report server. Each report server can handle a number of AMDs and Network Monitoring Probes. The report server processes the received data further, stores it in a database, and generates user-friendly reports. The reports can then be viewed and analyzed regularly or only when a network problem occurs.

Core CAS tasks

The CAS provides:

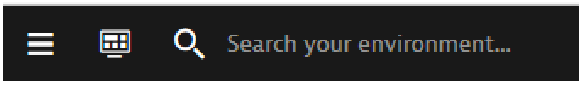
- Web analysis and reporting
- Decryption and analysis of HTTPS traffic
- Monitoring of SSL errors
- Analysis of middleware transactions (XML, SOAP, SAP RFC, and others)
- Analysis of various database protocols
- Analysis of the Oracle Forms protocol
- Analysis of Microsoft Exchange and SMTP protocols
- Analysis of a selection of SAP protocols
- Thin client (ICA) protocol analysis
- VoIP analysis
- VPN analysis
- WAN analysis
- Enterprise applications analysis and reporting
- Real-time reports, trending reports, and baseline calculations
- Detection of abnormal application usage and network usage patterns
- User diagnostics
- Report access management, publication, and sharing
- Customizable reports

For more information, see Protocols Supported by CAS.

CAS top menu

The top menu bar gives you instant access to DMI-based reports, the DMI tool for building your own reports, and CAS settings. The options available in the menu depends not only on the license type but also on the user rights.

Figure 1. CAS top menu bar



- Click ☰ to display a menu of CAS commands.
- Click ▦ to display the Dashboard and access your favorite reports.
- Click in the 🔍 Search your environment... edit box, type a search string, and press **Enter** to search your DC RUM environment for that string.