

VCC

Sarbanes-Oxley Compliance

Executive Summary

Global Maintech's Virtual Command Center (VCC) continues to lead in the development of new features for IT center operations. New features aid IT in compliance with the Sarbanes-Oxley Act. For example, VCC's AAA Security includes authentication, authorization, and auditing capabilities to ensure compliance. You will know that only authorized personnel have access to critical computer operations and that their activities are logged for later retrieval in their entirety.

The VCC's features are consistent with recommendations of a number of the Sarbanes-Oxley experts. Scott Wyban¹ and Randy Favero² have described the authentication features a must to be in compliance with the act.

The VCC runs on the latest, most secure Linux systems including the latest Red Hat servers with the NSA Security Enhanced Kernel. VCC provides an outboard solution that is not affected by any security problems of the systems it monitors and controls.

The VCC also offers customers the ability to log what other vendors' personnel are doing in your data center. Some of our customers ask vendors to go through VCC to access their products maintenance facilities, both locally and remotely. For example, a major bank's IBM Shark storage units are accessed via VCC, with auditing turned on.

VCC is ready and capable for monitoring and controlling that includes the Sarbanes-Oxley features to run economically from 1 or 2 systems all the way up to 600.

The following is a more detailed discussion of these critical features:

Authentication

VCC users must log in to the VCC server to use any of its facilities. The Linux telnet daemon is normally turned off. Thus, log in must be done via SSH. Linux's OpenSSH is a state of the art SSH implementation. Password logins should be turned off and some combination of X509 certificates, LDAP and RSA keys should be used to provide the best current day authentication commonly available. In addition, key cards and other security devices can be used. Thus management can be assured that state of the art authentication is used.

For full Sarbanes-Oxley compliance, LDAP should be used.

VCC uses X-Window displays tunneled over SSH for its GUI operation. This insures that all traffic between users' PCs and VCC is encrypted with state of the art encryption technology, making it almost impossible for eavesdroppers to monitor console traffic.

¹ Vice president of Corporate Communications for Boulder Corp.

² Vice president and general manager for Novell Corp.

Authorization

Sites can tailor separate VCC capabilities per user, group, console, monitored system and feature.

VCC's facilities are available via accounts created by each customer for each user. Every authorized member of the operations and support staff is assigned their own user identification on the VCC server.

All VCC users are assigned to groups. These groups govern what VCC facilities are available to users in the group. The VCC administrator can restrict group access to not have knowledge of individual consoles, only be allowed to view a console or have the ability to both view consoles and use them to enter commands.

Another, more privileged group is the VCC administrative group. Users in this group can administer the VCC configuration, scripts, users and groups. Each VCC facility and resource is governed by authorization.

Auditing and Accountability

Every VCC user's activities are logged for auditing purposes. This includes log in, opening VCC's windows, use of menu and dialog facilities.

Every keystroke from each console (whether or not displayed) is logged and every character output (whether or not displayed) is logged and stored. The information in the log for each console includes the name of the user logged into the VCC, each character typed, and the time of the day. VCC logs are backed up as needed.

This provides 100% auditing of who typed what and when on any console that is monitored.

In Summary

VCC's distinct advantage that arises from its continued development, along with its outboard operation, prevents manipulation without leaving tracks. Inboard systems do not have this capability. The key questions that executives should be asking their IT managers are:

1. Do the current operations facilities require the appropriate authentication and authorization to prevent improper use?
2. Does the facility log every keystroke so that improprieties are logged and retrieved to allow easy determination by whom and when they occur?