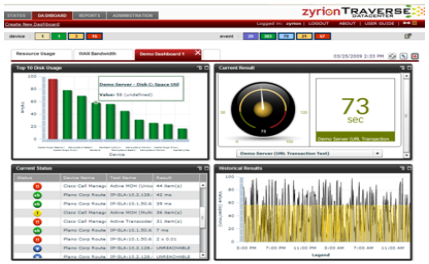
BSM and Network Performance Monitoring Solution Checklist



This checklist serves two purposes:

1. Guides organizations that are evaluating Traverse by listing out all the generic functions that should be exercised to get a comprehensive view and understanding of the capabilities of Traverse. This list summarizes the areas of Traverse that should be tested as part of a POC project. Note, this is by no means an exhaustive list of all the capabilities of Traverse, but is intended to cover the major areas in some degree of depth.

2. This checklist is also designed to help evaluators and decision makers through a solution selection process. The checklist provides a comprehensive set of dimensions to compare the alternative solutions.

Suggested Scoring Approch: 4 - Must Have; 3 - Nice to Have; 2 - Not Important Now; 1 - Not Important

	Traverse	<Other 1>	<Other 2>	Comments
Additional Items (placeholder area to specify functionality that may be not be covered in Sections A through E below)				
Feature				
Feature				
Feature				
Feature				
A. Installation and Configuration				
A1. User Administration				
Create separate departments/groups, where monitoring views/access can be separated by departmen				
Create users within a department				
Configure the privileges for end users				
Configure privileges for admin users				
Perform audit of user activity via reports				
A2. Adding Devices				
Add devices using UI, including automatically detecting supported test via monitoring profiles				
Define parent-child dependencies between devices				
Import a list of devices from a .csv file				
Automatically discover devices (L2, L3) and map the relationships between them				
Create manual dependencies between L2/L3 via the UI input				
Create manual dependencies via drag and drop				
Specify multiple community strings and multiple domain credentials during discovery				
Apply filtering during discovery to add/exclude specific device types				
Use API-based bulk import tool for adding devices (for large environments)				
Add support for a new/undetected device type (extend signature library)				
A3. Managing Device Configurations				
Schedule and execute automated discovery of ARP, MAC table, and neighbor data				
Manually back-up configuration for a device that has been enabled for network configuration mgmt				
Restore a historical configuration for a backed-up device that is network configuration enabled				
Compare backed up device configurations over time, to see what changes have been made				
Compare device configurations between two devices, to see what differences there are				
Search/query for devices using various parameters (e.g. MAC/IP address, DNS lookup, HW model, etc.)				
A4. Managing Tests				
Auto-discover tests for a given device				
Create a monitoring profile and apply to multiple devices				
Linked-device templates to allow master device profile to be associated with child devices				
Adaptive thresholds, enabling different warning and critical thresholds for different timeperiods				
Automatically validate the configuration parameters of existing tests (test parameter re-discovery)				
Automatically set the warning and critical thresholds for each test via baselining				
Create custom schedule for one or more tests				
Create composite or custom test/metrics by combining other metrics or via a calculation				
Create a web application transaction test (for 'synthetic' web transaction monitoring)				
Create a mail transaction test (for synthetic mail transaction monitoring)				
Create a DB query test (for synthetic DB query monitoring)				

Suppress a test (one time, for a given period, until unsuppressed)						
Manually add OIDs using a MIB browser						
B. Data Collection, Event Analysis and Alerting						
B1. Alarm/Alert Generation						
Select where alarm is triggered from if multiple collectors (e.g. DGE) are in operation						
Ensure no alert is created for a device if an upstream device has failed (parent-child hierarchy support)						
Suppress repeating alarms manually (via event manger) as well as automatically (action setting)						
Process syslog messages to generate event data						
Process application log to generate event data						
Process Windows events (WMI monitoring)						
Process SNMP traps from a router/switch/network-appliance/application						
Add new custom data source for generation of events to display in event console/manager						
Specify rule to find pattern in custom message string, transform and display in event console/manager						
B2. Event Handling						
Filter objects in event console/manager						
Sort objects in event console/manager						
Acknowledge, suppress and/or annotate in event console/manager						
Perform de-duplication in event console/manager						
Transform message in event console/manager						
Drill down to additional details in event console/manager						
Auto-clear events (e.g. via auto-clear parameter settings)						
Initiate custom on-demand actions in event console/manager						
View related events for a given event directly from event console						
View other related/affected/impacted devices for a given event						
View affected services as a result of an event						
B3. Actions / Notifications						
Create and execute automated actions for restart/reboot of a server and router						
Create and execute escalating notifications (as status on a test changes)						
Specify schedule for a particular action to only run during specific time of day, or day of week						
Create and initiate (on-demand) a custom action/notification using plug-in capability						
B4. SLA Management						
Create one or more SLA measurements, including calculation period, frequency and OK threshold						
Create SLA measurement for a test, device or service (container)						
Specify planned downtime schedules for SLA calculations						
Display SLA data in end-user dashboards and reports						
View 'time to compliance' and 'time to violation' for the measurement for the calculation period						
View historical compliance against SLA and drill-down to see time-period and compliance % detail						
View SLA data and compliance for different time-spans						
C. Business Service Management / Monitoring						
C1. Service Modeling / Containers						
Manually select/group devices to create a logical, service-oriented view (container) for monitoring						
Allow the same device to be mapped to multiple containers/services for monitoring						
Define rule/approach for automatically adding/removing devices to/from a service container						
Programmatically create/update containers/service-model via API commands						
Specify rule for determining severity of a container based on status of constituents						
Create a nested service container for monitoring (e.g. region to business application to devices)						
Create a 'Virtual Device' by grouping tests from multiple devices						
C2. Service Dashboards / Reports / Resolution Process						
Availability of service status views and customizable dashboards						
Monitor service status, and drill down to view status of underlying devices						
Run reports on service avaiability and performance						
View graphical/topological representation of devices supporting a service						
Create help links/notes for various objects for helping less experienced business/ops. users						
Creat context specific help text (e.g. specific to department, device, test or generic across all departments, etc.)						

D. Integrated Monitoring Dashboards and Reports						
D1. Dashboard Flexibility						
Access service-level views						
View services reliant on other services (e.g. email & credit-check may be part of ecommerce service)						
Access device-level views						
Access test-level views						
Access SLA compliance views						
Drill down from higher-level views to see device/element details						
Create and access custom dashboard (including dashboard components)						
Create read-only dashboard						
Lock out dashboard menus						
Create a public or private dashboard						
D2. Network Flow Analysis						
Drill-down from system and device level views to see details on network traffic between hosts						
Identify top 10 destinations communicating with a given device (source)						
Identify top N applications generating traffic from a device (source) for a user specified time period						
Access a network-wide view of the top-N sources, destinations, or applications						
D3. Reports						
Save report queries with relative dates						
Generate real-time reports						
Save reports to PDF for distribution/sharing						
Use saved reports to create scheduled reports that can be run automatically and emailed to recipients						
Create custom/ad-hoc report that includes various components from other pre-defined reports						
Create capacity planning reports that report days to threshold						
View trend reports for test/devices						
View related/complimentary metrics in a single graph/report						
View status grid by time for all tests for a device, and drill down on any time-period to see details						
View 95% percentile reports (e.g. performance reports)						
D4. Topology and Map Views						
Access graphical representation of devices in network, including the status & dependency relationships						
Access device information in the graphical representation by mousing over and/or clicking on device						
Access graphical representation of devices, organized by geographical location						
View status of services on a geographical map showing direct and indirect dependencies						
Drill down on hot spots from geographical view to see device level details						
Filter network map to isolate a service and its components and view dependencies						
E. Administration and Archtecture						
E1. Troubleshooting						
Invoke trouble-shooting tools from various status views						
Support pinging, tunneling, logging-into, etc. of devices for the purpose of trouble-shooting						
E2. Administration Capabilities						
Access Command Line Interface						
Specify scheduled maintenance periods to automatically suspend and resume tests for devices						
Utilize CLI to add/delete multiple devices						
Utilize CLI to Change thresholds across multiple devices						
Utilize CLI to change polling interval for multiple tests across multiple devices						
Use CLI to assign escalation or notification rule to multiple tests across devices						
E3. Signature Library						
Utilize supplied VMWare monitor						
Verify integration with vCenter and continuous monitoring of VMs configured with vMotion technology						
Utilize a supplied server monitor (applicable to your infrastructure)						
Utilize a supplied application monitor (applicable to your infrastructure)						
Utilize a supplied network monitor (applicable to your infrastructure)						
Create and utilize a new plug-in Java monitor						

Create and utilize a new plug-in script monitor					
E4. Integration API					
Authenticate user through verification via an external system (e.g. LDAP)					
Create work/trouble ticket in external ticketing system					
Inject data through an external data feed (behaves like data was collected by monitoring system itself)					
Programmatically access key objects, such as devices, tests, containers, users, etc					
Provide bulk import tools for configuration data, utilizing APIs					
E5. Plug-in Framework					
Support creation of pug-in monitors					
Support plug-in Java monitors and plug-in Script monitors					
Support plug-in actions that can invoke external systems, and pass data to external systems					
Ability to develop & add new device plug-in monitors with dev. effort of a few days to 1 week					
E6. Distributed, Resilient Architecture					
Verify agent-less data collection approach					
Verify horizontal scalability of data collection mechanism, and ease of scalability as well					
Verify polling, alerting and notification, even when data collectors are isolated					
Collect monitoring data from devices that are behind a secured fire-wall					
Execute performances test to see if there are any bottlenecks (e.g. DB) or single points of failure					