



SUN'S CONTROLTOWER APPLIANCE (CTA)

SunSM Remote Operations Management
White Paper
October 2008

This page left intentionally blank.

Table of Contents

Executive Summary	1
What is Sun's ControlTower Appliance	1
CTA Architecture	2
Predictive Collectors	2
Communication Protocols (Receptors)	2
Proactive Polling	3
XML Encapsulation	3
Event Filtering and Customization	4
Event Persistence	4
Event Transport	4
Management Access	5
Bastion Hosts	5
Application and Infrastructure Management	6
Summary	6

This page left intentionally blank.

Executive Summary

SunSM Remote Operations Management offers remote IT operations management that allows you to align your IT competencies with your critical business objectives. Sun securely delivers monitoring and management services within an ITIL-based framework to help you remain process-oriented while maximizing your environment's availability. Sun takes a systematic approach to provide you with a structured set of operational functions that help keep your environment running at peak performance.

In addition, Sun provides you with an integrated service delivery platform that helps enable full visibility into IT systems and the underlying business processes that these systems support. The cornerstone of this service delivery platform is the ControlTower Appliance (CTA), which allows Sun to stay connected to your environment 24x7, so you don't have to. The fundamental benefit of the CTA is that it provides secure remote operations management—anytime, anywhere.

What is Sun's ControlTower Appliance

Sun's ControlTower Appliance (CTA) is a proprietary, innovative tool designed to enable the secure management and monitoring of networks, devices, operating systems, and applications. This technology is based on the transfer of nonguaranteed protocols, such as Simple Network Management Protocol (SNMP) and User Datagram Protocol (UDP), over the public Internet and on-demand private networking for the execution of management support. The CTA features receptors that can be coded to monitor nearly any piece of infrastructure, anywhere in the world. This scalable tool currently handles hundreds of simultaneous alarms, and performs reliably by storing and forwarding data when the Internet is not available.

A key component of the Sun Remote Operations Management solution, the CTA enables Sun to deliver remotely monitored and managed IT operations services 24x7, to any location worldwide. This patent-pending technology represents Sun's third-generation monitoring and management platform, and possesses the features and form that make it the ideal platform to deploy in both service provider and corporate datacenters.

All successfully monitored devices and applications share three key monitoring metrics:

- **Reactive** – The device/application initiates the sending of an event to signify a change in state
- **Proactive** – An external entity connects to the device/application and queries its health
- **Predictive** – An external entity collects trended information over time to look for resource constraints or chronic issues occurring on the device/application

The CTA platform provides the tools to effectively monitor these metrics.

CTA Architecture

Sun developed the CTA to be extensible via hot swappable software modules built in pure Java™ technology. Through this architecture, the CTA can be extended to support new monitoring protocols simply and without impacting the overall architecture while maintaining many of its abstract interfaces. These interfaces provide common functionality across the platform, including filtering, event customization, and persistence of events.

A unique feature of the CTA is its ability to dynamically reconfigure its footprint based on traffic type and load. For example, should the CTA receive a high volume of SNMP traffic, the system changes its parameters to more efficiently receive SNMP at the expense of a few milliseconds delay on the delivery of events back to Sun. When the load returns to normal, the CTA removes these extra handlers to scale back to normal operating parameters.

Predictive Collectors

Predictive collectors query device/application agents (i.e., SNMP) to retrieve Key Performance Indicators (KPIs) such as CPU usage, memory usage, and swap, as well as lower-level indicators such as network performance (both throughput and errors). Over time these KPIs show trends in both the overall health of the application and also capacity bottlenecks. This method of monitoring has also been very successful in detecting new types of denial-of-service attacks against customers' environments. Predictive data is available in graphical form within the Sun ControlPoint management portal, where customers can interrogate and interact with data.

Communication Protocols (Receptors)

Receptors provide the reactive interface that allows devices/applications to send events to the CTA. Sun developed these receptors with extremely low latency and high throughput, so they are capable of handling hundreds of events per second. This design is required because many reactive events are delivered over unreliable IP protocols such as UDP (e.g., SNMP and SYSLOG). These protocols are based on widely adopted Internet Engineering Task Force (IETF) standards and, in some instances, they do not provide a mechanism for guaranteed delivery. The CTA receptor is designed with this in mind to ensure that the event data is captured locally and delivered to Sun's datacenter using a reliable transport.

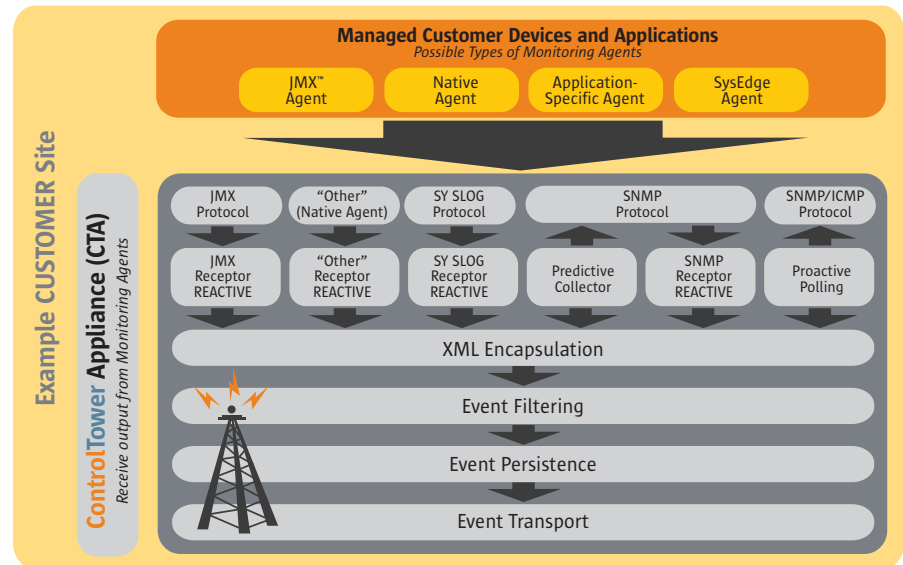


Figure 1: CTA architecture, designed for flexibility

Proactive Polling

Proactive polling is similar in design to the predictive interface, but focuses on more immediate indicators of impaired performance on the device or application. These indicators include information collected from the host itself, such as CPU utilization, in addition to information from external services that the device performs from the network, such as HTTP, Java DataBase Connectivity (JDBC™), and Internet Control Message Protocol (ICMP). Should these external services fall below thresholds (e.g., page load time > required or extended network latency), the CTA generates a failed condition and begins to exercise retry logic associated with each protocol. Should the retry also fail, an alarm is generated. This custom protocol retry algorithm eliminates many false positives from monitoring systems.

XML Encapsulation

The CTA normalizes events after they are polled or received by passing them through an XML encapsulation layer. Each event type (reactive, predictive, and proactive) is described using a Document Type Definition (DTD). Describing events in this manner has many benefits, including providing interoperability within Sun core systems and enabling customer to easily extend monitoring capabilities without the need to implement software modules again. A good example of this is the event-filtering interface. Because data is normalized, the interface no longer needs to understand the characteristics of each event type. Instead, it is able to apply processing rules across many types of events.

Event Filtering and Customization

Event filtering is another key characteristic of the CTA platform. In many cases, particularly with network and security devices, granular control of reactive events is significant but not possible. This lack of control results in many events that add little value being delivered to the CTA. The filtering layer permits the CTA to look for specific key words (or the lack of them in the case of negative matching) to prevent these events from entering the systems. A good example of this filtering is monitoring VPN devices. With these devices, many of the received events only signify positive status of a VPN, where the key reactive information is that of failed conditions. CTA rules permit exclusion of this information via one simple interface. The same filtering logic is also used to drive the event customizing feature. This feature provides a means to modify messages or grade severity level based on specific pattern match.

Event Persistence

The CTA typically delivers event information back to Sun via the Internet. Due to the nature of the Internet, it is not always possible to guarantee the availability of an outbound connection. The persistence layer works closely with the transport layer to queue events for delivery, and only removes them from the queue once the event is confirmed to have arrived using the CTA handshake protocol. The CTA is capable of working in a store-and-forward mode for many hours without losing any event information. When the CTA initiates its store-and-forward mode, an alarm is generated at the Sun ControlCenter so that an engineer can be engaged to troubleshoot this issue. In sites where Internet connectivity is not available, the CTA may also use private circuits or IPSec VPN encapsulation of the CTA transport.

Event Transport

Transportation of events occurs between the CTA and ControlTower servers located at Sun Remote Operations Management datacenters. All traffic from the CTA uses the push paradigm, which prevents the need for an inbound connection to provide monitoring/reporting services. Sun believes strongly in using open and auditable protocols between systems. To this end, all communications transport between the CTA and ControlTower servers takes place over HTTPS. Using known, open standards and secured ControlTower servers allows customers to implement simple security controls to permit only outbound HTTPS traffic between the CTA and ControlTower servers. These standards also prevent the need to make significant changes to customers' security policies.

Management Access

In addition to monitoring devices and applications, the CTA also provides a secure management channel called JumpGate for customers who want management services. JumpGate builds on the fundamental security principles defined by the C.I.A. Model— Confidentiality, Integrity, Availability—to help ensure that all action performed on the customer's behalf is completed in a secure manner and is fully accountable.

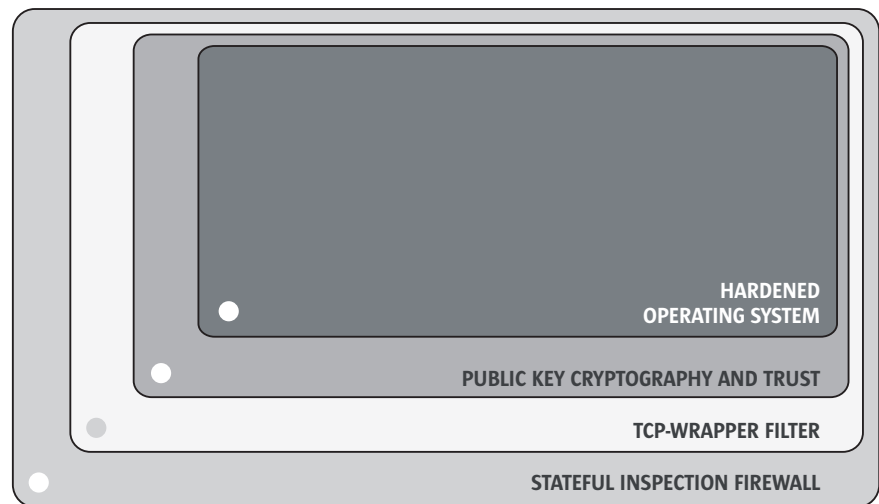


Figure 2: Maximum security design

Bastion Hosts

Access to JumpGate is restricted to only Sun hardened bastion hosts located within Sun datacenters by use of three independent security controls: firewall, tcp_wrappers, and public key trust. Bastion hosts require engineers to provide a strong authentication token before access is permitted. This authentication and all access are logged to a central logging server, which provides detailed audit trails of actions performed by Sun Remote Operations Management engineers. The customer is required to permit SSH2 traffic from the bastion hosts to the CTA. Again, SSH2 is a known and open protocol that makes securing this traffic easy to accomplish.

Management traffic between the bastion host and the CTA is encrypted using the 3DES algorithm often referred to as military-grade encryption. An extra layer of security is added by the CTA itself that only permits access from the bastion hosts using both firewall and tcp_wrapper technologies and requires a public key infrastructure (PKI) based authentication for each engineer before access is permitted. Each login (both successful and failed) is treated as a significant event that the CTA sends back to the ControlTower server for additional audit log creation.

Application and Infrastructure Management

Once connected and authenticated to the CTA, the Sun engineer is then able to launch a native management application to manage the device in question. The CTA supports management access via Windows Terminal Services, SSH, and Telnet. This management traffic only passes between the CTA and the customer's device. The traffic between the CTA and bastion host contains only keyboard, video, and mouse movements. At no point is the bastion host directly interacting with the customer's device. This mode of operation allows customers to implement the same security controls Sun provides within their own network building on the security-in-depth principle.

Each management protocol requires the Sun engineer to also authenticate again to the customer's device using native authentication provided by that device. Sun requires a dedicated account on each device for management access to provide full accountability of actions. The combination of Sun and the customer authentication records generates a fully accountable trail of actions performed by Sun on behalf of the customer.

Summary

The ControlTower Appliance encapsulates Sun's operational experience in developing a management and monitoring platform capable of delivering service to today's technology with an eye on emerging advancements in both management and monitoring services and protocols. Its small footprint and support for unreliable transport makes it ideal for delivery in both an Internet datacenter and a corporate datacenter.

This page left intentionally blank.

