WHITE PAPER

Traverse:
Identifying Root Causes of Service Performance Problems

TRAVERSE by Kaseya

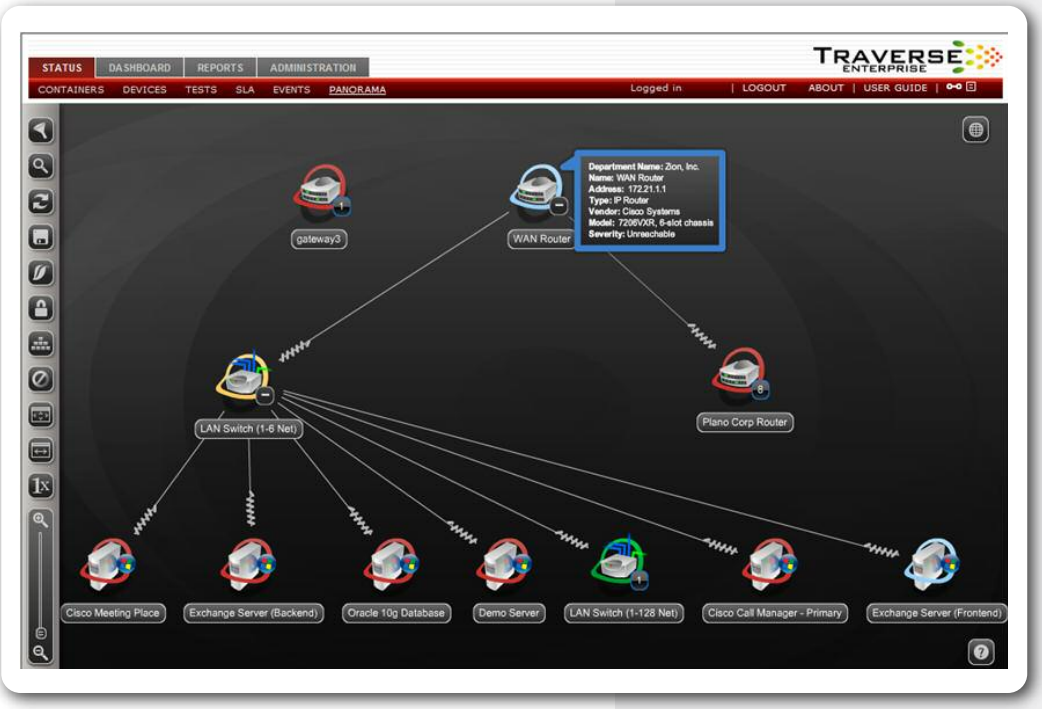
Today's organizations depend on their IT infrastructure to support mission-critical business services. The applications supporting business services are distributed in nature, span multiple departments as well as geographical locations, and are enabled by a complex web of network and computing technology. Rather than focus on just network downtime, performance monitoring and root-cause analysis in today's enterprises must concentrate on minimizing business downtime. This requires adopting a service-centric monitoring approach, and having the integrated monitoring capabilities to identify service problems and then conduct detailed diagnosis to determine the source of problems.

Traditional systems limit monitoring and root-cause analysis to the component level. However, with the enhanced role of IT as an enabler of business, it is increasingly important to extend monitoring and correlation to the service layer—to answer questions such as "why is the payroll service or online banking service running slow." Getting an answer to such questions in real time is critical to avoid material impact to the business.

Integrated Data Center Monitoring systems such as Traverse need to include root-cause analysis capabilities that extend beyond traditional network level analysis. The root-cause analysis capability in advanced solutions utilize a layered service object model designed to support drilling down through one or more hierarchical service impact views to device and test correlation maps, all the way to network flow detail. At each stage of the analysis, network operators/administrators are rapidly able to further narrow down the potential source of the problem, thereby dramatically reducing time to recovery for service performance.

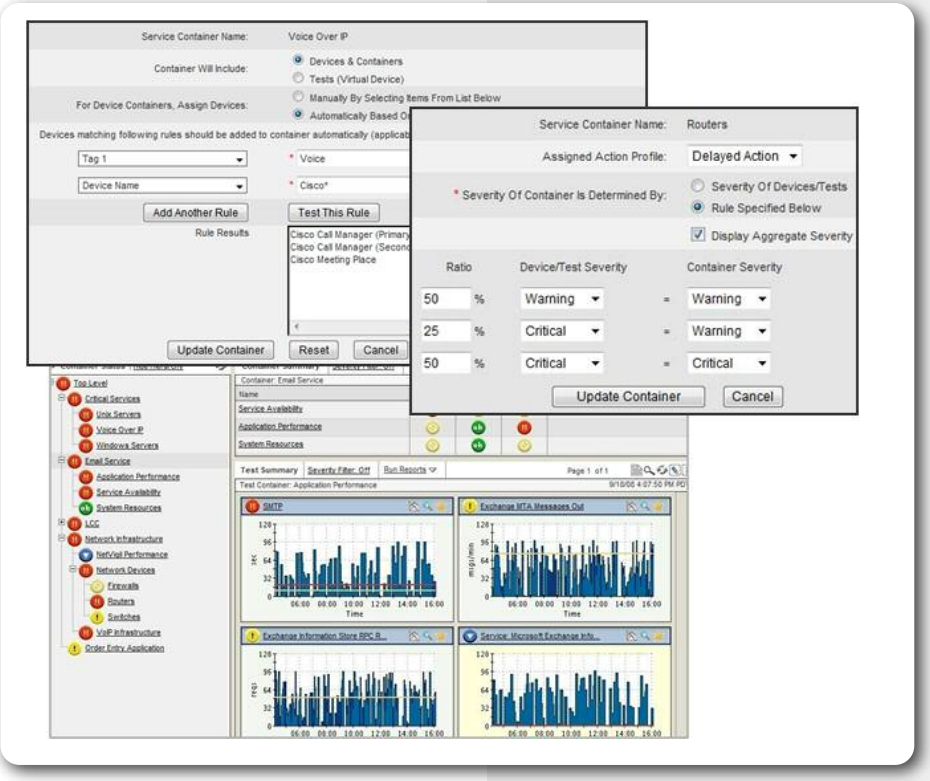
Model-based Root-cause Analysis

Traverse supports a model-based approach to root-cause analysis. The solution breaks a complex system into smaller elements (models) and then describes the attributes and behavior of each model. Using object-oriented concepts such as inheritance, creating a model library for complex services and very large networks is an easily manageable task. The model behavior in Traverse is not isolated to the network layer, but actually defines the behavior between the different components all the way up to the application and business service layer.



A rich and complete information database is essential for enabling performance monitoring and root-cause analysis. Traverse starts

building its database through intelligent discovery of the network. The discovery process does a complete L2/L3 network discovery to detect the relationship between the various devices on the network. It discovers network connectivity, disks, controllers, VLANs, file systems, fiber channel switches, printers, SAN, NAS devices, and more, as well as multiple, redundant paths in the network to prevent false suppressions. The process then discovers the capabilities, size, capacity, and other key attributes of each element, and goes on to discover applications running on various devices, such as databases, active directory, radius, DNS, mail, and application servers.

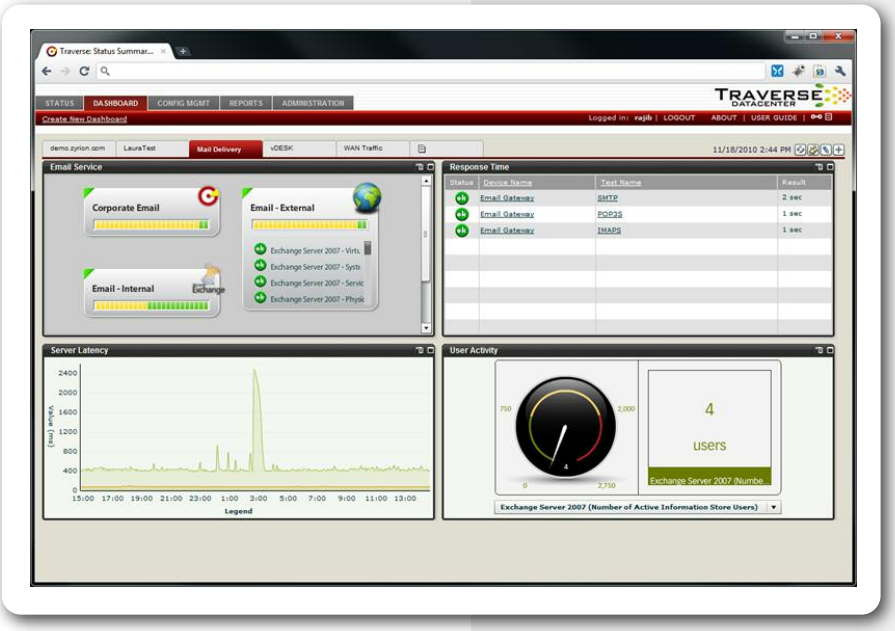


Business Service Containers in Traverse then support creating many-to-many, contextual and hierarchical mappings between the underlying networks/servers/applications and business services. They allow for the creation of logical, business-oriented views of the overall physical and virtualized network. Business Service Containers go beyond simple grouping, and support mapping the same device or component to multiple services. Additionally, containers can be mapped to containers to create a hierarchy of services for monitoring purposes.

Users can define different Service Level Agreements (SLAs) for different containers, create fault-tolerant redundant models within a container, and have nested containers with cascading alarms. Most importantly, the Business Service Container model is overlaid on top of the physical topology discovery/display model to provide service-relevant topology views, reduce alarm floods and enable rapid root-cause analysis of service performance degradation or downtime. The tight integration of the network and service modeling in Traverse allows providing a seamless solution.

Root-cause Analysis: Dashboard-to-device

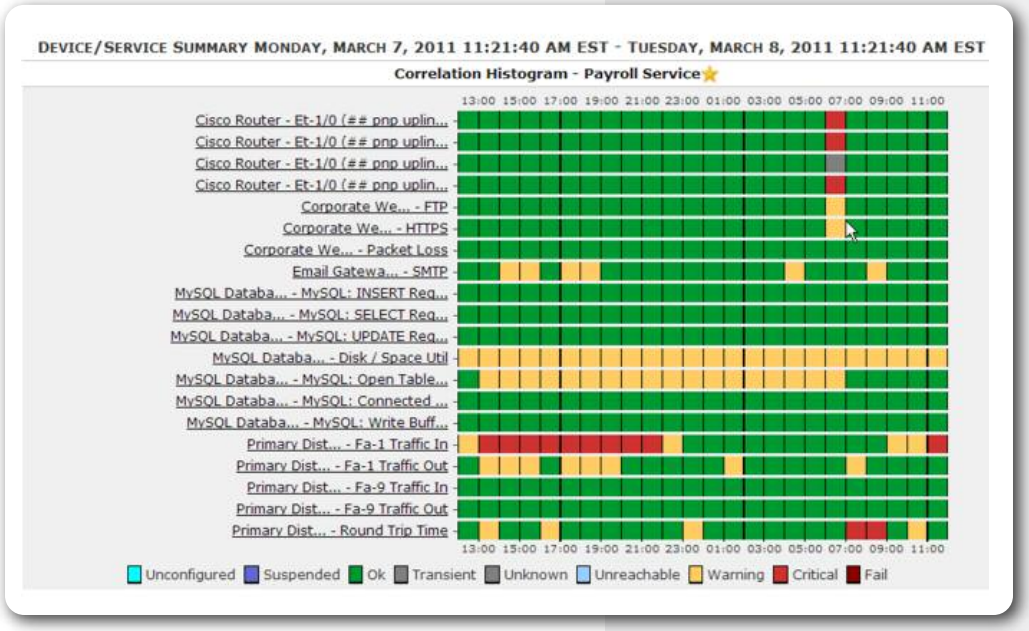
Within Traverse, users can monitor the performance of business services via service container status views and dashboards. Based on the alerting rules configured within the system, visual indicators (as well as other configuration notifications) will highlight if a given service is in a 'warning' or 'critical' state. Upon seeing the indicator or being notified of a potential problem with a service, the user can immediately drill down to the device and test views to identify the component that may be causing the degradation of service. For example, the number of open tables for a MySQL database may have exceeded the warning threshold, which in turn affected the business service that is dependent on the database.



TRAVERSE by Kaseya

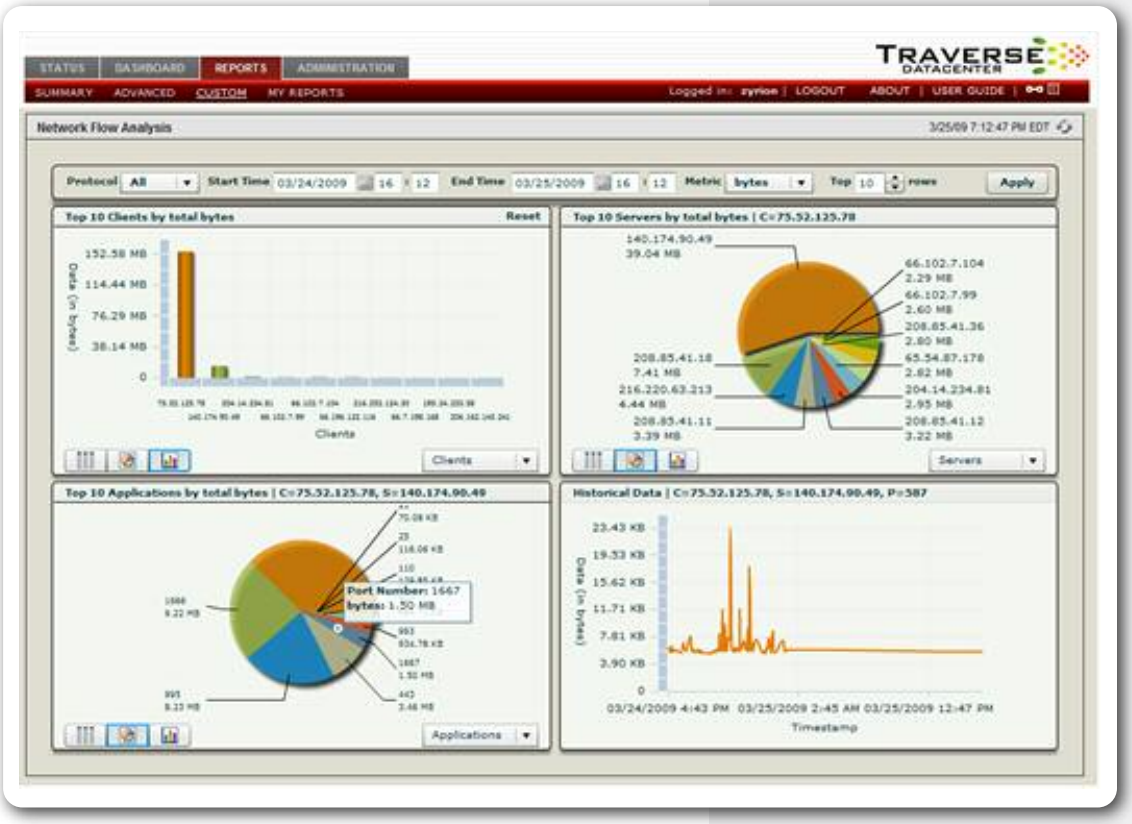
Root-Cause Analysis: Correlation Maps

The correlation maps provide a side-by-side view of the status of the key components for a given service over a 24-hour time period. This allows indentifying other components that may be in warning or critical state that might be the more appropriate place to dig deeper in terms of determining the source of service performance degradation. For example, a review of the correlation map may reveal that a port on the main distribution switch is in a critical state, which may indicate a high level of network traffic being the problem source, rather than some specific database issue.



Root-Cause Analysis: Network Flow Detail

From the correlation maps view (as well as device views), a user can drill down and see the full performance data for the given component or test, and then drill down to the network flow detail. The user can specify the time period for which flow analysis is to be performed, the metric of interest (e.g. bytes, packets, flows) and the number of sources or destinations to include in the analysis. The flow data can be displayed as a matrix, column chart or pie chart. For a given source, the specific applications generating the traffic can be viewed as well, and then the history of the traffic generated by a particular application can be displayed. This allows a user to identify the source of the unusual traffic burst that is affecting the performance of the business service. With this information in hand, the user is able to initiate remediation actions.



TRAVERSE by Kaseya

Root-cause Analysis: Future Trending

Root-cause analysis is typically an after-the-fact exercise, where activity for diagnosis and identification of problem sources is initiated after an alert has been generated. Getting out of the reactive cycle is an integral part of a comprehensive approach to root-cause analysis. This is done through analyzing future trends for performance metrics and predicting the future threshold violations. The trending data allows taking steps proactively to alleviate service performance problems. Traverse provides comprehensive trend reporting and automated thresholding capabilities to fix problem sources before they materially impact the performance of business services.

The Bottom Line

Root-cause analysis for service performance degradation can be a difficult exercise given the increasingly complex, inter-related, distributed infrastructure environment. A model-based approach to monitoring provides the required framework for efficient and effective root-cause analysis. This includes automated discovery of network-level components and the creation of mappings between business services and the underlying network technology. Intelligent alarming rules, along with seamless drill-down to device/test status and network flow, dramatically reduces the time to isolate the source of service problems. Traverse provides these capabilities through comprehensive and integrated data center monitoring functionality.

ABOUT TRAVERSE

Traverse is a next-generation monitoring solution from Kaseya, a global software solution provider with over 10,000 customers globally. Traverse's patented technology offers a distributed, scalable monitoring platform with rich data analytics and unified cloud & network management. Traverse allows enterprises and Managed Service Providers to optimize their IT operations with faster mean time to resolution for slow or failed IT services within their infrastructure. Customers leveraging Traverse include the Fortune 100 as well as small-sized and medium-sized businesses worldwide. For more information, visit **www.traverse-monitoring.com**

Rev 122815

TRAVERSE by Kaseya