Symantec™ Critical System Protection Version 5.2 RU8 UNIX Baseline Policy Reference Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 5.2.8

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing the UNIX Baseline Detection policy

This chapter includes the following topics:

Introduction

The Host Intrusion Detection policies have been redesigned and rewritten to enhance stability, provide greater ease of use and detection accuracy, and add functionality. Multiple policies have been reorganized into two baseline monitoring solutions for the Windows and the UNIX operating system environments.

- The Windows Baseline Detection Policy became available in release 5.2.6 (5.2 RU6).
- The UNIX Baseline Detection Policy became available in release 5.2 RU7.

The UNIX Baseline Detection policy includes the following improvements:

- The IDS policy has been rewritten to improve functionality and accuracy in monitoring security events.
- The file monitoring area has been redesigned and rewritten to provide a large number of new file and directory monitoring functions. For example, you can now control and enable the access, delete, modify, and create change monitoring functions by group.
- You can now perform advanced rule-by-rule tuning directly from the Symantec Critical System Protection console. These rules now also use ignore logic and select logic methodology.
- You can now configure and view all rule content from the Symantec Critical System Protection console, which removes the need to use the Authoring Tool.

- Policy option group naming conventions have been standardized for ease of administration. You can now enable and disable entire areas of the policies with option check boxes.
- Automatic application detection has been updated to enable and disable monitoring without the need for administrators to configure the policy individually per host.
- You can now configure many parameter options individually for each rule. For example, you can configure the Rule Name, Rule Severity, and Rule monitoring content separately for each rule.
- You can now select a severity level for each rule. You no longer need to know specific numerical values for the severity base types.
- New Web attack detection functionality has been built into the policy to provide monitoring of Web attacks. The types of attacks that are detected include basic SQL injection, directory traversal, vulnerable CGI requests, blacklist IP functionality, and vulnerability scanning detection. Malicious request strings, malicious extension requests, and malicious user agent strings are also detected.
- You can now mouse over parts of the user interface to display descriptions to assist in policy navigation and rule-by-rule overview.

UNIX-specific policy changes include the following improvements:

- Monitoring of individuals who log off of host systems.
- New compatibility with Symantec AntiVirus for Linux for monitoring Symantec software.
- New command monitoring that is accomplished by configuring the text log monitoring of user-defined or root bash or ksh history files. Superuser DO (sudo) commands are specifically monitored for privileged command inspection and retention. This new functionality provides the ID of the user who performs the command, the exact command performed, and a datestamp and timestamp. This functionality helps to meet various regulatory compliance requirements.
- Monitoring of suspicious binary file permission changes. This change helps to ensure that critical command-line executables are not subject to the malicious permissions changes that malware typically performs.
- Monitoring of malicious Loadable Kernel Modules (LKMs) to detect the loading of known malware-related LKM modules.
- Addition of a new **System Hardening Monitor**, which generates events when new auto start daemons or programs, such as the rc.d script, are added. It also monitors specific changes to inittab, a critical system configuration file.

- New UNIX malware detection that tracks file and directory creation activities from known UNIX forms of malware. Malware detection variants include rootkit detection and worm detection.

Table 1-1 illustrates how the existing policies from previous releases were combined with new options into the 5.2 RU7 top-level option groups.

Table 1-1 Detection options organization map

Options in previous releases	Detection option organization in release 5.2 RU7
User/Group_Configuration Privileged_User/Group_Configuration	System User and Group Change Monitor
System_Logon_Failure System_Logoff_Success System_Failed_Access_Status	System Login Activity and Access Monitor
System_SUDO_Monitor System_Root_Command_Monitor System_User_Command_Monitor	System Privilege Command and Bash History Monitor
System_AutoStart_Change (rc*.d) System_Service_Config_Monitor System_Xserver_Configuration System_RunLevel_Monitor (Inittab) System_Sysconfig_Monitor (Sysconfig)	System Hardening Monitor
Host_IDS_File_Tampering Critical_System_File_Monitor	System File and Directory Monitor
Symantec_AV_Linux_Client_Comms Symantec_AV_Unix_Client_Comms	System Symantec Software Monitor
USB_Connectivity_Activity CD/DVD_Burning_Activity	System External Device Activity Monitor
Generic_Web_Attack_Detection Malicious_LKM_Detection Unix_Generic_ Malware_and _Rootkit_Detection	System Attack Detection

Policy options

This chapter includes the following topics:

System User and Group Change Monitor

This option group section of the policy monitors for specific user and group change-based events.

Global User and Group Change Monitor Settings

Monitors user and group events such as when a user is added or deleted. Changes are detected by the user_monitor.sh script that monitors user configuration system files.

Table 2-1 Description of the **Monitor User and Group File(s) Checksum** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Global User and Group Change Monitor Settings
Option	Monitor User and Group File(s) Checksum
Description	Detects the changes that are made to global user and group accounts on the local system. The checksum is calculated at agent startup to determine whether the files was modified since Symantec Critical System Protection was last shut down.

Table 2-2 Description of the **User and Group Monitor Polling Interval** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Global User and Group Change Monitor Settings
Option	User and Group Monitor Polling Interval
Description	Sets how often files are polled for changes in status. A short polling interval could possibly impact system performance.

Table 2-3 Description of the **User and Group Configuration File Paths** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Global User and Group Change Monitor Settings
Option	User and Group Configuration File Paths
Description	Sets the configuration files to be monitored.

System User Configuration Changes

Detects changes in user accounts, such as the creation or deletion of a user, and changes in parameters such as user name, home directory, login shell, and so on.

Table 2-4 Description of the **User Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Created
Rule Name	User_Created
Severity	Warning
Description	Detects the creation of user accounts on the local system. **Note:** If this rule is unchecked, you cannot monitor user name change events.

Table 2-5 Description of the **User Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User Deleted
Rule Name	User_Deleted
Severity	Warning
Description	Detects the deletion of user accounts on the local system.

Table 2-6 Description of the **User's Password Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Password Changed
Rule Name	User_Password_Changed
Severity	Notice
Description	Detects the changes to users' passwords in user accounts on the local system.

Table 2-7 Description of the **User's Name Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Name Changed
Rule Name	User_Name_Changed
Severity	Notice
Description	Detects the changes to users' names in user accounts on the local system.

Table 2-8 Description of the **User's ID Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's ID Changed
Rule Name	User_ID_Changed
Severity	Notice
Description	Detects the changes that are made to users' IDs in system user accounts on the local system.

Table 2-9 Description of the **User's Primary Group Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Primary Group Changed
Rule Name	User_Primary_Group_ID_Changed
Severity	Notice
Specific Primary Groups	Sets user-defined groups. Default value is all groups.
Description	Detects the changes that are made to users' primary group ID numbers in system user accounts on the local system.

Table 2-10 Description of the **User's Full Name Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Full Name Changed
Rule Name	User_Full_Name_Changed
Severity	Notice
Description	Detects the changes that are made to users' full names in system user accounts on the local system.

Table 2-11 Description of the **User's Home Directory Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Home Directory Changed
Rule Name	User_Home_Directory_Changed
Severity	Warning
Description	Detects the changes that are made to users' home directories in system user accounts on the local system.

Table 2-12 Description of the **User's Login Shell Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Login Shell Changed
Rule Name	User_Login_Shell_Changed
Severity	Warning
Description	Detects the changes that are made to users' login shells in system user accounts on the local system.

Table 2-13 Description of the **User's Minimum Password Age Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Minimum Password Age Changed
Rule Name	User_Minimum_Password_ Age_Changed
Severity	Warning
Description	Detects the changes that are made to users' minimum password age parameter in system user accounts on the local system.

Table 2-14 Description of the **User's Maximum Password Age Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Maximum Password Age Changed
Rule Name	User_Maximum_Password_ Age_Changed
Severity	Warning
Description	Detects changes in users' maximum days between password changes parameter in system user accounts on the local system.

Table 2-15 Description of the **User's Maximum Days of Account Inactivity Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Maximum Days of Account Inactivity Changed
Rule Name	User_Passwd_ Inactivity_Days_Changed
Severity	Warning

Table 2-15 Description of the **User's Maximum Days of Account Inactivity Changed** parameters used *(continued)*

Parameter	Description
Description	Detects changes in the parameter that sets the maximum number of days that users can go without logging into their accounts before the account is made inactive.

Table 2-16 Description of the **User's Account Expiry Date Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Account Expiry Date Changed
Rule Name	User_Account_Expiry_Date_Changed
Severity	Warning
Description	Detects changes in the date when users' logins automatically expire.

Table 2-17 Description of the **User's Password Expire Warning Date Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Password Expire Warning Date Changed
Rule Name	User_Password_Expire_Warning_Date_Changed
Severity	Warning
Description	Detects changes in the date when users are warned that their password is about to expire.

Table 2-18 Description of the **User's Attribute Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System User Configuration Changes
Option	User's Attribute Changed

Table 2-18 Description of the **User's Attribute Changed** parameters used *(continued)*

Parameter	Description
Rule Name	User_Attributes_Changed
Severity	Warning
Description	Detects changes in users' attributes that are located in the /etc/user_attr file on the local system.

System Group Configuration Changes

This option subgroup section of the policy monitors for specific group configuration change-based events, such as the creation and deletion of groups.

Table 2-19 Description of the **Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Configuration Changes
Option	Group Created
Rule Name	Group_Created
Severity	Warning
Description	Detects the creation of a group. **Note:** If this rule in unchecked, you cannot monitor changes in a group's name.

Table 2-20 Description of the **Group Deleted** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Configuration Changes
Option	Group Deleted
Rule Name	Group_Deleted
Severity	Warning

Table 2-20 Description of the **Group Deleted** parameters used *(continued)*

Parameter	Description
Description	Detects the deletion of a group. **Note:** If this rule in unchecked, you cannot monitor changes in a group's name.

Table 2-21 Description of the **Group Membership Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Configuration Changes
Option	Group Membership Changed
Rule Name	Group_Membership_Change
Severity	Warning
Specific Membership Groups	Sets user-defined membership groups. Default value is all groups.
Description	Detects the addition or deletion of a user from a group.

Table 2-22 Description of the **Group Name Change** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Configuration Changes
Option	Group Name Change
Rule Name	Group_Name_Changed
Severity	Warning
Description	Detects a change in the name of a group. Group created and group deleted events are generated for group name changes.

Table 2-23 Description of the **Group Lock Flag Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Configuration Changes

Table 2-23 Description of the **Group Lock Flag Changed** parameters used *(continued)*

Parameter	Description
Option	Group Lock Flag Changed
Rule Name	Group_LockFlag_Changed
Severity	Warning
Description	Detects the changes to a group's lock flag.

Table 2-24 Description of the **Group ID Changed** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > System Group Configuration Changes
Option	Group ID Changed
Rule Name	Group_ID_Changed
Severity	Warning
Description	Detects the changes to a group's ID.

Privileged User and Group Configuration Activity

This option subgroup section of the policy monitors for privileged user and group configuration change-based events, such as the creation of superusers and superuser groups.

Table 2-25 Description of the **Superuser (root level) User Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Privileged User and Group Configuration Activity
Option	Superuser (root level) User Created
Rule Name	Superuser_Account_Created
Severity	Major
Description	Detects the creation of a superuser account.

Table 2-26 Description of the **Superuser (root level) Group Created** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Privileged User and Group Configuration Activity
Option	Superuser (root level) Group Created
Rule Name	Superuser_Group_Created
Severity	Major
Description	Detects the creation of a superuser account.

Table 2-27 Description of the **User's Global ID Changed to Superuser** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Privileged User and Group Configuration Activity
Option	User's Global ID Changed to Superuser
Rule Name	User_ID_Changed_to_Superuser
Severity	Critical
Description	Detects when a user's ID is changed to be a member of a superuser global group ID.

Table 2-28 Description of the **Group's Global ID Changed to Superuser** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Privileged User and Group Configuration Activity
Option	Group's Global ID Changed to Superuser
Rule Name	Group_ID_Changed_to_Superuser
Severity	Critical
Description	Detects when a group's ID is changed to be a member of a superuser global group ID.

Table 2-29 Description of the **User's Primary Group ID Changed to Superuser** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Privileged User and Group Configuration Activity
Option	User's Primary Group ID Changed to Superuser
Rule Name	User_PrimaryID_Added_SuperuserID_Change
Severity	Critical
Description	Detects when a user's primary group ID is changed to be a member of a root group ID.

Table 2-30 Description of the **Group Membership Changed User to Superuser** parameters used

Parameter	Description
Option Path	System User and Group Change Monitor > Privileged User and Group Configuration Activity
Option	Group Membership Changed User to Superuser
Rule Name	Root_Group_Added_SuperuserID_Change
Severity	Critical
Description	Detects when a user is added as a member of the root superuser group.

System Login Activity and Access Monitor

System Login Success Monitor

This option group section of the policy monitors specific logon and access events, including those that use FTP, telnet, rlogin, SSH, the local console, and the su utility.

FTP logon Options

This option group section of the policy monitors logons that occur over FTP.

FTP server reports to syslog

Set this option if your FTP servers report to syslog. On HP-UX operating systems, the wtmp file is also used to identify successful logons.

Table 2-31 Description of the **Root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > FTP logon Options > FTP server reports to Syslog
Option	Root logon
Rule Names	Root_FTP_Logon_Success_syslog
Severity	Warning
Description	Detects users who use FTP to log on as root.

Table 2-32 Description of the **Non-root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > FTP logon Options > FTP server reports to Syslog
Option	Non-root logon
Rule Names	User_FTP_Logon_Success_syslog
Severity	Warning
Description	Detects non-root users who use FTP to log on.

Server reports to a log file

Set this option if your FTP servers report to a log file. You must specify the pthe to the FTP log file.

Table 2-33 Description of the **Log Location** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > FTP logon Options > FTP server reports to a log file
Option	Log Location
Path	/var/log/vsftpd.log

Table 2-33 Description of the **Log Location** parameters used *(continued)*

Parameter	Description
Description	Sets the path to the FTP log file.

Table 2-34 Description of the **Root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > FTP logon Options > FTP server reports to a log file
Option	Root logon
Rule Name	Root_FTP_Logon_Success_Text_Log
Severity	Notice
Description	Detects root logon events that occur over FTP.

Table 2-35 Description of the **Non-root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > FTP logon Options > FTP server reports to a log file
Option	Non-root logon
Rule Name	User_FTP_Logon_Success_Text_Log
Severity	Notice
Description	Detects non-root user logon events that occur over FTP.

Telnet and Rlogin logon Options

This option group section of the policy monitors log ons that occur over Telnet and rlogin. The events are identified using the UNIX syslog. On HP-UX operating systems, the wtmp file is also used.

Table 2-36 Description of the **Root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > Telnet and Rlogin logon Options

Table 2-36 Description of the **Root logon** parameters used *(continued)*

Parameter	Description
Option	Root logon
Rule Name	Root_Telnet_Rlogin_Logon_Success
Severity	Warning
Description	Detects root logon events that occur over Telnet and rlogin.

Table 2-37 Description of the **Non-root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > Telnet and Rlogin logon Options
Option	Non-root logon
Rule Name	User_Telnet_Rlogin_Logon_Success
Severity	Warning
Description	Detects non-root users that log on over Telnet and rlogin.

SU Operation Options

This option group section of the policy monitors logons that involve the su utility. The events are identified using the UNIX syslog.

Table 2-38 Description of the **Root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SU Operation Options
Option	SU to root
Rule Name	SU_ToRoot_Success
Severity	Warning
Description	Detects the successful logons as root, monitored in the UNIX syslog.

Table 2-39 Description of the **Non-root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SU Operation Options
Option	SU to non-root
Rule Name	SU_ToUser_Success
Severity	Notice
Description	Detects the successful logons of non-root users.

SSH Remote logon Options

This option group section of the policy monitors log ons that occur over SSH. The events are identified using the UNIX syslog. On HP-UX operating systems, the wtmp file is also used.

Table 2-40 Description of the **Root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SSH Remote logon Options
Option	Root logon
Rule Name	Root_SSH_Logon_Success
Severity	Warning
Description	Detects logons as root that occur over SSH.

Table 2-41 Description of the **Non-root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SSH Remote logon Options
Option	Non-root logon
Rule Name	User_SSH_Logon_Success
Severity	Notice
Description	Detects non-root user logons that occur over SSH.

Local Console logon Options

This option group section of the policy monitors successful logons from the local console. The events are identified using the UNIX syslog. On HP-UX operating systems, the wtmp file is also used.

Table 2-42 Description of the **Root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > Local Console logon Options
Option	Root logon
Rule Name	Root_Local_Logon_Success
Severity	Warning
Description	Detects root user logon events that occur over the console.

Table 2-43 Description of the **Non-root logon** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > Local Console logon Options
Option	Non-root logon
Rule Name	User_Local_Logon_Success
Severity	Warning
Description	Detects non-root user logon events that occur over the console.

System Logoff Monitor

This option group section of the policy monitors successful root and user log offs from the local console and from remote access.

SU Operation Options

su command events are monitored from the UNIX syslog.

Table 2-44 Description of the **SU to root Logoff** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Logoff Monitor > SU Operation Options
Option	SU to root Logoff
Rule Name	SU_ToRoot_Logoff
Severity	Warning
Description	Detects the successful attempts to SU to root.

Table 2-45 Description of the **SU to non-root Logoff** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Logoff Monitor > SU Operation Options
Option	SU to non-root Logoff
Rule Name	SU_ToUser_Logoff
Severity	Warning
Description	Detects the successful attempts to SU to a non-root user.

SSH Remote Logoff Options

This option group section of the policy monitors successful logoffs from remote consoles. The events are identified using the UNIX syslog. On HP-UX operating systems, the wtmp file is also used.

Table 2-46 Description of the **Root logoff** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SSH Remote logoff Options
Option	Root logoff
Rule Name	Root_SSH_Logoff
Severity	Warning

Table 2-46 Description of the **Root logoff** parameters used *(continued)*

Parameter	Description
Description	Detects root user logoff events that occur over SSH from a remote console.

Table 2-47 Description of the **Non-root logoff** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SSH Remote logoff Options
Option	Non-root logoff
Rule Name	User_SSH_Logoff
Severity	Warning
Description	Detects non-root user logoff events that occur over SSH from a remote console.

Local Console Logoff Options

This option group section of the policy monitors successful logoffs from local consoles. The events are identified using the UNIX syslog. On HP-UX operating systems, the wtmp file is also used.

Table 2-48 Description of the **Root Logoff** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SSH Remote logoff Options
Option	Root Logoff
Rule Name	Root_Local_Logoff
Severity	Warning
Description	Detects root user logoff events that occur on the local console.

Table 2-49 Description of the **Non-Root Logoff** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Login Success Monitor > SSH Remote logoff Options
Option	Non-Root_Logoff
Rule Name	User_Local_Logoff
Severity	Warning
Description	Detects non-root user logoff events that occur on the local console.

System Failed Login Monitor

This option group section of the policy monitors user and root failed logon attempts from the local console and by remote access. They report attempts to log on to services that include local console sessions, telnet, Xwin, rsh, rlogin, and FTP. They also report failed attempts to change identification by using the su utility.

FTP logon failure

Set this option to detect failed logons over FTP.

Repeated FTP logon failures

Set this option to detect users' repeated failures to log on. You can set the number of failures that have to occur and the time interval within which the failures have to occur.

Table 2-50 Description of the **Number of logon failures in time interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP logon failure>Repeated FTP logon failures
Option	Number of logon failures in time interval
Value	blank value The user specifies this value.

Table 2-50 Description of the **Number of logon failures in time interval** parameters used *(continued)*

Parameter	Description
Description	Detects repeated failed logon attempts. Set the number of times a user can fail to log on in a specific time interval before an event is generated.

Table 2-51 Description of the **Time interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP logon failure>Repeated FTP logon failures
Option	Time interval
Duration	In days, hours, minutes, and seconds.
Description	Sets a specific time interval during which the failed logon attempts have to take place to generate an event.

Table 2-52 Description of the **FTP Repeated Failed Severity** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP logon failure>Repeated FTP logon failures
Option	FTP Repeated Failed Severity
Severity	Major
Description	Sets the severity of failed logon attempts.

FTP server reports to Syslog or WTMP

Set this option to detect logon failures that are reported in the UNIX syslog or, on HP-UX operating systems, in the wtmp file.

Table 2-53 Description of the **Root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP server reports to Syslog or WTMP
Option	Root logon failure

Table 2-53 Description of the **Root logon failure** parameters used *(continued)*

Parameter	Description
Rule Name	Root_FTP_Logon_Failure
Severity	Notice
Description	Detects failed attempts to log on over FTP as a root user that are reported in the syslog or wtmp file.

Table 2-54 Description of the **Non-root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP server reports to Syslog or WTMP
Option	Non-root logon failure
Rule Name	User_FTP_Logon_Failure
Severity	Warning
Description	Detects failed attempts to log on as a non-root user over FTP that are reported in the syslog or wtmp file.

FTP server reports to a log file

Set this option if your FTP servers report to a log file. You must specify the pthe to the FTP log file.

Table 2-55 Description of the **Path to FTP server log file** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP logon failure > FTP server reports to a log file
Option	Path to FTP server log file
Path	/var/log/vsftpd.log
Description	Sets the path to the FTP server log file.

Table 2-56 Description of the **Root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP logon failure > FTP server reports to a log file
Option	Root logon failure
Rule Name	Root_FTP_Logon_Failure_Text_Log
Severity	Notice
Description	Detects failed attempts to log on over FTP as a root user.

Table 2-57 Description of the **Non-root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > FTP logon failure > FTP server reports to a log file
Option	Non-root logon failure
Rule Name	User_FTP_Logon_Failure_Text_Log
Severity	Notice
Description	Detects failed attempts to log on over FTP as a regular user.

Telnet and Rlogin logon failure

This option group section of the policy monitors user and root failed logon attempts over Telnet and rlogin. The events are identified using the UNIX syslog. On HP-UX operating systems, the btmp file is also used.

Repeated Telnet or Rlogin logon failures

Set this option to detect users' repeated failures to log on over Telnet and rlogin. You can set the number of failures that have to occur and the time interval within which the failures have to occur.

Table 2-58 Description of the **Number of Logon Failures in Time Interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor >Telnet and Rlogin logon failure>Repeated Telnet or Rlogin logon failures
Option	Number of Logon Failures in Time Interval
Value	blank value The user specifies this value.
Description	Detects repeated failed logon attempts. Set the number of times a user can fail to log on in a specific time interval before an event is generated.

Table 2-59 Description of the **Time interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor >Repeated Telnet or Rlogin logon failures
Option	Time Interval
Duration	In days, hours, minutes, and seconds.
Description	Sets a specific time interval during which the failed logon attempts take place.

Table 2-60 Description of the **Telnet Repeated Failed Severity** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor >Telnet and Rlogin logon failure>Repeated Telnet or Rlogin logon failures
Option	Telnet Repeated Failed Severity
Severity	Major
Description	Sets the severity of the Telnet or rlogin failed logon attempts.

Table 2-61 Description of the **Root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor >Telnet and Rlogin logon failure
Option	Root logon failure
Rule Name	Root_Telnet_Rlogin_Logon_Failure
Severity	Warning
Description	Detects failed attempts to log on over Telnet or rlogin as a root user.

Table 2-62 Description of the **Non-root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor >Telnet and Rlogin logon failure
Option	Non-root logon failure
Rule Name	User_Telnet_Rlogin_Logon_Failure
Severity	blank value The user specifies this value.
Description	Detects failed attempts to log on over Telnet or rlogin as a regular user.

SU failure

Set this option to detect failures that involve the su utility. The events are identified using the UNIX syslog. On HP-UX operating systems, the btmp file and btmps file are also used.

Repeated SU failures

Set this option to detect users' repeated failures to use the su utility. You can set the number of failures that have to occur and the time interval within which the failures have to occur.

Table 2-63 Description of the **Number of Logon Failures in Time Interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SU failure>Repeated SU failures
Option	Number of Logon Failures in Time Interval
Value	blank value The user specifies this value.
Description	Detects repeated failed logon attempts that use the SU command. You can set the number of times a user can fail to log on in a specific time interval before an event is generated.

Table 2-64 Description of the **Time interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SU failure>Repeated SU failures
Option	Time Interval
Duration	In days, hours, minutes, and seconds.
Description	Sets a specific time interval during which the failed logon attempts take place.

Table 2-65 Description of the **SU Repeated Failed Severity** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SU failure>Repeated SU failures
Option	SU Repeated Failed Severity
Severity	Major
Description	Sets the severity of the SU failed logon attempts.

Table 2-66 Description of the **SU to root failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SU failure
Option	SU to root failure
Rule Name	SU_ToRoot_Failure
Severity	Warning
Description	Detects repeated failed attempts to log on as a root user.

Table 2-67 Description of the **SU to non-root failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SU failure
Option	SU to non-root failure
Rule Name	SU_ToUser_Failure
Severity	Notice
Description	Detects repeated failed attempts to log on as a regular user.

SSH logon failure

Set this option to detect failures to log on over SSH. The events are identified using the UNIX syslog. On HP-UX operating systems, the btmp file is also used.

Repeated SSH logon failures

Set this option to detect users' repeated failures to log on over SSH. You can set the number of failures that have to occur and the time interval within which the failures have to occur.

Table 2-68 Description of the **Number of Logon Failures in Time Interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SSH logon failure>Repeated SSH logon failures
Option	Number of Logon Failures in Time Interval

Table 2-68 Description of the **Number of Logon Failures in Time Interval** parameters used *(continued)*

Parameter	Description
Value	blank value The user specifies this value.
Description	Detects repeated failed logon attempts that are tracked using syslog or the btmp file (HP-UX). Set the number of times a user can fail to log on in a specific time interval before an event is generated.

Table 2-69 Description of the **Time interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SSH logon failure>Repeated SSH logon failures
Option	Time Interval
Duration	In days, hours, minutes, and seconds.
Description	Sets a specific time interval during which the failed logon attempts take place.

Table 2-70 Description of the **SSH Repeated Failed Severity** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SSH logon failure>Repeated SSH logon failures
Option	SSH Repeated Failed Severity
Severity	Major
Description	Sets the severity of the SSH failed logon attempts.

Table 2-71 Description of the **Root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SSH logon failure
Option	Root logon failure
Rule Name	Root_SSH_Logon_Failure

Table 2-71 Description of the **Root logon failure** parameters used *(continued)*

Parameter	Description
Severity	Warning
Description	Detects repeated failed attempts to log on as a root user.

Table 2-72 Description of the **Non-Root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > SSH logon failure
Option	Non-Root logon failure
Rule Name	User_SSH_Logon_Failure
Severity	Notice
Description	Detects repeated failed attempts to log on as a regular user.

Local logon failure

This option group section of the policy monitors user and root failed logon attempts from the local console. The events are identified using the UNIX syslog. On HP-UX operating systems, the btmp file is also used.

Repeated local logon failures

Set this option to detect users' repeated failures to log on from the local console. You can set the number of failures that have to occur and the time interval within which the failures have to occur.

Table 2-73 Description of the **Number of Logon Failures in Time Interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > Local logon failure>Repeated local logon failures
Option	Number of Logon Failures in Time Interval
Value	blank value The user specifies this value.

Table 2-73 Description of the **Number of Logon Failures in Time Interval** parameters used *(continued)*

Parameter	Description
Description	Detects repeated local failed logon attempts that are tracked using syslog or the btmp file (HP-UX). Set the number of times a user can fail to log on in a specific time interval before an event is generated.

Table 2-74 Description of the **Time interval** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > Local logon failure>Repeated local logon failures
Option	Time Interval
Duration	In days, hours, minutes, and seconds.
Description	Sets a specific time interval during which the failed logon attempts take place.

Table 2-75 Description of the **Local Repeated Failed Severity** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > Local logon failure>Repeated local logon failures
Option	Local Repeated Failed Severity
Severity	Major
Description	Sets the severity of the failed logon attempts from the local console.

Table 2-76 Description of the **Root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor > Local logon failure
Option	Root logon failure
Rule Name	Root_Local_Login_Failure
Severity	Warning
Description	Detects repeated failed attempts to log on as a root user.

Table 2-77 Description of the **Non-root logon failure** parameters used

Parameter	Description
Option Path	System Login Activity and Access Monitor > System Failed Login Monitor >Local logon failure
Option	Non-root logon failure
Rule Name	User_Local_Login_Failure
Severity	Notice
Description	Detects repeated failed attempts to log on as a regular user.

System Privileged Command and Bash History Monitor

This option group section of the policy monitors for specific privileged command and bash events.

Sudo Monitoring Options

Global Sudo Monitoring Settings

Table 2-78 Description of the **Authorized Sudo Users, Strings, or Commands (whitelisted)** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > Sudo Monitoring Options > Global Sudo Monitoring Settings
Option	Authorized Sudo Users, Strings, or Commands (whitelisted)
Value	blank value The user specifies this value.
Description	Use to set up a user-defined list of users, strings, and commands that are monitored for use with the sudo command.

Table 2-79 Description of the **Banned Sudo Commands (blacklisted)** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > Sudo Monitoring Options > Global Sudo Monitoring Settings
Option	Banned Sudo Commands (blacklisted)
Value	*rm -rf /*
Description	Use to set up a user-defined list of commands that are monitored when used with the sudo command.

Sudo Command Monitor

Table 2-80 Description of the **Sudo Command Monitor** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > Sudo Monitoring Options
Option	Sudo Command Monitor
Rule Name	Baseline_Sudo_Command_Watch
Severity	Notice
Description	Detects use of the sudo command.

Sudo Command Failure Monitor

Table 2-81 Description of the **Sudo Command Failure Monitor** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > Sudo Monitoring Options
Option	Sudo Command Failure Monitor
Rule Name	Baseline_Sudo_Command_Failure
Description	Detects the failures of sudo command use.

Sudo Authorization Failure Monitor

Table 2-82 Description of the **Sudo Authorization Failure Monitor** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > Sudo Monitoring Options
Option	Sudo Authorization Failure Monitor
Rule Name	Baseline_Sudo_Authentication_Failure
Severity	Warning
Description	Detects failures in the authorization of the sudo command.

Additional Sudo Monitoring Options

Table 2-83 Description of the **Additional Sudo Monitoring Options** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > Sudo Monitoring Options
Option	Additional Sudo Monitoring Options
Rule Name	System_PrivCmd_BashHist_Sudo_AddContent
Severity	Info
Description	Detects use of the sudo command.

User Command History Options

Table 2-84 Description of the **User 1 Command History Monitor** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > User Command History Options
Option	User 1 Command History Monitor

Table 2-84 Description of the **User 1 Command History Monitor** parameters used *(continued)*

Parameter	Description
Rule Name	Baseline_User_Command_Watch
Severity	Notice
User's Bash History Log File Path	/home/user1/.bash_history
Description	Monitors the commands used by a specific user.

Table 2-85 Description of the **User 2 Command History Monitor** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > User Command History Options
Option	User 2 Command History Monitor
Rule Name	Baseline_User2_Command_Watch
Severity	Notice
User's Bash History Log File Path	/home/user2/.bash_history
Description	Monitors the commands used by a second specific user.

Superuser (Root Level) Command History Options

Table 2-86 Description of the **Root Command History Monitor** parameters used

Parameter	Description
Option Path	System Privileged Command and Bash History Monitor > Superuser (Root Level) Command History Options
Option	Root Command History Monitor
Rule Name	Baseline_Root_Command_Watch

Table 2-86 Description of the **Root Command History Monitor** parameters used *(continued)*

Parameter	**Description**
Severity	Notice
Root's Bash History Log File Path	/root/.bash_history
Description	Monitors the commands used by users who are logged in as root.

Table 2-87 Description of the **Superuser Command History Monitor** parameters used

Parameter	**Description**
Option Path	System Privileged Command and Bash History Monitor > Superuser (Root Level) Command History Options
Option	Superuser Command History Monitor
Rule Name	Baseline_Superuser_Command_Watch
Severity	Notice
Superuser's Bash History Log File Path	/home/superuser/.bash_history
Description	Monitors the commands used by user who are logged in as superuser.

System Hardening Monitor

This option group section detects changes to the user-configurable files that are considered sensitive in maintaining the security posture of the operating system. It detects modifications of the system configuration that change whether it automatically runs code during system startup. This behavior is normal if an administrator needs to change autorun behavior. If unexpected, it can indicate that the system is being prepared to operate outside established security policy, or that it is about to be compromised.

Various areas are monitored to generate events for the administrator if either of the following entities changed any of the selected values:

- Malware

- A malicious individual attempting to lower the security posture of the host system

Table 2-88 Description of the **Daemon Run Level RC.D Monitor** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Auto Start Change Options
Option	Daemon Run Level RC.D Monitor
Rule Name	AutoStart_RC.D_Monitor
Severity	Warning
File Paths	/etc/rc.* /etc/rc.d/*
Additional Settings	You can also monitor the following events: ■ Monitor Value Addition to Run Level Files ■ Monitor Value Removal to Run Level Files ■ Monitor File Modification ■ Monitor File Creation ■ Monitor File Removal
Description	Detects changes to the daemon rc files on the computer.

Table 2-89 Description of the **System Run Level INITTAB Monitor** parameters used

Parameter	Description
Option Path	System Hardening Monitor > System Auto Start Change Options
Option	System Run Level INITTAB Monitor
Rule Name	AutoStart_Inittab_Monitor
Severity	Warning
File Paths	/etc/inittab

Table 2-89 Description of the **System Run Level INITTAB Monitor** parameters used *(continued)*

Parameter	Description
Additional Settings	You can also monitor the following events: ■ Monitor Value Additions to the Inittab File ■ Monitor Value Removal to the Inittab File ■ Monitor File Modification ■ Monitor File Creation ■ Monitor File Removal
Description	Detects changes to the inittab file on the computer.

System File and Directory Monitor

This option group section of the policy monitors for file and directory changes. It also includes a completely rewritten file monitoring area that was renamed System FileWatch Monitor. This new area provides enhanced configuration options to enable more precise monitoring of file and directory additions, deletions, modifications, and access attempts.

System FileWatch Monitor

This option group section of the policy monitors additions, deletions, modifications, and access attempts to the system critical files that are listed as monitored files. If you use a default security posture, then Symantec Critical System Protection automatically sets up the filewatch monitor for you. If you use your own security posture, you must select the files that you want to monitor so that the filewatch monitor functions correctly.

A wide range of options that enable very specific tuning of how the file or directory is monitored are available for each rule. A global settings area sets the following parameters for all rules in the filewatch monitor area:

- Polling Interval: The interval in which the file watch engine polls or checks the files that are configured for change monitoring. This option is available to enable tuning of how frequently files are polled for changes. You may want to adjust the default polling rate if your environment has a large number of files to be monitored. This adjustment helps to ensure that resources are not overly used for the filewatch engine. A drop-down selection criteria area is provided to easily switch polling interval frequency.

- Search Depth: The search depth is a configurable parameter. It specifies the recursion level, or number of directories and subdirectories that are monitored when you apply a wildcard path. For more information on recursion level and search depth, see the path to the existing definition.

Monitor System-Critical Files

Table 2-90 Description of the **Core System Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Core System Files
Rule Name	FileWatch_Sys_Core_Files
Severity	Warning
Monitor Paths	/bin/* /lib/* /sbin/* /stand/vmunix /unix /usr/bin/* /usr/lib/* /usr/sbin/* /usr/spool/cron/* /var/adm/cron/* /var/lib/objrepos/* /var/spool/cron/*
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-90 Description of the **Core System Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor the core system files that the operating system maintains. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-91 Description of the **Core System Configuration Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Core System Configuration Files
Rule Name	FileWatch_Sys_Core_Configuration_Files
Severity	Warning
Monitor Paths	/etc/*.conf /etc/*/*.conf /etc/*/*_config /etc/*/*config* /etc/*_config /etc/*config*
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-91 Description of the **Core System Configuration Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor the core system configuration files that the operating system maintains. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-92 Description of the **Setup Programs and Packages** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Setup Programs and Packages
Rule Name	FileWatch_Sys_Setup_Files
Severity	Warning
Monitor Paths	/usr/sbin/pkg* /var/lib/rpm/* /var/sadm/install/admin/*
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-92 Description of the **Setup Programs and Packages** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor the setup programs and packages that the operating system maintains. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-93 Description of the **Common Daemon Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Common Daemon Files
Rule Name	FileWatch_Sys_Common_Program_Files
Severity	Warning

Table 2-93 Description of the **Common Daemon Files** parameters used *(continued)*

Parameter	Description
Monitor Paths	

Table 2-93 Description of the **Common Daemon Files** parameters used *(continued)*

Parameter	Description
	/etc/cron.d/logchecker /etc/fs/*/mount /lib/svc/nfs/lockd /lib/svc/nfs/statd /opt/sbin/in.named /opt/sbin/lwresd /opt/sbin/name /sbin/auditd /sbin/klogd /sbin/syslogd /usr/lib/cups/daemon/cups-lpd /usr/lib/fs/*/moun /usr/lib/sendmail /usr/lib/ssh/sshd /usr/lib/zones/zoneadmd /usr/local/sbin/in.named /usr/local/sbin/in.tnamed /usr/local/sbin/lwresd /usr/local/sbin/named /usr/local/sbin/sshd /usr/sbin/atd /usr/sbin/automount /usr/sbin/cron /usr/sbin/crond /usr/sbin/cupsd /usr/sbin/in.named /usr/sbin/in.tnamed /usr/sbin/inetd /usr/sbin/lwresd

Table 2-93 Description of the **Common Daemon Files** parameters used *(continued)*

Parameter	Description
	/usr/sbin/named /usr/sbin/nmbd /usr/sbin/rpc.mountd /usr/sbin/smbd /usr/sbin/sshd /usr/sbin/syslogd /usr/sbin/xinetd /usr/sfw/sbin/nmbd /usr/sfw/sbin/smbd
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor the common daemon files that the operating system maintains. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-94 Description of the **Monitor Script Files and Cron Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Monitor Script Files and Cron Files

Table 2-94 Description of the **Monitor Script Files and Cron Files** parameters used *(continued)*

Parameter	Description
Rule Name	FileWatch_Sys_Script_Files
Severity	Warning
Monitor Paths	blank value The user specifies this value.
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor the user-defined script files and cron files that are used on the computer. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-95 Description of the **Solaris Specific Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Solaris Specific Files
Rule Name	FileWatch_Sys_Other_Files_Solaris
Severity	Warning
Monitor Paths	blank value The user specifies this value.

Table 2-95 Description of the **Solaris Specific Files** parameters used *(continued)*

Parameter	Description
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled
Description	Lets you monitor the critical user-defined files that are specific to the Solaris operating system. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-96 Description of the **AIX Specific Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	AIX Specific Files
Rule Name	FileWatch_Sys_Other_Files_AIX
Severity	Warning
Monitor Paths	blank value The user specifies this value.
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-96 Description of the **AIX Specific Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor the critical user-defined files that are specific to the AIX operating system. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-97 Description of the **Linux Specific Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Linux Specific Files
Rule Name	FileWatch_Sys_Other_Files_Linux
Severity	Warning
Monitor Paths	blank value The user specifies this value.
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-97 Description of the **Linux Specific Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor the critical user-defined files that are specific to Linux operating systems. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-98 Description of the **HPUX Specific Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	HPUX Specific Files
Rule Name	FileWatch_Sys_Other_Files_HPUX
Severity	Warning
Monitor Paths	blank value The user specifies this value.
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-98 Description of the **HPUX Specific Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor the critical user-defined files that are specific to the HP-UX operating system. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

Table 2-99 Description of the **Tru64 Specific Files** parameters used

Parameter	Description
Option Path	System File and Directory Monitor > System FileWatch Monitor > Monitor System-Critical Files
Option	Tru64 Specific Files
Rule Name	FileWatch_Sys_Other_Files_Tru64
Severity	Warning
Monitor Paths	blank value The user specifies this value.
Monitor Ops	Deleted, Created, Modified Accessed (not enabled by default)
Report File Differences	Available, Not Enabled
Date and Time Restriction	Available, Not Enabled

Table 2-99 Description of the **Tru64 Specific Files** parameters used *(continued)*

Parameter	Description
Description	Lets you monitor the critical user-defined files that are specific to the Tru64 operating system. If you check this option, you must specify at least one path in the subsequent list. **Note:** Symantec recommends that you only use the Report File Differences option on a select number of files. If you enable the reporting of file differences for a large number of files, that is, more than 1000, it may affect system resources. Symantec recommends that you test scenarios if large numbers of files require this detection functionality or if wildcard paths are used with this feature.

System Symantec Software Monitor

This option group area of the policy contains monitoring functions for Symantec software. Currently the monitored ancillary application is Symantec AntiVirus for Linux. The policy automatically detects if the host machine has Symantec AntiVirus for Linux installed.

Table 2-100 Description of the **Virus Detected** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Virus Detected
Rule Name	Virus_Detected
Severity	Critical
Description	Detects the discovery of a virus or Trojan horse by Symantec AntiVirus for Linux. This detection indicates that malicious software has arrived at the client side by email, download, document macro, or by disk-to-disk transfer. Immediate action is usually warranted.

Table 2-101 Description of the **Service Stopped** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Service Stopped

Table 2-101 Description of the **Service Stopped** parameters used *(continued)*

Parameter	Description
Rule Name	Service_Stopped
Severity	Warning
Description	Detects the stopping of the Symantec AntiVirus for Linux service. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the Symantec AntiVirus service has stopped, it reports this status.

Table 2-102 Description of the **Service Started** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Service Started
Rule Name	Service_Started
Severity	Notice
Description	Detects the starting of the Symantec AntiVirus for Linux service. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the Symantec AntiVirus service has started, it reports this status.

Table 2-103 Description of the **Scan Started** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Scan Started
Rule Name	Scan_Started
Severity	Notice
Description	Detects the starting of a manual scan of a host with Symantec AntiVirus for Linux. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that it has initiated a manual scan of the host, it reports this status.

Table 2-104 Description of the **Scan Canceled** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Scan Canceled
Rule Name	Scan_Canceled
Severity	Warning
Description	Detects the canceling of a manual scan of a host with Symantec AntiVirus for Linux. Symantec AntiVirus issues the status messages for various application conditions. When Symantec AntiVirus determines that it has been commanded to cancel a manual scan, it reports this status.

Table 2-105 Description of the **Scan Complete** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Scan Complete
Rule Name	Scan_Complete
Severity	Notice
Description	Detects the completion of a manual scan of a host with Symantec AntiVirus for Linux. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that it has successfully completed a manual scan, it reports this status.

Table 2-106 Description of the **New Virus Definition Loaded** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	New Virus Definition Loaded
Rule Name	New_Virus_Defintion_Loaded
Severity	Notice

Table 2-106 Description of the **New Virus Definition Loaded** parameters used *(continued)*

Parameter	Description
Description	Detects the updating of Symantec AntiVirus for Linux with the latest virus definitions. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that it has loaded a new virus definition file, it reports this status.

Table 2-107 Description of the **Virus Definitions are Current** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Virus Definitions are Current
Rule Name	Virus_Definitions_are_Current
Severity	Notice
Description	Detects that the installed virus definitions are current. Symantec AntiVirus for Linux issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the definitions are current, it reports this status.

Table 2-108 Description of the **Realtime Protection Loaded** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Realtime Protection Loaded
Rule Name	Realtime_Protection_Loaded
Severity	Notice
Description	Detects the disabling of the Symantec AntiVirus for Linux real-time system protection option. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the real-time protection option has been disabled, it reports this status.

Table 2-109 Description of the **Realtime Protection Disabled** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Realtime Protection Disabled
Rule Name	Realtime_Protection_Disabled
Severity	Critical
Description	Detects the disabling of the Symantec AntiVirus for Linux real-time system protection option. Symantec AntiVirus issues the status messages for various application conditions and errors. When Symantec AntiVirus determines that the real-time protection option has been disabled, it reports this status.

Table 2-110 Description of the **Virus Detected - Cleaned Failed** parameters used

Parameter	Description
Option Path	System Symantec Software Monitor > Symantec AntiVirus for Linux (SAVFL) Client Communication
Option	Virus Detected - Cleaned Failed
Rule Name	Virus_Detected_Cleaned_Failed
Severity	Critical
Description	Detects the discovery of a virus or Trojan horse by Symantec AntiVirus for Linux. This detection indicates that malicious software has arrived at the client side by email, download, document macro, or by disk-to-disk transfer. This event indicates Symantec AntiVirus client was unable to clean, remove, or quarantine the identified malware and the risk is still present on the system. Immediate investigation is required.

System External Device Activity Monitor

This option group subsection monitors for specific external device activity such as the various activities that are associated with USB devices. This activity should be monitored on an enterprise network, as such devices may pose the threat of data loss.

Table 2-111 Description of the **USB Device Connected** parameters used

Parameter	Description
Option Path	System External Device Activity Monitor > USB Device Activity
Option	USB Device Connected
Rule Name	USB_Device_Connected
Severity	Warning
Description	Detects a USB device connection event from the UNIX syslog.

Table 2-112 Description of the **USB Device Disconnected** parameters used

Parameter	Description
Option Path	System External Device Activity Monitor > USB Device Activity
Option	USB Device Disconnected
Rule Name	USB_Device_Disconnected
Severity	Warning
Description	Detects a USB device disconnection event from the UNIX syslog.

Table 2-113 Description of the **USB Device Additional Activity** parameters used

Parameter	Description
Option Path	System External Device Activity Monitor > USB Device Activity
Option	USB Device Additional Activity
Rule Name	USB_Device_Additional
Severity	Warning
Description	Detects user-defined USB device-related activities from the UNIX syslog.

System Attack Detection

This option group subsection contains basic Web attack monitoring criteria to thwart basic attacks on any Web server that produces any kind of access log.

The global settings area consists of the following:

- Alert only on Success Attack Attempt (Code 200): This area configures all the attack detection rules to look for the trailing code 200 when a suspicious string is found in the access log. Trailing code 200 means a successful process request. This setting dramatically decreases the amount of false positives and provides administrators with events that are considered processed by the hosting system.
- Web Access Log File Path: This area configures the Web access log path, which the rules in this policy subsection sift through to find malicious request strings. Symantec Critical System Protection provides a default location for the Apache Web server HTTP access log. Symantec recommends that you research which path location is best for this portion of the policy, since other Web server packages may be configured with different HTTP access log paths..

  Note: The log format must follow W3C guidelines.

- Whitelisted IP Addresses: This area configures the IP addresses that are allowed or otherwise ignored in this monitoring subsection. These IP addresses are for tools like automated vulnerability scanning systems on enterprise networks, where you know that at regular intervals Web attack tests occur.
- Blacklisted IP Addresses: This area configures the IP addresses that are not allowed access to the host system. Blacklisted IP addresses may be any addresses outside an internal network range if this area monitored an intranet Web host. Blacklisted IP addresses may also be known bad IP addresses from any of the blacklists available on the Internet.
- IIS HTTP Success Code: The IIS HTTP Success Code is the trailing HTTP code on all requests that signifies that the request has been successfully processed on the host Web system. A success code that is paired with a maliciously crafted URI string would indicate a possible compromised system.
- IIS HTTP Error Code: The IIS HTTP Error Code is the HTTP error code that signifies a bad HTTP request. A high frequency repeating number of these found in the access log signifies that a possible Web vulnerability scan is occurring.

Generic Web Attack Detection Options

Table 2-114 Description of the **Generic VA Scan Attempt** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic VA Scan Attempt
Rule Name	WebAttackDetection_Generic_VAScan
Severity	Warning
Invalid Count	20 Times in which a 404 or unknown request is received.
Invalid Interval	2 minutes Time frequency in which invalid count needs to occur to trigger event.
Description	Detects a possible VA scan by triggering an event within a specific administrator-defined threshold. If Symantec Critical System Protection receives a specified number of 404 error codes by a user-defined frequency, then this rule generates an alert on a possible VA scan attempt.

Table 2-115 Description of the **Generic Blacklisted IP Request Attempts** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic Blacklisted IP Request Attempts
Rule Name	Baseline_WebAttackDetection_Generic_BlackListedIP
Severity	Warning
Description	A simple rule that detects the access attempt by a blacklisted IP address that is found in the HTTP access log. You configure the blacklisted IP address in the Global Settings area. If you enable this rule, any attempt by the predefined blacklisted IP address generates an event.

Table 2-116 Description of the **Generic SQL Injection Attack Attempts** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic SQL Injection Attack Attempts
Rule Name	Baseline_WebAttackDetection_Generic_SQLInjection
Severity	Warning
Description	Detects the very simple and generic SQL injection-type attacks when it monitors the HTTP access log file. Primary and secondary select logic is used to ensure that accurate rule tuning can occur. You can customize this area to your needs to add further SQL injection measures.

Table 2-117 Description of the **Generic Directory Transversal Attempts** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic Directory Transversal Attempts
Rule Name	Baseline_WebAttackDetection_Generic_DirTransversal
Severity	Warning
Description	Detects possible directory transversal attempts in HTTP request strings. The generic strings for directory transversal attempts are provided. An individual or script attempting to transverse directories by HTTP request may be considered a malicious action.

Table 2-118 Description of the **Generic Malicious User Agent Request Attempts** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic Malicious User Agent Request Attempts
Rule Name	Baseline_WebAttackDetection_Generic_MaliciousUserAgent

Table 2-118 Description of the **Generic Malicious User Agent Request Attempts** parameters used *(continued)*

Parameter	Description
Severity	Warning
Description	Detects the malicious user agent strings in HTTP requests. Automated scripts commonly use bad user agents in large-scale attacks. Pre-scripted suites of programs also use them to attack a Web server. The presence of these known-bad user agent strings may indicate a malicious attempt to access your host Web system.

Table 2-119 Description of the **Generic Unwanted Extension Requests** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic Unwanted Extension Requests
Rule Name	Baseline_WebAttackDetection_Unwanted_Extension_Request
Severity	Warning
Description	Detects the unwanted or suspicious extension requests. Files that are requested with the extensions configured in this rule may indicate a malicious script or user. You can add or remove extensions in this area to customize this event per host system environment.

Table 2-120 Description of the **Generic Unwanted Directory Requests** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic Unwanted Directory Requests
Rule Name	Baseline_WebAttackDetection_Unwanted_Directory_Request
Severity	Warning
Description	Detects the unwanted or suspicious directory requests. Directory requests as configured in this rule may indicate a malicious script or user. You can add or remove sensitive directory paths in this area to customize this event per host system environment.

Table 2-121 Description of the **Generic Vulnerable CGI Requests** parameters used

Parameter	Description
Option Path	System Attack Detection > Web Attack Detection Options > Generic Web Attack Detection Options
Option	Generic Vulnerable CGI Requests
Rule Name	WebAttackDetection_Generic_VulnerableCGIRequest
Severity	Warning
Description	Detects the unwanted or suspicious CGI and script requests. CGI and script requests as configured in this rule may indicate a malicious script or user. You can add or remove sensitive directory paths in this area to customize this event per host system environment.

UNIX Rootkit File / Directory Detection

A global settings area sets the following parameters for all rules in the UNIX Rootkit File / Directory Detection area:

- A Polling Interval option controls the interval in which the software polls or checks the files and directories that are configured for change monitoring. This option is available to enable tuning of how frequently files and directories are polled for changes. You may want to adjust the default polling rate if your environment has a large number of files and directories to be monitored. This adjustment helps to ensure that resources are not overly used for the engine. A drop-down selection criteria area is provided to easily switch polling interval frequency.
- A Monitor Checksums option is available to enable the monitoring of a file's checksum during a file modification event. It reports the real-time SHA-256 hash comparison to the Symantec Critical System Protection console under the Event details. This option also enables the monitoring of file checksums as calculated at agent startup. It determines whether the file was modified since Symantec Critical System Protection was last shut down. This option provides detection ability even if the Symantec Critical System Protection service or daemon is shut down. If a monitored file is changed, once the Symantec Critical System Protection service or daemon is started, it compares the files in its monitored list to when it was shut down. Any differences are reported to the console.

Table 2-122 Description of the **Bash Door** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Bash Door
Rule Name	Rootkit_Detection_BashDoor
Severity	Critical
Monitor Paths	/tmp/mcliZokhb /tmp/mclzaKmfa
Description	Detects rootkit activity.

Table 2-123 Description of the **VOLC Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	VOLC Rootkit
Rule Name	Rootkit_Detection_VOLC
Severity	Critical
Monitor Paths	/usr/lib/volc
Description	Detects rootkit activity.

Table 2-124 Description of the **Illogic Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Illogic Rootkit
Rule Name	Rootkit_Detection_Illogic
Severity	Critical
Monitor Paths	/etc/ld.so.hash /lib/security/.config /usr/bin/sia
Description	Detects rootkit activity.

Table 2-125 Description of the **T0rn Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	T0rn Rootkit
Rule Name	Rootkit_Detection_T0rn
Severity	Critical
Monitor Paths	/etc/ttyhash /lib/ldlib.tk /sbin/xlogin /usr/info/.T0rn /usr/src/.puta /var/run/...dica
Description	Detects rootkit activity.

Table 2-126 Description of the **RK17 Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	RK17 Rootkit
Rule Name	Rootkit_Detection_RK17
Severity	Critical
Monitor Paths	/bin/rtty /bin/squit /sbin/pback /usr/src/linux/modules/autod.o /usr/src/linux/modules/soundx.o
Description	Detects rootkit activity.

Table 2-127 Description of the **RSHA Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection

Table 2-127 Description of the **RSHA Rootkit** parameters used *(continued)*

Parameter	Description
Option	RSHA Rootkit
Rule Name	Rootkit_Detection_RSHA
Severity	Critical
Monitor Paths	/etc/rc.d/arch/alpha/lib/.lib/* /etc/rc.d/rsha/* /usr/bin/chsh2 /usr/bin/kr4p /usr/bin/n3tstat /usr/bin/slice2
Description	Detects rootkit activity.

Table 2-128 Description of the **RH-Sharpe Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	RH-Sharpe Rootkit
Rule Name	Rootkit_Detection_RHSharpe
Severity	Critical

Table 2-128 Description of the **RH-Sharpe Rootkit** parameters used *(continued)*

Parameter	Description
Monitor Paths	/bin/.lpstree /bin/.ps /bin/ldu /bin/lkillall /bin/lnetstat /usr/bin/.lpstree /usr/bin/.ps /usr/bin/cleaner /usr/bin/ldu /usr/bin/lkillall /usr/bin/lnetstat /usr/bin/slice /usr/bin/vadim
Description	Detects rootkit activity.

Table 2-129 Description of the **Showtee Romaniam Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Showtee Romaniam Rootkit
Rule Name	Rootkit_Detection_Showteeromaniam
Severity	Critical
Monitor Paths	/usr/lib/.egcs /usr/lib/.kinetic /usr/lib/.wormie /usr/lib/libfl.so /usr/lib/liblog.o /usr/sbin/xntps
Description	Detects rootkit activity.

Table 2-130 Description of the **Optickit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Optickit Rootkit
Rule Name	Rootkit_Detection_Optickit
Severity	Critical
Monitor Paths	/usr/bin/xchk /usr/bin/xsf
Description	Detects rootkit activity.

Table 2-131 Description of the **Tele Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Tele Rootkit
Rule Name	Rootkit_Detection_Telekit
Severity	Critical
Monitor Paths	/dev/hda06 /usr/info/libc1.so
Description	Detects rootkit activity.

Table 2-132 Description of the **LRK Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	LRK Rootkit
Rule Name	Rootkit_Detection_LRK
Severity	Critical
Monitor Paths	/dev/ida/.inet /usr/lib/liblog.o
Description	Detects rootkit activity.

Table 2-133 Description of the **ADORE Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	ADORE Rootkit
Rule Name	Rootkit_Detection_Adore
Severity	Critical
Monitor Paths	/etc/bin/ava /etc/sbin/ava
Description	Detects rootkit activity.

Table 2-134 Description of the **KNARK Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	KNARK Rootkit
Rule Name	Rootkit_Detection_Knark
Severity	Critical
Monitor Paths	/dev/.pizda /dev/.pula /proc/knark
Description	Detects rootkit activity.

Table 2-135 Description of the **BOBkit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	BOBkit Rootkit
Rule Name	Rootkit_Detection_Bobkit
Severity	Critical

Table 2-135 Description of the **BOBkit Rootkit** parameters used *(continued)*

Parameter	Description
Monitor Paths	/tmp/.bkp/* /usr/include/.../* /usr/lib/.../* /usr/lib/.bkit-/*
Description	Detects rootkit activity.

Table 2-136 Description of the **HID Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	HID Rootkit
Rule Name	Rootkit_Detection_Hid
Severity	Critical
Monitor Paths	/var/lib/games/.k
Description	Detects rootkit activity.

Table 2-137 Description of the **ARK Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	ARK Rootkit
Rule Name	Rootkit_Detection_ARK
Severity	Critical
Monitor Paths	/dev/ptyxx /usr/lib/.ark?
Description	Detects rootkit activity.

Table 2-138 Description of the **Mithra Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Mithra Rootkit
Rule Name	Rootkit_Detection_Mithra
Severity	Critical
Monitor Paths	/usr/sbin/uboot
Description	Detects rootkit activity.

Table 2-139 Description of the **LOC Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	LOC Rootkit
Rule Name	Rootkit_Detection_LOC
Severity	Critical
Monitor Paths	/tmp/kidd0 /tmp/kidd0.c /tmp/xp /usr/lib/libmen.oo/.LJK2
Description	Detects rootkit activity.

Table 2-140 Description of the **Anonoiyng Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Anonoiyng Rootkit
Rule Name	Rootkit_Detection_Anonoiyng
Severity	Critical
Monitor Paths	/usr/sbin/kswapd /usr/sbin/mech

Table 2-140 Description of the **Anonoiyng Rootkit** parameters used *(continued)*

Parameter	Description
Description	Detects rootkit activity.

Table 2-141 Description of the **ZK Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	ZK Rootkit
Rule Name	Rootkit_Detection_ZK
Severity	Critical
Monitor Paths	/etc/sysconfig/console/load.zk
Description	Detects rootkit activity.

Table 2-142 Description of the **S-it Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	S-it Rootkit
Rule Name	Rootkit_Detection_Sit
Severity	Critical
Monitor Paths	/dev/sdhu0/tehdrakg/* /etc/rc.d/rc?.d/S23kmdac /lib/.x /lib/sk
Description	Detects rootkit activity.

Table 2-143 Description of the **F-it Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	F-it Rootkit

Table 2-143 Description of the **F-it Rootkit** parameters used *(continued)*

Parameter	Description
Rule Name	Rootkit_Detection_Fit
Severity	Critical
Monitor Paths	/dev/proc/fuckit/* /dev/proc/system-bins/init
Description	Detects rootkit activity.

Table 2-144 Description of the **Beastkit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Beastkit Rootkit
Rule Name	Rootkit_Detection_Beastkit
Severity	Critical
Monitor Paths	lib/ldd.so/bktools /usr/l/bin/idrun /usr/local/bin/.../bktd /usr/sbin/arobia/*
Description	Detects rootkit activity.

Table 2-145 Description of the **Tuxkit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Tuxkit Rootkit
Rule Name	Rootkit_Detection_Tuxkit
Severity	Critical
Monitor Paths	/dev/tux
Description	Detects rootkit activity.

Table 2-146 Description of the **Kenga3 Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Kenga3 Rootkit
Rule Name	Rootkit_Detection_Kenga3
Severity	Critical
Monitor Paths	/usr/include/..
Description	Detects rootkit activity.

Table 2-147 Description of the **ESRK Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	ESRK Rootkit
Rule Name	Rootkit_Detection_ESRK
Severity	Critical
Monitor Paths	/usr/lib/tcl5.3
Description	Detects rootkit activity.

Table 2-148 Description of the **FU Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	FU Rootkit
Rule Name	Rootkit_Detection_FU
Severity	Critical
Monitor Paths	/sbin/xc /usr/include/ivtype.h
Description	Detects rootkit activity.

Table 2-149 Description of the **SHKit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	SHKit Rootkit
Rule Name	Rootkit_Detection_Shkit
Severity	Critical
Monitor Paths	/etc/ld.so.hash /lib/security/.config
Description	Detects rootkit activity.

Table 2-150 Description of the **Ajakit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Ajakit Rootkit
Rule Name	Rootkit_Detection_Ajakit
Severity	Critical
Monitor Paths	/lib/.libgh-gh
Description	Detects rootkit activity.

Table 2-151 Description of the **zaRwT Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	zaRwT Rootkit
Rule Name	Rootkit_Detection_zaRwT
Severity	Critical
Monitor Paths	/bin/imin /bin/imout
Description	Detects rootkit activity.

Table 2-152 Description of the **Madalin Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Madalin Rootkit
Rule Name	Rootkit_Detection_Madalin
Severity	Critical
Monitor Paths	/usr/include/iceconf.h /usr/include/icekey.h /usr/include/iceseed.h
Description	Detects rootkit activity.

Table 2-153 Description of the **BMBL Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	BMBL Rootkit
Rule Name	Rootkit_Detection_BMBL
Severity	Critical
Monitor Paths	/etc/.bmbl /etc/.bmbl/sk
Description	Detects rootkit activity.

Table 2-154 Description of the **aPa Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	aPa Rootkit
Rule Name	Rootkit_Detection_aPa
Severity	Critical
Monitor Paths	/usr/share/.aPa
Description	Detects rootkit activity.

Table 2-155 Description of the **Enye-Sec Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Enye-Sec Rootkit
Rule Name	Rootkit_Detection_EnyeSec
Severity	Critical
Monitor Paths	/etc/.enyelkmHIDE^IT.ko
Description	Detects rootkit activity.

Table 2-156 Description of the **Override Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Override Rootkit
Rule Name	Rootkit_Detection_Override
Severity	Critical
Monitor Paths	/dev/grid-hide-pid- /dev/grid-hide-port- /dev/grid-show-pids /dev/grid-show-port- /dev/grid-unhide-pid-
Description	Detects rootkit activity.

Table 2-157 Description of the **PHALANX Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	PHALANX Rootkit
Rule Name	Rootkit_Detection_PHALANX
Severity	Critical

Table 2-157 Description of the **PHALANX Rootkit** parameters used *(continued)*

Parameter	Description
Monitor Paths	/bin/host.ph1 /etc/host.ph1 /usr/share/.home/ph1
Description	Detects rootkit activity.

Table 2-158 Description of the **Monkit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Monkit Rootkit
Rule Name	Rootkit_Detection_Monkit
Severity	Critical
Monitor Paths	/lib/defs /usr/lib/libpikapp.a
Description	Detects rootkit activity.

Table 2-159 Description of the **Balaur Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Balaur Rootkit
Rule Name	Rootkit_Detection_Balaur
Severity	Critical
Monitor Paths	/usr/lib/.egcs /usr/lib/.kinetic /usr/lib/.wormie
Description	Detects rootkit activity.

Table 2-160 Description of the **Bex2 Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Bex2 Rootkit
Rule Name	Rootkit_Detection_Bex2
Severity	Critical
Monitor Paths	/usr/include/bex
Description	Detects rootkit activity.

Table 2-161 Description of the **Dreams Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Dreams Rootkit
Rule Name	Rootkit_Detection_Dreams
Severity	Critical
Monitor Paths	/dev/ida/.hpd /dev/ttyoa /dev/ttyof /dev/ttyop /usr/bin/logclear /usr/bin/sense /usr/bin/sl2 /usr/lib/libsss
Description	Detects rootkit activity.

Table 2-162 Description of the **HJC Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	HJC Rootkit

Table 2-162 Description of the **HJC Rootkit** parameters used *(continued)*

Parameter	Description
Rule Name	Rootkit_Detection_hjc
Severity	Critical
Monitor Paths	/dev/hijackerz
Description	Detects rootkit activity.

Table 2-163 Description of the **Duarawkz Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Duarawkz Rootkit
Rule Name	Rootkit_Detection_Duarawkz
Severity	Critical
Monitor Paths	/usr/bin/duarawkz
Description	Detects rootkit activity.

Table 2-164 Description of the **Oz Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Oz Rootkit
Rule Name	Rootkit_Detection_Oz
Severity	Critical
Monitor Paths	/dev/.oz/.nap/rkit/terror
Description	Detects rootkit activity.

Table 2-165 Description of the **Portacelo Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Portacelo Rootkit

Table 2-165 Description of the **Portacelo Rootkit** parameters used *(continued)*

Parameter	Description
Rule Name	Rootkit_Detection_Portacelo
Severity	Critical
Monitor Paths	/var/lib/.../.ak /var/lib/.../.getty /var/lib/.../.hk /var/lib/.../.p /var/lib/.../.rs /var/lib/.../sssh_known_hosts
Description	Detects rootkit activity.

Table 2-166 Description of the **Slapper Bot Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Slapper Bot Rootkit
Rule Name	Rootkit_Detection_SlapperBot
Severity	Critical
Monitor Paths	/tmp/.b /tmp/.cinik /tmp/.font-unix-cinik
Description	Detects rootkit activity.

Table 2-167 Description of the **Scalper Bot Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Scalper Bot Rootkit
Rule Name	Rootkit_Detection_ScalperBot
Severity	Critical

Table 2-167 Description of the **Scalper Bot Rootkit** parameters used *(continued)*

Parameter	Description
Monitor Paths	/tmp/.a /tmp/.uua
Description	Detects rootkit activity.

Table 2-168 Description of the **Flea Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Flea Rootkit
Rule Name	Rootkit_Detection_Flea
Severity	Critical
Monitor Paths	/usr/lib/ldlibct.so /usr/lib/ldlibdu.so /usr/lib/ldlibns.so /usr/lib/ldlibpst.so
Description	Detects rootkit activity.

Table 2-169 Description of the **Ignokit Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Ignokit Rootkit
Rule Name	Rootkit_Detection_Ignokit
Severity	Critical
Monitor Paths	/lib/defs/p /lib/defs/q /lib/defs/r /lib/defs/s /lib/defs/t /usr/lib/.libigno/pkunsec

Table 2-169 Description of the **Ignokit Rootkit** parameters used *(continued)*

Parameter	Description
Description	Detects rootkit activity.

Table 2-170 Description of the **Ni0 Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Ni0 Rootkit
Rule Name	Rootkit_Detection_Ni0
Severity	Critical
Monitor Paths	/tmp/waza /var/lock/subsys/...datafile.../*
Description	Detects rootkit activity.

Table 2-171 Description of the **Devil Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	DevilRootkit
Rule Name	Rootkit_Detection_Devil
Severity	Critical
Monitor Paths	/dev/caca /dev/dsx /var/lib/games/.src
Description	Detects rootkit activity.

Table 2-172 Description of the **Redstorm Rootkit** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX Rootkit File / Directory Detection
Option	Redstorm Rootkit

Table 2-172 Description of the **Redstorm Rootkit** parameters used *(continued)*

Parameter	Description
Rule Name	Rootkit_Detection_Redstorm
Severity	Critical
Monitor Paths	/bin/... /var/log/tk02/see_all
Description	Detects rootkit activity.

UNIX WormFile / Directory Detection

A global settings area sets the following parameters for all rules in the UNIX WormFile / Directory Detection area:

- A Polling Interval option controls the interval in which the software polls or checks the files and directories that are configured for change monitoring. This option is available to enable tuning of how frequently files and directories are polled for changes. You may want to adjust the default polling rate if your environment has a large number of files and directories to be monitored. This adjustment helps to ensure that resources are not overly used for the engine. A drop-down selection criteria area is provided to easily switch polling interval frequency.
- A Monitor Checksums option is available to enable the monitoring of a file's checksum during a file modification event. It reports the real-time SHA-256 hash comparison to the Symantec Critical System Protection console under the Event details. This option also enables the monitoring of file checksums as calculated at agent startup. It determines whether the file was modified since Symantec Critical System Protection was last shut down. This option provides detection ability even if the Symantec Critical System Protection service or daemon is shut down. If a monitored file is changed, once the Symantec Critical System Protection service or daemon is started, it compares the files in its monitored list to when it was shut down. Any differences are reported to the console.

Table 2-173 Description of the **Adore Worm** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX WormFile / Directory Detection
Option	Adore Worm

Table 2-173 Description of the **Adore Worm** parameters used *(continued)*

Parameter	Description
Rule Name	Worm_Detection_AdoreWorm
Severity	Critical
Monitor Paths	/dev/.*/red.tgz /usr/bin/adore /usr/lib/libt /usr/sbin/adore
Description	Detects worm activity.

Table 2-174 Description of the **55808_A Worm** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX WormFile / Directory Detection
Option	55808_A Worm
Rule Name	Worm_Detection_55808aWorm
Severity	Critical
Monitor Paths	/tmp/.../a /tmp/.../r
Description	Detects worm activity.

Table 2-175 Description of the **Sadmind Worm** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX WormFile / Directory Detection
Option	Sadmind Worm
Rule Name	Worm_Detection_Sadmind
Severity	Critical
Monitor Paths	/dev/cuc
Description	Detects worm activity.

Table 2-176 Description of the **Omega Worm** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX WormFile / Directory Detection
Option	Omega Worm
Rule Name	Worm_Detection_Omega
Severity	Critical
Monitor Paths	/dev/chr
Description	Detects worm activity.

Table 2-177 Description of the **LDP Worm** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX WormFile / Directory Detection
Option	LDP Worm
Rule Name	Worm_Detection_LDP
Severity	Critical
Monitor Paths	/bin/.login /bin/.ps /dev/.kork
Description	Detects worm activity.

Table 2-178 Description of the **Lion Worm** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX WormFile / Directory Detection
Option	Lion Worm
Rule Name	Worm_Detection_LionWorm
Severity	Critical

Table 2-178 Description of the **Lion Worm** parameters used *(continued)*

Parameter	Description
Monitor Paths	/bin/mjy /dev/.lib /dev/.lib/lib/1i0n.sh /dev/.lib/lib/lib/dev/* /dev/.lib/lib/lib/netstat /dev/.lib/lib/scan/* /usr/man/man1/man1/lib/.lib/.x /usr/man/man1/man1/lib/.lib/in.telnetd /usr/man/man1/man1/lib/.lib/mjy
Description	Detects worm activity.

Table 2-179 Description of the **Cback Worm** parameters used

Parameter	Description
Option Path	System Attack Detection > UNIX WormFile / Directory Detection
Option	Cback Worm
Rule Name	Worm_Detection_CbackWorm
Severity	Critical
Monitor Paths	/tmp/cback /tmp/derfiq
Description	Detects worm activity.

Malicious Module Detection

A global settings area sets the following parameters for all rules in the UNIX Rootkit File / Directory Detection area:

- A Polling Interval option controls the interval in which the software polls or checks the files and directories that are configured for change monitoring. This option is available to enable tuning of how frequently files and directories are polled for changes. You may want to adjust the default polling rate if your environment has a large number of files and directories to be monitored. This adjustment helps to ensure that resources are not overly used for the engine.

A drop-down selection criteria area is provided to easily switch polling interval frequency.

- A Monitor Checksums option is available to enable the monitoring of a file's checksum during a file modification event. It reports the real-time SHA-256 hash comparison to the Symantec Critical System Protection console under the Event details. This option also enables the monitoring of file checksums as calculated at agent startup. It determines whether the file was modified since Symantec Critical System Protection was last shut down. This option provides detection ability even if the Symantec Critical System Protection service or daemon is shut down. If a monitored file is changed, once the Symantec Critical System Protection service or daemon is started, it compares the files in its monitored list to when it was shut down. Any differences are reported to the console.

Table 2-180 Description of the **Suspicious Loadable Kernel Module (LKM) Detection** parameters used

Parameter	Description
Option Path	System Attack Detection > Malicious Module Detection
Option	Suspicious Loadable Kernel Module (LKM) Detection
Rule Name	LKM_Suspicious_Module_Detection
Severity	Critical
Monitor Paths	/lib/adore_so /lib/cleaner_o /lib/flkm_o /lib/modules/adore_so /lib/phide_mod_o
Description	Detects suspicious activity related to Loadable Kernel Modules.

Suspicious Permission Change Detection

Table 2-181 Description of the **Suspicious Permission Change Detection** parameters used

Parameter	Description
Option Path	System Attack Detection
Option	Suspicious Permission Change Detection

Table 2-181 Description of the **Suspicious Permission Change Detection** parameters used *(continued)*

Parameter	Description
Rule Name	Suspicious_Perm_Change_Critical_Files
Severity	Critical
Monitor Paths	/bin/* /usr/bin/* /usr/local/bin*
Description	Detects suspicious changes in permissions in critical files and directories.